

**SHARP®**

# Sharp Remote Device Manager (SRDM)

## Operation Guide

# CONTENTS

<b>INTRODUCTION .....</b>	<b>3</b>	Device Discovery .....	39
<b>SHARP REMOTE DEVICE MANAGER (SRDM) .....</b>	<b>4</b>	Setting device discovery conditions .....	40
<b>BASIC SRDM OPERATIONS .....</b>	<b>5</b>	Managing SNMP settings .....	41
Launching SRDM .....	5	Registering devices in the Registered Devices List.....	42
Basic window configuration .....	7	Updating device status and data .....	42
<b>GROUP PANE.....</b>	<b>9</b>	Deleting devices.....	42
<b>GROUP CONCEPT .....</b>	<b>10</b>	Restoring deleted devices .....	42
<b>GROUP MANAGEMENT.....</b>	<b>11</b>	Copying or moving devices.....	43
Creating groups .....	11	Setting scheduled actions .....	43
Group Menu Items.....	15	Creating filters.....	46
Editing groups.....	17	Changing the conditions for icon display .....	47
Deleting groups .....	17	Setting E-Mail alerts.....	48
Restoring deleted groups .....	17	Accessing device operation panel remotely .....	50
<b>ACCOUNT MANAGEMENT .....</b>	<b>18</b>	<b>ADVANCED FEATURES .....</b>	<b>51</b>
<b>DEVICE/SYSTEM TAB .....</b>	<b>23</b>	[Device List] tab .....	53
[Registered Devices] tab .....	25	[Security Dashboard] tab .....	54
[Device Log] tab.....	27	[Power Management] tab.....	60
[Sub Group List] tab .....	27	[Device Cloning] tab.....	63
[Group Information] tab .....	28	<b>FILE DISTRIBUTION FEATURE.....</b>	<b>68</b>
[Device Discovery] tab.....	30	Preparing to Use File Distribution Feature.....	69
[Counter History] tab .....	30	File Upload .....	70
[Operation Log] tab.....	31	File Download .....	71
[Display Option] buttons .....	32	File Delete.....	71
<b>DEVICE DETAILS .....</b>	<b>33</b>	<b>TROUBLESHOOTING.....</b>	<b>72</b>
[Device Status] tab .....	34	<b>APPENDIX.....</b>	<b>73</b>
[Device Information] tab .....	35	Schedule Maintenance .....	73
[Device Log] tab.....	36	Case1: Login and Adding User Accounts with Default Account.....	74
[SNMP Settings] tab .....	36	Permission details.....	75
[Counter History] tab .....	37	Icons displayed in device images .....	78
[Operation Log] tab.....	38		
<b>DEVICE MANAGEMENT .....</b>	<b>39</b>		

# INTRODUCTION

---

## ■ Please note

- The explanations in this Guide assume that the person who installs the product and the users of the product have a working knowledge of Microsoft Windows.
- For information about the operating system, please refer to your operating system manual or the online help.
- Screenshots in this guide are using the theme "Enterprise Blue".
- Screenshots and contents in this guide may be changed. (As of June 2017)
- For the latest information on Sharp Remote Device Manager (hereinafter referred to as "SRDM") software and any considerations that are not described in this document, refer to "Readme" of SRDM. ["Readme" can be accessed from the \[Help\] menu.](#)

## ■ Attention

- The device information displayed by this software may not be able to accurately reflect the statuses of actual devices, depending on data retrieval timing and the network status.
- The counter values displayed by this software may vary from the counter values at the time of polling.
- This software makes no warranty as to the data handled by the software. Sharp Corporation assumes no responsibility for loss or corruption of data. It is recommended that the customer ensures that backing up of data has been carried out. Refer to the Setup Guide for information on how to back up databases.
- Please make sure that JavaScript is enabled on your Web browser settings. Cookies must be enabled for a browser on a client computer to run properly.

## ■ Warranty

While every effort has been made to make this document as accurate and helpful as possible, Sharp Corporation makes no warranty of any kind with regard to its content. All information included herein is subject to change without prior notice. Sharp Corporation is not responsible for any loss or damages direct or indirect arising from or related to the use of this document.

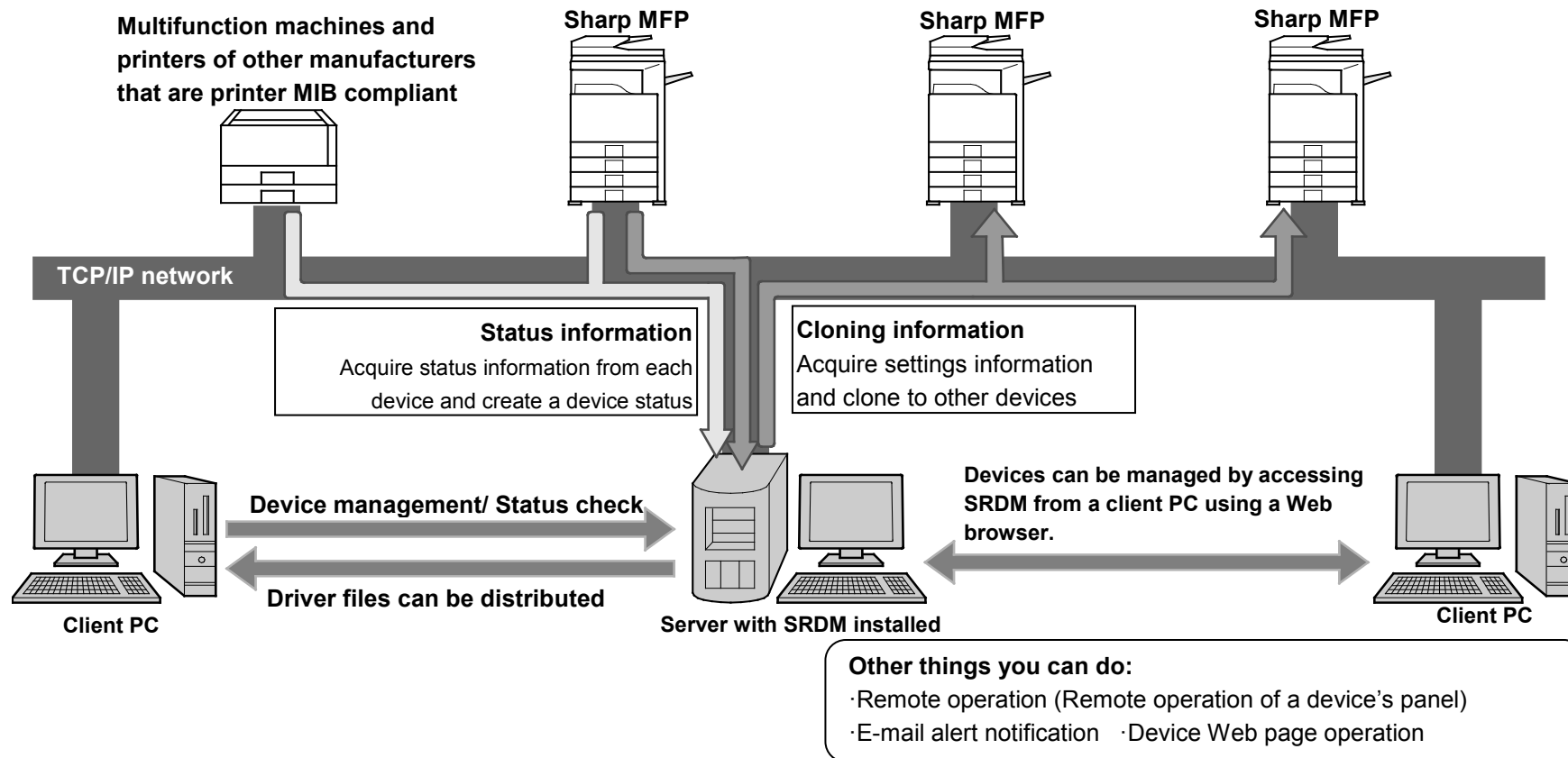
© 2014 SHARP CORPORATION

Reproduction, adaptation or translation without prior written permission is prohibited, except as allowed under copyright laws.

# SHARP REMOTE DEVICE MANAGER (SRDM)

SRDM makes it easy for users to manage and maintain a fleet of digital multifunction machines and printers (hereinafter referred to as "devices") connected by a TCP/IP network to the computer on which the software is installed. It provides a consolidated management of these devices and allows you to configure and receive e-mail notifications whenever a device status is changed to a warning or error state.

Other operations you can perform include cloning the settings between the devices, distributing the driver files to other users, displaying device web pages from SRDM to configure settings and controlling devices remotely.



- Digital multifunction machines and printers of Sharp and other manufacturers which can be managed using SRDM are referred to as "devices" in this guide.
- To fetch device data at certain intervals, set scheduled actions. For more information, refer to "[Setting scheduled actions](#)".



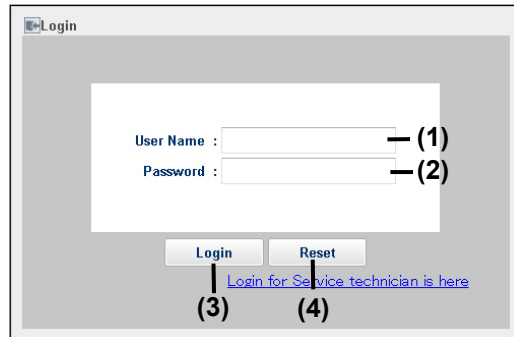
# BASIC SRDM OPERATIONS

## Launching SRDM

### ■ Launching SRDM on the computer (server) on which SRDM is installed

#### *When launching SRDM from SRDM Service Control Panel*

Click the [Open] button on the SRDM Service Control Panel. The web browser that is set as default is launched and SRDM is displayed.



#### *Launching from a browser*

Based on the desired communication protocol (http or https), enter any of the following URLs in the address bar of a web browser.

- HTTP connection (Default settings):  
http://<<ServiceIP address>>:8085/WebUI/
- HTTPS connection (Default settings):  
https://<<Service IP address>>:8086/WebUI/

In place of "<<Service IP address>>", enter the IP address which has been set as the service IP address for the common settings in the SRDM Control Panel or the computer name.

### ■ Launching from a PC via a network

You can use a web browser to access the computer that SRDM is installed on via any other computer which is connected to the same TCP/IP network. Open the web browser on the PC and then based on the desired communication protocol (http or https), enter any of the following URL in the address bar.

- HTTP connection (Default settings):  
http://xxxxxx:8085/WebUI/
- HTTPS connection (Default settings):  
https://xxxxxx:8086/WebUI/

Enter the IP address or host name of the computer on which SRDM is installed instead of "xxxxxx". Check with your administrator for the IP address and port number.

When SRDM is successfully accessed, the login screen opens.

### ■ Login to SRDM

#### 1. Enter User Name and Password in (1) and (2).

Default credentials:

- (1) User Name : admin
- (2) Password: (Generated by SRDM. Refer to the SRDM Server Software Setup Guide)

## BASIC SRDM OPERATIONS (CONTINUED)

### 2. Click the Login (3) button to log into SRDM

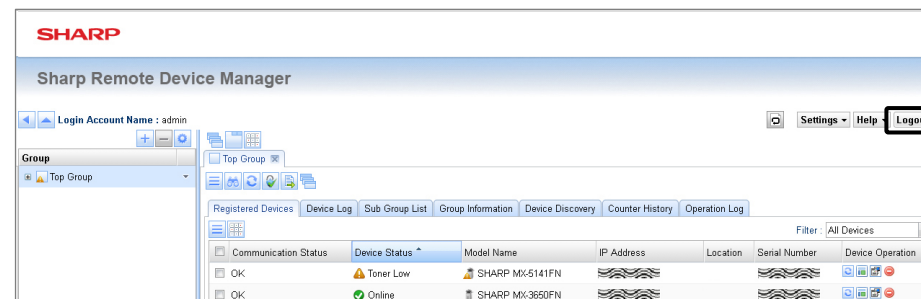
- If you want to reset the entry, click the Reset (4) button.



- It is recommended to change the password after first time login. To change the login password, open [Settings], select [Properties] and then click [Change password]. The password can be from 8 to 128 single-byte alphanumeric characters and/or symbols in length. A blank password or a password consisting of only spaces is forbidden.
- Account will be locked out for 30 minutes after 5 or more consecutive invalid login attempts.

### ■ Logout of SRDM

After login to SRDM, you can logout of SRDM by clicking on the [Logout] button at the upper right corner of the screen.

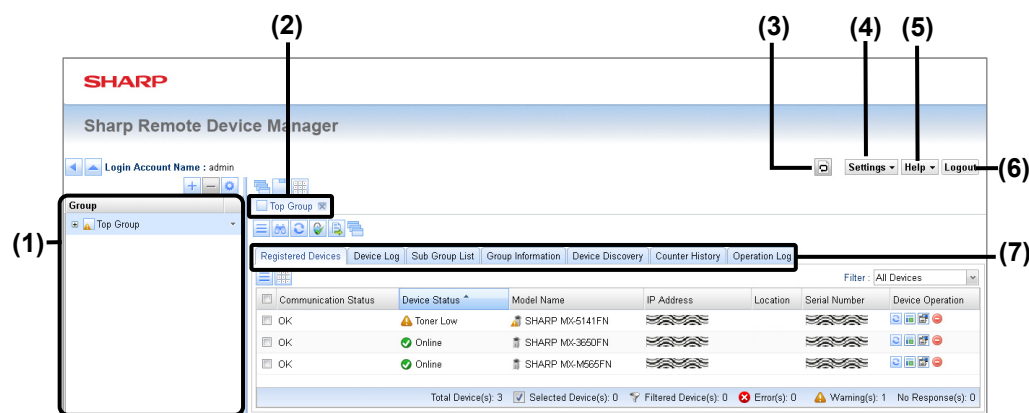


- If no operation is performed on SRDM for more than 30 minutes, the session is closed and logged out automatically.
- To prevent unauthorized use, it is recommended that you logout of SRDM after using it.

# BASIC SRDM OPERATIONS (CONTINUED)

## Basic window configuration

Below screen appears after you log in to SRDM.



The contents and the enabled items which are displayed in the screen may vary depending on the permissions assigned to the logged-in account (Refer to [“Permission details”](#)). In addition, the permissions which can be assigned will vary depending on the permissions available for the logged-in account. (Refer to [“Creating accounts”](#).)

This Operation Guide describes the display contents and operations when the user is logged on to an account with system administrator permissions, group administrator permissions or account manager permissions.

### Group pane

In the Group pane, available groups will be displayed in tree format.

### [Group] tabs

The [Group/Device] tabs are displayed in the [Group] tab area. The [Group] tab for a specific group can be opened by clicking on the Group name in the Group pane. The [Device] tab for a specific device can be opened by clicking on a specific device in the device list. To close the tab which is open, click on the tab close button “✕”.

### [Refresh] button “🔄”

Click the [Refresh] button to update the group tree and the displayed tab contents with the latest information from SRDM server.

### [Settings] button

When you click the [Settings] button, a menu will appear asking you to choose from Themes, Download Log, SMTP Settings, Scheduled Action, E-mail Alerts, Schedule Log Delete, Schedule Maintenance, System Log, Account Management and Properties.

- Themes: Allow you to change the UI display theme setting.
- Download Log: You can download various logs generated by SRDM.
- SMTP Settings: You can make mail server settings for mail alerts. For more information, refer to [“Setting E-Mail alerts”](#).
- Scheduled Action: You can set various operations such as device discovery and registration, device status updating and device information updating to be carried out automatically according to scheduled settings. For more information, refer to [“Setting scheduled actions”](#).
- E-mail Alerts: You can use this to set items such as the contents of e-mail alerts and sending destinations. For more information, refer to [“Setting E-mail alerts”](#).
- Schedule Log Delete: You can set the duration of log data.
- Schedule Maintenance: You can carry out periodic optimization of the SRDM database automatically. For more information, refer to [“Schedule Maintenance”](#).
- System Log: You can view and delete SRDM system logs and output them as XML-formatted files.
- Account Management: You can create, edit and delete accounts and roles, and cancel account locks. In addition, you can view account-related operation logs. For more information, refer to [“Account Management”](#).
- Properties: Allows you to edit the properties of logged-in accounts.

## BASIC SRDM OPERATIONS (CONTINUED)

---

### [Help] button

When you click the [Help] button, a menu will appear asking you to choose from Operation Guide (this document), Read Me and About. SRDM version information can be viewed by clicking on "About".



To view the Operation Guide in PDF format, Adobe® Reader® or Acrobat® Reader® from Adobe Systems incorporated is required. Adobe® Reader® can be downloaded from "<http://www.adobe.com/>"

### [Logout] button

Click to log out from SRDM when you are ready to log out.

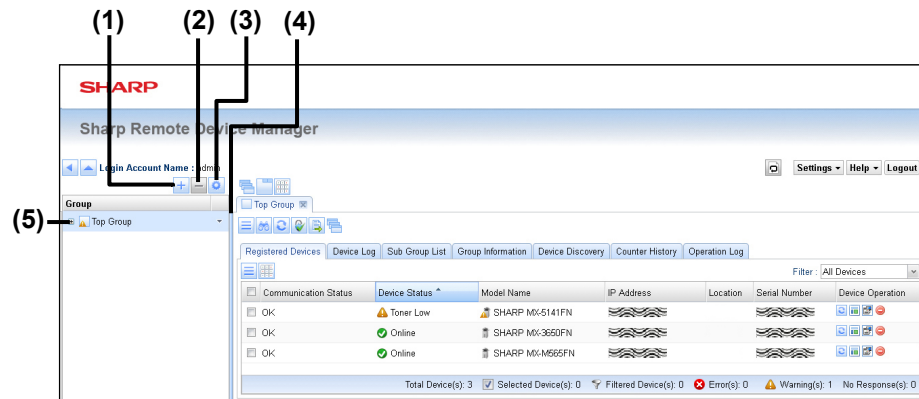
### [Device/System] tabs

[Device/System] tabs display device information or group information depending on the selected tab.

# GROUP PANE

The Group pane is the area displayed on the left side of the window. The group structure is displayed in a tree format in the Group pane. Furthermore, it contains buttons which can be used to create groups, delete groups and edit group settings.

The width of the Group pane can be changed by dragging the vertical slide bar and it can be minimized and restored by clicking on it.



## (5) Group Tree

The group structure is displayed in a tree format.

### (1) [Create Group] button “+”

Click to create a new group or device group. If any device group is selected, this button will be disabled.

### (2) [Delete Group] button “-”

Click to delete the group that is selected. If “Top Group” is selected, this button will be disabled.

### (3) [Group Settings] button “⚙️”

Depending on the selected group type, this button displays options to edit the settings.

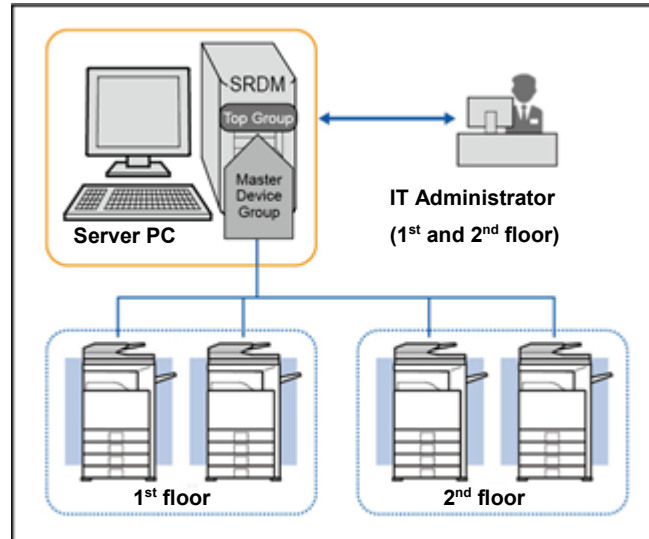
### (4) Slide bar

Click to minimize or restore the group pane. The width of the group pane can be changed by dragging the slide bar.

# GROUP CONCEPT

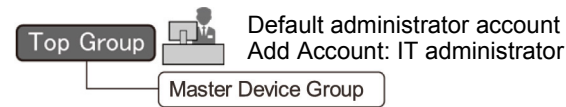
SRDM allows you to perform device management efficiently and safely by grouping devices. The following scenarios explain grouping of devices based on their location, etc.

## Customer's office

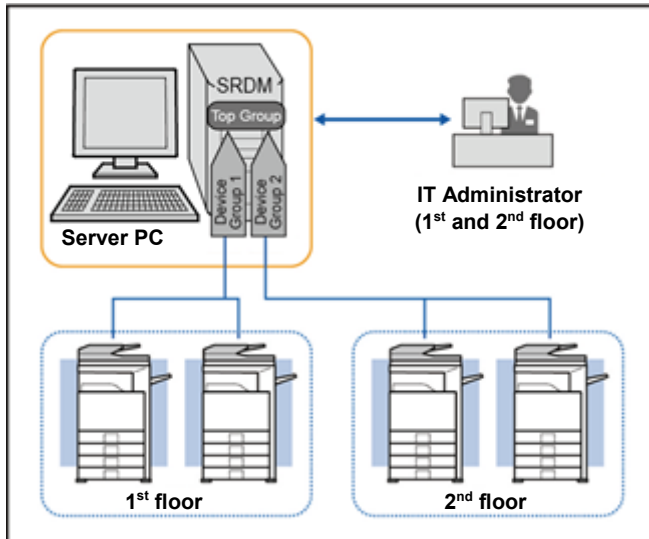


This is the most basic configuration. In this example, one IT administrator manages all the devices in the office as one group.

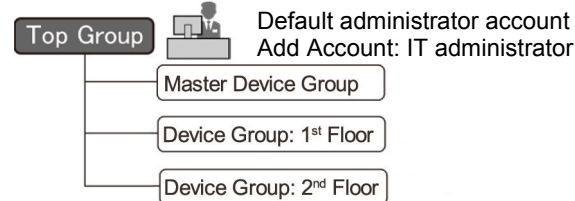
### Group pane image



## Customer's office



### Group pane image



### Configuration method

Register managed devices in each device group.



# GROUP MANAGEMENT

## Creating groups

You can use “Create Group” option to group and manage devices and also to combine device groups for management.

### ■ Groups

There are two types of group in SRDM.

Type	Purpose
Group 	Devices to be managed are divided into groups based on elements such as their location, attributes and departments.
Device group 	Groups of devices within the SRDM server network which have been discovered and registered.

### ■ Default groups

Default groups “Top Group” and “Master Device Group” are created automatically when you install SRDM. The “Master Device Group” is a sub group of the “Top Group”. You can create groups and device groups under this default “Top Group”.

- Top Group: This is the default group which can be used to manage all the other groups created by users and also the devices discovered in SRDM.
- Master Device Group: This group can be used to discover and manage all the devices which are available in the network where SRDM Server is installed.

### ■ Creating groups

Groups can be created by the following steps.

1. In the Group pane, click the “+” button next to the main group to create a sub group.

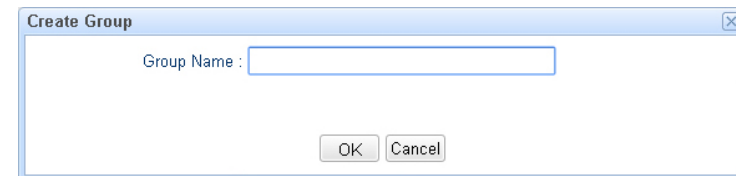
2. Click [Create] and then select [Group].



You can also create a group by clicking on the main group, clicking the [Create] button “+” and then selecting [Group].

3. Enter the group name and click the [OK] button.

The group name can include up to 64 alphanumeric characters (except \, /, :, \*, ?, “, <, > or |). A blank group name or a name consisting of only spaces is forbidden.



# GROUP MANAGEMENT

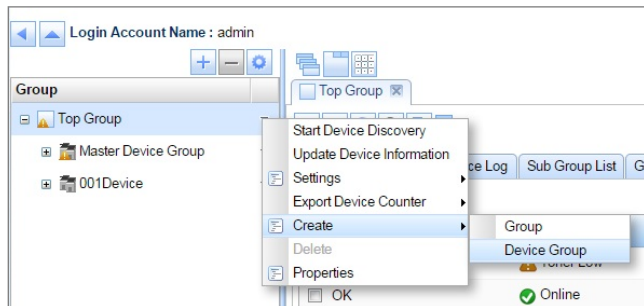
## ■ Creating device groups

Registered devices can be grouped. The following functionalities are available for the individual device groups:

- Search and register devices
- Update device status
- Download counter data and more

You can group devices by the following procedure.

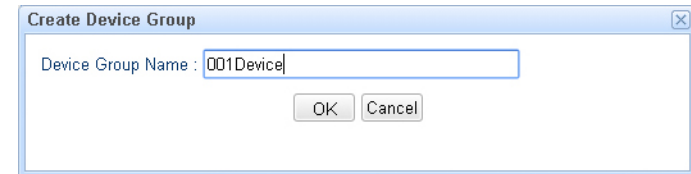
1. In the Group pane, click the “▼” button next to the main group where the new device group is to be created.
2. Click [Create] and select [Device Group].



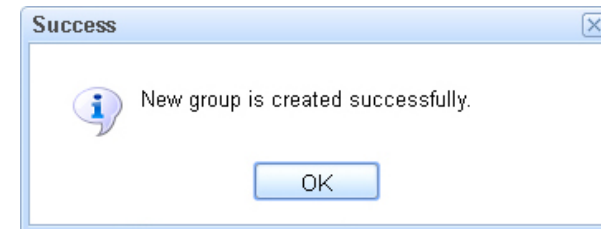
You can also create a device group by clicking on the main group, clicking the [Create] button “+” and then selecting [Device Group].

3. Enter the device group name and click the [OK] button.

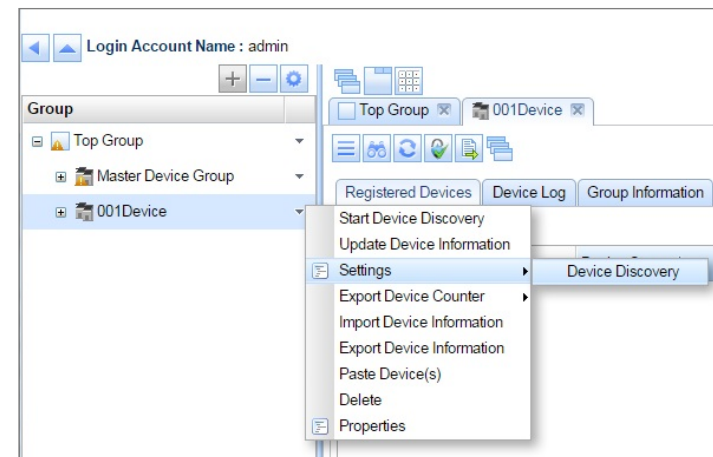
The group name can include up to 64 alphanumeric characters (except \, /, :, \*, ?, “, <, > or |). A blank group name or a name consisting of only spaces is forbidden.



4. Click the [OK] button on the Group Created dialog box.



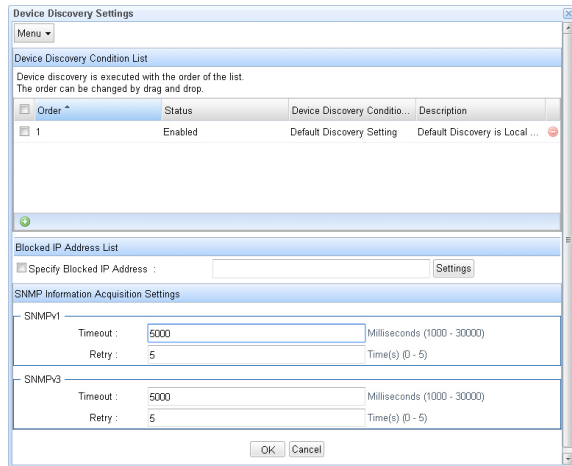
5. In the Group pane, click the “▼” button next to the newly created device group.
6. Click [Settings] and select [Device Discovery].



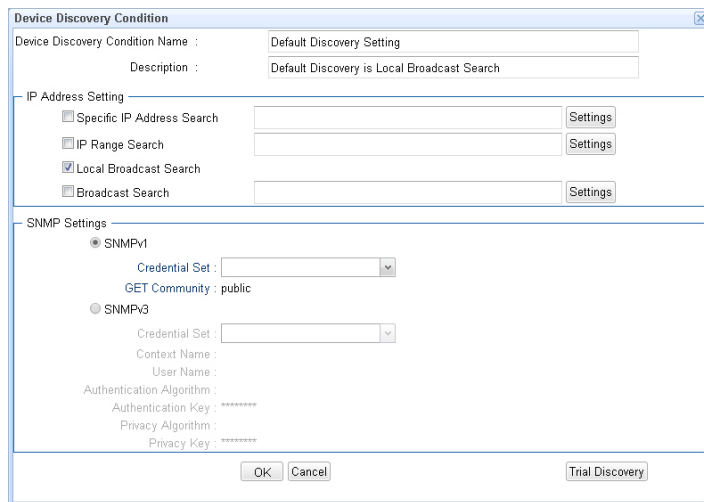


# GROUP MANAGEMENT

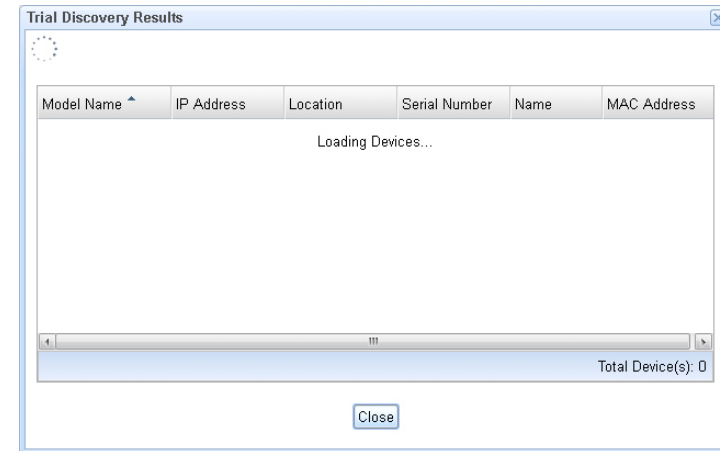
7. If you would like to apply custom device discovery settings, in the Device Discovery Condition List, click [Order 1, Default Discovery Setting] and modify the values accordingly.



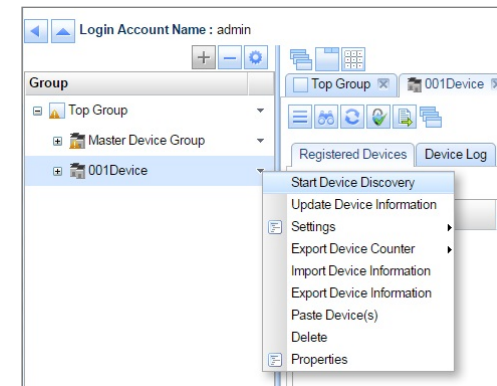
8. Set the device search conditions on the Device Discovery Condition Settings and click [OK].



9. You can test discovery settings by clicking the [Trial Discovery] button.



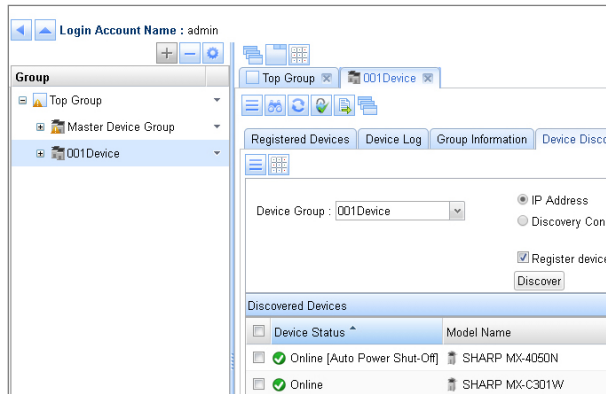
10. In the Group pane, click [Start Device Discovery] from the device group menu.



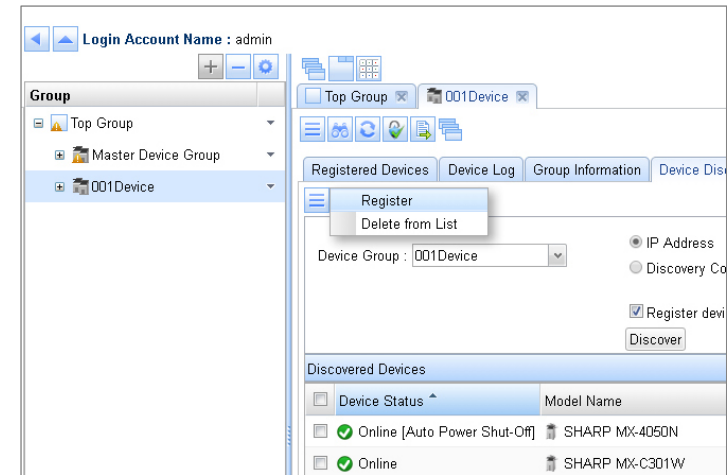
# GROUP MANAGEMENT

## 11. A list of new devices is displayed.

The devices found by the discovery are displayed in the [Device Discovery] tab.



Place the check mark next to the desired devices and select [Register] from the menu. The registered devices will be displayed in the [Registered Devices] tab.



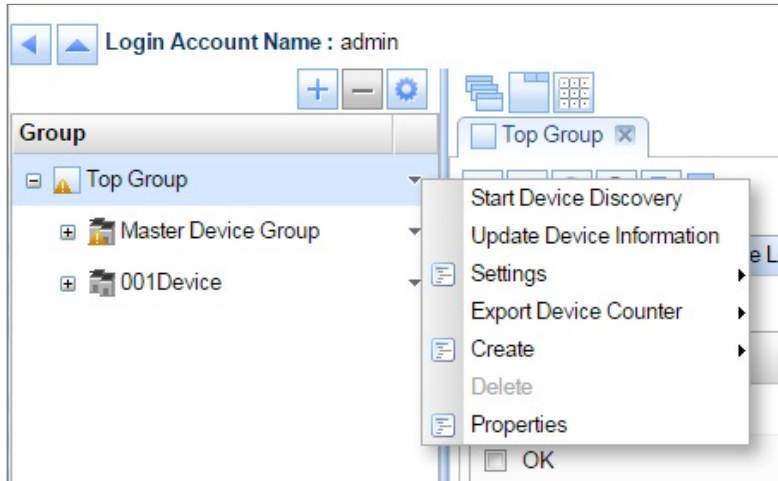
You can discover and register the devices by clicking the [Discover] button in the [Device Discovery] tab. For more information, refer to "[Device Discovery](#)".

# GROUP MANAGEMENT

## Group Menu Items

If you click on a [Group] tab menu “☰” which is just below the [Group] tab, depending on the selected group type various menu items will be displayed as described below.

### ■ Menu items for groups



- **Start Device Discovery:** Starts device discovery operation based on discovery configurations available in all device groups under this selected group. For more information about discovery configuration and discovery feature refer to [“Device Discovery”](#).
- **Update Device Information:** Click to start updating information for all devices belonging to the group.

- **Settings:** This allows you to configure the status settings and also you can view the available filter list.

Using “Status Settings”, you can change the display conditions for status icons. For more information, refer to [“Changing the conditions for icon display”](#).

Filter List screen allows you to view, create and edit the filters. For more information, refer to [“Creating filters”](#).

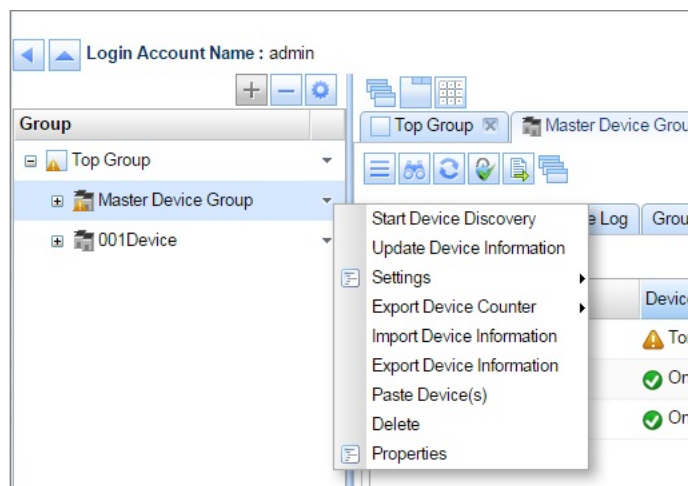
- **Export Device Counter:** You can save/export the counter data of all the devices in the group as an XML file.
- **Create:** Click to make a new authority group or device group. For more information, refer to [“Creating groups”](#).
- **Delete:** Click to delete a group that is selected. For more information, refer to [“Deleting groups”](#)

Note: If "Top Group" is selected; this option will be disabled.

- **Properties:** Click to edit the group name.

# GROUP MANAGEMENT

## ■ Menu items for device groups



- **Start Device Discovery:** Starts device discovery operation based on discovery configuration. For more information about discovery configuration and discovery feature refer to "[Device Discovery](#)"
- **Update Device Information:** Click to start updating information for all devices belonging to the group.
- **Settings:** This allows you to configure the below items
  - **Device Discovery:** You can configure discovery condition. For more information, refer to "[Device Discovery](#)"

- **Export Device Counter:** You can export the counter data of all devices in the group as an XML file
- **Import Device Information:** Using this option, you can import the device information which is exported from a different SRDM instance as an xml format.
- **Export Device Information:** Using this option, you can export the device information as an xml format.
- **Paste Device(s):** This option allows you to copy the devices from other device group to this selected device group.
- **Delete:** Click to delete a group that is selected. For more information, refer to "[Deleting groups](#)".
- **Properties:** Click to edit the group name.

# GROUP MANAGEMENT

## Editing groups

You can edit group settings by following the procedure below.

1. In the Group pane, click the “✎” button for the group to be edited.
2. Click [Properties].
3. Edit the group name on the Properties dialog box.

## Deleting groups

You can delete groups by following any of the procedures below.

From Group Pane:

1. In the Group pane, click the “✎” button for the group you wish to delete.
2. Click [Delete].
3. Click the [Yes] button in the confirmation dialog box.

From Sub Group List:

1. In the [Sub Group List] tab of the Group, select the groups you wish to delete.
2. Click the [Sub Group List] tab menu “☰”.
3. Click [Delete].

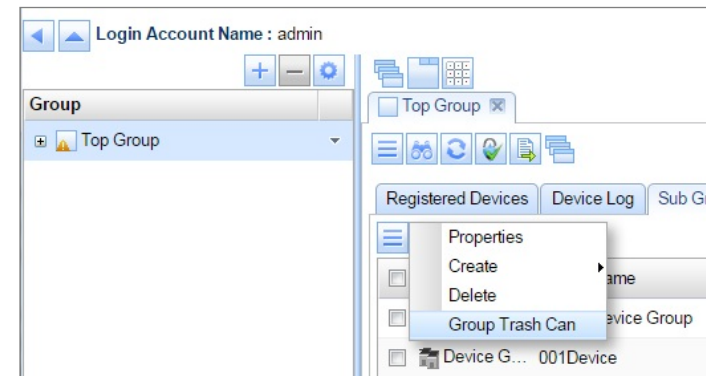


“Top Group” cannot be deleted.

## Restoring deleted groups

Groups which have been deleted are transferred to the Group Trash Can. You can restore a group that has been deleted, by following the procedure below.

1. Click on the [Sub Group List] tab of the currently-selected group.
2. Click the [Sub Group List] tab menu “☰”.
3. Click [Group Trash Can].
4. Select the group(s) to be restored and then click the [Restore] button.



You can permanently delete a group by deleting it from the Group Trash Can. Note that groups which have been permanently deleted cannot be restored.

# ACCOUNT MANAGEMENT

When using SRDM, an account is required in order to log into the SRDM server. In SRDM, a variety of different permissions are assigned to each account, and this allows you to manage accounts so that depending on the purpose of an account, only the functions which are applicable to that account can be used. Accounts which have account management permissions can be accessed from the "SRDM (Account Management)" page, and they can be used to carry out account management functions.

## Accounts and roles

Users of SRDM can utilize the accounts which have been assigned to them in order to log into the SRDM server and to utilize the functions of SRDM. Accounts always have one set of permissions corresponding to the purpose of the account. In SRDM, this "set of permissions" is referred to as a "role". Roles which do not have any permissions are viewing roles. Accounts which have viewing roles can only use viewing functions.

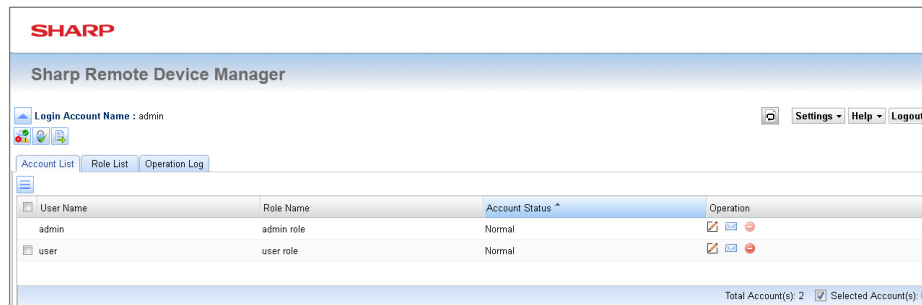
## Default accounts and default roles

SRDM has two default types of account and two default types of role available. The default accounts and default roles are as follows.

Account name	Role name	Purpose
admin	admin role	Administrator account with an administrator role
user	user role	Viewing user account with a viewing role

## Account Management

[Account List] tab

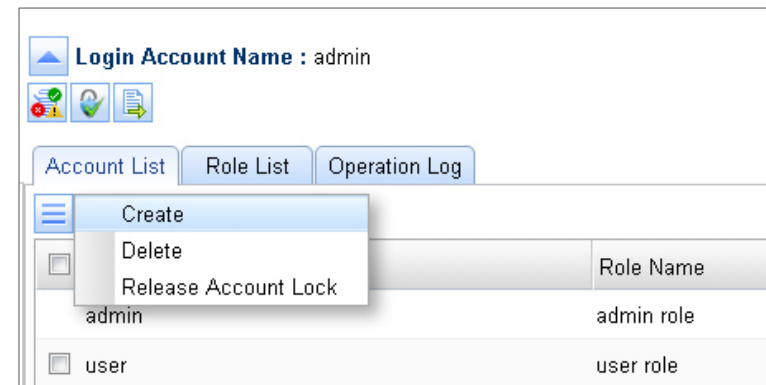


You can use the [Account List] tab to carry out tasks such as creating, editing and deleting accounts and unlocking locked accounts.

## Creating accounts

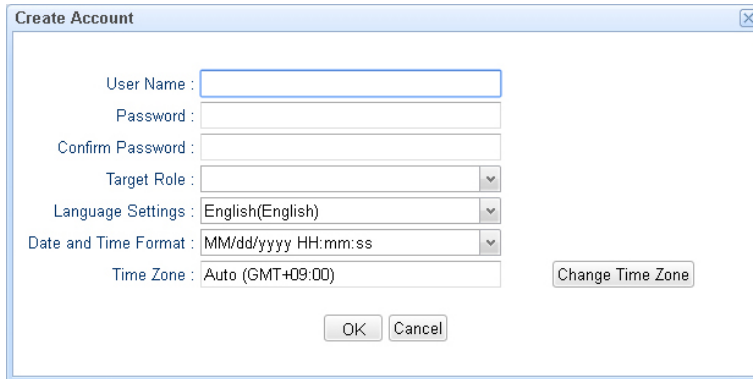
You can create a new account by following the procedure below.

1. Click the menu button "☰", and then select [Create].



# ACCOUNT MANAGEMENT

## 2. Enter the necessary details.



The 'Create Account' dialog box contains the following fields and controls:

- User Name:
- Password:
- Confirm Password:
- Target Role:
- Language Settings:
- Date and Time Format:
- Time Zone:
- 

User Name: The name of this account

Password: The password to be used for logging into SRDM using this account

Target role: The role needed for this account

Language Setting: The language setting to use for this account

Date And Time Format: The format for the date and time to be used for this account

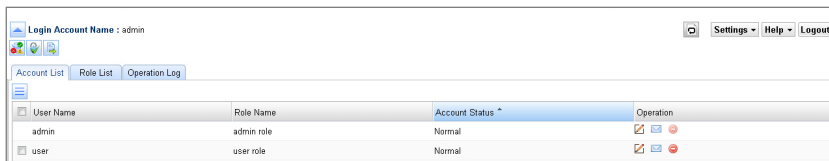
Time Zone: The time zone to be used for this account

## 3. Click the [OK] button.

## Editing accounts

You can edit accounts which have already been created by following the procedure below.

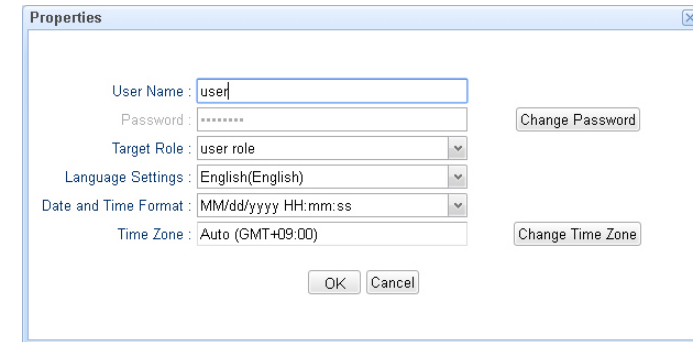
### 1. Click the account edit button " ".



User Name	Role Name	Account Status	Operation
admin	admin role	Normal	
user	user role	Normal	

## 2. Edit the details, and then click the [OK] button.

Note: You cannot change the user name or role of an account which is currently logged in.



The 'Properties' dialog box contains the following fields and controls:

- User Name:
- Password:
- Target Role:
- Language Settings:
- Date and Time Format:
- Time Zone:
- 

## Deleting accounts

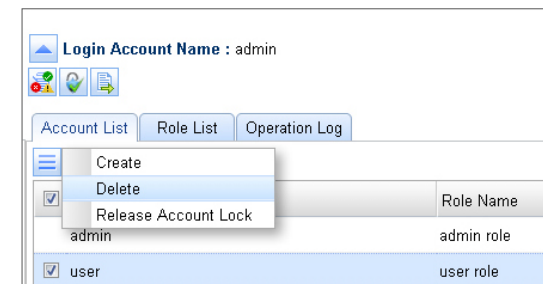
You can delete accounts which have already been created by following either of the procedures below.

### ■ Deleting from the menu button " ":

#### 1. Select the check box of the account to be deleted.

Note: You can delete multiple accounts at the same time by selecting more than one check box. However, you cannot select or delete accounts which are currently logged in.

#### 2. Click the menu button " ", and then select [Delete].



User Name	Role Name
admin	admin role
user	user role

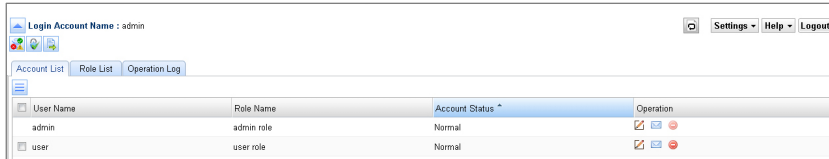
Context menu options: Create, Delete, Release Account Lock

#### 3. Click the [Yes] button in the confirmation dialog box.

# ACCOUNT MANAGEMENT

## ■ Deleting using the delete button "🗑️":

1. Click the delete button "🗑️" of the account to be deleted.

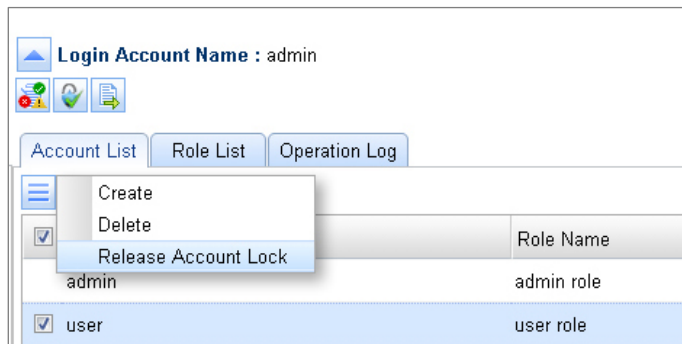


2. Click the [Yes] button in the confirmation dialog box.  
Note: When deleting using the delete button, you cannot delete multiple accounts at the same time.

## Unlocking accounts

If you make an error logging into the same account five times in a row, the account will be temporarily locked, and logging into that account will not be possible for 30 minutes. This is called "account locking". When an account has been locked, "Account status" in the [Account List] tab shows "Locked". You can unlock an account by following the procedure below.

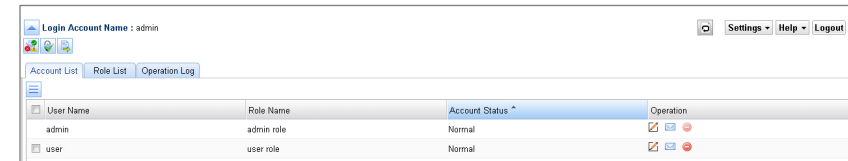
1. Select the check box of the account to be unlocked.  
Note: You can unlock multiple accounts at the same time by selecting more than one check box.
2. Click the menu button "☰" and select [Unlock Account].



## Account information notifications via e-mail

You can send an e-mail messages containing information on accounts which have already been created to users that you specify by following the procedure below.

1. Click the e-mail notification button "✉️" of the account to send information for.



2. Enter the required information.

The screenshot shows a dialog box titled 'E-mail Notification'. It has fields for 'To:', 'Cc:', and 'Bcc:'. The 'Subject:' field is pre-filled with '[SRDM] Account Information'. Below these fields is a 'Body:' section with a text area containing the following text:  
Login Page URL(s):  
HTTP URL : http://\*\*\*\*\*:8085/WebUI/  
HTTPS URL : https://\*\*\*\*\*:8086/WebUI/  
User Name : admin  
Password :  
Contact :  
At the bottom of the dialog box are 'OK' and 'Cancel' buttons.

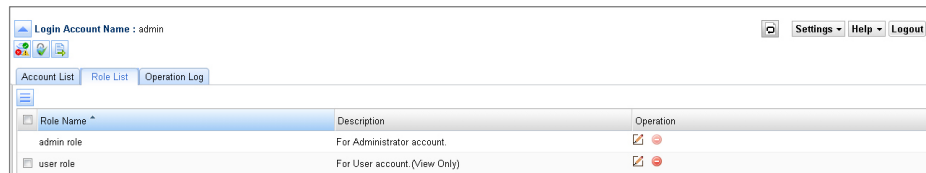
To: E-mail address send the e-mail to  
Cc: E-mail address to send a copy of the e-mail to  
Bcc: E-mail address to send a blind copy of the e-mail to  
Subject: Subject of the e-mail  
Body: Main body text of the e-mail message. The password and contact are blank by default, so you should edit them as necessary.

3. Click the [OK] button.



# ACCOUNT MANAGEMENT

## [Role List] tab

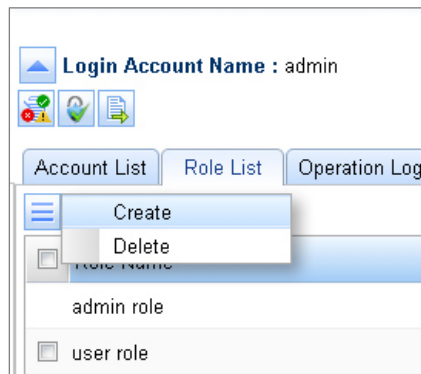


You can use the [Role List] tab to create, edit and delete roles.

## Creating roles

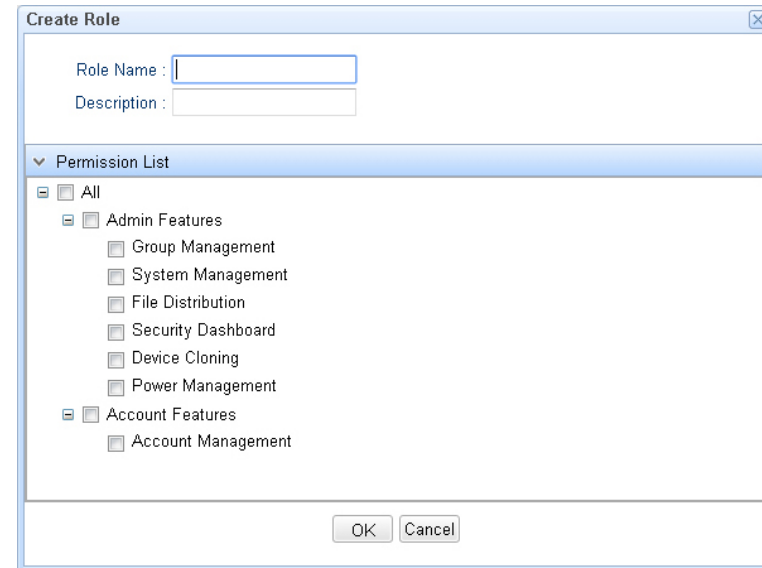
You can create new roles by following the procedure below.

1. Click the menu button "☰", and then select [Create].



2. Enter the role name and description, and then click the check boxes to select the permissions to assign to that role.

Note: For details on permissions, refer to "[Permission details](#)".

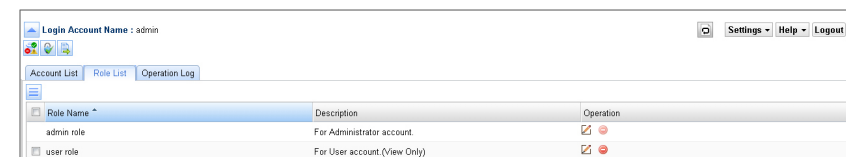


3. Click the [OK] button.  
Note: If you click the [Yes] button in the confirmation dialog box which is displayed, you can then create a new account. For details on creating new accounts, refer to "[Creating accounts](#)".

## Editing roles

You can edit roles which have already been created by following the procedure below.

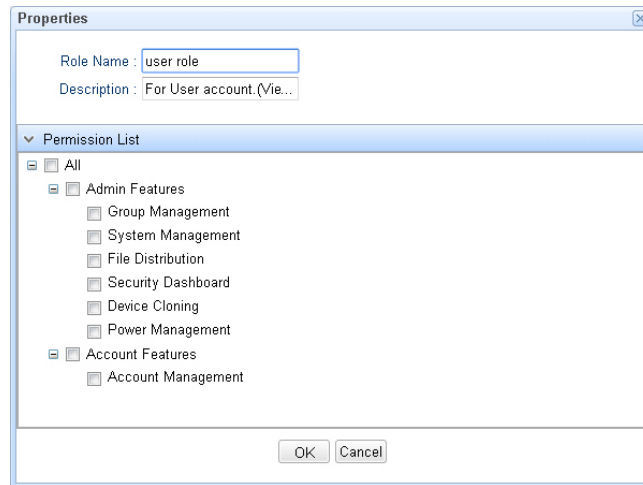
1. Click the account editing button "✎".



# ACCOUNT MANAGEMENT

2. Edit the items, and then click the [OK] button.

Note: You cannot change the role of an account which is currently logged in.



## Deleting roles

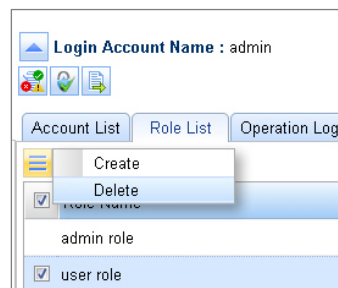
You can delete roles which have already been created by following either of the procedures below.

### ■ Deleting from the menu button "☰":

1. Select the check box of the role to be deleted.

Note: You can delete multiple roles at the same time by selecting more than one check box.

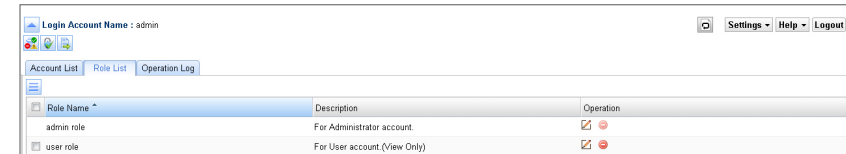
2. Click the menu button "☰", and then select [Delete].



3. Click the [Yes] button in the confirmation dialog box.


### ■ Deleting using the delete button "⊖":

1. Click the delete button "⊖" of the role to be deleted.

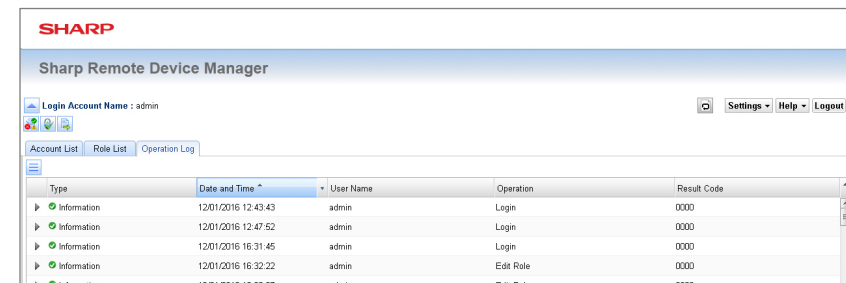


2. Click the [Yes] button in the confirmation dialog box.

Note: When deleting using the delete button, you cannot delete multiple roles at the same time.

 If you delete a role which is currently assigned to an account, the corresponding account will no longer have any role assigned to it, and will become a viewing account only.

## [Operation log] tab

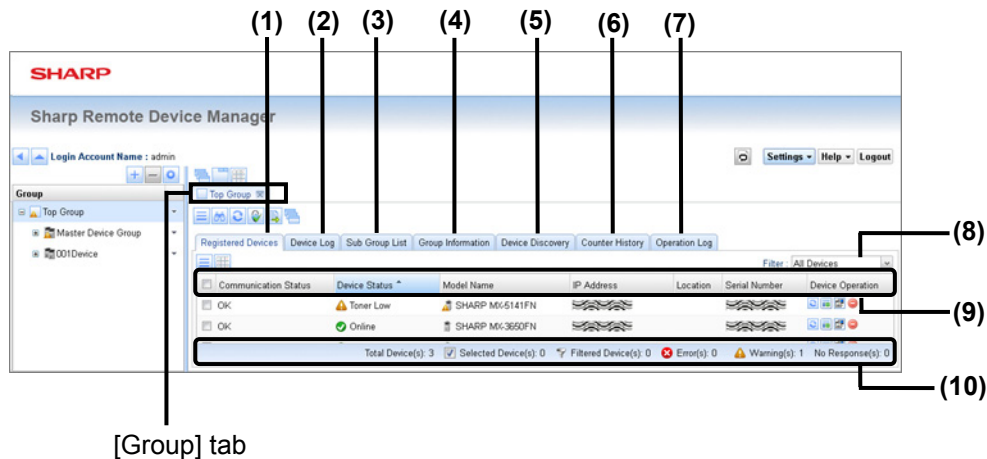


You can use the [Operation log] tab for tasks such as checking operation logs for account-related operations such as creating, editing and deleting accounts and roles, and unlocking accounts, and also for exporting files in XML format.

# DEVICE/SYSTEM TAB

If you click on a group in the group tree, a [Group] tab will be displayed.

The device/system tabs are displayed in the [Device/System] tab area. To perform operations like device discovery, refer to “[DEVICE MANAGEMENT](#)”.



[Group] tab

## (1) [Registered Devices] tab

Devices that belong to the group selected in group pane are displayed.

## (2) [Device Log] tab

Logs of all devices that belong to the group are displayed in the tab.

## (3) [Sub Group List] tab

If the group has sub-groups, the sub-groups are displayed in the tab.

## (4) [Group Information] tab

This displays summary of all the devices information belong to the group.

## (5) [Device Discovery] tab

This displays new devices that have been found during device discovery operation. Furthermore, you can specify the search conditions and execute the device discovery on this tab.

## (6) [Counter History] tab

This displays a counter history graph of all the devices together for each group.

## (7) [Operation Log] tab

This shows the operation logs for all devices belonging to the group.

## (8) Filter box

This lets you use and create filters to display devices based on the defined criteria in the selected filter.

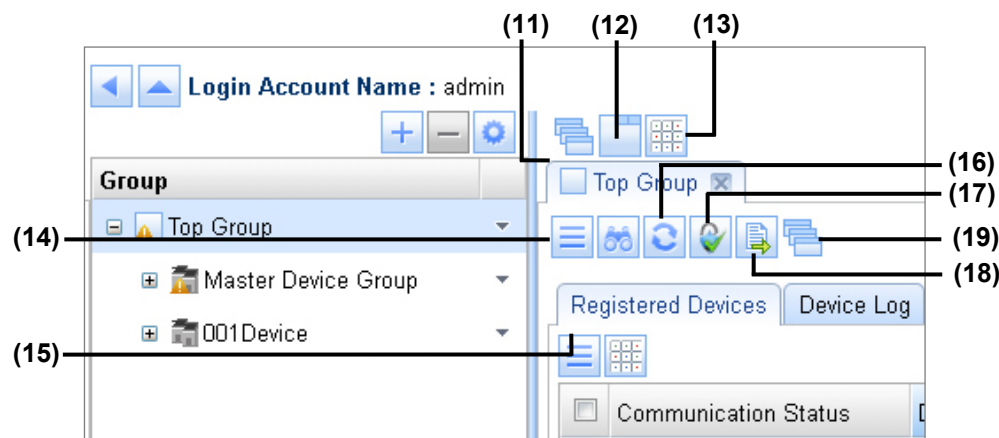
## (9) Column header

You can click on column header to sort the items in the device list in ascending or descending order. By right-clicking on a column header, you can carry out operations such as selecting the columns to be displayed, setting the sorting method and using simple filters.

## (10) Status bar

This displays information such as the total number of devices, the number of selected devices, and number of filtered devices and so on.

# DEVICE/SYSTEM TAB



## (11) [Window view] button “ This button lets you switch the group display to window display. (Refer to “[Display Option buttons](#)”.)

## (12) [Tab view] button “ This button lets you switch the group display to tab display. (Refer to “[Display Option buttons](#)”.)

## (13) [Tile view] button “ This button lets you switch the group display to tile display. (Refer to “[Display Option buttons](#)”.)

## (14) [Group] tab menu “ Click to display the [Group] tab menu. Available menu items differ based on the selected group type. (Refer to “[Group menu items](#)”)

## (15) [Device Discovery] buttons “ Click to start or stop the search for devices.

## (16) [Device Information Update] buttons “ Click to start or stop the updating of information for all devices belonging to the group.

## (17) [SRDM (Advanced Features)] button “ Open the SRDM (Advanced Features) window. You can use security setting management functions, power management functions and cloning functions in the “Advanced Features” window. For more information about the advanced features, refer to “[ADVANCED FEATURES](#)”.

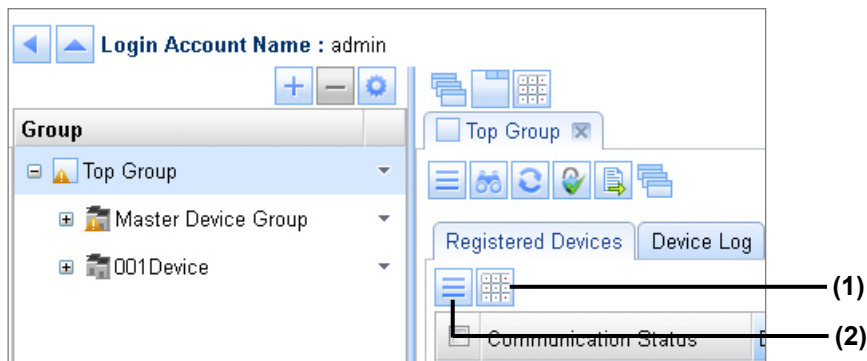
## (18) [SRDM (File Distribution)] button “ Open the SRDM (File Distribution) window. The “file distribution” feature allows you to share files such as MFP drivers with other SRDM users as a ZIP file. For more information about the advanced features, refer to “[FILE DISTRIBUTION FEATURE](#)”

## (19) [Switch To Window] button “ This button lets you switch the group/device tab which is currently displayed to window view display.

# DEVICE/SYSTEM TAB

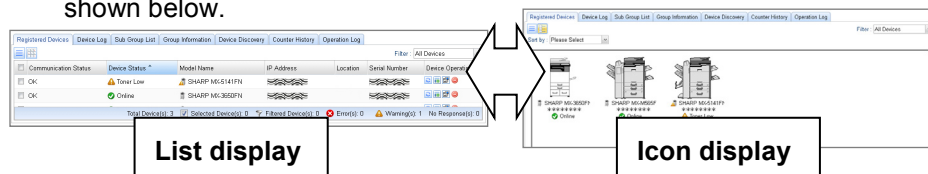
## [Registered Devices] tab

If you click on the [Registered Devices] tab, registered devices will be displayed in a list.



### (1) [Toggle Display] button “”

This button lets you switch between list display and icon display as shown below.



### [Registered Devices] tab menu “”




If you click on the [Registered Devices] tab menu, the following menu items will be displayed.

- Update Device Information: Updates the information for all/selected devices by fetching latest information from the devices




- Delete Device: Removes the selected devices from the list and moves them to the Device Trash Can. This also removes the devices from device search conditions based on selection.
- Device Trash Can: Opens the Device Trash Can window with list of deleted devices.

## ■ Status Description





Device information which is displayed in gray indicates devices which are not responding for communication.

- “” icon: Indicates that the status is normal.
- “” icon: Indicates that a warning status exists.
- “” icon: Indicates that an error status exists.

## ■ Icons displayed in front of model names

Icons such as “” are device status icons which are displayed at the bottom-left of the device name. If the status is normal like online, only the device icon “” is displayed without any error or warning status. In addition, devices with a lock icon such as “” displayed at the bottom-right are Data Security Kit (DSK) models.

## ■ Device operation

- “” button: Updates the device status
- “” button: Opens the device web page
- “” button: Opens the device remote operation panel
- “” button: Removes the device from the list and move it to Device Trash Can.

## DEVICE/SYSTEM TAB

---



If the “Communication Error(XXXX)” is appeared in the “Communication Status” column, some error might be occurred for communication between the SRDM and the device. For more information, refer to “[TROUBLESHOOTING](#)”.

## [Device Log] tab

The status logs for all registered devices to the group are displayed in the [Device Log] tab.

Date and Time	Communication S...	Device Status	Model Name	IP Address	Location	Serial Number	Name
12/15/2016 14:07:22	OK	Online	SHARP MX-360FN				
12/15/2016 14:07:20	OK	Online	SHARP MX-M565FN				MX-M565FN
12/15/2016 14:07:17	OK	Toner Low	SHARP MX-S141FN				
12/07/2016 10:23:59	OK	Paper Empty	SHARP MX-360FN				
12/07/2016 10:23:57	OK	Online	SHARP MX-M565FN				MX-M565FN

The device log contains information of all the devices available in the group such as communication status, device status, model name, IP address, serial number, name and location. Whenever updating of information is performed, a new entry will be created for each device.

The device log can be exported as a XML file.

### ■ [Device Log] tab menu “ If you click on the [Device Log] tab menu “ 1. XML File Output: Exports/saves all the device log data as an xml file. 2. Delete All Device Logs: Deletes all the device log data.



Note that the deleted log data cannot be restored.

## [Sub Group List] tab

The information about the sub groups which are created under the selected group is available in Sub Group List. The available information includes group types, group names and group paths.

Group Type	Group Name	Group Path	Settings
Device Group	Master Device Group	Top Group	Settings
Device Group	001Device	Top Group	Settings

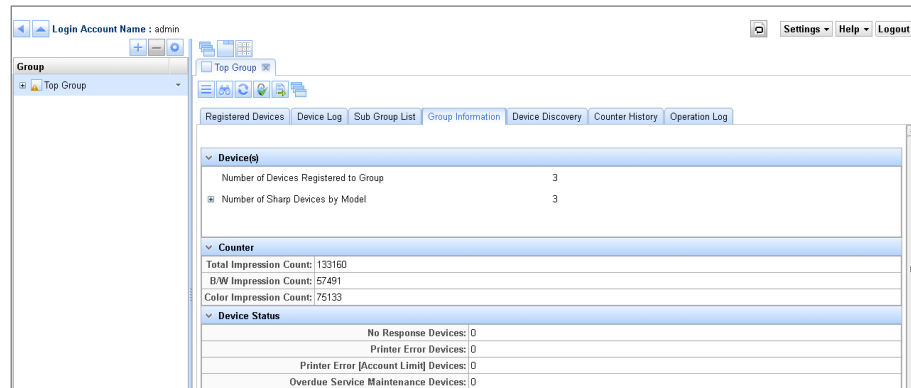
The [Settings] button for device groups allows you to edit device discovery settings and rename the group.

### ■ [Sub Group List] tab menu “ If you click on the [Sub Group List] tab menu “ - Create (Group, Device Group): You can create device groups under the selected group. - Delete: Deletes the selected group. - Group Trash Can: Displays list of the groups under the selected group which were deleted before. - Properties: You can edit the group name.

# DEVICE/SYSTEM TAB

## [Group Information] tab

Information such as total counter information, number of devices by model and number of devices by device status and number of devices by service code is displayed in the [Group Information] tab.



### – Information displayed in [Group Information] tab

The following information is displayed in the [Group Information] tab.

- Number of devices in the group
  - Number Of Devices Registered To Group
  - Number Of Sharp Devices By Model
- Total counter data of all devices in the group
  - Total Impression Count
  - B/W Impression Count
  - Color Impression Count

- Number of devices having same device status

- Communication Error Devices
- Printer Error Devices
- Printer Error [Account Limit] Devices
- Overdue Service Maintenance Devices
- Paper Jam Devices
- Marker Supply Missing Devices
- Toner Empty Devices
- Paper Empty Devices
- Offline Status Devices
- Printer Warning Devices
- Toner Low Devices
- Paper Low Devices
- “Near to Overdue Service Maintenance” Warning Devices
- Online [Auto Power Shut-Off] Devices
- Warm Up Devices
- Online Status Devices



## DEVICE/SYSTEM TAB

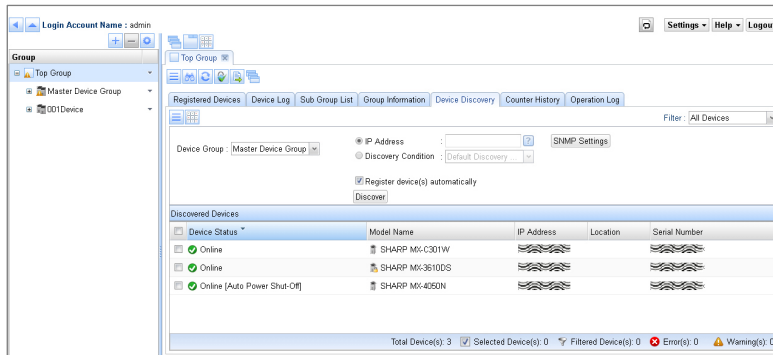
---

- Number of devices having same service code
  - Number of devices having “TA” service code
  - Number of devices having “CA” service code
  - Number of devices having “AA” service code
  - Number of devices having “TK1” service code
  - Number of devices having “TK2” service code
  - Number of devices having “FK1” service code
  - Number of devices having “FK2” service code
  - Number of devices having “FK3” service code
  - Number of devices having error codes

# DEVICE/SYSTEM TAB

## [Device Discovery] tab


Devices which are found during device discovery (refer to “[Device Discovery](#)”) are displayed in the [Device Discovery] tab.



To manage the devices, you need to register the discovered devices. After registration the devices will be moved to [Registered Devices] tab.

- In order to manage the devices which have been found during device discovery, you must register the devices.
- If you use the [Discover] button to discover the devices, registering devices depends on the state of the “Register device(s) automatically” check box. For more information, refer to “[Device Discovery](#)”.

### ■ [Device Discovery] tab menu “”

If you click on the [Device Discovery] tab menu “”, the following menu will be displayed.

1. Register: Registers the selected discovered devices. After registration these devices will be moved to the [Registered Devices] tab.
2. Delete From List: Deletes the discovered devices from the list.

## [Counter History] tab

The [Counter History] tab allows you to view the total counter history of all devices registered to the group in a graphical format.

You can select time period from the drop down menu. Using the check boxes on the upper right of the graph allows you to select the counter types.

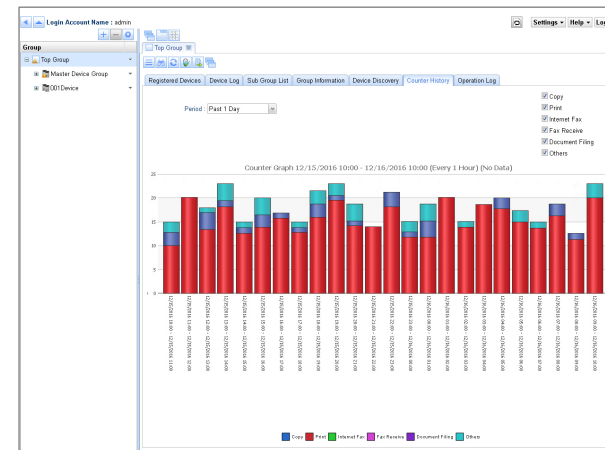
Following is a list of the available options.

Period:

- Past 1 Day , Past 1 Month, Past 1 Year

Counter Types:

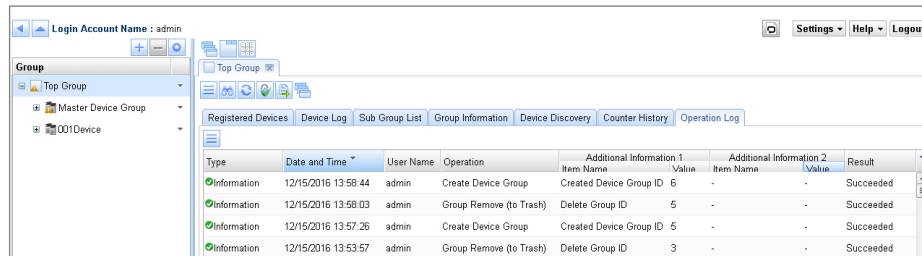
- Copy, Print, Internet Fax, Fax Receive, Document Filing, Others



- This graph is created by using the data that has been acquired according to the Scheduled Action > Device Information Update. In order to capture counter data, Scheduled Action needs to be enabled. For more information, refer to “[Setting scheduled actions](#)”.
- If the acquisition of data was not performed during a particular interval, "No Data" will be displayed in the graph for that particular interval.
- In order to display this graph, "Schedule Log Delete" must be set to a setting other than "Latest one Log".


## [Operation Log] tab

The operation log contains all SRDM system operation logs performed in this group. The log information includes who logged on and what options are changed, what operations are performed. The log information also displays the result of the operation and the time of the event.



Type	Date and Time	User Name	Operation	Additional Information 1 Item Name	Additional Information 2 Item Name	Result
Information	12/15/2016 13:58:44	admin	Create Device Group	Created Device Group ID 6	-	Succeeded
Information	12/15/2016 13:58:03	admin	Group Remove (to Trash)	Delete Group ID 5	-	Succeeded
Information	12/15/2016 13:57:26	admin	Create Device Group	Created Device Group ID 5	-	Succeeded
Information	12/15/2016 13:53:57	admin	Group Remove (to Trash)	Delete Group ID 3	-	Succeeded

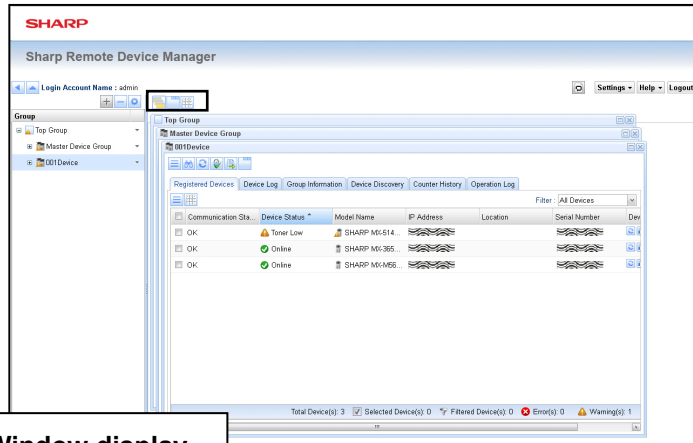

### ■ [Operation Log] tab menu “”

If you click on the [Operation log] tab menu “”, the following menu will be displayed.

1. XML File Output: Exports/saves all the SRDM operations log data as an xml file.
2. Delete All Operation Logs: Deletes all the log data.

# DEVICE/SYSTEM TAB

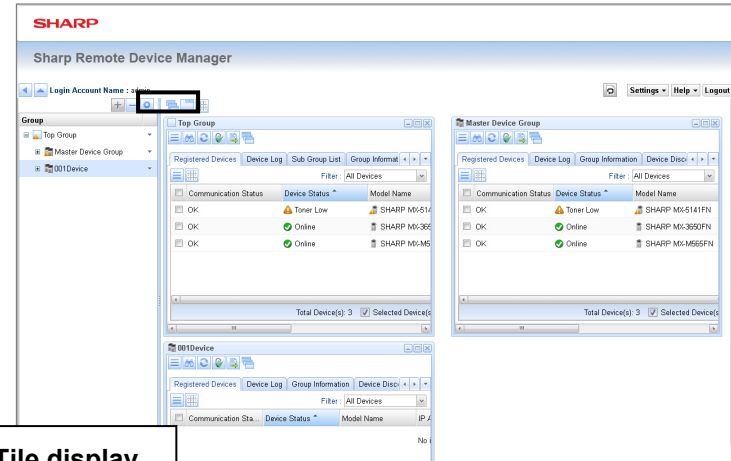
## [Display Option] buttons

You can switch the group display option to windows, tabs, and tile display by clicking on the display option buttons “Switch To Window 

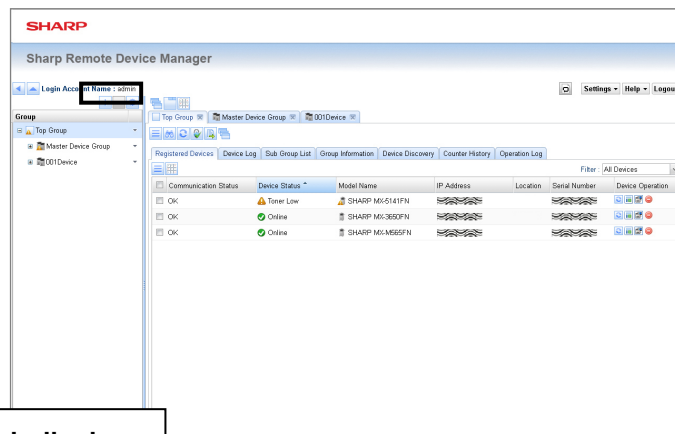
The screenshot shows the Sharp Remote Device Manager interface with the 'Window display' mode selected. The main content area displays a table of registered devices. A callout box highlights the 'Switch To Window' button in the top toolbar.

Communication Sta.	Device Status	Model Name	IP Address	Location	Serial Number	Dev
OK	Toner Low	SHARP MX-514				
OK	Online	SHARP MX-365				
OK	Online	SHARP MX-M56				

Window display



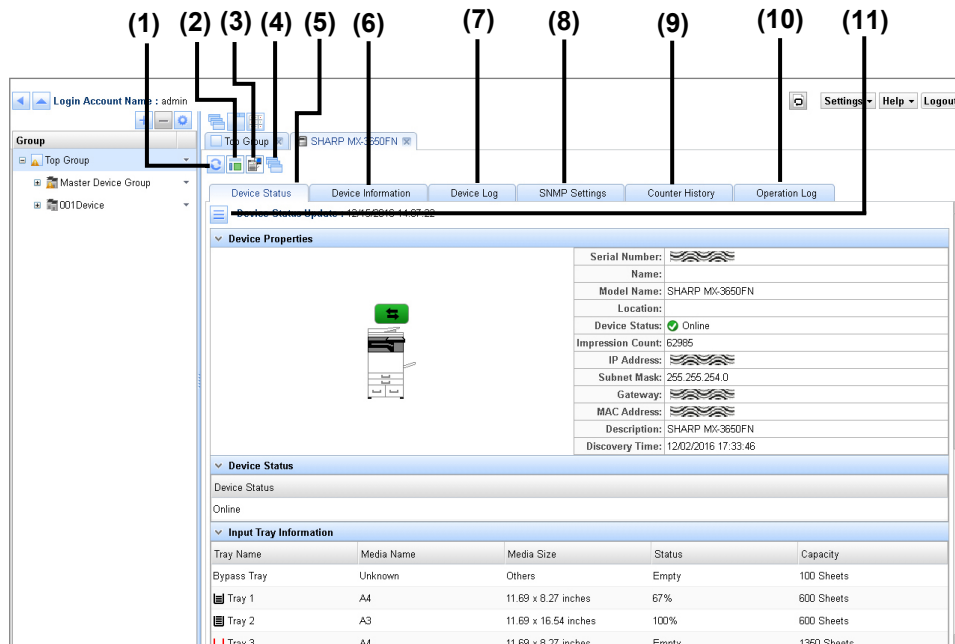
Tile display



Tab display

# DEVICE DETAILS

By clicking on a device in the registered devices list, a tab for the selected device will be opened. The device tab is displayed in the [Device/System] tab area. (Refer to “[BASIC SRDM OPERATIONS](#)”.)



- (1) **[Device Information Update] button “”**  
This updates the device information.
- (2) **[Device Web Page] button “”**  
This opens the device’s web page in a new browser tab.
- (3) **[Remote Operation] button “”**  
This opens a remote operation panel in a new window. For more information, refer to “[Accessing a device operation panel remotely](#)”.
- (4) **[Switch To Window] button “”**  
This button lets you switch the device tab to window display.
- (5) **[Device Status] tab**  
This displays detailed information relating to the device status, such as device properties, input tray information, toner information, error

codes and maintenance codes . For more information, refer to “[\[Device Details\] tab](#)”.

- (6) **[Device Information] tab**  
This displays detailed information about the device operating status and settings, such as number of pages printed by the device, number of pages transmitted by the device and print settings. For more information, refer to “[\[Device Information\] tab](#)”.
- (7) **[Device Log] tab**  
This displays the status log for the device. For more information, refer to “[\[Device Log\] tab](#)”.
- (8) **[SNMP Settings] tab**  
This displays the SNMP settings of the device. For more information, refer to “[\[SNMP Settings\] tab](#)”.
- (9) **[Counter History] tab**  
This displays counter history graph of the selected device. For more information, refer to “[\[Counter History\] tab](#)”.
- (10) **[Operation Log] tab**  
This displays the operation log for the device. For more information, refer to “[\[Operation Log\] tab](#)”.
- (11) **Tab Menu button “”**  
This displays the tab menu. For more information, refer to the respective details menus in the [Device Status tab](#), [Device Information\] tab](#), [\[SNMP Setting\] tab](#) and [\[Operation Log\] tab](#). Furthermore, this is not displayed when the [\[Counter History\] tab](#) is selected.

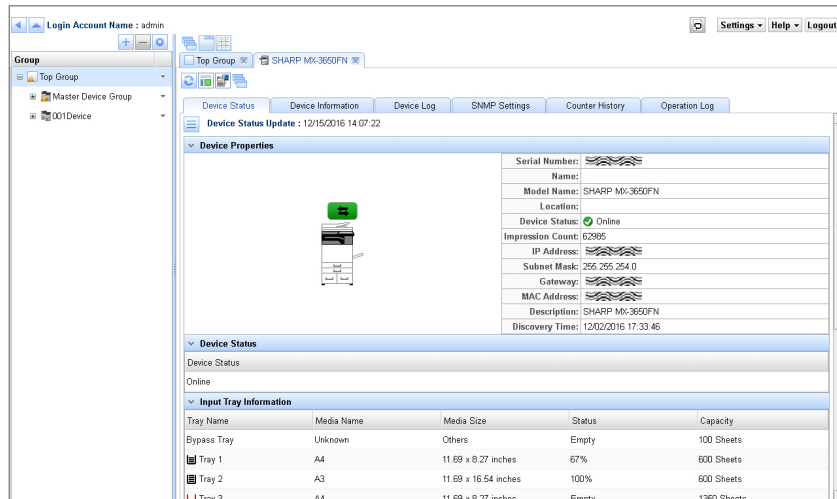


For more information, refer to further pages of this document.

# DEVICE DETAILS

## [Device Status] tab

In the [Device Status] tab, you can check detailed information relating to the device such as device properties and status, input tray status, toner status, error codes and maintenance codes.



### ■ Information displayed in [Device Status] tab

The following information is displayed for the selected device.

- Date and time of last communication received by SRDM from the device for tasks such as status updates or information updates.
- Device Properties: Device image, serial number, name, model name, location, device status, impression count, IP address, subnet mask, gateway, MAC address, description and discovery time.
- Device Status: All the current statuses of the device are displayed (Ex: Paper Jam, Toner Low, Overdue Service Maintenance).

- Input Tray Information: Status of all the available input trays and media information.
- Toner Status: Status of all the toners.
- Error Code: Error code if occurred in the device.
- Maintenance Code: Maintenance code if occurred in the device.



- If you would like to check the most up-to-date information, carry out a device information update.
- It may not be possible to obtain detailed information from devices from other manufacturers and older Sharp devices. If the corresponding information cannot be obtained, “#N/A” will be displayed.

### ■ [Device Status] tab menu “☰”

If you click on the [Device Status] tab menu “☰”, the following menu will be displayed.

- Device Web Page: Displays device web page in a separate browser window.
- Remote Operation: Displays device operation panel in a separate browser window.

# DEVICE DETAILS

## [Device Information] tab

You can use the [Device Information] tab to check detailed information about the device operating status and settings, such as number of pages printed by the device, number of pages transmitted by the device and print settings.

Device Usage (Output)			
	Total	Black-White	Color
Total	62499	13891	48598
Copy	3337	1635	1702
Prints	59119	12230	46889
Internet Fax Receive	0	#N/A	--
Fax Receive	6	6	--
Prints (Document Filing)	27	20	7
Others	0	0	0

Device Usage (Send)			
	Total	Black-White	Color
Total	0	0	0
Scan Send	0	#N/A	0
Internet Fax Send	0	#N/A	--
Fax Send	0	0	--
Scan to HDD	0	#N/A	0

Print Setting Information	
Settings	Value
Default Input Tray	Auto Select

### ■ Information displayed in [Device Information] tab

The following information is displayed in the [Device Information] tab.

- Device Information Update: The date and time when SRDM last accessed the device to carry out tasks such as discovery or information updating
- Device Usage (Output): Information for the print counter
- Device Usage (Send): Information for the page transmission counter
- Print Setting Information: List of default print settings

- If you would like to check the latest information, carry out a device information update.



- It may not be possible to obtain detailed information from devices from other manufacturers and older Sharp devices. If the corresponding information cannot be obtained, "#N/A" will be displayed.

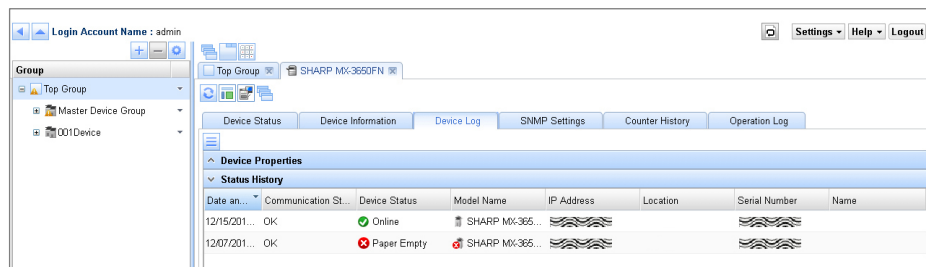
### ■ [Device Information] tab menu "☰"

If you click on the [Device Information] tab menu "☰", the following menu will be displayed.

- Device Information Update: Gets the latest information from the device.
- Device Web Page: Displays the web page for the device in a separate window.
- Remote Operation: Displays the operation panel for the device in a separate window.
- Export Device Counter: Saves the counter data for the device as an XML file.

## [Device Log] tab

The status log for the device is displayed in the [Device Log] tab.



### ■ [Device Log] tab menu “☰”

If you click on the [Device Log] tab menu “☰”, the following menu will be displayed.

- XML File Output: Exports/saves all the device log data as an xml file.
- Delete All Device Logs: Deletes all the device log data.

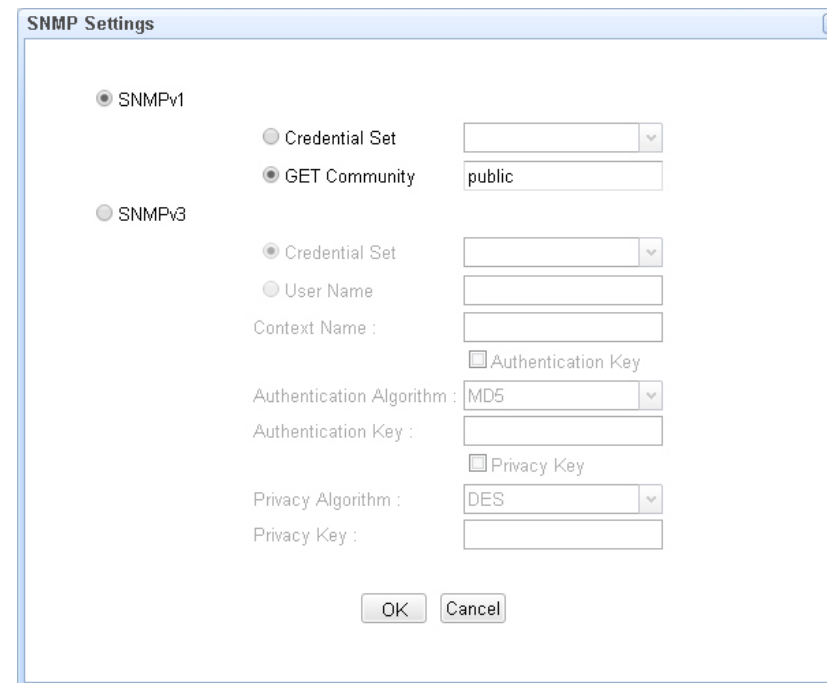
## [SNMP Settings] tab

SNMP settings information like SNMP version and credentials which were used while performing the discovery or recent device information update operation on the device is displayed.

### ■ [SNMP Settings] tab menu “☰”

If you click on the [SNMP Settings] tab menu “☰”, the following menu will be displayed.

SNMP Settings: You can change the SNMP settings for a registered device using this option. Once updated, these latest credentials will be used by SRDM for further operations on the device like “Schedule Setting” and “Device Information Update”.



- For a successful communication with device using SNMP protocol, the SNMP settings in SRDM must be configured in accordance with the network settings for the device.
- To modify the SNMP settings for multiple devices at once in SRDM, refer to “[Managing SNMP settings](#)”.



# DEVICE DETAILS

## [Counter History] tab

The counter history graph of the device is available under the [Counter History] tab.

### ■ Counter history graph

This displays the counter history of the selected device in a graph format. Each bar in the graph indicates the number of pages printed during the time interval indicated in the X-axis.

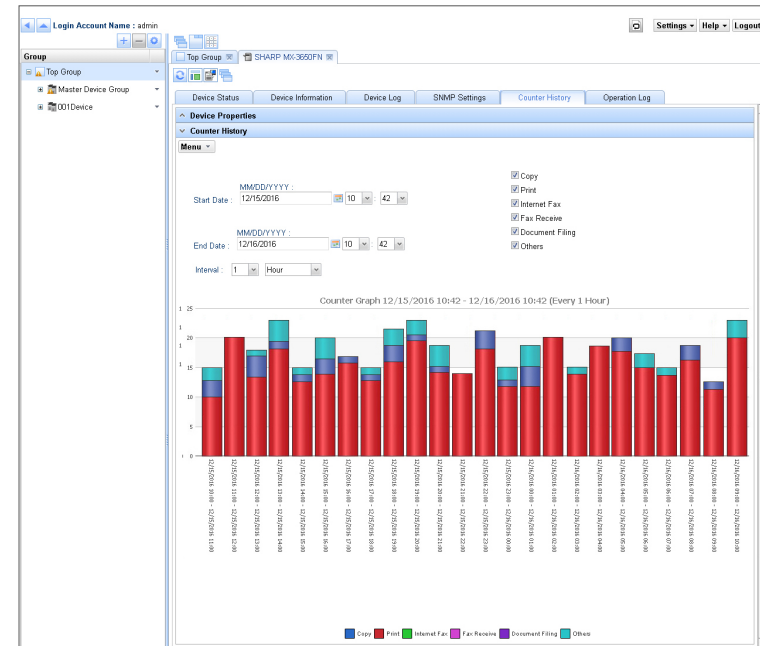
You can specify any time duration and interval, however the number of data points which are to be shown in the graph should not exceed 40. Using the check boxes in the upper right of the graph allows you to select the counter types. Below are the list of counter types available to select.

Counter Types:

- Copy
- Print
- Internet Fax
- Fax Receive
- Document Filing
- Other

### ■ [Counter History] tab menu button

- Default: Resets the time duration and interval to default. The default duration is past 1 day from the current time with 1 hour interval.
- XML File Output: Exports/saves the displayed counter history data as an xml file.

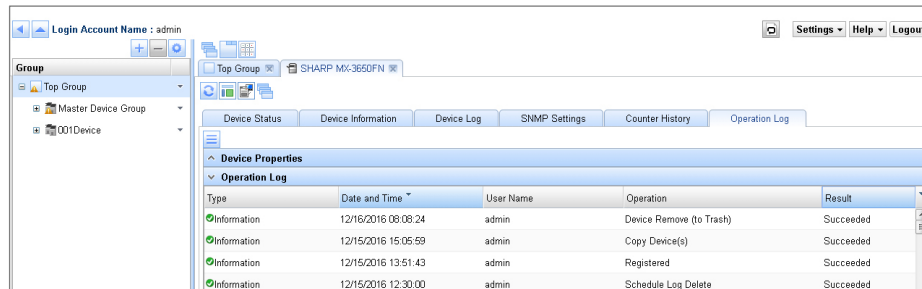


- This graph is created by using the data that has been acquired during the scheduled device information update and manual status update operations.
- An error message is displayed if the data points are more than 40 i.e., the specified time duration is more and interval is less.
- If the acquisition of data was not performed during a particular interval, "No Data" will be displayed in the graph for that particular interval.
- In order to display this graph, "Schedule Log Delete" must be set to a setting other than "Latest one Log".

# DEVICE DETAILS

## [Operation Log] tab

Log of operations which are performed in SRDM on the device such as device status and information updates, editing SNMP settings, delete device (move to trash can), copy device, move device are displayed in the [Operation Log] tab.



Type	Date and Time	User Name	Operation	Result
Information	12/16/2016 09:09:24	admin	Device Remove (to Trash)	Succeeded
Information	12/15/2016 15:05:59	admin	Copy Device(s)	Succeeded
Information	12/15/2016 13:51:43	admin	Registered	Succeeded
Information	12/15/2016 12:30:00	admin	Schedule Log Delete	Succeeded

### ■ [Operation Log] tab menu “☰”

If you click on the [Operation Log] tab menu “☰”, the following menu will be displayed.


1. XML File Output: Exports/saves all the device operation log data as an xml file.
2. Delete all Operation Logs: Deletes all the device operation log data.


# DEVICE MANAGEMENT





## Device Discovery

You can discover network connected devices by following any of the procedure given below.

Search using [Menu] button 

1. Click the [Group] tab menu .
2. Click [Start Device Discovery].

Discovered devices will be listed in the [Device Discovery] tab. Device discovery can be performed also by clicking the  button.

The  icon will be displayed and the  button will change to  while the device search is in progress. To stop the device search, click . The default discovery is set to search the local network only. Discovery settings can be changed to search across the subnet as described below.

### Search using [Discover] button

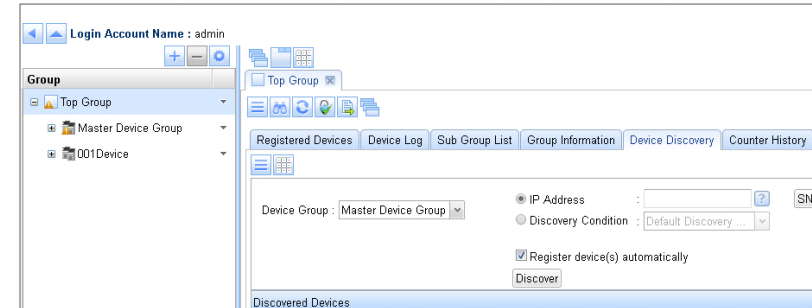
1. Click on the [Device Discovery] tab of the logged-in group.
2. You can select either the [IP Address] or [Discovery Condition] radio button.

#### [IP Address]

- a. Select [IP Address] field and enter the IP address to discover the device.
- b. By default this discovery option uses default SNMP settings, but if you want to perform discovery with different SNMP settings, click the [SNMP Settings] button and select the settings. This settings dialog is same as the [SNMP Settings](#) dialog available in the [SNMP Settings] tab of the registered device.

#### [Discovery Condition]

- a. You can select discovery conditions from the list of available [Discovery Condition] for the selected Device Group.



3. Click the [Discover] button.



- If the “**Register device(s) automatically**” check box is checked, the discovered devices will be registered automatically and the registered devices will be displayed in [Registered Devices] tab.
- If the “**Register device(s) automatically**” check box is unchecked, then discovered devices will be displayed in the [Device Discovery] tab > [Discovered Devices] grid.
- In order to manage the devices you must register the discovered devices. For more information, refer to “[Registering devices to the Registered Devices List](#)”.

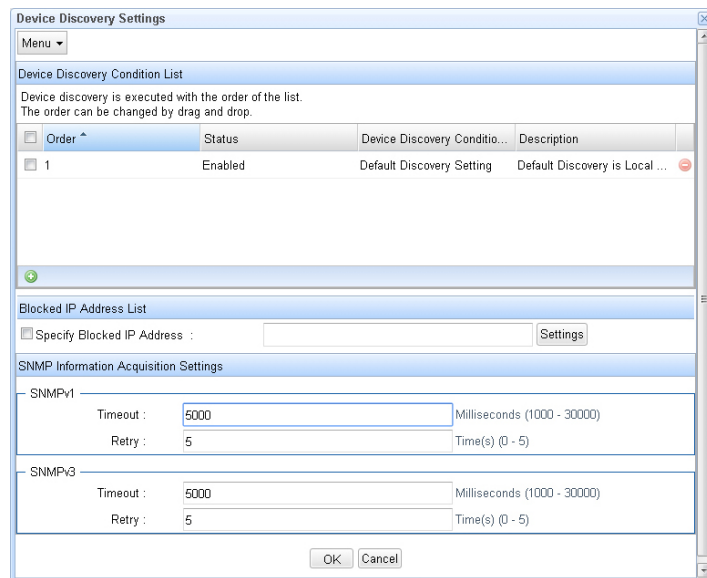
## Setting device discovery conditions

You can change the discovery settings of any device group with the following steps:

1. Click the [Device/System] tab menu “☰” of a device group.
2. Click [Settings] > [Device Discovery].
3. To create a new search condition, click the [Create Discovery Condition] from the [Edit] menu.

A new discovery condition can also be added by clicking on the “+” button which is available in the bottom left corner of the “Device Discovery Condition List” section of the dialog box.

To change the existing condition settings, click the condition that you want to change in the [Device Discovery Condition List].



4. Enter Device Search Condition Name, Description, IP Address Settings and SNMP Settings and click the [OK] button.
5. If there are any devices to be excluded from the search conditions, add their IP addresses to the “Specify Blocked IP Address” and then click the [OK] button.

Multiple device search conditions can be created and selected. Furthermore, the device discovery search conditions can be managed per device group.

The search conditions can be customized to include multiple search criteria including specific IP addresses, IP address ranges, local broadcast and broadcast searching.

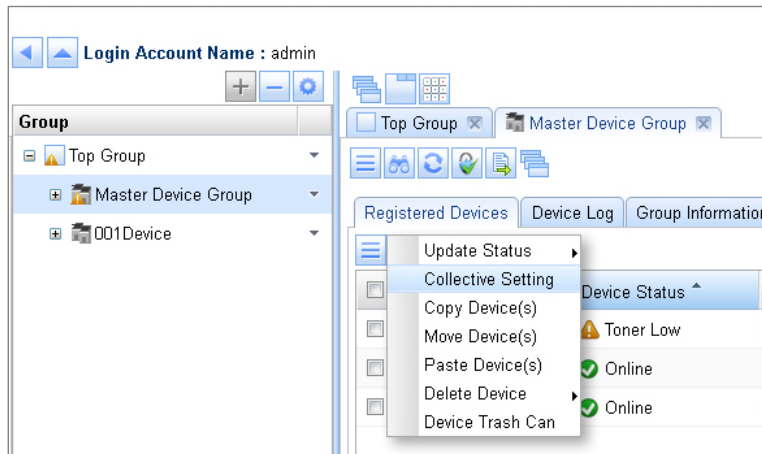


If the context name has been set in the SNMP v3 settings of older Sharp devices, an error may occur during discovery. If this happens, delete the context name from the settings and repeat the discovery operation.

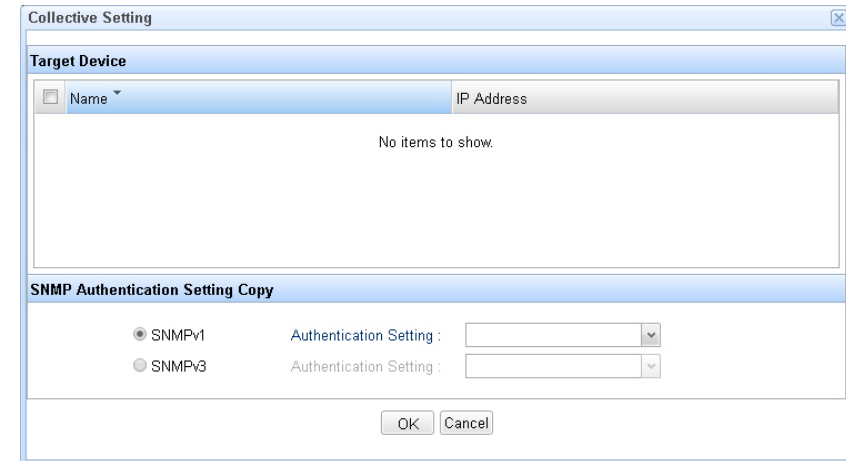
## Managing SNMP settings

If SNMP settings of one or more devices are changed at the device side after the discovery, you will need to update the SRDM SNMP settings to match the MFP device settings. For SNMPv1, the GET Community Name should match the one in the MFP device settings. For SNMPv3, the User Name, Authentication Key and Privacy Key should match the SNMPv3 settings in the MFP device.

You can manage the SRDM SNMP settings by following the procedure below.



1. Open the [Registered Devices] tab under device group and select the devices for which SNMP settings have to be updated.
2. Click the [Registered Devices] tab menu “☰” of a Device Group.
3. Click [Collective Setting].



4. Select the radio button of the SNMP version to be used to perform SNMP communication under “SNMP Authentication Setting Copy” and select the desired settings.

You can also create new set of SNMP credentials to use by selecting “Create New” or update the available credential set by selecting “Edit/Delete”.

Multiple SNMP settings can be created and selected for use depending on the application. Furthermore, the SNMP settings can be managed separately for each device group. The SNMP settings which have been created can be used in “Collective Setting” mentioned above.

SNMP settings can also be made individually in the [SNMP Settings] tab under each device tab. For more information, refer to “[[SNMP Settings](#)] tab”.




If the context name has been set in the SNMP v3 settings of older Sharp devices, an error may occur during discovery. If this happens, delete the context name from the settings and repeat the discovery operation.

## Registering devices in the Registered Devices List

Devices which have been found during device discovery are listed in the [Device Discovery] tab. You should register the discovered devices, in order to view and manage them under the [Registered Devices] tab.


You can register the discovered devices by following the procedure below.


1. **Select the devices you wish to register in the [Device Discovery] tab.**
2. **Click the [Device Discovery] tab menu “**


Registered devices will not be listed under the [Device Discovery] tab.


## Updating device status and data


You can update the device information by following the procedure below:

1. **Click the [Registered Devices] tab button “


You can also update the device data by selecting the devices and then clicking the “

If you click “


The “

To cancel the device information update, click the “

## Deleting devices**

To delete a device from the registered device list, click the delete “


Furthermore, you can delete multiple devices at once by following the procedure below.

1. **Select the devices to be deleted.**
2. **Click the [Registered Devices] tab menu “- a. **Click [Delete from List] to delete the devices from list (or)**
- b. **Click [Delete From Search Condition] to delete the devices from list and also to exclude the deleted devices from further discovery****

The list of devices which are excluded from discovery are listed in “Specify Blocked IP Address” field of the “[Setting device discovery conditions](#)” window.

## Restoring deleted devices

Deleted devices are moved to the Device Trash Can. The devices can be restored to the registered devices list by following the procedure below:

1. **Click the [Registered Devices] tab menu “**

You can permanently delete a device by deleting it from the Device Trash Can. Note that devices which have been deleted permanently cannot be restored, however these devices can be discovered again using the device discovery function.

## Copying or moving devices

In SRDM, registered devices can be copied or moved between device groups. You can do this by using any of the procedures below.

### ■ Drag and drop from Registered Devices list

Registered devices can be moved or copied to a different device group using the drag and drop option by following the procedure below.

1. Select the devices you wish to copy or move from the device group.
2. Drag the devices and drop on the target device group listed in the group tree pane.
3. Select the required operation from the displayed “Copy or Move Device(s)” dialog box.

### ■ Using the copy or move devices option in the Registered Devices menu

Registered devices can be moved or copied to a different device group using the options available in the menu by following the procedure below.

1. Select the devices you wish to copy or Move from device group.
2. Select [Copy Device(s)] or [Move Device(s)] from the registered devices list menu.
3. Select the target device group.
4. Select [Paste Device(s)] from the registered devices list menu.

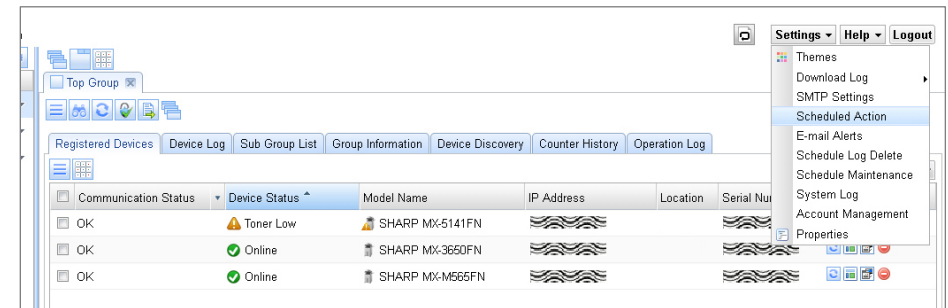
- If multiple copy or move operations are performed before a paste operation, only the latest copy or move information is stored.
- In case of copy operation, the device information is available even after executing paste, therefore, if "paste" is executed on multiple device groups, the same devices will be copied to the respective device groups. For move, the information is deleted after executing paste on one device group.



## Setting scheduled actions

You must set the scheduled actions such as device discovery and status updates by following procedure:

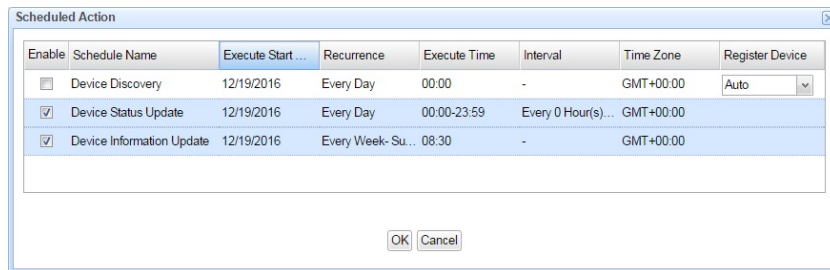
1. Select [Settings] and then click [Scheduled Action].





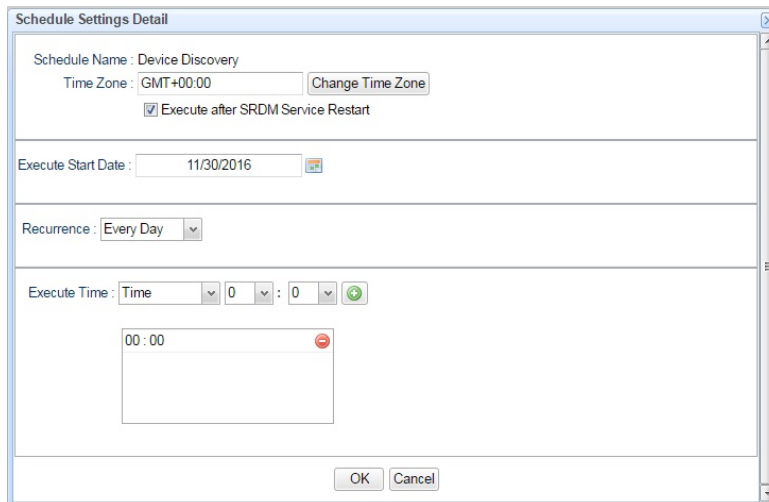
# DEVICE MANAGEMENT

2. Click [Device Discovery], [Device Status Update] or [Device Information Update] to open the Schedule Settings Detail dialog box.



Enable	Schedule Name	Execute Start ...	Recurrence	Execute Time	Interval	Time Zone	Register Device
<input type="checkbox"/>	Device Discovery	12/19/2016	Every Day	00:00	-	GMT+00:00	Auto
<input checked="" type="checkbox"/>	Device Status Update	12/19/2016	Every Day	00:00-23:59	Every 0 Hour(s)...	GMT+00:00	
<input checked="" type="checkbox"/>	Device Information Update	12/19/2016	Every Week- Su...	08:30	-	GMT+00:00	

3. Make the settings.



Schedule Name : Device Discovery  
Time Zone : GMT+00:00   
 Execute after SRDM Service Restart

Execute Start Date : 11/30/2016

Recurrence : Every Day

Execute Time : Time 0 : 0

00 : 00

- i. Set the time zone.
- ii. Select or unselect “Execute after SRDM Service Restart” check box to choose whether or not to carry out device discovery and device status and device information updates after the SRDM server is restarted..

**Note:** By default this option will be selected for device discovery and unselected for device status and device information updates.

- iii. Set execution start date.
- iv. To have the operation run periodically, select [Recurrence]. Following recurrence intervals are available for selection.
  - a. **Every Day:** Scheduled operation will be executed every day.
  - b. **Every Week:** You can select one or more days of the week to perform the schedule operation.
  - c. **Every Month:** You can select one or more days of the month to perform the schedule operation.
- v. Specify the “Execute Time”. Execution time can be specified as multiple times in a day or multiple times in a specific time interval of the day. Below is the description of each option.
  - a. **Time:** You can select specific time of the day in hours and minutes like 15:30 etc. After selecting the time, click on add “+” button to add to the execution time list.  
  
Multiple times of the day can be specified by adding time selection repeatedly with different values.
  - b. **Time Range:** You can specify time range of the day during which schedule operation to happen.



The shortest schedule setting which can be set in [Device Information Update] is for updating to occur once per day.

4. The “Register Device” column in the Scheduled Action dialog box indicates whether the devices need to be registered manually (Manual) or automatically (Auto) after scheduled discovery.

The default setting for a scheduled action is disabled. To enable each action, place a check mark in the "Enable" box



## ■ Types of scheduled action

There are three types of scheduled action: “Device Discovery”, “Device Status Update” and “Device Information Update”.

Details for each action are given below.

### – **Device Discovery:**

A scheduled action for device discovery.

For more information, refer to “[Device Discovery] tab”.

### – **Device Status Update:**

A scheduled action for device status updates. For more information, refer to “[Device Status] tab”.

### – **Device Information Update:**

A scheduled action for device status and data updates.

- When setting device discovery as a scheduled action, it is recommended that you set the interval to once per day.
- If the number of the registered devices is 20 or fewer, it is better to set the schedule interval of Device Status Update to 3 minutes or more.
- If the number of the registered devices is around 100, it is better to set the schedule interval of Device Status Update to 5 minutes or more.
- If the number of the registered devices is around 500, it is better to set the schedule interval of Device Status Update to 20 minutes or more .



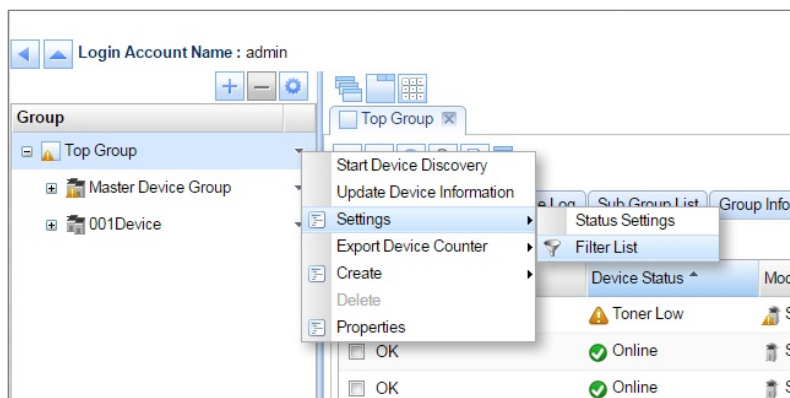

## Creating filters

To view the devices information based on certain criteria such as viewing devices having a status of “Paper Jam”, you can create and use filters in the [Registered Devices], [Device Log] and [Device Discovery] tabs.

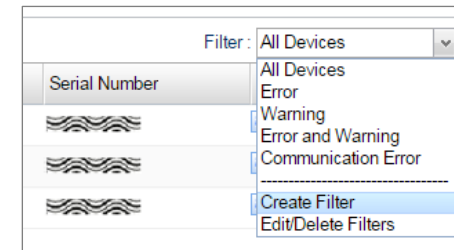
You can also use any of the default filters:

1. **All Devices:** Displays all the registered devices information
2. **Error:** Displays devices information whose current status is in any error condition. Ex: “Paper Jam”, “Toner Empty” etc.
3. **Warning:** Displays devices information whose current status is in any warning condition. Ex: “Paper Low”, “Toner Low” etc.
4. **Error and Warning:** Displays devices information whose current status is in any error or warning condition.
5. **Communication Error:** Displays information for devices whose communication status is “Communication Error”.

You can create new filters containing your own preferred filter conditions by following the procedure given below.

1. Click the [Group] tab menu “A screenshot of the device management software interface. The top left shows 'Login Account Name : admin'. Below it is a 'Group' tree view with 'Top Group', 'Master Device Group', and '001Device'. A context menu is open over the '001Device' group, listing options like 'Start Device Discovery', 'Update Device Information', 'Settings', 'Export Device Counter', 'Create', 'Delete', and 'Properties'. The 'Settings' option is selected, and a sub-menu is visible with 'Status Settings', 'Filter List', and 'Device Status'. The 'Filter List' option is highlighted. In the background, a table shows device status with columns for 'Device Status' and 'Mod', with rows for 'Toner Low', 'Online', and 'Online'.

The filter creation/modification screen can also be accessed by selecting “New Creation” or “Edit/Delete Filters” from the filter list box as shown below.



3. Click [Menu] at the top-left of the Filter list dialog box and then select [Create filter].
4. Enter the filter name and filter conditions and then click the [OK] button.

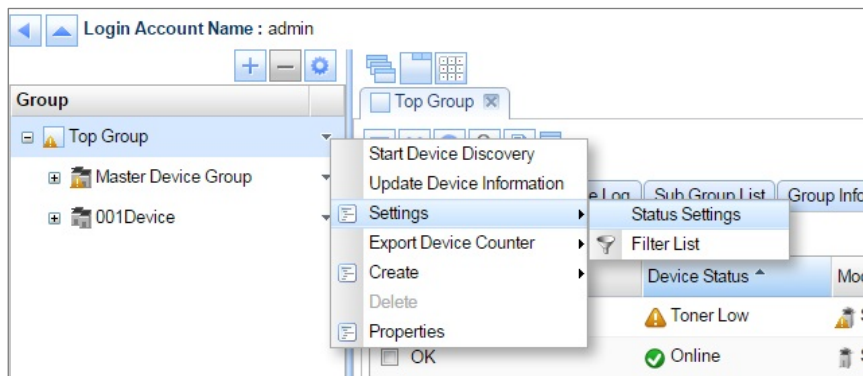


You can also right-click the column header to use simple filters. Use whichever method best suits your application.

## Changing the conditions for icon display

You can change the display conditions for status icons (“✔”, “⚠” and “✖”), paper level icons (“📄”, “📄”, “📄”, “📄” and “📄”) and toner level icons (“🖨”, “🖨”, “🖨” and “🖨”). To change the condition, follow the procedure given below.

1. Click the [Group] tab menu “☰” of a logged-in group.
2. Select [Settings] and then click [Status Settings].



3. To change the display conditions for the paper level icons or toner level icons, click the respective [Settings] button.
4. To change the display conditions for the status icons, unselect the change the alert level for the respective status.
5. Click the [OK] button.

## Setting E-Mail alerts

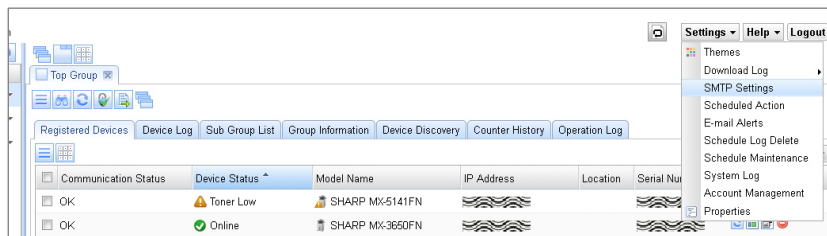
When device status changes to any of the warning or error status, such as when the toner level becomes low, e-mail alerts can be sent as a notification of the change in device status. In order to use e-mail alerts, you need to configure SMTP server settings and also select the statuses which require to be notified along with e-mail addresses of the concerned members.

You can configure the SMTP settings and e-mail alerts by following procedure.

### ■ SMTP server settings

You can configure SMTP server settings by following the procedure given below.

1. Click the [Settings] button on the top right of the screen and then click "SMTP Settings".



2. Enter the IP address and port number of the mail host (SMTP server).
3. Enter "From Address".
4. If the mail host requires E-Mail authentication, select the "E-mail Authentication" check box and then enter the user name and password.
5. If the mail host supports SSL communication, select "SSL" checkbox.
6. You can check the communication status with the mail host by clicking on [Check Mail Host] button.
7. Click on the [OK] button to save the settings.

A screenshot of the 'SMTP Settings' dialog box. It has a title bar with a close button. The dialog contains several input fields: 'Mail Host (SMTP):', 'Port No:', 'From Address:', 'User Name:', and 'Password:'. There are three checkboxes: 'E-mail Authentication', 'Change Password', and 'SSL'. At the bottom, there are three buttons: 'Check Mail Host', 'OK', and 'Cancel'.

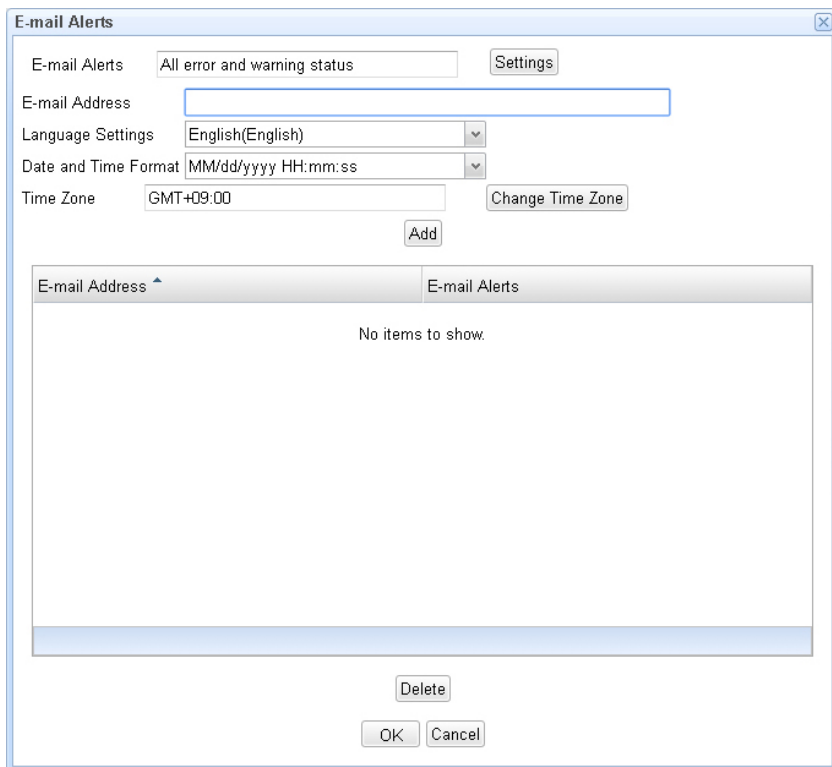
Only one E-Mail server setting can be made for each SRDM system.

# DEVICE MANAGEMENT

## ■ Setting notification statuses and destination addresses

You can set notification statuses and destination e-mail addresses by the following procedure.

1. Click the [Settings] button.
2. Select [E-Mail Alerts].



The screenshot shows the 'E-mail Alerts' configuration window. At the top, there is a dropdown menu for 'E-mail Alerts' set to 'All error and warning status' and a 'Settings' button. Below this is an 'E-mail Address' text field. Further down are 'Language Settings' (English(English)), 'Date and Time Format' (MM/dd/yyyy HH:mm:ss), and 'Time Zone' (GMT+09:00) with a 'Change Time Zone' button. An 'Add' button is positioned below the time zone settings. The main area of the window is a table with two columns: 'E-mail Address' and 'E-mail Alerts'. The table is currently empty, displaying 'No items to show.' At the bottom of the window, there are 'Delete', 'OK', and 'Cancel' buttons.

3. Click the [Settings] button to select the statuses.

4. Enter the notification e-mail addresses for receiving e-mail alerts in the E-mail Address field and then click the [Add] button.
5. You can configure any number of status alert conditions by repeating the above steps 3 & 4.
6. Click the [OK] button.



You can enter multiple E-Mail addresses in the E-Mail address field by entering a delimiter character between each address. The delimiter characters that can be used is “,”.

# DEVICE MANAGEMENT

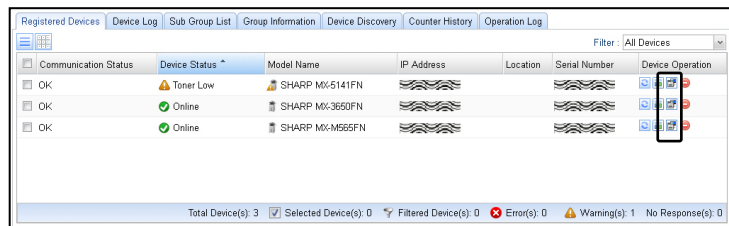
## Accessing device operation panel remotely

You can remotely access and operate a supported device operation panel.

To access the operational panel of a device, follow the steps below from SRDM and at the target device.

### Operations in SRDM:

1. Click the [Remote Operation] button on the [Registered Devices] tab.



2. Click the [Connect] button on the remote operation connection screen.




3. Click the [OK] button once the authentication screen is displayed.
4. Enter the password as required by the device settings. If you are unable to log in, contact your authorized servicing dealer.

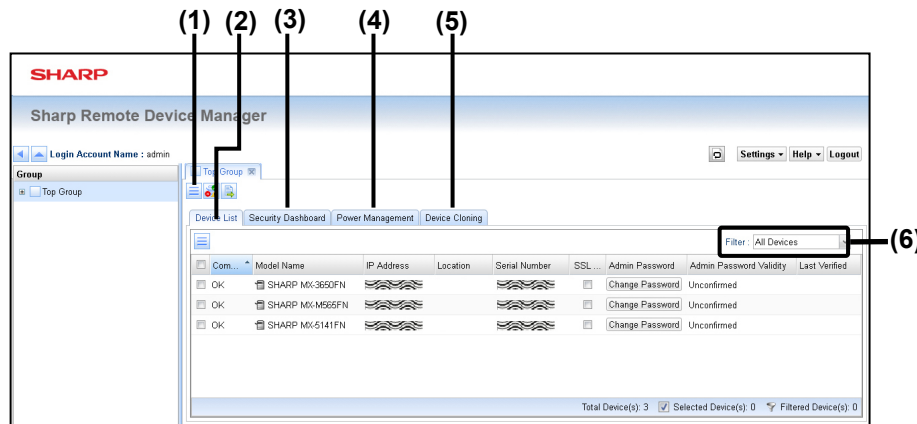
### Operations at device:

1. When the confirmation screen is displayed on the device's operation panel, touch or select the [OK] button.
2. Once connected, you can remotely control the MFP device panel.

- For more information about which models support the remote operation function, refer to "Readme". "Readme" can be accessed from the [Help] button of SRDM.
- To use the remote operation function, you must first enable remote operation in each device's system settings. For more information, see the device's Operation Guide.
- This function can be used with Chrome or IE10 or later versions.

# ADVANCED FEATURES

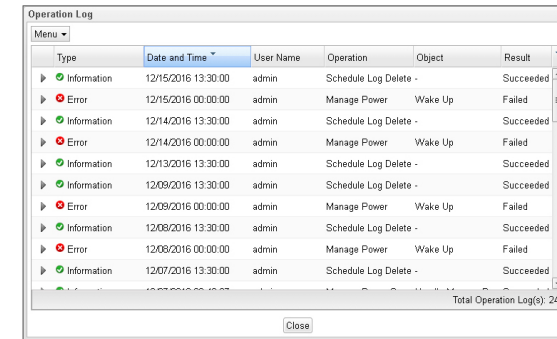
If you click the [SRDM (Advanced Features)] button “” on the [Group] tab, the SRDM (Advanced Features) window will be displayed. You can use security setting management functions, power management functions and cloning functions in the Advanced Features window.




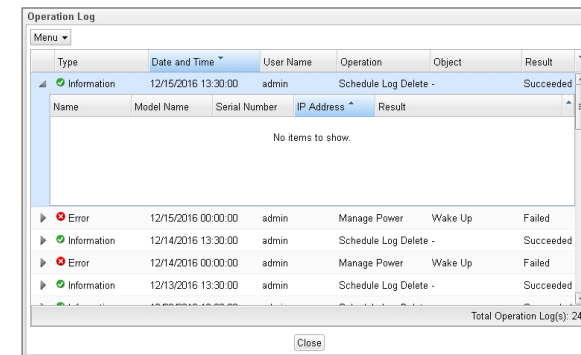
## (1) [Group] tab menu “”

If you click on the [Group] tab menu, the following menu will be displayed.

- **Log Management:** This menu provides option to view “Operation Log”. “Operation Log” contains the log of all security related operations performed by the user in this group like the result of login attempt to devices, changes to administrator password to be used by SRDM to access the devices, result of applying security policy to devices. Each log entry contains information such as “Type”, “Date”, “Login Group id”, “User Name”, “Operation”, “Object” and “Result” of the operation.



Click the “” icon next to the log entry to display the details of change on attempted devices as shown below.



## ■ Operation Log Menu

If you click on the [Menu] in the [Operation Log] window, the following menu will be displayed.

1. **Update Logs:** Click to fetch the latest information from SRDM server.
2. **XML File Output:** Click to output all the operation log data as XML file.
3. **Delete all Operation Logs:** Deletes all the operation log data.

# ADVANCED FEATURES

- **E-Mail Settings:** This menu provides option to view and configure E-Mail Alerts.

- 1) Click on “Settings” button to select the security policy settings.
- 2) Enter the notification e-mail addresses for receiving e-mail alerts in the E-mail Address field and then click the [Add] button.
- 3) Select the e-mail notification language, date format and time zone.
- 4) Click the [Add] button.
- 5) Click the [OK] button.



You can enter multiple E-Mail addresses in the E-Mail address field by entering a delimiter character between each address. The delimiter characters that can be used is “,”.

## [Device List] tab

This displays list of registered devices which support advanced features and belong to logged-in group. For more information, refer to “[[Device List](#)] tab”

## [Security Dashboard] tab

You can check and apply different security levels to the MFP using this feature. It also allows you to verify whether the MFP security level is same as the security level set in SRDM.

For more information, refer to “[[Security Dashboard](#)] tab”

## [Power Management] tab

This tab allows you to use the Power Management feature. For more information, refer to “[[Power Management](#)] tab”.

## [Device Cloning] tab

This tab allows you to use the Device Cloning feature. For more information, refer to “[[Device Cloning](#)] tab”.

## Filter box

This lets you use and create filters to display devices based on the defined criteria in the selected filter. For more information, refer to “[[Creating Filters](#)]”



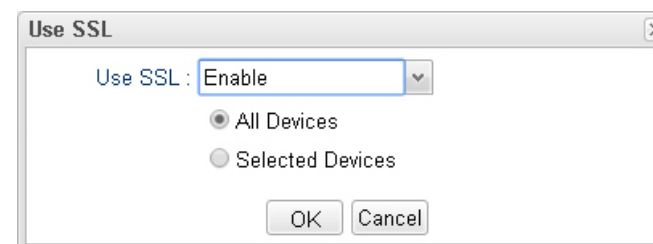
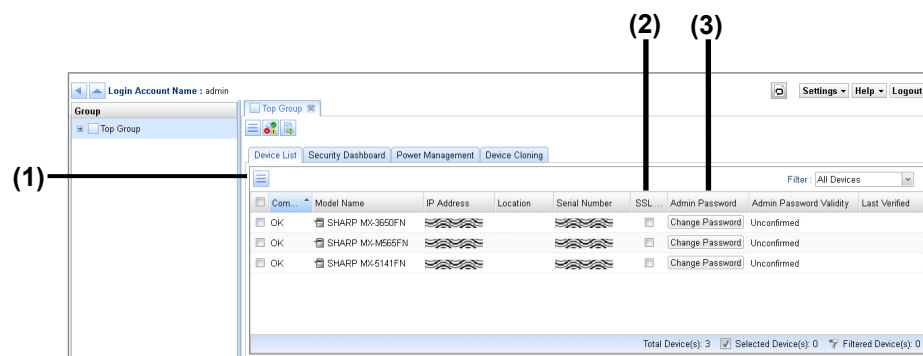
Devices which do not support advanced features are not displayed in Advanced Features Window.

Points (3), (4), (5): These tabs will be displayed based on the permissions available for the logged-in user.



## [Device List] tab

In order to use the advanced features, you need to set preferred communication protocol for each device and also provide administrator password to access advanced features of the device.

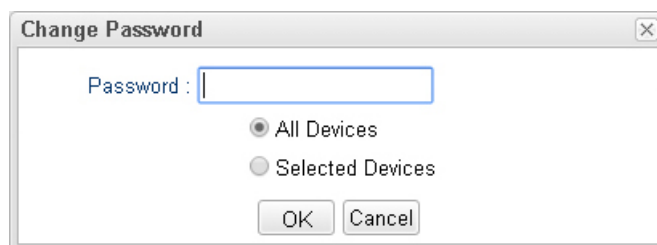


- **Login Attempt:** Allows you to verify whether the login attempt to the selected devices using the administrator password provided in SRDM is successful or not.

### (1) [Device List] tab menu “☰”

If you click the menu button, the following menu items will be displayed.

- **Change password:** Allows you to set the administrator password in SRDM for authenticating with the devices while performing security operations. You can set the password for a group of selected devices or for all devices at once.



- **Use SSL:** You can set SSL to encrypt the data which is transferred between the devices and SRDM as part of security operations, device cloning etc.

### (2) SSL Communication

Select SSL checkbox of each device to encrypt the data which is transferred between the devices and SRDM as part of security operations, device cloning etc. You can use device list menu option “Use SSL” to set SSL for multiple devices at once.

### (3) Admin Password

Click the [Change Password] button of the target device to set an administrator password in SRDM for authenticating with the device while performing security operations.

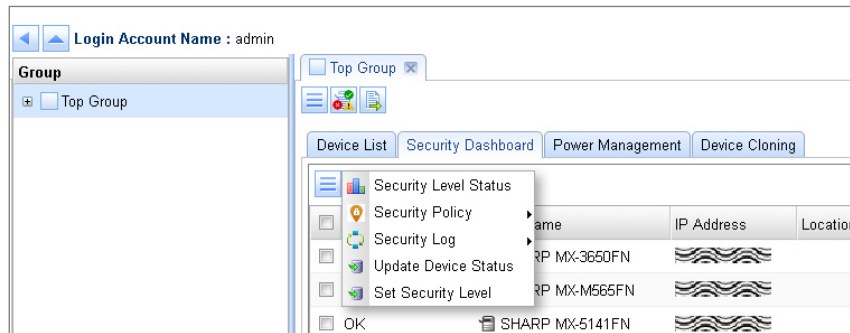
You can use device list menu option “Change Password” to specify password for multiple devices at once.

You can use device list menu option “Login Attempt” to verify whether the login attempt to the devices using the administrator password provided in SRDM is successful or not.

## [Security Dashboard] tab

Using the Security Dashboard features in SRDM, you can manage the security settings of multiple devices at once.

This [Security Dashboard] tab screen allows you to check and apply security settings to the devices. You can also verify whether the device security level is matching with the security level set in SRDM.



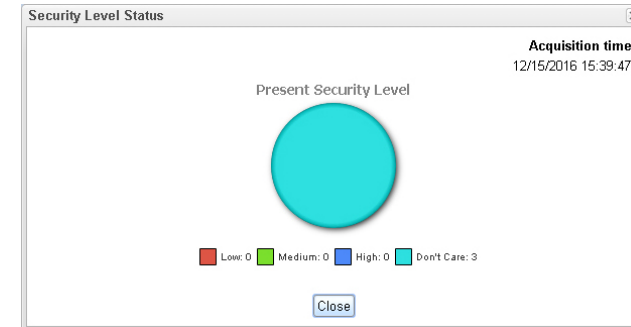
The security dashboard features cannot be used for DSK (Data Security Kit) installed devices; Hence “Check” & “Apply” button will not be displayed for DSK installed devices.

### ■ [Security Dashboard] tab menu “☰”

If you click on the menu, the following items will be displayed, which allows you to perform various security related operations as described below.

#### 1. Security Level Status:

This option displays whether devices have low, medium or high security level settings



#### 2. Security Policy:

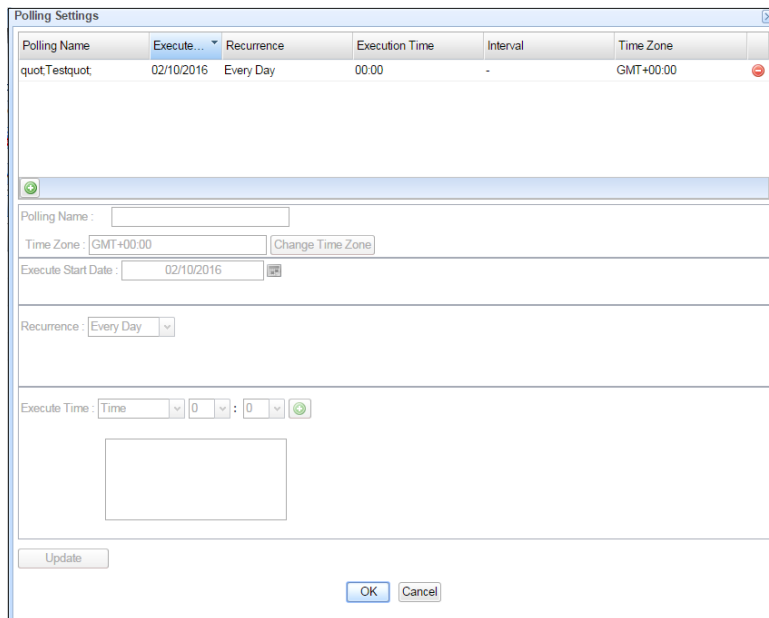
This option allows you to schedule polling for security policy, set security policy settings and apply security policy to device.

##### a) Polling Settings:

You can create and edit schedules for polling the security policy. If Security “Check” has not been done manually even once, security check by polling will fail.

If you click the polling settings menu, polling settings window will display as follows.

# ADVANCED FEATURES



The Polling Settings dialog box contains a table with the following data:

Polling Name	Execute...	Recurrence	Execution Time	Interval	Time Zone
quot;Testquot;	02/10/2016	Every Day	00:00	-	GMT+00:00

Below the table are input fields for: Polling Name, Time Zone (GMT+00:00), Execute Start Date (02/10/2016), Recurrence (Every Day), and Execute Time (Time, 0:00). Buttons for Update, OK, and Cancel are at the bottom.

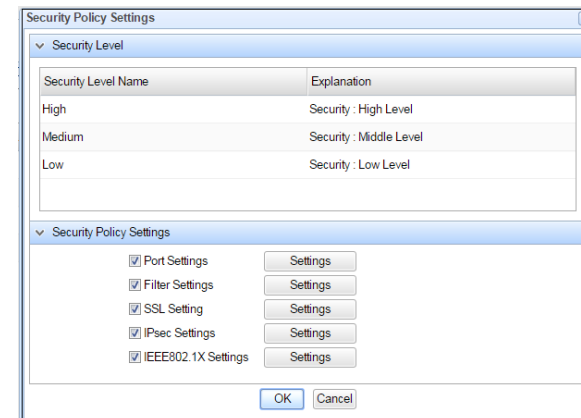
## Settings can be done by using following procedure

1. Click on add “+” button in the polling settings list to add a new schedule polling.
2. Set the name for polling.
3. Set the time zone and execution start date.
4. To have the operation run periodically, select recurrence. Following recurrence intervals are available for selection.
  - a. Every Day: Scheduled operation will be executed every day.
  - b. Every Week: You can select one or more days of the week to perform the schedule operation.
  - c. Every Month: You can select one or more days of the month to perform the schedule operation.
5. Specify the “Execute Time”. Execution time can be specified as multiple times in a day or multiple times in a specific time interval of the day. Following is the description of each option.

- a. Time: You can select specific time of the day in hours and minutes like 15:30 etc. After selecting the time, click on add “+” button to add to the execution time list.
- b. Multiple times of the day can be specified by adding time selection repeatedly with different values.
- c. Time Range: You can specify time range of the day during which schedule operation to happen.
- d. Click [Update] button to reflect the changes in the schedule list.
- e. Click [OK] button to save the created or updated schedules

## b) Security Policy Settings:

By using this option, you can update the security level and security policy on Security Dashboard associated with specified group. This settings dialog allows you to set “Port Settings”, “Filter Settings”, “SSL Settings”, “IPsec settings” and “IEEE802.1X Settings”.



The Security Policy Settings dialog box shows a table for Security Level and a list of settings:

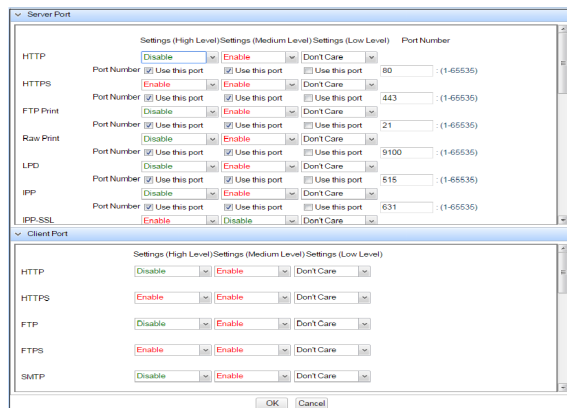
Security Level Name	Explanation
High	Security : High Level
Medium	Security : Middle Level
Low	Security : Low Level

Below the table are checkboxes for: Port Settings, Filter Settings, SSL Setting, IPsec Settings, and IEEE802.1X Settings, each with a corresponding Settings button. Buttons for OK and Cancel are at the bottom.

# ADVANCED FEATURES

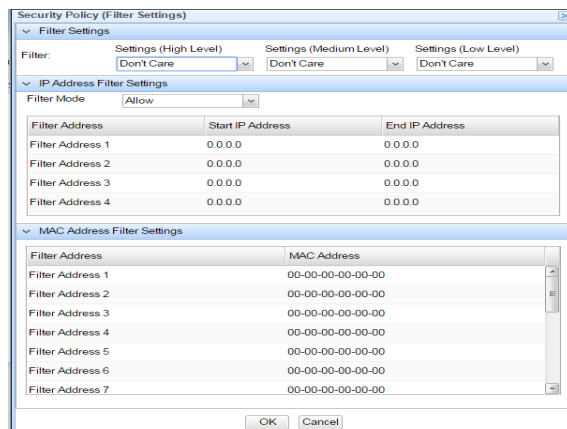
- **Port Settings**

By using this window, you can update server and client port information of security policy. This also updates security level (“High”, “Medium”, “Low”) for client and server port. Default value for Server Port and Client Port for each type of protocol is displayed as shown in the following window



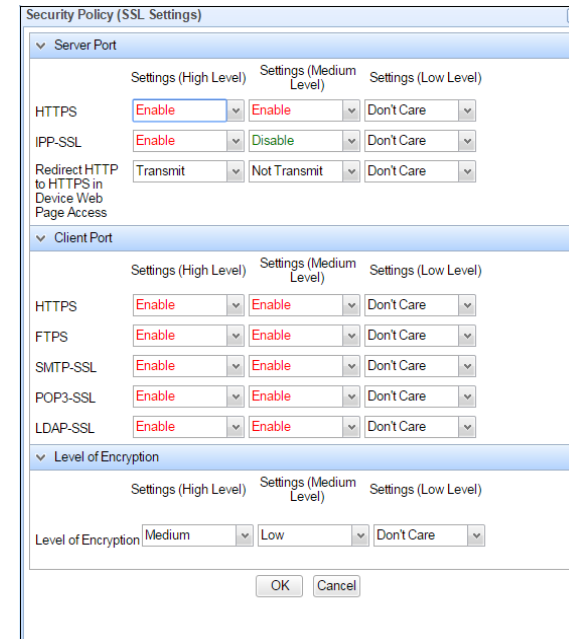
- **Filter Settings**

By using this window, you can allow or deny the access to the device. You can filter based on IP address and MAC address.



- **SSL Settings**

By using this window, you can set SSL setting for server and client. It allows you to enable or disable the SSL encryption for each protocol. You can specify the level of encryption for each type.

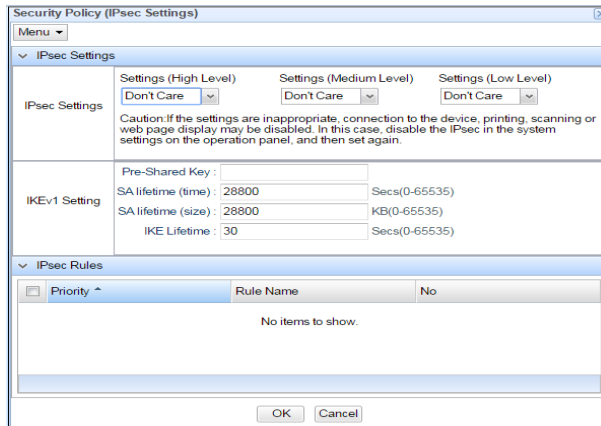


# ADVANCED FEATURES

- **IPsec Settings**

By using this settings window, you can set IPsec and IKEv1 settings.

You can add or delete the IPsec rules by using menu option “IPsec Rules”.

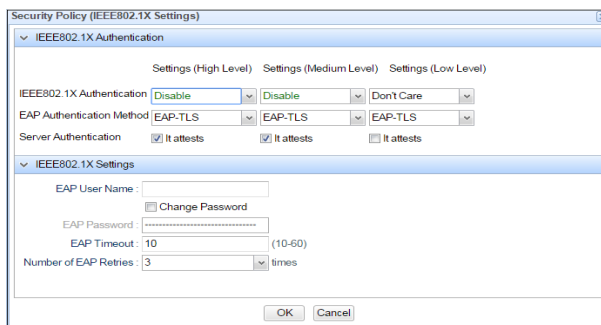


**Add** –This menu item can be used to add new IPsec Setting rules.

**Delete** –This menu item will be used to delete the selected IPsec rules. After deleting, IPsec rules list will be refreshed

- **IEEE802.1X settings**

This allows you to set IEEE authentication level and settings



- c) **Apply Security Policy to Device:**

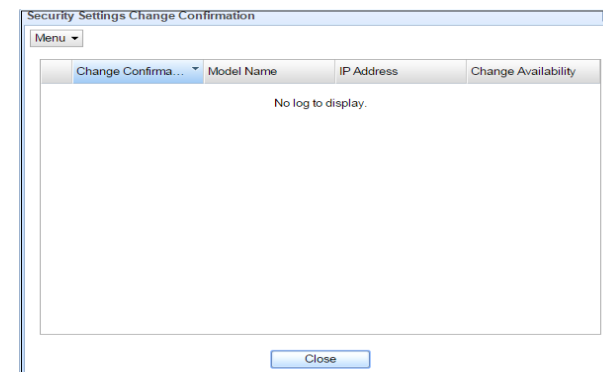
This allows you to set the security policy to the device. Before setting the security policy, it is mandatory to set the security level for the device with any of the security level. For more information. refer to “[Applying security policies](#)”.

### 3. Security Log:

This menu option allows you to view the security logs based on group and also based on each device. When you click this security log menu, the following options will be displayed.

- a) **Security Settings Change (Group)**

This will display the difference between settings applied for one or more devices in security policy settings screen (security values managed in SRDM) and settings fetched from device at the time of polling. Setting differences are displayed in red color text. When you click the Security Settings Change (Group) menu the following window will be displayed.



This window contains the information about “Change Confirmation Time”, “Model name”, ”IP Address” and “Change Availability” of the device.

# ADVANCED FEATURES

If you click the [Menu] button, the following menu will be displayed:

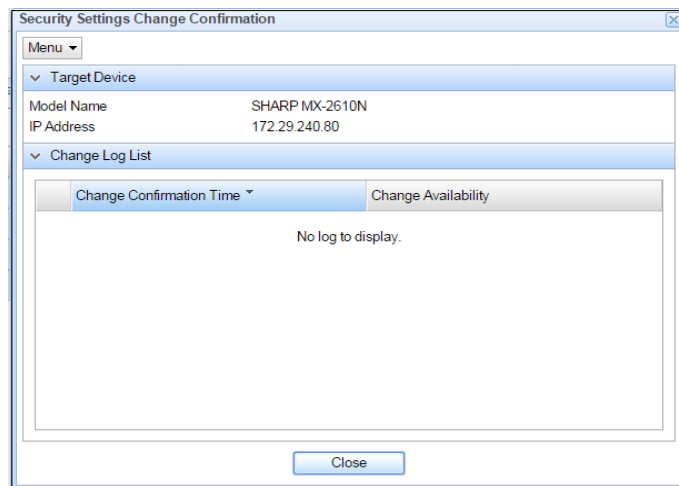
**Update:** Fetches the latest logs

**Check result:** Gets the device based security settings change

## b) Security Settings Change (Device)

This displays the difference of settings applied for the selected device in security policy settings screen and settings fetched from device at the time of polling. Difference will be displayed in red color text.

When you click the Security Settings Change (Device) menu the following window will be displayed



This window contains the information such as “Change Confirmation Time” and “Change Availability” from selected device.

If you will click on menu, following item will be displayed

**Update:** To get the latest logs

**Check Result:** To get the group based security settings change



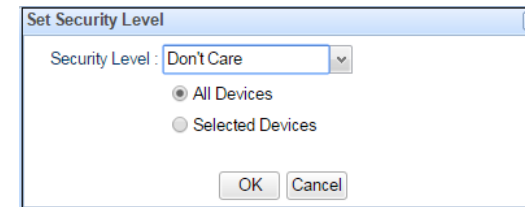
In some cases due to the time lag of the acquisition timing of the Security Setting file at and after applying the Security Policy, changes may not be found correctly.

## 4. Update Device Status:

This allows you to perform security check for the selected devices (Checkbox is ON) with security level is set. For more information, refer to [“Checking security policies”](#).

## 5. Set Security Level:

If you click on this menu following window will be displayed. This allows you to set security level with High, Medium, Low and Don't Care for selected devices.



To use security dashboard features, the target device should meet the following conditions:



- HTTP and HTTPS communication should be enabled
- The ports to be used for HTTP and HTTPS should be 80 and 443 respectively
- The feature “Data Backup (Send)” should be enabled

If any of the above settings are changed in the MFP, then Security Dashboard features cannot be used from SRDM.

## ■ Security policies

You can apply the security policy and check the security status of devices by following the procedures below.

### 1. Applying security policies

You can overwrite the security settings of the devices by applying any security policies defined in SRDM using the following procedure.

- 1) In [Device List] tab, select “SSL communication ON/OFF” for the respective devices.
- 2) Provide “Admin Password” to be used by SRDM to authenticate with the device and verify the Login is successful.  
Refer to “[Device List] tab” for more information.
- 3) In [Security Dashboard] tab, select the check boxes (at the left side of the Device List) for the devices to apply the security settings.
- 4) Click the [Security Dashboard] tab menu “☰”.
- 5) Click [Security Policy] > [Apply Security Policy to Device]

Note: Clicking the [Apply] button displayed in “Security Policy” column of [Security Dashboard] tab, allows you to apply the Security Settings for each device.

While the security policies are being applied, the “In progress” icon “🔄” will be displayed to the right of the [Security Dashboard] tab menu. Result of the operation “Succeeded” or “Failed” will be displayed in “Last Applied” column.



If the security policies are applied successfully, you will be able to click [Check] button for checking the security policy.

### 2. Checking security policies

You can check whether security settings are appropriate for the security policies for each device by the procedure given below.

- 1) In [Security Dashboard] tab, select the check boxes (at the left side of the device list) for the devices to check the security settings.
- 2) Click the [Security Dashboard] tab menu “☰” and click [Update Device Status].

While the security policies are being checked, the “In progress” icon “🔄” will be displayed on the right side of the [Security Dashboard] tab menu. Result of the operation, “Changed” or “No Difference” will be displayed in “Result” column.



You must apply security policy before performing check operation.

You can run security policy checking at regular-intervals by following the procedure given below.

- 1) Click the [Security Dashboard] tab menu “☰”.
- 2) Click [Security policy] > [Polling Settings].
- 3) Set the date and time for executing the schedule operation and click the [OK] button.

You can also check the security policy for each device by clicking the [Check] button in the Security Dashboard.

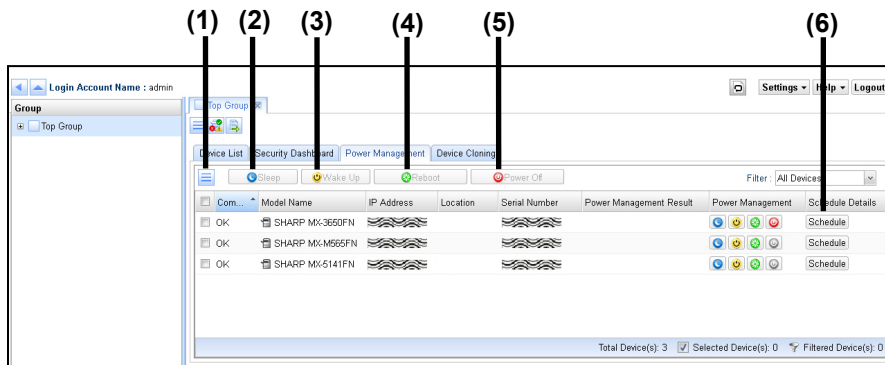


After changing the Security Policy, click [Security Policy] > [Apply Security Policy to Device], You will not be able to confirm the Security Policy until you apply.

# ADVANCED FEATURES

## [Power Management] tab

Using the Power Management feature in SRDM, you can manage the power settings for the devices. This [Power Management] tab allows you to execute sleep, wakeup, reboot and power off on multiple devices at once. You can also edit the power management operation schedules for devices.



### (1) [Power Management] tab menu “☰”

If you click on the menu, the following items will be displayed

**Create Schedule:** Allows you to create a schedule for power management operations to be executed on the devices.

**Edit Schedule:** You can edit the schedule for power management operations for the devices.

### (2) [Sleep] button “🌙”

This allows you to change the status of the device to automatic power shutoff mode.

### (3) [Wake up] button “😊”

This allows you to change the status of device to wake up mode.

### (4) [Reboot] button “🔄”

This allows you to reboot the device.

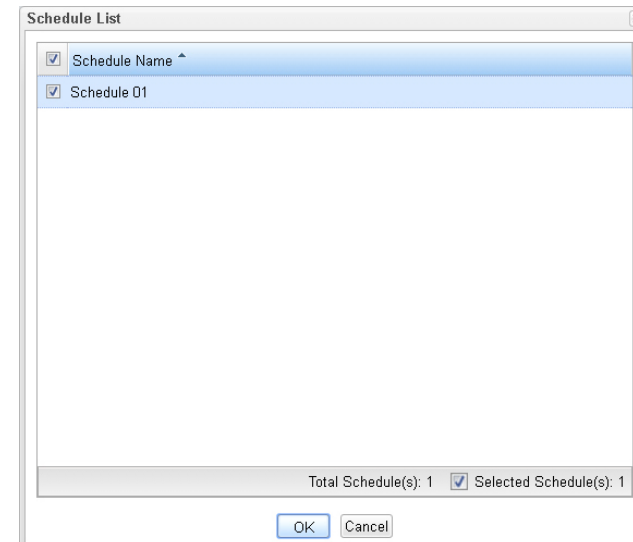
### (5) [Power off] button “🔴”

This allows you to switch off the device.

Note: This option will be available only on supported devices.

### (6) [Schedule] button “📅”

This allows you to select the power management operation schedule for the device.





# ADVANCED FEATURES


## ■ Executing Power management operations

You can execute the power management options by clicking on the respective buttons in device list under [Power Management] tab or by creating and assigning the schedule as described in the procedures below.

### 1. Manual Power Management

- a. Select the check boxes (at the left side of the device list) for the devices to run the power management functions.
- b. Click the [Sleep], [Wake up], [Reboot] or [Power Off] button which are available on right of the [Power Management] tab.

When the power status are changed, the results of the operation (success or failure) will be displayed in the “Power Management Result” Column of [Power Management] Tab.



- You can also change the power status for each device by clicking the [Sleep] icon “🌙”, [Wake up] icon “😊”, [Reboot] icon “🔄” or [Power off] icon “🔴” displayed for each device in the device list.
- If the buttons for a device are grayed out in the [Power Management] tab, then power management functions cannot be used for that device.

### 2. Schedule Power Management

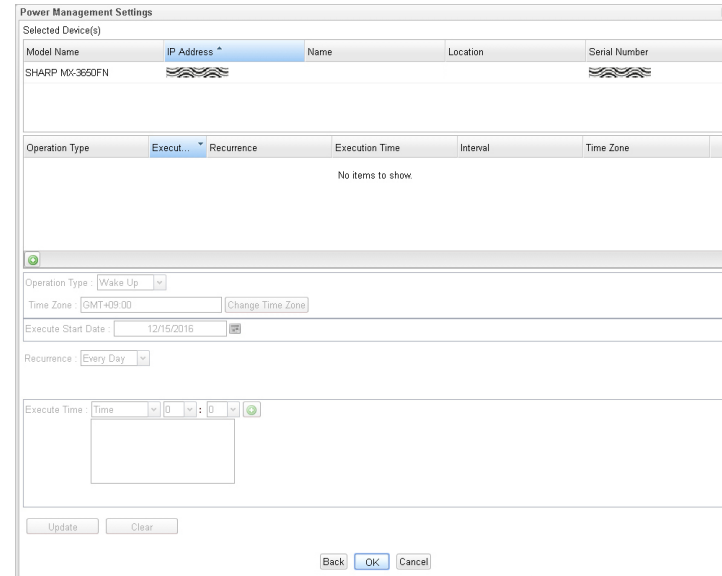
Schedules enable you to perform specified operations such as “wake up”, “sleep”, “reboot” and “power off” for a device at a specified time.

#### ■ Create and execute a schedule

You can create schedules for executing power management options at regular-intervals by following the procedure below.

1. Select [Create Schedule] from the [Power Management] menu.

### 2. Configure the settings as indicated on the dialog box.



You can use this dialog to create schedule for power management options such as “Wake Up”, “Sleep”, “Reboot” and “Power Off”

3.

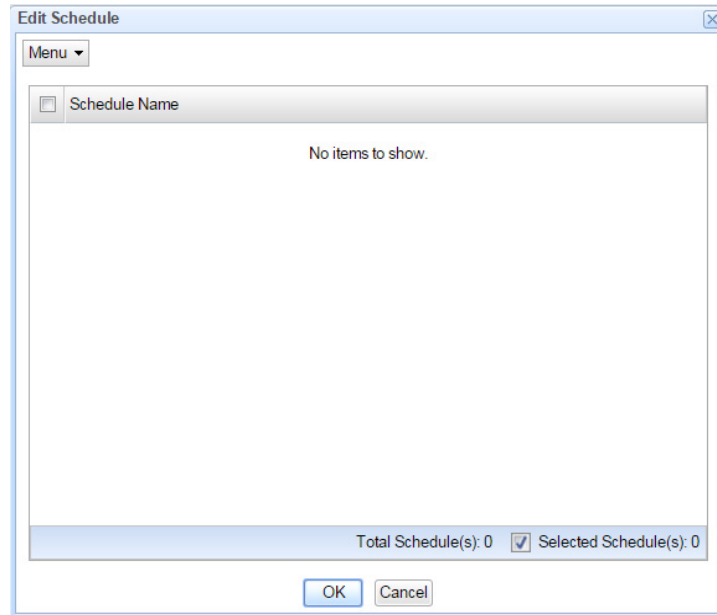
# ADVANCED FEATURES

## ■ Edit a schedule

You can update the existing schedules by following the procedure below.

### 1. Select [Edit Schedule] from the [Power Management] menu.

This opens the following dialog with the list of already created schedules.



### 2. Select “Menu” button which is available on top left.

When you click the [Menu] button, the following menu items will be displayed.

- Create Schedule Edit Schedule  
You can create a new schedule by clicking this option. For more information, refer to [“Schedule Power Management”](#).
- Delete Schedule  
You can delete the schedules which are selected in the list of schedules with a confirmation dialog.
- Exit  
Close the dialog.

# ADVANCED FEATURES

## [Device Cloning] tab

### ■ Overview

The [Device Cloning] tab allows you to copy the settings and registration information of one device (source) to the other compatible devices (target devices). Using this functionality you can perform operations such as user registration on all similar devices at once.

This feature supports two types of cloning:

- **Device Cloning:** This feature lets you save the setting information of a device and copy it to other devices.
- **Storage Backup:** This feature lets you save the address book information and user information of a device and copy them to other devices.

Refer to the following table for the list of items which are part of Device Cloning and the Storage Backup operations.

Features	Clone able items	Contents
Device Cloning	System settings	Initial Settings, Paper Feed Tray Settings, Receiving/Forwarding Settings, Printer Environment Settings, User Management, Energy Saving Settings, Operation Settings, Device Settings, Copy Settings, Printer Settings, Fax/Image Transmission Settings, Operation Settings, Scanner Settings, Internet Fax Settings, Document Filing Settings, Security Settings, Sharp OSA Settings
	Web Page Settings	Network Settings, Application Settings (except for Boiler plate/Forwarding Table), E-mail Alert/Status, Port Settings/Filter settings, Set Custom Link
Storage Backup	Registration information	Address book, User registration information, Copy (Letter print Boiler plate), Job program, Fax/image transmission (Boiler plate), Metadata set

\* These contents may vary depending on the device model, attachment options, etc.

### ■ Pre-requisites for Using Device Cloning & Storage Backup

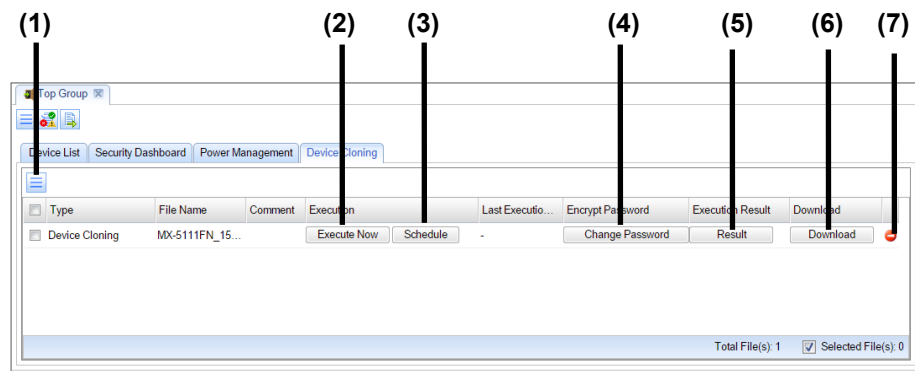
- For device models that support Device Cloning and Storage Backup, refer to "Readme" of SRDM. "Readme" can be accessed from [Help] button of SRDM.
- Before following the procedures involved in device cloning and storage backup, refer to "[[Device List](#)] tab", and set the administrator password for each device to be used by SRDM.



- When the Device Cloning file or Storage Backup file is acquired from a specific device and imported into another device, the settings may not be reflected properly if the device models are different.

# ADVANCED FEATURES

## ■ Device Cloning Execution



### (1) [Device Cloning] tab menu “☰”

If you click the menu button, the following menu items will be displayed.

- Device Cloning File Upload: This allows you to upload the device cloning files to SRDM by fetching from the devices or from any cloning file stored on your PC. For more information, refer to [“Uploading Files”](#)
- Storage Backup File Upload: This allows you to upload the device storage backup files to SRDM by fetching from the devices or from any storage backup file stored on your PC. For more information, refer to [“Uploading Files”](#)
- Delete File: This allows you to delete one or more number of files will be deleted at once. For more information, refer to [“Delete file menu option:”](#).
- Operation Log: This displays the operation logs for device cloning and storage backup operations.

## ■ Uploading Files

The settings data of a source device (Device Cloning or Storage Backup data) can be uploaded to SRDM in any of the following ways

- Upload by directly fetching from the device
- Upload the existing setting file which is obtained by exporting from the device web page.

The following procedure explains the steps to upload the file

1. Click the [Device Cloning] tab menu “☰”
2. Click the [Device Cloning File Upload] or [Storage Backup File Upload]. Select whether to acquire the information directly from the device or use the already acquired file.

The dialog box 'Device Cloning File Upload' contains the following elements:

- From Device :
- Model Name :**
  - IP Address :
  - Name :
  - Location :
  - Serial Number :
- From Source File :  No file chosen
- Encryption Password (5 - 16 Characters)
- (\*) It is highly recommended to set the encryption password. This will be used to encrypt the data fetched from MFP.
- Download Password
- (\*) It is highly recommended to set the download password. This password is required to download this settings file.
- Comment :
-

4.

# ADVANCED FEATURES

- **Encryption password:** This is used to encrypt the files when directly acquiring the information from the device.
- **Download password:** This is used to restrict the download operation and misuse of the data, it is recommended to set the download password.



- The uploaded file may be visible to other users. Therefore, it is strongly recommended that you set an encryption password and also download password.

3. You can write comments about the file to be uploaded in the Comment column 4. Click the [Upload] button.

## (2) Execute Now (Device Cloning / Storage Backup)

You can copy the selected cloning or storage backup file to the target devices by following the procedure below.

1. Click the [Execute Now] button to copy Storage Backup / Device Cloning on selected device.  
“Execute Device Cloning Settings” or “Execute Storage Backup Settings” dialog will be displayed

<input type="checkbox"/>	Model Name	Name	Location	Serial Number
<input type="checkbox"/>	SHARP MX-2610N			1504829Y00
<input type="checkbox"/>	SHARP MX-2640N	\TEST	\TEST	3507666000

Retry Intervals (0 - 10 Times) : 0  
Retry Interval Time (1 - 1500 Minutes) : 60

When neither the content of the file nor the selected device are suited, the cloning "Disclaimer" is not correctly done. Moreover, when the device which is not supported is chosen, it will not operate correctly.

Execute Cancel

This dialog allows you to select the target devices on which the execution (Cloning or Storage Backup) has to be applied

2. Select the Target Devices.
3. Set the retry intervals (how many times the execute operation needs to be tried again in case of a failure).
4. Set the retry interval Time (Time gap between the execute operations in case of a failure).
5. Click the [Execute] button to start operation

**Note:** You must restart the device, after applying device cloning or storage backup settings.

## (3) Schedule (Scheduled operation for cloning/storage backup)

You can create schedules to perform the cloning operation on specific date and time automatically by following procedure.

1. Click the [Schedule] button of the setup file for cloning.  
This opens the Schedule List dialog

<input checked="" type="checkbox"/>	Schedule Name	Scheduled Date And Time	Scheduled Time Zone
<input checked="" type="checkbox"/>	Test	02/12/2016 16:14	GMT+00:00

Total Schedule(s): 1  Selected Schedule(s): 1

OK

# ADVANCED FEATURES

This screen displays the list of schedules created corresponding to the selected file. This allows you to create new schedules, edit the existing schedules and also to delete the existing schedules.

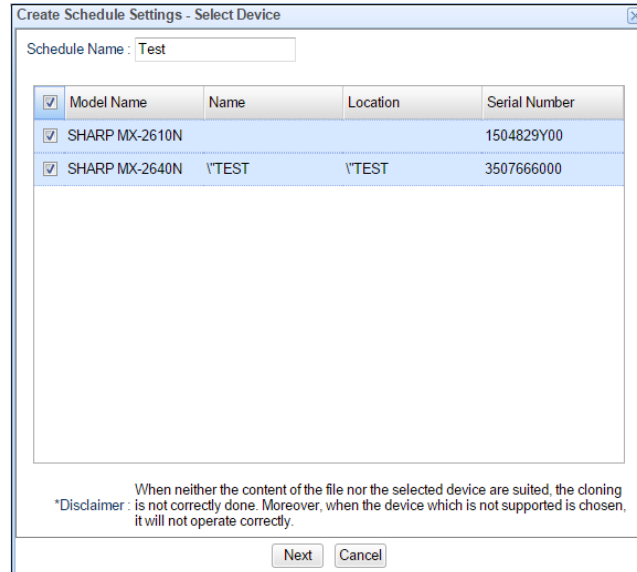
## ● Schedule List menu

If you click on the [Menu] in the [Schedule List] window, the following menu items will be displayed.

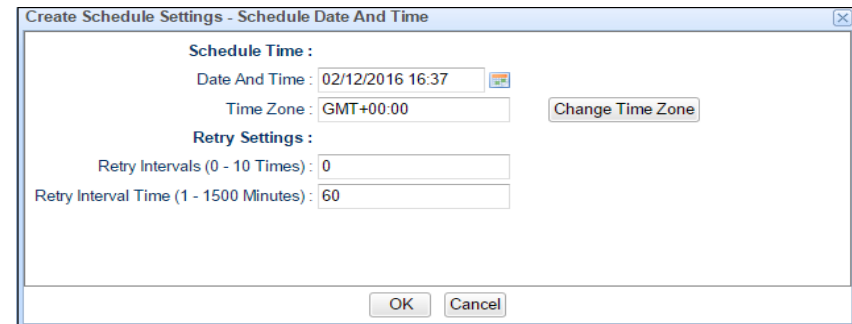
1. Create Schedule: Allows you to create a new schedule for cloning or storage backup execution. For more information, refer to [Create Schedule](#).
2. Edit: Allows you edit the selected schedule. Edit Schedule windows will be displayed with user selected values that can be updated.
3. Delete Schedule: Allows you to delete the selected schedules.

## ▪ Create Schedule

1. Select the target devices and click on Next,



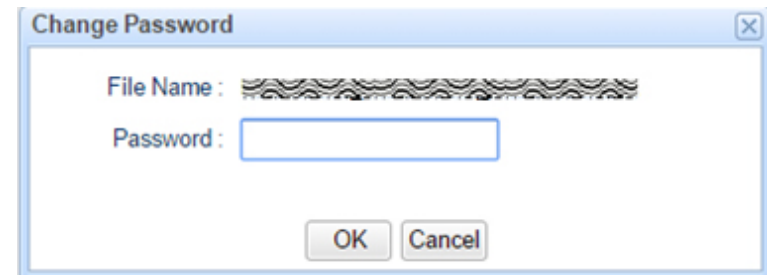
2. Create Schedule Settings-Schedule Date and Time window will be displayed.



3. Set the schedule time values, execution start date and time zone.
4. Specify Retry Interval and Retry Interval Time values.
5. Click OK.

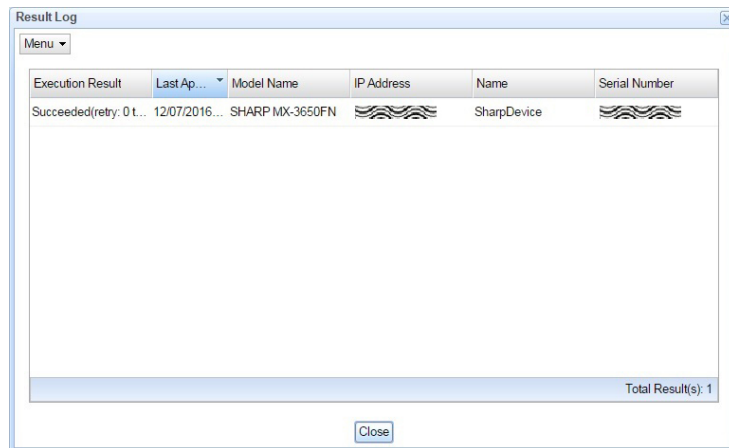
## (4) Change Password

If you click the [Change Password] button, Change Password window will be displayed. This allows you to change the encryption password of the corresponding file.



## (5) Result (Check the Results of Cloning)

If you click the [Result] button, the result log will be displayed.



### ● Result Log menu

If you click on the [Menu] in the [Result Log] window, the following menu items will be displayed.

1. Update Logs: Fetches and displays latest logs from SRDM server.
2. XML File Output: Exports/saves all the SRDM operations log data as an xml file.
3. Delete All Result Logs: Deletes all the result log data.

## (6) Download

You can download any of the available files listed in the [Device Cloning] tab by following the procedure below.

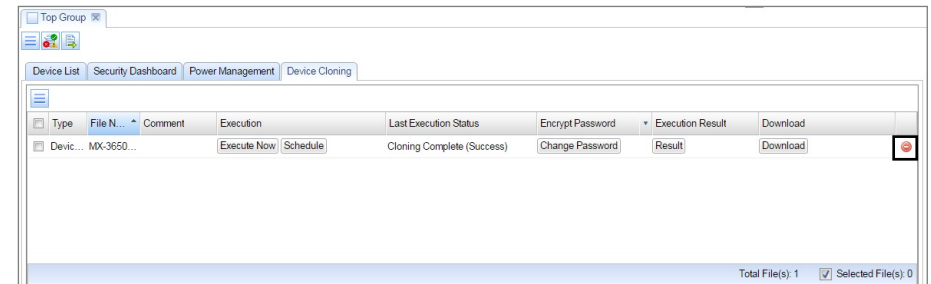
1. Click the [Download] button of the file
2. If prompted, enter the download password to continue the download operation.

## (7) Delete Icon “”

You can delete the files by any of the following procedures.


- **File delete icon:** You can use this option to delete one file at a time.

1. Click the [Delete] icon “” of the corresponding file in list.




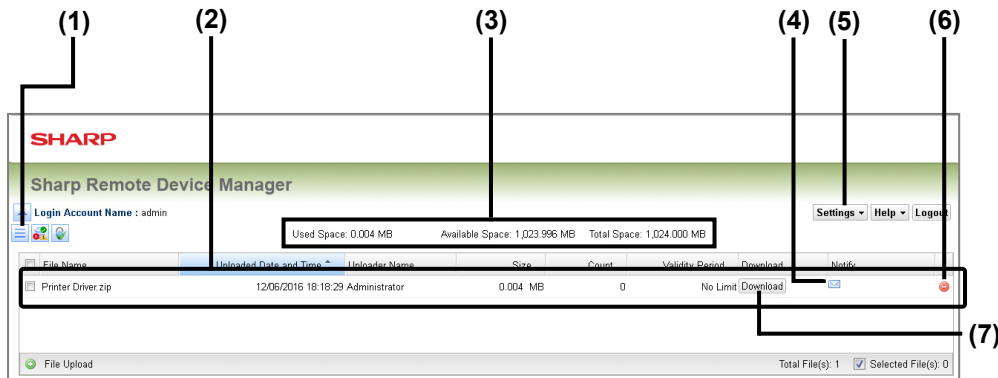
2. A confirmation message will be popped up whether to delete the file or not.
3. File will be deleted if “Yes” is clicked otherwise file will not be deleted.

- **Delete file menu option:** You can use this option to delete one or more number of files at once.

1. Select the files to be deleted from list.
2. Click the [Device Cloning] tab menu “”.
3. Click “Delete File”.
4. Click the [Yes] button on confirmation message to delete the selected files.

# FILE DISTRIBUTION FEATURE

If you click the [SRDM (File Distribution)] button  on the [Group] tab, file distribution screen is displayed. The “file distribution” allows you to share files such as MFP drivers with other SRDM users as a ZIP file.



## (1) [File Distribution] menu “ If you click the [Group] tab menu “ - Refresh: This refreshes file list with the latest information from SRDM server. - File Download: Initiates selected file download operation. For more information, refer to “[File Download](#)”. - Force Delete: Deletes all the selected files after successful authentication and refreshes the file list. - File Upload: Initiates file upload operation. For more information, refer to “[File Upload](#)”. - Operation Log: Displays log data of all file operations (Ex: Upload, download, delete etc.) performed by the users.

- View File Information: Displays selected file information like size, expiry date, uploader name, URL to download etc.
- Edit File Information: Allows you to edit the selected file information like validity period, expiry date and time, file management password and download password.

## (2) Upload File List

List of the files which are uploaded to SRDM server for distribution are displayed.

## (3) Storage Details

Displays the disk space usage information as below.

- Used Space: Amount of space used by the uploaded files in MB.
- Available Space: Amount of remaining space available for uploading the files in MB.
- Total Space: Total amount of space allocated for file distribution in MB as specified in “[Preparing to use file distribution feature](#)”.

## (4) Email Notification setting button “ You can send an e-mail notification to the users informing about the uploaded file (Ex: MFP Drivers) which can be downloaded from SRDM for their use.

Please note that SMTP server should be configured before using this feature. For more information about SMTP server configuration, please refer to “[Setting E-Mail alerts](#)”



# FILE DISTRIBUTION FEATURE

## (5) [Settings] button

When you click the [Settings] button, a menu will appear asking you to choose from Themes, Download Log, System Settings, SMTP Settings, Schedule Log Delete, and “Account Management”.

- Themes: Allow you to change the UI display theme.
- Download Log: You can download various logs generated by SRDM.
- System Settings: You can configure System Settings related with File upload operation.
- SMTP Settings: You can configure mail server settings for mail alerts. For more information, refer to “[Setting E-Mail alerts](#)”
- Schedule Log Delete: You can set the duration of log data.
- Account Management: Click to open “SRDM(Account Management)”.

## (6) Delete button “”

Deletes the selected file after successful authentication and refreshes the file list. For more information, refer to “[File Delete](#)”.

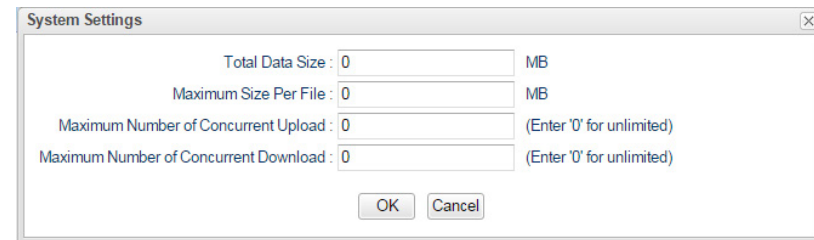
## (7) [Download] button

Initiates download operation of the file. For more information, refer to “[File Download](#)”.

## Preparing to Use File Distribution Feature

Before uploading the files, you must configure the system settings by following procedure.

1. Click the [Settings] button.
2. Click the [System Settings] button to display the System Settings dialog and configure.



Total Data Size:	0	MB
Maximum Size Per File:	0	MB
Maximum Number of Concurrent Upload:	0	(Enter '0' for unlimited)
Maximum Number of Concurrent Download:	0	(Enter '0' for unlimited)

OK Cancel

**Total Data Size:** Total size of the data users can upload to SRDM (In Megabytes)

**Maximum Size Per File:** Maximum size of a file users can upload to SRDM (In Megabytes)

**Maximum Number of Concurrent Upload:** Maximum number of file uploads operations which can be performed in parallel. Enter “0” (Zero) to allow unlimited number of upload operations in parallel.

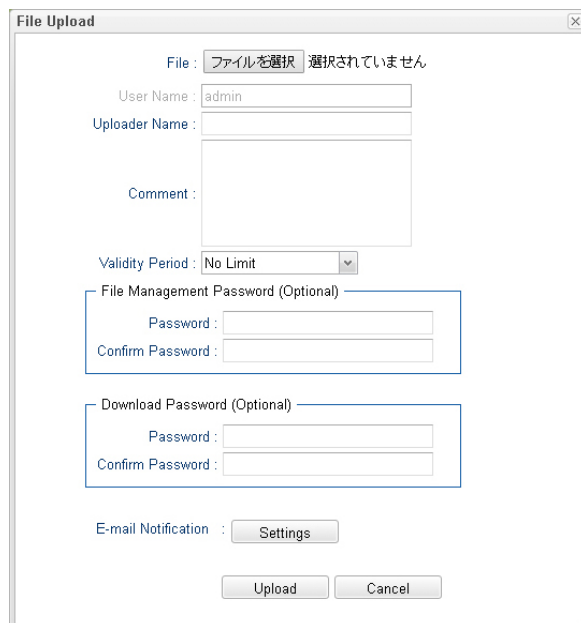

**Maximum Number of Concurrent Download:** Maximum number of file downloads operations which can be performed in parallel. Enter “0” (Zero) to allow unlimited number of download operations in parallel.

3. Click the [OK] button to save the settings.

# FILE DISTRIBUTION FEATURE

## File Upload

You can upload the files to SRDM for distribution to other users by following procedure.

1. Click the [File Distribution] menu “

3. Select the file to be uploaded and enter required information.

**Choose File:** Select the file to be uploaded.

**User Name:** Your user name will be automatically displayed.

**Uploader Name:** Enter your name.

**Comment:** Any description about the uploaded file like “MFP driver files for windows” etc. can be provided.

**File Management Password:** Password for managing the file. This password needs to be provided in below cases.

- To delete the file.
- To send e-mail notification with file information.

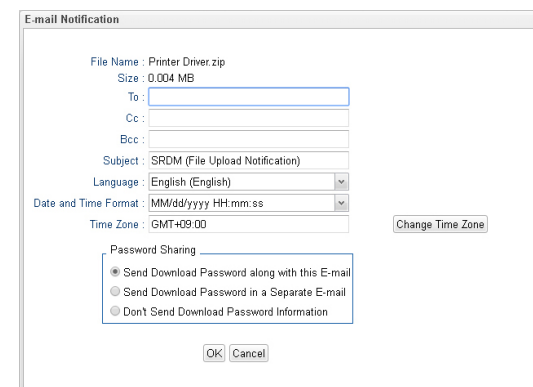
**Download Password:** Password to download the file.



You can set any file management password and download password that you wish.

**Validity Period:** Duration of the file to maintain on SRDM server before automatic delete.

**E-mail Notification:** You can send e-mail notification with information about the file, by clicking on “Settings” button as below.



After providing the information click on “OK”



SMTP server should be configured before using e-mail notification feature. For more information about SMTP server configuration, please refer to “[Setting E-Mail alerts](#)”.

4. Click on “Upload” to complete the upload operation.  
Uploaded file will be listed in the file list.

## File Download

You can download the files by any of the following procedures.

- Download from SRDM UI
  1. Access the SRDM (File Distribution) UI.
  2. Click the [Download] button of the corresponding file.
  3. Enter the file download password to start downloading.

- File Download from Email Notification

You can initiate file download operation from the received e-mail notification message by following procedure.

1. Click on the download link provided in the notification e-mail.  
Below is the sample format of the e-mail notification.

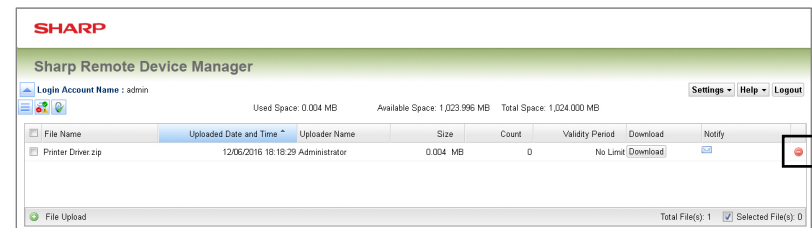

Uploaded file information is as follows:



```
Uploaded File Name      : MFP_Driver_File.zip
Uploaded Date and Time  : 12/07/2016 13:14:15
Uploader Name          : test
Validity Period        : No Limit
Comment                :
Download Link          : https://xxx.xxx.xxx.xxx:xxxx/fd/?fileId=158d77d2767987800dfsafsb6
Password               : 12345678
```

2. SRDM Login screens will be displayed using the default browser. Enter your SRDM login credentials (Login screen does not appear, if you have already logged in).
3. If a download password has been set, enter the password to start downloading.

## File Delete

You can delete the uploaded files by any of the following procedures.

- File delete icon: You can use this option to delete one file at a time.
  1. Click the [Delete] icon “The screenshot shows the 'Sharp Remote Device Manager' web interface. At the top, it displays 'Sharp Remote Device Manager' and 'Login Account Name : admin'. Below this, there are statistics for 'Used Space: 0.004 MB', 'Available Space: 1,023,996 MB', and 'Total Space: 1,024,000 MB'. A table lists files with columns for 'File Name', 'Uploaded Date and Time', 'Uploader Name', 'Size', 'Count', 'Validity Period', 'Download', and 'Notify'. One file, 'Printer Driver.zip', is listed with an upload date of '12/06/2016 18:18:29' and an uploader of 'Administrator'. A red delete icon is highlighted in the 'Notify' column for this file. At the bottom, it shows 'File Upload' and 'Total File(s): 1' with a checkbox for 'Selected File(s): 0'.

2. Enter the file management password to delete the selected file.
- Force delete menu option: You can use this option to delete one or more files at once.
    1. Select the files to be deleted from the file list.
    2. Click the [File Distribution] menu “

System administrator privileges are required in order to force delete uploaded files.

# TROUBLESHOOTING

Problem	Causes and Remedies
After starting SRDM, I entered the user name and the password, but I cannot log in	<p>Confirm the URL of the SRDM that you want to access and the user name, and check the initial password from the SRDM Service Control Panel.</p> <p><b>Note:</b> To view the initial password, launch SRDM Control Panel and click on [System] menu and select the [Administrator Password Management]. This initial password is used for logging into the default account.</p>
I entered the password, which was displayed in the “Administrator Password Management”, but I cannot log in	If you have changed the password in the UI, a password different from what was displayed in the SRDM Service Control Panel has been set. Enter the password that was set in the UI.
I cannot upload a file	Because of the limitations of the Proxy server, you might not be able to transfer large files.
I cannot login to SRDM	<p>The available space on HDD of the PC on which the SRDM server is installed might be too small. Stop the SRDM service temporarily and increase the available space on HDD (6GB or more). Then, restart the service.</p> <p>If you use the Version Up Tool, the initial password will be the one set for SRDM in the previous version.</p>
The “Communication Error(0201)” is appeared in the “Communication Status” column of the device list	An unexpected error has occurred. Please restart SRDM service.
The “Communication Error(0301)” is appeared in the “Communication Status” column of the device list	<p>There is no response from the device. It may be caused by the following reasons:</p> <ul style="list-style-type: none"> <li>- The device’s power turns off.</li> <li>- The device is disconnected from network.</li> </ul> <p>Please check availability of the device.</p>
The “Communication Error(0303)” is appeared in the “Communication Status” column of the device list	<p>A different MAC address from registered devices has been detected. It may be caused by the following reasons:</p> <ul style="list-style-type: none"> <li>- A different device is being set for the IP address of the registered device.</li> <li>- Registered device’s MAC address has been changed for some reason.</li> </ul> <p>Please execute the device discovery to solve the error. (Refer to “<a href="#">Device Discovery</a>”.)</p> <p>On DHCP (Dynamic Host Configuration Protocol) environment, the IP address will be changed dynamically. Therefore, “Communication Error(0303)” will be appeared if SRDM confirms the devices status after the IP address has been changed. The scheduled device discovery is recommended on DHCP environment. (Refer to “<a href="#">Setting scheduled actions</a>”.)</p>

## Schedule Maintenance

SRDM database files become larger after a period of use. The database file does not become smaller even when data is deleted from the database. In addition, when the size of the database file becomes large, it can have an effect on the performance of SRDM, for example by slowing down the display of SRDM pages. By optimizing the database, you can reduce the size of the database file and improve the performance of SRDM.

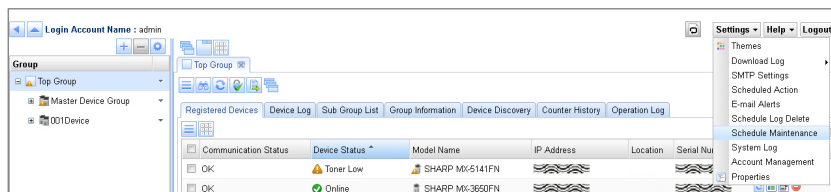
With SRDM, the scheduled maintenance function can be used to automatically schedule optimization of the database file.



- Optimization does not compress the data; what it does is delete unneeded records in order to make the size of the database file smaller.
- If the amount of free space on the hard disk drops below 6 GB, the SRDM service will stop and logging in will not be possible.

Scheduled maintenance can be set by following the procedure below.

1. Click the [Settings] button, and then select [Scheduled Maintenance] from the menu.



2. Select the [Execute Scheduled maintenance] check box, and then enter the required information in the form.

- Time Zone: This sets the time zone. To change the setting, click the [Change Time Zone] button, and then select the applicable time zone from the list.

3. Start Date: This sets the date when the scheduled maintenance is to start. You can also click the calendar icon "📅" and select the date from the calendar.
  - Recurrence: This sets the timetable for running the scheduled maintenance. If you select "Every Week", check boxes will be displayed for you to select the days of the week. You can select more than one weekday at the same time.
  - Execute Time: This sets the time of the day to carry out the scheduled maintenance.
4. If you would like to be notified of the results of scheduled maintenance, select the "Notify Result by E-Mail" check box, and enter the required details.
    - E-mail address: This sets the destination e-mail address for sending the e-mail containing the results of the scheduled maintenance.
    - Language Setting: This sets the language to be used for the e-mail containing the results of the scheduled maintenance.
    - Date and Time Format: This sets the format for the date and time appearing in the e-mail containing the results of the scheduled maintenance.
  4. Click the [OK] button.



In order to send e-mails containing the results of scheduled maintenance, you need to configure SMTP server settings beforehand. For more information on SMTP settings, refer to "Setting E-Mail alerts".

### Case1: Login and Adding User Accounts with Default Account

When you login to SRDM with the default account ("admin"), you can use SRDM with administrator privileges.

#### ■ Login with Default Account ("admin")

When you start using SRDM, you first log into SRDM using the default "admin" account.

(Refer to "[Launching SRDM](#)" section for the login procedure using the default "admin" account)

When you login with the default account, following permissions are available.

- Group Management
- System Management
- File Distribution
- Security Dashboard
- Device Cloning
- Power Management
- Account Management

For more information on registering accounts, refer to "[Account Management](#)".

#### ■ Logging in using the "user" account

When you log into SRDM using the default "user" account, you can use SRDM as a user who is allowed to view the information for devices which have already been registered.

# APPENDIX

## Permission details

SRDM places limits on functions by means of permissions. Functions which cannot be used are not displayed in the UI or cannot be operated. Granting or removing the permissions can be done when accounts are created or when accounts are edited. If no permissions have been applied, only viewing of data will be possible. The following items will be displayed when group management permission is granted.

Group pane	Buttons	Create Group button		
		Delete Group button		
		Group Settings button		
		Group menu button		
Group tab	Buttons	Menu button		
		Discovery button		
		Device Information Update button		
	Tabs	[Registered Devices] tab	Menu button	Update Device Information
				Delete Device
			Device operation	Device Trash Can
				Device Information Update button
		Device Web Page button		
		Remote Operation button		
		[Device Log] tab	Menu button	Device delete button
				XML File Output
		[Sub Group List] tab	Menu button	Delete All Device Logs
				Properties
				Create
				Delete
		[Group Information] tab		Group Trash Can
[Device Discovery] tab	Menu button	Register		
		Delete From List		
[Counter History] tab				
[Operation Log] tab	Menu button	XML File Output		
		Delete All Operation Logs		

# APPENDIX

[Device] tab	Buttons	Device Information Update button		
		Device Web Page button		
		Remote Operation button		
	Tabs	[Device Status] tab	Menu button	Device Web Page Remote Operation
		[Device Information] tab	Menu button	Device Information Update Device Web Page Remote Operation Download Counter Data
		[Device Log] tab	Menu button	XML File Output Delete All Device Logs
		[SNMP Settings] tab	Menu button	SNMP Settings
		[Counter History] tab	Menu button	Default XML File Output
		[Operation Log] tab	Menu button	XML File Output Delete All Operation Logs
		[Settings] button	Themes	
	Schedule Settings			
	E-Mail Alerts			
	Properties			

The following items can be displayed when system management permission is granted.

[Settings] button	Download Log
	SMTP Settings
	Schedule Log Delete
	Scheduled Maintenance
	System Logs



# APPENDIX

The following items will be displayed when file distribution permission is granted.

[Group] Tab	button	SRDM (File Distribution) button

The following items will be displayed when security dashboard permission is granted.

[Group] Tab	button	SRDM (Advanced Features ) button
SRDM (Advanced Features) Screen	Tab	[Security Dashboard] Tab

The following items will be displayed when device cloning permission is granted.

[Group] Tab	button	SRDM (Advanced Features ) button
SRDM ( Advanced Feature) Screen	Tab	[Device Cloning] Tab

The following items will be displayed when power management permission is granted.

[Group] Tab	button	SRDM (Advanced Features ) button
SRDM (Advanced Features) Screen	Tab	[Power Management] Tab

The following items will be displayed when account management permission is granted.

Setting button	Button	Account Management button
Account Management window	Tab	[Account List] tab
		[Role List] tab

# APPENDIX

## Icons displayed in device images

Icons showing the status of a device are displayed along with the device image in the [Device Status] tab.











Status other than “Online [Auto Power Shut Off]”, warm-up and online can be set to show at different levels (Normal, Warning, Error). For more information, refer to [“Changing the conditions for icon display”](#).

The device status corresponding to each icon are as follows.

Status name	Icon		
	Normal	Warning	Error
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			

Status name	Icon		
	Normal	Warning	Error
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			

# APPENDIX

Status name	Icon		
	Normal	Warning	Error
Printer Warning [Output tray missing]			
Near Overdue Service Maintenance			
Online [Auto Power Shut Off]			
Warm-Up			
Online			
Unknown			

**SHARP®**

SHARP CORPORATION