SHARP

SYNAPPX™

SYNAPPX™ MANAGE

Operation Guide

Contents

Introduction

Please Note

- This Operation Guide assumes that users have a working knowledge of Microsoft Windows® and the Internet. The images and procedures in this guide are taken from Windows® 10 and Google Chrome™. Other operating systems and browsers may display content differently. The screenshots and contents used in this Operation Guide may change without notice. (The information is as of April 2025.)
- This Operation Guide is intended to be used alongside the individual manuals for each MFP, printer, and display.
- To access the most up-to-date information regarding Synappx Manage software features not described in this guide, refer to the [Help] menu within Synappx Manage for a direct link to the official Synappx Manage website or view the Appendix Section [of this document]. Some strings may be displayed as hyperlinks in emails. Hyperlinks can be disabled in the client's email settings.

Cautions

The device information displayed on this service is subject to change based on network connectivity and data retrieval timing. Therefore, it may not always reflect the latest status of the device. The counter values displayed by this service may vary from the counter values at the time of polling.

It is important to note that this application and service do not guarantee the safety of the data being handled. Sharp Corporation does not take responsibility for any loss or corruption of data. It is advised that customers regularly back up all their data as a precautionary measure.

Glossary of Terms, Procedures, Icons, and Buttons

This Glossary reviews common procedures, buttons, and icons used throughout Synappx Manage, as well as parameters and restrictions for their use. Individual sections of this guide may include unique applications of these features when used with a specific function of the software. Detailed descriptions of these features can be found in their respective sections.

Terms

Agent: A program that works in the background to gather and report system data.
Application Programming Interface (API): The parts of a program with which the user interacts. Some elements of these can be customized to suit the user's needs.
IT Main: Role for customer IT administrators
Service Main: Role for guest administrators (service persons of Dealer or Direct channel)
Client ID: A unique identifier for a browser-device pair that links a client device to Google Workspace.
Synappx Go: One of the Synappx brand services to which Synappx Manage belongs. It brings consistent meeting experiences across personal devices with enhanced security capability for IT. For more information, refer to the official website.
Domain Alias: A custom name admins give to domains so users can quickly identify them.
Groups: Devices and displays can be organized into Groups
Instance: A single copy of a program.
IP Address: IP address of the device/display to be registered
Password: The password assigned to a display or device that allows the user to control its settings via Synappx Manage.
Port Number: Data communications TCP port number selected for the display (default value for "SSH" is 10022, otherwise, S-format: 10008, N-format: 7142)
Valid port numbers are between 1025~65535.
S-format: A unified remote control command system within the Sharp model display.
N-format: A unified remote control command system within the Sharp NEC Displays Solutions model display.
Security Policy: Specifies which devices are covered by which security measures. Security policies can be customized to a point, though some security procedures are mandatory in accordance with Sharp's Terms of Use. If these terms are not met, some functionality, like software and security updates, will be lost.
Silent Installation: If this setting is enabled, you can edit "Emulation" and "TCP/IP Port settings". These settings are applied automatically when the agent or print driver is installed.
Simple Filter: Used to filter results in the Device List by a variety of criteria, such as IP Address or Serial Number.
User Name (Display): The user name assigned to a display or device that allows the user to gain authorized access to control the device settings via Synappx Manage.

Note:
In the "MFP/Printer Management" section of this guide, MFPs and printers are referred to as "**devices**".

In the "Display Management" section of this guide, Sharp displays are referred to as "**displays**".

Icons

Icon	Name	Function
	Hide	Content will not be displayed (a string of dots will be displayed instead.) (default)
	Show	Content will be displayed.
	Trash	Deletes selected item(s)
	Add	Adds an item to a selected location
	Subtract/ Remove	Removes item from a selected location
	Actions	Opens a selection of available actions. Actions are specific to each item.
	Apply Filter	Used to apply the filter you set.
	Arrows (Up/Down)	Sort lists alphabetically in Ascending (Up) or Descending (Down) order.
	Refresh Device(s)	Updates the information with the latest information from the Synappx Manage server.
	Refresh Screen	Updates a field with latest information. Refreshes the browser page to bring the displayed content up to date.
	Status: Normal	Indicates the status of a process/item is functioning normally.
	Status: Error	Indicates a process/item is not functioning normally, experiencing a known error.
	Status: Warning	Indicates the status of a process/item is functioning with attention required.
	Status: Communication Error	The device is not communicating. However, the Status was Normal before communication was lost.
		The device is not communicating. However, the Status was Error before communication was lost.
		The device is not communicating. However, the Status was Warning before communication was lost.
	Checkboxes	Allow users to select multiple items when applying changes.
	Radio Button	Used to select one of several options.

	Device Web Page	Displays management page for a selected device.
	Remote Operation	Engages remote operation of a selected device.
	All Devices	Displays security device information for all registered devices.
	Download	Used to download data to the cloud or to a local folder.
	Delete File	Used to delete files temporarily stored in the cloud.
	DSK model	Represents DSK applied MFP.
	Registration Status: Imported Device	Indicates the device is imported by the system or service user via the device list. Disappears after the device is registered.

Buttons

Name	Function
Sleep	Power Management: Puts a selected device to sleep
Wake Up	Power Management: Wakes up a selected device
Reboot	Power Management: Reboots a selected device
Cancel	Exits dialog box, cancels current operation
Groups	Assigns a Group Name to a device
Apply Schedule	Sets the specified device(s) to perform operations, such as sleep and wake up, at scheduled times.
Remove Schedule	Removes the applied schedule operation from the specified device(s)
Columns	Allows user to add or remove columns displayed in the device list
Import/Export	Uploads/downloads a specific file.
Refresh Interval	Sets interval for automatic information updates
Show Filter/ Hide Filter	Show Filter button: Click to show Simple Filter in the list. Hide Filter button: Click to hide Simple Filter.
Change Input	Switches the input mode for registered devices.
Execute	Device Cloning/Storage Backup: Execute a function of these pages.
Item Selection	Device Cloning/Storage Backup: Select items to be copied.
Schedule List	Display a list of pre-defined schedules when you want a function to run periodically.

Conditions

Restoring deleted items

Synappx Manage does not have a restore function. Any files, events, logs, or other stored data deleted will be permanently deleted. Once deleted, all files, events, logs, or stored data are permanently removed. Only devices, can be restored if deleted, by re-registering them. While files and logs can be exported, they cannot be re-imported into Synappx Manage, once they have been deleted.

Filtering items for deletion

Only the filtered log events for the specified category will be deleted. For instance, if **Agent**

Management is selected, only the Agent Management related log events will be deleted. Other events (such as for the MFP/Printer Management or Power Management) will not be deleted.

Network Connection
The PC Synappx Manage Agent is installed on must be connected to the Internet and remain turned on. Sleep mode should be turned off to ensure the PC running the Agent remains in active operation.

Selecting single or multiple items to be edited/removed (checkboxes)
When selecting items from a list to apply changes, selecting checkboxes next to each device can apply changes to multiple selections simultaneously. Additionally, selecting the first checkbox in the title field selects all items in the list.

Searching Case Sensitivity
Searches are not case sensitive. For instance, searching "SHARP" and "Sharp" will yield the same results.

Filtering Lists
When the **Show Filter** button is displayed top right of a list, click the button and displayed simple filter in the first row of the list. Select the desired filtering criteria from the list.

Click the Apply Filter icon . For fields without a list icon , type in the filtering criteria directly. For example, to find devices with an IP address beginning with "172", type "172" into the "IP Address" field. Multiple filtering criteria can be entered. For instance, if you type "SHARP" into the "Model Name" field and "172" into the "IP Address" field, you can display only the devices which have both "SHARP" in their model name and "172" as part of their IP address.

Guidelines for Naming and Text Entry

User Names (Display)
Valid: A-Z, a-z, 0-9, hyphen ("-"), and underscore ("_").
Character Range: 1-8
Passwords
Valid: A-Z, a-z, 0-9, hyphen ("-"), and underscore ("_").
Character Range: 5-255
Note: The hardware password requirements follow each hardware's password specifications.
Print Driver Names
Valid: Single-byte, alphanumeric
Invalid: Space anywhere in name, blank field, line break, or any of the following characters: \/:*?"<>|
Character Range: 1-64
Device Type Names
Valid: Single-byte, alpha-numeric, Space, "-", and "_"
Blank is not allowed

Character Range: 1-64

Agent Names

Invalid: Credential name with only space is not allowed.
Any of the following characters: \/:*?"<>|
Blank is not allowed
Character Range: 1-64

Policy Name

Invalid: Name with only space is not allowed.
Any of the following characters: \/:*?"<>|
Blank is not allowed
Character Range: 1-64

Email

The destination for sending the created report via email. Multiple email addresses can be entered in the **Email Address** field with a delimiter character ";" or "," between each address.

Searching

Case sensitivity: Searches are NOT case sensitive. E.g., querying "SHARP" will yield the same results as "Sharp".

Note:
The PC that Synappx Manage Agent is installed on must be connected to the Internet and remain turned on. Sleep mode should be turned off to ensure the PC running the Agent remains in active operation.

Synappx Manage Overview

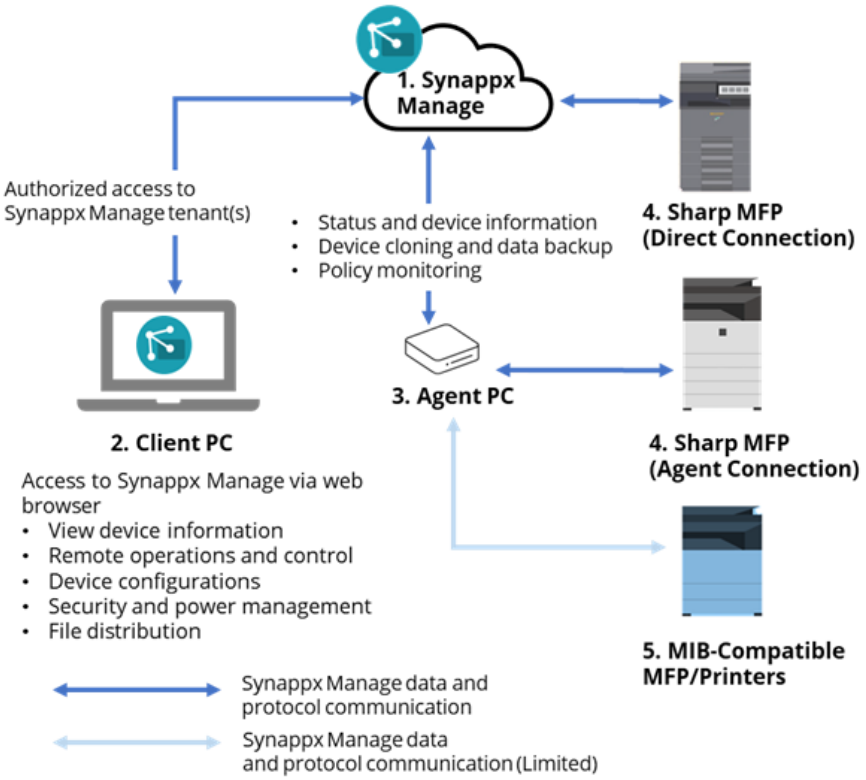
Synappx Manage is an end point management and monitoring service. It is designed for IT administrators and authorized Sharp service providers to remotely manage office products, such as Multifunctional Printers (MFPs) and displays, via the Synappx Admin Portal.

The key features of Synappx Manage include:

- Device discovery/registration
- Device information capture
- Device status and consumable monitoring
- Email alerts (MFPs/Printers)
- Remote configurations
- Cloning and storage backup (MFPs/Printers)
- Scheduled actions/tasks
- Security policy and power management (MFPs/Printers)
- Reporting and analytics (MFPs/Printers)

Managing Multifunction Machines and Printers

Synappx Manage provides status of registered devices in the device list. With the email notification feature, registered users can be notified when the device status is detected as “Warning” or “Error”. Other available features include cloning a device’s configuration file to other devices, accessing a device’s web page, and remotely controlling device settings such as power, security policy management, and more.



Synappx Manage MFP/Printer Monitoring Diagram

MFP/Printer (Device) Monitoring Features

1. Synappx Manage Cloud Service
   Establish authorized access to Synappx Manage tenants from client.
2. Client PC
   Access to Synappx Manage via web browser.
   - View device information
   - Remote operations and control
   - Device configurations
   - Security and power management
   - File distribution
3. Agent PC (when required)
   Establish secure communication between MFP/printer devices with Synappx Manage

- Status and device information
- Device cloning and data backup
- Policy monitoring
- Remote operation and control

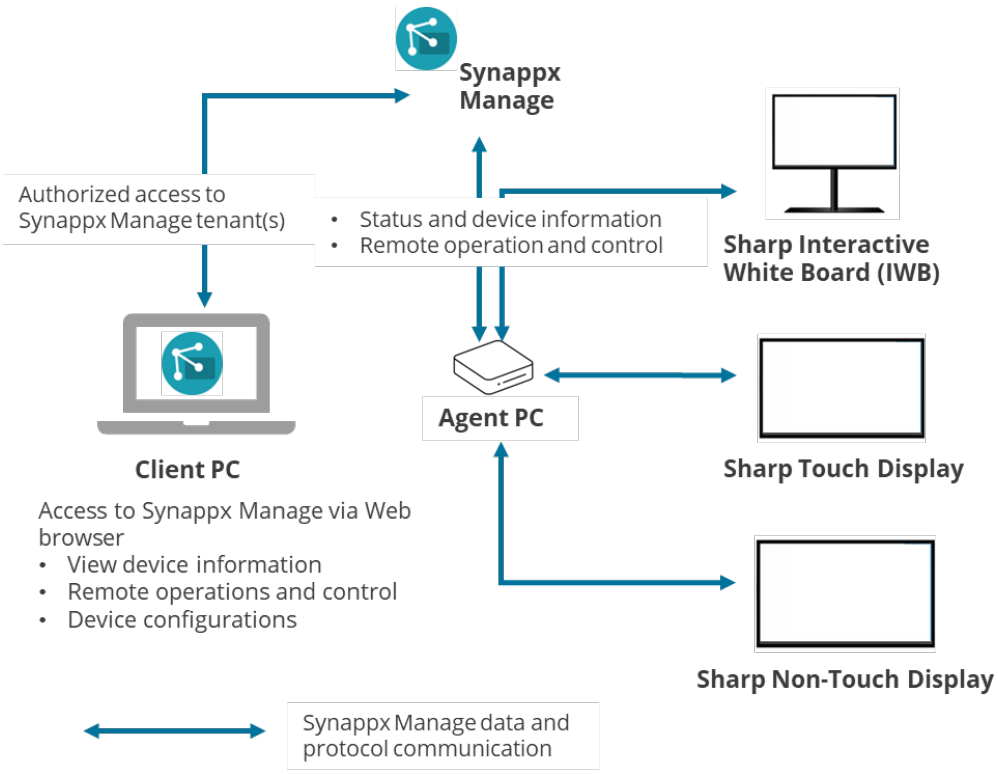
4. Sharp MFPs
   Target and registered MFPs and Printers. There are two methods to connect to Synappx Manage.
   - Agent Connection
   - Direct Connection
5. MIB-Compliant MFP/Printers
   Target and registered MFPs and Printers. Limited functionality for non-Sharp devices.

Notes:

- For differences and details on direct connection and agent connection, go to Device Connection Options.
- Scheduled operations can be used to acquire and update device information at regular intervals. For details, go to Updating Device Data in the "MFP/Printer Management" section of this guide.
- The device's HTTPS settings (server port) must be enabled to view device's web page using Synappx Manage. Target devices and client PCs must be connected to the same network to access device web pages.
- The device's Remote Operation Panel settings (server port) must be enabled to access the Operation Panel remotely using Synappx Manage.

Managing Displays

Synappx Manage helps IT administrators monitor status, capture information, and remotely access display's power management (wake up/sleep) and input modes.



Synappx Manage Display Monitoring Diagram

Display Monitoring Features:

(1) Synappx Manage Cloud Service
Establish authorized access to Synappx Manage tenants from client.

(2) Client PC
Access to Synappx Manage via web browser.
- View device information
- Remote operations and control (inc. power and input management)
- Device configurations

(3) Agent PC (the same agent PC can be used for MFPs and printers)
Establish secure communication between display devices with Synappx Manage.
- Status and device information
- Remote operation and control

(4) Sharp display devices
Target and registered display devices to be managed under Synappx Manage cloud service.

Notes:
To manage displays, the displays need to be connected to a network, and the **RS-232C/LAN Switching** communication setting must be set to **LAN**.

Scheduled operations can be used to acquire and update device information at set intervals. For details, refer to “Updating Device Data” in the “Display Management” section of this guide.

To view the device’s web pages using Synappx Manage, target devices and the client PCs must be connected to the same network.

System Requirements

Synappx Manage Major Components
1. Synappx Manage Agent (Windows OS) 2. Admin Portal 3. Cloud System (Microsoft® Azure)

A stable internet connection is required.

Microsoft 365® Service Plans	
Business	Microsoft 365 Business Basic/Standard/Premium
Enterprise	Microsoft 365 Enterprise E3/E5 Microsoft 365 Enterprise F1/F3
Education	Microsoft 365 Education A3/A5

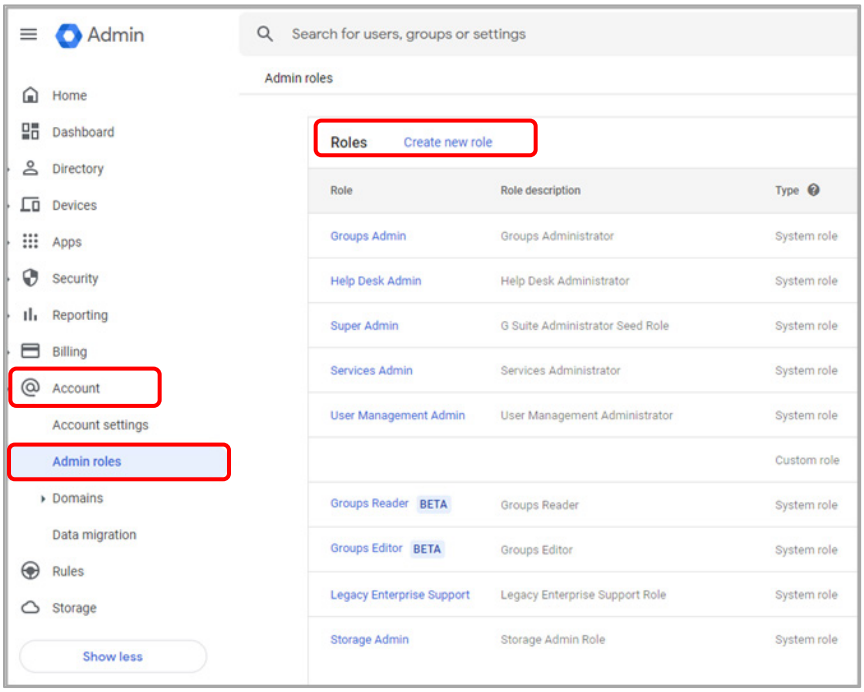
Google Workspace™ Service Plans
Business Starter
Business Standard
Business Plus
Enterprise

Synappx Manage Agent
• Microsoft Windows® 10 or 11 64-bit, Windows Server 2016 or 2019 or 2022 64-bit • Minimum 4GB RAM • Minimum 5GB disk space (Requirements can vary based on the number of logs that the Agent supports.) • Internet connectivity
Admin Portal
Browser-based: Google Chrome and Microsoft® Edge (latest versions)

Pre-Requisites for Google Workspace™ (IT Main Access)

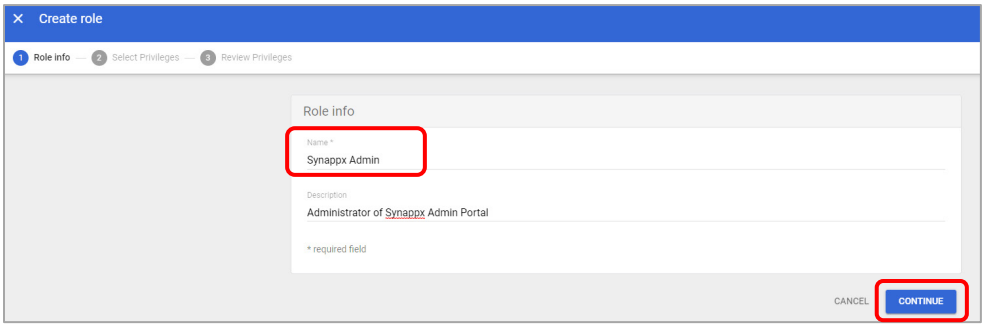
Before logging in to the Admin Portal, follow the steps described in the second welcome email to allow Synappx to communicate with your Google Workspace instance. This includes creating a custom scope for Google users who also need to configure or manage Synappx. The steps are shown below.

1. Select Google Workspace as your cloud service provider in the initial welcome email.
2. Upon receiving the second welcome email, follow the instructions to set up your Google Workspace Admin Console to communicate with Synappx.
3. In Chrome or Edge web browser, go to admin.google.com.
4. On the left menu, select **Account**. Select **Admin roles** and **Create new role**.



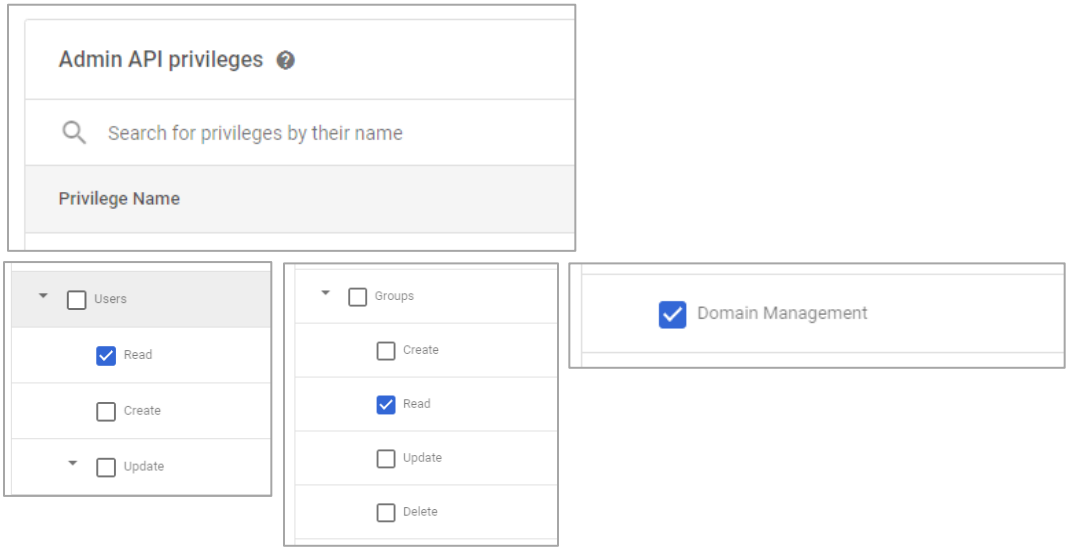
Create New Role

5. Enter custom role name (e.g. **Synappx Admin**) under **Role info**, add a description (if desired) and select **Continue**.



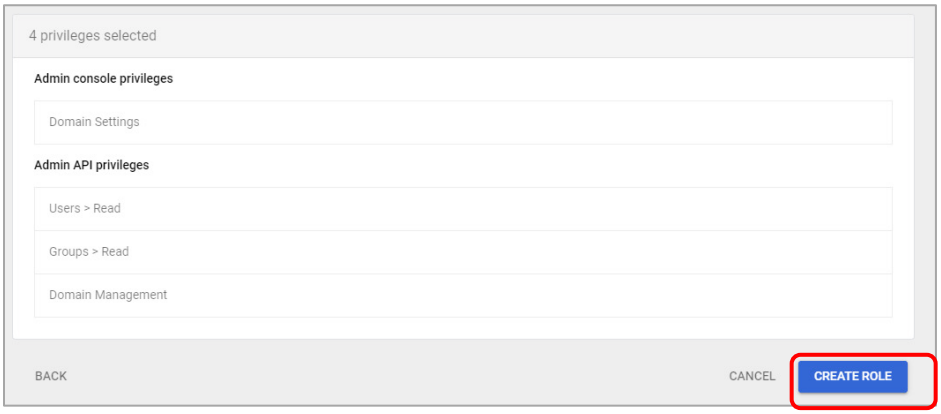
Naming New Synappx Admin Role

6. Scroll to **Admin API privileges**, scroll down or search to find three privileges below, configure as shown and select **Continue**.
    a. Enable **Users**, **Read**.
    b. Enable **Groups**, **Read**.
    c. Enable **Domain Management**.



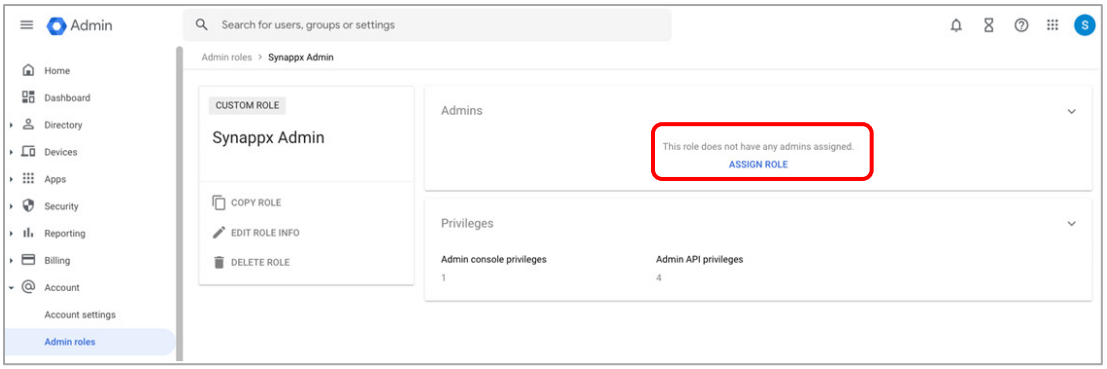
Required Admin APIs

7. Select **Create Role**.



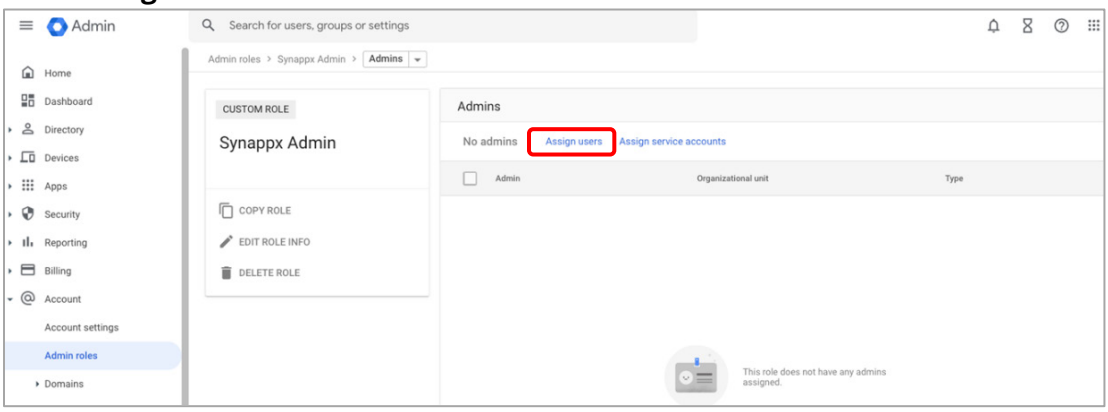
Summary of Selected APIs For New Role

*On the left menu, select **Account**, then **Admin roles**. Select the new custom role name (e.g. Synappx Admin), then click on **Assign Role**.*



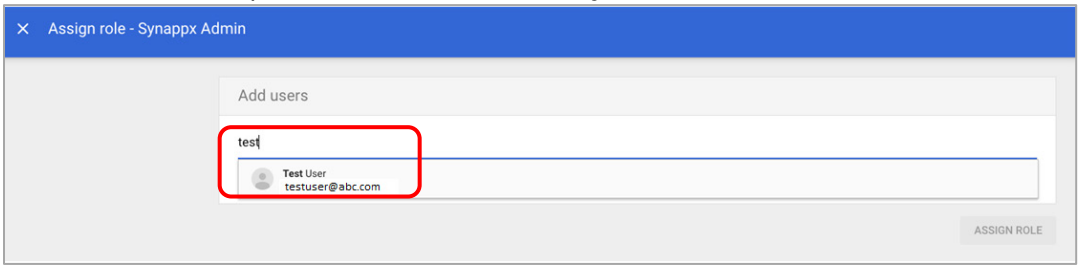
Assign New Role

8. Select **Assign Users**.



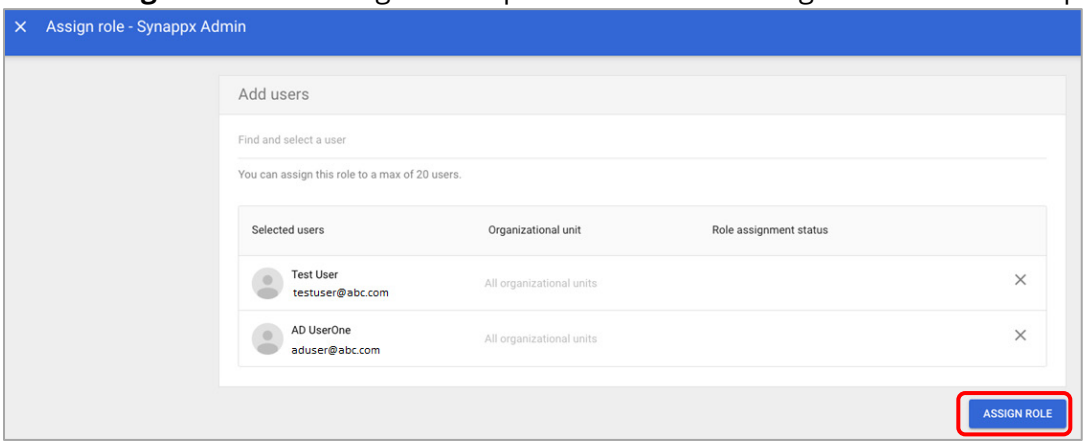
Assign Users to New Role

9. Type a few characters for each username you want to add for this custom role, select name from the dropdown and continue until you've added all the users.



Search and Add Users to New Role

10. Select **Assign Role**. The Google Workspace custom role configuration is now complete.



Shows Selected Users to Add to New Role

Synappx Manage Setup and Configuration Overview

Your authorized Sharp service provider will invite you to use Synappx Manage. Upon acceptance of the invitation, set up and configure Synappx Manage, following the steps below as well as those listed in the email. (Each step will be covered in more detail later in this section)

Step1: Choose Provider (applicable only to IT Main during the initial setup)

- Follow the directions in the welcome email to select Microsoft 365, Google Workspace or Custom Account as the identity provider.
- Follow the procedures in the confirmation email specific to Microsoft 365, Google Workspace or Custom Account.
    - Google Workspace: Create a custom role and assign it to others who is admins of Admin Portal (requires Google Workspace admin privileges).

Step2: Log in to the Admin Portal

- Use Microsoft 365, Google Workspace or Custom Account credentials to log in to the Admin Portal.
- Microsoft 365: First administrator requires Azure admin privileges to log in.
- Use Sharp-Start login if you are a service provider. (Synappx Manage role is required)

Step3: Device Connection Options

Select the device connection method, Agent Connection or Direct Connection. The device list can be imported via .CSV by Service Main role user.

Setup Agent Connection

- Create a new Agent to communicate with the Synappx Manage cloud.
- Download, install and configure the Agent software.

Setup Direct Connection

- Establish direct connection between device and Synappx Manage cloud service.

Step4: Register MFPs/Printers (Agent Connection)

- Perform device discovery to locate MFPs/printers connected to the network.
- Select the MFP/Printer to register with Synappx Manage.

Step5: Register Displays (Agent Connection)

- Perform device search to locate the displays connected to the network.
- Select and register the display connect to Synappx Manage.

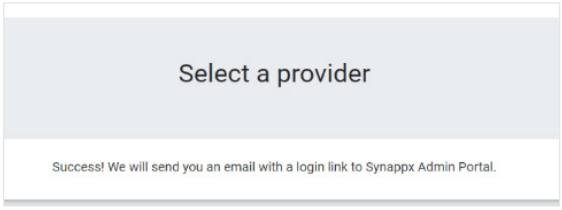
Note:
When changing the device connection on an MFP that is already connected and registered, delete the MFP in Synappx Manage and reregister the device.

The **Monitoring and Management** page for MFP/Printers may contain a list of devices that should be registered with Agent Connection or Direct Connection in advance.

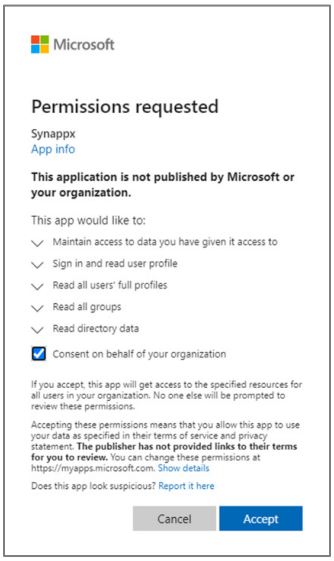
Choose Provider (Applicable only to IT administrators during the initial setup)

After a Synappx account is created for your organization, a user from your organization must be designated as the administrator. The administrator will receive an email with a link to select Microsoft 365, Google Workspace or Custom Account as an identity provider. The selected identity provider defines how Synappx manages the users within the organization.

Log in to the Admin Portal (IT Main)
The **Synappx Admin Portal** is a browser-based platform designed for administrators to manage key components (e.g., devices) of Synappx Manage. Administrators log in using the organization's Microsoft 365, Google Workspace account or Custom Account. It is recommended that the administrator use the latest version of Microsoft Edge™ or Google Chrome™. An administrator can log in to the Synappx Admin Portal via the link provided in the confirmation email.

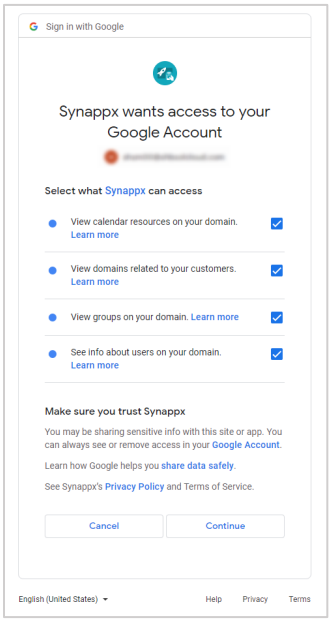


For Microsoft 365:
After the administrator selects Microsoft 365 as an identity provider, a confirmation email with a link to the Admin Portal will be sent to the administrator's inbox. Select the link and log in with Microsoft 365 credentials. At initial login, a permissions request prompt will appear on the screen. Select **Accept** to allow Synappx applications to access selected Microsoft services on behalf of your organization.



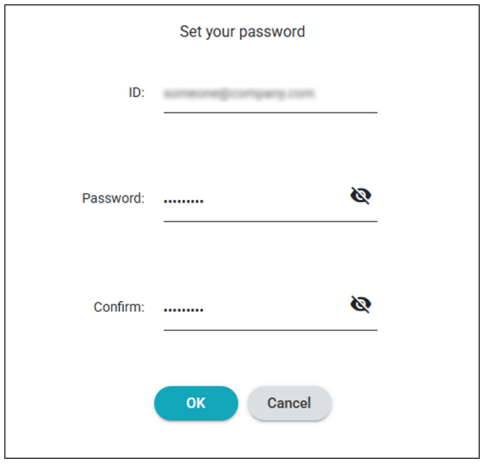
Microsoft Permission Request for Azure Global Admin

For Google Workspace™:
If the administrator selects Google Workspace as an identity provider and administrator is a Super Admin of Google Workspace, administrator can log in Admin Portal by granting permission like the image below. Please check each permission and select Continue. If the administrator is not a Super Admin of Google Workspace, a Super Admin must assign a custom role to administrator before administrator logs in to Admin Portal. After the custom role assignment, administrator logs in the same way as a Super Admin.



Google Workspace Permission

For Custom Account:
If the administrator selects Custom Account as the identity provider, a password setting screen will be displayed, once the password is created, a confirmation email with a link to the Admin Portal will be sent to the administrator's inbox. Select the link and log in with Admin Portal with Custom Account.

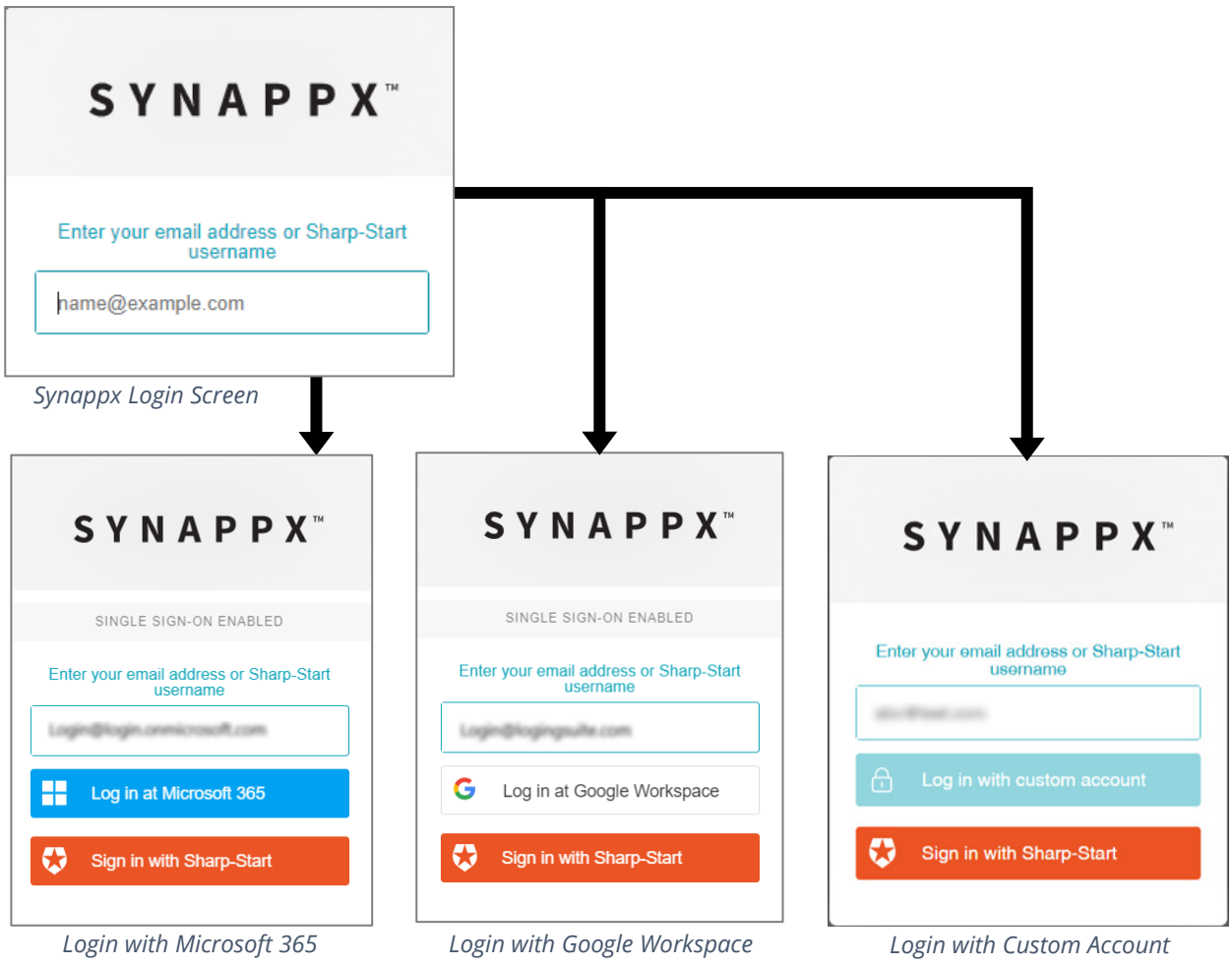


Set Your Password

Note:
Google Workspace admins must complete the Admin Console setup before logging in to the Admin Portal. The primary administrator must have admin privileges for Azure Active Directory or Google Workspace to authorize Synappx Manage features for users. Additional administrators must also have the same privileges as the administrator (Custom Role as described above). Sharp-Start login option is for service providers.

Login Process

1. Use your Microsoft 365, Google Workspace or Custom Account credentials to log in to the Synappx Admin Portal via the latest version of Google Chrome or Microsoft Edge. After typing your email in the Synappx login page, click **Log in to Microsoft 365** if you are using Microsoft credentials, **Log in at Google Workspace** if you are using Google credentials, or **Log in with custom account**. (Do not select "Sign with Sharp-Start", which is reserved for technical service login, a guest admin login)



Synappx Login Screen

Login with Microsoft 365

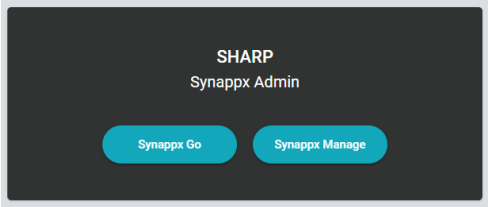
Login with Google Workspace

Login with Custom Account

2. **Microsoft 365**: Click **Accept**.
   Google Workspace: Check each permission and select **Continue**.
   Custom Account: Need no action.

   Note:
   Agreement with the Terms of Use is only required with the initial Admin Portal login agreement.

3. If Synappx Go service is subscribed, these options will appear in a pop-up window to select a service. Select **Synappx Manage**.

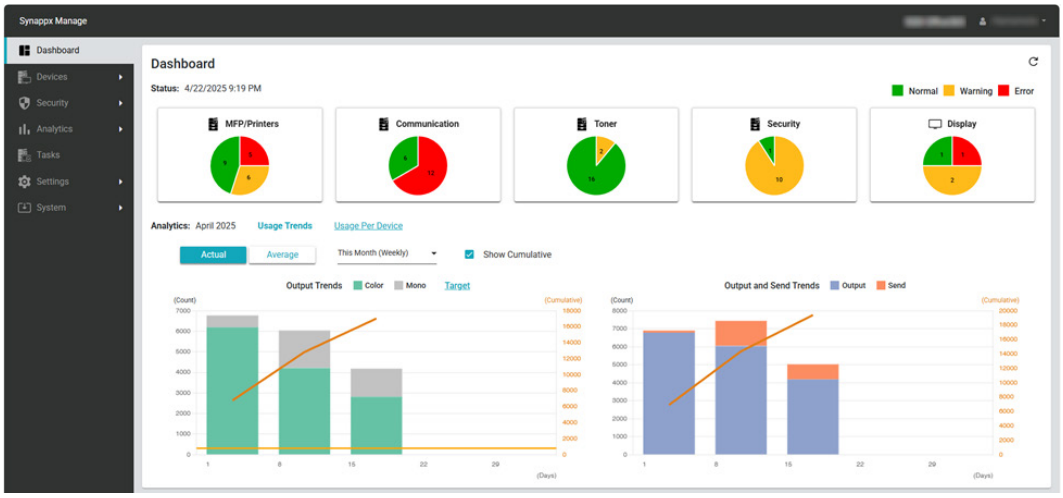


Synappx Service Selection

4. Review the **Terms of Use** (Synappx Privacy Policy) for Synappx Manage users (and Synappx Go if also licensed). These Terms of Use are only granted to users for Synappx application use.

5. Select **Agree** to continue.

The **Synappx Manage** homepage will appear.



Synappx Manage Homepage

Device Connection Options

There are two options to register MFP/printer in Synappx Manage. One is using a Synappx Manage agent installed on a local PC (Agent Connection). The other is to connect the MFP and Synappx Manage directly and register the MFP (Direct Connection). Select optimal connection method based on the following criteria. The device list can be preloaded, and once the devices connect to Synappx Manage, their information will automatically populate. The machine ID field is not editable once it is imported to Synappx Manage.

If any of the following conditions apply, an agent is required. Select via Agent Connection when you register the device.

- Managing display devices. The direct connection method is not yet supported on the display devices.
- Managing MFPs do not support the direct connection method. Go to Appendix: Direct connection supported models for direct connection supported models.

There are differences in the available functions and the process execution timing between direct connection and agent connection:

Functionality Difference

Equipment	Agent Connection	Direct Connection
PC for install agent	Required	Not required
Function	**Agent Connection**	**Direct Connection**
MFP Monitoring & Management	✓	✓
MFP Power Management (Sleep/Wake Up/Reboot)	✓	✓
Device Web Page	✓	✓
Remote Operation Panel	✓	Not applicable
Power & Input Schedules	✓	✓
Device Cloning	✓	✓
Storage Backup	✓	✓
Address Book	Not applicable	✓
Print Drivers	✓	✓
Firmware	✓	✓
Custom Device Types	✓	Not applicable
Display Related Features	✓	Not applicable

Timing Difference

In the agent connection, actions requested from the Synappx Manage are triggered immediately. In the direct connection, requested actions are triggered at MFP polling timing which is set every 60 mins to optimize network bandwidth and security efficiency.

Action Examples:

- Device Information Update (MFP/Printers)
- Power Management (MFP/Printers)
- Device Cloning
- Storage Backup
- Apply Security Policy
- Check Security Policy

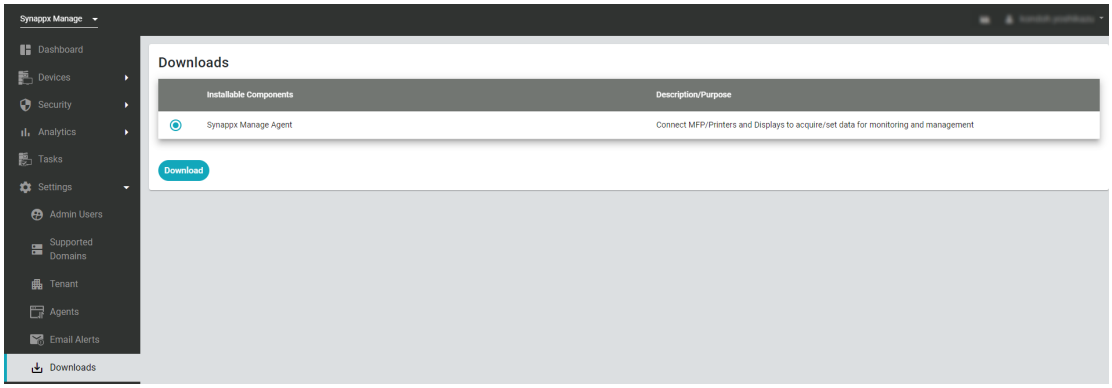
Agent Connection

Synappx Manage agent software can be installed on a local PC to establish connections with managed devices and Synappx Manage cloud service. Follow the steps below:

Step 1: Download Agent

Download the agent file using one of the following options:

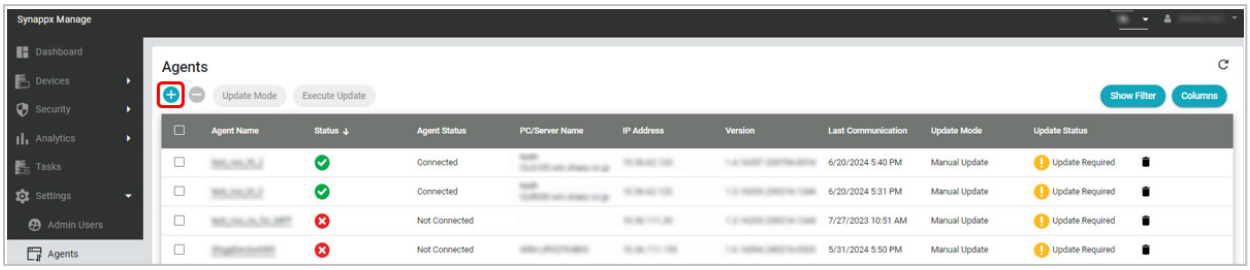
Option 1: On Downloads page



Downloads page

- Go to **Settings** in the Synappx Manage portal.
  On the **Downloads** page, click **Download** to open the **Agent Name Setting for Download Agent** dialog box.
- Input the Agent's name in the **Agent Name** field (64 characters or fewer) and click **OK** to open the Download Agent dialog box on the **Agent Settings** page.
- Download the agent file Sharp Synappx Manage Agent.zip, following dialogues and license agreement.

Option 2: On Agents page



Agents page

- Go to **Settings** in the Synappx Manage portal. On the **Agents** page, click the Add Agent icon ⊕ to open the Add Agent dialog box.
- Enter an agent name in the **Agent Name** field. (64 characters or fewer).
  The agent name will appear in the **Synappx Manage Agent Settings** dialog box.
- Click **Save**. The new agent will appear on the agent list.
- Click the registered agent name from the Agents list to open the **Agent Settings** page.
- Click **Download Agent** to open the **Download Agent** dialog box. Download the agent file Sharp Synappx Manage Agent.zip, following dialogues and license agreement.

  Note:
  If the Agent file cannot be downloaded, change the browser settings to allow pop-ups and redirects. The agent name displayed in the Synappx Manage Agent Settings box will not be updated when the agent name is changed in the **Agent Settings** page.

Step 2: Install and Activate Agent

A couple of steps are required to install and activate the agent to ensure secure communications. If a single agent is not sufficient to communicate with targeted devices, the communication range can be extended by installing multiple agents in one tenant. Follow the steps below to install and configure the agent:

Note:
The Synappx Manage Agent runs background services to communicate with devices. Therefore, the Agent PC or server must be turned on and running. Agents cannot operate while a computer is in sleep mode. The Synappx Manage Agent uses port 8088 for local communications. Ensure no other application on the agent PC/server is using port 8088.
To achieve optimal performance, additional Agent installs may be required for the following environments:

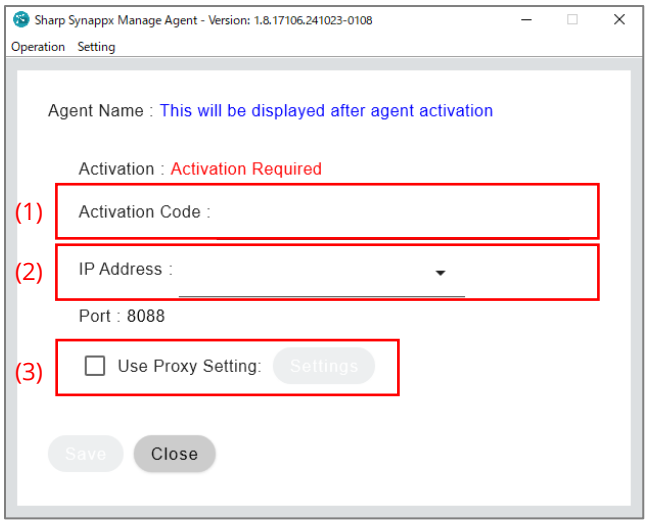
- When the number of devices exceeds 400 in one tenant.
- Multiple Local Area Networks in your network. Install an Agent for each LAN.

Installing the Synappx Manage Agent

1. Download and unzip file. Files can be stored in any folder on the PC.

2. Double-click **Sharp Synappx Manage Agent.msi** to start Sharp Synappx Manage Agent Setup Wizard.
3. When the **Setup Wizard** appears, click **Next**.
4. The **Destination Folder** screen will appear. This screen describes the default target directory for installation. To change the destination click **Change** and select the desired folder, then click **Next**.
5. The **Windows Defender Firewall Setting** screen will appear. This screen allows the user to select whether the Wizard will add exceptions to the Windows Defender Firewall. By default, the Wizard does not add exceptions.
   To manually add exceptions, uncheck the checkbox and click **Next**. See "Appendix" for more information on manually adding exceptions.

   Note:
   If a firewall other than Windows Defender Firewall is enabled, configure the firewall following the firewall's directions.
6. The **Ready to install Sharp Synappx Manage Agent** screen will appear. Click **Install**. The installation could take up to several minutes to complete. When the Completed Setup Wizard screen appears, click **Finish**, keeping the **Launch Sharp Synappx Manage Agent** checked. When agent installation begins, the system will show a **User Account Control** screen. Click **Yes** to proceed. This is a standard Windows installation process.
7. The **Sharp Synappx Manage Agent** dialog box will appear. Make the necessary settings to start the service.



Sharp Synappx Manage Agent dialog box

(1) **Activation Code**: Paste the Activation Code copied from the **Agent Settings** page in the **Activation Code** field to activate the Agent.

Note:

Activation Code is valid for 72 hours, after which you can return to this page and generate a new code. The Download Agent dialog box appears when the Activation Code is issued. The Activation Code is also displayed on the **Agent Settings** page.

(2) **IP Address**: Enter the IP address of the PC, either manually or from the pull-down menu.

(3) **Use Proxy Settings**: If connecting to the Internet via a proxy, select the **Use Proxy Settings**, then click **Settings** to open the **Proxy Settings** dialog box. Enter your proxy server information. Selecting **Use Windows Settings** will allow the user to use the settings of the Windows PC on which the Agent is installed. Click **OK**.

Note:
When an agent is installed, some systems may show "Microsoft Defender SmartScreen" and block the installation. This is a standard Windows installation process.

8. After clicking **Save**, a confirmation dialog box will appear. Click **OK** to save the settings and start the Agent.
9. The **Sharp Synappx Manage Agent** dialog box will appear again. Confirm the **Agent Name** and **Activated** status, then click **Close**. The service will still run after closing the box. Go to the Agents section for more details on using and managing agents.

Note:
When the agent is not working properly, you may restart the agent service by selecting **Restart** in the **Operation** menu in the agent.

Step 3: Discover and Register Devices

Register MFPs/Printers

Add Device Discovery Condition(s)

1. In the MFP/Printers tab of Agent Settings page, click the Add Discovery Condition icon ⊕ in the SNMP Settings to open the **Add Discovery Condition** dialog box.

MFP/Printers tab in Agent Settings page

2. Configure the Discovery Condition.

Add Discovery Condition dialog box

- **IP Address/Range Settings**: To search the local network or specific IP addresses or IP address range.
- **SNMP Settings**: Set the SNMP network settings for Synappx Manage to match the SNMP settings required for registered devices. The SNMP settings must be configured correctly for a device to communicate via SNMP protocol. If you want to use a non-default Credential Set, you must register it in advance. Please refer "Credential Set" for details.

Note:
The range of IP addresses for discovery is up to 65534 addresses. For successful communication with devices using the SNMP protocol, the SNMP settings in Synappx Manage must be configured to match the SNMP settings on the device(s) to ensure the discovery process complies with the organization's security policy.

3. Click **Save**. The configured discovery condition will be saved and appear in the **SNMP Settings** area.
4. If necessary, multiple Discovery Conditions can be added by repeating Steps 1-3.

Edit Device Discovery Condition

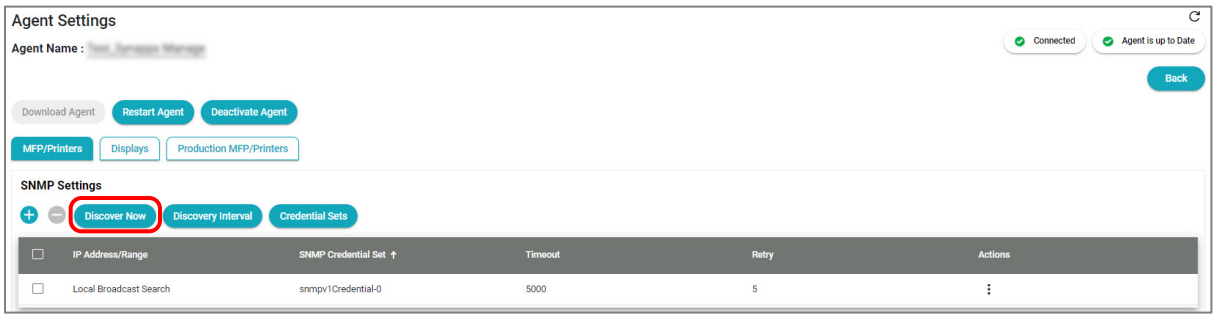
1. In the **MFP/Printers** tab of the **Agent Settings** page, click the Actions icon ⋮ and select **Edit** to open the **Edit Discovery Condition** dialog box.
2. Edit the Discovery Condition.
3. Click **Save**.

Remove Device Discovery Condition(s)

- To delete a Condition, click the Actions icon ⋮ and select **Remove** from the pull-down menu.
- To delete multiple Conditions at once, select the checkboxes of the conditions to be removed, then click the Remove Discovery Condition icon ⊖.

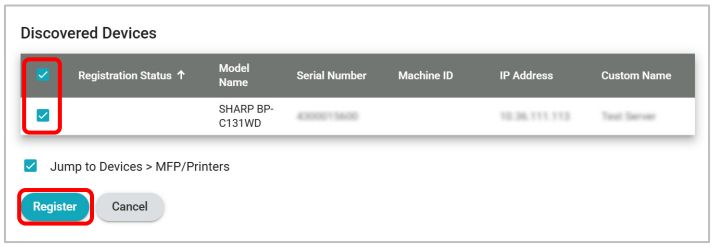
Discovering Devices

1. In the **MFP/Printers** tab of the **Agent Settings** page, click **Discover Now** to start discovering devices with listed discovery condition(s).
   To exclude IP addresses from discovery results, add them to the "**Blocked IP Address**" list before clicking **Discover Now**.



Discover Now for MFP/Printers

2. In the **Discovered Devices** dialog box, select the devices to be registered in the network and click **Register**.



Discovered Devices dialog box for MFP/Printers

Note:
To auto display the **Monitoring & Management** page after the devices are registered, select **Jump to Devices > MFP/Printers**.

3. Device Discovery is initially set to be performed daily. To disable scheduled device discovery, click **Discovery Interval** to open the dialog box and unselect the checkbox. Click **Save**.

Discovery Interval dialog box

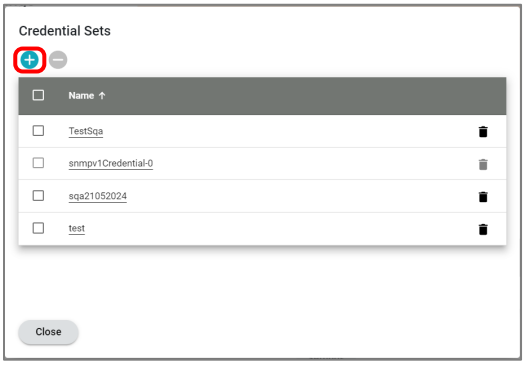
Credential Sets

In this menu, you can configure SNMP security settings. The credentials and security settings registered here are used in the agent.

1. In the **MFP/Printers** tab of the **Agent Settings** page, click **Credential Sets** button to open the settings screen.

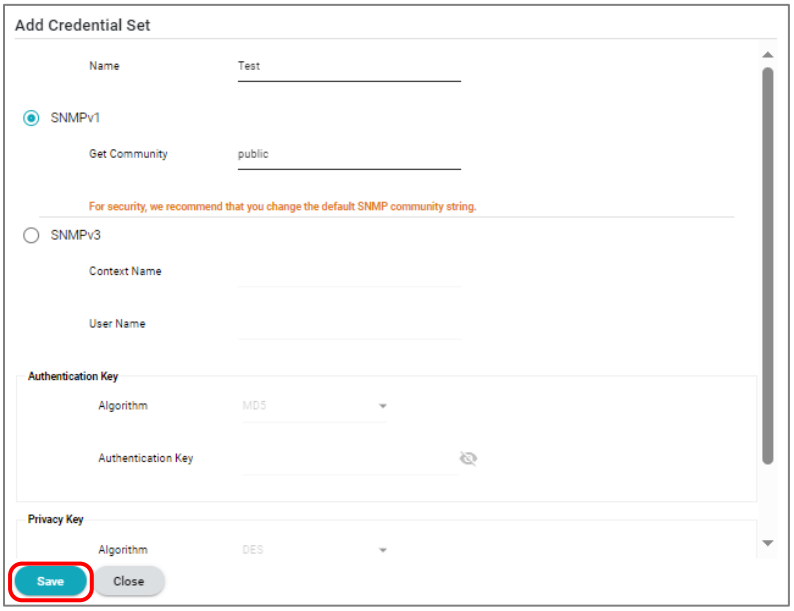
Credential Sets for MFP/Printers

2. Click the Add Credential icon ⊕ to open the **Add Credential Set** dialog box.



Credential Sets dialog box

3. Configure SNMP security settings, including a nick name for the settings, and click **Save**.

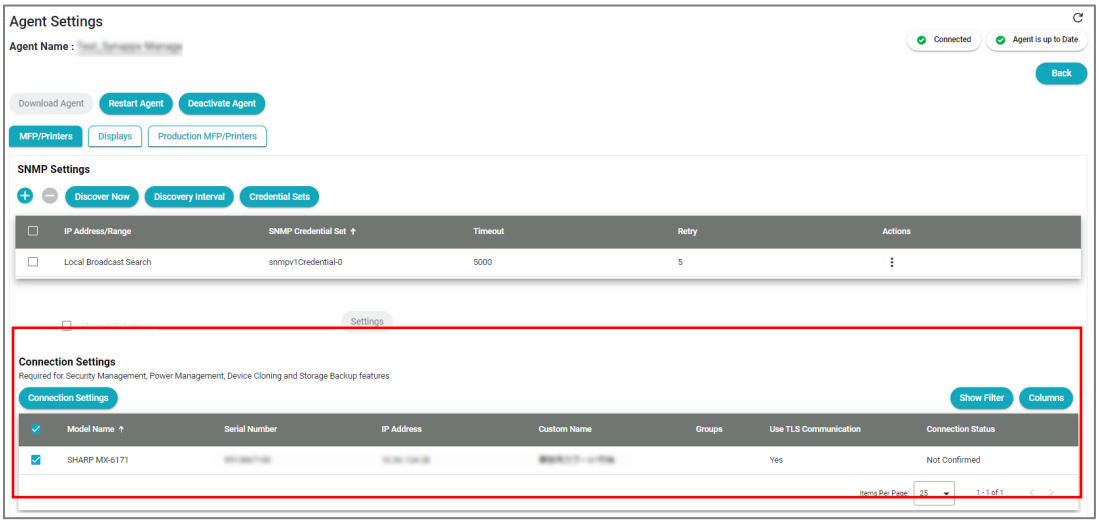


Add Credential Sets dialog box

If you want to edit settings, check the registered name in the **Credential Sets** dialog.

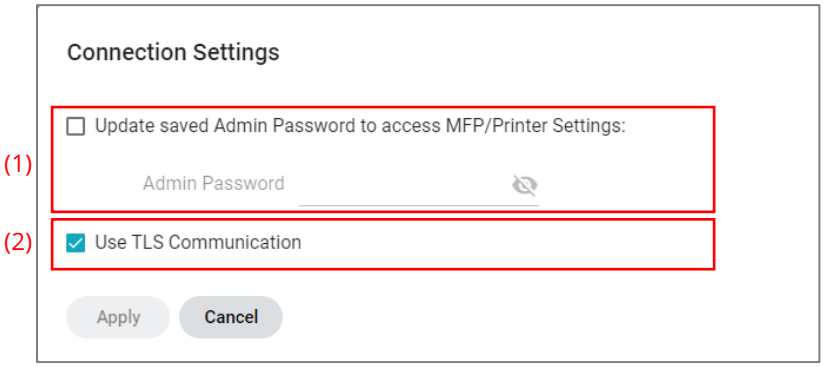
Configure Connection Settings

In this menu, you can change an administrator's access password used for device authentication while performing security-related operations. Multiple devices can be selected at once to change several administrator passwords simultaneously.



Connection Settings for MFP/Printers in Agent Settings page

1. Scroll down to the **Connection Settings** area in the MFP/Printers tab.
2. Select the target device(s) to store the Admin Password.
3. Click **Connection Settings**.



Connection Settings dialog box

(1) **Update saved Admin Password to access MFP/Printers Settings**: Enabling this option inputs **Admin Password** to update the saved Admin Password (at least five characters). The Admin Password Rewrite function in the Security Policy Settings allows to change the Admin Password in MFP/Printers as well as the saved Admin Password to access the MFP/Printers settings in Manage.

Note: If you logged in as Service Main, register **Service Password**.

(2) **Use TLS Communication**: Enabling this option encrypts the data that is transferred between the devices and Synappx Manage Agent as part of security operations, device cloning etc.

4. Click **Apply**.

Note:
Go to the Guidelines for Naming and Text Entry > Passwords for password guidelines. To toggle password visibility, use the icons next to the password entry fields (,).

Register Display Devices

Prepare for SSH communication

If SSH communication is not used, this step is not necessary. Proceed to "Add Device Search Condition(s)".

1. Click the **Displays** tab to show the **Connection Settings for Displays**.
2. Click **Generate New** button. If SSH key generate succeeds, a dialog box is displayed.
3. After confirm dialog box, click **Download** to download SSH key.

Displays tab in Agent Settings page (SSH key)

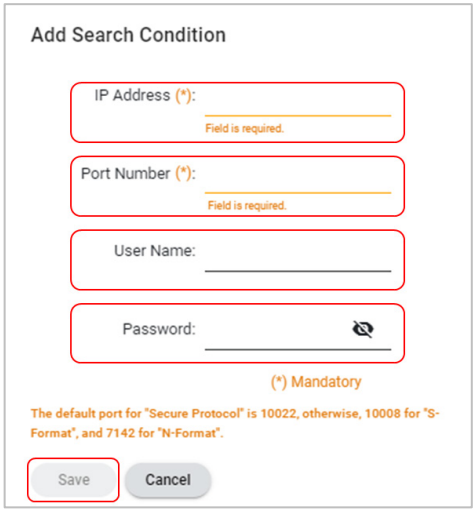
4. Open the downloaded file and apply the key to display device which will be registered to Synappx Manage.

Add Device Search Condition(s)

1. Click the **Displays** tab to show the **Connection Settings for Displays**.

Displays tab in Agent Settings page

2. Click the Add Search Condition icon ⊕ in the **Connection Settings for Displays** area to open the **Add Search Condition** dialog box.
3. Configure the Search Condition.



Add Search Condition dialog box

- **IP Address** (Mandatory): IP address of the display to be registered.
- **Port Number** (Mandatory): Data communications TCP port number selected for the display (Default value for "SSH" is 10022, otherwise, S-format: 10008, N-format: 7142). Valid port numbers are between 1025~65535.
- **User Name**: The user name assigned to a display that allows the user to gain authorized access to control the display settings via Synappx Manage.
- **Password**: The password assigned to a display that allows the user to control the display settings via Synappx Manage. The password requirement varies per display model.

4. Click **Save**. The configured search condition will be saved and appear in the **Connection Settings for Display** area.

5. If necessary, multiple Search Conditions can be added for each device by repeating Steps 1-4.

Edit Device Search Condition

1. In the **Displays** tab of **Agent Settings** page, click the Actions icon ⋮ for the Condition to be edited. Select **Edit** from the pull-down menu to open the **Edit Search Condition** dialog box.
2. Edit the Search Condition.
3. Click **Save**.

Remove Device Search Condition(s)

- To delete a Condition, click the Actions icon ⋮ and select **Remove**.
- To delete multiple Conditions at once, select the checkboxes of the conditions to be removed, then click the Remove Search Condition icon ⊖.

Searching Devices

1. In the **Displays** tab of the **Agent Settings** page, click **Search** to start searching devices with the listed Search Condition(s).

Search for Displays

2. Select the device to be registered from the **Searched Devices** dialog box, then click **Register**.

Searched Devices dialog box for Displays

If **Jump to Devices > Displays** is selected, the **Monitoring & Management** page will be displayed after the displays are registered.

Technical Service Features

Features for service providers are categorized as Technical Service. To access the features, the user needs to login as a Guest Administrator. To perform some of the technical features require the FSS settings on the devices connected to the installed agent. Please refer to the service manual for more details on how to configure FSS settings.

Register Production MFP/Printers

Use only to add some models (BP-1200, BP-1250M/1360M). Contact your dealer or service person for more information.

Restart Agent

Restart Agent button allows you to restart the agent. It is recommended to use this when the agent is not working properly.

Restart Agent button

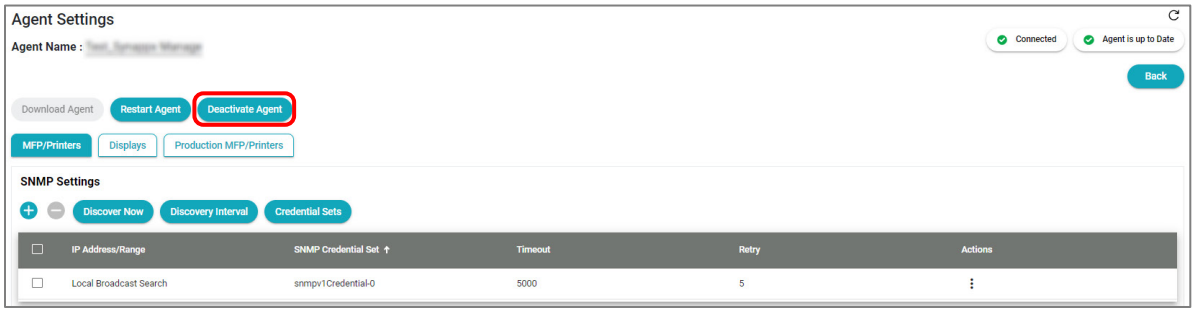
How to Restart Agent

1. Open the **Agent Settings** page for the agent you want to restart, click the **Restart Agent** button.

2. A confirmation message will appear, please click the **OK** button to continue.

Deactivate Agent

Deactivate Agent button allows you to deactivate agent. You can use it in situations for example, you want to move agent to other PC, you find any problem in working agent, and so on.



Deactivate Agent button

How to Deactivate Agent

1. Open the **Agent Settings** page for the agent you want to deactivate, click the **Deactivate Agent** button.

2. A confirmation message will appear, please click the **OK** button.

   Note:
   When an agent, which was previously activated, is deactivated, it loses its ability to communicate while it is deactivated. However, once the agent is activated again, all the settings associated with it will take over.

Direct (Agentless) Connection

Direct connection provides simple and faster setup without requiring on-premise software installations and updates. The following models support direct connections:

Color MFP

MX-3061/3071/3561/3571/4061/4071/5071/6071 series
MX-3061S/3071S/3561S/3571S/4061S/4071S/5071S/6071S series
MX-2651/3051/3551/4051/5051/6051 series
MX-C303W/C304W series
MX-C303WH/C304WH series
BP-60C31/60C36/60C45 series, BP-70C31/70C36/70C45/70C55/70C65 series
BP-50C26/50C31/50C36/50C45/50C55/50C65/55C26 series
BP-90C70/90C80 series
BP-C533WR/C535WR series, BP-C533WD/C535WD/C542WD/C545WD series
BP-C542PW/C545PW series
BP-C131WD/C131PW series

B/W MFP

MX-M3071/M3571/M4071/M5071/M6071 series
MX-M3071S/3571S/4071S/5071S/6071S series
MX-M2651/M3051/M3551/M4051/M5051/M6051 series
MX-B376W/B476W/B356W/B456W series
MX-B376WH/B476WH/B356WH/B456WH series
BP-70M31/70M36/70M45/70M55/70M65 series
BP-50M26/50M31/50M36/50M45/50M55/50M65 series
BP-70M75/70M90 series
BP-B537WR/B540WR/B547WD/B550WD series
BP-B547PW/B550PW series

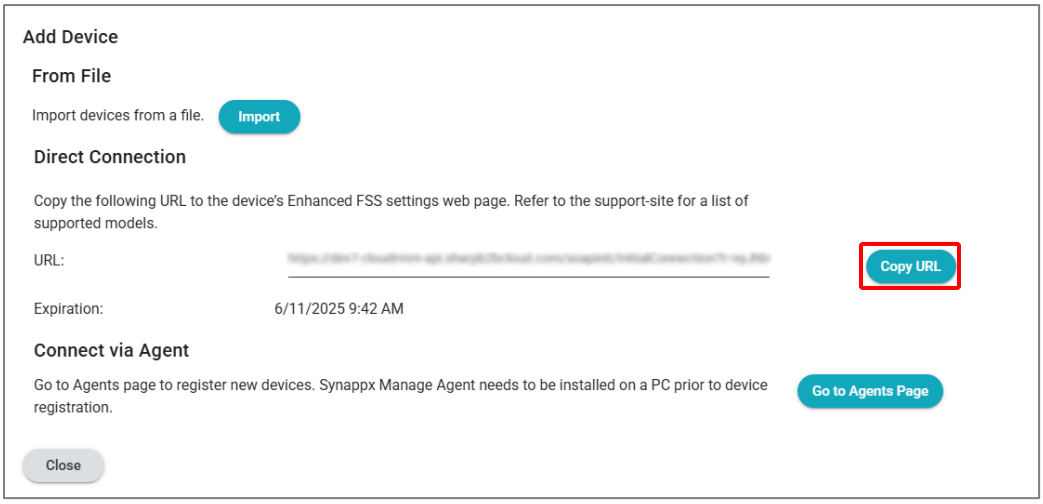
Note:
When changing an MFP that is already registered with an agent to direct connection, delete the MFP before establishing the direct connection. Go to Deleting Devices for detail.

Follow the steps below to configure each device.

1. In the **Monitoring & Management** page, click Register Device icon ⊕.

Monitoring & Management page

2. In the **Add Device** dialog, click **Copy URL** button to copy the URL. The URL is valid for 30 days; complete the following steps within 30 days.

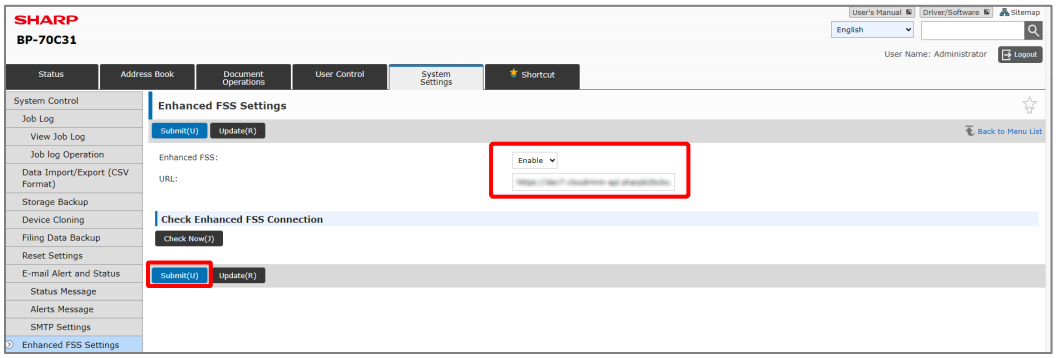


Add Device dialog

3. Connect to the following URL with browser, and log in to a device as an administrator.

   <<*IP address of MFP*>>/sysmgt_enhanced_fss.html

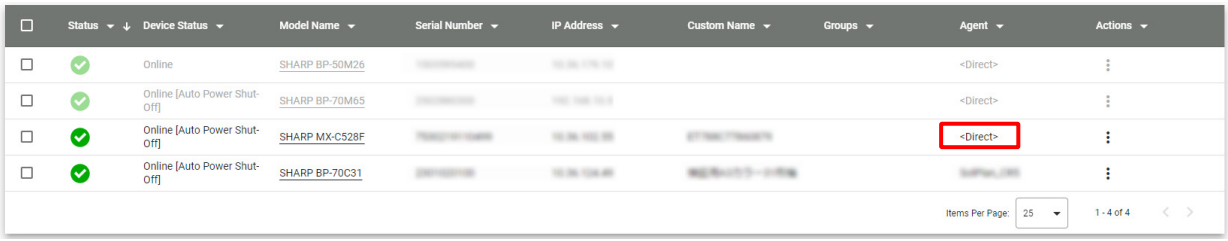
4. Go to the Enhanced FSS setting under the System Settings, set **Enhanced FSS** to **Enable**, and enter the URL you copied in step 2 in the **URL** field. Then, click **Submit** to apply.



Enhanced FSS Settings page

5. Reboot the MFP.

6. Confirm that the device appears in the device list with the <Direct> status.



Device List

Some models require the .eSF application installed on an MFP to establish direct connection. The application is available through your authorized service provider.

Applicable Models:

Color MFP
MX-C357F/C407F/C507F/C557F/C607F/C407P/C507P/C607P series
MX-C428F/C528F/C528P/C358F/C428P series

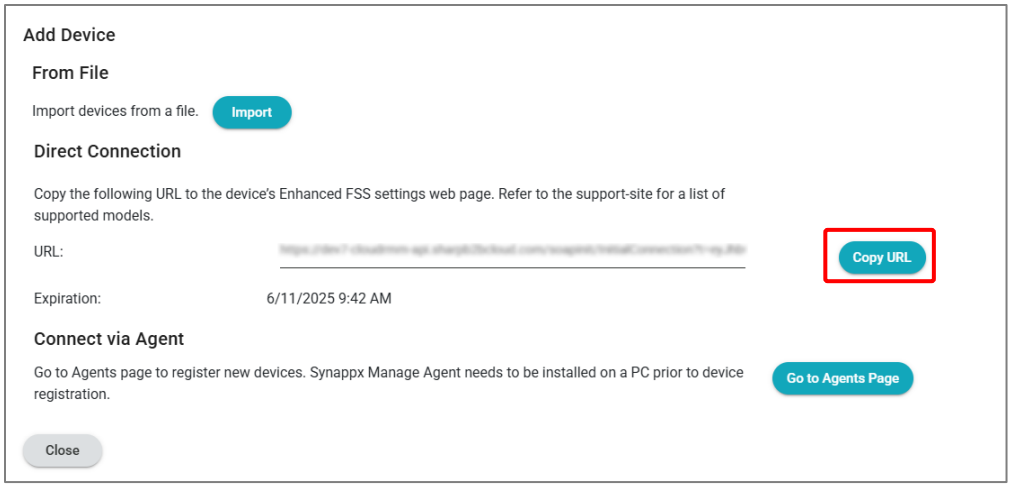
B/W MFP
MX-B557F/B707F/B557P/B707P series
MX-B467F series, MX-B468F series

Once the .eSF application for Synappx Manage is installed, follow the steps below to complete the device registration.

1. In the **Monitoring & Management** page, click Register Device icon .

Monitoring & Management page

2. In the **Add Device** dialog, click **Copy URL** button.



Add Device dialog

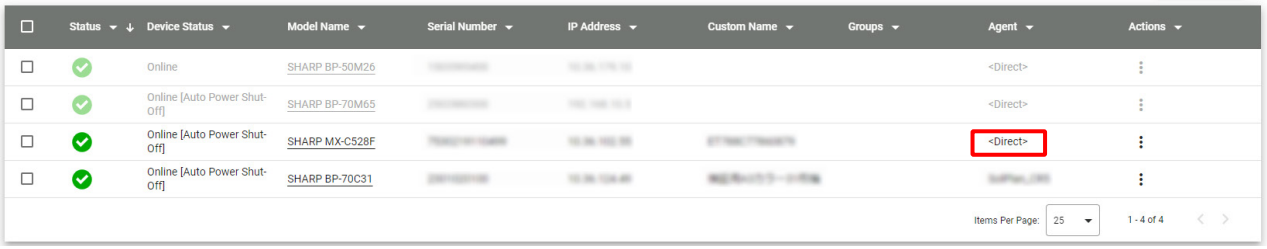
3. From global download site, install the .eSF application for Direct Connection to MFP.

4. Connect to device web page of MFP and logs in as an administrator.

5. From **the Select Option** list on the left side, select **Apps**. On the right side, from the apps list, select the Installed app in step 3 and click **configure** button.

6. Enter the URL copied in step 2 into the **Server URL** field and click **Apply** button.

7. Confirm that **Agent** column in the device list shows <Direct>.



Device List

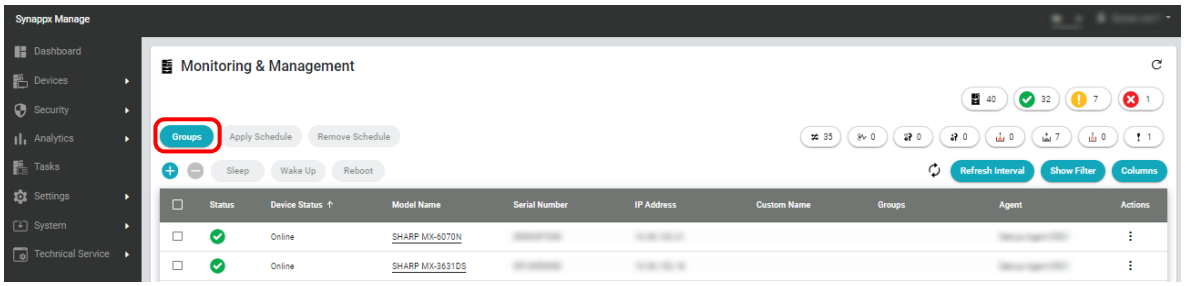
Grouping Devices

Registered devices can be grouped, which allows settings to be applied to multiple devices simultaneously.

The same device can be added to multiple groups. A group can contain both MFP/printers and displays. Grouping functions, such as adding and removing devices from groups, are identical for both device types.

Create a New Group Name

1. At the **Monitoring & Management** page, click **Groups** to open the **Groups** dialog box.

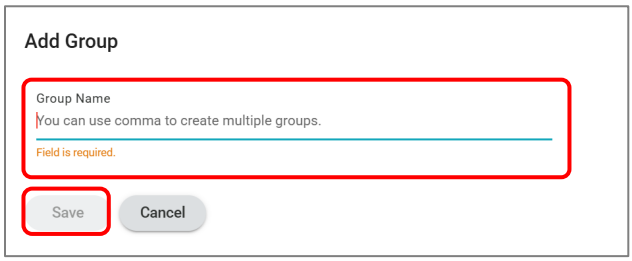


Monitoring & Management page

2. Click the Add Group icon ⊕.

Add Group icon

3. Enter the Group Name, then click **Save**. When the "Group created successfully" dialog box appears, click **OK**. The group is automatically listed in the grid. (Max: 500 Groups) Multiple groups can be created at once by entering Group Names separated with ",".



Add Group dialog box

4. Click **Close** to close the dialog box.

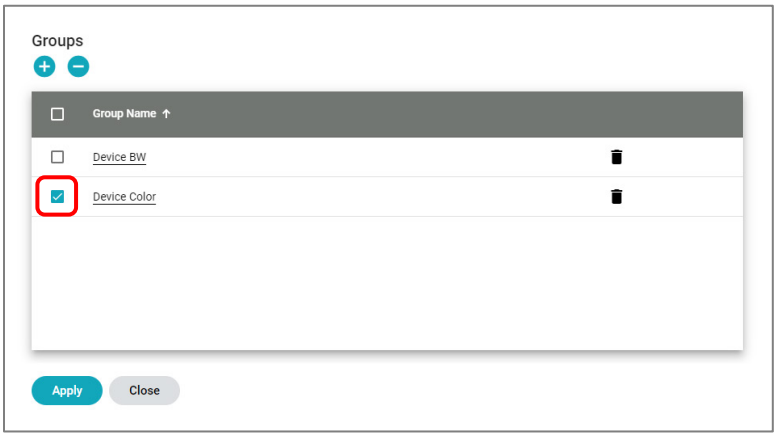
Close button

Add Device(s) to Group(s)

After the Group(s) is/are created, registered devices can be added to the selected Group(s). Multiple devices can be added simultaneously.

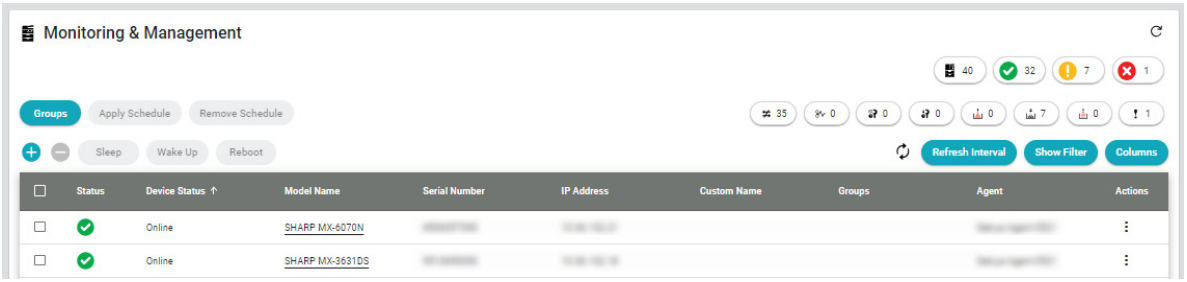
1. At the **Monitoring & Management** page, select the checkboxes next to the device(s) to be added to the Group(s).
2. Click **Groups** to open the **Groups** dialog box.

3. Select one or more Groups by selecting the checkbox(es) for the Group(s).



Select one or more Groups

4. Click **Apply** to add the selected device(s) to the selected Group(s).
When the "Group applied successfully" dialog box appears, click **OK**. The selected devices will be added to the group. The Group Name will appear in the **Groups** column.



Group Name in Groups column

If the selected device already has belonged to different groups, the checkbox next to the corresponding group name will appear as ▬. When devices are added to multiple groups, the group registration is automatically merged.

Examples:
- Device #1: Belongs to the groups "Home Office" and "Color"
- Device #2: Belongs to the groups "Corporate Office" and "Monochrome"

A new group called "2nd Floor" is created and Device #1 and Device #2 are added to the group.

Results:
- Device #1: Belongs to the groups "Home Office", "Color", and "2nd Floor"
- Device #2: Belongs to the groups "Corporate Office", "Monochrome", and "2nd Floor"

Remove Device(s) from Group

Remove devices with the following steps. When a device is removed from the Group, the settings applied to the device will remain unchanged.

1. On the **Monitoring & Management** page, select the checkbox(es) of the device(s) to be removed from the group.
2. Click **Groups** to display the **Groups** dialog box.

   Uncheck the box next to the name of the Group.
3. Click **Apply** to remove the Device(s).
   When the "Group applied successfully" dialog box appears, click **OK**.

Remove Group

When the group name is deleted, the group will be removed. However, the settings applied to these devices will remain unchanged.

1. At the **Monitoring & Management** page, click **Groups** to open the Groups dialog box.
2. Groups can be deleted individually or several at a time.

- To delete a Group Name, click the Trash icon .
- To delete multiple Group Names at once, select the checkboxes of the Names to be deleted, and then click the Remove Group icon .

Optional Settings

Administrator Management

Add/Remove Administrators
Administrators can also add and remove other administrators from the system. Additional administrators do not require Azure administrator privileges. However, additional administrator (except guest admins) need to be a member of the organization's Microsoft 365 or Google Workspace environment, and they must have privileges of Google Workspace. (Unless the administrator has selected Custom Account as the identity provider.)

Administrator Roles
There are two types of administrators. IT administrators and guest administrators. IT administrators (IT Main and IT Helpdesk) are designed for the tenant's IT personnel and must be a member of the organization. The guest administrator (Service Main, Service Support, Service View) is designed for the authorized Sharp service providers.

Note:
Any guest administrators are not invited or listed on the Admin Portal for the tenant that have preconfigured guest administrators.

The following table describes functions/permissions of the IT administrators:

Menu Bar		Functions	IT Main	IT Helpdesk
Dashboard		(All functions)	✓	✓
Devices	MFP/Printers	(Page access)	✓	✓
		Groups	✓	
		Apply Schedule	✓	
		Remove Schedule	✓	
		Register Device (+)	✓	✓
		Delete Device (-)	✓	
		Sleep/Wake Up/Reboot	✓	✓
		Refresh Now	✓	✓
		Refresh Interval	✓	
		Show/Hide Filter	✓	✓
		Columns	✓	✓
		Actions: Device Web Page	✓	✓
		Actions: Remote Operation	✓	✓
		Actions: Apply/Change Schedule	✓	
		Actions: Remove Schedule	✓	
		Actions: Download Driver File	✓	✓
		Actions: Select Device Type	✓	
		Actions: Remove	✓	

Menu Bar		Functions	IT Main	IT Helpdesk
		Select a Model Name for Device Information	✓	✓
	MFP/Printers > Device Information	(Page access)	✓	✓
		Sleep/Wake Up/Reboot	✓	✓
		Device Web Page	✓	✓
		Remote Operation	✓	✓
		Download Driver File	✓	✓
		Refresh Now	✓	✓
	Displays	(Page access)	✓	✓
		Groups	✓	
		Apply Schedule	✓	
		Remove Schedule	✓	
		Register Device (+)	✓	
		Delete Device (-)	✓	
		Sleep/Wake Up	✓	✓
		Change Input	✓	✓
		Refresh Now	✓	✓
		Refresh Interval	✓	
		Show/Hide Filter	✓	✓
		Columns	✓	✓
		Actions: Device Web Page	✓	✓
		Actions: Apply/Change Schedule	✓	
		Actions: Remove Schedule	✓	
		Actions: Apply Custom Name	✓	
		Actions: Remove Custom Name	✓	
		Actions: Remove	✓	
		Select a Model Name for Device Information	✓	✓
	Displays > Device information	(Page access)	✓	✓
		Sleep/Wake Up	✓	✓
		Change Input	✓	✓
		Device Web Page	✓	✓
		Refresh Now	✓	✓
	Power & Input Schedules	(All functions)	✓	
	Device Cloning	(All functions)	✓	
	Storage Backup	(All functions)	✓	
	Address Book	(All functions)	✓	
	Print Drivers	(All functions)	✓	✓
	Custom Device Types	(All functions)	✓	
	Firmware	(All functions)	✓	

Menu Bar		Functions	IT Main	IT Helpdesk
Security	Security Control	(Page access)	✓	✓
		Apply Policy	✓	
		Remove Policy	✓	
		Check Policy Now	✓	
		Check Policy Interval	✓	
		Show/Hide Filter	✓	✓
		Columns	✓	✓
	Security Policies	(All functions)	✓	
Analytics	Fleet Report	(All functions)	✓	
	Usage Report	(Page access)	✓	✓
		Export Usage Report	✓	
	Security Report	(Page access)	✓	✓
		Export Violation Logs	✓	
Tasks		(All functions)	✓	✓
Settings	Admin Users	(All functions)	✓	
	Supported Domains	(All functions)	✓	
	Tenant	(All functions)	✓	
	Agents	(Page access)	✓	✓
		Add Agent (+)	✓	
		Delete Agent (-)	✓	
		Update Mode	✓	
		Execute Update	✓	
		Show/Hide Filter	✓	✓
		Columns	✓	✓
		Actions: Delete	✓	
	Agents > Agent Settings (Except for tab area)	(page access)	✓	✓
		Download Agent	✓	
		Generate Activation Code	✓	
		Copy Activation Code	✓	
		Restart Agent	✓	
		Deactivation Agent	✓	
	Agents > Agent Settings > MFP/Printers	Discovery Now	✓	✓
		Discovery Interval	✓	
		Credential Sets	✓	
		(All other functions)	✓	
	Agents > Agent Settings > Displays	(All functions)	✓	
	Agents > Agent Settings > Production MFP/Printers	(All functions)	✓	

Menu Bar		Functions	IT Main	IT Helpdesk
	Email Alerts	(All functions)	✓	✓
	Downloads	(All functions)	✓	
System	Admin Log	(All functions)	✓	
	Operation Log	(All functions)	✓	
	Device Log	(All functions)	✓	
	About	(All functions)	✓	✓

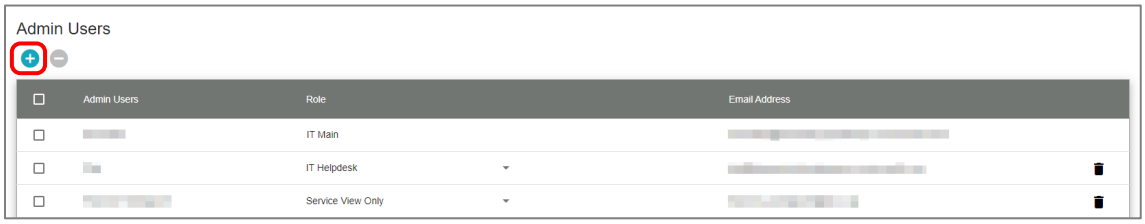
Adding Additional Administrators

Administrators can be added if you have valid role within the Synappx Manage.

Roles	IT Main	IT Helpdesk	Service Main	Service Support	Service View Only
IT Main can add	✓	✓			
IT Helpdesk can add					
Service Main can add			✓	✓	✓
Service Support can add					
Service View Only can add					

Adding IT Main or IT Helpdesk

1. Go to **Settings** in the Admin Portal. On the **Admin Users** page, click the Add Admin icon ⊕ to open the **Add Admin** dialog box.



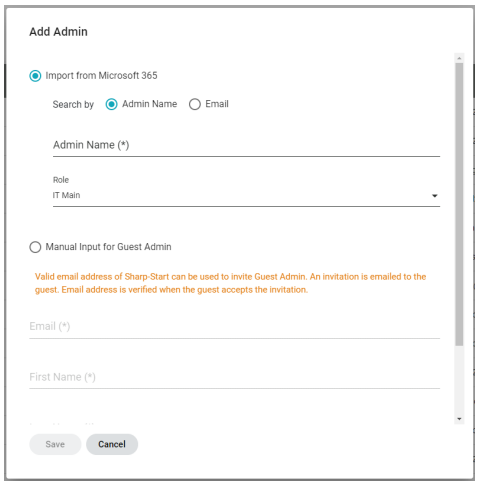
Admin Users page

2. Enter the Admin Name or email address. A list of possible names will appear as you type. Select a candidate from this list.

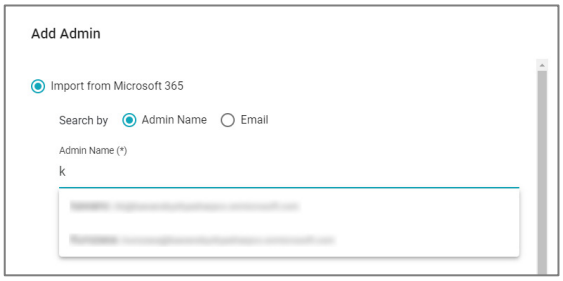
Note:

- No input suggestions will be listed in case the administrator has selected Custom Account as the identity provider. Only direct input is available.
- "Manual Input for Guest Admin" option will not be available for the tenant that have preconfigured guest administrators.

In the **Search by** field, select which input to use.

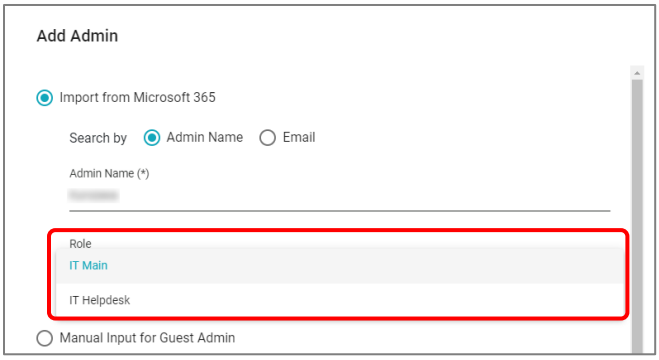


Add Admin dialog box



Person Search

3. Under **Role**, choose **IT Main** for full administrative privileges or **IT Helpdesk** for limited privileges. (See Administrator Management for more information). The role can be edited later by selecting the Admin Name.

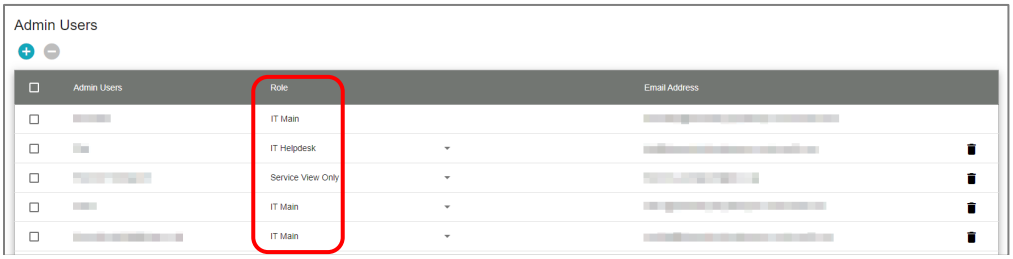


Role Selection

4. Click **Save**. The new administrator will appear on the **Admin Users** list.
5. The **Select Services** dialog box will appear. If necessary, enable other Synappx services to be accessed as Admin and click **Save**.

Select Services dialog box

Change Role for Admin Users



Role column of Admin Users page

The role assigned to the account can be changed based on the permissions given to that user role.

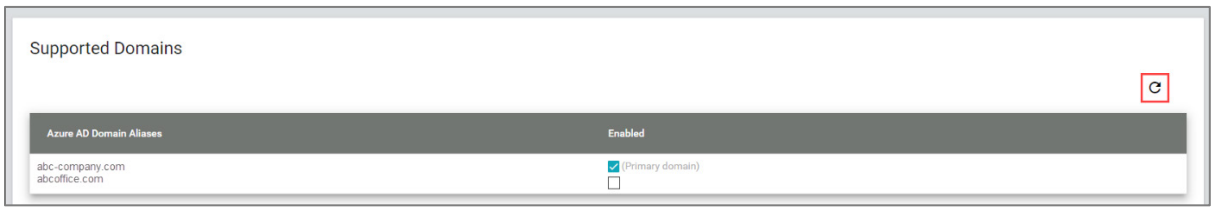
Role Change

Supported Domains

The **Supported Domains** page automatically collects domain aliases from Azure Active Directory or Google Workspace. (Unless the administrator has selected Custom Account as the identity provider.) All domains are enabled by default.
In the case of Microsoft 365 account users, it cannot automatically retrieve and display domains without the necessary permissions. In that case, a text box will appear to enter a subdomain name.

> **Caution**:
> When the domain is disabled, associated users will also be disabled.

Admins can choose which domain aliases to enable or disable by checking and unchecking the boxes. These settings apply to Synappx Manage and Synappx Go. Primary domains cannot be unselected. Click the Refresh icon ↻ to view new domain aliases added to Azure AD or Google Workspace.



Supported Domains page

Tenant Name

Tenant Setting page allows to change the **Tenant Name** (1) to be displayed.

Tenant Settings page

Agents

Agents page

Avalable information on the agent page

(1)	Agent Name	The name for the agent When the hyperlink is clicked, the agent Settings UI opens
(2)	Status	● – Connected ● – Newly Connected or In Progress ● – Not Connected
(3)	Agent Status	Newly Connected – New agent connection Connected – When agent is connected Not Connected – When agent is not connected Not Activated – When agent is not activated Updating – When agent update is in progress
(4)	PC/Server Name	Name of PC/server where the agent is installed
(5)	IP Address	IP address of PC/server where the agent is installed
(6)	Version	Version of Agent which is installed
(7)	Last Communication	Date and time when latest information was received by the agent
(8)	Update Mode	Manual Update – Agent update process is set for manual Auto Update – Agent update process is set for auto-update (Not Supported) – Update mode is not supported
(9)	Update Status	● Up to Date – When agent is up-to-date ● In Progress – When agent update is in progress ● Update Required – When newer agent is available (Unknown) – When status is unknown

Agent Update

Synappx Manage agents can be updated manually or set to automatically be updated.

a) Manual Update
b) Auto Update

How to set the Agent update preference:

1. In the **Agents** page, select agent(s).

Update Mode for Agents page

2. Click **Update Mode** to open the **Update Mode** dialog box.
3. Select the update mode, either **Manual Update** or **Auto Update**, and click **Save**.

a) Manual Update

1. In the **Agents** page, select the agent(s) indicated as **Update Required**.
2. Click **Execute Update** to start the update process.
3. Once the update is complete, the **Update Status** will change to **Up to Date**. (Refresh screen ↻ operation may be required.)

b) Auto Update

1. Agents configured with auto update will automatically check the availability of the updated agent every 10 minutes.
2. The update process will start automatically when the newer agent is detected.
3. Once the update is completed, the **Update Status** will change to **Up to Date**. (Refresh screen ↻ operation may be required.)

Additionally, you can download the agent installer from the download page to manually apply the updated agent file.

> **Note**:
> When agent installation begins, the system will show the **User Account Control** screen. Click **Yes** to proceed. This is a standard Windows installation process.
> While uninstalling a previous version of the agent, a dialog box may appear indicating application(s) that need to be closed to continue uninstallation. Close the specified application(s) and click **Retry**. While updating, a dialog may appear indicating that the update installation completely removes the previous version. Select **Yes** to continue.

Uninstalling the Agent (Windows 10)

The installed agent on PC can be removed using the standard uninstall procedure for Windows operating systems.

1. Select the Windows Start menu, then select **Settings > Apps > Apps & features**.
2. Select the **Sharp Synappx Manage Agent**, and then select **Uninstall**. A **User Account Control** screen will appear. Click **Yes** to proceed.
3. On the **Agents** page of Synappx Manage, click the Trash icon in the row containing the Agent name to be deleted.

Email Alerts

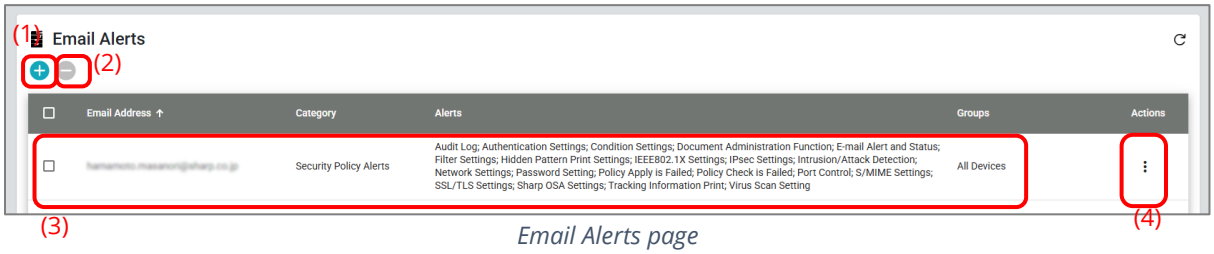
There are four types of email alerts that are sent to a designated administrator(s) when a specified event occurs:

Alerts	Things to be Notified
Device Status Alerts	Printer Error, Printer Error [Account Limit], Overdue Service Maintenance, Paper Jam, Marker Supply Missing, Toner Empty, Cover Open, Paper Empty, Specified Input Tray Empty, Specified Input Tray Missing, Specified Output Tray Full, Specified Output Tray Missing, Offline, Printer Warning, Toner Low, Paper Low, Input Tray Missing, Output Tray Full, Output Tray Near Full, Output Tray Missing, Printer Warning [Output Tray Missing], Near Overdue Service Maintenance
Security Policy Alerts	Policy Apply is Failed, Policy Check is Failed, Security Policy Violation
Agent Alerts	Lost Communication, New Version Available, Agent Update
Other Status Alerts	Communication Error, Toner Collection

Each email alert contains the status information of the target device.

Note:
If the toner collection container's status is not in the normal state when the tray & supply information is updated, an alert for toner collection will be sent.

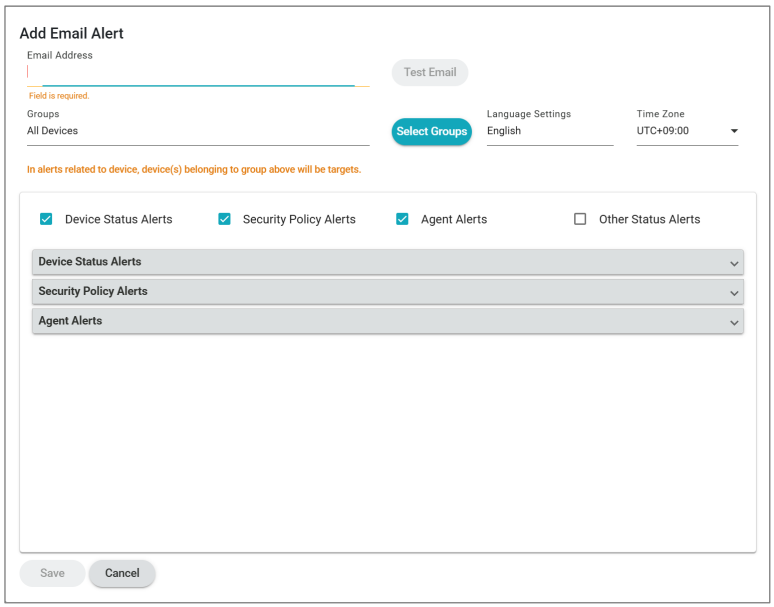
Email Alerts Page



Email Alerts page

(1) **Add Email Alert icon**
To add a new email alert.
(2) **Remove Email Alert icon**
Deletes the selected email alert(s).
(3) **Email Alerts List**
Shows the configured email alerts.
(4) **Actions icon**
Edits or deletes the email alert.

How to Add Email Alerts

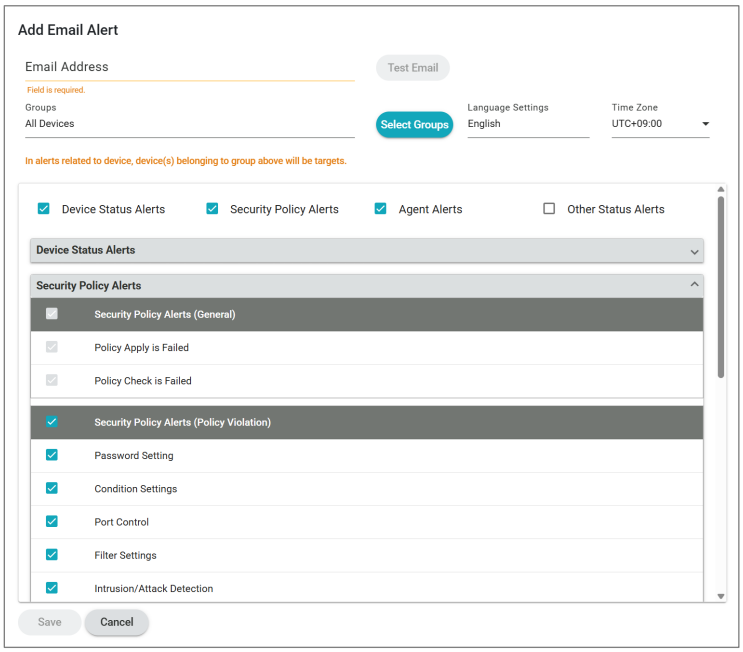


Add Email Alert

1. In the **Email Alerts** page, click Add Email Alert icon .
2. Enter the notification email addresses for receiving email alerts in the **Email Address** field. Multiple email addresses can be entered by entering a delimiter character ";" or "," between each address. If you would like to send a test email, click the **Test Email** button.
3. Click the **Select Groups** button to open **Groups** dialog box. Select the target device groups for the specified alert.

4. Select the language and time zone for the email notifications.
5. Check the checkboxes for the items from **Device Status Alerts**, **Security Policy Alerts**, **Agent Alerts**, and **Other Status Alerts** for which you want to set a detailed alert.
6. Only the items checked above will be displayed, then set further details.
7. Click **Save**.

Note:
When the security policy alerts are enabled, an email alert is sent when communication or authentication fails.



Security Policy Alerts Settings

Edit Email Alert

1. Click the Actions icon ⋮ for the Email Alert to be edited. Select **Edit** from the pull-down menu.
2. Edit the Email Alert settings in the **Edit Email Alert** dialog box.
3. Click **Save**.

Remove Email Alert(s)

- To delete an Alert, click the Actions icon ⋮ and select **Remove**.
- To delete multiple Alerts at once, select the checkboxes for the Alerts to be removed, then click the Remove Email Alert icon ⊖.

Dashboard

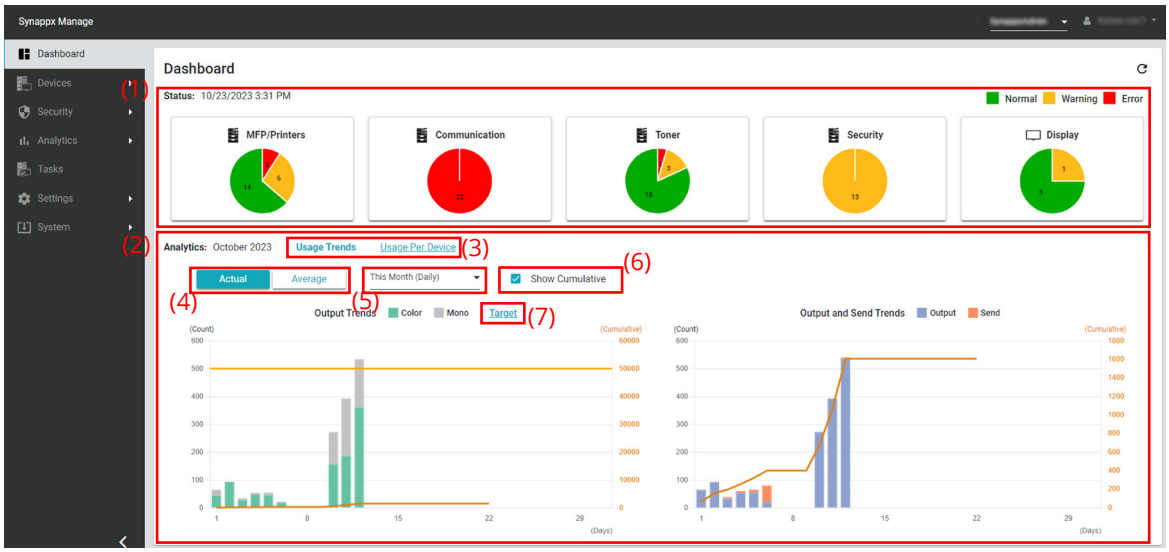
The dashboard provides a snapshot of managed devices with a summary of status (**Status**) as well as visualized MFP/printer usage trends (**Analytics**/**Device List**).

Status Section

- A list of affected device list will be displayed by selecting a status chart

Analytics/Device List Section (The data is collected every seven days)

- View usage trends by selecting **Usage Trends** (default) or **Usage Per Device**
- Provides usage trends of the total managed devices or per device trend for most used and least used.



Dashboard page with usage trends

(1) **Snapshots of device status**

Each pie graph provides quick access to devices requiring attention. Green is Normal, Yellow is Warning and Red is Error. The following categories are available:

- MFP/Printers Status
- Communication Status
- Toner Status
- Security Status
- Display Status

The number displayed on the pie area indicates the number of affected devices. Click the status chart to display the list of the affected devices.

(2) **Data and device analytics** (default **Usage Trends**)

The left usage trend graph shows the total output of the managed MFP/Printers in the tenant for the current month. Hover over a graph bar to see color, mono and total counts. The right usage graph includes total output and send counts. Hover over a bar to see details.

The graph values are an increment from the previous data collection.

(3) **Usage Trends or Usage Per Device**
Display the **Usage Trends** to view the total data of the managed devices and **Usage Per Device** to view the data of the most and least used devices.

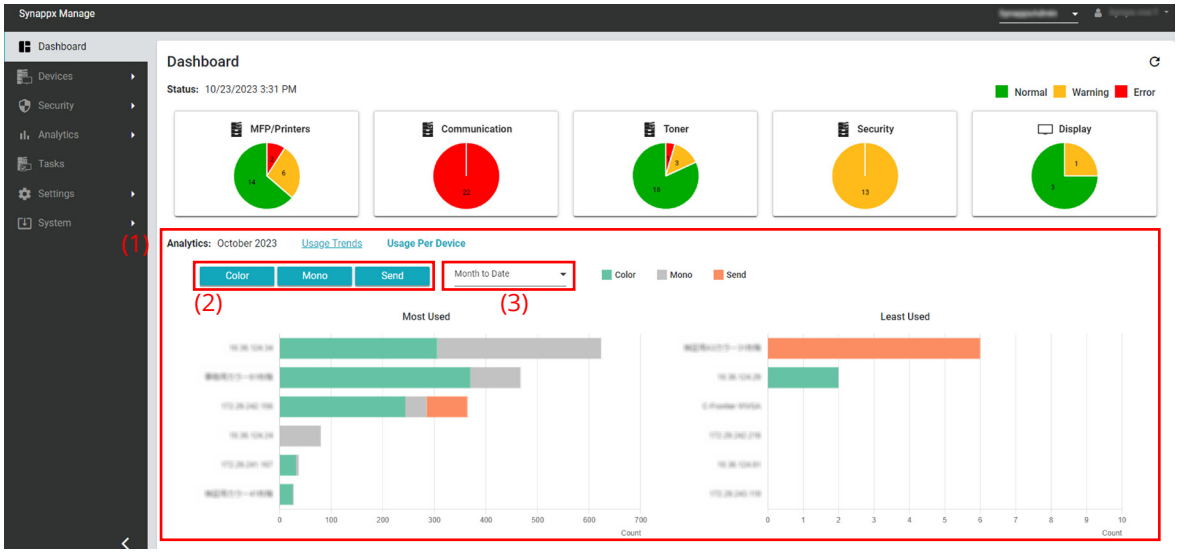
(4) **Actual/Average selection buttons**
Click to turn ON/OFF; when the average data is ON (highlighted in teal color), average usage data is displayed in the graph.

(5) **Counting period selection**
Select data period to be displayed in the graph. “This Month (Weekly)”, “This Month (Daily)”, or “Past Year” can be selected.

(6) **Cumulative checkbox**
Toggle the checkbox ON/OFF; when it is ON, the monthly target (if set) and the current cumulative total counts are displayed.

(7) **Monthly Target Print Volume**
Click this hyperlink to open the **Output Target** dialog. In this dialog, you can set a target monthly print volume for the tenant. A line indicating the volume will appear on the graph. It allows for visual comparison with the cumulative print total.

When **Usage Per Device** is selected in Analytics, the following will be displayed in the Analytics section.



Dashboard page with usage per device

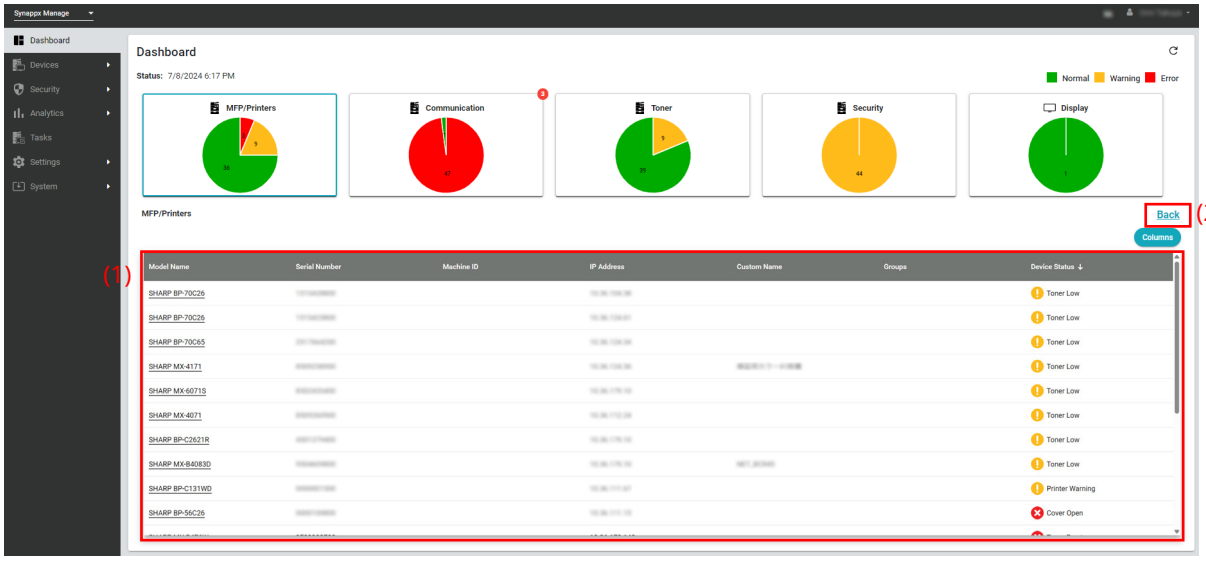
(1) **Usage per device analytics**
The usage per device graph shows the usage data of the most and least frequently used MFP/Printers in the tenant. Hover over each graph bar to see the output and send count details. The value is an increment from the previous data collection.

(2) **Color/Mono/Send selection buttons**
By default, all buttons are selected (teal colored). To filter the most and least used devices based on a subset of color, mono or send, select the button (turns white) to remove them from the usage data results. Touch a button again it to add back to the results.

(3) **Counter data/Average data selection**
Select the data to be displayed. “Month to Date” or “Average/Month” can be selected.

MFP/Printer Device List

Selecting a graph in the status section will display a device list in the dashboard section showing affected devices in that category. The list also shows the types of errors.



Dashboard page with a list of MFP/Printer devices

(1) **Error and Warning Device List**
Displays a list of devices in the selected status group. Access more detailed device information by clicking the model’s name.

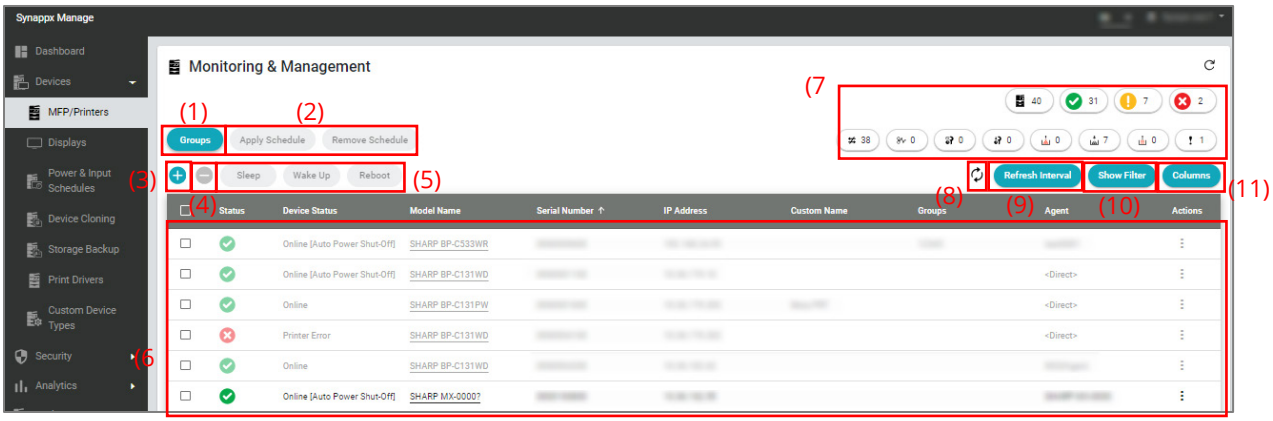
(2) **Back button**
Click the back button to go back to the default view with **Analytics**.

MFP/Printer Management

The MFP/Printer Management section describes the functions for managing multifunction devices (MFPs) and printers (devices).

Monitoring & Management Page

The monitored devices are listed on the **Monitoring & Management** page. You can view data and perform remediation through remote access.



MFP/Printers Monitoring & Management page

Overview of Buttons and Icons

(1) **Groups button**

Assigns a group name to each device.

(2) **Schedule buttons (Apply/Remove)**

Icons to apply power schedule to a device or devices.

(3) **Register Device icon**

Adds a new MFP/printer from the devices which appear in the “(6) Device List”.

(4) **Remove Device icon**

Removes the selected MFP/printer(s) from the devices that appear in the “(6) Device List”.

(5) **Power management buttons**

If a device(s) is selected via checkbox, the device’s power can be controlled. The available operations are **Sleep**, **Wake Up** and **Reboot**. (Refer to “Power Management" for details on using the power management buttons.)

(6) **Device List**

Managed devices will be listed. By selecting the model name, you can access detailed information for each device. You can filter and sort the list using the simple filter and arrow options.

Header options:

- Status
- Device Status
- Model Name
- Serial Number
- IP Address
- Custom Name
- Groups
- Actions
  - Device Web Page
  - Remote Operation
  - Apply/Change Schedule
  - Remove Schedule
  - Download Driver File
  - Select Device Type
  - Remove

(7) **Device status icons**

Show statuses for each device in the "(6) Device List". The Device List can be filtered so only the devices with those icons beside them are displayed.

(8) **Refresh all registered devices icon** 

Updates the information shown in the "(6) Device List" with the latest information from the Synappx Manage server.

(9) **Refresh Interval button**

Option for information auto update after a predetermined period.

(10) **Show Filter button**

Allows user to use simple filter. For more detail of simple filter, refer "Filtering Using Simple Filter".

(11) **Columns button**

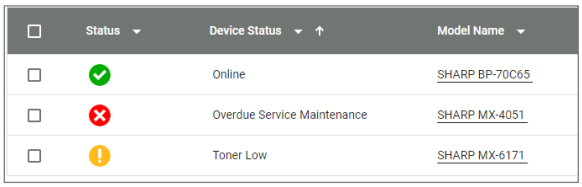
Adds or removes columns displayed in the "(6) Device List".

Note:

If "Communication Error (XXXX)" is displayed in the Communication Status column, it is possible that a communication error has occurred between Synappx Manage and the device. (For more information, go to Troubleshooting)

Device Status

The status for each device is shown in the device list in the **Monitoring & Management** page. The status is divided into two parts, **Status**, which shows the general status with colored icons ("Normal", "Warning" or "Error"), and the **Device Status** column, which shows more specific status (paper jam, toner low, overdue service maintenance, etc.).



Device Status column

A summary of the device status is displayed in the upper right corner of the **Monitoring & Management** page. The general status appears in the first row, and the more specific status appears in the second row. The numbers beside each icon show the total number of registered devices with that status. When the icon is clicked, the applicable device list will be displayed.

A summary of the device status

Status icons

The device status icons can be used to apply simple filters to the device list. Go to Filtering Using the Status Display Icons in Filtering to the Device List for details.

Icon	Status
	All Devices: Displays device information for all registered devices. The same device may be counted in more than one status. In such cases, the number will not match the total value of the number of Normal / Warning / Error units.
	Normal: Indicates that the status for the device is or .
	Warning: Indicates that the status for the device is (e.g., "Paper Low", "Toner Low", etc.) or .
	Error: Indicates that the status for the device is (e.g., "Paper Jam", "Toner Empty", etc.) or .
	Communication Error: Indicates that the status for the device is "Communication Error".
	Paper Jam: Indicates that the status for the device is "Paper Jam".

Icon	Status
	**Overdue Service Maintenance**: Indicates that the status for the device is “Overdue Service Maintenance”
	**Near Overdue Service Maintenance**: Displays device information for devices whose status is “Near Overdue Service Maintenance”
	**Toner Not Available**: Indicates that the status for the device is “Toner Not Available” or “Marker Supply Missing”, etc.
	**Toner Low**: Indicates that the status for the device is “Toner Low”.
	**Paper Not Available**: Indicates that the status for the device is “Paper Not Available” or “Specified Input Tray Missing”, etc.
	**Printer Error**: Indicates that the status for the device is “Printer Error”.

Power Management

Synappx Manage can be used to remotely operate power settings such as sleep, wake up, and reboot for supported devices. Go to the Appendix: Readme section for the information on supported devices.

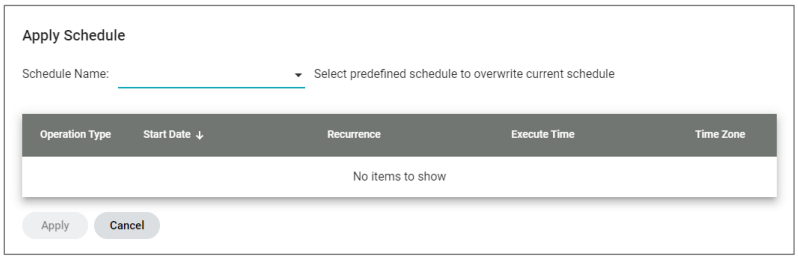
The power management buttons are in on both the **Monitoring & Management** page and the **Device Information** page. The operation procedures are slightly different. On the **Monitoring & Management** page, multiple devices can be selected, and the same power management operation is applied to all selected devices. On the **Device Information** page, the power management operation is only available for the displayed device. **Device Information** page can be reached by clicking the Model Name.

Scheduled Power Management Operations

Power management options can be executed automatically at regular intervals.
The schedule to be applied to the device(s) is predefined in the **Power & Input Schedule** page. Go to the “Power & Input Schedule Management” section for more details.

Applying a Power Management Schedule

1. In the **Device List** on the **Monitoring & Management** page, select the device(s) to which you want to apply a power management schedule. Multiple devices can be selected simultaneously by using the checkboxes.
2. Click **Apply Schedule** to open the **Apply Schedule** dialog box. By clicking on the Actions icon ⋮ and selecting **Apply/Change Schedule**, the **Apply/Change Schedule** dialog box can be opened.



Apply Schedule

3. In the **Schedule Name** field, select the name of the predefined schedule to be applied, then click **Apply**.

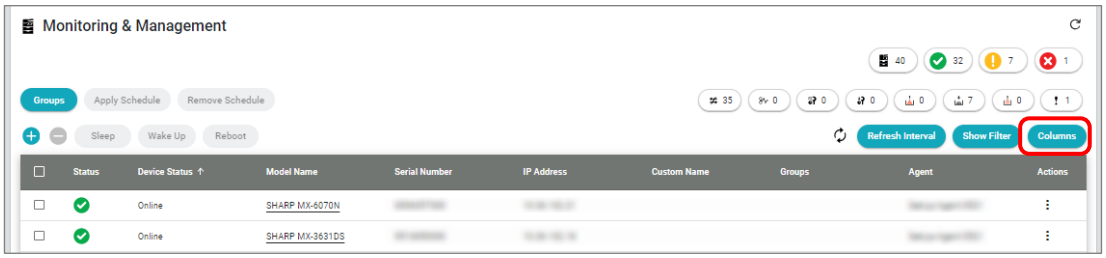
Removing a Power Management Schedule

1. Select device(s) to be removed from the power management schedule in the device list of the **Monitoring & Management** page.
2. Click **Remove Schedule** to remove the applied schedule(s). Click the Actions icon ⋮ for the device to be removed and select **Remove Schedule** from the pull-down menu.

Adding and Deleting Columns in the Device List

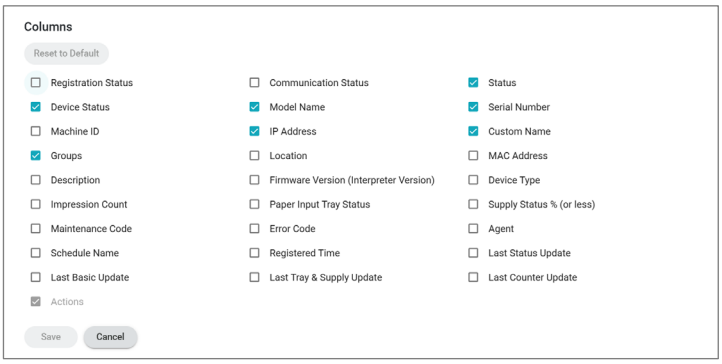
You can customize the columns for convenient access to data and information that you frequently use.
Registration Status column allows to indicate the device is imported by the system or service user via the device list.

1. Click **Columns** to open the Columns dialog box.



Monitoring & Management page

2. Select the checkboxes for the column names to be displayed.
   To reset to the default settings, click **Reset to Default**. Then, click **Save**.



Columns dialog box

Sorting the Device List

Each column in the device list (except groups and actions column) can be sorted alphabetically in ascending or descending order, using the white arrow next to the column name.

Device Status column, sorted in ascending alphabetical order

Filtering the Device List

There are two ways to filter the device list: by clicking the **Status Display Icons** or by using the **Simple Filter**.

Filtering Using the Status Display Icons

The device list can be filtered to show only devices with a specific status (e.g., only devices with a "Warning" condition, or only devices which are overdue for service maintenance), by clicking the relevant status icon in the corner of the **Monitoring & Management** page.

Device Status icons

To undo the filter and show all devices, click the Display All Devices icon .

Filtering Using Simple Filter

The simple filter allows users to search the device list using a variety of criteria, such as IP address or serial number.

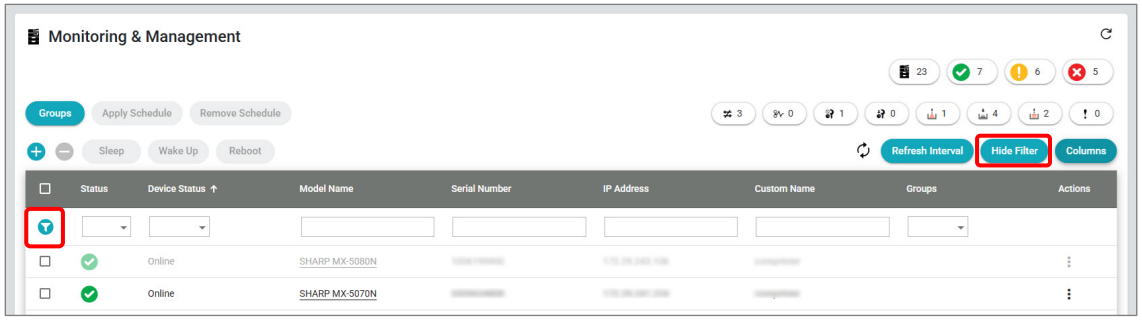
1. Click the **Show Filter** button to show the Simple Filter.

Filtering Using Simple Filter

2. Set the filtering criteria and click the Apply Filter icon .

   To clear the simple filter, click the **Hide Filter** button. While simple filter is displayed, the **Show Filter** button changes to the **Hide Filter** button.

   For guidelines and restrictions for filtering lists, go to the Glossary > Procedures > Filtering Lists.



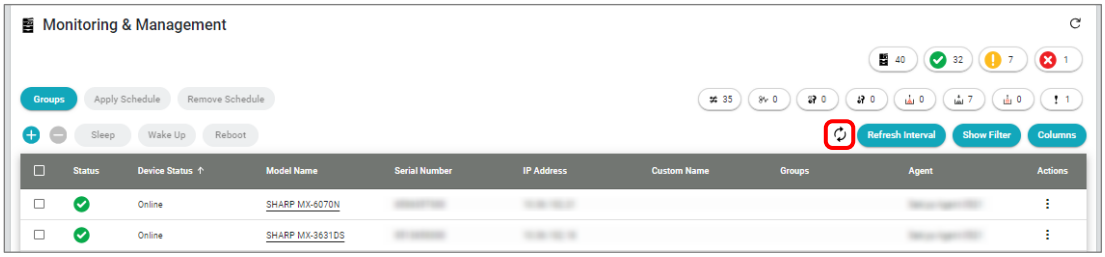
Simple Filter

Updating Device Data

Use the following steps to update device data for all devices listed in the **Monitoring & Management** page:

Refresh All Registered Devices

1. Click the Refresh all registered devices icon .



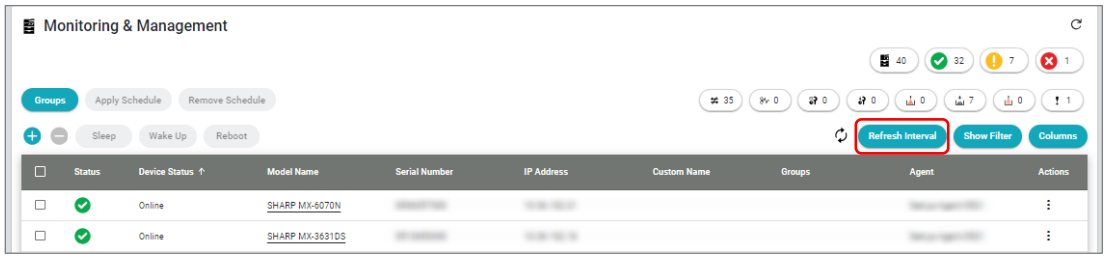
Refresh all registered devices icon

All information in the device list and the numbers shown next to the device status icons will be updated.

Auto Refresh

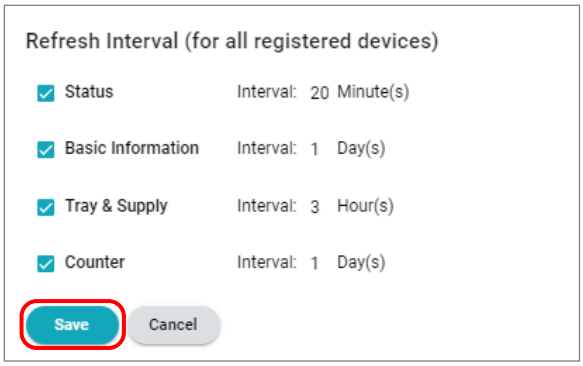
By default, device information is automatically retrieved and updated at predetermined intervals. To check the interval or change what information is included in the updates, do the following:

1. In the **Monitoring & Management** page, click **Refresh Interval**.



Refresh Interval

2. The **Refresh Interval (for all registered devices)** dialog box displays the auto refresh interval for each item and allows the user to enable/disable auto refresh for each item. After the setting is changed, click **Save**.



Refresh Interval (for all registered devices) dialog box

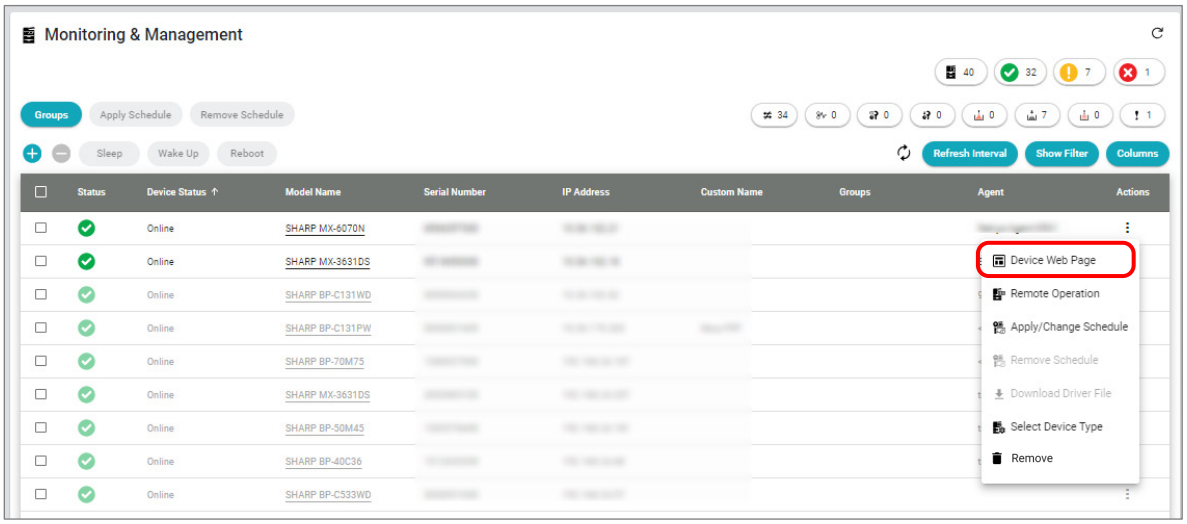
Accessing a Device Web Page

Device web page can be accessed on the **Monitoring and Management** page, and on the **Device Information** page.

Note:
The device's HTTPS settings (server port) must be enabled to view that device's web pages using Synappx Manage. In direct connection, target devices and client PCs must be connected to the same network to access device web pages.

Access device web page in the Monitoring & Management page

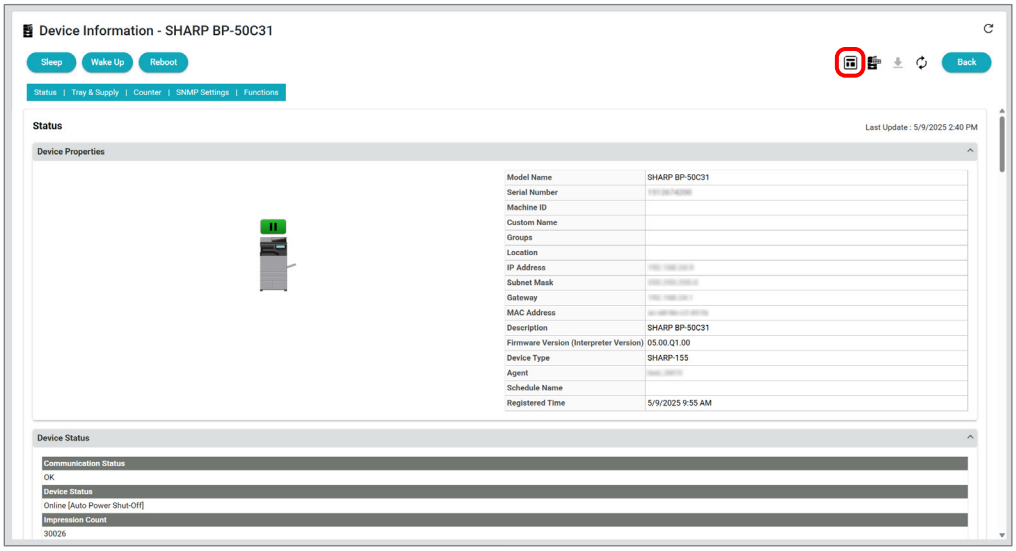
1. Click the Actions icon ⋮ in the row belonging to the device.
2. Select **Device Web Page** from the pull-down menu.



Accessing a Device Web Page via the Monitoring & Management page

Access device web page in the device Information page

1. From the device list on the **Monitoring & Management** page, click the name of the device.
2. On the **Device Information** page, select the device web page .



Accessing a Device Web Page via the Device Information page

Remote Access to Device Operation Panel

Compatible devices operation panel can be controlled remotely via Synappx Manage. To use this function, be sure to register the MFP with Agent Connection.

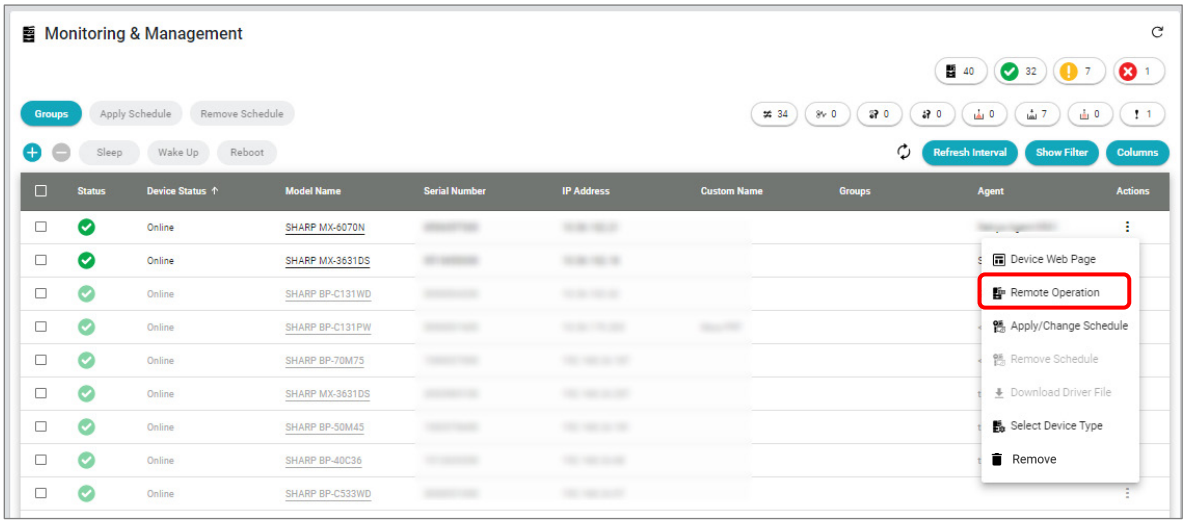
Note:

- There are differences in functions between Agent Connection and Direct Connection. In agent connection, it can remotely operate the Operation Panel via the Internet. In direct connection, it can be remotely operated only via intranet.
- Remote operation must be enabled in the device's system settings.

Accessing a Device's Operation Panel via the Monitoring & Management page

1. Click the Actions icon ⋮ in the row belonging to the device.

2. Click **Remote Operation**.



Accessing a Device Operation Panel via the Monitoring & Management page

3. Click **Connect** in the remote operation connection window.

   If the specified port number for the remote operation panel on the target device is not 5900, change the port number on the target device. Enter a password when required. If you want to change the password settings, contact your authorized service dealer.

Remote Operation Connection window

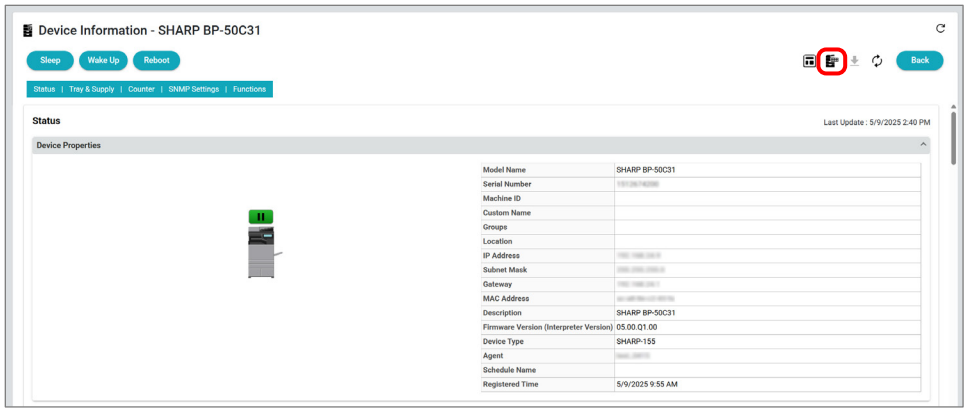
4. A confirmation dialog box is displayed, click **OK**.

Operations at device

When the confirmation screen is displayed on the device's operation panel, tap **OK**. Once connected, the device's control panel can be operated remotely.

Accessing a Device's Operation Panel via the Device Information page

1. In the Device List on the **Monitoring & Management** page, click the "Model Name" for the device.
2. In the **Device Information** page, click the Remote Operation icon .



Accessing a Device Operation Panel via the Device Information page

3. Click **Connect** in the remote operation connection window.
   (If the specified port number on the target device is not 5900, change the port number to "5900". Enter the view password as required by the device settings. If you want to change the view password settings, contact your authorized service dealer.)

Remote Operation Connection window

4. A confirmation dialog box is displayed, click **OK**.

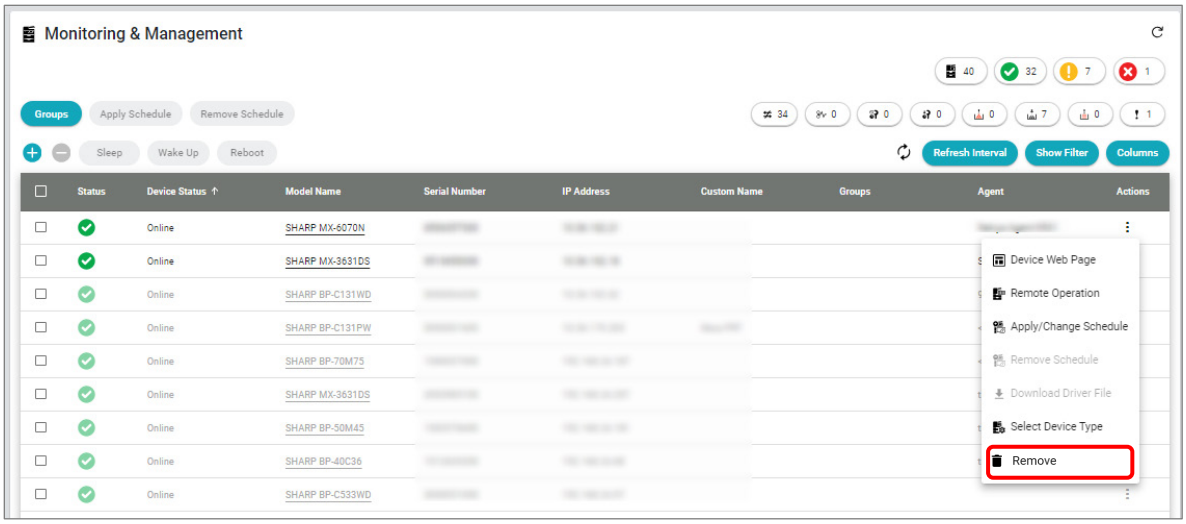
Operations at device

When the confirmation screen is displayed on the device's operation panel, tap **OK**. Once connected, you can remotely control the device's operation panel.

Deleting Devices

Information for all devices shown on the **Monitoring & Management** page can be deleted by using the following procedure:

Note:
A device cannot be restored once it is deleted. Multiple devices cannot be simultaneously deleted using this procedure. Each device must be deleted individually.



Deleting Devices

- To delete a device, click the Actions icon ⋮ for the device and select **Remove**.
- To delete multiple devices at once, select the checkboxes in first column of the devices to be removed, then click the Remove Device icon ⊖.

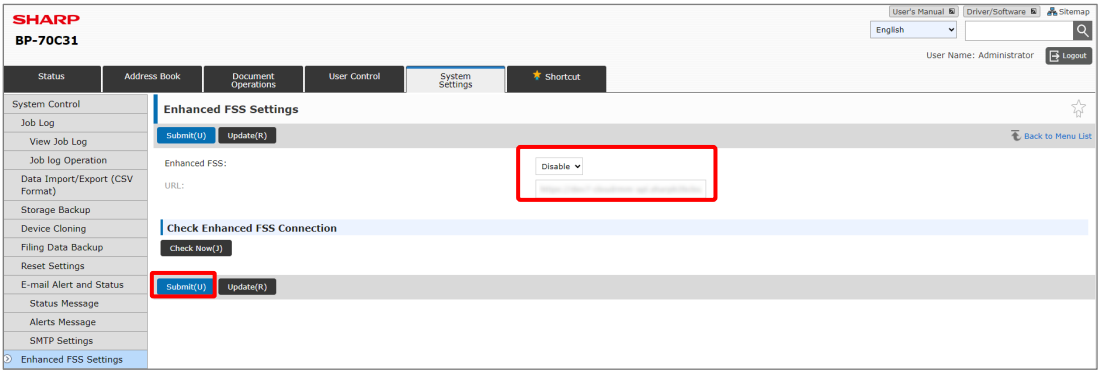
A confirmation dialog box will appear. Click **OK** to delete the device(s), or **Cancel** to cancel.

To delete an MFP connected via direct connection, the enhanced FSS settings of the device web page must be updated/removed after the above steps.

1. Connect to the following URL with browser and log in as an administrator.

<<*IP address of MFP*>>/sysmgt_enhanced_fss.html

2. Set the setting of **Enhanced FSS** to **Disable**.
3. Click **Submit** button.



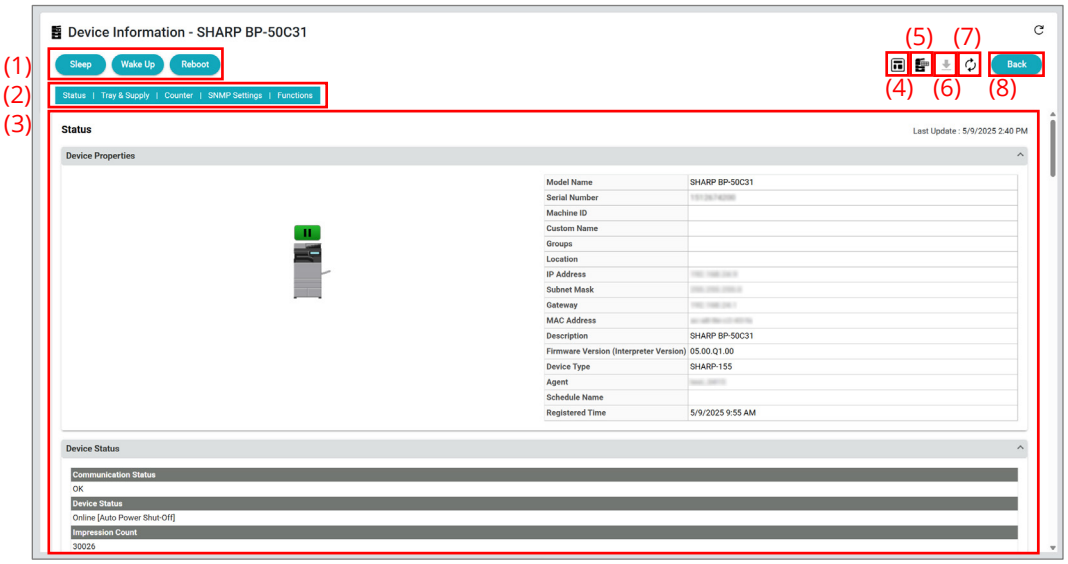
Enhanced FSS Settings page

4. Reboot the MFP.

Device Information page

In the **Model Name** column, select the target device. A **Device Information** page opens. Scroll up and down through the sections to view the device information.

Note:
The information displayed on the device information page is not automatically updated. To update the information, click the Refresh Screen icon at the top right. The information will not be updated the system cannot obtain the updated device information due to some errors (e.g., network connection errors), or the status will be shown as "N/A".



Device Information page

Buttons and Icons

(1) **Power management buttons**
Controls power management operations such as sleep, wake up and rebooting for the displayed device.

(2) **Device information links**
Scrolls to the corresponding section of the device information display area.

(3) **Device information display area**
Shows the properties and status information for the selected device.

(4) **Device web page icon**
Displays the management web page for the selected device.

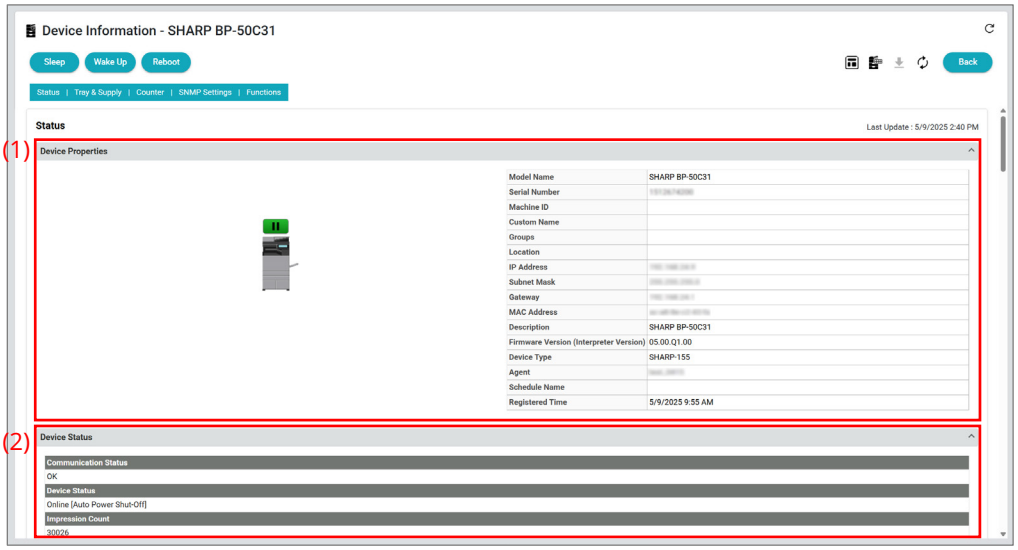
(5) **Remote Operation icon**
Activates remote operation.

(6) **Download Driver File icon**
Downloads the customized print driver file.

(7) **Refresh This Device icon**
Updates the information with the latest information from the Synappx Manage server.

(8) **Back button**
Returns to the **Monitoring & Management** page from the **Device Information** page.

Status Display Area



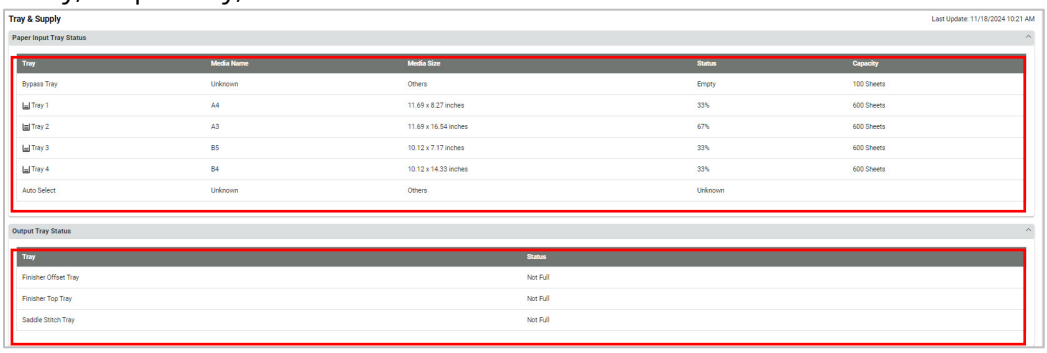
Status Display Area

(1) **Device Properties**: Model Name, Serial Number, Machine ID, Custom Name, Groups, Location, IP Address, Subnet Mask, Gateway, MAC Address, Description, Firmware Version (Interpreter Version), Device Type, Agent, Schedule Name, Registered Time.

(2) **Device Status**: Communication Status, Device status, Impression Count, Maintenance Code, Error Code.

Tray & Supply Display Area

The **Tray & Supply** display area contains detailed information about supply condition status for the input tray, output tray, and toner level.



Tray & Supply Display Area (1)

(1) **Paper Input Tray Status**
(2) **Output Tray Status**

Tray & Supply Display Area (2)

(3) **Supply Status**

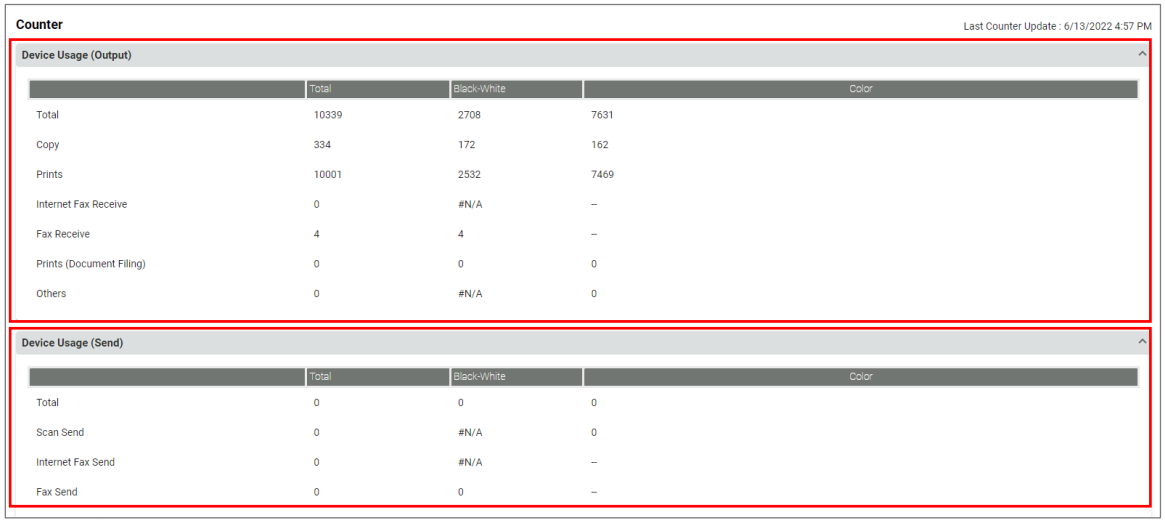
- Supply Information: Installed toner cartridges and toner collection container
- Status % (or less): Remaining toner percentage in each toner cartridge and status of toner collection container

The following information is available only in case the related data is obtained.

- Predicted Print Count: Predicted print count (Total) when toner in each cartridge will be used up based on current usage
- Predicted End Date: Predicted date when toner in each cartridge will be used up based on current usage
- Toner Forecast: Graphically displays the relationship between the remaining toner percentage of each toner cartridge and the number of printed pages, based on predictions based on current usage.

Counter Display Area

The **Counter** display area contains detailed information about the device operating status. For instance, the number of pages printed, and number of pages transmitted.



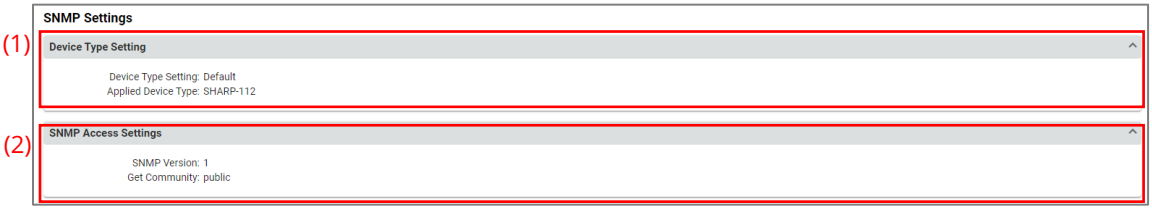
Counter Display Area

(1) **Device Usage (Output)**

(2) **Device Usage (Send)**

SNMP Settings Display Area

SNMP setting information, including SNMP version and credentials used during device discovery, are displayed here. Updated device information and the device's type setting (device family) are displayed here as well.



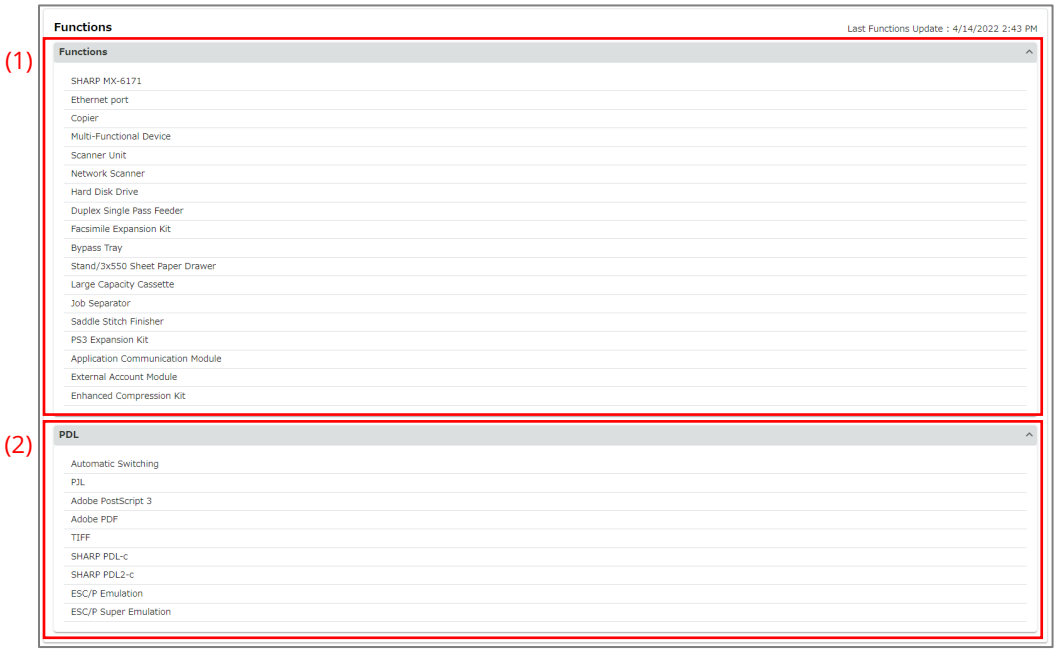
SNMP Settings Display Area

(1) **Device Type Setting**: Device Type information detected for the device. The counter information obtained from the target device via SNMP is handled based on the detected Device Type.

(2) **SNMP Access Settings**: Accesses the target device using the credentials displayed and obtains information.

Functions Display Area

The **Functions** display area displays a list of functions that are available for the device. These functions include options and printer description languages (PDL) used by the printer.



Functions Display Area

(1) **Functions**

(2) **PDL**

Managing non-Sharp Printers (Custom Device Types)

All Sharp devices are automatically mapped with the proper Sharp SNMP (Simple Network Management Protocol) OID (Object Identifier). For third-party printer management, Sharp provides a starter set of custom device types for select manufactures and models. When non-Sharp devices are discovered, generic device type is applied to the device automatically. If more detailed information is required, apply pre-loaded custom device type. Once mapped, for example, with select models, you can view total color pages vs mono pages for the third-party printer or MFP.

Available Device Types

The following device types are applied when MFP/printer devices are discovered.

For Sharp devices:

- **Sharp model specific device types**
  The model specific device type "SHARP-*model name*" is automatically applied to supported Sharp models.
- **Sharp generic device type**
  "SHARP Generic Device" will be applied to non-supported Sharp models.

For non-Sharp devices:

- **Generic device type**
  "Generic Device Type" is applied to a SNMP compliant non-Sharp device when the device is discovered through a SNMP discovery. Synappx Manage collects data from generic counter and/or toner data. The information captured via generic device types may vary per model/device.
- **Custom device type**
  Synappx Manage provides a starter set of custom device types for select manufactures and models to capture more granular data. When non-Sharp devices are discovered, Generic device type is applied to the device automatically. When more detailed information is required, apply pre-loaded custom device type. Once the pre-loaded device type is applied, for example, for select models, you can view total color pages vs mono pages for the third-party printer or MFP. You can also import SNMP OID using Synappx Manage's Custom Device Type Import feature. You can also create and edit your own Custom Device Type to match the data you wish to acquire.

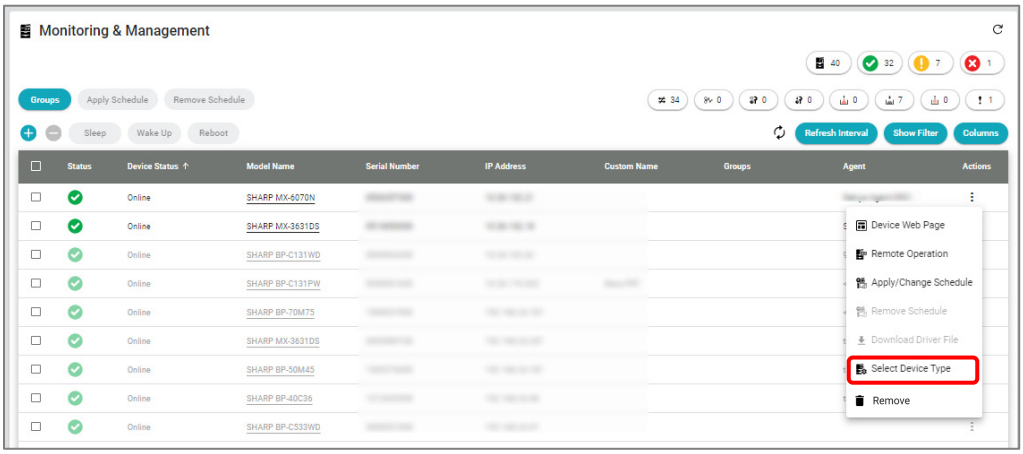
  Caution:
  Synappx Manage cannot guarantee the data accuracy from the 3rd party printers. Data types and accuracy may vary per model/device and how the device responds. The MIB (Management Information Base) definitions are subject to change by each manufacture

and Synappx Manage attempts to present the data which are obtained by the SNMP queries, based on the given MIB definitions. If you wish to add or update the pre-loaded 3rd party printer device types, contact your authorized Sharp service provider.

Mapping Device Types

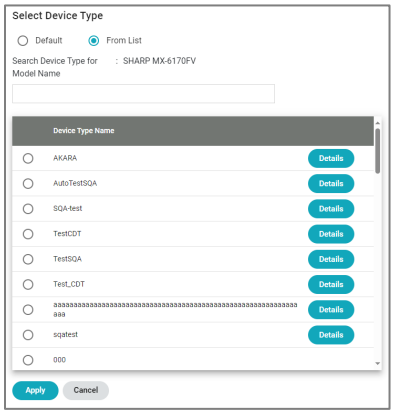
By mapping the custom device types to non-Sharp models, you may capture additional data.

1. In the MFP/Printers **Monitoring & Management** page, click the Actions icon ⋮ and **Select Device Type** from the pull-down menu to open the **Select Device Type** dialog box.



Setting a Device Type

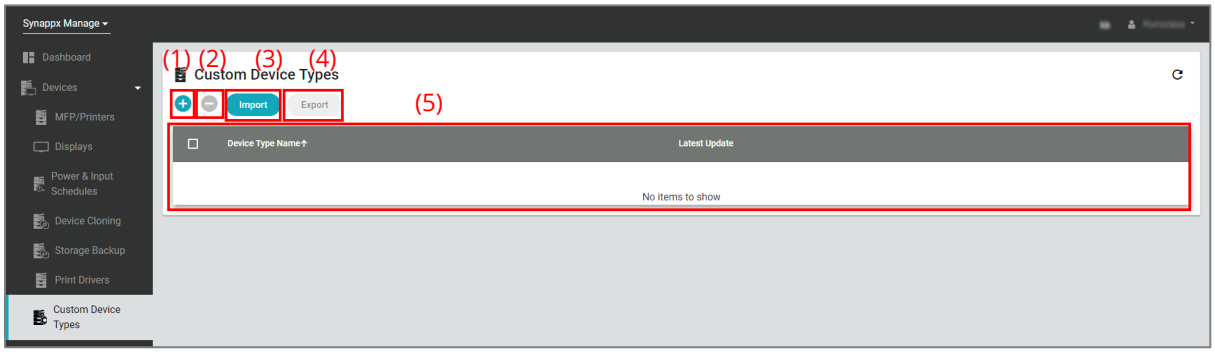
2. In the **Select Device Type** dialog, select **From List**. Device types that are added to the tenant (Adding and Saving a Custom Device Type) and pre-loaded device types will be displayed. **Details** button appears only for user registered device types. Select a device type from the list and click **Apply** button. You can type a few words to find matching device types. At the top of the dialog, you will see the model name of the selected device in the format "Search Device Type for: XXXX (Model Name)". This can be copied and entered the search box. Device type setting will be applied when device information is refreshed.



Select Device Type dialog box

Custom Device Types Page

In this page, you can create or edit your own custom device, defining the OIDs you want to get. You can export it, save it, and then import and restore it at any time.



Custom Device Types page

(1) **Add Custom Device Type icon**
Adds a new custom device type.

(2) **Remove Custom Device Type icon**
Removes the uploaded custom device type(s) from the uploaded custom device type list.

(3) **Import button**
Uploads a custom device type file.

(4) **Export button**
Downloads the specified custom device type(s).

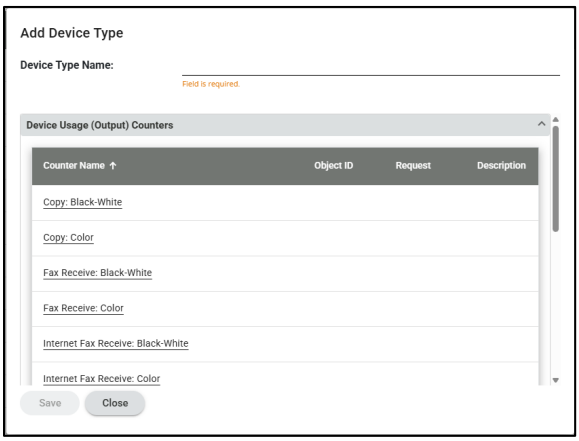
(5) **Uploaded Custom Device Type List**
Lists the uploaded custom device types.

Managing Custom Device Types

Under Devices, click **Custom Device Types** to display the **Custom Device Types** page.
The following actions can be performed from this page:

a) Adding/Saving a custom device type
b) Editing a custom device type
c) Deleting a custom device type
d) Importing/Exporting a custom device type

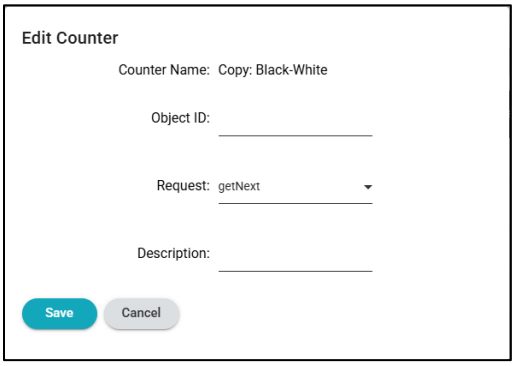
Adding and Saving a Custom Device Type



Add Device Type dialog box

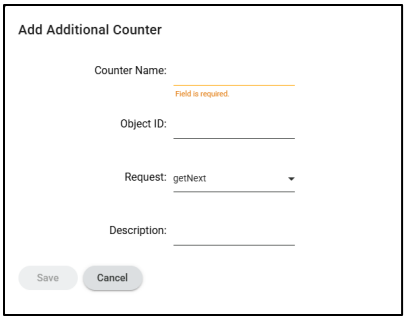
A custom device type can be created using the following procedure:

1. On the **Custom Device Type** page, click the Add Device Type icon to open the **Add Device Type** dialog box. Here, you can create a new Custom Device Type.
2. Enter the name of the new Custom Device Type into the **Device Type Name**. (Single-byte alpha-numeric, Space, "-" and "_" are valid.)
3. Register all Object IDs that correspond to counter information of another company's device into the **Device Usage (Output) Counters** area of the **Add Device Type** dialog box. Click each Counter Name to open the **Edit Counter** dialog box.



Edit Counter dialog box

   a) **Object ID**: An MIB object ID used to obtain counter information.
   b) **Request**: SNMP request type (get, getNext)
   c) **Description**: Any text (such as a name of the counter referred to from the designated object ID).
4. Click **Save**.
5. To display counter information other than the display items shown in Device Usage (Output) Counters, register them into the **Additional Counters** area. Click the Add icon at the top of the area to open the **Add Additional Counter** dialog box.



Add Additional Counter dialog box

a) **Counter Name**: Any text to be listed as a counter name.
b) **Object ID**: An MIB object ID used to obtain counter information.
c) **Request**: SNMP request type (get, getNext)
d) **Description**: Any text (such as a name of the counter referred to from the designated object ID).

6. Click **Save**.

Editing a Custom Device Type

Saved custom device types are listed in the **Custom Device Type** page. Click the name of the device type to open the **Edit Device Type** dialog box. Edit the device type as needed and save the changes.

Deleting a Custom Device Type

- To delete a Custom Device Type, click the Trash icon .
- To delete multiple Custom Device Types at once, select the checkboxes of the Custom Device Types to be deleted, then click the Remove Custom Device Type icon .

A confirmation dialog box will appear. Click **OK** to delete the Custom Device Type.

Importing/Exporting Custom Device Type(s)

Custom device type files (JSON) exported from Synappx Manage can be imported.

1. Click **Import** to open the **Import Device Type** dialog box.
2. Click **Browse** to navigate to the folder where the Custom Device Type file was saved.
3. Select the file and click **Open**. The selected file name will appear in the File Name field.
4. Click **Import** to start uploading.

   Note:
   If a custom device type with the same name has already been registered, it cannot be imported.

Exporting a Custom Device Type

1. Select the checkboxes for the Custom Device Type to be exported.
2. Click **Export** to start downloading the file.

   Note:
   When multiple custom device types are selected for export, they will be combined into one file. When importing a file with multiple custom device types, the device types will be split and saved. You can also check the import results in the **Device Type Import Results** dialog box that appears after importing.

Display Management

To manage display devices, the display devices need to be registered to the Synappx Manage. The target display devices must be configured to connect to a local area network (LAN), and the RS-232C/LAN SELECT communication setting must be set to LAN.

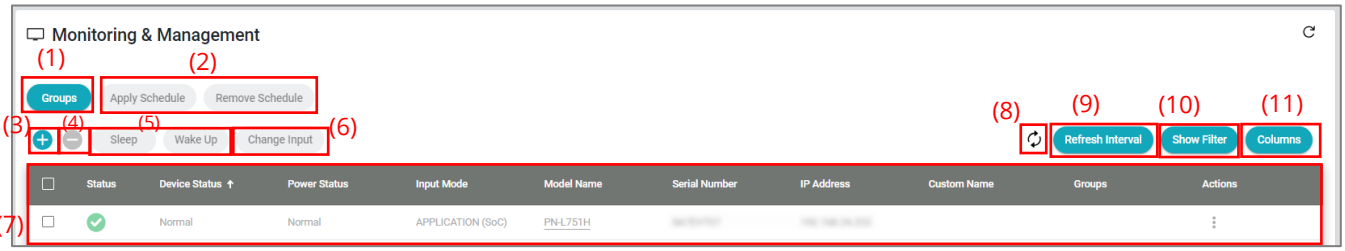
The display devices need to be awake for Synappx Manage to retrieve device information, as well as to perform remote control.

Cautions:

- When POWER SAVE MODE is ON and the device is in standby mode, remote control is not available.
- When the device is in the input signal waiting mode (Energy Mode is set to home mode), remote control is not available.
- When the display device's power is off, Synappx Manage may not be able to retrieve information, or the display may not accept commands.

Monitoring & Management page

The **Monitoring & Management** page allows you to access key information and actions for the managed devices.



Displays Monitoring & Management page

Buttons and Icons

(1) **Groups button**

Assigns a group name to each display. Devices that are assigned the same group name are managed together as a group.

(2) **Schedule buttons (Apply/Remove)**

Manage scheduled power operations.

(3) **Register Device icon**

Adds a new display from the devices that appear in the "(7) Device List".

(4) **Remove Device icon**

Removes the selected display(s) from the devices that appear in the "(7) Device List".

(5) **Power management buttons**
Used to sleep or wake up a compatible device.

(6) **Change Input button**
Changes the input source of the device.

(7) **Device List**
Displays a list of registered devices. By clicking the model's name, you can view detailed information of each device. The list can be sorted and filtered by clicking the **Show Filter** button.

(8) **Refresh all registered devices icon**
Refresh and update the device information.

(9) **Refresh Interval button**
Allows users to automatically update information after a predetermined period.

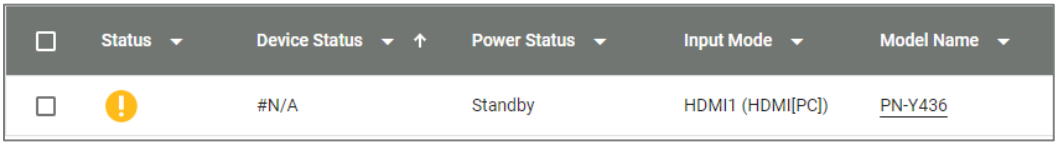
(10) **Show Filter button**
Allows user to use simple filter. For more detail of simple filter, refer "Filtering Using Simple Filter".

(11) **Columns button**
Adds or removes columns displayed in the Device List.

Device Status

The status of each device is shown on the **Monitoring & Management** page.

- The **Status** column uses visual icons to show general status ("Normal", "Error" or "N/A").
- The **Device Status** column contains a more specific description of the status.



Device Status column

Power Management

Synappx Manage can be used to remotely access device's power, such as sleep and wake up for supported devices.

The Power Management options are available on the **Monitoring & Management** page and the **Device Information** page. On the **Monitoring & Management** page, multiple devices can be selected, and the same power management operation is applied to all selected devices.

After selecting a power state transition, a confirmation box is displayed.

Display Input Management

Device input mode can be managed on the **Monitoring & Management** page or the **Device Information** page. On the **Monitoring & Management** page, the input mode policy can be applied to all selected devices. On the **Device Information** page, the input mode is applied to the selected device.

Note:

- Available input modes will vary depending on the display model. Some display models may not support remote control, or the list may not contain all supported methods. For more information, refer to the display's Operation Manual.
- If the desired input mode is not found in the pull-down menu, select **Toggle change for input mode** and click **Send** until your desired input mode is obtained on the target display.

Via the Monitoring & Management page

1. In the device list, select the devices to apply the input policy.
2. Click **Change Input** to open the **Change Input** dialog box.
3. Click the **Select Input** area to open a list of available input modes.
4. Select the desired input mode.
5. Click **Send** to request the device to change input mode.

Via the Device Information page

1. Click **Change Input** to open the **Change Input** dialog box.
2. Click the **Select Input** area to open a list of available input modes.
3. Select the desired input mode.
4. Click **Send** to request the device to change input mode.

After defining the input policy, a confirmation box "Command Send is succeeded" will be displayed. Click **OK**.

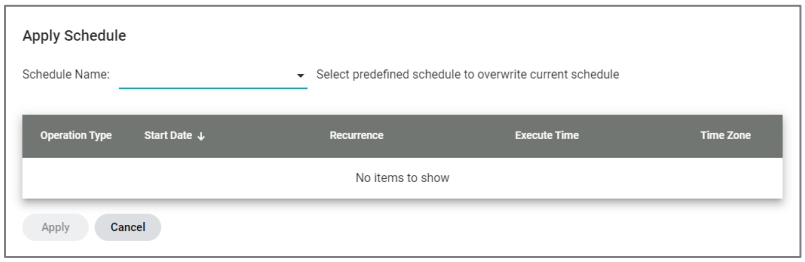
Deploying Scheduled Power & Input Management

The power & input policy can be deployed automatically at scheduled intervals. (Go to Power & Input Schedules Management for policy setups)

Follow the steps to apply power management schedule to a device or devices.

1. In the device list on the **Monitoring & Management** page, select the device(s) to which you want to apply the power management schedule.

2. Click **Apply Schedule** to open the **Apply Schedule** dialog box.



Apply Schedule dialog box

Note:
The **Apply/Change Schedule** dialog box can also be opened from the Actions icon ⋮ and selecting **Apply/Change Schedule**.

3. In the **Schedule Name** field, select the name of the predefined schedule to be applied.
4. Click **Apply**.

Removing a power management schedule from a device

Select device(s) to be removed from the power management schedule in the Device List on the **Monitoring & Management** page. Click **Remove Schedule**.

Basic Functionality of the Monitoring and Management Page

Like the MFP/printer device management, each device information is displayed on the device list. You can manage columns, sorting and filtering the device list. Follow the links for more information.

- Adding and Deleting Columns
- Sorting the Device List
- Filtering the Device List
- Updating Device Data

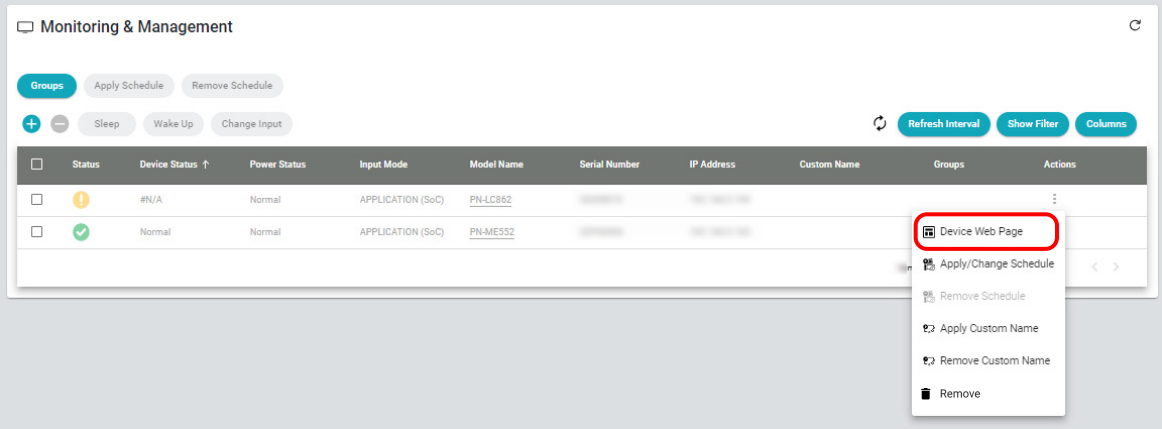
Accessing a Device Web Page

There are two ways to access device web pages from Synappx Manage. One is via the **Monitoring & Management** page; the other is via the **Device Information** page for the device.

Note:
Device webpage access is available on the device which has embedded webpage on the hardware. The target device and the display PC must be connected to the same network.
To access device's web page:

Accessing a device web page in the Monitoring & Management page

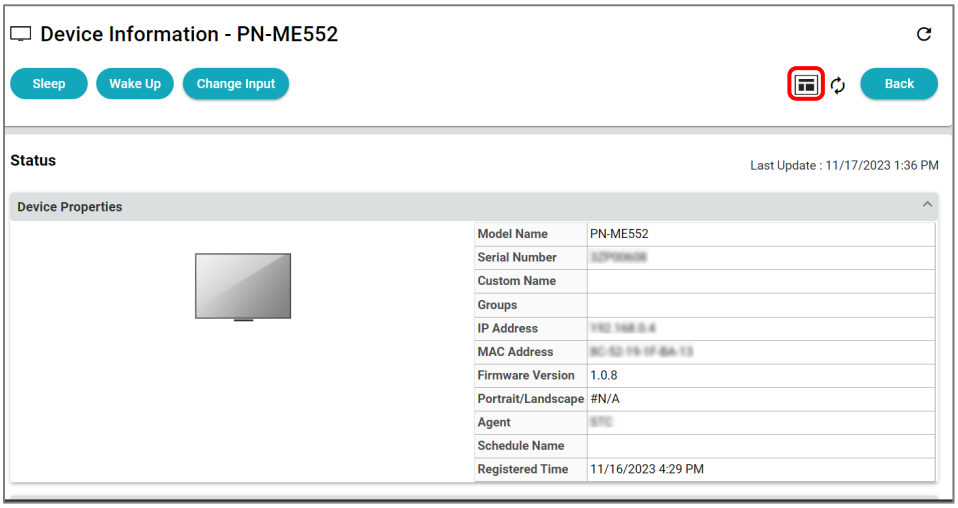
1. Click the Actions icon ⋮ in the row belonging to the device.
2. Select **Device Web Page** from the pull-down menu.



Accessing a Device Web Page via the Monitoring & Management page

Accessing a device web page via the Device Information page

1. In the device list of the **Monitoring & Management** page, click the model's name to open the device's information page.
2. Click the Device Web Page icon .



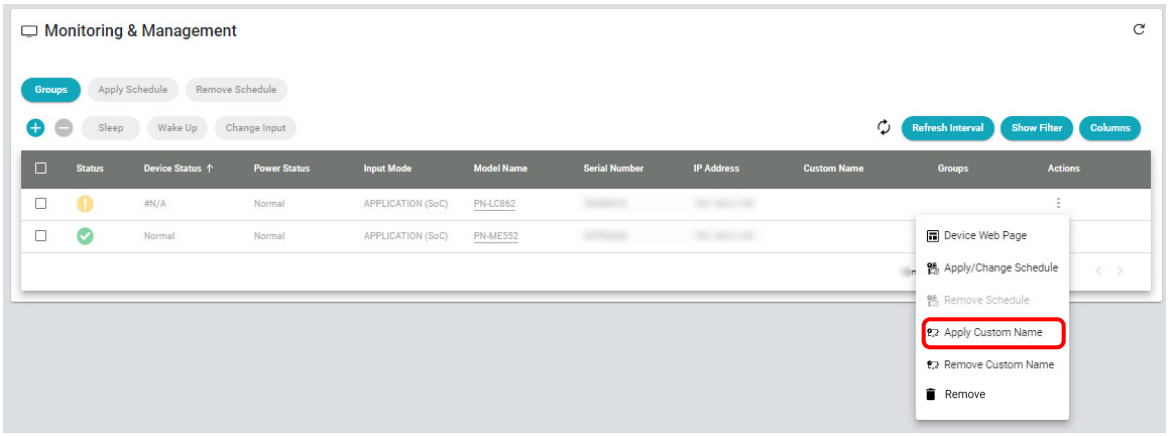
Accessing a Device Web Page via the Device Information page

Applying a Custom Name

Custom names would help you to find target devices in the Synappx Manage.

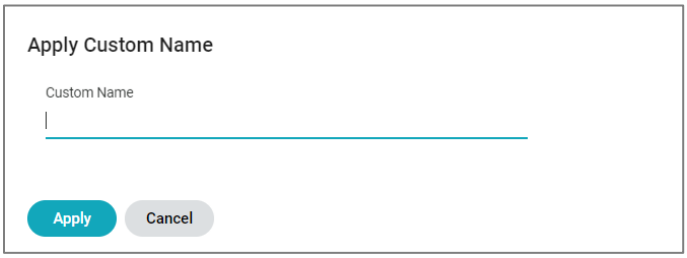
To create a custom name, follow the steps below.

1. Click the Actions icon ⋮ for the device.
2. Select **Apply Custom Name** from the pull-down menu to open the **Apply Custom Name** dialog box.



Apply Custom Name in pull-down menu

3. Enter an optional character string to identify the device. (Up to 64 characters). Click **Apply**.



Apply Custom Name dialog box

Removing a Custom Name

To remove a custom name, click the Actions icon ⋮ for the device and select **Remove Custom Name** from the pull-down menu.

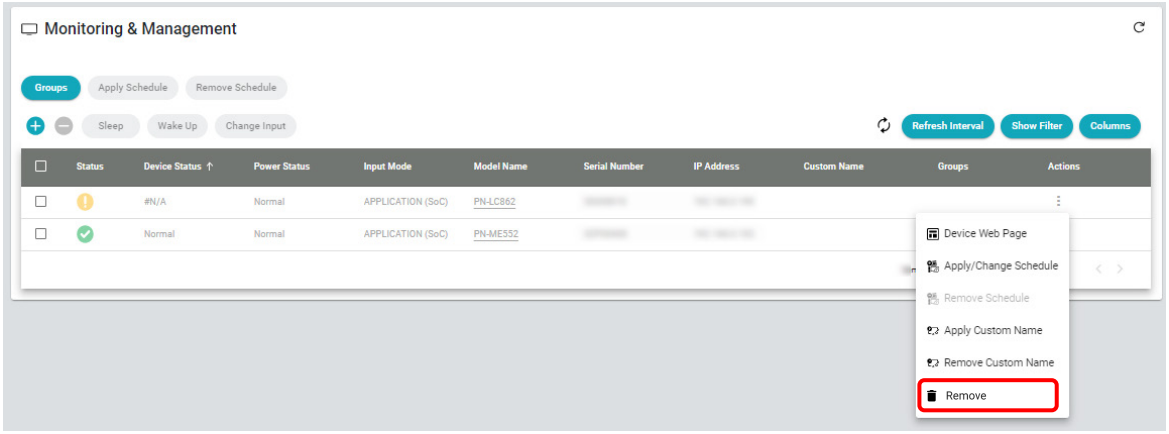
Deleting Devices

Devices can be deleted using the following procedures:

- To delete one device, click the Actions icon ⋮ for the device to be deleted, then select **Remove**.
- To delete multiple devices simultaneously, select the checkboxes for the devices to be removed, then click the Remove Device icon ⊖. A confirmation dialog box will appear. Click **OK** to delete the device.

Note:

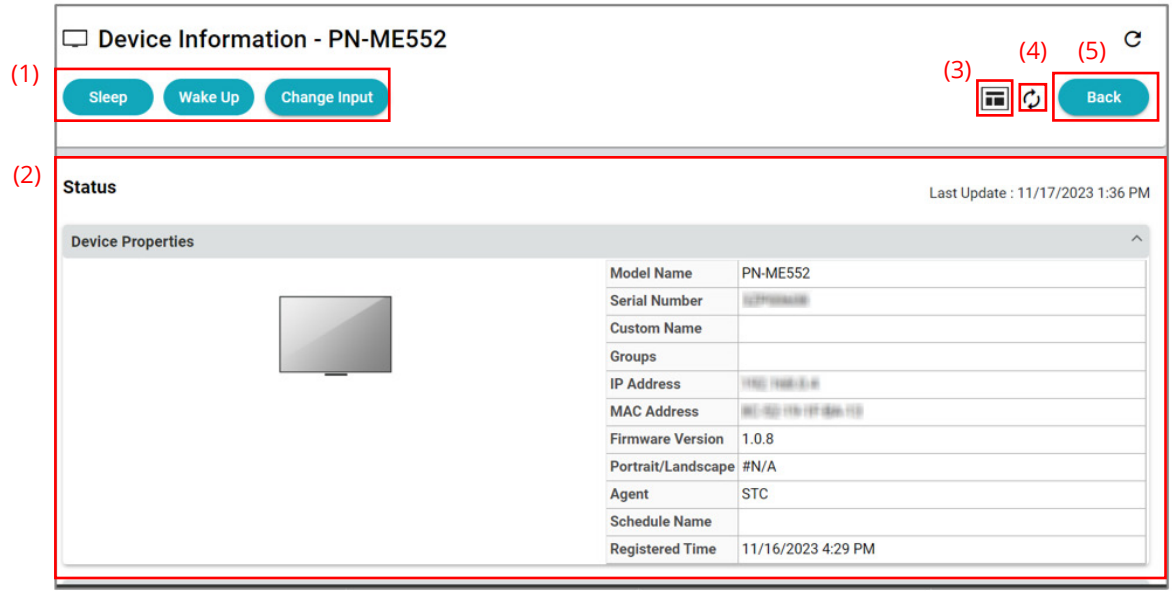
A device cannot be restored once it has been deleted. The only way to add it again is to re-register the device.



Deleting Devices

Device Information page

Click the **Model Name** for the device to show a page containing device information.



Device Information page

Buttons and Icons

(1) **Device operation buttons**
Carry out power operations such as sleep, wake up, and changing the input of the display device. (Go to Power Management Operations for details on using the **Sleep** and **Wake Up** buttons, and Display Input Management Operations for details on using the **Change Input** button.)

(2) **Device status display area**
Shows the properties and status information for the selected device.

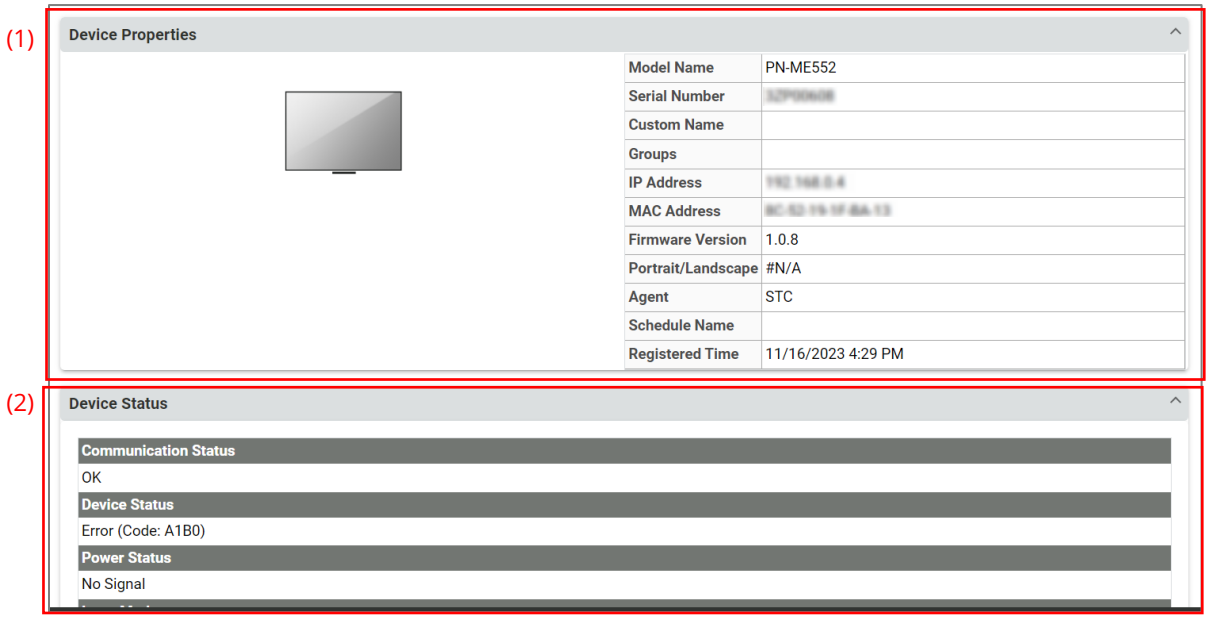
(3) **Device web page icon**
Click the device web page button to display the management web page for the selected device.

(4) **Refresh This Device icon**
Updates the information with the latest information from the Synappx Manage server.

(5) **Back button**
Click the **Back** button to return to the **Monitoring & Management** page from the **Device Information** page.

Note:
The information displayed on the device information page is not automatically updated. To update this information, return to the **Monitoring & Management** page. When the corresponding information cannot be obtained in case of errors (e.g., network errors), the value will not be updated, or "N/A" will be displayed for the status. To open the device web page, the target display and the display PC must be connected to the same network.

Status Display Area



Status Display Area

(1) **Device Properties**: Model Name, Serial Number, Custom Name, Groups, IP Address, MAC Address, Firmware Version, Portrait/Landscape (installing direction), Agent, Schedule Name, Registered Time

(2) **Device Status**: Communication Status, Device Status, Power Status, Input Mode, Brightness, Color Mode, Screen Size, Volume, Mute, Temperature Sensor, Temperature, Usage time

The following items are available in the device information page:

Items	Contents
Device Status	Only displayed for compatible models. (For incompatible models, "N/A" is displayed.) Shows the result of monitoring the display hardware. If an abnormality is detected, contact a SHARP dealer.
Temperature Sensor	Shows the status of the sensor-based temperature monitoring. A code is displayed when an abnormal temperature is detected. For more information, refer to the RS-232C command table in the display's Operation Manual.

Items	Contents
Temperature	Shows the temperature (°C) detected by the display's sensors; if there are multiple sensors, readings will be displayed with commas separating them
Usage Time (Approx. Hours)	Shows the total operating time (approximate, unit: hours). When the AC power supply to the display is cut off, the "minutes" information of the operating time will be reset.

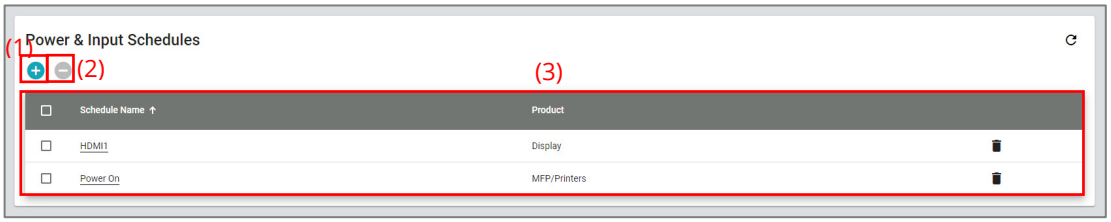
Power & Input Schedule Management

You can create a power management schedule for **Sleep**, **Wake Up** and **Reboot** (Reboot for MFPs/printers only). For displays, if a change is made while a device is off or asleep, the input will be changed following the set policy when the device wakes up.

Note:
The procedure for creating schedules is basically the same for both MFPs/printers and displays. The setting dialog box varies slightly depending on whether the schedule is being set for an MFP/printer or a display.

Power & Input Schedules page

Schedules can be managed using the **Power & Input Schedules** page.



Power & Input Schedules page

(1) **Add Power & Input Schedule icon**
Adds a new power & input schedule. (Refer to Adding New Power & Input Schedule for details.)

(2) **Remove Power & Input Schedule icon**
Removes the selected power & input schedule(s) from the predefined schedule list.

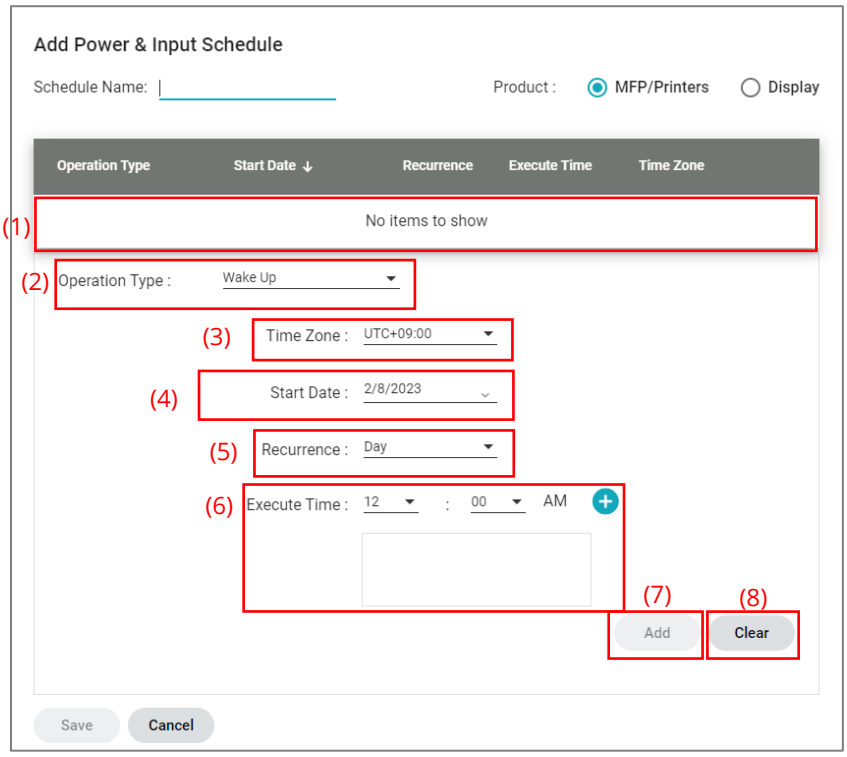
(3) **Predefined Schedule List**

Adding New Power & Input Schedule

1. In the **Power & Input Schedules** page, click the Add Power & Input Schedule icon to open the **Add Power & Input Schedule** dialog box.
2. Enter a schedule name in the **Schedule Name** field.
3. Select **MFP/Printers** or **Display** as the target product for the schedule to be defined.
4. Make the required settings. (See the Settings for MFP/Printers section or Power Management section for Displays) and click **Save**.

Schedule Settings for MFP/Printers

When **MFP/Printers** are selected in the **Add Power & Input Schedule** dialog box, the following settings will be displayed:



Add Power & Input Schedule dialog box for MFP/Printers

The following settings can be made for MFPs/printers.

(1) **Scheduled Operation List**: Lists the scheduled operations.

(2) **Operation Type**: **Wake Up**, **Sleep** or **Reboot**.

(3) **Time Zone**: Select the time zone.

(4) **Start Date**: Specifies the date to start the scheduled operation.

(5) **Recurrence**: Sets the recurrence interval (**Day** or **Week**) of the scheduled operation.

(6) **Execute Time**: Specifies the execution time of the scheduled operation. To add the time, select the hour and minute from the respective pull-down lists and click the Add Time icon .

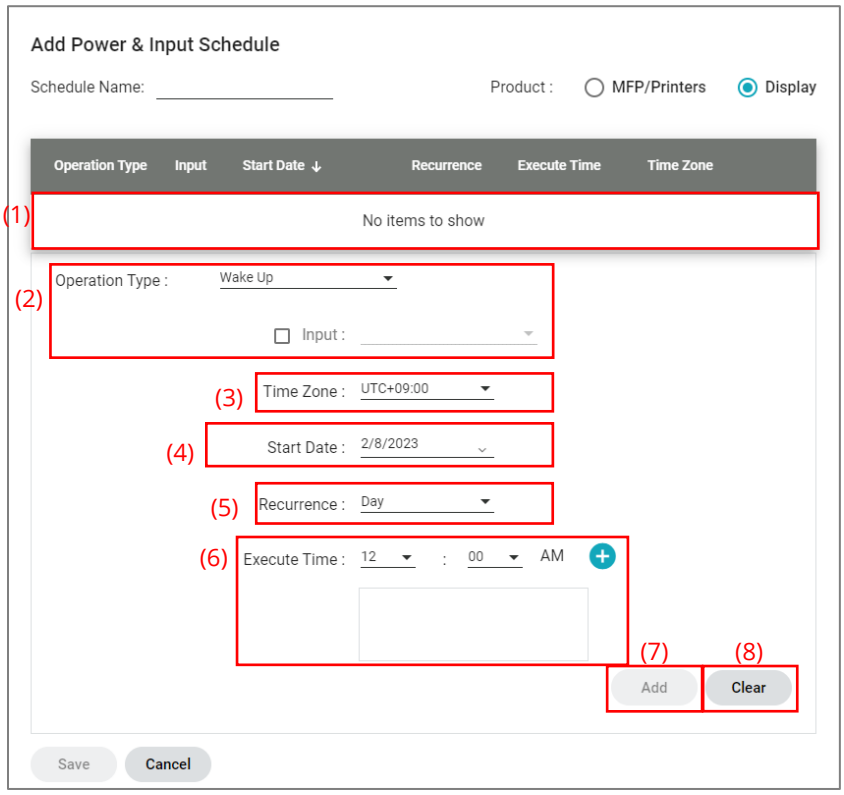
Multiple times can also be specified. Click the Trash icon to remove the time.

(7) **Add button**: Adds the configured settings into the "(1) Scheduled Operation List".

(8) **Clear button**: Clears the configured schedule settings that have not yet been added to the "(1) Scheduled Operation List".

Schedule Settings for Displays

When **Display** is selected in the **Add Power & Input Schedule** dialog box, the following settings will be displayed:



Add Power &Input Schedule dialog box for Display

The options for display settings are the same as the options for MFPs/printers, However, in **Operation Type** for displays, the input mode can be changed after returning from a power standby state. After selecting **Input** with the checkbox, select the input mode to be switched.

Editing Power & Input Schedule

1. In the **Power & Input Schedules** page, click the schedule name to open the **Edit Power & Input Schedule** dialog box.
2. Edit the settings as desired (except Product selection) and click **Save**.

Deleting Power & Input Schedule

- To delete a schedule, click the Trash icon .
- To delete multiple schedules at once, select the checkboxes of the devices to be deleted, then click the Remove Power & Input Schedule icon .

A confirmation dialog box will appear. Click **OK** to delete the schedule, or **Cancel** to cancel.

Device Cloning and Storage Backup

Device Cloning and Storage Backup copy configurations between devices to minimize setup requirements for multiple devices. **Device Cloning** copies the device configurations and registration information from one MFP/printer (source device) to other compatible MFPs/printers (target devices). This enables the user registration feature to be performed on multiple devices simultaneously. **Storage Backup** copies address book data and user information between MFPs/printers.

Cautions:
Cloning across different model families is not supported due to differences in setting values. Device Cloning is not available for the devices managed by Active Directory (AD) Sharp security group policy. Synappx Manage will not overwrite the AD policy. Device specific values such as IP address, device name, serial number, machine code as well as cloud connect (enable/disable), product keys, and device certificate will not be cloned.

Cloneable Items:
Cloneable items are listed below. It may vary depending on the device model.

Function	Cloneable items
Device Cloning	Application Settings (Excluding Pre-Set Text/Forward Table), Billing Code, Copy Settings, Custom Link Setting, Data Receive/Forward Settings, Default Settings, Device Control, Document Filing Settings, E-mail Alert And Status, Energy Save, Fax Settings, Image Send Settings, Internet Fax Settings, Keyboard, Manual Fax Receive, Network Settings, Operation Settings, Port Control/Filter Settings, Printer Condition Settings, Printer Settings, Scan Settings, Security Settings, Sharp OSA Settings, Shortcut Key, Tray Settings, User Control
Storage Backup	Address Book, Copy (Pre-set Text), Image Send (Pre-set Text), Job Programs, Metadata Set, User Register Information

Prerequisites for Using Device Cloning & Storage Backup

Go to MFP/Printers management for information on the device models that support device cloning and storage backup.

Before following the procedures involved in device cloning and storage backup, the administrator password must be set for each device used in Synappx Manage. To use device cloning and storage backup functions, the target device must meet the following conditions:

- HTTPS communication should be enabled.
- The ports to be used for HTTPS should be 443.
- The “Data Backup (Send)” feature should be enabled.

Note:
If a user does not have permission to use the device cloning or storage backup functions, **Device Cloning** and **Storage Backup** option will not be displayed in the Synappx Manage portal menu.

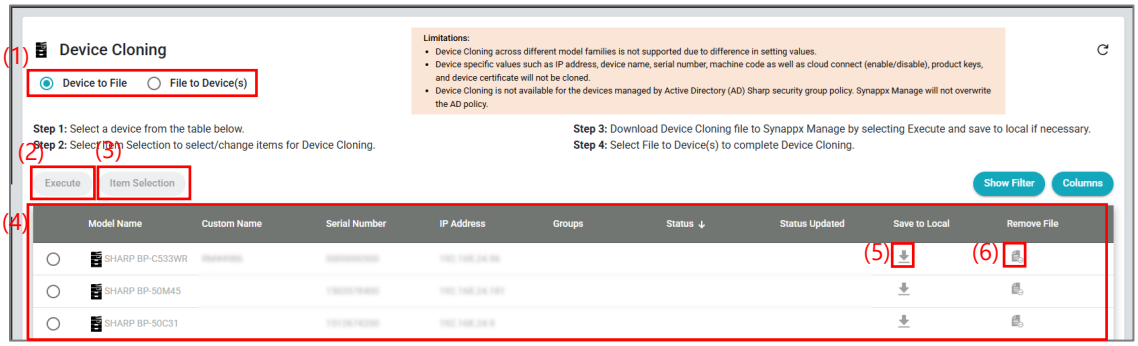
Device Cloning

The device cloning feature copies setting/configuration information from one device to other devices. Be sure to follow the steps below.

A copy of the source device data must be made using the Device-to-File procedure, then that data can be applied to the target device using the File-to-Device procedure.

Device Cloning page – Device to File

Device Cloning – Device to File must be performed first. This feature saves a file containing the settings for the specified items.



Device Cloning page – Device to File

(1) **Operation selection**: **Device to File** should be selected. Switch to the Device to File settings screen.

(2) **Execute button**: Downloads and saves the Device Cloning file according to the specified settings.

(3) **Item Selection button**: To select items to be contained in the cloning file from available cloning item lists.

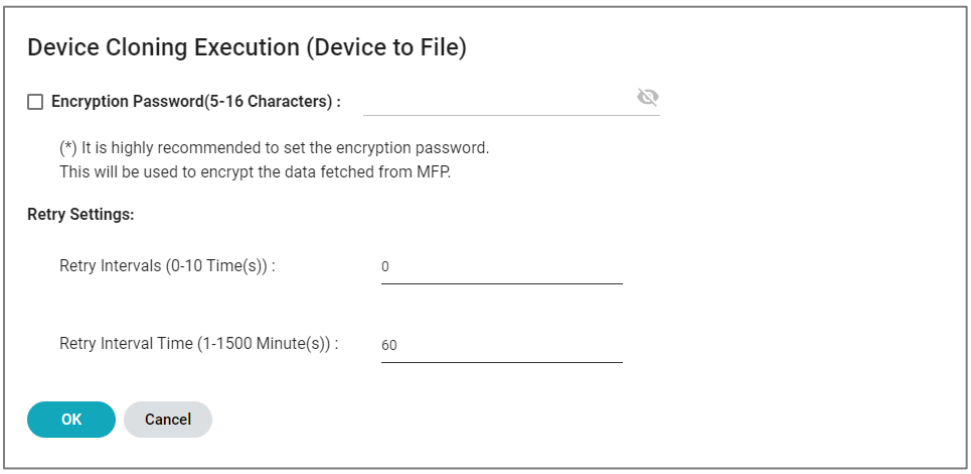
(4) **Source Device List**: Select one device to be the source.

(5) **Save to Local button**: Download the file saved in the cloud to local. It is activated when the file is saved to the cloud by the **Execute** button.

(6) **Remove File button**: Delete the file saved in the cloud. It is activated when the file is saved to the cloud by the **Execute** button.

Downloading and Saving the Device Cloning file

1. On the **Device Cloning** page, select **Device to File** to switch to the Device to File settings screen.
2. To find the device to retrieve the Device Cloning file more easily, click **Show Filter** to open the filter function.
3. Select one device to be the source. The **Item Selection** button will be enabled.
4. Click **Item Selection** to open the **Item Selection** dialog box. Select the items to be contained in the Device Cloning file.
5. Click **Save**.
6. Click **Execute** to open the **Device Cloning Execution (Device to File)** dialog box. If necessary, change any settings you wish to change in the dialog box.

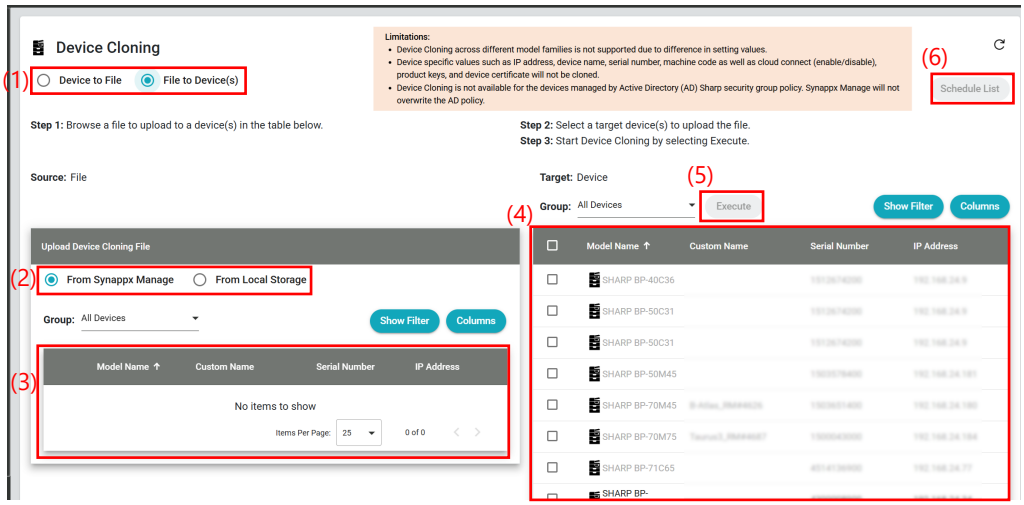


Device Cloning Execution (Device to File) dialog box

7. Click **OK** to start downloading the file. Files downloaded here are stored in the cloud.
   To save this file locally, click the **Save to Local** button.
   To delete this file from cloud, click the **Remove File** button.

Device Cloning page – File to Device(s)

Device Cloning – File to Device(s) clones to the specified device(s) with the saved Device Cloning file.



Device Cloning page – File to Device(s)

(1) **Operation selection**: **File to Device(s)** should be selected. Switch to the File to Device(s) settings screen.

(2) **Source File selection**

- **From Synappx Manage**: See "(3) Cloud-Saved File List"
- **From Local Storage**: For the Device Cloning file for the device (See "Downloading and Saving the Device Cloning file"), or directly from the device's web page.

(3) **Cloud-Saved File List**: In Device to File, files saved in the cloud are displayed here.

(4) **Target Device List**: Select a target device or devices to clone.

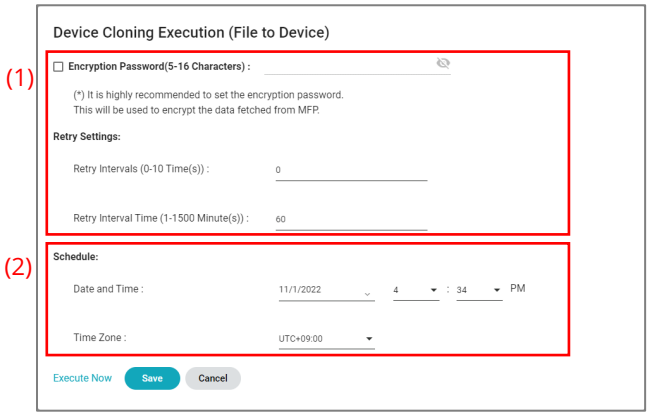
(5) **Execute button**: Execute to clone now or set a schedule.

(6) **Schedule List button**: Manages File-to-Device schedule.

Uploading the Device Cloning file to Target Device(s)

1. In the **Device Cloning** page, select **File to Device(s)** to switch to the File to Device(s) settings screen.
2. To find the Device Cloning file, select **From Synappx Manage** or **From Local Storage**.
   - **From Synappx Manage**: Select a file from cloud-saved file list.
   - **From Local Storage**: Click **Browse** to navigate to the folder where the Device Cloning file was saved. Select the file and click **Open**. The selected file name will appear in the **Upload Device Cloning File** area.
3. To list the device(s) to be uploaded the Device Cloning file, select **Group**.
4. Select one or more device(s) to be the target.

5. Click **Execute** to open the **Device Cloning Execution (File to Device)** dialog box. If necessary, make the necessary settings in the upper part of dialog box. (Area (1) in the figure)



Device Cloning Execution (File to Device) dialog box

6. Device Cloning can be executed immediately or at a scheduled time.
   - To perform Device Cloning now, click **Execute Now**.
   - To perform Device Cloning at a scheduled time, specify the Schedule (Area (2) in the figure), and click **Save**. Once **Save** is clicked, "(6) **Schedule List** button" becomes valid.

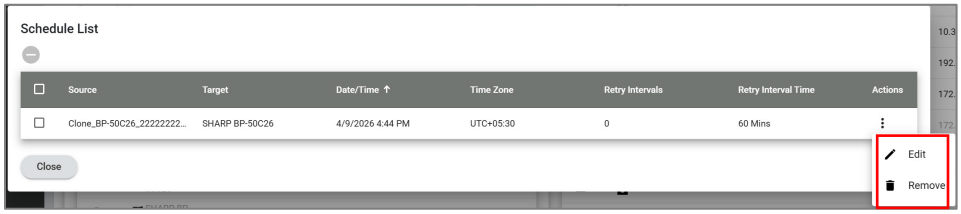
Managing the Scheduled Device Cloning – File to Device(s) operation

Scheduled Device Cloning operations can be edited or deleted. Click **Schedule List** to open the **Schedule List** dialog box.

- To edit a schedule, click the Actions icon ⋮ for the schedule to be edited. Select **Edit**.
- To delete a schedule, click the Actions icon ⋮ for the schedule to be deleted. Select **Remove**.
- To delete multiple schedules at once, select the checkboxes of the schedules to be deleted, then click the Remove Schedule icon ⊖.

A confirmation dialog box will appear. Click **OK** to delete the schedule.

Note:
Schedules will be deleted after execution is completed.



Schedule List dialog box – Edit or Remove

Storage Backup

The storage backup feature lets you save the data such as address book information and user information from a device and copy them back to the device or move the data to other devices.

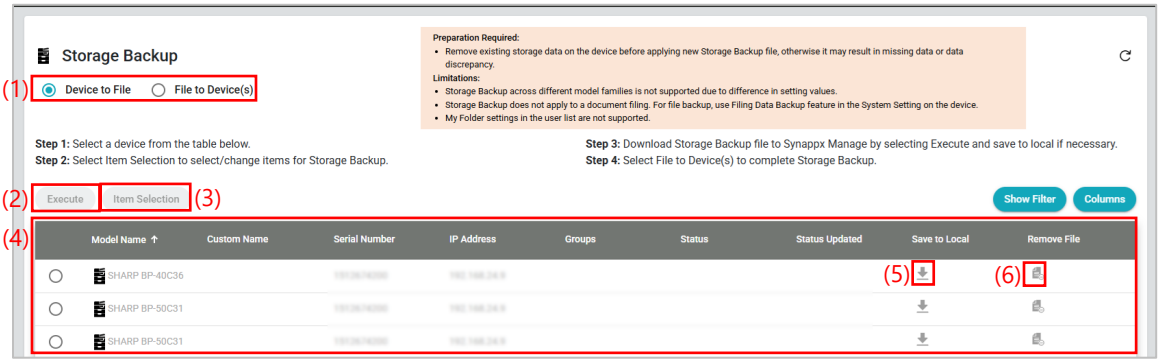
A copy of the source device data must be made using the Device-to-File procedure, then the data can be applied to the target device using the File-to-Device procedure.

Cautions:

Remove existing storage data on the device before applying new storage backup file, otherwise it may result in missing data or data discrepancy. The storage backup does not apply to document filing. For file backup, use the Filing Data Backup feature in the System Setting on the device. In addition, My Folder settings in the user list are not supported.

Storage Backup page – Device to File

Storage Backup – Device to File allows users to create a storage backup file containing specified items such as address book data.

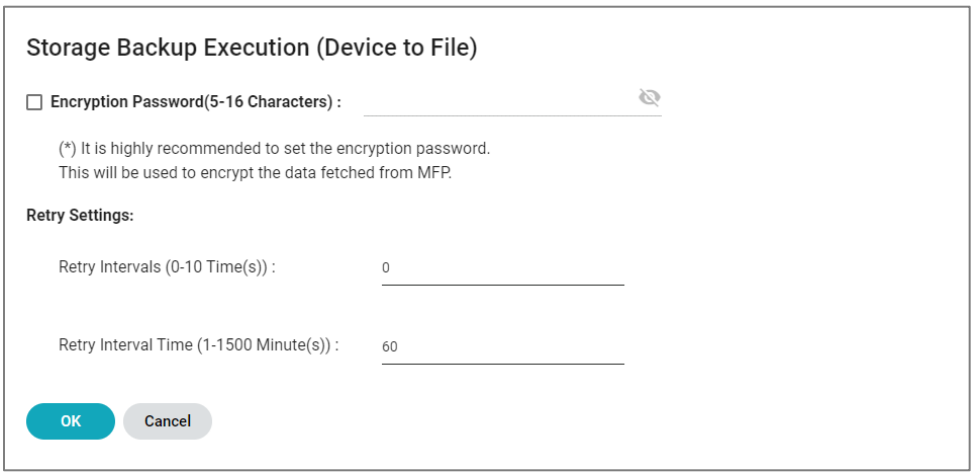


Storage Backup page – Device to File

(1) **Operation selection**: **Device to File** should be selected. Switch to the Device to File settings screen.
(2) **Execute button**: Downloads and saves the Storage Backup file according to the specified settings.
(3) **Item Selection button**: **Item Selection** allows users to select items to be contained in the Storage Backup file from available cloning item lists.
(4) **Source Device list**: Select one device to be the source.
(5) **Save to Local button**: Download the file saved in the cloud to local. It is activated when the file is saved to the cloud by the **Execute** button.
(6) **Remove File button**: Delete the file saved in the cloud. It is activated when the file is saved to the cloud by the **Execute** button.

Download and Save the Storage Backup file

1. In the **Storage Backup** page, select **Device to File** to switch to the Device to File settings screen.
2. To find the device to retrieve the Storage Backup file more easily, click **Show Filter** to open the filter function.
3. Select one device to be the source. The **Item Selection** button will be enabled.
4. Click **Item Selection** to open the **Item Selection** dialog box. Select the items to be contained in the Storage Backup file from the available backup item lists.
5. Click **Save**.
6. Click **Execute** to open the **Storage Backup Execution (Device to File)** dialog box. If necessary, make the necessary settings in the dialog box.

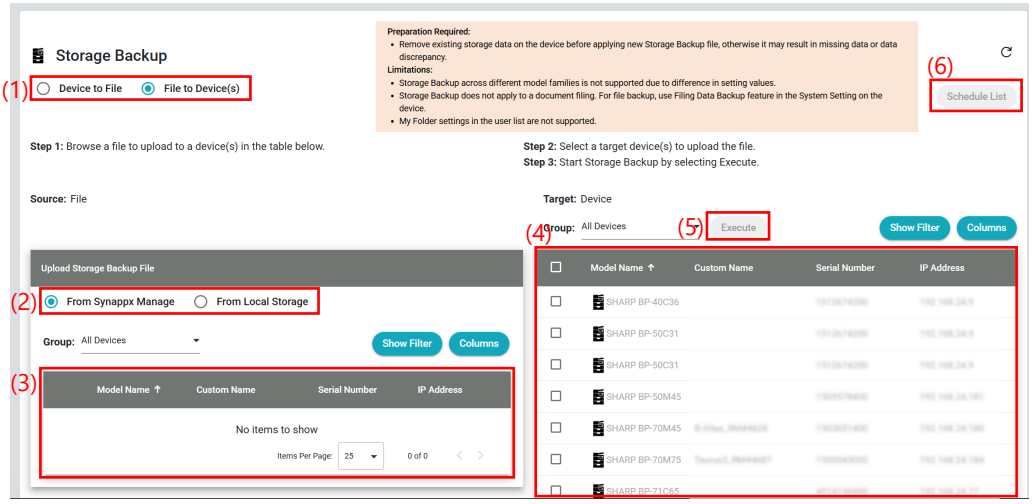


Storage Backup Execution (Device to File) dialog box

7. Click **OK** to start downloading the file. Files downloaded here are stored in the cloud.
   To save this file locally, click the **Save to Local** button.
   To delete this file from cloud, click the **Remove File** button.

Storage Backup page – File to Device(s)

Storage Backup – File to Device(s) allows users to apply the saved storage backup file to target devices.



Storage Backup page – File to Device(s)

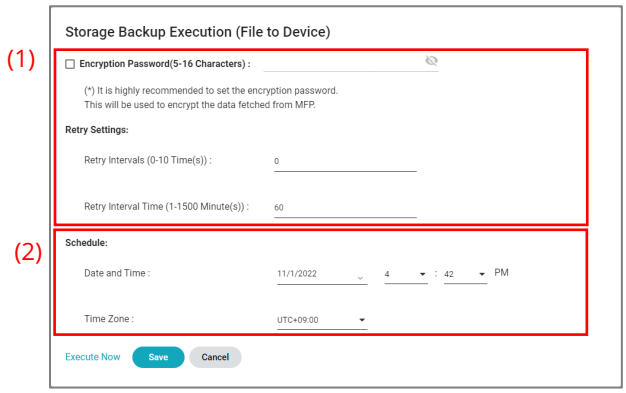
(1) **Operation selection**: **File to Device(s)** should be selected. Switch to the File to Device(s) settings screen.
(2) **Source File selection**
- **From Synappx Manage**: See "(3) Cloud-Saved File List"
- **From Local Storage**: For the Storage Backup file for the device (See "Downloading and Saving the Storage Backup file" section.) or directly from the device's web page.

(3) **Cloud-Saved File List**: In Device to File, files saved in the cloud are displayed here.
(4) **Target Device List**: Select a target device or devices to clone.
(5) **Execute button**: Execute to apply now or set a schedule.
(6) **Schedule List button**: Manages File to Device(s) schedule.

Uploading the Storage Backup file into Target Device(s)

1. In the **Storage Backup** page, select the **File to Device(s)** to switch to the File to Device(s) settings screen.
2. To find the Storage Backup file, select **From Synappx Manage** or **From Local Storage**.
   - **From Synappx Manage**: Select a file from cloud-saved file list.
   - **From Local Storage**: Click **Browse** to navigate to the folder where the Storage Backup file was saved. Select the file and click **Open**. The selected file name will appear in the Upload Storage Backup File area.
3. To find the device(s) to be uploaded the Storage Backup file, select **Group** to list the associated devices.
4. Select one or more device(s) to be the target.

5. Click **Execute** to open the **Storage Backup Execution (File to Device)** dialog box. If necessary, make the necessary settings in the upper part of dialog box. (Area (1) in the figure)



Storage Backup Execution (File to Device) dialog box

6. Storage Backup can be executed immediately or at a scheduled time.
   - To perform Storage Backup now, click **Execute Now**.
   - To perform Storage Backup at a scheduled time, specify the Schedule (Area (2) in the figure) and click **Save**. Once **Save** is clicked, "(6) **Schedule List** button" becomes valid.

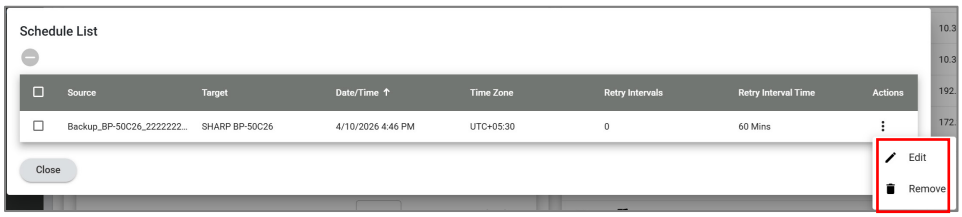
Managing the Scheduled Storage Backup – File to Device(s) operation

Saved scheduled Storage Backup operations can be edited or deleted. Click **Schedule List** to open the **Schedule List** dialog box.

- To edit a schedule, click the Actions icon ⋮ for the schedule to be edited. Select **Edit**.
- To delete a schedule, click the Actions icon ⋮ for the schedule to be deleted. Select **Remove**.
- To delete multiple schedules at once, select the checkboxes of the schedules to be deleted, then click the Remove Schedule icon ⊖.

A confirmation dialog box will appear. Click **OK** to delete the schedule.

Note:
Schedules will be deleted after execution is completed.



Schedule List dialog box – Edit or Remove

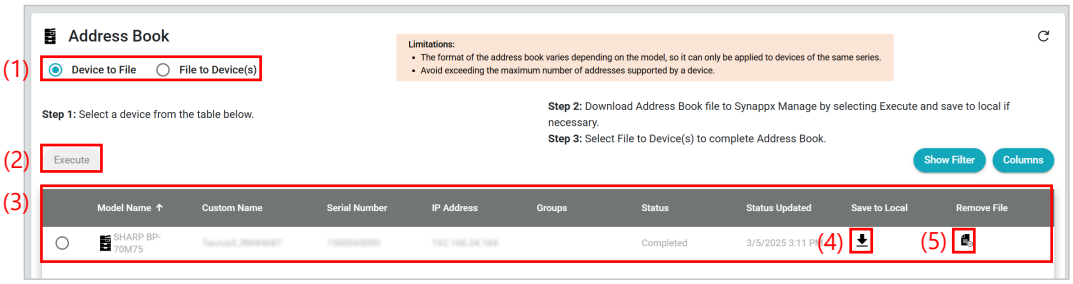
Address Book

The Address Book feature copies address book information from one device to other devices. Be sure to follow the steps below.

A copy of the source device data must be made using the Device-to-File procedure, then that data can be applied to the target device using the File-to-Device procedure.

Address Book page – Device to File

Address Book – Device to File must be performed first. This feature saves a file containing the address information registered in the device.



Address Book page – Device to File

(1) **Operation selection**: **Device to File** should be selected. Switch to the Device to File settings screen.

(2) **Execute button**: Downloads and saves the Address Book file.

(3) **Source Device List**: Select one device to be the source.

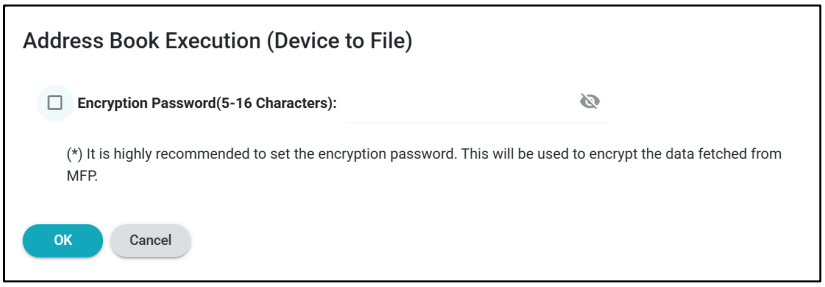
(4) **Save to Local button**: Download the file saved in the cloud to local. It is activated when the file is saved to the cloud by the **Execute** button.

(5) **Remove File button**: Delete the file saved in the cloud. It is activated when the file is saved to the cloud by the **Execute** button.

Downloading and Saving the Address Book file

1. On the **Address Book** page, select **Device to File** to switch to the Device to File settings screen.
2. To find the device to retrieve the Address Book file more easily, click **Show Filter** to open the filter function.
3. Select one device to be the source.

4. Click **Execute** to open the **Address Book Execution (Device to File)** dialog box.
   If necessary, change any settings you wish to change in the dialog box.

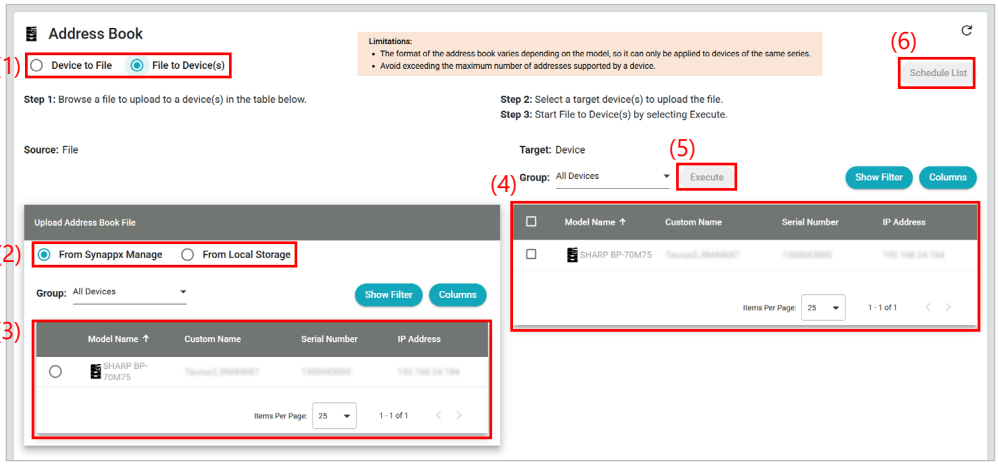


Address Book Execution (Device to File) dialog box

5. Click **OK** to start downloading the file. Files downloaded here are stored in the cloud.
   To save this file locally, click the **Save to Local** button.
   To delete this file from cloud, click the **Remove File** button.

Address Book page – File to Device(s)

Address Book – File to Device(s) allows users to apply the saved address book file to target devices.



Address Book page – File to Device(s)

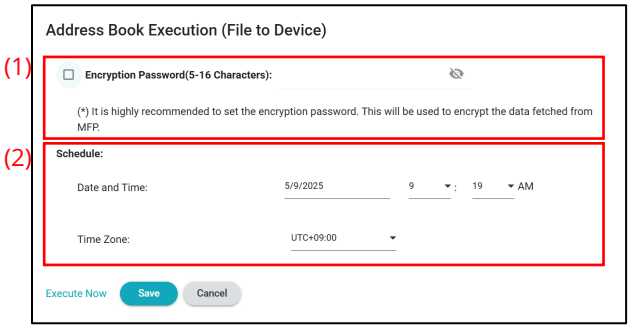
(1) **Operation selection**: **File to Device(s)** should be selected. Switch to the File to Device(s) settings screen.
(2) **Source File selection**
- **From Synappx Manage**: See "(3) Cloud-Saved File List"
- **From Local Storage**: For the Address Book file for the device (See "Downloading and Saving the Address Book file"), or directly from the device's web page.

(3) **Cloud-Saved File List**: In Device to File, files saved in the cloud are displayed here.
(4) **Target Device List**: Select a target device or devices to clone.
(5) **Execute button**: Execute to apply now or set a schedule.
(6) **Schedule List button**: Manages File-to-Device schedule.

Uploading the Address Book file to Target Device(s)

1. In the **Address Book** page, select **File to Device(s)** to switch to the File to Device(s) settings screen.
2. To find the Address Book file, select **From Synappx Manage** or **From Local Storage**.
   - **From Synappx Manage**: Select a file from cloud-saved file list.
   - **From Local Storage**: Click **Browse** to navigate to the folder where the Address Book file was saved. Select the file and click **Open**. The selected file name will appear in the Upload Address Book File area.
3. To list the device(s) to be uploaded the Address Book file, select **Group**.
4. Select one or more device(s) to be the target.

5. Click **Execute** to open the **Address Book Execution (File to Device)** dialog box. If necessary, make the necessary settings in the upper part of dialog box. (Area (1) in the figure)



Address Book Execution (File to Device) dialog box

6. Address Book can be executed immediately or at a scheduled time.
   - To perform Address Book now, click **Execute Now**.
   - To perform Address Book at a scheduled time, specify the Schedule (Area (2) in the figure), and click **Save**. Once **Save** is clicked, "(6) **Schedule List** button" becomes valid.

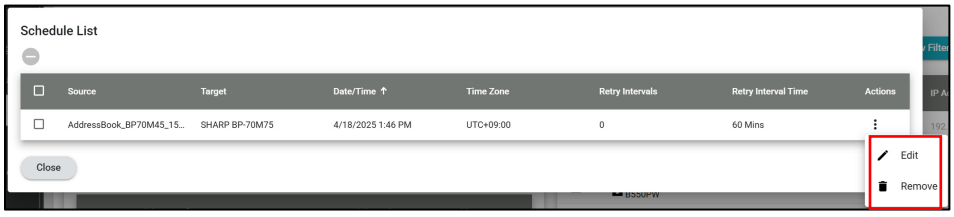
Managing the Scheduled Address Book – File to Device(s) operation

Scheduled Address Book operations can be edited or deleted. Click **Schedule List** to open the **Schedule List** dialog box.

- To edit a schedule, click the Actions icon ⋮ for the schedule to be edited. Select **Edit**.
- To delete a schedule, click the Actions icon ⋮ for the schedule to be deleted. Select **Remove**.
- To delete multiple schedules at once, select the checkboxes of the schedules to be deleted, then click the Remove Schedule icon ⊖.

A confirmation dialog box will appear. Click **OK** to delete the schedule.

Note:
Schedules will be deleted after execution is completed.



Schedule List dialog box – Edit or Remove

Print Driver Management

The print driver management function lets you upload print drivers from Sharp to Synappx Manage and to apply them to devices which are being managed. You can also create driver packages containing customized default settings (such as color mode and 2-sided printing) and operations such as installation methods and distributing packages to users. Under **Devices**, click **Print Drivers** to display the Print Drivers list page.

Note:
The Print Drivers management function only supports print drivers for Pages.

- The storage space for uploading the Print Drivers is 500MB.
- The maximum file size that can be uploaded is 100MB.

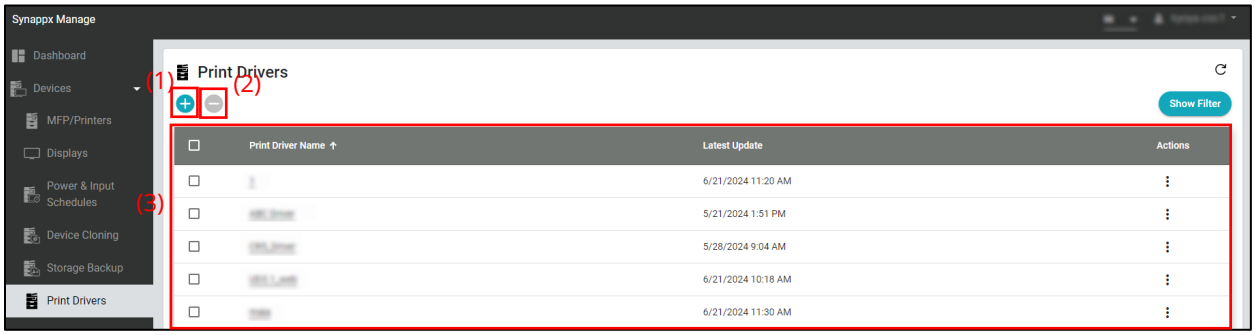
Print Drivers Management operations by administrator

The primary tasks that can be performed by administrators include:

- Creating and uploading print driver packages
- Notifying users of the URL for the uploaded driver package by email
- Changing the settings of uploaded driver packages
- Deleting uploaded driver packages

Print Drivers page

The configured print drivers are managed using the **Print Drivers** page.



Print Drivers page

(1) **Add Print Driver icon**
Refer to "Creating and uploading print driver packages" for more details.

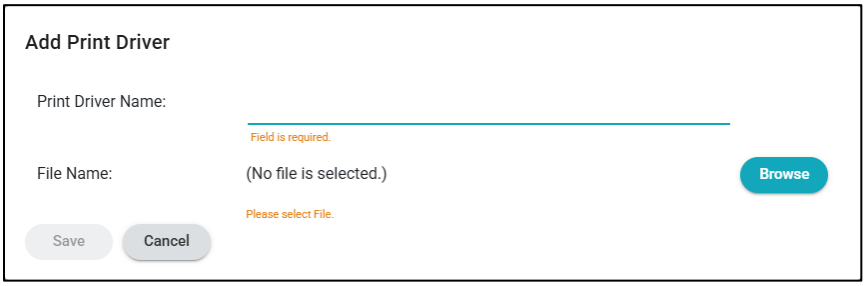
(2) **Remove Print Driver icon**

(3) **Uploaded Print Driver List**

Creating and uploading print driver packages

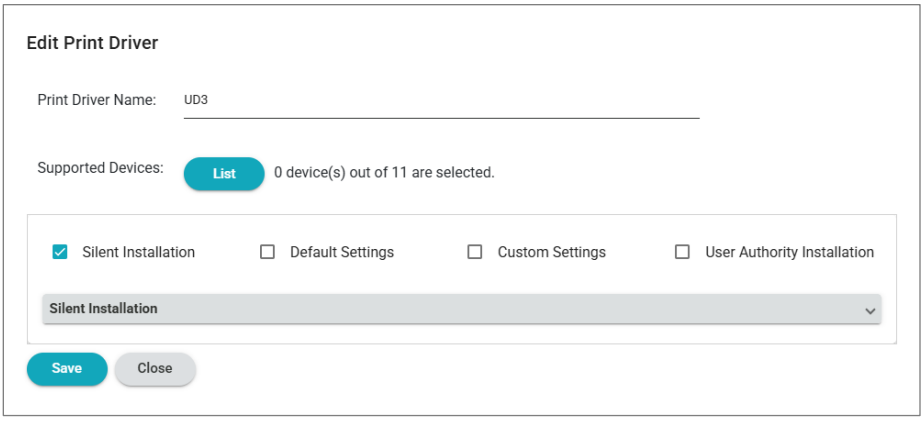
Print driver packages can be created and uploaded to Synappx Manage:

1. The print drivers to be uploaded can be obtained from the Sharp Global website. Download the print driver file in .exe or .zip format from the software download service.
2. In the **Print Drivers** page, click the Add Print Driver icon ⊕ to open the **Add Printer Driver** dialog box.



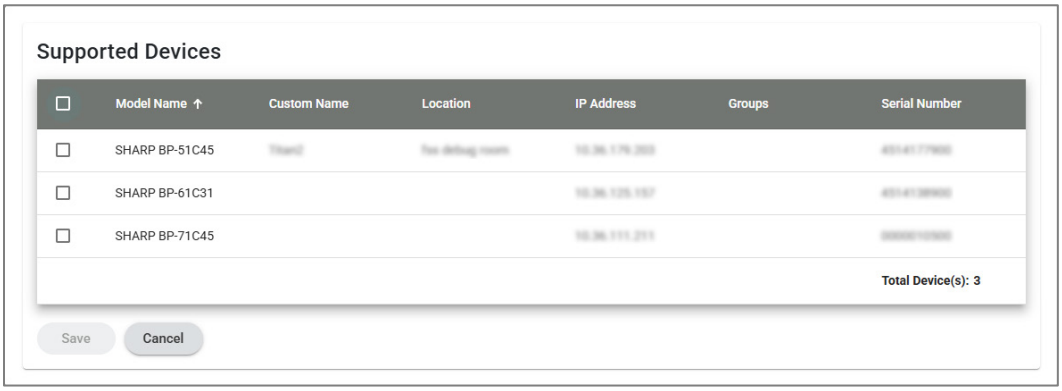
Add Print Driver dialog box

3. Enter the name used to identify the driver package in the Print Driver Name field. (Refer to "Glossary > Guidelines for Naming and Text Entry > Print Driver Names" for character limitations.)
4. Click **Browse** to navigate to the folder where the file (.ZIP or .EXE file) was saved in Step 1.
5. Select the file and click **Open**. The selected file name will appear in the File Name field.
6. Click **Save** to start uploading.
7. Once a new print driver is registered, **Add Print Driver** dialog is closed and automatically **Edit Print Driver** dialog is popped up.



Edit Print Driver dialog box

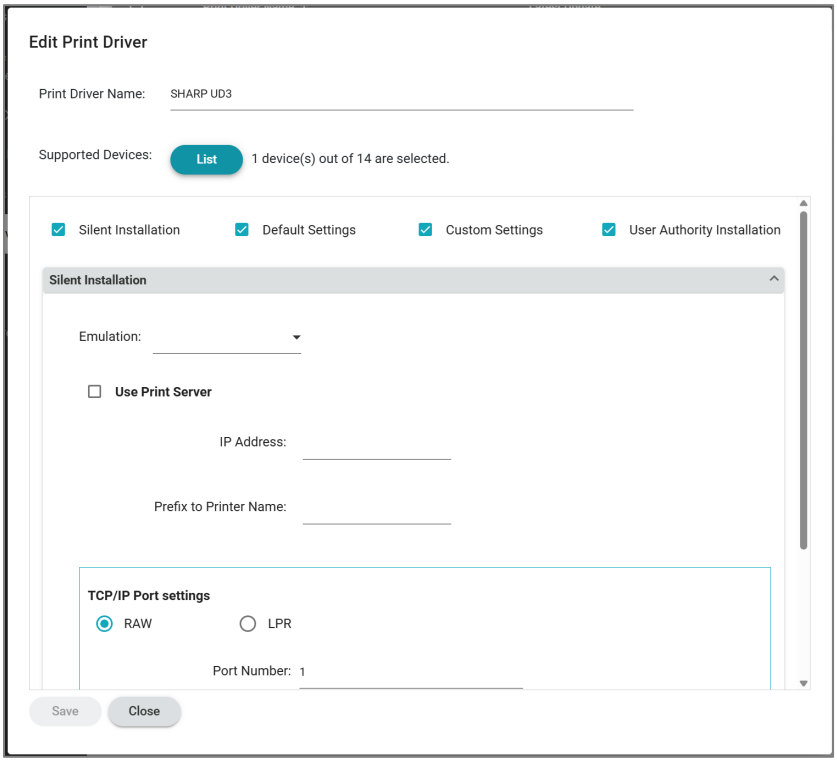
(1) Click **List** to display the registered devices that support the print driver. Select the checkbox for the target device for the print driver, then click **Save** on the **Supported Devices** dialog box.



Supported Devices dialog box

(2) Check the items to be configured and display the settings menu.

8. Configure the driver settings for your checked items.



Edit Print Driver dialog box

Silent Installation: You can edit "Emulation" and "TCP/IP Port settings". These settings are applied automatically when the print driver is installed.

- **Emulation**: Sets the emulation for the print driver that has been installed.

- **Use Print Server**: If you use a print server, enable this item and set the IP address of the print server.
  - If the target print driver is a UD (Universal Driver), you can enter a Prefix to **Printer Name**. If the prefix to printer name box is left blank, it will be set as "Print Server PCL6".
  - If the target print driver is not a UD (Universal Driver), a prefix to **Printer Name** cannot be set. The print server with the specified IP address will be used for the configuration. The printer's name is a character string containing the model name of the linked device in the same way as when a print server is not used.
- **TCP/IP Port settings**: Sets the TCP/IP port for the print driver that has been installed. If specifying a queue name, use alphanumeric characters.

Default Settings: You can edit the default settings for "Color Mode", "2-Sided Printing", and "Staple".

- **Color Mode**: The default value can be selected from "Auto", "Color" and "Grayscale". If the target device does not support color printing, then color printing will not be possible, regardless of which setting is selected.
- **2-Sided Printing**: The default value can be selected from "None", "Long Edge", and "Short Edge". If the target device does not support 2-sided printing, then 2-sided printing will not be possible, regardless of which setting is selected.
- **Staple**: The default value can be selected from "None", "1 Staple" and "2 Staples". If the target device does not support stapling, then stapling will not be possible, regardless of which setting is selected.
- **Printing Policy**:
  - Document Filing: Enable/disable document filing.
  - User Authentication: Enable/disable user authentication.
  - Use Windows Login Name as 'Login Name': Enable this setting if the Windows login name is to be used as the login name for the device.
  - Print Release: Enable/disable document print release.

Custom Settings: You can edit the settings for "Forced B/W Print" and "Change Driver Name".

- **Forced B/W Print** (color printing not allowed): Sets whether forced black-and-white printing is enabled or disabled.
- **Change Driver Name** (identical to product version): If this setting is enabled, you can add a suffix to the driver's name and use that as the same name for the product driver.

User Authority Installation: You can set it so that the driver can be installed by a preauthorized administrator.

9. Click **Save** to save your settings.

Sending links to uploaded driver package via email

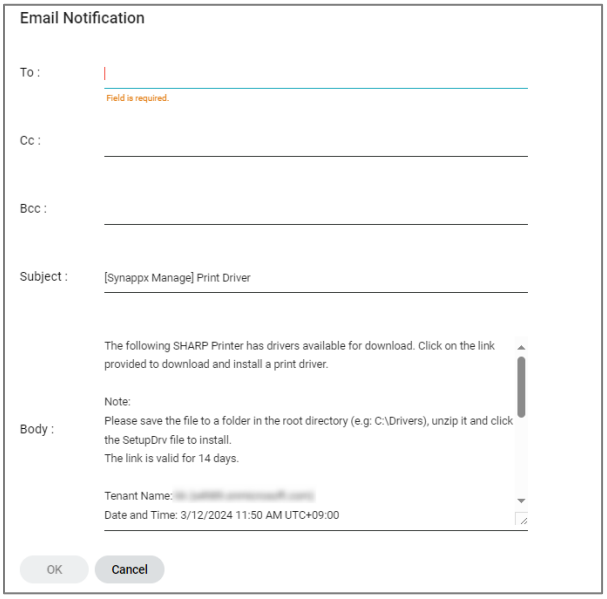
The URLs of print driver packages uploaded to Synappx Manage can be sent to specified recipients as notification emails.

Setting email notifications

1. In the **Print Drivers** page, click the Actions icon ⋮ for the print driver to be notified. Select **Mail** from the pull-down menu to open the **Supported Devices** dialog box.
2. Select the checkboxes of the devices used for printing (multiple selections allowed), then click **Next**.

Supported Devices dialog box

3. Specify the recipient address, subject, and body of the email. Multiple email addresses by entering a delimiter character ";" or "," between each address. When all fields have been entered, click **OK**.



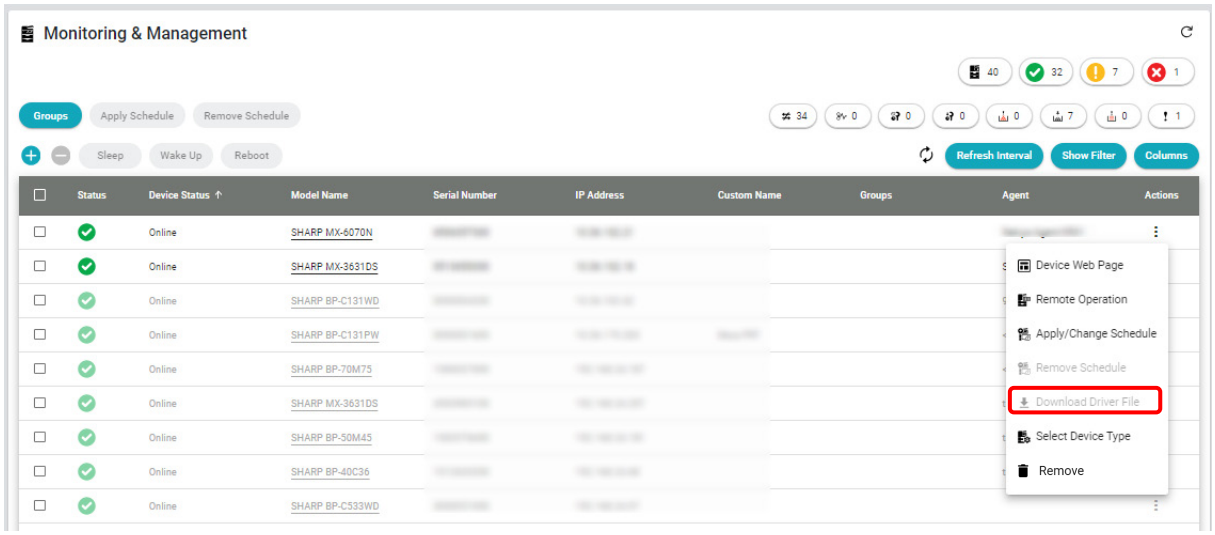
Email notifications

Downloading Print Drivers

Print driver packages can be accessed either by logging in to Synappx Manage or clicking the URL in the notification email (see "Sending links to uploaded driver package via email"). Downloading drivers by logging into Synappx Manage.

MFP/Printers Monitoring & Management page

Click the Actions icon ⋮ for the device to get the print driver. Select **Download Driver File** from the pull-down menu to open the **Print Drivers** dialog box.



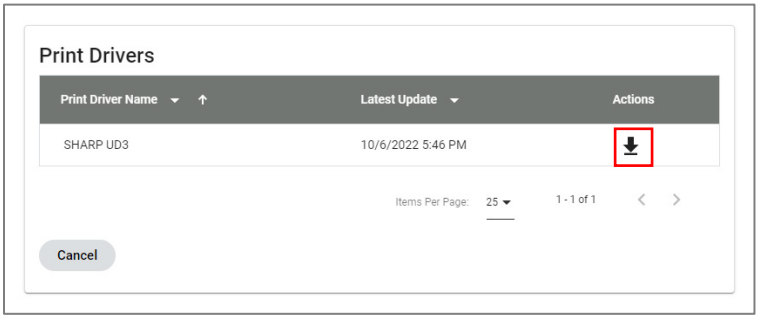
MFP/Printers Monitoring & Management page

MFP/Printers Device Information page

Click the Download Driver File icon ⬇ to open the **Print Drivers** dialog box.

MFP/Printers Device Information page

The **Print Drivers** dialog box will be displayed. Click the Download Driver File icon ⬇ to start downloading the Print Driver.



Print Drivers dialog box

Downloading drivers from the URL(s) in notification email

Print driver package can be downloaded by accessing the URLs that appear in the notification email sent by the print driver management function. In this case, there is no need to log in to Synappx Manage.

The URLs are valid for 2 weeks.

Notification email

Downloaded Driver Package Name

Depending on the configuration and the type of Print Driver uploaded, the file name will be as follows:

Case	Driver Package Name	Example
“Use Print Server” is enabled, and an uploaded driver is UD (Universal Driver).	<Printer Name>.zip	[Prefix]_Print_Server_PCL6.zip
“Use Print Server” is not enabled, and an uploaded driver is not UD (Universal Driver).	SHARP_<Model Name>_ <Serial Number>_<Emulation>.zip	SHARP_MX-6070_12345678_PCL6.zip

Installing Print Drivers

Save the downloaded file to any folder in the root directory (e.g.: 'C:\Drivers').
To install the print driver, double-click the "SetupDrv.exe" file in the print driver package.

Note:
Depending on the operating environment, a "Security Warning" dialog box may be displayed when installing the print driver.

Changing Settings for Uploaded Print Drivers

In the **Print Drivers** page, click the Print Driver Name, then adjust settings. For more information on each setting, refer to "Creating and uploading print driver packages".

Note:
To change the password for users, select the "Change Password" checkbox.

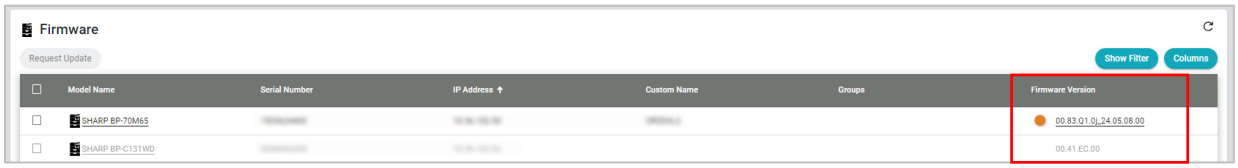
Deleting Uploaded Print Drivers

To delete a print driver, click the Actions icon ⋮ for the print driver to be deleted, then click **Remove**. To delete multiple print drivers at once, select the checkboxes of the print drivers to be deleted, and then click the Remove Print Driver icon ⊖.
A confirmation dialog box will appear. Click **Yes** to delete the print driver(s).

Request Firmware Update

The firmware feature allows you to view the firmware version of each MFP. If when new firmware is available, you can request an update from your service provider who has access to your tenant.

Firmware page



Firmware page

In the **Firmware Version** column, you can view firmware versions and status. An orange icon will be displayed when newer firmware is available.

Icon	Description
	This icon is displayed when newer firmware is available for the device. When hovering the mouse over the icon, the new firmware version is displayed. Click on the icon to view the new firmware details. (Available only in the US. View the supported models for this feature.)
	This icon is displayed to inform that the current firmware is special firmware.

Request Update

Request Update can be performed only on the models that icon  is displayed. This feature allows you to send an email requesting firmware updates to the entered email address..

1. Check the checkbox of the MFP for which you want to request a firmware update and click the **Request Update** button.

2. **Request Update** dialog is displayed. Then, enter the email address of your service provider and click **Send**. After this, Your firmware update request will be sent to your service provider.

Security Management

Using the security management feature, the security settings of multiple MFPs and printers (devices) are remotely set, managed and monitored.

Using Synappx Manage, you can remotely configure and specify security settings as a security policy. When a policy is applied to a device or devices, Synappx Manage will start monitoring all settings covered in the Security Management feature. The items that are unchecked and not configured using Synappx Manage will be monitored based on the configuration set on the device when the policy is applied. When a difference is detected, the violation is recorded or optionally an email alert will be generated. When violations are detected on the selected items in the policy, they are automatically remediated to the policy default.

Security policy management is performed in the following steps.

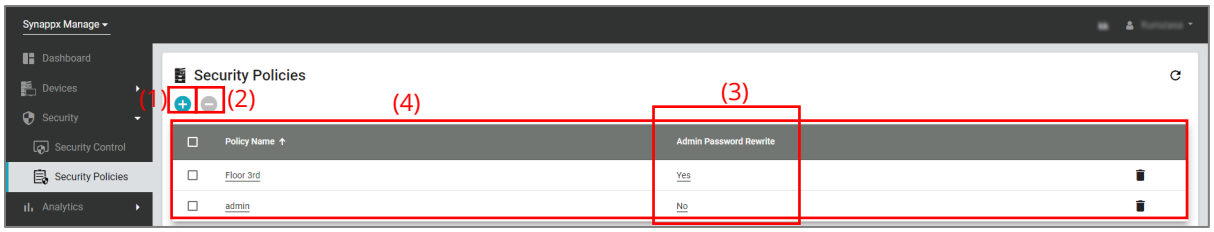
Step 1: Create Security Policy
Step 2: Apply Security Policy to each device
Step 3: Check Security Policy compliance for each device (manual or automatic)

Caution:
Security Policy management is not available for the devices managed by Active Directory (AD) Sharp security group policy. Synappx Manage will not overwrite AD policy.

Security Policies for Devices with Data Security Kits (DSK):
Although Synappx Manage detects configuration changes against the security policy, details on changes are not viewable on the DSK enabled devices as the data is protected via encryption. Therefore, e-mail alerts generated by security management will not include details on affected settings.

Security Policies page

The **Security Policies** page allows users to manage (create, edit, and delete) Security Policies.



Security Policies page

(1) **Add Security Policy icon**

(2) **Remove Security Policy icon**

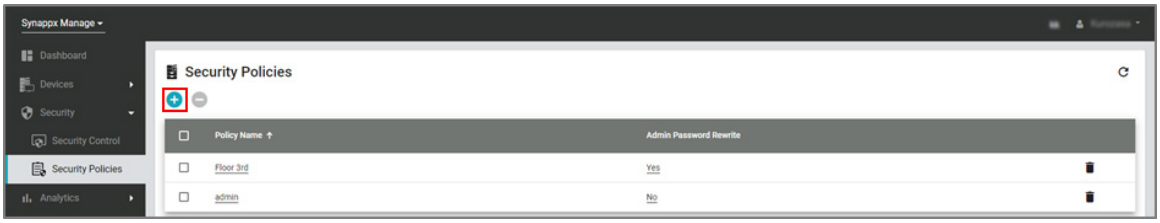
(3) **Admin Password Rewrite option**

Applies a new Admin Password to the target devices. (Refer to "Admin Password Rewrite option".)

(4) **Security Policies List**

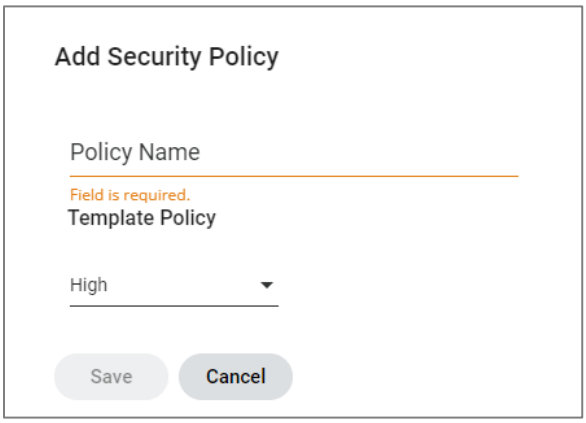
Adding a New Security Policy

Once a new Security Policy is registered in the list, edit the Security Policy settings.



Adding a New Security Policy

1. On the **Security Policies** page, click the Add Security Policy icon to open the **Add Security Policy** dialog box.



Add Security Policy dialog box

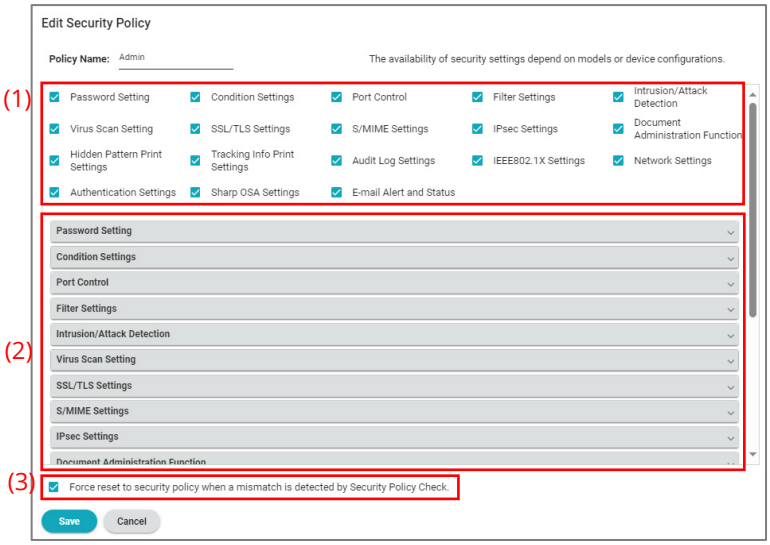
2. Enter a **Policy Name**, select a **Template Policy**, and click **Save**. **Template Policy** can be selected from **High**, **Medium**, **Low** and created policies.

Editing the Security Policy

Configure the security policy by defining each security preference.

1. On the **Security Policies** page, click the name of the security policy to be edited.
2. In the **Edit Security Policy** dialog box (1), select the security policy settings that will be applied to the policy. The options include:
   - Password Setting
   - Condition Settings
   - Port Control

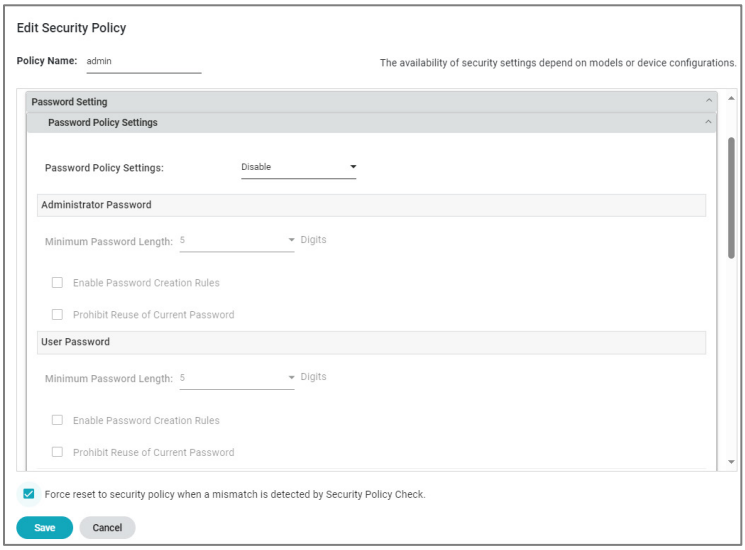
- Filter Settings
- Intrusion/Attack Detection
- Virus Scan Setting
- SSL/TLS Settings
- S/MIME Settings
- IPsec Settings
- Document Administration Function
- Hidden Pattern Print Settings
- Tracking Info Print Settings
- Audit Log Settings
- IEEE802.1X Settings
- Network Settings
- Authentication Settings
- Sharp OSA Settings
- E-mail Alert and Status



Edit Security Policy dialog box

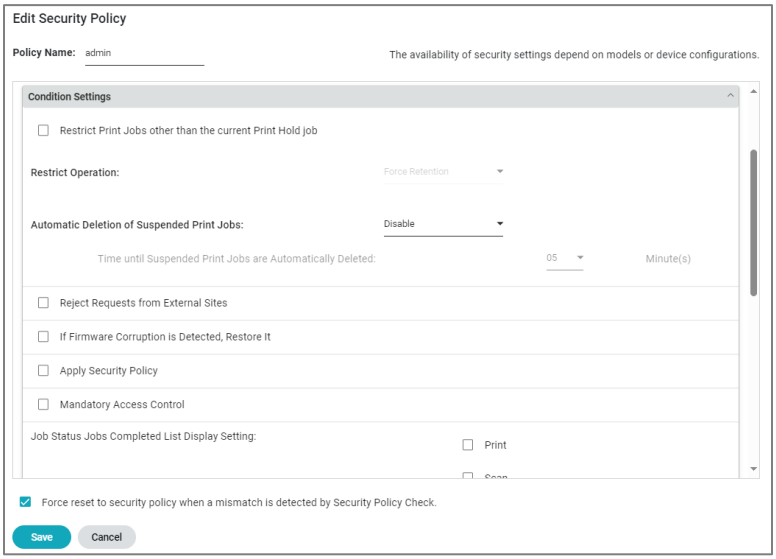
3. Click on each setting item (2) to display and edit detailed settings. Options include Enable, Disable and Don't Apply. When “Don't Apply” is selected, the item is ignored and the setting values on MFP will not be changed.

Password Setting: Set rules for creating passwords and restrict access to the Device Web Page with passwords.



Password Setting

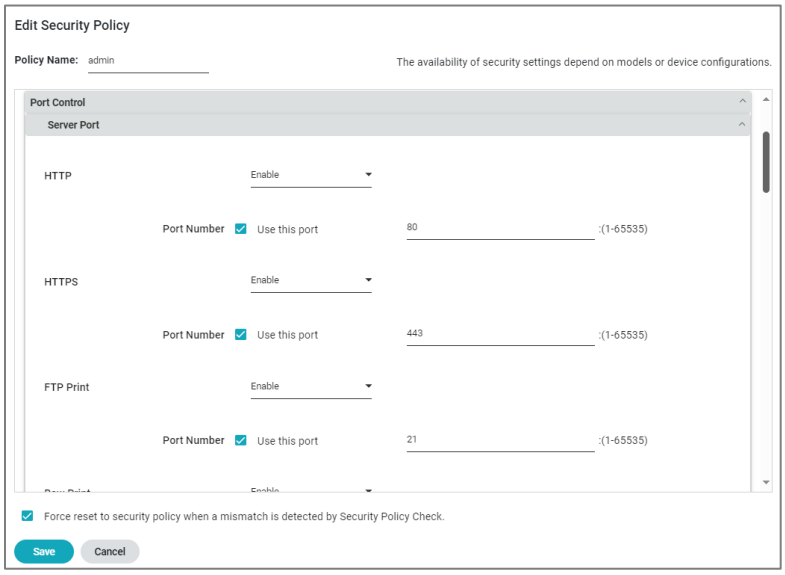
Condition Settings: Set condition settings for MFP security.



Condition Settings

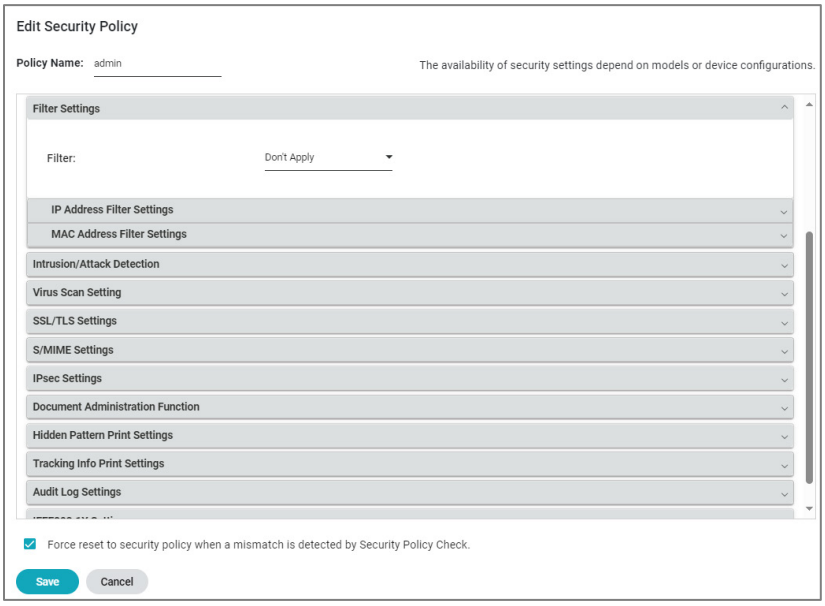
Note:
Mandatory Settings here must be set to ON if you want to set up E-mail Alerts regarding Condition Settings.

Port Control: Update the server and client port settings for the security policy. This example shows default values.



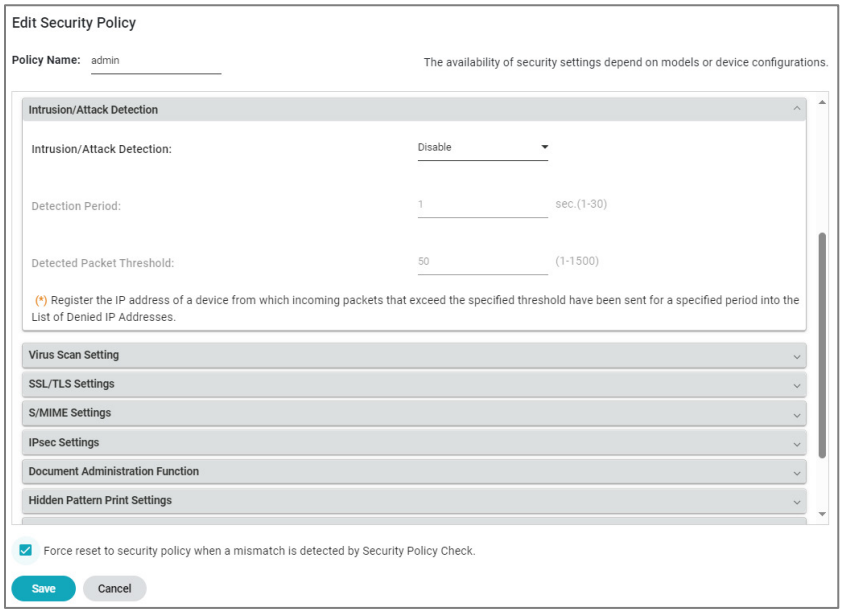
Port Control

Filter Settings: Allow or deny access to specific devices.



Filter Settings

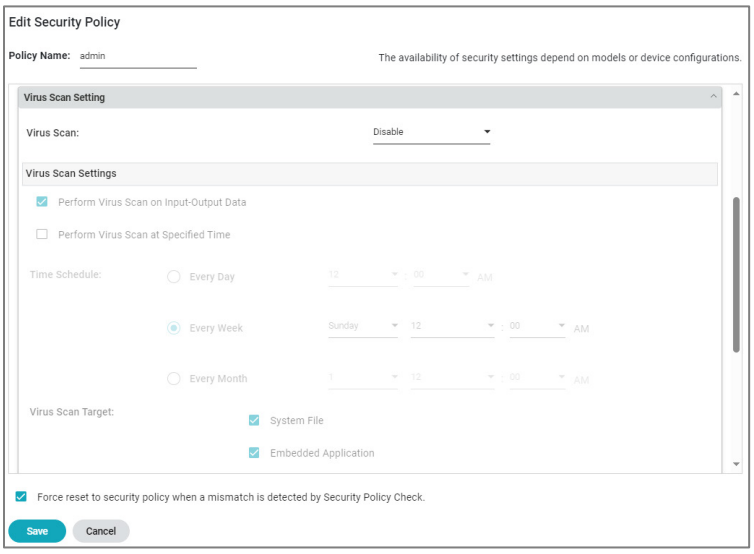
Intrusion/Attack Detection: Switch whether Intrusion/Attack Detection is enabled or disabled and adjust definition of Intrusion and Attack.



Intrusion/Attack Detection

Note:
Intrusion/Attack Detection must be set to “enable” if you want to set up E-mail Alerts regarding Intrusion/Attack Detection.

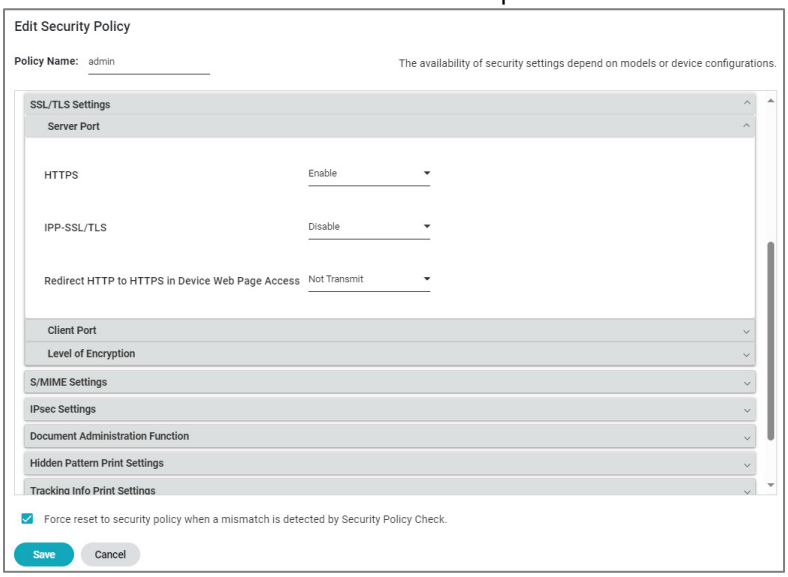
Virus Scan Setting: Configure settings related to virus scan targets and scheduling.



Virus Scan Setting

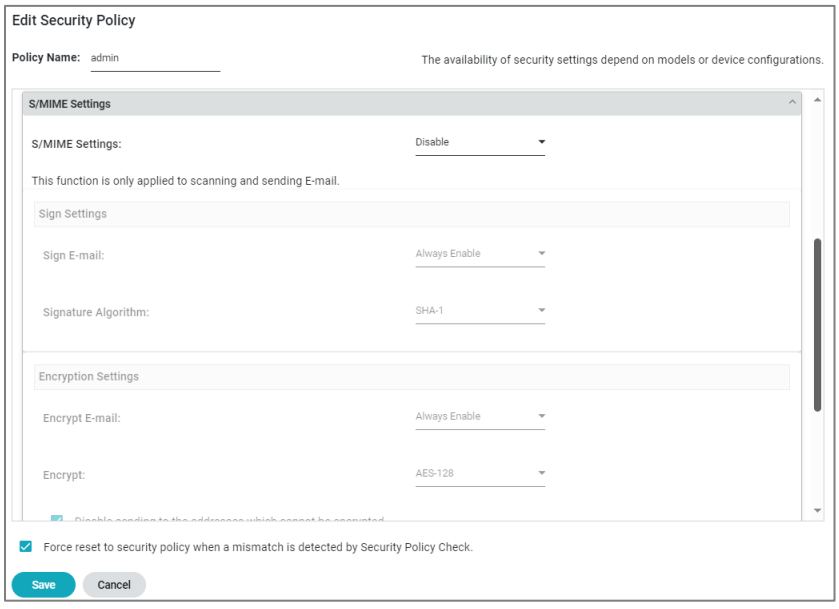
Note:
To use this function, the Virus Scan Kit must be installed in the MFP.

SSL/TLS Settings: Change encrypted communication between the server and the client. SSL/TLS encryption can be enabled or disabled for each protocol.



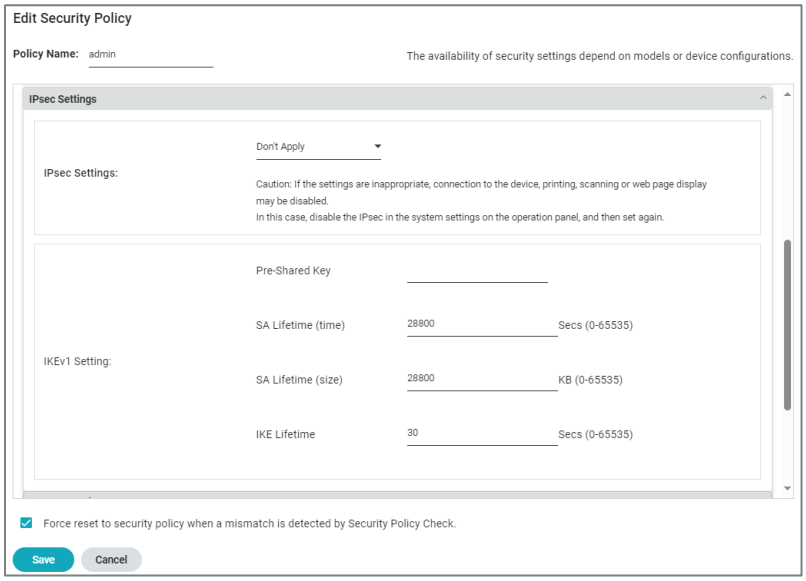
SSL/TLS Settings

S/MIME Settings: Adjust S/MIME signature settings or encryption settings.



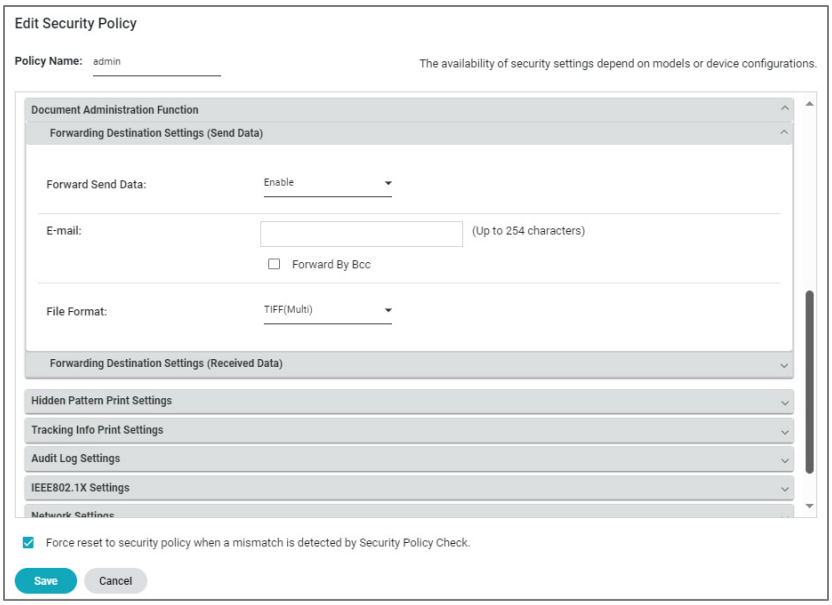
S/MIME Settings

IPsec Settings: Adjust IPsec and IKEv1 settings. Use the IPsec Rules menu options to add or delete IPsec rules.



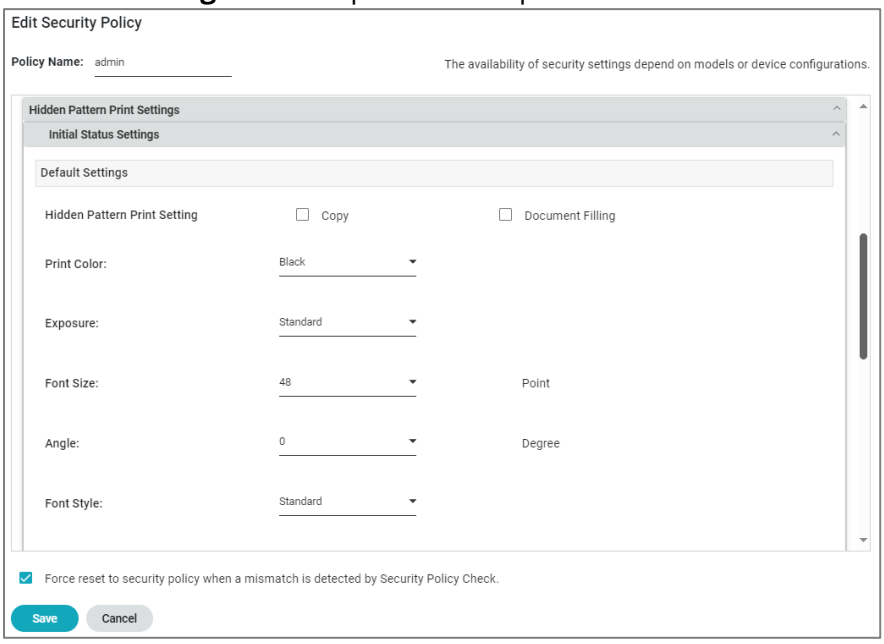
IPsec Settings

Document Administration Function: Set forwarding destination settings. When the MFP sends data, the sent data is also shared with the email address you set.



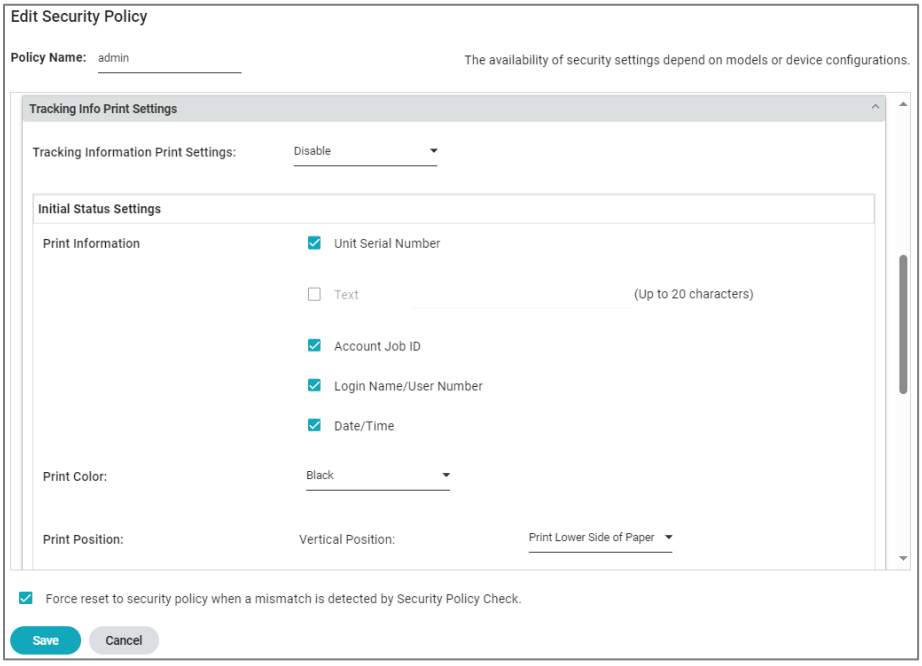
Document Administration Function

Hidden Pattern Print Settings: Set and print hidden patterns.



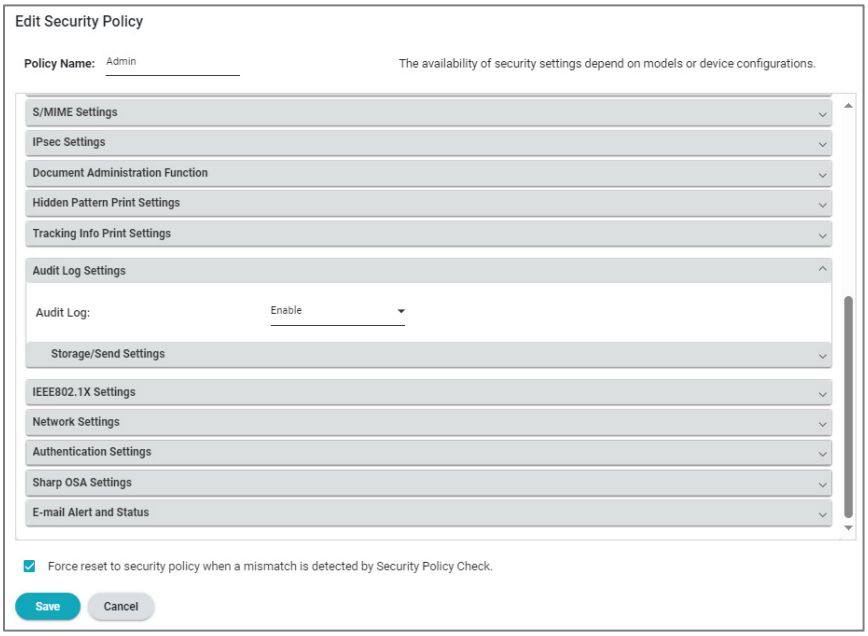
Hidden Pattern Print Settings

Tracking Info Print Settings: Set tracking information.



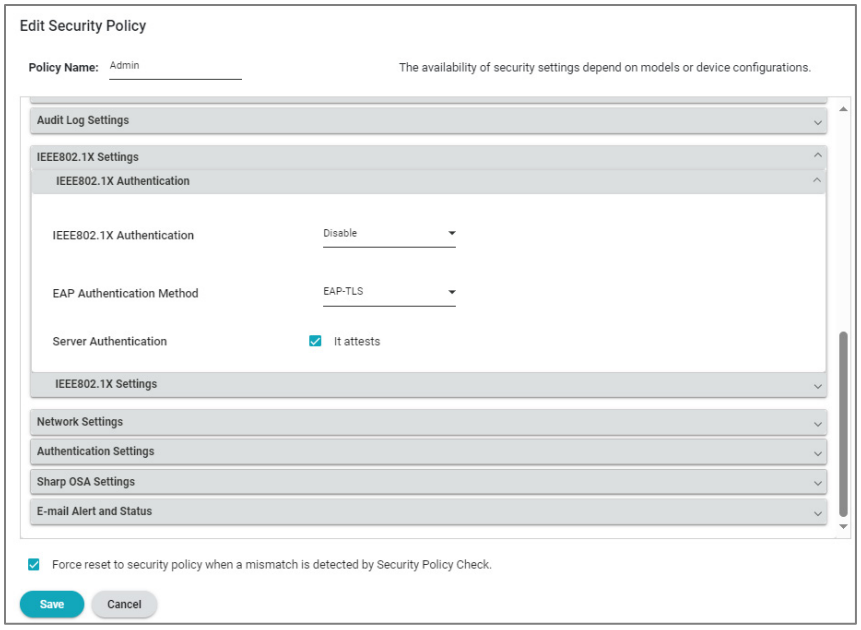
Tracking Information Print Settings

Audit Log: Settings for sending real-time MFP event log to Syslog/SIEM server. (Storage/Send Settings are part of Audit Log Settings.)



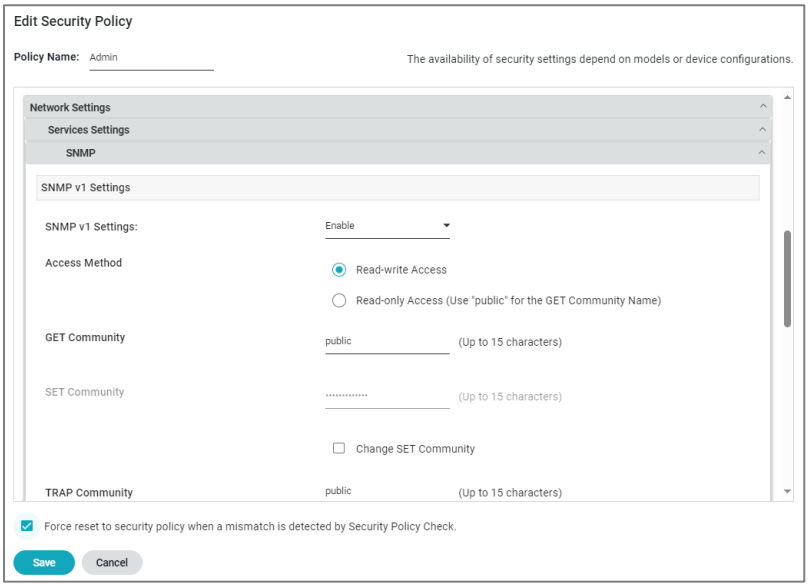
Audit Log Settings

IEEE802.1X Settings: Set the IEEE authentication level for the organization's enterprise network.



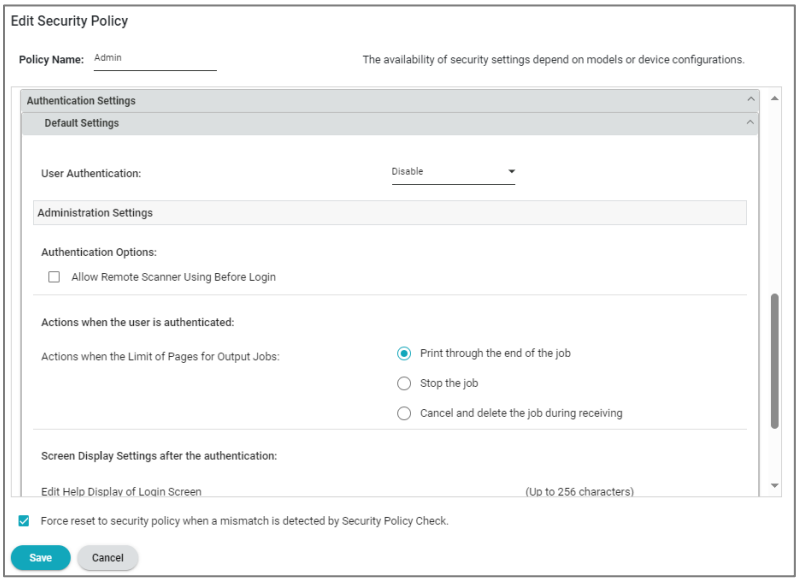
IEEE802.1X Settings

Network Settings: Set detailed setting for Network, such as SNMP settings and SMB settings.



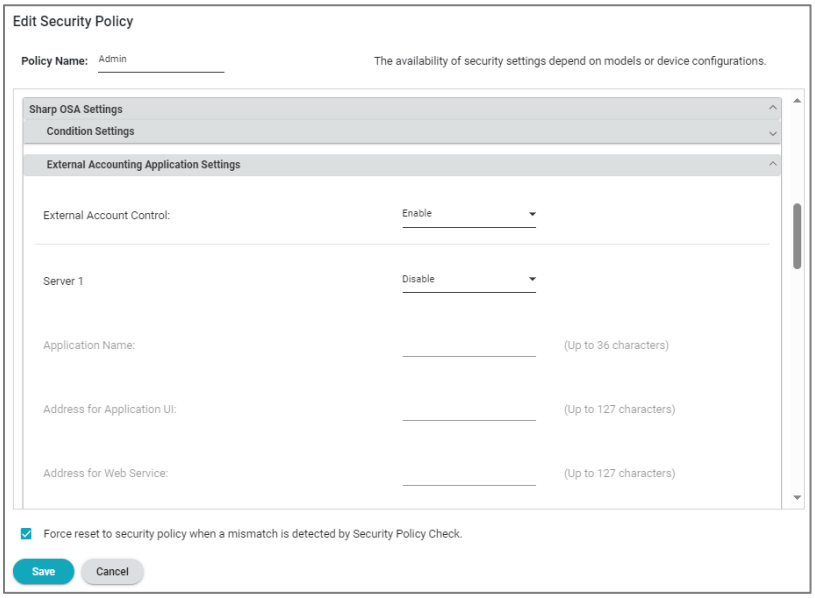
Network Settings

Authentication Settings: Set detailed settings for user authentication. User authentication for Sharp OSA and local login are supported.



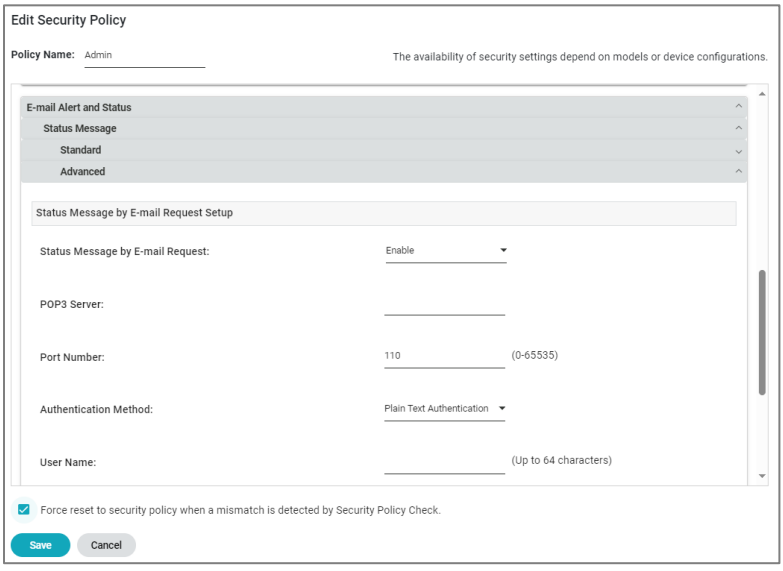
Authentication Settings

Sharp OSA Settings: Set detailed settings for Sharp OSA (External Authority).



Sharp OSA Settings

E-mail Alert and Status: Set detailed settings for device e-mail alerts and status notifications.



E-mail Alert and Status

Cautions:
When HTTPS is disabled in the Storage/Send Settings, some features that require secure communication are disabled. Such features include device cloning, storage backup, security control, and power management. The same situation occurs even if you change the HTTPS port number.

4. For automated remediations when policy violation is detected, select **Force reset to security policy when a mismatch is detected by Security Policy Check**.
5. When finished, click **Save**.

Admin Password Rewrite option

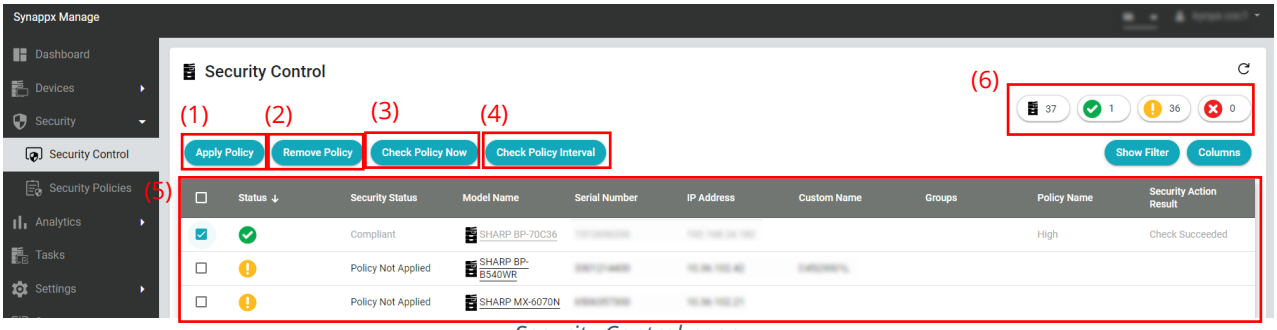
The **Admin Password Rewrite** option allows to apply a new admin password to the target devices.

1. In the **Security Policies** page, click **No** for the **Admin Password Rewrite** option to open the **Admin Password Rewrite Setting** dialog box.
2. Select the checkbox **Admin Password Rewrite** to enable the **Admin Password** field.
3. Enter a new admin password into the **Admin Password** field. Enter a new admin password into the **Admin Password (Confirmation)** field to confirm.
4. Click **Save**. The **Admin Password Rewrite** option indication changes to **Yes**.

Note:
Be sure to use passwords that comply with each device's own password restrictions.

Security Control page

The **Security Control** page allows to check and apply security settings on the devices as well as verify that a device's security settings match the Synappx Manage security policy. If force reset is selected, Synappx manage automatically change the device settings to the policy default when policy mismatch is detected.



Security Control page

(1) **Apply Policy button**
Applies a security policy to the selected devices.

(2) **Remove Policy button**
Removes the selected device(s) from the Security Policy targets.

(3) **Check Policy Now button**
Immediately checks that selected devices conform to the Security Policy.

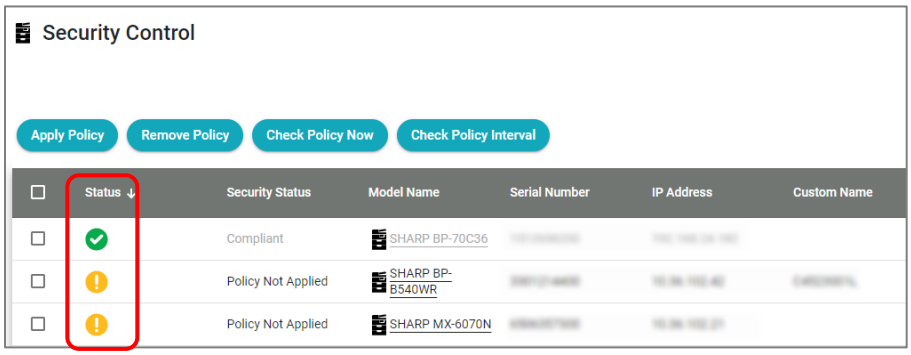
(4) **Check Policy Interval button**
Switches interval at which system ensures devices conform to the Security Policy.

(5) **Device List**
List of managed devices that includes security status for each device.

(6) **Security policy status icons**
A summary of device status and how security policies are applied.

Security Policy Status

The current security policy status for each device is displayed in the device list on the **Security Control** page.



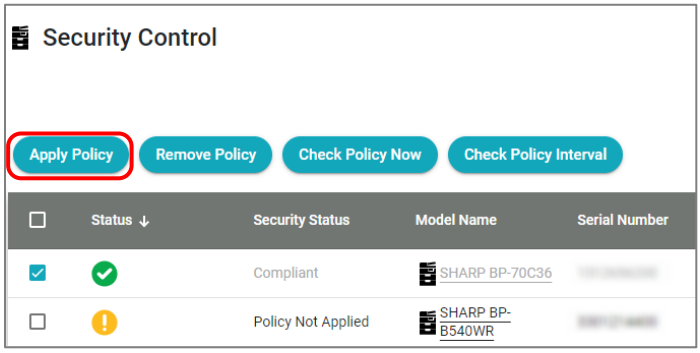
Security policy status

Status icon reference:

Icon	Status
	All Devices: Displays security device information for all registered devices.
	Normal: Indicates that a security policy has been applied correctly to the device.
	Warning: Indicates that no security policy has been applied to the device.
	Error: Indicates that there is a problem with the security policy information for the device. (e.g.: "Unknown Status", "Non Compliant", etc.)

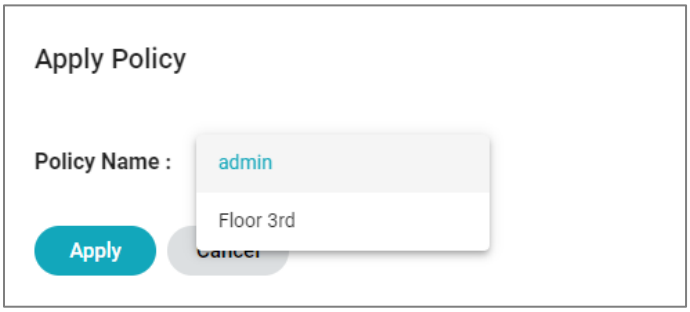
Applying the Security Policy to Device(s)

1. In the **Security Control** page, select the checkbox(es) for the target device(s).



Applying the Security Policy to Device(s)

2. Click **Apply Policy**.
3. Click the **Policy Name** field to open the pull-down menu. Select the policy name you wish to use for the device.

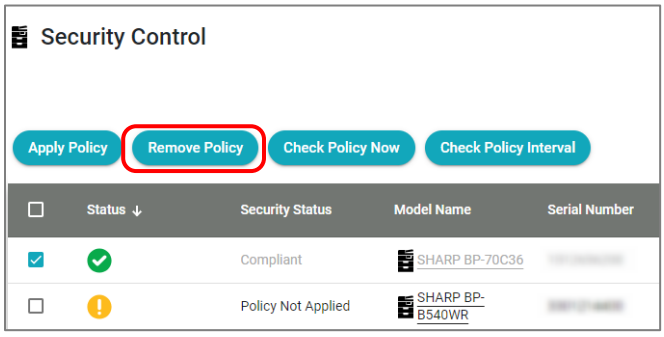


Policy Name Selection

4. Click **Apply**.
5. When the security policy is successfully applied to each target device, the status will change to **Compliant**, and the applied policy will be displayed.

Removing Device(s) from the Security Policy target

1. In the **Security Control** page, select the checkbox(es) for the target device(s) to be removed from the applied Security Policy.

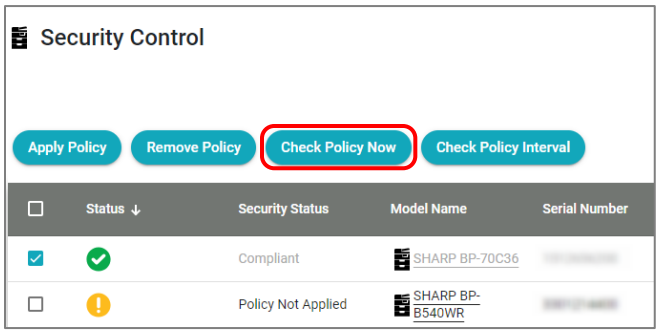


Removing Device(s) from the Security Policy target

2. Click **Remove Policy**.
3. When the selected device(s) policies are successfully removed, the status displayed for each selected target device will change as follows:
   - **Security Status**: Policy Not Applied
   - **Policy Name**: (blank)
   - **Security Action Result**: (blank)

Checking Security Policy Manually

1. In the **Security Control** page, select the checkbox(es) for the device(s) you want to check for compliance with the Security Policy.



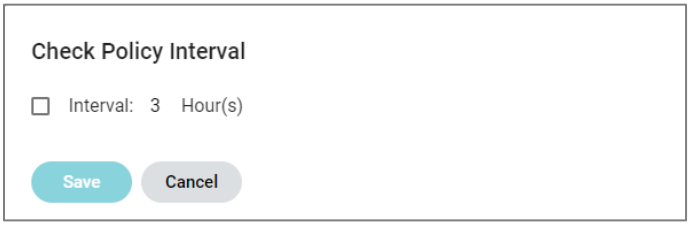
Checking Security Policy Manually

2. Click **Check Policy Now**.
3. When the security policy check is successfully completed, the status displayed for each selected device will change as follows:
   - **Security Status**: (Check Result: Compliant, Non Compliant, etc.)
   - **Security Action Result**: Check Succeeded

Checking Security Policy Automatically

Automatically checks security policy compliance at a regular interval.

1. On the **Security Control** page, click **Check Policy Interval** to open the **Check Policy Interval** dialog box. Ensure that **Interval** setting is enabled.



Check Policy Interval dialog box

2. Click **Save** if the settings have been changed.
3. The security policy check is performed every three hours.
4. Each time the security policy check is performed, the status displayed for each checked target device will change depending on the results:
   - **Security Status**: (Check Result: Compliant, Non Compliant, etc.)
   - **Security Action Result**: Check Succeeded

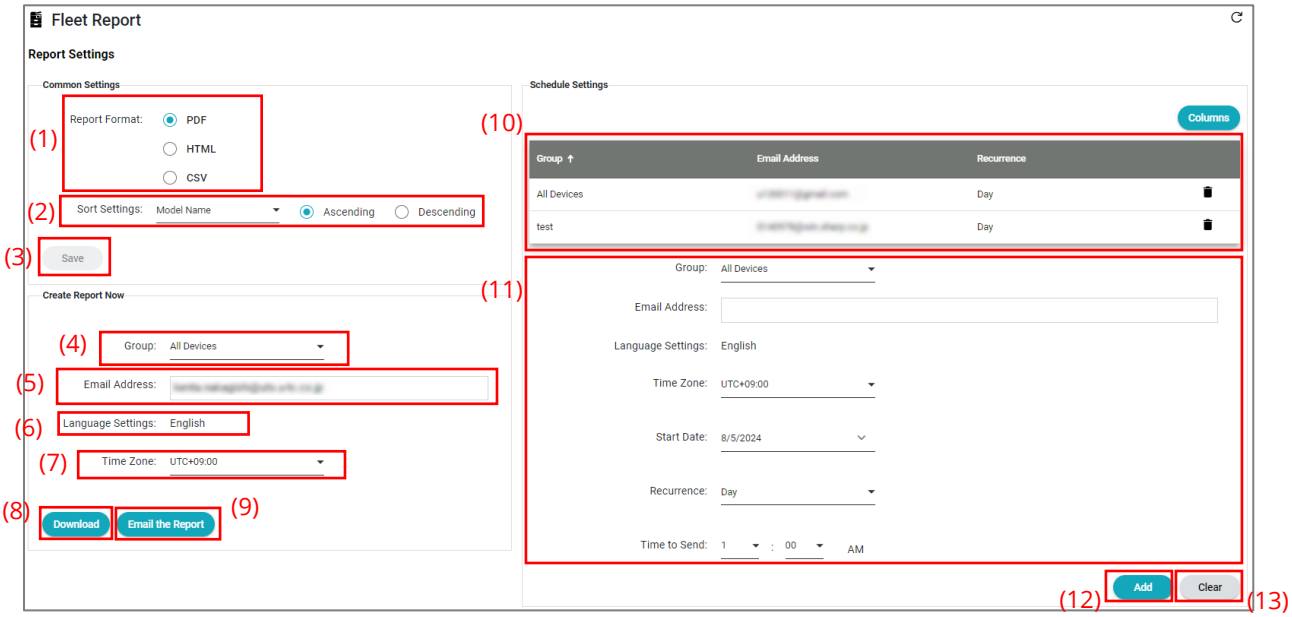
Analytics

Synappx Manage provides three types of reports which can provide summarized data, as follows:

- **Fleet Report**: List of MFPs and printers in the specified Group
- **Usage Report**: Usage by function or daily of MFPs and printers in the specified Group
- **Security Report**: Status of applying Security Policies and detecting policy violations for MFPs and printers in the specified Group

Fleet Report

The **Fleet Report** allows to create a report with counter information for each function type for MFPs and printers in the specified group. This page consists of three areas, which are **Common Settings**, **Create Report Now**, and **Schedule Settings**.



Fleet Report page

Common Settings Area

Configure settings related to the overall report, for example report format.

(1) **Report Format radio buttons**
Users can select the format (PDF, HTML or CSV) of the report to be generated.

(2) **Sort Settings pull-down menu and radio buttons**
Determines the sort order of devices listed in the report.
The pull-down menu allows the user to select the item (Model Name or IP Address) to be sorted.
The radio buttons select the order (Ascending or Descending) of the specified item.

(3) **Save button**
Save the configured common settings.

Create Report Now Area
To create a report, fill out the required settings to generate it.

(4) **Group pull-down menu**
Allows the user to specify the Group containing the devices to be listed.

(5) **Email Address field**
The destination for sending the created report via email. Multiple email addresses can be entered in the **Email Address** field with a delimiter character ";" between each address.

(6) **Language Settings**: English

(7) **Time Zone pull-down menu**
Select the time zone for the report's date and time.

(8) **Download button**
Creates and downloads a report with the configured settings.

(9) **Email the Report button**
Creates a report with the configured settings and sends the report to the specified emails.

Schedule Settings Area
Set up for receiving periodic reports. The schedule for issuing reports can be set on a group-by-group basis. Only one schedule can be set per group.

(10) **Schedule List**
Allows the user to confirm a list of groups to which the schedule is currently registered.

(11) **Scheduled Email settings**
Schedules can be determined per group. Available schedule setting items are as follows:

- **Group**
- **Email Address**
- **Language Settings**
- **Time Zone**
- **Start Date**
- **Recurrence** (Day, Week, or Month)
- **Time to Send**

(12) **Add button**
Fix the settings in (11) and add them to the list in (10).

(13) **Clear button**
Cancel the settings made in (11).

How to Generate a Fleet Report

1. On the **Fleet Report** page, set the following items in the **Common Settings** area according to the contents of the Fleet Report to be created:
   - **Report Format**
   - **Sort Settings**
2. Depending on the availability of the created Fleet Report, perform the following operations:

2-1. To get the Fleet Report download or immediately via email:

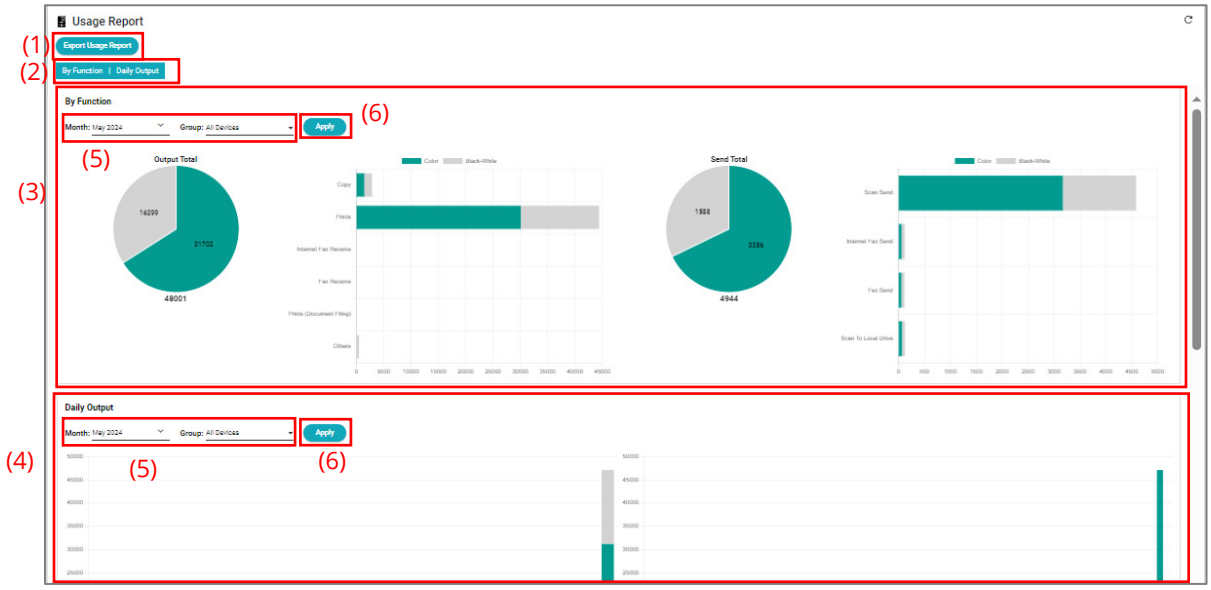
(1) Enter the items in the **Create Report Now** area.

(2) To get it immediately, click **Download** or **Email the Report**.

2-2. To send the Fleet Report to be created on a scheduled basis, set the items in the **Scheduled Settings** and click **Add**.

Usage Report

The **Usage Report** allows the creation of a report with usage information in a specified period for the specified group.



Usage Report page

(1) **Export Usage Report button**
Allows the user to specify settings to export a usage report and send report in mail.

(2) **Report Content links**
Scrolls to the corresponding content of the Usage Report display area.

(3) **By Function Report area**
Shows Output by Function and Send by Function for the specified Group on the last month.

(4) **Daily Output area**
Shows Daily Output for the specified Group on the selected month and previous month.

(5) **Period and Group pull-down menu**
Select the target Group for usage statistics.

(6) **Apply button**

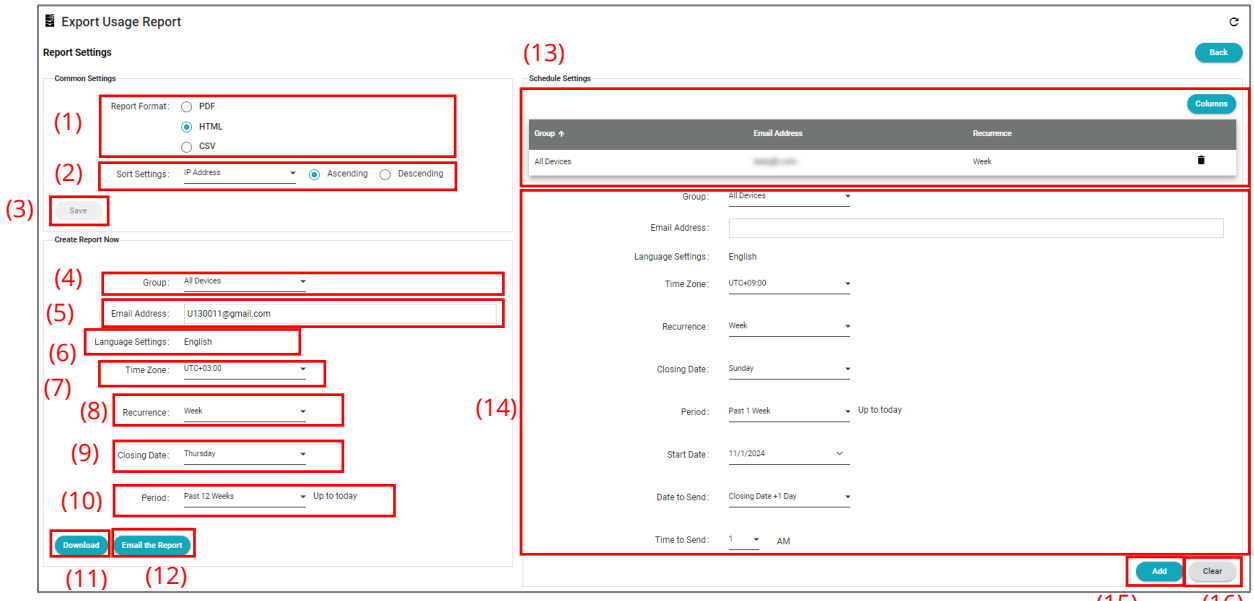
Changing the Target Group for Usage Report

Target groups can be specified for each **By Function** area and **Daily Output** area.

1. In the **Usage Report** page, set the **Group** settings items according to the contents of the Usage Report to be created.
2. Click **Apply**.

How to Generate a Usage Report

The **Export Usage Report** page allows the user to export a usage report based on the settings.



Export Usage Report page

Common Settings Area

(1) **Report Format radio buttons**
Users can select the format (PDF, HTML or CSV) of the report to be generated.

(2) **Sort Settings pull-down menu and radio buttons**
Determines the sort order of devices listed in the report.
The pull-down menu allows the user to select the item (Model Name or IP Address) to be sorted.
The radio buttons select the order (Ascending or Descending) of the specified item.

(3) **Save button**

Create Report Now Area

(4) **Group pull-down menu**
Allows the user to specify the Group containing the devices to be listed.

(5) **Email Address Field**
The destination for sending the created report via email. Multiple email addresses can be entered in the **Email Address** field with a delimiter character "**;**" between each address.

(6) **Language Settings**: English

(7) **Time Zone pull-down menu**
Select the time zone for the report's date and time.

(8) **Recurrence pull-down menu**
Select the recurrence period for the report's date and time.

(9) **Closing Date**
It is not currently available for the usage report.

(10) **Period pull-down menu**
Select the number of periods based on the recurrence setting.

(11) **Download button**
Creates and downloads a report with the configured settings.

(12) **Email the Report button**
Creates a report with the configured settings and emails to the specified emails.

Schedule Settings Area

(13) **Schedule List**
Allows the user to confirm a list of groups to which the schedule is registered.

(14) **Scheduled Email settings**
Schedules can be determined per group. Available schedule setting items are as follows:

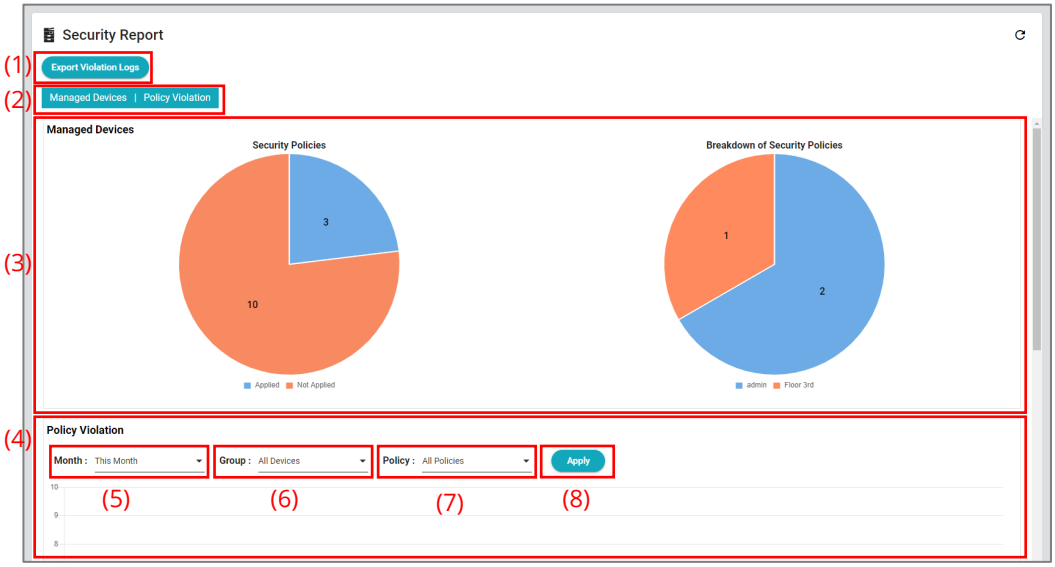
- **Group**
- **Email Address**
- **Language Settings**
- **Time Zone**
- **Recurrence** (Week or Month)
- **Closing Date**
- **Period**
- **Start Date**
- **Date to Send**
- **Time to Send**

(15) **Add button**
Add the configured settings.

(16) **Clear button**
Clear settings and restore to default settings.

Security Report

The **Security Report** describes how the security policies are applied to the managed devices. This data can be exported as a CSV, PDF or HTML file by selecting **Download**.



Security Report page

(1) **Export Violation Logs button**
Allows the user to export a violation log file for the specified period.

(2) **Report Content links**
Scrolls to the corresponding content of the Security Report display area.

(3) **Managed Devices Report area**
Shows the status of Security Policy application to the device.

(4) **Policy Violation Report area**
Shows the violation and remediation counts of policy violations for the month.

(5) **Month pull-down menu**
Select the target Month to check for policy violations.

(6) **Group pull-down menu**
Select the target Group to check for policy violations.

(7) **Policy pull-down menu**
Select the target Security Policy to check for policy violations.

(8) **Apply button**

Export Violation Logs

The **Export Violation Logs** feature allows the user to export a violation log file for the specified period.

Export Violation Logs page

(1) **Report Format radio buttons**
Users can select the format (PDF, HTML or CSV) of the report to be generated.

(2) **Group pull-down menu**
Allows the user to specify the target Group.

(3) **Language Settings**: English

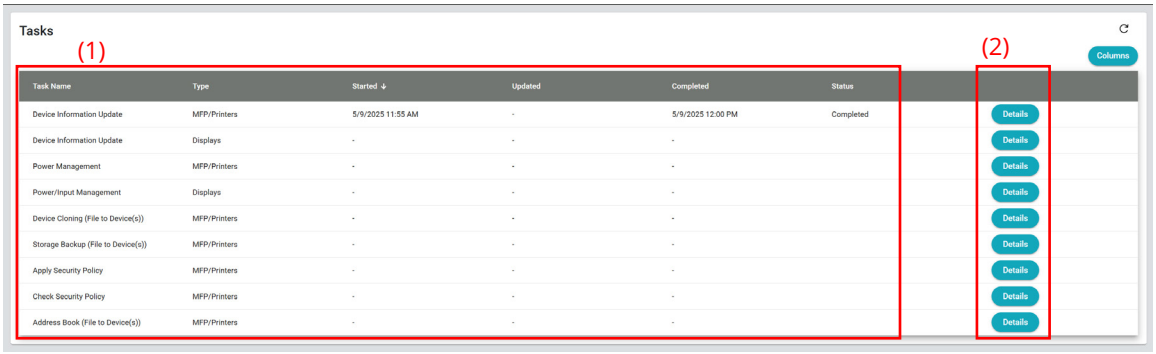
(4) **Date Range (Start Date, End Date) month view**
Specify the period (start date and end date) of data to be exported.

(5) **Download button**
Creates and downloads a report with the configured settings.

(6) **Back button**

Tasks

Some Synappx Manage functions may depend on the MFP's communication interval. This page gives you the status, such as whether they are in progress or have already been completed.



Tasks page

(1) **Task List**
A list of running tasks is displayed.

(2) **Details button**
Display the **Details** dialog. In the dialog, the start and end times of tasks in progress and their results are displayed.

System

Synappx Manage provides log data to assist with troubleshooting and issue resolution. The logs can be viewed from the **System** page.

There are three types of logs:

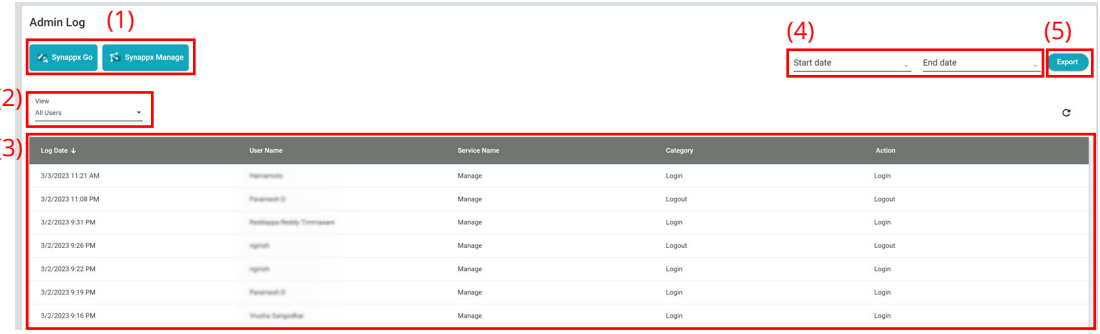
Type	Function
Admin Log	A record of administrator actions at the Synappx admin portal.
Operation Log	A record of user operations performed by users.
Device Log	A record of the history and results of operations performed on all registered devices in the group.

Admin Logs

Since multiple administrators can configure and manage the system, the Admin Log provides a record of the actions performed by each administrator on the Admin Portal.
If Synappx Manage and Synappx Go are licensed, Admin Logs for all services are available on this page.

A record of admin operations appears in the **Admin Log** page.

This list of operations can be filtered to display only the operations which fulfill certain criteria. The Admin Log for the specified period can also be saved in a .CSV file in zip format.



Admin Log page

(1) **Filter buttons by available service**
Switch the Admin Log to be displayed for each available service.

(2) **Filter by User**
Display Admin Logs associated with certain Admin users.

(3) **Admin Log display area**

(4) **Start date and End date filters for Export**
Sets a date range for the exported Admin Log.

(5) **Export button**
Saves the Admin Log for a specified period as a .CSV file.

Filtering Admin Log Events

The Admin Log events can be filtered by available service (e.g., Synappx Go or Synappx Manage) or by the user.

Filtering Admin Log Events

1. To filter log events by available service, click each button (1) (Synappx Go or Synappx Manage) to select and unselect the corresponding services.

   Note:
   Buttons corresponding to unselected services will be displayed with a white background.

2. To filter log events by user, click the **View** field (2) to open the pull-down menu, and select the User name to be listed.

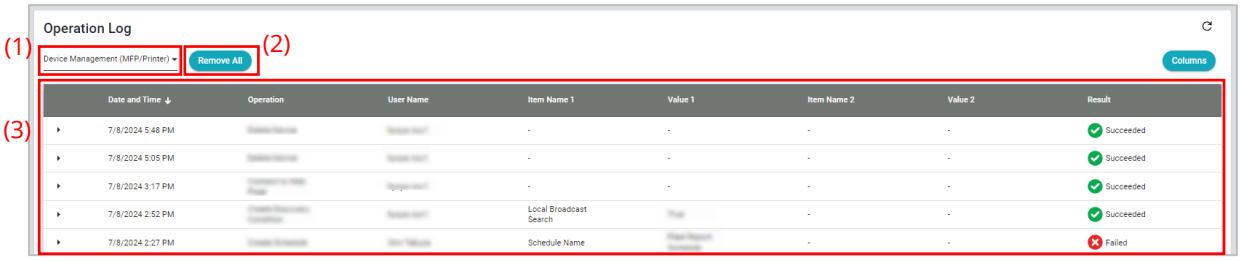
Exporting Admin Log Events

The log events displayed in the **Admin Log** page will then be saved to the specified folder as a zipped .CSV file. The file name for the downloaded file will be in the format "xx (month)-yy (date) -zz (year)_Synappx_Admin_Log", where:

1. Click the **Start date** field to display the calendar. Select the Start date for log events to be exported.
2. Click the **End date** field to display the calendar. Select the End date for log events to be exported.
3. Click **Export** to start downloading.

Operation Logs

The operation log records the operations performed on devices in Synappx Manage.



Operation Log page

(1) **Filter by Management feature**
Filters the Operation Log by a specific management feature.

(2) **Remove All button**
Removes all entries in the Operation Log.
All log events relating to the currently displayed category will be deleted from the Operation Log.

(3) **Operation Log display area**
The Operation Log can appear according to specified filtering criteria.

The following information is displayed in the Operation Log:

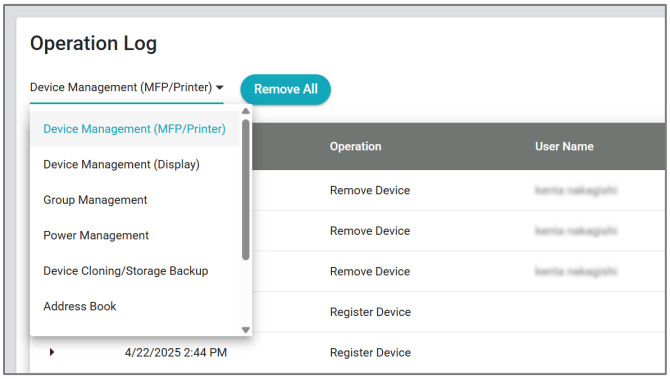
Item	Contents
Date and Time	Date and time when the operation was carried out
Operation	Type of operation (e.g., Add Schedule, Apply Schedule, Manage Power)
User Name	Name of user who carried out the operation
Item Name 1	The details in these columns will vary depending on the type of operation which is carried out. e.g., if a Fleet Report is generated, the "Item 1" and "Value 1" columns will show that the "Format" of the report is "PDF". In cases where no additional information applies, these columns will be blank.
Value 1	
Item Name 2	
Value 2	
Result	Indicates the result of the operation ("Succeeded" or "Failed").

Filtering Operation Log Events

The Operation Log events can be filtered by each management feature, so that only the operations relating to the specified category (such as MFP/Printer Management or Power Management, etc.) are displayed.

1. In the **Operation Log** page, click the management feature field.

2. From the pull-down menu, select the management feature to be shown.



Filtering by Management Feature

Sorting the Operation Log

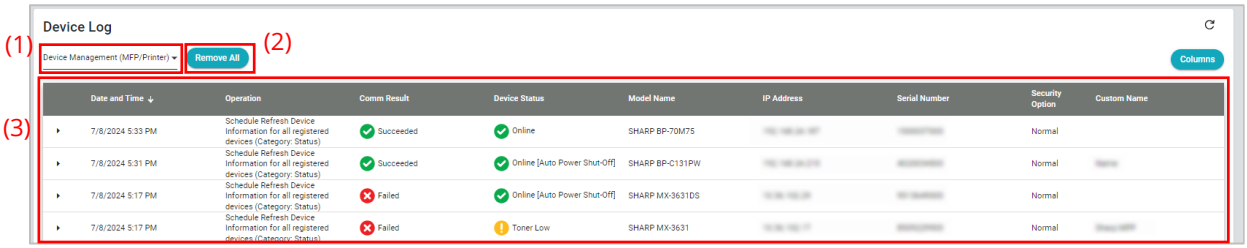
The Operation Log can be sorted alphabetically, in ascending or descending order, using the white arrow next to the column name.

Deleting Operation Log Events

Select **Remove All** to delete operation logs. Only the filtered log events for the specified category will be deleted. Items cannot be restored once they have been deleted.

Device Logs

The device log page displays the history and results of operations performed on all registered devices.



Device Log page

(1) **Filter by Management feature**

(2) **Remove All button**

Removes all entries and log events related to the currently displayed category from the Device Log.

(3) **Device Log display area**

The Device Log can appear for the specified filtering criteria.

The information in the device log:

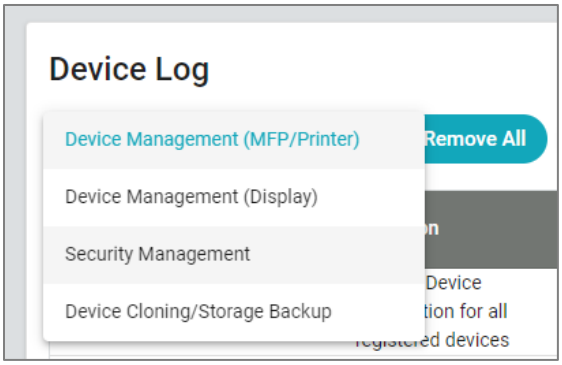
Item	Contents
Date and Time	Date and time when the operation was carried out
Operation	Type of operation (e.g., Add Schedule, Apply Schedule, Manage Power)
Comm Result	Indicates the result of the operation ("Succeeded" or "Failed").
Device Status	Status of the device (Normal, Warning or Error)
Model Name	Model name acquired from the display
IP Address	IP address input at the time of device registration
Serial Number	Manufacturing number acquired from the display
Security Option	Indicates if the device is equipped with the Data Security Kit (DSK). If equipped, "DSK" is displayed; if not, "Normal" is displayed.
Custom Name	User-chosen character string input at the time of device registration

Note:
Device log events cannot be restored once they have been deleted. Only the log events for the currently selected log category will be deleted. For instance, if Device Management (MFP/Printer) is selected, only the Device Management (MFP/Printer) events will be deleted. Other events, such as Device management (Display) or Security Management, will not be deleted.

Filtering Device Log Events

The device log events can be filtered by log category, so that only the log relating to the specified category, such as Device Management (MFP/Printer) or Security Management, etc., are displayed.

1. In the **Device Log** page, click the Log Category field.
2. Select the type of operation from the pull-down menu you would like displayed.



Device Log page

Deleting Device Log Events

1. Use the “Filtering Device Log Events” procedure to select for Device Logs you want to delete.
2. Select **Remove All**. Only the filtered log events for the specified category will be deleted. Items cannot be restored once they have been deleted.

About page

The version information of the Synappx Manage service in use is displayed.

Troubleshooting

Agent Installation Troubleshooting

Problem	Causes and Remedies
Error message is displayed when Sharp Synappx Manage Agent Setup Wizard is starting.	• Error message: “Setting file not found.” Cause: The "settings.properties" file does not exist in the same folder as the .MSI file. Remedies: Start the installer from the directory where the downloaded .ZIP file is extracted. Confirm that the "settings.properties" file exists in the same directory as the installer. • Error message: “Failed to copy setting file.” Cause: Copying settings.properties failed. Remedies: Confirm that you are trying to install with correct user account and it is installed in the correct directory.
Error message is displayed when Sharp Synappx Manage Agent Setup Wizard is running.	• Error message: “The specified directory is not empty.” Cause: The destination folder for installation is not empty. Remedies: Delete the installation destination directory. • Error message: “Port is not available.” Cause: Port 8088 is in use. Remedies: Stop the application using port 8080. • Error message: “An error occurred. (99)” Cause: An internal error has occurred. Remedies: Reboot the system and try the installation again.

Agent Settings Troubleshooting

Problem	Causes and Remedies
Error code is displayed when the Sharp Synappx Manage Agent dialog box starts.	Ensure that AgentServiceLauncher and AgentService are running as Windows service. • F005-E901: Agent service is not running.
Error code is displayed when Save button is pressed in the Proxy Settings dialog box.	Check the input value for the following error codes. • F001-E103: Check Error for Username of Proxy Settings • F001-E104: Check Error for Password of Proxy Settings • F001-E107: Check Error for IP Address of Proxy Settings • F001-E108: Check Error for Port number of Proxy Settings Ensure that AgentServiceLauncher and AgentService are running as Windows service. • F001-E901: Agent service is not running.
Error code is displayed when Save button is pressed in the Sharp Synappx Manage Agent dialog box.	Check the input value for the following error codes. • F001-E103, F002-E103: Check Error for Username of Proxy Settings • F001-E104, F002-E104: Check Error for Password of Proxy Settings • F001-E107, F002-E107: Check Error for IP Address of Proxy Settings • F001-E108, F002-E108: Check Error for Port number of Proxy Settings • F002-E101: Check Error for IP Address Check the Manage Service's operational status and Proxy Settings. • F003-E003, F004-E003: Connection error to Manage Service Enter Activation Code. • F003-E105: Invalid Activation Code Activation Code expired or already activated • F003-E106: Activation Error Ensure that AgentServiceLauncher and AgentService are running as Windows service. • F001-E901, F002-E901, F003-E901, F004-E901: Agent service is not running.

MFP/Printer Troubleshooting

Problem	Causes and Remedies
"Communication Error (0301)" is displayed in the "Communication status" column of the Device List.	Causes: There is no response from the device for some reason, such as the power supply for the device is turned off, or the device is disconnected from the network. Remedies: Check the power supply and network settings for the device.
"Communication Error (0303)" is displayed in the "Communication status" column of the Device List.	A model name or serial number different than those belonging to registered devices detected. Causes: This may occur when a different device has been connected to the IP address that has been set for the registered device. Remedies: • Repeat the device discovery procedure to clear the error. (Refer to "Searching Devices".) • In a DHCP (Dynamic Host Configuration protocol) environment, IP addresses are changed dynamically. Accordingly, after an IP address has changed, "Communication Error (0303)" will be generated the next time Synappx Manage checks the device status. • If using Synappx Manage in a DHCP environment, use the schedule settings to regularly carry out device discovery. (Refer to "Power & Input Schedules Management".)
"Communication Error (0201)" is displayed in the "Communication status" column of the Device List.	Causes: A communication error that occurs when there is no response from the Agent. Remedies: • Ensure the Agent is running. • Check the network environment of the PC on which the Agent is installed. • If the Agent UI doesn't start, restart your PC and try again.
"Communication Error (Result:7)" is displayed in the log for System>Device Log>Security Management.	Causes: • Communication with the target device failed when security policies were being checked. • The status of the target device did not allow execution. (e.g., The setting screen was displayed on the operation panel.) Remedies: Check the status of the target devices and execute again.
"Communication Error (Result:12)" is displayed in the log for System>Device Log>Security Management.	

Problem	Causes and Remedies
"Communication Error (Result:13)" is displayed in the log for System>Device Log>Security Management.	Causes: • Communication with the target device failed when security policies were being applied. • The status of the target device did not allow execution. (e.g., The setting screen was displayed on the operation panel.) Remedies: Check the status of the target devices and execute again.
"Communication Error (Result:14)" is displayed in the log for System>Device Log>Security Management. "Communication Error (Result:15)" is displayed in the log for System>Device Log>Security Management.	Causes: • Communication with the target device failed when security policies were being processed. • The status of the target device did not allow execution. (e.g., The setting screen was displayed on the operation panel.) Application of policies was completed. Remedies: If necessary, check the status of the target devices and execute again.
Search results are not displayed even though the device exists.	Causes: Error in search conditions. Or the device is already registered.
"Communication Error (0310)" is displayed in the "Communication status" column of the Device List	Causes: An unexpected communication error occurred with the target device. Remedies: Confirm the connected network environment.
"Communication Error (0330)" is displayed in the "Communication status" column of the Device List	Causes: The SNMP v1 setting of the direct connected MFP is disabled. Remedies: Check the SNMP v1 setting of the device's network configuration.

Display Troubleshooting

Problem	Causes and Remedies
Unable to register a display in Synappx Manage.	Causes: The target display is not configured to connect with the network, preventing communication. Remedies: Confirm the network settings of the display and try the registration process again.
Device information is not displaying correctly in the Devices>Displays page ("UNSELECTED" or "-9998" is displayed)	Causes: The status of the target display prevented data from being properly acquired. The "RS-232C/LAN switch" setting is not set to "LAN". Remedies: Confirm the status of the display and then attempt to update the device information.

Problem	Causes and Remedies
Device information is not displaying correctly in the Devices>Displays page ("#N/A" or "-9999" is displayed) or the display cannot be operated via Synappx Manage.	Causes: The status of the target display prevented data from being properly acquired. • POWER SAVE MODE is set to ON for the display and the display is in standby mode. • Even when POWER SAVE MODE is set to OFF for a display, depending on the power status of the display, Synappx Manage may not be able to retrieve information or the display may not accept commands. Remedies: Confirm the status of the display and then attempt to update the device information.
Device information is not displaying correctly in the Devices>Displays page ("UNKNOWN" or "-9997" is displayed)	Causes: The device information of the applicable item has not been retrieved from the target display. Remedies: Confirm the status of the display and then attempt to update the device information.
Search results are not displayed even though the device exists.	Causes: • Error in search conditions • Device is already registered
"Communication Error (0310)" is displayed in the "Communication status" column of the Device List.	Causes: An unexpected communication error occurred with the target display. Remedies: Confirm the connected network environment.

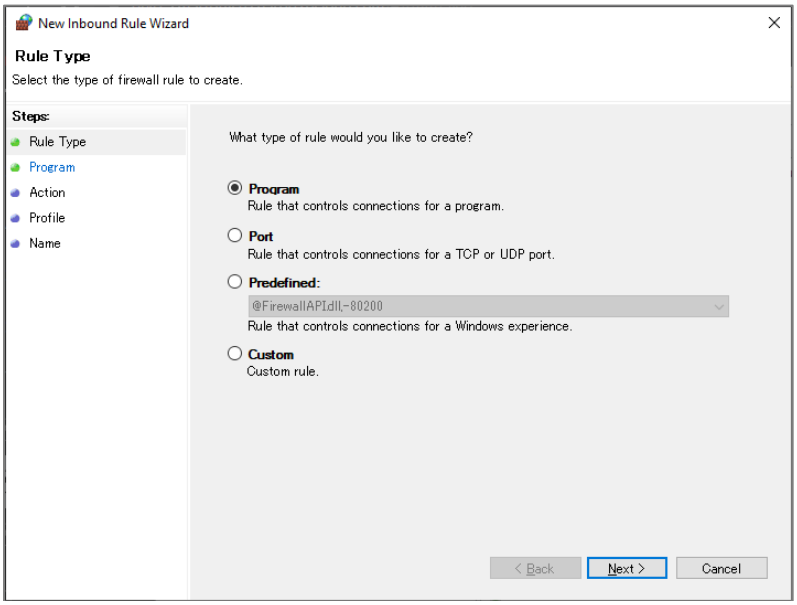
Appendix

This section describes the latest Synappx Manage system requirements, known issues, workarounds, and limitations.

Windows Firewall Settings

The Windows Firewall settings of the computer on which Synappx Manage Agent is installed must be updated, so that the Agent can communicate with other devices which all are connected via TCP/IP network.
To open the relevant port and allow the protocol, configure the following settings:

1. On the desktop screen of a computer in which the Agent is to be installed, press the Windows key and the "R" key at the same time.
2. The **Run** dialog box will open. Enter "WF.msc" and click **OK**.
3. To add a new rule:
   1) Select **Inbound Rules**, then right-click **Inbound Rules** and select **New Rule...**.
   2) Follow the on-screen instructions to add the new rule.



Windows Firewall Settings

Select the settings for the new rule. Use the default settings for all other items.

- For **Rule Type**, select **Port**, and click **Next**.
- For **Protocol and Ports**, select **TCP**. Select **Specific Local Ports** and enter "8088". Then click **Next**.
- After selecting connection settings, and rule application option, enter any name in **Name**.

4. Select **Exit** from **File** menu.
   A confirmation screen will appear. Click **Yes** and then **Save** to save the console.

List Grid User Interface Behaviors

Select All

The “Select All” checkbox will select the items displayed on that page. If the user does any of the following action(s), the “Select All” selection will be reset:

- Changing “Items per page” in the bottom of the list grid
- Navigating to the next page or previous page
- Unselecting any of the selected items in the page
- Clicking “Filter” from the dashboard

If all items on a page are selected one at a time, “Select All” will be enabled.

- If any item is left unchecked, “Select All” will be unchecked.

If the user does any of the following, items selection on a page (partially / fully) will be reset:

- Changing “Items per page” in the bottom of the list grid
- Navigating to the next page or previous page
- On unselecting any of the selected items in the page
- On clicking “Filter” from the dashboard

MFP/Printers Management

Difference between MFP status and detected status on Synappx Manage

If multiple errors occurred on a device at the same time as “Printer Error [Account Limit], Synappx Manage will not detect "Printer Error [Account Limit]".

"Local Broadcast Search" Failure

A broadcast search may not be successful, depending on router settings/limitations. Alternatively, try to use **IP Range Search**.

Port settings for Remote Operation

When using the Remote Operation feature on the following models, connect with port number 5901:

MX-C357F/C407F/C507F/C557F/C607F/C407P/C507P/C607P
MX-B557F/B707F/B557P/B707P
MX-B427W/B467F/B427PW/B467P
MX-C428F/C528F/C528P/C358F/C428P/B468F

Some PC keyboard keys allow the user to operate the panel remotely instead of using the device's hard keys.

SNMPv3 settings on MFP/Printer

When using the following models, the default setting "Authentication, Privacy" (Display language: English) should be selected for the Minimum Authentication Level:

MX-C357F/C407F/C507F/C557F/C607F/C407P/C507P/C607P
MX-B557F/B707F/B557P/B707P
MX-B427W/B467F/B427PW/B467P
MX-C428F/C528F/C528P/C358F/C428P/B468F

Fiery Print Server-Equipped Devices

Synappx Manage does not support any Fiery Print Server-equipped devices.

Supported MFPs for Device Cloning, Storage Backup, Address Book, Security Control and Power control features.

Device Cloning, Storage Backup, Address Book, Security Control and Power control features are not available for MFPs that do not support these functions. If these functions are not supported on an MFP, the MFP does not appear in each feature screen. Supported functions on each MFP are as follows:

Model	Device Cloning, Storage Backup	Address Book	Security Control	Power Control
BP-B537WR/B540WR/B547WD/ B550WD series BP-B547PW/B550PW series	✓	✓**	✓	✓
BP-90C70/90C80 series	✓	✓**	✓	✓
BP-70M75/70M90 series	✓	✓**	✓	✓
BP-60C26/60C31/60C36/60C45/ 70C26/70C31/70C36/70C45 series	✓	✓**	✓	✓
BP-70C55/C65 series	✓	✓**	✓	✓
BP-40C26/50C26/50C31/40C36/ 50C36/50C45/55C26 series	✓	✓**	✓	✓
BP-50C55/50C65 series	✓	✓**	✓	✓
BP-70M31/70M36/70M45/70M55/ 70M65 series	✓	✓**	✓	✓
BP-50M26/50M31/50M36/50M45/ 50M55/50M65 series	✓	✓**	✓	✓
BP-30M28/30M31/30M35 series	✓		✓	✓
BP-20M22/20M24/20M28/20M31 series				
MX-7081/8081 series	✓		✓	✓
MX-3061/3071/3561/3571/4061/ 4071/5071/6071 series	✓		✓	✓
MX-2651/3051/3551/4051/5051/ 6051/6151 series	✓		✓	✓

Model	Device Cloning, Storage Backup	Address Book	Security Control	Power Control
MX-M3071/M3571/M4071/M5071/ M6071 series	✓		✓	✓
MX-M2651/M3051/M3551/M4051/ M5051/M6051 series	✓		✓	✓
MX-6580/7580 series	✓		✓	✓
MX-3060/3070/3560/3570/4060/ 4070/5070/6070 series	✓		✓	✓
MX-3050/3550/4050/5050/6050 series	✓		✓	✓
MX-2630 series	✓		✓	✓
MX-M3070/M3570/M4070/M5070/ M6070 series	✓		✓	✓
MX-M3050/M3550/M4050/M5050/ M6050 series	✓		✓	✓
MX-M2630 series	✓		✓	✓
MX-5141/5140/4141/4140 series	✓		✓	✓
MX-2640/3140/3640 series	✓		✓	✓
MX-2615/3115 series	✓		✓	✓
MX-2614/3114 series	✓		✓	✓
DX-2000/2500 series	✓		✓	✓
MX-M6570/M7570 series	✓		✓	✓
MX-B376W/B476W/B356W/B456W series	✓		✓	✓
MX-B355W/B455W series	✓		✓	✓
MX-C303W/C304W series	✓		✓	✓
MX-C301 series	✓		✓	✓
MX-M1056/M1206 series	✓		✓	✓
MX-M905 series	✓		✓	✓
MX-M1055/M1205 series	✓		✓	✓
MX-M654/M754 series	✓		✓	✓
MX-M365/M465/M565 series	✓		✓	✓
MX-M364/M464/N564 series	✓		✓	✓
MX-M265/M266/315/M316 series				
MX-C357F/C407F/C507F/C557F/ C607F/C407P/C507P/C607P/B557F/ B707F/B557P/B707P series				
MX-B427W/B467F/B427PW/B467P series				
MX-C428F/C528F/C528P/C358F/ C428P/B468F series				
BP-90C70/90C80 series	✓	✓**	✓	✓
BP-C533WR/C535WR/C533WD/ C535WD/C542WD/C545WD series BP-C542PW/C545PW series	✓	✓**	✓	✓

Model	Device Cloning, Storage Backup	Address Book	Security Control	Power Control
BP-1200C/1200S series				
BP-1250M/1360M series				
BP-C131WD/C131PW series	✓*		✓*	✓*

*: Direct Connection Only **: Direct Connection Only, Latest Firmware is required.

Note:
The actual devices with Data Security Kit have not been tested.
For information of the management of BP-1200C/1200S, BP-1250M/1360M, contact your dealer or nearest SHARP Service Department.

Direct Connection supported models

Direct Connection supported models are as follows:

Color MFP

MX-3061/3071/3561/3571/4061/4071/5071/6071 series
MX-3061S/3071S/3561S/3571S/4061S/4071S/5071S/6071S series
MX-2651/3051/3551/4051/5051/6051 series
MX-C303W/C304W series
MX-C303WH/C304WH series
BP-60C31/60C36/60C45 series, BP-70C31/70C36/70C45/70C55/70C65 series
BP-50C26/50C31/50C36/50C45/50C55/50C65/55C26 series
BP-90C70/90C80 series
BP-C533WR/C535WR series, BP-C533WD/C535WD/C542WD/C545WD series
BP-C542PW/C545PW series
BP-C131WD/C131PW series
MX-C357F/C407F/C507F/C557F/C607F/C407P/C507P/C607P series (via .eSF application)
MX-C428F/C528F/C528P/C358F/C428P series (via .eSF application)

B/W MFP

MX-M3071/M3571/M4071/M5071/M6071 series
MX-M3071S/3571S/4071S/5071S/6071S series
MX-M2651/M3051/M3551/M4051/M5051/M6051 series
MX-B376W/B476W/B356W/B456W series
MX-B376WH/B476WH/B356WH/B456WH series
BP-70M31/70M36/70M45/70M55/70M65 series
BP-50M26/50M31/50M36/50M45/50M55/50M65 series
BP-70M75/70M90 series
BP-B537WR/B540WR/B547WD/B550WD series
BP-B547PW/B550PW series
MX-B557F/B707F/B557P/B707P series (via .eSF application)
MX-B467F series (via .eSF application)
MX-B468F series (via .eSF application)

Display devices management

Accessing Device Web Pages

The http communication allows the user to access the device web pages.
The following table shows whether a device web page is available for each display:

Sharp models

Model	Device Web Pages
PN-L705H/PN-70TH5, PN-L805H/PN-80TH5	✓
PN-L401C/PN-40TC1, PN-L501C/PN-50TC1	
PN-L651H/PN-65TH1, PN-L751H/PN-75TH1, PN-L851H/PN-85TH1	
PN-R426, PN-R496, PN-R556, PN-R606, PN-R706	✓
PN-Y326, PN-Y436/Y436P, PN-Y496/Y496P, PN-Y556/Y556P	
PN-V701	✓
PN-UH431, PN-UH501, PN-UH551, PN-UH861	
PN-HW431, PN-HW501, PN-HW551, PNHW651, PN-HW751, PN-HW861	
PN-65HC1, PN-C751H/PN-75HC1, PN-C861H/PN-86HC1, PN-CE701H/PN-70HC1E	
PN-HW431T, PN-HW501T	
PN-HS431, PN-HS501, PN-HS551	
PN-HY431, PN-HY501, PN-HY551	
PN-HE651, PN-HE751	✓
PN-HC651, PN-HC751, PN-HC861	✓
PN-L652B, PN-L752B, PN-L862B	
PN-LC652, PN-LC752, PN-LC862	
PN-LM431, PN-LM551	
PN-LA652, PN-LA752, PN-LA862	✓
4W-B55FT5U, B65FT5U, B75FT5U, B86FT5U	
4P-B43EJ2U, B50EJ2U, B55EJ2U, B65EJ2U, B75EJ2U, B86EJ2U	

Sharp NEC Displays Solutions models

Model	Device Web Pages
C651Q C751Q, C861Q, C981Q, V554Q, V654Q, V754Q, V864Q, V984Q, P654Q, P754Q	
P435, P495, P555, MA431, MA491, MA551, M751, M861	✓
C750Q, C860Q, M321, M431, M491, M551, M651	✓
ME431, ME501, ME551, ME651	✓
E328, E438, E498, E558, E658, E758, E868	✓
PN-ME432, PN-ME502, PN-ME552, PN-ME652, PN-ME752, PNME862, PN-ME982	✓
PN-P436, PN-P506, PN-P556, PN-P656 PN-M322, PN-M432, PN-M502, PN-M552, PN-M652	✓
CB651Q, CB861Q, CB751Q	

"Color Mode" displayed as Device information
For the following displays, the Picture Mode setting is displayed as the Color Mode:
PN-HE651/HC651, PN-HE751/HC751, PN-HC861

In the following case, the content will be different from the actual setting:

Displayed "Color Mode"	Picture Mode Setting
Media Player (or PC)	Conferencing

"Screen size" displayed as Device information
For the following displays, some input modes display "Screen Size" information that is different than the actual screen size:

PN-Y326, PN-Y436/Y436P, PN-Y496/Y496P, PN-Y556/Y556P

Affected input modes: HDMI[AV], D-SUB[COMPONENT], D-SUB[VIDEO] or Media Player

Displayed "Screen Size"	Actual Screen Size
Zoom (or Zoom1)	Normal
Zoom2	Dot by Dot

PN-65HC1, PN-CE701H/70HC1E, PN-C751H/75HC1, PN-C861H/86HC1

Displayed "Screen Size"	Actual Screen Size
Normal	Dot by Dot
Dot by Dot	4:3

PN-L652B/L752B/L862B, PN-LC652/LC752/LC862
When Actual Screen Size is "Wide", the Screen Size displayed on Synappx Manage is "Unknown".

“Usage Time” displayed as Device information
For the following displays (N-format), because the "Usage Time" definition is different from other displays, the "Usage Time" tends to be large value more than on other displays:

PN-LA652/LA752/LA862, PN-L652B/L752B/L862B, PN-LC652/LC752/LC862

Registering displays to Synappx Manage
Synappx Manage cannot complete device registration when the following devices are in standby mode. Change the device settings from standby mode to power on mode.
PN-UH431/UH501/UH551/UH861, PN-HW431/HW501/HW551/HW651/HW751/HW861,
PN-HW431T/HW501T, PN-HS431/HS501/HS551, PN-HY431/HY501/HY551
PN-CE651H/65HC1, PN-CE701H/70HC1E, PN-C751H/75HC1, PN-C861H/86HC1,
PN-HE651/HE751, PN-HC651/HC751/HC861

Power Control for Displays
Once the following devices are switched to standby mode, Synappx Manage cannot communicate with them:
PN-CE651/65HC1, PN-CE701H/70HC1E, PN-C751H/75HC1, PN-C861H/86HC1
PN-Y436P/Y496P/556P

Notes for PN-HC651, PN-HC751, PN-HC861, PN-HE651, PN-HE751
Set the Energy Mode settings to Office mode.
While the display is in standby mode, it cannot respond to scheduled Input Change.

Notes for 4W-xxxx series and 4P-xxxx series
For the following displays, make sure that the latest firmware is applied and then set POWER SAVE MODE to OFF. When POWER SAVE MODE is set to ON, Synappx Manage cannot control in the standby mode/input signal waiting state.

4W-B55FT5U/B65FT5U/B75FT5U/B86FT5U
4P-B43EJ2U/B50EJ2U/B55EJ2U/B65EJ2U/B75EJ2U/B86EJ2U

Notes for E328, E438, E498, E558, E658, E758, E868
They automatically shift to Power-Save mode over time and Synappx Manage cannot get any information of displays in Power-Save mode. Set the setting of [Quick Start] to “ON” to prevent automatic shift to Power-Save mode.

SYNAPPX™

For more information, visit the Synappx support site.

Access the Synappx Terms of Use at https://business.sharpusa.com/synappx-support/about/termsofuse.
Access the Synappx Privacy Policy at https://business.sharpusa.com/synappx-support/About/Privacy.
Access the Synappx End User License Agreement at https://business.sharpusa.com/synappx-support/about/EULA.

(US_Rev.25_05_1)