



# KMnet Policy Manager

User Guide



## Legal Notes

Unauthorized reproduction of all or part of this guide is prohibited.

The information in this guide is subject to change without notice.

We cannot be held liable for any problems arising from the use of this product, regardless of the information herein.

## Regarding Trademarks

Microsoft®, Windows®, and Active Directory® are registered trademarks of Microsoft Corporation in the U.S. and/or other countries.

All other brand and product names herein are registered trademarks or trademarks of their respective companies.

Examples of the operations given in this guide use the Windows 7 printing environment. Essentially the same operations are used for Microsoft Windows Vista, Windows XP, Windows Server 2008, and Windows Server 2003.

# Table of Contents

## Chapter 1 Policy Manager

---

## Chapter 2 Starting Policy Manager

---

Setting Up the Server from the Printing System .....	2-1
Enabling SSL on the Device .....	2-2
Specifying the Spooler Port on the Client PC .....	2-2
Adding a Spooler Port .....	2-3
Setting Up the Spooler from the Admin Console-Spooler .....	2-3
Options .....	2-4
Setting Options .....	2-4
Register Devices .....	2-5
Registering Devices .....	2-6

## Chapter 3 Policy Manager Organization

---

Main Menu .....	3-1
File Menu .....	3-1
Edit Menu .....	3-2
Manage Menu .....	3-2
Help Menu .....	3-3
Policy Context Menu .....	3-4
Domain, Organization Unit, or Local Context Menu .....	3-4
Hierarchical List .....	3-4
Views .....	3-5

## Chapter 4 Policy Management

---

Policies Tab .....	4-1
Predefined Policies .....	4-2
Creating a Policy .....	4-2
Adding Filters .....	4-3
Adding, Editing, or Removing a Domain .....	4-3
Assigning Policies .....	4-4
Viewing or Editing Policies .....	4-4
Deleting a Policy .....	4-4

## Chapter 5 User Management

---

Creating a New Local User .....	5-1
Viewing or Editing User Properties .....	5-2
Deleting a User .....	5-2

## Chapter 6 Group Management

---

Creating a New Local Group .....	6-1
Adding Members to a Group .....	6-2
Editing or Viewing Group Properties .....	6-2

---

Deleting a Group .....	6-3
------------------------	-----

## **Chapter 7 Users or Groups Search**

---

Searching for Users or Groups .....	7-1
-------------------------------------	-----

## **Chapter 8 Access Log**

---

Viewing the Access Log .....	8-1
Searching on the Access Log .....	8-1
Exporting the Access Log .....	8-2
Clearing the Access Log .....	8-2

## **Chapter 9 Admin Console-Spooler**

---

Admin Console-Spooler Toolbar .....	9-1
Print Jobs Current View .....	9-1
Searching for Print Jobs .....	9-2
Spooler Print Jobs List .....	9-2
Spooler Print Job Context Menu .....	9-3
Print Job Properties .....	9-3
Viewing Print Job Properties .....	9-4
Configuring Spooler Settings .....	9-4

## **Chapter 10 Client Viewer**

---

Policy Manager Server Connection .....	10-1
Opening a Connection to the Policy Manager Server .....	10-1
Client Viewer Toolbar .....	10-1
Print Jobs Current View .....	10-2
Searching for Print Jobs .....	10-2
Client Print Jobs List .....	10-3
Print Job Context Menu .....	10-3
Print Job Properties .....	10-4
Viewing Print Job Properties .....	10-4

# 1 Policy Manager

Policy Manager can be used with a variety of printing systems supporting network authentication and authorization. It extends Microsoft® Active Directory® authentication for printing systems and provides secure private printing. With Policy Manager, an administrator can authenticate and authorize usage by user and organizational units for security and cost control. The application manages policies, domain groups and users, and local groups and users without affecting existing domain settings.

## **Identification and Authorization**

Identification and authentication require each user to have a unique identity and provides the proof procedure for verifying that the user is the individual they claim to be. Based on system settings, users can be identified and authenticated using Windows domain accounts, local Policy Manager accounts, as well as ID cards.

## **Access Control**

Device access control provided by Policy Manager enables centralized user access control management for all participating printing systems, letting only those authorized use or configure them.

## **Logging**

Policy Manager provides centralized end user access logging. This gives a system administrator a detailed overview of each user's access on all connected printing systems.

## **Secure Job Release**

Using the job spooler service, users can send jobs securely to the spooler server. They can then log in to a printing system connected to the Policy Manager authentication server and release their jobs. Installation of the secure job release feature is optional. Policy Manager can be used as an authentication and authorization solution without the job spooler server.

## **Network Security**

Policy Manager ensures that sensitive user information is securely transported between printing systems, Policy Manager, and domain directories. Policy Manager can lock user accounts when excessive unsuccessful login attempts are detected, and terminate a communication session after a certain period of inactivity.

## **Print Job Security**

Policy Manager provides print job security in several ways. Print jobs are transmitted to the job spooler server over SSL and stored using industry standard AES 256 encryption. Jobs are sent securely to the printing system using IPPS. Communication between the Client Viewer and the job spooler server is over HTTPS only.

## **Database Security**

All information stored in the database is securely encrypted, and domain passwords are never stored on the printing system or the Policy Manager server.

## 2 Starting Policy Manager

At startup, Policy Manager requires a **User name** and **Password**. For initial login, use “Admin” as the default for both.

For successive logins, use any login name or password set up in Policy Manager that has an effective policy of **Permit** in the **Server administration** option.

- 1 Open Policy Manager.
- 2 Type the **Server** name, or click **Refresh** to list in the **Server** text box all of the servers found on the network from which you can select.
- 3 Type the **User name** and **Password** (maximum of 64 characters for each) in the text boxes displayed. Or, click **Use Windows authentication** to use your Microsoft Windows account as the login.
- 4 Click **Log in**. If the login is successful, the application opens. If the login fails, an error message appears. If the number of failed login attempts exceeds what is specified for **Number of failed logins before account is locked** in **Options**, the user account is locked and the system administrator is notified by e-mail.  
  
The **Trial version** dialog box is displayed when you first log on to Policy Manager, or if you have not activated the server. It will display the number of days remaining for your 90-day free trial period.
- 5 Click **Continue trial**, or activate your license by typing the **Server license key** and clicking **Activate**. After activating the license key, it is necessary to register the device by using **Manage > Registered devices** in the main menu. When the device is registered, then the device’s authentication method automatically switches to network authentication. If you need to obtain a license key, click **Copy** to copy the **Machine number** of your computer to the Clipboard. You will need to provide this number in order to obtain a license from your sales representative.

### Setting Up the Server from the Printing System

You can set up the server using the device’s operation panel.

- 1 Press **System Menu**.
- 2 Press **User Login / Job Accounting**.
- 3 For **User Login Setting**, press **Next**.
- 4 For **User Login**, press **Change**.

- 5 Press **Network Authentication**.
- 6 For **Server Type**, press **Ext**.
- 7 Select a domain from the **Default Domain** list.
- 8 In the **Host Name** text box, type the host name or IP address of the computer where the Policy Manager server is installed.
- 9 In the **Port** text box, use the numeric keypad to type the same port number specified during installation (the default port is 9093).
- 10 To save the settings, press **OK**.

## Enabling SSL on the Device

You can set up network authentication using the printing system's operation panel. SSL must be turned on for Policy Manager to operate.

Printing also requires an Internet Printing Protocol (IPP) server for handling requests from IPP client devices. IPP over SSL is used for the Secure Job Release feature and to provide secure communication.

To enable this function, the IPP settings must be made as follows.

### IPP setting

Port number: 631

### IPP over SSL setting

Port number: 443

See the Operations Guide for your printing device for the procedure to enter or check these settings.

## Specifying the Spooler Port on the Client PC

The spooler port replaces the standard TCP/IP printer port and redirects print jobs to the spooler server.

To select an existing printer port:

- 1 Click **Start > Devices and Printers**.
- 2 Right-click on a printer and select **Printer properties**. Depending on your Windows settings, you may be prompted to log in before you can access printer options.
- 3 Click the **Ports** tab, and select **Spooler Port** from the list. You must previously have added the **Spooler Port** for it to appear in the list.
- 4 Click **Configure Port** to change the configuration of the selected existing port.
- 5 In the **Port Configuration** dialog box, your available options are displayed:  
**Port name**

The port name is read-only and cannot be modified. This is the port name specified when the port was previously added.

**Server address**

Type the full server address, including the port number of the spooler server.

You can also click **Refresh** to search for servers. The search results appear in the **Server address** list. The server address is displayed as *host name:port*.

Click **OK** to save your settings. The spooler port is added to the list of ports in Printer Properties.

## Adding a Spooler Port

To add a new spooler port:

- 1 Click **Start > Devices and Printers**.
- 2 Right-click on a printer and select **Printer properties**.
- 3 Click the **Ports** tab.
- 4 Click **Add Port**.
- 5 In the **Printer Ports** dialog box, select the **Spooler Port** from the **Available port types** list box. Then click **New Port**.
- 6 In the **Port Configuration** dialog box, enter the following information:

**Port name**

Type a name to identify the port in the port list. The default name is Policy Manager.

**Server address**

Type the full server address, including the port number of the spooler server.

You can also click **Refresh** to search for servers. The search results appear in the **Server address** list. The server address is displayed as *host name:port*.

Click **OK** to save your port configuration settings. The spooler port is added to the list of ports in Printer Properties.

## Setting Up the Spooler from the Admin Console-Spooler

To set up the spooler from the Admin Console-Spooler:

- 1 In the menu, click **Manage > Set up spooler**.
- 2 In the **Spooler Setup** dialog box, select **Enable spooler server**. If selected, this check box provides the option to search for spooler servers in the network and connect to them. If the check box is clear and **OK** is clicked, any existing connection to the spooler server is deactivated.

- 3 Type the full server address, including the port number. Alternatively, click **Refresh** to list in the **Server** text box all of the spooler servers found on the network.
- 4 Click **OK** to validate the connection to the server. If the connection is successful, the dialog box closes. If a connection cannot be made, an error message appears.

## Options

The **Options** dialog box provides settings for:

- Mail server e-mail connections
- Failed login notification
- Access log backup
- Schedule for clearing access log
- ID card authentication

### Setting Options

In the **Options** dialog box, you can specify settings for system functions.

- 1 In the main menu, click **Manage > Options**.
- 2 The **Mail** section shows your available options:
  - Host**  
Type an SMTP server name.
  - Port**  
Type an SMTP server port number (valid range is from 1 to 65535).
  - Require authentication**  
Click this check box if you want to specify a **User name** and **Password** login for the SMTP Server.
  - Sender name**  
Type the name of the e-mail sender. The default is **Administrator**.
  - Receiver e-mail address**  
Type the e-mail address of the recipient.
  - Test connection**  
Click **Test connection** to verify that the **Mail** settings are correct.  
If unable to connect to the mail server, an error message appears. Review the **Mail** settings and make sure they are correct. If connection is made, a message is displayed.
- 3 Click **Access** to expand this section.
  - Number of failed logins before account is locked**  
Type the maximum number of failed login attempts within a period of 2 minutes before the user account is locked. When the number is exceeded, the user account is locked and the system administrator is notified by e-mail.

The value is a count of failed logins from all printing systems (valid range of attempts is 3 to 50).

**Subsequent delay before unlocking account (minutes)**

Type the number of minutes for the amount of time that the system must wait before automatically making the account available for logging on (valid range is 0 to 30 minutes). If set to 0, the administrator must manually unlock all accounts by clicking **Manage > Unlock all accounts**.

**4** Click **Access log backup** to expand this section.

**Backup interval (days)**

Type the number of days (between 1 and 30) before the user access log is automatically backed up. The default is 7 days. The first access log backup will occur after the initial number of days specified in this text box.

**Backup location**

Policy Manager displays the location where the access log is stored. This location cannot be edited.

**Access log backup file name**

Type a filename for the access log. The file must be in .XML format.

**Clear access log after backup**

Removes all entries in the access log after a backup is completed.

**Use time stamp**

Adds a time stamp to the filename to distinguish it from other backup files and to provide overwrite protection.

**5** Click **Access log clear** to expand this section.

**Clear access log schedule**

Select a schedule for clearing the access log: **Daily**, **Weekly**, **Monthly**, or an **Interval in days**. Specify the **Time**, **Day**, **Date**, or **Days** for the schedule selection.

**Export access log before clearing**

Select this option to automatically save the access log before removing it from the Policy Manager database.

**6** Click **ID card authentication** settings to expand this section.

**ID card authentication**

Select one method for ID card authentication. **ID card only** requires the user to use an ID card at login. **ID card and password** requires the user to both use an ID card, and type a password at login.

---

**Note:** The printing system setting must match the Policy Manager ID card authentication setting. In the printing system's operation panel, the setting is a **Password Login** option that must be set to **On** or **Off**, depending on the selected setting in Policy Manager.

---

## Register Devices

Before you can register devices on the server, you must first enter the license key for the server in the **Licensing** dialog box that appears after logging on to Policy Manager.

You can use the **Registered Devices** dialog box to view or delete registered devices, or to search for devices that you want to register. If you want to add more devices than allowed under your license, you need to replace the license with one supporting a larger number of devices. You cannot activate a license key with fewer supported devices than the one previously activated.

Devices configured on the server before you activate a license will not be included in the total number of supported devices. For example, if your license supports 50 devices and you already have 30 devices configured, then only 50 devices will be supported, not 80 devices.

## Registering Devices

You can use the **Registered Devices** dialog box to view or delete registered devices, or to search for devices that you want to register on the Policy Manager server. You can register devices up to the total number allowed under your license.

To view or delete devices with an activated license:

- 1 Click **Manage** in the toolbar, then select **Registered devices**.

### Serial number

The unique number that identifies the specific device.

### Model name

The model name of the device.

### Address

The IP address for the device (for example, 10.10.11.104).

### Host name

The host name for the device.

The **Registered Devices** dialog box enables you to search for devices you want to register (up to the allowable limit). You can also move column headers by dragging them to the desired location in the column header bar.

- 2 To delete a device from the list of registered devices, select the device in the list, then click the **Delete devices** icon in the toolbar. A confirmation dialog box appears. Click **Delete**.
- 3 When finished viewing or deleting registered devices, click **Close**.

## Searching for Devices to Register

The **Registered Devices** dialog box enables you to search for all devices on the network, for a specified IP address, or for a range of IP addresses. The search will only occur if the number of registered devices on the network is fewer than the total allowable number displayed in the lower left corner of the dialog box. You can register up to the total number of allowable devices for a server license.

To search for devices you want to register, follow these steps:

- 1 In the **Registered Devices** dialog box, click the **Discover devices** icon in the toolbar.  
The **Device Discovery** wizard is displayed.

- 2** On the **Select discovery method** page, select how you want to search for devices to be registered:

**On your local network**

Search for all devices on the local network by selecting **IPv4** or **IPv6** (the default is IPv4).

**By IP address**

Search for devices by entering their IP addresses (v4 or v6) or host names.

**By IP address range**

Search for devices by entering a range of IP addresses (v4 or v6).

Click **Next**.

If searching by IP address or host name, the **Specified address discovery** or **Specified address range discovery** page is displayed. If searching for all devices on the local network, then the **Select discovery method** page is displayed.
- 3** To search for all devices on the local network, on the **Select discovery method** page select the type of discovery to use: **IPv4** or **IPv6** (the default is IPv4). Then click **Next**.
- 4** To search for devices by IP address, on the **Specified address discovery** page type the **IP address or host name** in the text box. This address identifies where Policy Manager is installed (for example, 10.10.50.50). Click **Add**. The device IP addresses you enter appear in the **Selected targets** list. You can also click **Import** and the **Open** dialog box appears where you can select a valid .CSV file. After clicking **Open**, the device addresses or host names in the .CSV file are added to the **Selected targets** list on the **Specified address discovery** page. Click **Next**.
- 5** To search for a range of devices, on the **Specified address range discovery** page enter the **Starting IP address** and the **Ending IP address**, using a maximum of 10 ranges. Click **Add**. The IP address range appears in the **Selected network segments** box. Click **Next**.
- 6** Enter the communication settings for the devices:

**Communication timeout (seconds)**

The number of seconds the application will try to establish a connection with the device.

**SNMP communication retries**

The number of retries to establish communication with the device after a communication failure.

**Use SNMPv1/v2**

Type the **Read community** name for the device that will be used in requesting information. Type the **Write community** name for the device to be used for changing its configuration. The **Read community** and **Write community** are sent with all SNMP receive and send requests, and must match the community values on the device.

**Use SNMPv3**

Type a **User name** and **Password** set on the device.

Click the **Authentication** check box and select the **HASH** method (MD5 or SHA1). Click the **Privacy** check box and select an **Encryption** method (DES or AES).

When finished entering communication settings information, click **Next**.

- 7** Type the **Login user name** in the **Administrator login** text box, then type the **Login password** in the **Administrator password** text box up to a maximum of 64 characters. Next, choose the **Authentication mode switch**, which defines the type of user authentication on the device. Select **Use local authentication** or **Use settings on the device** for the authentication mode.
- 8** When finished entering communication settings information, click **Next**. The **Confirm discovery** page is displayed that shows your selections.
- 9** Click **Discover** to begin discovering devices, or click **Back** to change any of the communication settings. The **Select devices for registration** page is displayed that lists all devices on the network and their status. To display all of the devices on the network, click the **Show all devices** check box.
- 10** Select one or more devices in the list with a “Supported” status, but no more than the maximum allowable by the license. Click **Register**. If incorrect authentication settings were entered on the **Communication settings** page, then an “Authentication error” status is displayed for the device. Click **Close**. The registered devices will now appear in the **Registered Devices** dialog box.

# 3 Policy Manager Organization

Policy Manager screen components are organized to help the administrator quickly and efficiently manage authentication. The main screen is composed of the application menu, and left and right panes. The hierarchical list in the left pane lets an administrator quickly navigate between organizational units and policies. The view pane on the right changes according to the selection in the hierarchical list.

## Main Menu

The main menu is located in the upper left corner of the screen. Basic operations you can perform in Policy Manager are in this menu. The menu operates like a standard Microsoft Windows application menu. The main menu options are: **File**, **Edit**, **Manage**, and **Help**.

## File Menu

The **File** menu provides options for moving data into and out of Policy Manager.

### **Back up database and settings**

Saves a copy of the Policy Manager database, access logs, and settings. The backup file is saved with the default extension of .KAA.

### **Restore database and settings**

Retrieves a previously saved Policy Manager backup file. The restored database overwrites the current one. Always save the current database before opening another one.

### **Import ID card information**

Reads ID card information from the user-specified .CSV file. Policy Manager then attempts to find the matching login user name and domain in the database or the Active Directory. If a match is found, the user's ID card information is overwritten with the information from the file. The file contains the following: login user name, domain, and ID card information.

### **Import account IDs**

Reads account ID information from the user-specified .CSV file. The application then attempts to find the matching login user name and domain in the database or Active Directory. If a match is found, the user's Account ID information is overwritten with the information from the file. The file contains the following: login user name, domain, and account ID information.

### **Export access log**

An access log entry is automatically generated and saved whenever the Policy Manager service receives an authentication request from a printer device. The user access logs are exported to a file in .XML or .CSV format.

### **Open connection**

Lets you log in to the Policy Manager server.

**Exit**

Closes and exits Policy Manager.

**Edit Menu**

The **Edit** menu provides tools for managing information in the Policy Manager database.

**Undo, Cut, Copy, Paste, Select all**

These options match the standard Microsoft Windows editing tools.

**Refresh**

Updates the data of the currently selected item in the hierarchical list or view.

**Properties**

If a user or group is selected in the left view pane, opens a dialog box that displays information about the selection. This information can be edited for local users and groups. The **User Properties** dialog box shows **General**, **Account**, **Effective policy**, **Group membership**, and **ID card** information. The **Group Properties** dialog box shows the **Group name** and the **Members** list.

**Delete (policy, group, user)**

Removes the selected local user, local group, or policy from the database. When an organizational unit is selected in the left view pane, the policy link is deleted. You can delete single or multiple selections of a single object type. The specific type of deletion appears in the Delete option (for example, **Delete group**).

**Delete job**

In the Spooler view, **Delete job** lets you delete jobs that have Ready status when **Active** or **All** jobs is selected in the jobs list. You can also delete jobs by highlighting the jobs in the list and clicking the delete icon in the toolbar, or right-clicking on a job in the list and selecting **Delete job** from the context menu.

**Search**

Moves the cursor to the **Search text** box in the **Users** tab, **Groups** tab, or the **Spooler view**. **Search** reviews the list in the view pane and displays the found matches.

**Manage Menu**

The **Manage** menu provides options for creating, editing, and viewing data, or controlling the operations of Policy Manager. (Note that the options displayed in the File menu may vary depending on your selections in the left view pane.)

**New policy, New local group, New local user**

Used to create a new local user, group, or policy depending on the contents of the view pane.

With **Local** selected in the left pane, the subject of the view pane tab is the displayed menu option. For example, if the view pane shows the **Users** tab, the **Manage** menu reads **New local user**.

**Assign policy**

Available if a domain, organizational unit, or **Local** is selected in the left pane. In the **Assign Policy** dialog box you can apply a policy to domains or organizational units.

**Add filter**

With a policy selected in the left pane, use **Add Filter** to narrow the printing privileges for **Groups** or **Users**. You can also apply the search filter to domain or **Local** groups or users, or both, by selecting **All**. Search for groups or users by clicking the magnifying glass icon in the toolbar.

#### **Registered devices**

You can view or delete registered devices in the **Registered Devices** dialog box. You can use the **Delete devices** icon in the toolbar to delete registered devices, or you can search for devices to register by clicking the **Discover devices** icon.

#### **Set up spooler**

Enables you to specify the spooler port by typing the full server address, or by searching for spooler servers on the network. You can then test the connection.

#### **Spooler settings**

Enables you to change **Mail settings**, **Job settings**, and **SNMP settings**.

#### **Unlock all accounts**

Restores access to all users who made more login attempts than the maximum number specified in the **Options** dialog box.

#### **Show access log**

Displays the user access log. Records are posted to this log every time printer device makes an authentication request to Policy Manager.

#### **Clear access log**

Removes all entries in the access log from the Policy Manager database. Exported entries in the access log are not affected.

#### **Purge historical jobs**

Permanently removes all the Released, Expired, and Deleted print jobs. This option is available when the current view is **Released jobs**, **Expired jobs**, or **Deleted jobs**.

#### **Add domain**

Opens the **Add New Domain** dialog box.

#### **Edit domain**

Opens the **Edit Domain** dialog box where you can change the domain's user credentials.

#### **Remove domain**

Enables you to remove a domain from Policy Manager. A confirmation dialog box appears before removal.

#### **Options**

Enables the administrator to configure system settings and backup settings.

### **Help Menu**

The **Help** menu provides access to user assistance, and information about Policy Manager.

#### **KMnet Policy Manager Help**

Provides access to Policy Manager user assistance topics.

#### **Kyocera Mita Online**

Opens a web browser and links to <http://www.kyoceramita.com> for more information. This link may change depending on the locale.

### About KMnet Policy Manager

Opens the **About** dialog box for the Policy Manager software. It shows the name, version and copyright information.

## Policy Context Menu

Policy Manager handles authentication by defining policies for users.

To open the policy context menu, right-click a policy in the left pane.

#### Add filter

Opens the **Add Filter** dialog box that lets you add a local or domain user, or group, as a filter for the selected policy. This selection is not available for the **Other** policy.

#### Delete policy

Enables you to remove a selected policy from Policy Manager. A confirmation dialog box appears before the policy is deleted. This selection is not available if **Apply** is enabled in the **Policy >Properties** view. The policies for **Administrator** and **Other** cannot be deleted.

#### Refresh

For a selected policy, the policy information is refreshed in the right pane.

## Domain, Organization Unit, or Local Context Menu

Right-click a domain, any organizational unit, or **Local** in the hierarchical list to open this context menu. Note that **Edit domain** and **Remove domain** are unavailable for the default domain.

#### Assign policy

Opens the **Assign Policy** dialog box for assigning policies to the selected domain, organizational unit, or **Local**.

#### Refresh

Refreshes the information displayed for a selected domain, organizational unit, or **Local**.

#### Add domain

Opens the **Add New Domain** dialog box where you can provide information for creating a new domain.

#### Edit domain

Opens the **Edit Domain** dialog box where you can change the domain's user credentials.

#### Remove domain

Removes a selected domain from Policy Manager. A confirmation dialog box appears before the domain is deleted.

## Hierarchical List

Policy Manager objects shown in the hierarchical list are **Policies**, domains (the names of local domains accessible by browsing), **Spooler**, and **Local**. Objects (domains, organizational units, and **Local**) with assigned policies that are not inherited are identified with a different icon.

#### Policies

This is the default selection in the hierarchical list. **Policies** can be expanded to show all individually-added policies. With **Policies** selected in the hierarchical list, the list of policies is also displayed in the view pane.

#### **Domain**

This list displays information from the Active Directory. Select a domain or organizational unit, and then a tab to display the following in the view pane:

The **Policies View** lists all the inherited and assigned policies to this organizational unit.

The **Groups View** lists groups under the selected domain or organizational unit.

The **Users View** lists users under the selected domain or organizational unit.

#### **Local**

Manages local groups and local users. **Local** does not have subordinates.

#### **Spooler**

Manages the printing devices on the Policy Manager spooler server.

## Views

In the hierarchical list, you can view or edit properties, groups, and users if a domain, **Local**, or any of the subordinates is selected.

#### **Policies View**

This view is the current view, if **Policies** or any of its subordinate policies is selected in the hierarchical list.

#### **Domain or Local View**

There are several tabs available:

##### **Policies**

View the policy with the highest priority (top of the list).

##### **Groups**

View and edit group properties.

##### **Users**

View and edit user properties.

## 4 Policy Management

Device restrictions are set by creating policies, assigning them to organizational units, and then creating filters to narrow them down to users or groups. These steps are the same as for any other Active Directory policy, with the exception that the policies and filters are stored on the Policy Manager server instead of the Active Directory server.

The overall method for managing policies is to first create applicable policies, and then to apply them as needed. Policies can be created and applied in various ways. For example, an administrator might choose to apply all or most of the policies at the domain or **Local** level, and have specific users and groups as filters in the policy. Or, the administrator might apply the policy to a very specific organizational unit, and not use filters.

If **Policies** is selected in the hierarchical list, the view pane displays the list of predefined and user-defined policies. **Administrator** and **Other** are predefined policies that cannot be deleted. Using this **Policies** view, user-defined policies can be added, edited, deleted, or filters can be assigned. The total number of policies and the number of selected policies in the list is shown in the lower left corner of the window.

### Policies Tab

The **Policies** tab for organizational units contains lists of **Assigned policies** and **Inherited policies**. They are used to calculate the effective policy for a user who belongs to the selected organizational unit. These lists show policies in order of precedence. The policy at the top of the list has the highest priority.

Use the **Policies** tab to view or edit the **Assigned policies**, or to view the **Inherited policies**.

Use the **Inherited policies** list to show all the inherited policies for the selected organizational unit. **Administrator** and **Other** policies are predefined policies that stay at the bottom of the list, since they are the fallback policies with the lowest priority.

The policies listed in the **Assigned policies** list have higher priority than those listed in the **Inherited policies** list. Select a policy and use the arrow buttons to move a policy up or down in priority.

A policy is considered for the user, if it has no filters, or the filter list includes the user, or if it includes the group that the user belongs to.

To calculate the effective policy, the application first determines if a policy is valid for the user, starting with the highest priority policy from the **Assigned policies** list. When the first valid policy is found, all settings except the **Not configured** settings from that policy will be part of the effective policy for the user. The application then searches through the list of **Assigned policies** attempting to set **Not configured** settings. If after searching the **Assigned policies** list the effective policy has not been fully calculated, the **Inherited policies** list is searched.

The effective policy is calculated when all the policy settings have a value other than **Not configured**.

## Predefined Policies

Policy Manager provides two default policies:

### Administrator

The **Administrator** policy is assigned to the Policy Manager administrator account and grants the right to change Policy Manager configurations and settings. This policy cannot be edited or deleted.

The **Administrator** policy is assigned to **Local**. It always contains the default local user **Server Administrator** in the filter, and allows the assigning or unassigning of any user. By default **Server administration** is set to **Permit**, **Access level** is set to **Administrator**, and **Print restriction** is set to **Not configured**. Unassigning the policy is not allowed. The predefined local **Server Administrator** filter is automatically assigned to this policy. Other filters can also be assigned.

### Other

**Other** is assigned to all users that do not have any other policy assigned to them. The **Other** policy is assigned to the **Local** or domain root. This policy cannot be deleted, but it can be edited by the administrator. The **Not configured** setting is unavailable in the **Other** policy, since it has the lowest priority.

## Creating a Policy

Before assigning policies, the administrator must create the policies in Policy Manager. In the **New Policy** dialog box, settings are available in **General**, **Device**, and **Job execution** sections. To expand or collapse a particular section, click the arrow icon in the section's title bar.

- 1 In the hierarchical list, select **Policies**. Click **Manage > New policy**.
- 2 Click to expand the **General** section. Type a new **Policy name** in the text box.
- 3 Filters can be any group or user that this policy specifically applies to. To add a filter to the policy, click **Add**. Continue with the steps for the **Add Filter** dialog box.
- 4 To delete a filter from the list, select the filter, then click **Remove**.
- 5 Click to expand the **Device** section. For **Access level**, select the level of privilege for configuring device settings. The options are **Administrator**, **User**, or **Not configured**. The default setting is **Not configured**.
- 6 Click to expand the **Job execution** section. For each device function, select **Not configured** (inherits setting), **Reject usage** (restricts use), or **Off** (no restrictions). The default setting is **Not configured**. Settings may vary by device model.
- 7 To save the policy settings, click **New**.

## Adding Filters

You can add filters to a policy. Adding filters limits the policy's scope to only those users and groups included in the filter list.

- 1 In the hierarchical list, select **Policies**.
- 2 In the view pane, select a policy from the list.
- 3 Click the **Add filter** icon.
- 4 In the **Add Filter** dialog box, from the search criteria list select **Groups and users**, **Groups only**, or **Users only**. The search is limited to this selection.
- 5 From the next search criteria list, select **All**, **Local**, or a domain.
- 6 Type an alphanumeric search term (maximum of 64 characters) in the text box.
- 7 Click the magnifying glass icon to start the search. Search results are displayed in the dialog box list.
- 8 Click to select users and groups from the list.
- 9 Click **Add** to add the filters to the selected policy.

## Adding, Editing, or Removing a Domain

You can add, edit, or remove a domain from the database.

### Add domain

To add a new domain, in the hierarchical list, right-click on a domain to open the context menu. Select **Add domain**. All fields are required. Domain and user credentials for accessing the domain must be valid.

Enter the following domain information:

#### Domain

Select from the list of available domains.

#### User name

Type the name of the domain's user.

#### Password

Type the user's password.

Click **Add** to save the domain. The new domain is added to the hierarchical list.

### Edit domain

To edit a domain, in the hierarchical list, right-click on a domain to open the context menu. Select **Edit domain**. A dialog box appears that allows you to change the **User name** and **Password** for logging on to the domain. The **Domain** name cannot be edited.

### Remove domain

To remove a domain, from the hierarchical list, right-click on a domain to open the context menu. Select **Remove domain**. A confirmation dialog box appears before the domain is deleted. Click **Remove** to delete the domain from the hierarchical list.

## Assigning Policies

You can assign policies to a domain, organizational unit, or **Local**. Newly assigned policies default to the lowest priority in the policies list. You can rearrange assigned policies in the **Policies** tab.

- 1 In the hierarchical list, select a domain, organizational unit, or **Local**.
- 2 Select the **Policies** tab.
- 3 Click **Manage > Assign policy**.
- 4 In the **Assign Policy** dialog box, click to select policies from the list.
- 5 Click **Assign** to apply the policy to the selected item in the hierarchical list.

## Viewing or Editing Policies

To view or edit a policy's properties:

- 1 In the hierarchical list, select **Policies**. Double-click on a policy in the view pane.
- 2 View the information about the policy in the view pane. You can click the arrow icons to expand or close the sections that display policy settings.
- 3 To change the policy name, edit the name in the **Policy name** text box. The policy name cannot be edited for **Administrator** and **Other**. Click **Apply**.
- 4 To add a filter that defines the users or group for the policy, click **Add**. Continue with the steps for the **Add Filter** dialog box. Or, delete a filter from the list by selecting the filter and clicking **Remove**.
- 5 To change the access level, in **Access level** under the **Device** section, select the level of privileges for configuring device settings. The options are: **Administrator**, **User**, or **Not configured**.
- 6 To change the function for a device, click the arrow icon to expand the **Job execution** section. Then select **Not configured** (inherits setting), **Reject usage** (restricts use), or **Off** (no restrictions). Settings may vary by device.
- 7 To save your policy settings changes, click **Apply**. Or, click **Revert** to return the policy settings to what they were before you changed them.

## Deleting a Policy

You can delete a policy from the policy list.

- 1** In the hierarchical list, select **Policies**.
- 2** In the policies list, select a policy.
- 3** Right-click and select **Delete policy**, or click **Edit > Delete policy**.
- 4** In the confirmation dialog box, click **Delete** to remove the policy from the list.

# 5 User Management

The **Users** tab lets you manage domain and local users. You can view and edit domain and local users, delete local users, and create new local users. The predefined **Administrator** user cannot be deleted. The **Users** tab is available in the view panel when you select a domain, or any of its subordinates, in the hierarchical list. It is also available when **Local** is selected.

The users list displays all users of the organizational unit selected in the hierarchical list. Only direct subordinates of the selected organizational unit are displayed. If you select **Local** in the hierarchical list, all local users are displayed. The total number of users, and the number of selected users in the list, is shown in the lower left corner of the window.

These features are available in the **Users** tab:

### **New user**

Adds a local user to the Policy Manager database. **Local** must first be selected in the hierarchical list.

### **Delete user**

Removes a local user from the database.

### **User properties**

Lets you view or edit the information for the selected user. The **User Properties** feature is only available if a single user is selected.

### **Search**

Searches the user's name, login name, e-mail address, or account ID.

## Creating a New Local User

You can add a new local user to the users list.

- 1** In the hierarchical list, select **Local**, then select the **Users** tab in the view pane.
- 2** Click the **New user** icon.
- 3** In the **New Local User** dialog box, type a **User name** (maximum of 32 characters) in the text box.
- 4** Type a **Subname** (maximum of 32 characters) in the text box. **Subname** is only available for Japanese, Traditional Chinese, Simplified Chinese, and Korean.
- 5** Type the user's login information:
  - Login name**  
Type a **Login name** (maximum of 64 characters) in the text box.
  - Password**  
Type a **Password** (maximum of 64 characters).

**E-mail address**

Type an **e-mail address** (maximum of 128 characters).

- 6** Select **Use default account ID** or **Use specific account ID**, and type an account ID in the text box. Account IDs are used by the printing system to monitor usage. The default account ID is **Other**, which always exists for the printing system.
- 7** Type the **ID number** from the user's ID card.
- 8** Click **New** to save the information to the Policy Manager database.

## Viewing or Editing User Properties

You can edit or view the properties of a local user. For a domain user, you can view the properties, but only **Account ID** and the **ID number** of the ID card can be edited.

- 1** In the hierarchical list, select **Local**, and then select the **Users** tab in the view pane. In the users list, select one user.
- 2** Click the **User properties** icon.
- 3** In the **User Properties** dialog box, edit the available properties:
  - User name**
  - Subname**
  - Login name**
  - Password**
  - E-mail address**
  - Account ID**
  - ID number** of the ID card.**Effective policy** and **Group membership** cannot be edited.
- 4** When finished editing user information, click **Save**.

## Deleting a User

You can delete a selected user or users from the users list.

- 1** In the **Users** tab, click to select a user from the users list.
- 2** Click the **Delete user** icon.
- 3** In the confirmation dialog box, click **Delete** to remove the user from the users list.

# 6 Group Management

The **Groups** tab is for managing domain and local groups. You can also create, edit or delete local groups. The application lets you view all groups. The **Groups** tab is available in the view pane, if a domain or any of its subordinates is selected in the hierarchical list. It is also available if **Local** is selected.

The groups list displays all groups of the organizational unit selected in the hierarchical list. Only direct subordinates of the selected organizational unit are displayed. If **Local** is selected in the hierarchical list, all local groups are displayed. The total number of groups and number of selected groups are displayed in the lower left corner of the window.

The **Groups** tab supports the following options:

### **New group**

Opens the **New Group** dialog box to create a local group to add to the database.

### **Delete group**

Removes the selected groups from local groups only.

### **Group properties**

Opens the **Group Properties** dialog box for a single group where you can view or edit the information.

### **Search**

Lets you search the group list by name.

## Creating a New Local Group

To add a new local group to the group list:

The **Members** list in the dialog box displays all the added users and groups to the local group being created. For each member, the list displays the **Name**, **Type** (User or Group), and **Distinguished Name**.

- 1** In the hierarchical list, select **Local**. Then click the **Groups** tab in the view pane.
- 2** Click **Manage > New local group**.
- 3** In the **New Group** dialog box, type a unique **Group name** (maximum of 64 characters) in the text box. The group name must be unique and differ from any **Group name** that already exists in the group list.
- 4** Click **Add member** to add local or domain users, and local or domain groups, as members of the group being created.
- 5** To delete users or groups from the members list, select the members and click **Remove member**. The members are immediately deleted from the list.

- 6 When finished entering group information, click **Save** to save the information to the Policy Manager database.

## Adding Members to a Group

You can add local or domain users or groups to a local group.

- 1 In either the **New Group** or **Group Properties** dialog box, click **Add member**.
- 2 Select a search type from these options:
  - Groups and users** (default)
  - Groups only**
  - Users only**
- 3 Select a search location from these options:
  - All** (default)
  - Local**
  - [Domain]**
- 4 Type an alphanumeric search term (maximum of 64 characters) in the text box.
- 5 Click the magnifying glass icon, or press **Enter** to start the search process.

The search term is compared to all properties of locations selected in the search location. The search list shows only instances containing text matching the search term. The list shows these values: **Name**, **Type** (User or Group), and **Distinguished name**. **Distinguished name** is a unique identifier for the users and groups. Different organizational units can have the same name, so this name specifies each of them.

Status information at the bottom left of the dialog box shows the number of items selected out of the total search items.
- 6 Click to select a member from the search list.
- 7 When finished selecting members, click **Add** to save the members to the selected group.

## Editing or Viewing Group Properties

You can view or edit the properties of a local group. Domain group properties cannot be edited.

- 1 In the hierarchical list, select **Local**, and then select the **Groups** tab in the view pane. In the groups list, select one group.
- 2 Click the **Group properties** icon.
- 3 In the **Group Properties** dialog box, you can edit the **Group name**, or edit the **Members** by clicking **Add member** or **Remove member**.

- 4 When finished editing group information, click **Save**. The revised information is saved to the Policy Manager database.

## Deleting a Group

You can delete a selected group, or groups, from the groups list.

- 1 In the **Groups** tab, click to select a group from the groups list.
- 2 Click the **Delete group** icon.
- 3 In the confirmation dialog box, click **Delete**. The group is now removed from the database.

# 7 Users or Groups Search

This feature performs a search on the users list in the **Users** tab, or the groups list in the **Groups** tab, whichever is displayed in the view pane. The search can find exact matches for full or partial strings. Search strings are not saved if you move from view to view.

## Searching for Users or Groups

To search the users list or groups list:

- 1** Select a domain, organizational unit, or **Local** in the hierarchical list, and click the **Users** tab or **Groups** tab in the view pane.
- 2** In the **Search text** box at the upper right, type an alphanumeric search term (maximum of 64 characters).
- 3** To clear the search, click the magnifying glass icon beside the text box. This deletes any text in the text box, and restores the view to the original list of users or groups before the search.

# 8 Access Log

Records are posted to the user access log every time a printing device (MFP) makes an authentication request to Policy Manager.

## Viewing the Access Log

You can view the access log as a record of user logins.

- 1 Click **Manage > Show access log**.
- 2 To rearrange the order of the columns, drag the column heading to the desired location.
- 3 To sort by a particular column, in ascending or descending order, click the desired column heading.
- 4 To copy list data, click to select users from the search list. On the selected users, right-click and select **Copy**.

## Searching on the Access Log

To search the access log with a full or partial search string:

- 1 Click **Manage > Show access log**.
- 2 Type an alphanumeric search term (maximum of 64 characters) in the text box. The access log can be searched for any of the following:
  - Login**  
The login name of the user who made the authentication request.
  - Access time**  
The date of the authentication request.
  - Status**  
The status of the authentication request, either **Success** or **Fail**.
  - Access point**  
The IP address of the user making the authentication request.
  - ID card**  
The ID card number of the user making the authentication request.
- 3 To clear the search, click the magnifying glass icon beside the text box. This deletes any text in the text box, and restores the view to the original list of entries before the search.

## Exporting the Access Log

To save the access log to a file, follow these steps:

- 1 Click **File > Export access log**.
- 2 Type a filename or browse for saving the access log. Select an extension for the access log file: .XML or .CSV.
- 3 Click **Save**.

## Clearing the Access Log

The **Clear Access Log** feature removes all access logs from the Policy Manager database. Exported access logs are not affected.

- 1 Click **Manage > Clear access log**.
- 2 In the confirmation dialog box, click **Clear** to remove all access log entries from the Policy Manager database.

# 9 Admin Console-Spooler

The Admin Console-Spooler manages print jobs stored in the spooler server, and lets you configure the spooler settings.

In the hierarchical list, click **Spooler** to open this view.

## Admin Console-Spooler Toolbar

At the top of the print jobs list, the Admin Console-Spooler toolbar provides these options:

### Delete job

Removes one or more selected print jobs from the current view, and adds them to the **Deleted jobs** list. A confirmation dialog box appears before the job is deleted.

### Current view

Opens a list of view types for different categories of print jobs: **Active jobs**, **All jobs**, **Expired jobs**, **Deleted jobs**, and **Released jobs**. The selected current view type is preserved for the next session after exiting the Admin Console-Spooler.

### Help

Opens user assistance for the Admin Console-Spooler.

### Search

Searches the **Job name**, **Source**, and **Destination** columns in the print job list.

## Print Jobs Current View

The Admin Console-Spooler can display the print job list by different job conditions. **Active jobs** is the default view type. Change the view by selecting from the view type list in the toolbar.

### Active jobs

Shows print jobs that have a status of **Ready**, **Spooling**, or **Printing**, or jobs that have an error code awaiting some action. This view displays all the available jobs list columns: **Job name**, **Owner**, **Status**, **Copies**, **Size**, **Received**, **Expiry**, **Source**, and **Destination**.

### All jobs

Shows all jobs that have not been purged. Like **Active jobs**, this view displays all the available jobs list columns.

### Expired jobs

Shows jobs whose expiration date has passed. The administrator sets the expiration date for print jobs. If a print job is not released and has passed the expiration date, it can no longer be released. Expired jobs can be purged, but not deleted. This view displays: **Job name**, **Owner**, **Source**, **Received**, and **Expiry** job list columns.

### Deleted jobs

Shows print jobs deleted by the user or administrator. A job must be purged by the administrator to be permanently removed from the database. This view displays: **Job name**, **Owner**, **Source**, and **Received**.

### Released jobs

Shows print jobs released from the device and finished printing without error. A released job must be purged by the administrator to be permanently removed from the database. This view displays: **Job name**, **Owner**, **Source**, **Destination**, and **Details** job list columns.

## Searching for Print Jobs

You can search the print jobs list. The searchable columns are: **Job name**, **Source**, and **Destination**.

- 1 In the **Search text** box at the upper right, type an alphanumeric search term (maximum of 64 characters). As you type, the view shows print job matches for partial text up to and including the finished search term.
- 2 To clear the search, click the **Clear search** icon beside the text box. This deletes any text in the text box, and restores the view to the original list of print jobs before the search.

## Spooler Print Jobs List

The print jobs list displays a list of all server print jobs for one user, based on the view type. The default view is **Active jobs**. The list is initially sorted by the date and time the spooler received the job. To rearrange the order of the columns, drag the column heading to the desired location. To sort by a particular column, in ascending or descending order, click the desired column heading. Right-click on a print job to open a context menu. Multiple selections may be made from the list.

Columns vary by the view type, but several of these are displayed:

### Job name

The print job name sent by the printer driver.

### Owner

The name of the user who submitted the print job.

### Status

The progress or condition of the print job.

### Copies

The number of copies that have to be printed.

### Size (bytes)

The size of the print job in bytes.

### Received

The date and time the print job was received by the spooler.

### Expiry

The date and time that the print job will be deleted from the server.

### Source

The IP address of the computer that originated the print job.

### **Destination**

The IP address of the device where the print job will be released.

## **Spooler Print Job Context Menu**

The print job context menu lets you cancel, delete, or purge a print job from the spooler. Select one or multiple print jobs and right-click to open the context menu.

The print job selections available are as follows:

### **Cancel**

Stops transmission of the job during printing to the printing system. After a **Cancel**, the status of the job changes back to **Ready**.

### **Delete job**

Removes one or more selected print jobs from the current view, and adds them to the **Deleted jobs** list. A confirmation dialog box appears before the job is deleted.

### **Purge**

Permanently deletes the job from the current view and also from the Policy Manager database. A confirmation dialog box appears before the job is purged.

### **Job properties**

Opens a dialog box that shows detailed information about the job.

## **Print Job Properties**

The **Job Properties** dialog box lets you view details about a selected print job.

### **General**

This section contains basic information about the print job.

#### **Job name**

The print job name sent by the printer driver.

#### **Owner**

The name of the user who submitted the print job.

#### **Copies**

The number of copies set for the print job.

#### **Pages**

The number of pages contained in the print job.

### **Activity log**

This section shows information on print job activity.

#### **Time**

The time at which the status of the job was updated.

#### **User name**

The name of the user who submitted the print job.

#### **Status**

The current status of the print job.

#### **Source**

The IP address of the computer that originated the print job.

**Destination**

The IP address of the printing system.

## Viewing Print Job Properties

You can view details about a print job in the **Job Properties** dialog box.

- 1 Right-click on a single print job in the print jobs list.
- 2 Select **Job properties**.
- 3 View **General** information and the **Activity log** for that print job.
- 4 Click **Close**.

## Configuring Spooler Settings

To change the spooler settings, follow these steps:

- 1 In the toolbar, click **Manage**, and then click **Spooler settings**. The **Spooler Settings** dialog box is displayed, showing the available spooler settings. The spooler settings options that you have available include: **Mail settings**, **Job settings**, and **SNMP settings**.
- 2 In the **Mail settings** section, specify the following:
  - Host**  
The SMTP server name. Use up to a maximum of 128 ASCII characters.
  - Port**  
The SMTP server port number. Use a range of 1 to 65535.
  - Require authentication**  
Click this check box to specify a **User name** and **Password** used for e-mail access. Use up to a maximum of 128 characters.
    - User name**  
The user name for logging in to the SMTP server. Use up to a maximum of 128 ASCII characters.
    - Password**  
The password for logging in to the SMTP server. Use up to a maximum of 128 ASCII characters.
    - Sender name**  
The user name of the e-mail sender. Use up to a maximum of 128 ASCII characters.
    - Receiver e-mail address**  
The e-mail address of the user who will receive e-mail notifications. Use up to a maximum of 128 ASCII characters.
    - Test connection**  
Click this button to test if the **Mail settings** are correct.

- 3** In the **Job settings** section, specify the following:

**Job retention days**

The number of days the print job must be held on the server before it expires. Use a range of 1 to 30; the default is 7. Move the sliding indicator to select the number of retention days.

**Max storage space (%/GB)**

When stored jobs reach the maximum space, the spooler server will stop accepting print jobs. Move the sliding indicator to select the maximum storage space.

**Warning percentage limit (%)**

If the warning percentage limit is exceeded, an e-mail notification is sent to the administrator warning that storage space is approaching capacity. Use a range of 1 to 99; the default is 80. Move the sliding indicator to select the warning percentage limit.

- 4** In the **SNMP settings** section, specify the following:

**SNMP communication retries**

Click the drop-down menu and select the number of times, after an initial failure, the system should attempt to establish SNMP communication with the device. Use a range of 0 to 5 times.

**SNMP version**

Select **Use SNMP v1/v2** or **Use SNMP v3** to access the specific properties for the selected version.

These communication settings are for SNMP v1/v2 only:

**Read Community and Write Community**

Type the device's **Read Community** name for requesting information. Type the device's **Write Community** name for changing configurations. The **Read Community** and **Write Community** are sent with all SNMP receive and send requests, and must match the community values on the device.

These communication settings are for SNMP v3 only:

**User name**

Enter up to a maximum of 32 characters for the user name.

**Password**

Enter up to a maximum of 32 characters for the password.

**Authentication**

Click the **Authentication** check box, then select a **HASH** method (MD5 or SHA).

**Privacy**

Click the **Privacy** check box, then select an **Encryption** method (DES or AES).

- 5** When finished specifying spooler settings, click **Save**.

# 10 Client Viewer

Client Viewer is an application installed on a client's computer. It lets an individual view their personal print job list and delete jobs if needed. The Client Viewer communicates with Policy Manager to retrieve the basic details about each print job.

---

**Note:** If you have not already installed Client Viewer, for instructions see the [Policy Manager Installation Guide](#).

---

## Policy Manager Server Connection

Only domain users or registered local users in Policy Manager, or Windows account users, are authorized to use Client Viewer.

At the start of the Client Viewer application, the **Client Viewer Login** dialog box appears. If the **Use Windows authentication** check box is selected, Client Viewer will automatically use the Microsoft Windows account of the login user for authentication and the dialog box will not appear at Client Viewer startup in the future.

The server uses information in the login dialog box to determine if the login request is from a valid user. If an error occurs during authentication, an error message appears and you are returned to the login dialog box.

### Opening a Connection to the Policy Manager Server

You can create or change the connection to the Policy Manager server.

- 1** To access the **Client Viewer Login** dialog box at any time after startup, in the toolbar click **Open connection**.
- 2** If registered in the Policy Manager system, select **Use a specific user name**, then type your **User name** and **Password** in the text boxes. Or, click the **Use Windows authentication** check box for the server to use your Microsoft Windows account as the login.
- 3** Type the server name and port, separated by a colon, in the **Server** text box. Or, click **Refresh** to discover servers running on the local network, then select one from the drop-down list.
- 4** Click **Log in**.

## Client Viewer Toolbar

At the top of the print jobs list, the Client Viewer toolbar provides the following options:

**Open connection**

Opens the **Client Viewer Login** dialog box for user authentication and the server name.

#### **Delete job**

Removes one or more selected print jobs from the current view, and adds them to the deleted jobs list. A confirmation dialog box appears before the job is deleted.

#### **Current view**

Opens a list of options for views of different categories of print jobs: **Active jobs**, **All jobs**, **Expired jobs**, **Deleted jobs**, and **Released jobs**. The selected current view type is preserved for the next session after exiting Client Viewer.

#### **Help**

Opens user assistance for Client Viewer.

## Print Jobs Current View

Client Viewer can display the print job list by different job conditions. **Active jobs** is the view type default. Change the view by selecting from the view type list in the toolbar at the top of the print job list.

#### **Active jobs**

These are print jobs that have a status of **Ready**, **Spooling**, or **Printing**, or jobs that have an error code awaiting some action. This view displays all the available jobs list columns: **Job name**, **Status**, **Copies**, **Size**, **Received**, **Expiry**, **Source**, and **Destination**.

#### **All jobs**

These are all jobs that have not been purged. Like **Active jobs**, this view displays all the available jobs list columns.

#### **Expired jobs**

The administrator sets the expiration date for print jobs. If the job is not released from the server and it passes the expiration date, the job can no longer be released. Expired jobs are eventually purged from the server by the administrator. Expired jobs can only be purged and cannot be deleted. This view displays the **Job name**, **Source**, **Received**, and **Expiry** job list columns.

#### **Deleted jobs**

These are print jobs deleted by the user or the administrator. The job must be purged by the administrator to be permanently removed from the database. This view displays the **Job name**, **Source**, and **Received** job list columns.

#### **Released jobs**

These print jobs have been released from the device and finished printing without error. **Released jobs** can be purged by the administrator to be permanently removed from the database. This view displays the **Job name**, **Source**, and **Destination** job list columns.

## Searching for Print Jobs

You can search the print jobs list. The searchable columns are: **Job name**, **Source**, and **Destination**.

- 1 In the **Search text** box at the upper right, type an alphanumeric search term (maximum of 64 characters). As you type, the view shows print job matches for partial text up to and including the finished search term.
- 2 To clear the search, click the **Clear search** icon beside the text box. This deletes any text in the text box, and restores the view to the original list of print jobs before the search.

## Client Print Jobs List

The client print jobs list displays a list of all server print jobs for one user, based on the view type. The default view is **Active jobs**. The list is initially sorted by the date and time the spooler received the job. To rearrange the order of the columns, drag the column heading to the desired location. To sort by a particular column, in ascending or descending order, click the desired column heading. Right-click on a print job to open a context menu. Multiple selections may be made from the list.

Columns vary by the view type, with some of these displayed:

**Job name**

The print job name sent by the printer driver.

**Status**

The progress or condition of the print job.

**Copies**

The number of copies that will be printed.

**Size**

The size of the print job in bytes.

**Received**

The date and time the print job was received by the spooler.

**Expiry**

The date and time that the print job will be deleted from the server.

**Source**

The IP address of the computer that originated the print job.

**Destination**

The IP address of the device where the print job will be released.

## Print Job Context Menu

The print job context menu lets you cancel or delete your own print jobs, or view your print job's properties. Select one or multiple print jobs, then right-click to open the context menu.

The selections available in the menu depend on the current status of the print job.

**Cancel**

Stops transmission of the job during printing to the printing system. After a **Cancel**, the status of the job changes back to **Ready**.

**Delete job**

Removes one or more selected print jobs from the current view, and adds them to the **Deleted jobs** list. A confirmation dialog box appears before the job is deleted.

**Job properties**

Opens a dialog box that shows detailed information about the job.

## Print Job Properties

The **Job Properties** dialog box lets you view details about a selected print job.

**General**

This section contains basic information about the print job.

**Job name**

The print job name sent by the printer driver.

**Owner**

The name of the user who submitted the print job.

**Copies**

The number of copies set for the print job.

**Pages**

The number of pages contained in the print job.

**Activity log**

This section shows information on print job activity.

**Time**

The time at which the status of the job was updated.

**User name**

The name of the user who submitted the print job.

**Status**

The current status of the print job.

**Source**

The IP address of the computer that originated the print job.

**Destination**

The IP address of the printing system.

## Viewing Print Job Properties

You can view details about a print job in the **Job Properties** dialog box.

- 1** Right-click on a single print job in the print jobs list.
- 2** Select **Job properties**.
- 3** View **General** information and the **Activity log** for that print job.
- 4** Click **Close**.

## KYOCERA MITA AMERICA, INC.

### **Headquarters:**

225 Sand Road,  
Fairfield, New Jersey 07004-0008  
TEL : (973) 808-8444  
FAX : (973) 882-6000

### **New York Branch:**

30-30 47th Avenue  
Long Island City, NY 11101  
TEL : (718) 289-2500  
FAX : (718) 289-2501

### **Northeastern Region:**

225 Sand Road,  
Fairfield, New Jersey 07004-0008  
TEL : (973) 808-8444  
FAX : (973) 882-4401

### **Midwestern Region:**

201 Hansen Court Suite 119  
Wood Dale, Illinois 60191  
TEL : (630) 238-9982  
FAX : (630) 238-9487

### **Western Region:**

14101 Alton Parkway,  
Irvine, California 92618-7006  
TEL : (949) 457-9000  
FAX : (949) 457-9119

### **Southeastern Region:**

3100 Breckinridge Blvd. NW Building 100,  
Suite 105 Duluth, Georgia 30096  
TEL : (770) 729-9786  
FAX : (770) 729-9873

### **Southwestern Region:**

2825 West Story Road,  
Irving, Texas 75038-5299  
TEL : (972) 550-8987  
FAX : (972) 570-4704

### **National Operation Center & National Training Center:**

2825 West Story Road,  
Irving, Texas 75038-5299  
TEL : (972) 659-0055  
FAX : (972) 570-5816

### **Latin America Division:**

8240 N.W. 52nd. Terrace Dawson Building,  
Suite 108 Miami, Florida 33166  
TEL : (305) 421-6640  
FAX : (305) 421-6666

## KYOCERA MITA CANADA, LTD.

6120 Kestrel Road, Mississauga,  
Ontario L5T 1S8, Canada  
TEL : (905) 670-4425  
FAX : (905) 670-8116

## KYOCERA MITA MEXICO, S.A. DE C.V.

Av. 16 de Septiembre #407  
Col. Santa Inés,  
Azcapotzalco México,  
D.F. 02130, México  
TEL : (55) 5383-2741  
FAX : (55) 5383-7804

## KYOCERA MITA Brazil Ltda.

Av. Tambore, 1180 Mob.B-09 CEP 06460-000  
Tambore-Barveri-SP,  
Brazil  
TEL : (55) 11-4195-8496  
FAX : (55) 11-4195-6167

## KYOCERA MITA Asia Limited

16/F., Mita Centre,  
552-566, Castle Peak Road,  
Tsuen Wan, New Territories, Hong Kong  
Phone: (852)-2610-2181

KYOCERA MITA (Thailand) Corp., Ltd.  
335 Ratchadapisek Road, Bangsue,  
Bangkok, 10800, Thailand  
Phone: (66)-2-586-0333

KYOCERA MITA Singapore Pte Ltd.  
121 Genting Lane, 3rd Level,  
Singapore 349572  
Phone: (65)-6741-8733

KYOCERA MITA Hong Kong Limited  
16/F., Mita Centre,  
552-566, Castle Peak Road,  
Tsuen Wan, New Territories,  
Hong Kong  
Phone: (852)-2429-7422

KYOCERA MITA Taiwan Corporation  
6F., No.37, Sec. 3, Minquan E. Rd.,  
Zhongshan Dist., Taipei 104, Taiwan R.O.C.  
Phone: (886)-2-2507-6709

KYOCERA MITA Korea Co., Ltd.  
18F, Kangnam bldg, 1321-1,  
Seocho-Dong, Seocho-Gu, Seoul, Korea  
Phone: (822)-6933-4050

KYOCERA MITA India Private Limited  
First Floor, ORCHID CENTRE  
Sector-53, Golf Course Road, Gurgaon 122  
002, India  
Phone: (91)-0124-4671000

## **KYOCERA MITA EUROPE B.V.**

Bloemlaan 4, 2132 NP Hoofddorp,  
The Netherlands  
Phone: +31.20.654.0000  
Home page: <http://www.kyoceramita-europe.com>  
Email: [info@kyoceramita-europe.com](mailto:info@kyoceramita-europe.com)

**KYOCERA MITA NEDERLAND B.V.**  
Beechavenue 25, 1119RA Schiphol-Rijk  
The Netherlands  
Phone: +31.20.58.77.200

**KYOCERA MITA (UK) LTD**  
8 Beacontree Plaza  
Gillette Way Reading Berks RG2 0BS,  
U.K.  
Phone: +44.1189.311.500

**KYOCERA MITA ITALIA S.p.A.**  
Via G. Verdi, 89 / 91, 20063 Cernusco s/N  
Milano, Italy  
Phone: +39.02.92179.1

**S.A. KYOCERA MITA BELGIUM N.V.**  
Sint-Martinusweg 199-201, 1930 Zaventem,  
Belgium  
Phone: +32.2.720.9270

**KYOCERA MITA FRANCE S.A.**  
Espace Technologique de St Aubin  
Route de l' Orme  
91195 Gif-sur-Yvette CEDEX, France  
Phone: +33.1.6985.2600

**KYOCERA MITA ESPAÑA S.A.**  
Edificio Kyocera, Avda de Manacor No. 2,  
28290 Las Matas (Madrid),  
Spain  
Phone: +34.91.631.8392

**KYOCERA MITA FINLAND OY**  
Atomitie 5C, 00370 Helsinki,  
Finland  
Phone: +358.9.4780.5200

**KYOCERA MITA (SCHWEIZ)**  
Hohlstrasse 614, 8048 Zürich  
Switzerland  
Phone: +41.44.908.4949

**KYOCERA MITA DEUTSCHLAND GMBH**  
Otto-Hahn-Str. 12 D-40670 Meerbusch,  
Germany  
Phone: +49.2159.918.0

**KYOCERA MITA GMBH AUSTRIA**  
Eduard-Kittenberger-Gasse 95,  
1230 Wien,  
Austria  
Phone: +43.1.86338

**KYOCERA MITA SVENSKA AB**  
Esbogatan 16B 164 75 Kista,  
Sweden  
Phone: +46.8.546.55000

**KYOCERA MITA NORGE**  
Postboks 150 Oppsal, NO 0619 Oslo  
Olaf Helsetsvei 6, NO 0694 Oslo,  
Norway  
Phone: +47.22.62.73.00

**KYOCERA MITA DANMARK A/S**  
Ejby Industrivej 1, DK-2600 Glostrup,  
Denmark  
Phone: +45.7022.3880

**KYOCERA MITA PORTUGAL LDA.**  
Rua do Centro Cultural, 41 (Alvalade) 1700-106 Lisboa,  
Portugal  
Phone: +351.21.843.6780

**KYOCERA MITA SOUTH AFRICA (PTY) LTD.**  
49 Kyalami Boulevard,  
Kyalami Business Park Midrand,  
South Africa  
Phone: +27.(0)11.540.2600

## **KYOCERA MITA AMERICA, INC.**

Headquarters:  
225 Sand Road,  
Fairfield, New Jersey 07004-0008,  
U.S.A.  
Phone: (973) 808-8444

**KYOCERA MITA AUSTRALIA PTY. LTD.**  
Level 3, 6-10 Talavera Road, North Ryde,  
N.S.W. 2113 Australia  
Phone: (02) 9888-9999

**KYOCERA MITA NEW ZEALAND LTD.**  
1-3 Parkhead Place, Albany  
P.O. Box 302 125 NHPC, Auckland,  
New Zealand  
Phone: (09) 415-4517

## **KYOCERA MITA Asia Limited**

16/F., Mita Centre,  
552-566, Castle Peak Road,  
Tsuen Wan, New Territories, Hong Kong  
Phone: (852)-2610-2181

## **KYOCERA MITA Corporation**

2-28, 1-chome, Tamatsukuri, Chuo-ku  
Osaka 540-8585, Japan  
Phone: (06) 6764-3555  
<http://www.kyoceramita.com>

