Web SmartDeviceMonitor
Administrator's Guide

Preface

Thank you very much for using the Web SmartDeviceMonitor software product.

This manual is written for network administrators to explain how to setup and operate Web SmartDeviceMonitor. Please read this manual for effective use of this product.

This manual mainly describes the site planning and installation and setup procedures of Web SmartDeviceMonitor. For an explanation of the operation of each screen, see the related on-line Help.

Trademarks

Microsoft, Windows, and Windows NT are registered trademarks of Microsoft Corporation in the United States and/or other countries.

Pentium is a registered trademark of Intel Corporation.

Other company names and product names are trademarks or registered trademarks of their respective companies. They are used for explanations in this manual and the rights of their owners. Use of these marks does not infringe on the rights of the owners.

- The product name of Windows® 98 is Microsoft® Windows® 98.

- The product name of Windows® Me is Microsoft® Windows® Millennium Edition (Windows Me).

- The product names of Windows® 2000 are as follows:
  Microsoft® Windows® 2000 Professional
  Microsoft® Windows® 2000 Server
  Microsoft® Windows® 2000 Advanced Server

- The product names of Windows® XP are as follows:
  Microsoft® Windows® XP Home Edition
  Microsoft® Windows® XP Professional

- The product names of Windows Server ™ 2003 are as follows:
  Microsoft® Windows Server™ 2003 Standard Edition
  Microsoft® Windows Server™ 2003 Enterprise Edition
  Microsoft® Windows Server™ 2003 Web Edition

- The product names of Windows NT® 4.0 are as follows:
  Microsoft® Windows NT® Workstation 4.0
  Microsoft® Windows NT® Server 4.0

TABLE OF CONTENTS

1. Overview

2. Installation Planning

3. Installation

4. Configuring Web SmartDeviceMonitor

5. Device Management

6. Maintenance

7. Appendix

1. Overview

What is Web SmartDeviceMonitor?

Web SmartDeviceMonitor is a Web-based device management software solution. It provides a centralized control point for organization, configuration, and error feedback of network based printers and multi-function devices. This solution greatly reduces the device administrative burdens of IT network administrators, help desk personnel, and desktop support personnel.

Web SmartDeviceMonitor is installed on a network server and does not require any additional software to be installed. Device management services are provided to client computers via a standard Web browser.

ABH002S1

❖ **Web SmartDeviceMonitor value and benefits:**

- Easy Installation
- Immediate error feedback via graphical icons
- Self-contained application (no additional software required on server or client computers)
- Status monitoring of the network devices, and retrieval and registration of information from network devices
- Batch configuration of devices
- Remote configuration of newly installed devices
- Detailed view of device-specific information
- Automatic discovery of devices across TCP/IP network segments
- Group organization and management of devices within an enterprise environment
- E-mail notification of device errors to single or multiple e-mail addresses
- Easy device search by specifying the model name, printing speed, device type (Color or Black & White), etc.
- Multi-language support (English, German, French, Italian, Spanish, Dutch)

Product Features

Characteristics of Web SmartDeviceMonitor

Web SmartDeviceMonitor can satisfy the device management needs required by corporations implementing large TCP/IP networks. Although not exclusive, these environments typically are multi-site with large numbers of devices to manage.

❖ **Easy installation**

The applications installation wizard systematically guides the user through the installation process. The user is not required to install any additional Web server applications. All necessary Web services are self contained and loaded upon installation. This greatly reduces the learning curve and reduces the resource requirement of the Web server.

Client computers only require a standard Web browser to access the application server. This effectively eliminates any client set-up time by IT administrators.

❖ **Unified user interface**

Web SmartDeviceMonitor has a unified Web browser based user interface that is operating system independent. This greatly reduces the learning curve within environments that have a mixture of different client operating systems.

❖ **Accessibility**

Devices that support Printer MIB (RFC 1759), MIB-II (RFC 1213), and Host Resource MIB (RFC 2790) can be remotely monitored and configured. Web SmartDeviceMonitor provides a device page for displaying device status and making settings for each device.

The status information from devices of other manufactures or the ability to configure those devices cannot be guaranteed. Although Printer MIB, MIB-II, and Host Resource MIB are defined standards, they can be implemented differently by each manufacturer.

Detected device errors can be reported via e-mail.

Any client computer with Web access to the application server can access all the provided management tools

Device discovery can take place across TCP/IP subnets.

Devices can be grouped by location or department.

❖ **Superior search function**

Device searches can use a variety of search criteria options. Search criteria can be defined by IP address, model name, or status information.

Functions of Web SmartDeviceMonitor

❖ **Discovery**

Web SmartDeviceMonitor automatically discovers devices that support Printer MIB (RFC 1759), MIB-II (RFC 1213), and Host Resource MIB (RFC 2790). Once the discovery is performed, a device database is created for all discovered devices. When subsequent discoveries are performed, new devices are added to the device database and information for existing devices is updated.

❖ **Device sorting**

Once devices have been discovered, they can be easily sorted to isolate the desired device.

❖ **Screen data export**

The displayed device list can be exported as a CSV file. This file can be imported into a spreadsheet program. These lists are useful when analyzing a company's device assets.

❖ **Group management**

Devices can easily be added to groups after they have been discovered. The creation and organization of groups greatly increases the device management efficiency of large IT departments.

❖ **Security**

The security level is determined by the account used when logging on. There are three types of privileges for accounts used in the application: "Administrators", "Users", and "Device Administrators". Security can also be applied to groups by setting a group password.

❖ **Status monitoring**

Current status information appears upon discovery and status polling of devices. Graphical icons give users quick and easy identification of device status. Icons change as the status of the device changes.

❖ **Error notification**

E-mail error notification can be configured for devices or groups. Conditions that trigger an e-mail notification can be custom configured per device or group. Multiple e-mail recipients can be configured to receive e-mail error notification. A SMTP server is required for e-mail notification.

❖ **Displayed columns customization**

The number of columns displayed in the device list can be custom configured. Users have control of what columns are displayed and the order of these columns.

❖ **Initial setting**

Newly installed devices in local networks can be configured remotely, using the NIB Setup Tool.

❖ **Batch configuration**

Multiple network devices can be configured by batch. This function is useful when configuring identical settings for devices that are in the same category.

❖ **Device page**

Device-specific information is displayed graphically and intuitively. Settings can also be changed from within the device page.

Administrators Guide / Help

1

Administrators Guide

The Administrator's Guide includes installation and setup instructions. Additional information is provided to illustrate how devices are managed by the application.

Help

Help is incorporated into the application to quickly assist users with operational procedures.

System Requirements

Server Requirements

Item	Description
Computer	CPU: Pentium III 500 MHz or higher recommended
	Memory: 256 MB or more recommended
	Free HDD space before installation: Minimum 500 MB
	Free HDD space at execution: Minimum 400 MB
Operating System (English, German, French, Italian, Spanish, Dutch) [*1]	Windows NT Server 4.0 : Service Pack 6a or later
	Windows 2000 Professional / Server / Advanced Server (i386) : Service Pack 3 or later
	Windows XP Professional
	Windows Server 2003 Standard Edition / Enterprise Edition
Network	TCP/IP must be installed and configured correctly.

Client Requirements

Item	Description
Operating System (English, German, French, Italian, Spanish, Dutch) [*2]	Windows 98/98SE/Me
	Windows NT Workstation 4.0 / Server 4.0(i386) : Service Pack 6a or later
	Windows 2000 Professional / Server / Advanced Server (i386)
	Windows XP Home / Professional
	Windows Server 2003 Standard Edition / Enterprise Edition
Network	TCP/IP must be installed and configured correctly.
Browser	Microsoft Internet Explorer 5.01 or later (5.5 or later recommended)
	(For Windows NT, and XP, JavaVM must be installed to use the Initial Setting function.)
Screen Resolution	800x600 or better (1024x768 or better recommended)

Printer and Multi-Function Device Requirements

Item	Description
Network Protocol	TCP/IP
Message Exchange Protocol	Printer MIB (RFC 1759), MIB-II (RFC 1213), and Host Resource MIB (RFC 2790)

Protocols Used

Item	TCP/IP
Device Information Acquisition	SNMP
Device Setting	SNMP
Display on Browser	HTTP (By default, port number 9090 is used.)

[*1] Supported languages are as follows; English, German, French, Italian, Spanish, Dutch.
Any of the supported languages can be selected for the installation language. The operating system can be in any of the supported languages. Any combination of supported operating system language and installation language can be used.
(The interface language in Web SmartDeviceMonitor server cannot be changed after installation.)

[*2] For operations using a web browser on client computers, the interface language can be selected at logon, regardless of the language selected at installation.

2. Installation Planning

Planning and Introducing Web SmartDeviceMonitor

Proper planning is required to successfully use Web SmartDeviceMonitor. It is essential to gather the required device, group, and network information prior to installation. The following flowchart illustrates a recommended installation plan:

Acquire the TCP/IP Network Map Information
- Logical Subnets
- Physical Segments
- Subnet Masks
- IP Addresses
- Routers / Switches

Define the Device Management Needs
- Define the range of network segments to be managed
- Define the organizational device management needs
- Define the SNMP community names

Define Personnel and Logon Privileges
- Primary Administrator (Administrators Privileges)
- Secondary Administrator (Administrators Privileges)
- IT Help Desk (Administrators Privileges)
- IT Desktop Support (Administrators Privileges)
- Advanced Technical Support (Administrators Privileges)
- Clients (Users Privileges)

cy-002

2

Define Group Requirements
- Location
- Department
- Device capabilities
- Device type and/or characteristic
- Define Group Passwords

Determine Device Discovery Policy
- Broadcast
- Ping Sweep

Prepare Server
- Meet or exceed minimum requirements

Installation and Configuration
- Install and configure Web SmartDeviceMonitor

Training and Departmental Access
- Provide adequate training for users
- Designate access for appropriate IT departmental unit

ABH003S1

Collecting Network Information

Initial setup will require detailed information about your IP network. The configuration process will be greatly reduced by acquiring this information prior to installation.

❖ **IP segmentation and addressing**
  - Logical Subnets
  - Physical Segments
  - Subnet Masks
  - IP Addresses
  - SNMP Community Names
  - Routers / Switches

❖ **SMTP server IP address**
  A valid SMTP server address needs to be configured if the e-mail error notification function is required. It will be necessary to acquire this information from your e-mail administrator.

❖ **Network device list**
  If possible, it is recommended to acquire a master list of all network devices deployed. This information will benefit the administrator when configuring groups by location or capability.

Account Management

Account management provides essential tools to maintain a superior level of server security and data integrity within enterprise environments.

The account used to log on determines a user's access privileges. Account management maintains a database that defines a users level of access to available management functions. This secure measure defines a users operational privilege, which prevents any undesirable configuration changes to be made.

Account Privileges

Web SmartDeviceMonitor provides the following three types of application specific account privileges:

- Administrators
- Device Administrators
- Users

$\mathcal{P}$ Reference

For details about privileges, see p.38 "Accounts".

Default Accounts

When installation is complete, the following two accounts are provided by default.

Default account	Privilege	Default password
Admin	Administrators	Password set at installation
User	Users	Same as the "Admin" default password

It is possible to add accounts after installation, as necessary. Up to 50 accounts can be created including the "Admin" and "User" accounts. Administrators privileges are required to register new accounts.

$\mathcal{P}$ Reference

For details about registering new accounts, see p.39 "Registering Accounts".

❖ **Administrators privileges accounts**

An Administrators privileges account, or accounts with Administrators privileges, can be assigned to key operators. These give access to all available functions, system configuration settings, network, account, and NIB settings. In IT environments, these settings are normally managed in the following areas:

- IT System and/or Network Administrators
- IT Helpdesk
- IT Desktop Support
- Advanced Technical Support

When logged on using an Administrators privileges account, group passwords are not required.

❖ **Users privileges accounts**

Users privileges accounts can be assigned to general users. These limit access to all available software functions. These accounts allow users to view the device list, view group information, and view the event log.

❒ Devices with embedded Web servers often allow network configuration changes. It is recommended that the network configuration section be password protected to restrict access to these functions.

Device Group Policy

Network devices can be segmented into groups. The creation of smaller groups enables easier and more efficient device management. Devices can be added to a group based on its location, capability, or defined functionality. Some examples of groups are as follows:

- Location: (Floor, Building, Remote Site, etc.)
- Department (Sales, Engineering, Marketing, etc.)
- Color / Black and White Devices
- IP Address Range
- Speed (PPM)
- E-mail Notification

Prior to installation, it is recommended to create a group plan that will determine the following:

- Quantity of Groups
- Group Members
- Location Requirements by Organization
- Group Requirements by Device Capabilities

Determining the Device Group Policy

In large IP network enterprises, it is possible to have a large number of devices that require remote management. In this case, the device management list can quickly become un-manageable. To overcome this issue, smaller more manageable groups can be created. Each organization will have unique needs when defining device groups.

An Administrators privileges account and password is needed to create, modify, rename, or add and delete devices in a group.

🔍Reference

For details about creating device groups, see p.32 "Device Group Creation".

Passwords for Device Groups

Passwords for device groups can be used to prevent unauthenticated users from changing the device group properties. Any user can view device group information.

By default, group passwords are not set. If a group password is set, users cannot make changes unless they enter the password.

❖ **Group passwords and administration**

Administrators privileges are required to create and manage device groups. Users that have Administrators privileges can perform the following tasks:
- Create a New Group
- Change the Name of a Group
- Add Devices to a Group
- Access Group Device Lists
- Delete a Group
- Assign Passwords to Groups

If a user logs on with a "User" logon privilege, the following grouping tasks can be performed:
- View Groups
- Access Group Device Lists

Discovery planning

In large IP enterprise environments, it is typical to have a large number of IP subnet ranges implemented. The application has the ability to discover devices on all or select network segments. It is recommended that a master list of network segments be created prior to discovery configuration. Selected administrators can then quickly configure the subnets that they are required to manage. By isolating device subnet discovery, the discovery time is decreased. Smaller device discovery lists are also easier to manage.

Determining the Discovery Policy

The application's discovery function identifies devices that support Printer MIB (RFC 1759), MIB-II (RFC 1213), and Host Resource MIB (RFC 2790).

To expedite the discovery configuration process, it is important to identify the network segments and IP address ranges that will require device management. The IP network administrator can typically supply the following information:

- Network Range
  - Local Network
  - Remote network
- Discovery Range
  - Specified Subnet
  - Specified Address Range
- Recommended Polling Timing

Two TCP/IP discovery methods are available. It is important to understand the discovery methodology to ensure network efficiency and discovery time.

❖ **Broadcast**

The Broadcast discovery method discovers devices by sending a general SNMP request to all devices contained in the local or specified network.

❖ **Ping Sweep**

The Ping Sweep discovery method discovers devices contained in a range of IP addresses by sending a SNMP request to each IP address.

🔍**Reference**

For details about the discovery method and discovery configuration, see p.27 "Discovery".
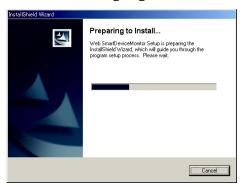
Installing Web SmartDeviceMonitor

This section describes installation procedure for Web SmartDeviceMonitor: both new and update (overwrite) versions.

If Web SmartDeviceMonitor or the previous product (Web SmartNetMonitor) is already installed, the update (overwrite) is automatically installed.

To keep device information from the previous product (Web SmartNetMonitor), do not uninstall it. Perform update (overwrite) installation to preserve device information.

🖉 Note
❒ Installation requires Windows administrative privileges on the server system. Once installed, Web SmartDeviceMonitor cannot be overwritten by the previous product (Web SmartNetMonitor).

1 **Double-click the setup.exe icon to start the InstallShield Wizard. Select the installation language (*1 *2). The [Preparing to Install] dialog box appears.**

Clicking **[Cancel]** will terminate the installation, if necessary. If the Windows installer is not installed or is outdated, the computer will restart automatically. Once restarted, the display in step **2** will appear.

*1 Supported languages are as follows; English, German, French, Italian, Spanish, Dutch.
   Any of the supported languages can be selected for the installation language. The operating system can be in any of the supported languages. Any combination of supported operating system language and installation language can be used.
   (The interface language in Web SmartDeviceMonitor server cannot be changed after installation.)
*2 For operations using a web browser on client computers, the interface language can be selected at logon, regardless of the language selected at installation.

B **The [Welcome to the Web SmartDeviceMonitor Install Wizard] dialog box appears.**

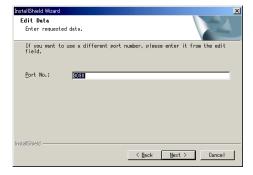Click **[Next]** to continue installation.

🖉 Note

❒ If there is device information preserved, clicking **[Next]** displays the confirmation message about keeping it. To keep device information, select **[Yes]** to proceed to step **G**. If this installation is a previous product update (Web SmartNetMonitor), selecting **[Yes]** takes you to step **F**. To clear device information, select **[No]** to proceed to step **C**.

C **The [Choose Destination Location] dialog box appears.**

Select the folder where Web SmartDeviceMonitor is to be installed. Then, click **[Next]**.

The default folder is **[System Device]**: Program Files RMWSNM.

D **The [Edit Data] dialog box appears.**

Enter the port number used by the Web browser.

The default port number is 9090. This port is selected to prevent duplication of any other HTTP service that may already be in use.

Click **[Next]**.

E **Enter the "Admin" password, and then click [Next].**

Up to 16 alphanumeric characters, spaces, and symbols can be entered for the password. The following characters cannot be used: " & ' = ^ | * ; ? > , <

The password entered here is reflected as the initial value of the "User" logon account password.
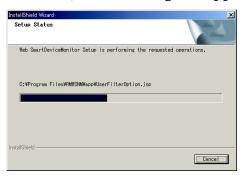
If necessary, change the "User" password after installation.
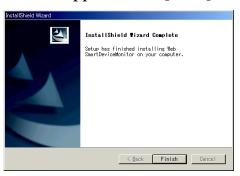

F **The [Start Copying Files] dialog box appears. The setting values appear. If OK, click [Next] to begin the installation.**

G **The [Setup Status] dialog box appears next to indicate the setup progress.**

19

H **When the message about completing the installation of Web SmartDevice-Monitor appears, click [Finish] to complete installation.**

I **After installation, Web SmartDeviceMonitor automatically starts initial discovery for the local segments.**

J **Check that installation has terminated normally.**

Click the **[Start]** button, and then click **[Programs]**. Check that Web SmartDeviceMonitor has been added to the **[Programs]** menu.

K **Install Device Graphic Update Module after installing Web SmartDeviceMonitor.**

🖉 **Note**

❒ Device Graphic Update Module is required for displaying graphic images in Device Page and displaying device status.

Preserving Device Information

Device information can be preserved when the application is uninstalled. When device information is preserved during uninstallation, it can be retained when the application is reinstalled.

✎ Note

❒ To keep device information from the previous product (Web SmartNetMonitor), do not uninstall it. Perform update (overwrite) installation to preserve device information.

If you decide not preserve the device information, it will be deleted when Web SmartDeviceMonitor is uninstalled.

Note the following about preserving the device information:

- When the application is installed for the first time, no device information is preserved.
- The device information preserve option is available only when uninstalling or installing updates (overwrite).

Note the following when re-installing Web SmartDeviceMonitor:

- If the device information is preserved when the application is uninstalled, it will be possible to preserve this information upon re-installation.
- If the device information is not preserved when the application is uninstalled, device information cannot be preserved when the app0lication is re-installed.

The following table contains information about preserved items, passwords, and so on for different types of installation.

	Installation directory	Port number, Admin / User passwords	Preserved items
New installation	Location specified at installation. The default is **[System-Drive]**: \Program Files\RM-WSNM.	Passwords specified at installation. The default port number is 9090. Password must be entered at installation.	None
Update (overwrite) installation from Web SmartDeviceMonitor with "preserve option" not selected	Directory of the previous installation cannot be changed.	Passwords specified at installation. The default port number is 9090. Password must be entered at installation.	None
Update (overwrite) installation from Web SmartDeviceMonitor with "preserve option" selected	Directory of the previous installation cannot be changed.	The current values cannot be changed.	• Basic preserve d items • Account setting

21

	Installation directory	Port number, Admin / User passwords	Preserved items
Update (overwrite) installation from the previous product (Web SmartNetMonitor) with "preserve option" selected	Directory of the previous installation cannot be changed.	Passwords specified at installation. The current port number cannot be changed. Password must be entered at installation.	Basic preserved items

The following are the basic preserved items in the table above:

- List columns setting
- List entries setting
- Discovery setting
- Staus Poling setting
- E-mail setting
- Custom searches
- Group passwords
- E-mail Addresses
- e-mail notification conditions
- Discovered devices
- Groups
- Filters
- Port number

Note

❒ Update installation from the previous product (Web SmartNetMonitor) does not keep account settings even if the preserve option is selected. Only two accounts: "Admin" and "User" are provided, as with the first installation. Add accounts and specify passwords as required.

Reference

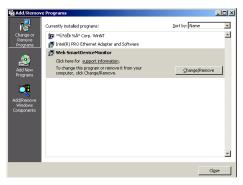For details about accounts, see p.38 "Accounts".

Uninstalling

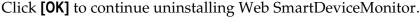Use **[Add/Remove Programs]** of Windows Control Panel to uninstall Web Smart-DeviceMonitor.

Note

❒ For details about uninstalling the previous product (Web SmartNetMonitor), see Web SmartNetMonitor Administrator's Guide.

❒ To keep device information from the previous product (Web SmartNetMonitor), do not uninstall it before updating.

A **Quit Web SmartDeviceMonitor if it has been started.**

B **Click the [Start] button, point to [Settings], and then click [Control Panel].**

C **Double-click [Add/Remove Programs].**

The **[Add/Remove Programs]** dialog box appears.

D **Select Web SmartDeviceMonitor, and then click [Change/Remove].**

E **The confirmation message about uninstalling the application appears.**

Click **[OK]** to continue uninstalling Web SmartDeviceMonitor.
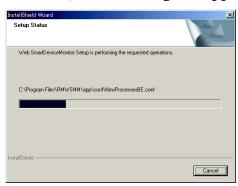
F **The message asking to preserve the list of devices and device information appears.**

Click **[Yes]** to preserve the device information. The device information can then be preserved when the application is re-installed.

Click **[No]** to uninstall the application without preserving the device information.

23

G **The [Setup Status] dialog box appears next to indicate the deletion progress.**

H **When the message about completing maintenance appears, click [Finish] to complete deletion.**

User Interface

Browsing the Application from a Client

To access the Web SmartDeviceMonitor server from a client, launch a Web browser and enter the following URL in the address line:

http://[IP address]: [port number]/wsdm

The default port number is 9090.

If the access to the Web SmartDeviceMonitor server is successful, you will be prompted for a login name, password, and language.

Enter a login name and password, and select a language to access Web Smart-DeviceMonitor window.
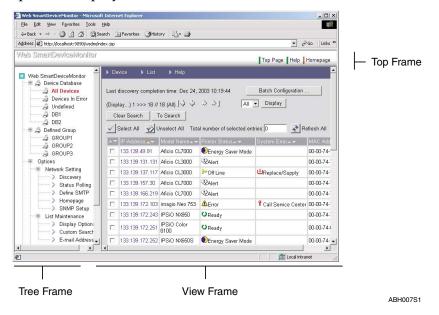
Web SmartDeviceMonitor Window

This section describes the main application window. The window consists of the following three frames:

- Top Frame:
    - Displays the product name and links to the top page, home page, and help topics.
- Tree Frame:
    - Displays the applications major functions and subheadings. The tree frame lists the categorized and defined groups and the configuration-related functions. The available menu items and content displayed in the view frame depend on the function selected in the tree.

- View Frame:
  - Displays the device list of discovered devices. The device list columns contain status information for the discovered devices. The menu bar at the top of the view frame displays the available menu items according to the contents displayed in the view frame. The menu bar appears when a device or group list is displayed.

Top Frame

Tree Frame   View Frame

ABH007S1

Discovery and Status Polling

The application periodically performs device discovery to identify and confirm all devices in the discovery IP target range. This information is then recorded in the device database. The status polling function periodically updates the device status information. Status polling information is recorded in the device database.

Discovery

The scheduled discovery function is used to add new devices as required. When searching for a device, the device that matches the criteria from the device database is detected.

A device database containing all device information is created when discovery is performed for the first time. After the device database is created, discovery is performed periodically. The database is then queried for device information.

Device discovery uses the standard SNMP protocol to detect devices.

The management information base (MIB) is an object set that defines the available types of devices. The application can detect devices that conform to Printer MIB (RFC 1759), MIB-II (RFC 1213), and Host Resource MIB (RFC 2790).

Devices must have an IP address to be detected.

Devices can also be registered in the device database manually, by specifying their IP addresses.

❖ **Items updated during device discovery:**
- Model Name
- Device Name
- MAC Address
- Comment
- IP Host Name
- PPM
- B&W / Color
- NIB Model
- NIB Version
- NetWare Print Server
- NetWare Mode
- NetWare File Server
- NetWare Context Name
- Input Tray
- Input Tray Paper Size
- Input Tray Paper Orientation
- Input Tray Remarks
- Output Tray
- Toner Color

❖ **Discovery setup**
Broadcast is used to detect devices in a specified TCP/IP subnet. Ping sweep is used to detect devices within the specified IP address range.

❖ **Broadcast:**
Broadcast is a discovery method that discovers devices by sending a general SNMP request to all devices contained in the local or specified network and listens for the responses from the devices.
If Web SmartDeviceMonitor detects a device that has not been recorded in the device database or incorrect device information in the database, it updates the database with the current information.
Multiple subnets can be specified (up to 255 subnets).

✐ **Note**
❒ You can also specify a classless subnet mask (255.255.128.0, 255.255.255.224, etc.).
Broadcast may not be effective depending on the network environment. For example, if Discovery is performed over the local segment, devices may not be discovered depending on the router broadcast settings or device subnet address settings. In this case, use Ping Sweep to perform Discovery.
Discovery cannot be performed if the routers do not pass broadcast packets.

❖ **Ping Sweep:**
Ping sweep is a discovery method that discovers devices contained in a range of IP addresses by sending a SNMP request to each IP address. An address range can be specified.
Because ping sweep is extremely accurate, it can be very slow on large networks.

📝 **Note**

❒ You can also specify a classless subnet mask (255.255.128.0, 255.255.255.224, etc.).
The time required by discovery depends on the network environment and discovery method. It is recommended to set the device discovery process to occur during off hours to minimize the effect on the network.

Use **[Options]**-**[Network Setting]**-**[Discovery]** to set the following items.

Item	Explanation
Broadcast:	
Local Network	Enable/disable broadcast for local nets.
Specified Subnet	Specify the subnet for performing broadcast.
Modify Subnet List	Modification of subnet list function.
Ping Sweep:	Enable/disable ping sweep for a specified IP range.
Specified IP Address	Specify the IP range of the ping sweep target. Specify Address must be on.
Discovery Schedule and Time to Refresh	The date and time and interval for performing Discovery can be specified.
	Default: 00:00 daily
Timeout (sec.)	Specify the device response wait time.
	A larger timeout value increases discovery time if a device is not connected to the network for some reason such as its power is turned off.
	Default: 3 seconds

Use **[Options]**-**[Network Setting]**-**[SNMP Setup]** to set the following items.

Item	Explanation
Read Community Name	Specify the community name when reading device information.
	Default: public
Write Community Name	Specify the community name when writing device information.
	Default: admin

Read community name is used for "get" operations (status and information). Write community name is used for "set" operations (energy saver, reset, job cancellation, and batch configuration).

Set the same read community name and write community name specified for the network device.

❖ **Starting discovery**

When the Discovery settings are changed, the discovery process starts immediately.

❖ **Performing immediate discovery**

Discovery can be performed immediately regardless of the discovery schedule configured in the device discovery settings.

Use **[Options]**-**[Network Setting]**-**[Discovery]**-**[Apply]** to perform discovery.

Item	Explanation
Apply	Send the start discovery command to the Web SmartDevice-Monitor server.

❖ **Registering a device manually**

Select **[Device]**-**[Register Device]** on the device database page. Specify the device's IP address to discover and register it in the device database.

Status Polling

To retrieve the device status information, the application polls each device recognized by the discovery method. Discovery is based on the configured schedule. Once complete, the newly retrieved device status information is used to update the device database.

❖ **Items updated during status polling:**

- System Error
- Printer Status
- Scanner Status
- Fax Status
- Copier Status
- Total Counter
- Printer Counter
- Fax Counter
- Copier Counter
- Input Tray Status
- Output Tray Status
- Toner Status
- Error Details
- Latest Communication Time
- MAC Address

✎ **Note**

❒ If a device with a status of "No Response" is physically moved, the device must be manually deleted from the device database.

Some device information in the device list may appear in gray text or background in the following state:

- Immediately after update (overwrite) installation of Web SmartDeviceMonitor, the background of device information preserved from the previous product (Web SmartNetMonitor) may appear gray. When Web SmartDeviceMonitor detects the device, device information appears normally.

- If the preceding status polling failed to get the latest status from a device for some reason, the device information appears in gray characters.

❖ **Status Polling setup**
Use **[Option]**-**[Network Setting]**-**[Status Polling]** to set the polling interval.

Item	Explanation
Polling Interval	Specify the interval for retrieving the status of devices monitored by the application.
	A smaller value enables faster device feedback, however network traffic increases.
	Default: 60 minutes
Polling Timeout	Specify the device response wait time.
	A larger timeout value enables more acknowledgement responses from devices, however, polling time increases.
	Default: 3 seconds

4

Device Groups

Devices on a network can be logically grouped. Devices can also be registered in multiple groups.

By assigning a password to a group, only those users who have the password can update the group. Administrators privileges are needed to create or rename groups.

Device Group Creation

Devices can be arbitrarily grouped according to your organizational needs. Some examples of device grouping methods are as follows:

- Location: (Floor, Building, Remote Site etc.)
- Department (Sales, Engineering, Marketing, etc.)
- Color / Black and White Devices
- IP Address Range
- Speed (PPM)
- E-mail Notification

Users that have an Administrators privileges account can perform the following group tasks:

- Create a new group
- Change the name of a group
- Add devices to a group
- Access group device lists
- Delete a group
- Specify e-mail addresses
- Assign passwords to groups

The **[Defined Group]** page displays all registered group lists.

❖ **Creating a new group**
   Navigate to the **[Defined Group]** page. Select **[Group]**-**[Create Group]** on the **[Defined Group]** page. Then, enter the name of the group to be added. Click **[Apply]** to display the new group in the group list.

Device Group Maintenance

❖ **Adding devices to groups**

To add devices to an existing device group, use the **[All Devices]** page to select the device to be added. Next, select **[Device]**-**[Add To Group]** on the menu bar to initiate device selection. The next display enables a user, who logged on using an account with Administrators privileges, to select the group to which the device will be added from the list (pulldown menu). Click **[Enter]**. The device is added to the group and the **[All Devices]** page reappears.

Multiple devices can be added simultaneously to a group by selecting multiple devices from the device list.

❖ **Deleting devices from groups**

On the **[Defined Group]**page, select the group from which you want to delete a device in the tree, and then select the device to be deleted in the view frame. Click **[Device]**-**[Delete Device]** on the menu bar. On the **[Delete Device(s)]** page, click **[Yes]**. The selected device is then deleted from the group.

Multiple devices can be deleted simultaneously from a group by selecting multiple devices from the device list.

❖ **Deleting groups**

On the **[Defined Group]** page, select the group to be deleted from the group list, and then click **[Group]**-**[Create Group]** on the menu bar. On the **[Delete Group]** page, click **[Yes]**. The group is then deleted.

Device Group Security

A user with an Administrators privileges account and password can assign a unique password to a group. Applying a group password prevents unauthorized users from changing or deleting the group. By default, no password is assigned to the group.

If a password is assigned to a group, the application will request this password if a user attempts to change the group contents.

If the group password is deleted, the application will not request any password if a user attempts to change the device group contents.

❖ **Setting device group passwords**

A group password can be set when creating the group. Select **[Group]**-**[Create Group]** on the **[Device Database]** page, and then click **[Specify Password]**.
On the **[Specify Password]** page, enter the password to be set.

❖ **Setting group passwords after creating device groups**

Group passwords can be set after groups have been created. On the **[Defined Group]** page, click the group name in the group list to display the group property page.
Click **[Specify Password]** to display the password page, and then enter the password to be set.

❖ **Deleting group passwords**
To delete a password, enter "null" for the password setting.
(If no password has been set, skip the **[Old Password]** setting.)

4

E-mail Notification

E-mail notification enables device error messages to be sent to user definable e-mail addresses. This function requires a valid SMTP mail server to be configured within the application.

E-mail Notification Contents

The contents of the sent e-mail are as follows:

❖ **From:**
Sender address

❖ **To:**
Recipient address specified on the **[Confirm E-mail Address]** page under **[Device/Group]**-**[E-mail Setup]**.

❖ **Subject:**
Subject of the e-mail

❖ **Error Contents**

❖ **Error Details (including the service call No.)**

❖ **Device Information**
Host Name
IP Address
MAC Address
Model Name
Serial Number
NIB Comment
NIB Version
Total Counter
Printer Version
System Version
Emulation Name
Emulation Version
Device Page URL (a device page can be accessed using this URL)
(If the e-mail software is capable of handling active URLs, clicking the address will enable direct access to the device).
Reference (contact information)
Registered Group

Timing for Sending Error Messages

If status polling detects a device error, e-mail is promptly sent to the specified address.

E-mail Configuration Settings

Select **[Options]**-**[Network Setting]**-**[Define SMTP]**.

Item	Explanation
SMTP Server	Specify the SMTP server that is used to send e-mail.
From	Specify the sender e-mail address. This is usually the e-mail address of the administrator.
Subject	Specify the e-mail subject.
Reference	Specify the contact information. Reference is used as the contact information in the sent e-mail.

Creating address lists

Use the **[E-mail Addresses]** page to specify the e-mail addresses where the device error status is to be sent.

Register the e-mail addresses to be displayed as candidates.

Select **[Options]**-**[List Maintenance]**-**[E-mail Addresses]** to create an e-mail address list.

Item	Explanation
Add New	Use the following procedure to register a new e-mail address.
Modify	Use the following procedure to change a registered e-mail address.
Delete	Use the following procedure to delete unnecessary e-mail addresses.

❖ **Setting e-mail addresses for error messages**

Use **[All Devices]** to select a device. Select **[Device]**-**[E-mail Setup]** from the menu bar. Set the desired e-mail address for each of the listed error conditions for the selected device.

It is possible to configure e-mail notification by group. Click **[Defined Group]** to select a group. Select **[Group]**-**[E-mail Setup]** from the menu bar. Set an e-mail address for each of the following errors for the devices belonging to the selected group.

- Call Service Center
- No Toner
- Paper Misfeed
- No Paper
- Cover Open
- Miscellaneous Error
- Off Line
- Low Toner
- Attention

Displaying the **[Confirm E-mail Address]** page allows you to confirm and/or change the current e-mail address setting for errors.

To display a device's e-mail address setting, select the device on the device list page, and then select **[Device]**-**[E-mail Setup]** to display the **[Confirm E-mail Address]** page.

To display a group's e-mail address setting, select the group on the **[Defined Group]** page, and then select **[Group]**-**[E-mail Setup]** to display the **[Confirm E-mail Address]** page.

Display	Explanation
Blank	No e-mail address is set.
E-mail address	The e-mail addresses already set for the device/group are displayed. If multiple devices/groups are selected, the e-mail addresses are displayed only if they are set for all devices/groups. If any of these devices/groups has a different e-mail address, no e-mail address is displayed and the "Different e-mail addresses" message appears.
"Different e-mail addresses" message	Different e-mail addresses are set for different devices/groups. This appears only when multiple devices/groups are selected.

E-mail address settings for individual devices can be exported to a file in CSV format for confirmation.

37

Accounts

By default, the "Admin" and "User" accounts are created upon installation. Up to 50 user accounts can be issued, including the default accounts. A password must be assigned to each account.

When creating accounts, assign one of the following levels of privilege for each account:

- Administrators
- Users
- Device Administrators

The table below lists the operations available for each type of privilege.

Operation	Administrators	Users	Device Admin- istrators
[Options] > **[List Maintenance]** > **[Display Options]**	yes	no	no
[Options] > **[Network Setting]** > **[Discovery]**	yes	no	yes
[Options] > **[Network Setting]** > **[Status Polling]**	yes	no	yes
[Options] > **[Network Setting]** > **[SNMP Setup]**	yes	no	yes
[Options] > **[Network Setting]** > **[Define SMTP]**	yes	no	yes
[Options] > **[List Maintenance]** > **[Custom Search]**	yes	no	no
[Options] > **[List Maintenance]** > **[E-mail Addresses]**	yes	no	no
[Options] > **[List Maintenance]** > **[Homepage]**	yes	no	no
[Options] > **[Login Users]** : Registering, changing, and deleting users	yes	no	no
[Device Database] > Editing filter properties	yes	no	no
[Defined Group] > Editing group properties	yes	no	no
[Device Database] > **[Filter]** > **[Create Filter]**	yes	no	no
[Defined Group] > **[Group]** > **[Create Group]**	yes	no	no
[Device Database] > **[Device]** > **[Add To Group]**	yes	no	no
[Device Database] / **[Defined Group]** > **[Device]** > **[E-mail Setup]**, **[Defined Group]** > **[Group]** > **[E-mail Setup]**	yes	no	no

Operation	Administrators	Users	Device Administrators
Displaying the device Web page from **[Device Page]**	yes	yes	yes
[Options] > **[NIB Setup Tool]**	yes	no	yes
Displaying **[Event Log]** page	yes	no	yes
[Defined Group] > **[Group]** > **[Energy Saver]**, [**Energy Saver Off]** **[Device Database]** / **[Defined Group]** > **[Device]** > **[Energy Saver]**, **[Energy Saver Off]**	yes	no	yes
[Reset] on the device page	yes	no	yes
[Cancel Current Job] and **[Cancel All Jobs]** on the device page	yes	no	yes
[Device Database] / **[Defined Group]** > **[Batch Configuration]**	yes	no	yes
[Device Database] > **[Device]** > **[Delete Device]**	yes	no	no
[Defined Group] > **[Device]** > **[Delete Device]**	yes	no	no

Registering Accounts

Use **[Option]**-**[Login Users]**-**[Add New]** to register a new account. The users currently registered appear on the **[User Account Setting]** page. Click **[Add New]** to display the **[Each Account Setting]** page, and then enter the user name you want to register. In addition, select a privilege you want to assign to the account.

Passwords must also be assigned for accounts. Up to 16 alphanumeric characters, spaces, and symbols can be entered for the password. The following characters cannot be used:

" & ' = ^ | * ; ? > , <

Administrators privileges are required to register new accounts.

4

Using the Device Database

All devices that are registered in the device database are displayed on the **[All Device]** page. The following capabilities can be accessed from the device database page:

- Changing the display
  The device display range and order can be changed.

- Searching
  Devices can be searched based on user definable search criteria. Narrow search is also available.
  The search criteria can be saved and re-used for subsequent device searches.

- Displaying the device page
  A device page can be displayed to view detailed information specific to that device. From the device page, users can also access the internal Web management service of the network device.

- Registering devices to a group
  A selected device can be registered to an existing group.

- Displaying the error history
  The error history of a selected device can be displayed.
  The displayed error history can be exported as a CSV file.

- Saving the device list to a file
  A list of all devices based on the search results can be exported as a CSV file.

- Setting e-mail notification
  E-mail error notification can be sent to delegated personnel upon device error. E-mail recipients can be configured utilizing this tool.

- Controlling devices
  Energy Saver mode can be initiated to the ON or OFF setting.

- Deleting devices
  Devices can be deleted from the device database.

- Updating information
  Status queries can be performed to retrieve and update device status. Update information appears and is added to the device database upon status polling completion.

The devices displayed on the **[All Device]** page can be organized using various filters, according to the administrator's device management needs. By default, the **[Devices In Error]** and **[Undefined]** filters, which might be used frequently, are provided. Use filters to effectively extract the target devices.

- **[Devices In Error]** filter
  All devices with error status are extracted regardless of the group that they belong to.

- **[Undefined]** filter
  Devices that do not belong to any defined group are extracted.

The operations performed on the device database page are reflected directly to the device database. For example, when a device is deleted on the **[All Devices]** page, the device is deleted from the device database.

Device List Columns

Device list columns are used to display device status and other information about discovered devices. The following aspects of device list columns can be custom configured based on your organizational needs:

- Type of columns
- Number of columns
- Order of columns

❖ **Default device list columns**

- IP Address
- Model Name
- Printer Status
- System Status
- MAC Address

❖ **Optional device list columns**

- Device Name
- PPM
- B&W / Color
- Scanner Status
- Fax Status
- Copier Status
- NIB Model
- NIB Version
- Total Counter
- Printer Counter
- Fax Counter
- Copier Counter
- Latest Communication Time
- NetWare Print Server
- IP Address
- Registered Groups
- Comment
- Host Name

❖ **Changing the device list columns**
To add, remove, or change the order of device list columns, follow these instructions:
Select **[Options]**-**[List Maintenance]**-**[Display Options]** to view the current display list column settings. To add a column, select the desired column in the **[Available Selection]** list, and then click **[Add]**. To remove a column, select the desired column in the **[Display]** list, and then click **[Delete]**. To change the order, select the desired column in the **[Display]** list, and then click up or down arrow.
The resulting changes made to device list columns are then displayed in the device list page.

❖ **Changing the number of list entries**
The number of devices that appear in the device list can be configured as follows:
• Display "All" devices
• 25 devices
• 50 devices
• 100 devices
Select **[Options]**-**[List Maintenance]**-**[Display Options]** to display the current list entry settings. Select the desired list entry amount for the device list in the **[Default Number of List Lines]** box.

❖ **Searching for devices**
Specific devices can be found using one or more of the following search criteria. User-defined search criteria saved in custom searches are additional search options.
• All Devices
• Device Name
• Comment
• Model Name
• MAC Address
• Host Name
• IP Address
• IP Host Name
• NIB Model
• NIB Version
• PPM
• B&W / Color
• Printer Status
• Scanner Status
• Fax Status
• Copier Status
• Total Counter
• Latest Communication Time
• NetWare Print Server
• Registered Groups
On the **[All Devices]** page, click **[To Search]** to perform a search using the above mentioned search criteria. Clicking **[Search]** initiates the search command.

5

43

❖ **Sorting the device list**

Devices can be sorted in ascending or descending order for each device list column being displayed. This is achieved by selecting the up and down arrows located at the right of each display list column heading.

❖ **Exporting the device list**

The information (e.g., model names, IP addresses, printer status, page counter) of registered devices can be exported as a CSV file.

On the menu bar, select **[List]**-**[Export]** and select the location where the exported file is to be saved.

❖ **Setting e-mail addresses for error messages**

Select **[All Devices]** to select a device to configure e-mail notification settings. Select **[Device]**-**[E-mail Setup]** on the blue heading tool bar. An e-mail address can be configured for each of the following error conditions:

- Call Service Center
- No Toner
- Paper Misfeed
- No Paper
- Cover Open
- Miscellaneous Error
- Off Line
- Toner Almost Empty
- Attention

   $\mathcal{P}$**Reference**

   For details about e-mail address settings, see p.35 "E-mail Notification".

❖ **Setting energy saver mode to OFF / ON position**

The energy saver mode can be set for single or multiple devices.

Select the device or device(s) to be modified by selecting the check box beside the device name. Select **[Device]** (or **[Group]** in the group list) - **[Energy Saver]** or **[Energy Saver Off]** on the blue heading tool bar. Select **[OK]** to initiate your selection.

Custom Search

A custom search narrows the device search thus reducing the number of devices to be detected. This enables specific devices to be found faster.

Clicking **[To Search]** on the **[All Devices]** page displays the **[Search]** area at the bottom of the device list.

When clicking **[Search]**, the search is performed using the selected search criteria. When one or more matching devices are detected, they appear in the result list.

To narrow the search further, select new search criteria and perform the search again. Search criteria can be added to the **[Custom Search History]**.

The following table lists the available items with comparison conditions for a custom search.

Item	Comparison condition
Device Name	Include, Not Include, Same, Not Same
Comment	Include, Not Include, Same, Not Same
Model Name	Include, Not Include, Same, Not Same
MAC Address	Include, Not Include, Same, Not Same
IP Host Name	Include, Not Include, Same, Not Same
NIB Model	Include, Not Include, Same, Not Same
NIB Version	Include, Not Include, Same, Not Same
NetWare Print Server	Include, Not Include, Same, Not Same
IP Address	Include, Same, Not Same, More Than, Less Than, Same as or More Than, Same as or Less Than
PPM	Same, Not Same, More Than, Less Than, Same as or More Than, Same as or Less Than
B&W / Color	Same, Not Same
System Error	Same, Not Same
Printer Status	Same, Not Same
Scanner Status	Same, Not Same
Fax Status	Same, Not Same
Copier Status	Same, Not Same

❖ **Specifying parameters that accompany search criteria**
The following items must be entered depending on the selected search criteria.

Item	Explanation
Device Name	Character string
Comment	Character string
Model Name	Character string
MAC Address	Character string
IP Address	Character string
IP Host Name	Character string
NIB Model	Character string
NIB Version	Character string
PPM	Character string
NetWare Print Server	Character string
B&W / Color	B&W or color
System Error	Status selection
Printer Status	Status selection
Scanner Status	Status selection
Fax Status	Status selection
Copier Status	Status selection

For a character string, the devices that include the entire specified character string appear in the search result.
For a numeric value, the devices that have a value exceeding the specified value appear in the search result.

❖ **Parameter addition**
Add a parameter according to the selected search option to perform a narrow search.

❖ **Custom search registration**
The performed search criteria can be registered and reused.
In **[Custom Search]**, click **[Save Custom Search]**, and then specify a custom search name to register the displayed search criteria.
Up to 100 custom searches can be registered.

❖ **Custom search rename / deletion**
Use **[Option]**-**[List Maintenance]**-**[Custom Search]** to rename and delete custom searches.

Item	Explanation
Change Name	Rename user defined filters.
Delete	Delete user defined filters.

Filters Creation

The application provides a method for registering the status and conditions of the devices as a filter in advance, so that you can manage and monitor the devices. This method is effective for extracting devices within specific IP address ranges or devices that have specific error states.

Predefining the devices to be searched is more convenient than searching manually by using the device list.

By default, **[Devices In Error]** and **[Undefined]** filters are configured.

❖ **Adding new filters**
Select **[Filter]**-**[Create Filter]** on the **[Device Database]** page. Then, enter the name of the filter to be added. Select a filtering criterion in the **[Search Component]** list, and then specify the appropriate option and parameter to configure the search criterion. Click **[Apply]** to display the new filter in the filter list.

❖ **Setting passwords**
If necessary, a password can be set when creating the filter. Select **[Filter]**-**[Create Filter]** on the **[Device Database]** page, and then click **[Specify Password]**. On the **[Specify Password]** page, enter the password to be set.

❖ **Setting passwords after creating filters**
Passwords can be set after filters have been created. On the **[Device Database]** page, click the filter name in the filter list to display the filter property page. Click **[Specify Password]** to display the password page, and then enter the password to be set.

5

Using Groups

Once the group function is selected from the tree menu, group specific options can be selected from the headings located on the menu bar. The following configuration options are available when working with groups:

- Changing the display
  All available groups with their associated devices appear.
  The display range and order of the groups and devices can be changed.

- Creating groups
  A new group can be created.

- Deleting groups
  Existing groups can be deleted.

- Deleting device registration
  A device can be released from a group.

- Displaying error history
  Device error history can be displayed by group or by device.
  Error history can also be exported as a CSV file.

- Saving group list
  The group list or list of devices registered to a group can be exported as a CSV file.

- Setting e-mail notification
  E-mail notification can be configured for groups.
  Recipient e-mail addresses can be registered for groups.

- Energy Saver mode settings
  Devices can be switched to and recovered from the Energy Saver mode.

- Updating information
  Status polling is performed to retrieve group device status. Updated information is written to the device database and appears within the device list page.

❖ **Changing the number of group list entries**
The number of groups that appear in the group list can be configured as follows:
- Display "All" groups
- 25 groups
- 50 groups
- 100 groups
Select **[Option]**-**[List Maintenance]**-**[Display Options]** to display the current list entry settings. Select the desired list entry amount for the group list in the **[Default Number of List Lines]** box.

❖ **Sorting the group list**
Groups can be sorted in ascending or descending order for each group list column being displayed. This is achieved by selecting the up and down arrows located at the right of each column heading.

❖ **Exporting the group list**

The information (e.g., model names, IP addresses, printer status, page counter) of the registered devices can be exported as a CSV file.

On the menu bar, select **[List]**-**[Export]**, and then select the location where the exported files is to be saved.

❖ **Setting e-mail addresses for error messages**

Select **[Defined Group]** to select the desired group to configure e-mail notification. Select **[Group]**-**[E-mail Setup]** on the blue heading tool bar. An e-mail address can be configured for each of the following error conditions:

- Call Service Center
- No Toner
- Paper Misfeed
- No Paper
- Cover Open
- Miscellaneous Error
- Off Line
- Low Toner
- Attention

🔍**Reference**

For details about e-mail address settings, see p.35 "E-mail Notification".

Displaying the Device List of Each Group

The device lists of groups can be displayed. When a device group appears, the same operations as those of **[Device Database]** are enabled.
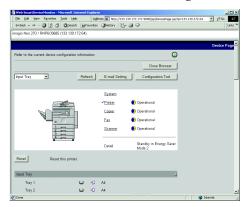
The following function is available only for groups. It is not available for **[Device Database]**.

- Delete Device
  The group attribute of the device is deleted from the device database.

Using Device Page

In **[All Devices]**, click the IP address of the target device to display a device page specific to that device. Detailed information of individual devices can be displayed from this page. If a device page of a device that is not stored in the device database is accessed, a message indicating that the device does not exist appears.

Operations that can be performed from the device page are as follows:

- Resetting the device
- Canceling the current print job
- Canceling all jobs - the current print job and spooled jobs
- Setting the e-mail notification address

✐ Note
❒ To perform the reset and cancel functions described above, the SNMP write community name must be the same as the device's.

Items that can be displayed and checked on the device page are listed below. Items that can be displayed vary depending on device type.

- Input Tray
- Output Tray
- Toner
- Counter
- Optional Units
- Functions
- Document Server
- Printer Language
- Reference
- Network
- Registered Group

❖ **Linking to the Web pages of devices**
Click **[Configuration Tool]** to link directly to the device Web page.
The device Web page supports the detailed device settings. If the device does not support a function, the corresponding item or button is not displayed.

5

Using Batch Configuration

For example, when changing items such as the community name and password, the settings can be configured by batch for multiple devices. Batch configuration can reduce the administrative burdens and time resulting in reduced management costs.

The following tables list the items that can be configured by batch.

❖ **General**

Item	Explanation	Setting
NetWare protocol	NetWare protocol status setting	Enable / disable
AppleTalk protocol	AppleTalk protocol status setting	Enable / disable
NetBEUI protocol	NetBEUI protocol status setting	Enable / disable
URL name	Name of the "Homepage" or "URL" hyperlink in the device page header area	Character string
URL	URL to the "Homepage" or "URL" hyperlink in the device page header area	Character string
Device control panel menu lock	Control panel setting	Enable / disable

❖ **TCP/IP**

Item	Explanation	Setting
Network boot	TCP/IP boot information	Enable /disable
WINS	WINS status setting	Enable /disable
Primary WINS server	Primary WINS server setting	Address
Secondary WINS server	Secondary WINS server setting	Address
LPR	LPR status setting	Enable /disable
RSH/RCP	RSH/RCP status setting	Enable /disable
DIPRINT	DIPRINT status setting	Enable /disable
FTP	FTP status setting	Enable /disable
IPP	IPP status setting	Enable /disable

❖ **SNMP**

Item	Explanation	Setting
Community name	Community name setting	Character string
Access type	SNMP community access type setting	Not accessible, read-only, read-write, trap
Protocol type	SNMP community protocol type setting	TCP / IP+IPX, IPX, TCP/IP , OFF
Manager IP address	Host IP address setting	Address
Manager IPX address	Host IPX address setting	Address

❖ **AppleTalk**

Item	Explanation	Setting
Setup zone name	Name of operation zone where the printer belongs	Character string

❖ **NetBEUI**

Item	Explanation	Setting
Workgroup name	Workgroup where the printer belongs	Character string
Notify Print Completion	NetBEUI interface mode setting	

❖ **Paper Type**

Item	Explanation	Setting
Tray 1 to n paper type (including bulk input tray and by-pass tray)	Paper type setting of each mounted tray	Plain/recycled paper, etc.
Bulk input tray paper type	Paper type setting of mounted bulk input tray	Plain/recycled paper, etc.
Bypass tray paper type	Paper type setting of mounted bypass tray	Plain/recycled paper, etc.

❖ **Displaying devices and items that can be configured by batch**

Select the devices or groups to be batch configured, and then click **[Batch Configuration]**. The **[Batch Configuration]** page appears.

Clicking **[Batch Configuration]** with no device selected allows you to batch configure all devices in the device list.

📝 **Note**

❒ Combine the search function and batch configuration for more effective batch configuration.

On the **[Batch Configuration]** page, the selected devices or groups are roughly categorized using three colors (red, yellow, and green), based on the types of items that can be configured. The maximum number of items can be configured by batch by selecting the devices that have the same color from the categorized devices. However, the same items cannot always be set for all devices categorized by the same color.

📝 **Note**

❒ The items that cannot be configured are not listed.

Batch configuration results can be checked by using the event log. Use **[All Log]**-**[Batch Configuration]** to view the event log.

📝 **Note**

❒ Some devices that are not eligible for categorization do not appear in the categorized list.

Using NIB Setup Tool

The Administrators or Device Administrators privileges are required to access the NIB (Network Interface Board) setup tool.

This tool can be used to access and configure the NIB settings of network devices directly from the client computer. The following settings can be configured with the NIB setup tool:

- Device name and device comments
- TCP/IP
- NetWare
- NetBEUI
- AppleTalk
- NIB tool password

To ensure security, access to the NIB setup configuration settings can be password protected.

✐ Note

❒ The NIB setup tool configuration is limited to devices located on the local IP network segment.

Using Event Logs

Web SmartDeviceMonitor operation logs can be displayed and are stored in a database. Unnecessary logs can also be deleted.

Operation logs from up to 45 days are saved. When 45 days are exceeded, the operation logs are deleted automatically in units of days starting from the oldest operation logs.

During daily management, it is recommended that the operation logs be saved periodically as a CSV file.

The event items are described below:

Level

Indicates the severity of the log contents.

❖ **Error**
Indicates a severe error. Data or function information has been lost.
For example, the device database cannot be opened or updated.

❖ **Warning**
Informs the user to take preventative action.
For example, e-mail cannot be sent, out of memory, or status polling cannot be performed.

❖ **Information**
Indicates that processing was performed normally.

Function

Indicates the function for which the event occurred.

The function classifications are as follows:

- Discovery
- Status
- Energy Saver
- Energy Saver Off
- Reset
- Job Cancel
- Batch Configuration
- E-mail
- Settings
- Common
- Other (network communication process, account-related process, and so on)

Error Codes

The error codes appear as six-digit values (AABCCC) as shown in the following table.

The first two digits provide important information for notifying the Service Center.

The third digit is 0 or 1. Zero indicates that the administrator should take the required action. One indicates that the Service Center should be notified.

The fourth, fifth, and sixth digits indicate the error code defining the type of error.

Code	Description
AA	Module number 00: Front-end Server 01: Back-end Server 02: Common module
B	Person in charge 0: Administrator 1: Developer (Call Service Center)
CCC	Actual error number. Described in detail below.

The actual error numbers are 3-digit numbers which are described in the following tables.

❖ **General Errors and Others**

Code	Description
000	Completed properly.
001	The operation wasn't completed in time.
002	Object creation has failed.
003	Unknown error has occurred.
004	One or more of required objects not found.
005	One or more of required objects not stored.
006	Data type is invalid.
007	Obtaining the value has failed.
008	Setting the value has failed.

❖ **System**

Code	Description
100	Obtaining the system data has failed.
101	The program has been activated.
102	An error has occurred while starting the service.

❖ **Resources**

Code	Description
150	Expand memory space.
151	The operation has been suspended because of low memory.
152	Shared use failure has occurred.

❖ **Database**

Code	Description
200	No database is open.
201	Setting database has failed.
202	Opening the database has failed.
203	Closing the database has failed.
204	The object cannot be found in the database.

❖ **Files**

Code	Description
250	Opening the data file has failed.
251	Exporting the data file has failed.
252	File not found.

❖ **MO (managed object)**

Code	Description
300	Adding MO has failed.
301	Deleting MO has failed.
302	Updating MO has failed.
303	Obtaining MO data has failed.

❖ **Thread**

Code	Description
350	Creating thread has failed.

❖ **Communication**

Code	Description
400	Communication error has occurred.
401	Communication was not completed in time
402	Access was rejected.
403	MIB write has failed.

❖ **IF**

Code	Description
450	Reference is invalid.
451	Not supported.
452	Internal error has occurred.

❖ **Modules**

Code	Description
500	Starting the module has failed.
501	Parameter is invalid for starting the module.

❖ **Batch Configuration**

Code	Description
550	Batch configuration has started.
551	Some of the configurations were successful.
552	All of the configurations have failed.
553	No response from the Configuration Server.
554	The device does not support the function.
555	Batch configuration is complete, but some values were set differently from those specified.
556	The connected model is different in MAC Address from the registered.

5

Contents

An explanation corresponding to the error code appears.

Device Address

The IP address of the device used for communication for the event appears.

The IP address appears for the following function types: Discovery, Status, Energy Saver, Energy Saver Off, and Reset.

Client Address

The IP address of the client computer used for the operation appears.

Login User Name

The account used for the operation appears.

59

Module

The module for which the error occurred is recorded. This information does not appear on screen. However, it is saved to a file in CSV format.

Comment

Information related to the error is recorded.

The information does not appear on screen. However, it is saved to a file in CSV format.

The following table lists the comments when the event ends normally.

Event	Comment
Device discovery has started.	Discovery target range
Device discovery has finished.	Target device IP address
Device status update has finished.	Target device IP address
Discovery setting complete.	The contents of all Discovery settings
Status Polling setting complete.	The contents of all Status Polling settings
E-mail setting complete.	The contents of all E-mail settings
User logon	Logged on user name

Changing the Number of Error Log Lines

The number of logs displayed on the event log screen can be specified.

Use **[Options]**-**[List Maintenance]** to display the **[Display Options]** page. Select the number of logs to be displayed per page from the **[Error Log]** list.

Stopping and Starting Services

Web SmartDeviceMonitor services starts automatically when installation is completed.

Services can also be stopped and started using the application menu.

If the services are manually stopped, they will automatically start when the system is restarted.

🖉 Note
❒ You need the operating system's Power User privileges or higher to perform the operations described here.

Stopping services

A **Click the [Start] button, point to [Programs]-[Web SmartDeviceMonitor], and then click [Stop Service].**

Starting services

A **Click the [Start] button, point to [Programs]-[Web SmartDeviceMonitor], and then click [Start Service].**

Discovery is performed.

Changing the Port Number after Installation

This section describes how to change the port number set during the installation process.

A **Click the [Start] button, point to [Programs]-[Web SmartDeviceMonitor], and then click [Change Port].**

The **[Change Port]** dialog box appears.

B **Enter the new port number, and then click [OK].**

The new port number is set.

If you choose to change the port number via the application, the service will be stopped and started automatically.

C **The confirmation message about stopping the service appears. To change the port number, click [OK].**

Initializing the Web SmartDeviceMonitor and Settings

This section describes how to initialize the device database and the settings that the application stores.

Initialization clears the device database and resets the settings to the condition immediately after installation.

Before executing initialization, it is recommended that the device database and settings be backed up.

A **Click the [Start] button, point to [Programs]-[Web SmartDeviceMonitor], and then click [Initialize].**

The Web SmartDeviceMonitor service is stopped during initialization.

B **In the same way as installation, enter the "Admin" account password and port number.**

The password and port number entered here are used as the initial settings after initialization.

C **Click [Start Initialize] to perform initialization.**

6

Backing Up and Restoring the Web SmartDeviceMonitor and Settings

It is recommended that the administrator back up the Web SmartDeviceMonitor device database and settings periodically, to ensure there is a set of backups in case the current database or settings becomes corrupted or otherwise unusable.
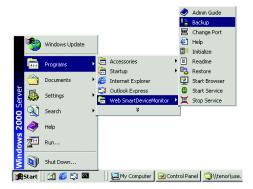
📝 Note

❒ Restoring from the backup file of the previous product (Web SmartNetMonitor) is not supported.

This section describes how to back up and restore the device database and settings that the application stores.

Backing Up the Web SmartDeviceMonitor and Settings

A **Click the [Start] button, point to [Programs]-[Web SmartDeviceMonitor], and then click [Backup].**

The Web SmartDeviceMonitor service is stopped during backup.

B **A dialog box for entering the file location appears. Enter the file location for storing the backup files.**

C **The following message appears when backup is completed.**

Restoring the Web SmartDeviceMonitor and Settings

A **Click the [Start] button, point to [Programs]-[Web SmartDeviceMonitor], and then click [Restore].**

The Web SmartDeviceMonitor service is stopped during restoring.

B **A dialog box for entering the file location appears. Enter the location where the backup files are stored.**

C **The following message appears when restoring is completed.**

65
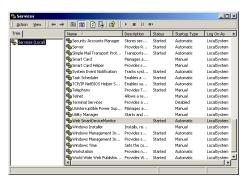
Monitoring Web SmartDeviceMonitor Service

Use the Windows Management Tools to check whether the Web SmartDevice-Monitor service is active.

(For Windows 2000)

A **Click the [Start] button, point to [Settings]-[Control Panel], and then click [Administrative Tools].**

B **Double-click [Services].**

The **[Services]** dialog box appears.

C **In the [Services] list, check the status of the Web SmartDeviceMonitor service.**

7. Appendix

Troubleshooting

In the event of an application error, take the appropriate action listed in the table below.

Trouble	Possible cause and solution
Web SmartDeviceMonitor cannot be installed correctly.	Windows administrative privilege is required when installing Web SmartDeviceMonitor.
	Stop the Web SmartDeviceMonitor service before you update Web SmartDeviceMonitor.
	Uninstall any previous version of Web SmartDeviceMonitor before installing any new version.
	The install completion window is sometimes hidden by the active window. To bring the window to the front, click the corresponding button on the task bar.
Web SmartDeviceMonitor cannot be uninstalled correctly.	Stop the Web SmartDeviceMonitor service before you uninstall.
	Windows administrative privilege is required when uninstalling Web SmartDeviceMonitor.
"No Response from Device" is displayed for the device status.	If the device is not powered, turn it on.
	Check the network is functioning normally.
	If the network traffic is high, the devices may not respond or part of the device information may not be retrieved. For example, when a device is accessed simultaneously from several computers, this may occur (the number of computers depends on the environment). If this phenomenon occurs, use **[Options]**-**[Network Setting]**-**[Status Polling]** to increase the wait time in the **[Polling Timeout]** box.
Discovery takes too much time.	If a wide target range is specified for **[Broadcast]** or **[Ping Sweep]** in **[Options]**-**[Network Setting]**-**[Discovery]**, Discovery will take time. Use the **[Modify Subnet List]** or **[Manager IP Address]** page to narrow the target range, and then perform Discovery.
Discovery does not detect devices successfully.	If Discovery is performed over the local segment, devices may not be detected depending on the router broadcast settings or device subnet address settings. In this case, Ping Sweep may be used to discover the devices.
	If a device is not connected to the network for some reason such as its power is turned off, Discovery cannot detect the device.

Trouble	Possible cause and solution
The NIB setup tool displays the MAC address as "Not Obtained".	There is a possibility that the MAC Address might be displayed as "Not Obtained" when trying to browse through Network Setup Tool via the TCP/IP protocol.
	To check the MAC addresses of the devices, select the target device in the **[NIB Setup Tool-Network board]** list, and then click **[Next]**.
The Web SmartDeviceMonitor logon window does not appear.	The port number specified on the client computer is incorrect.
	Specify the same port number as that of the Web SmartDeviceMonitor server. The default port number is 9090.
The device list, error history, or event log cannot be exported as a CSV file.	Internet Explorer 6 automatically activates Microsoft Excel (or other spreadsheet application) as a plug-in when you select **[Export]**.
	If the CSV file is not associated with an application, use a text editor application (e.g. Notepad) to associate the CSV file with an application.
	If the CSV file is associated with an application, save the exported data from within the plug-in application.
	To associate a CSV file with an application, click **[Folder Options]** on the **[Tools]** or **[View]** menu of Windows Explorer.
	Then, assign the association using the **[File Types]** tab of the **[Folder Options]** dialog box.
	In some cases, the CSV file may be downloaded automatically without the Download Confirmation dialog box being displayed.
	If this occurs, click the **[File Types]** tab in the **[Folder Options]** dialog box from Windows Explorer.
	Then, select the **[Confirm open after download]** check box of the CSV file settings.
Clicking **[Energy Saver]** in the **[Group]**or **[Device]**Device menu does not switch the device to Energy Saver mode.	The SNMP write community name for the device and Web SmartDeviceMonitor may not match.
	Set the same SNMP write community name for the device and Web SmartDeviceMonitor.
Clicking **[Energy Saver Off]** in the **[Group]** or **[Device]** menu does not recover the device from Energy Saver mode.	
Clicking **[Reset]** in the **[Device Page]** does not reset the device.	
Clicking **[Cancel Current Job]** or **[Cancel All Jobs]** on the device page does not cancel the print job.	

7

Trouble	Possible cause and solution
Immediately after Web Smart-DeviceMonitor update (over-write) installation, the device information preserved from the previous product (Web Smart-NetMonitor) appears gray.	When Web SmartDeviceMonitor detects the device, device information appears normally.
Device information is displayed with gray characters.	The preceding status polling failed to get the latest status from the device for some reason.
Only two accounts: "Admin" and "User", were provided after update (overwrite) installation of the previous product (Web SmartNetMonitor).	Device information is kept, but not account settings. Add accounts as required.

7

INDEX

Part of illustrations or explanations in this guide may differ from your product due to improvement or change in the product.

⚙️Important

❒ It is possible that any document or data stored in the personal computer will be damaged or lost by user error during operation or software error. Be sure to back up all important data beforehand.

❒ Do not remove or insert any disk while operating this software.

❒ The supplier disclaims all responsibility for the documents or data created using this product.

❒ THE SUPPLIER SHALL NOT BE LIABLE TO YOU FOR DAMAGES OR LOSS OF ANY DOCUMENT OR DATA PRODUCED BY USING THIS SOFTWARE.

❒ THE SUPPLIER SHALL NOT BE LIABLE TO YOU FOR ANY CONSEQUENTIAL, INCIDENTAL OR INDIRECT DAMAGES (INCLUDING, BUT NOT LIMITED TO, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF BUSINESS INFORMATION, AND THE LIKE) CAUSED BY FAILURE OF THIS SOFTWARE OR LOSS OF DOCUMENTS OR DATA, NOR FOR ANY OTHER DAMAGES ARISING OUT OF THE USE OF THIS SOFTWARE, EVEN IF THE SUPPLIER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Web SmartDeviceMonitor Administrator's Guide