Web SmartDeviceMonitor Standard

Setup Guide

Read this manual carefully before you use this product and keep it handy for future reference.

Introduction

This manual contains detailed instructions and notes on the operation and use of this product. For your safety and benefit, read this manual carefully before using the product. Keep this manual in a handy place for quick reference.

Preface

Thank you for purchasing Web SmartDeviceMonitor Standard.

This guide explains the system (specification) requirements of the Web SmartDeviceMonitor Standard and how to install the software for administrators of Web SmartDeviceMonitor Standard. To get optimum results from Web SmartDeviceMonitor Standard, be sure to read this guide first. Keep this guide handy for easy reference.

Trademarks

Microsoft®, Windows®, Windows NT®, Windows Server®, Windows Vista®, and SQL Server™ are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Pentium is a registered trademark of Intel Corporation.

Other product names used herein are for identification purposes only and might be trademarks of their respective companies. We disclaim any and all rights to those marks.

The proper names of the Windows operating systems are as follows:

- 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 Vista are as follows:
  Microsoft® Windows Vista® Ultimate
  Microsoft® Windows Vista® Enterprise
  Microsoft® Windows Vista® Business
  Microsoft® Windows Vista® Home Premium
  Microsoft® Windows Vista® Home Basic
- The product names of Windows Server 2003 are as follows:
  Microsoft® Windows Server® 2003 Standard Edition
  Microsoft® Windows Server® 2003 Enterprise Edition
- The product names of Windows Server 2003 R2 are as follows:
  Microsoft® Windows Server® 2003 R2 Standard Edition
  Microsoft® Windows Server® 2003 R2 Enterprise Edition
- The product names of Windows NT 4.0 are as follows:
  Microsoft® Windows NT® Workstation 4.0
  Microsoft® Windows NT® Server 4.0

How to Read This Manual

Symbols

The following set of symbols is used in this manual.

Important
Indicates a situation that may result in property damage or malfunction if instructions are not followed. Be sure to read the instructions.

Preparation
Indicates information or preparations required prior to operating.

Limitation
Indicates a function's limitations.

Note
Indicates supplementary relevant information.

Reference
Look here for further information.

[ ]
Indicates on-screen keys and items.

【 】
Indicates keys on the computer's keyboard.

Terminology

The following is an explanation of the terminology used in this manual:

❖ **Device**
A "device" is a printer or multifunction machine connected to a network. Though the term generally includes routers, hubs, and other network devices, "device" in this manual is limited to printers and multifunction machines.

❖ **Discovery**
This refers to the process of discovering network connected devices by Web SmartDeviceMonitor Standard.

❖ **Device Log**
The term "device log" refers to both job logs and access logs retrieved from a device.

Screens

The explanations in this manual use screen images from Windows Server 2003 Standard Edition Service Pack1, Windows XP Professional Service Pack 2, and Internet Explorer 6.0 Service Pack 2. If you use another version of Windows, screen images may differ; however, you can perform the same steps.

TABLE OF CONTENTS

4. Usage Examples and Settings

5. Appendix

1. Pre-Installation Checks

Web SmartDeviceMonitor Standard Components

Web SmartDeviceMonitor Standard includes the following components:

- The DeviceMonitor function module
  To perform DeviceMonitor functions.
- The LogMonitor function module
  The module to implement the LogMonitor functions.
- Web Services (Apache)
  To support the services of Web SmartDeviceMonitor Standard.

  Note

  ❒ It may be possible to select IIS depending on the OS in use. See Windows Help for the IIS installation method.
- MSDE2000 Service Pack 4
  A database for log management.

  Note

  ❒ You can use SQL Server 2005 as a database server. For details about installing SQL Server 2005, see p.10 “Settings When Using SQL Server 2005” and Windows Help.
- ManagementTool
  A tool for managing Web SmartDeviceMonitor Standard.
- SSL Setting Tool
  A tool for issuing and importing a CA server certificates for encrypting communication channels using the SSL protocol.

  Reference

  For details about the SSL Setting Tool, see "Encrypting Communication Channels", *Web SmartDeviceMonitor Professional IS/Standard Operation Guide*.
- Authentication Manager
  A tool for unifying user authentication settings.

Server tools and modules are all installed at the same time by the installer when the product is installed in a server that runs Web SmartDeviceMonitor Standard.

Authentication Manager is a Windows application. This is installed in the administrator's computer rather than the server.

Product Specification Check

Check that the server and administrator's computers satisfy the specification detailed below.

1

Server Specification

To operate Web SmartDeviceMonitor Standard, the server computer must meet the following requirements:

Item	Description
Computer	CPU: Pentium compatible 1 GHz or higher (Pentium 4 compatible 2.8 GHz or higher recommended) Memory: 1 GB or more Minimum available hard disk space before installation: 800 MB. It is necessary, however, to retain capacity separately for storing log data. **Important** ❒ Computer names can contain the following characters only: upper and lower case letters (A-Z, a-z), numbers (0-9), and hyphens (-).
Operating System	Windows 2000 Professional / Server / Advanced Server (i386) : Service Pack 4 or later Windows XP Professional: Service Pack 2 or later Windows Server 2003 Standard Edition / Enterprise Edition: Service Pack 1 or later Windows Server 2003 R2 Standard Edition / Enterprise Edition: Service Pack 1 or later **Note** ❒ It is not compatible with Windows XP Professional x64 Edition or Windows Server 2003 x64 Edition.
Language of the operating system	Dutch, English, French, German, Italian, Spanish *1
Data Base	MSDE 2000 Service Pack 4 SQL Server 2005 Express Edition Service Pack 1 or later **Note** ❒ MSDE 2000 Service Pack 4 is included in the Web SmartDeviceMonitor Standard installer.
Browser	The following browsers with JavaScript enabled: • Internet Explorer 6.0 Service Pack 1 or later • Internet Explorer 7.0 **Reference** For details about activating JavaScript, see p.4 “Activating browser JavaScript”.

Item	Description
Network	TCP/IP must be installed and configured correctly. **Important** ❒ Implement management using fixed IP addresses.

*1 You can install in the language selected on the corresponding operating system. When you install this application in an operating system other than the corresponding operating systems, English is set.

Client System Requirements

Item	System requirements
Computer	CPU: Pentium compatible 500 MHz or higher recommended Memory: 128 MB or higher recommended Capacity of Hard Disk: In accordance with the operating system recommendation
Operating System	Windows 2000 Professional / Server / Advanced Server (i386): Service Pack 4 or later Windows XP Home Edition / Professional: Service Pack 2 or later Windows Vista x86/x64 Ultimate / Enterprise / Business / Home Premium / Home Basic Windows Server 2003 Standard Edition / Enterprise Edition: Service Pack 1 or later Windows Server 2003 R2 Standard Edition / Enterprise Edition: Service Pack 1 or later
Operating System Language	English, German, French, Italian, Spanish, Dutch *1
Browser	The following browsers with JavaScript enabled: • Internet Explorer 6.0 Service Pack 1 or later • Internet Explorer 7.0 **Reference** For details about activating JavaScript, see p.4 “Activating browser JavaScript”.
Network	TCP/IP needs to be installed and properly configured.
Screen Resolution	1024x768 or higher recommended

*1 You can install in the language selected on the corresponding operating system. When you install this application software in an operating system other than the corresponding operating systems, English is set.

Activating browser JavaScript

1 **Select [Internet Options...] on the Internet Explorer [Tools] menu.**
The **[Internet Options]** dialog box appears.

2 **Click the [Security] tab.**

3 **Click [Custom Level...].**
The **[Security Settings]** dialog box appears.

4 **Select [Enable] in [Active scripting] displayed under [Scripting].**

5 **Click [OK].**
The **[Security Settings]** dialog box closes.

6 **Click [OK].**
The **[Internet Options]** dialog box closes.

Authentication Manager Requirements

Authentication Manager is a Windows application. Install it in the administrator's computer.

Item	Description
Computer	Available hard disk space: 20 MB or higher
Operating System	Windows 2000 Professional / Server / Advanced Server (i386) : Service Pack 4 or later Windows XP Home Edition / Professional: Service Pack 2 or later Windows Vista x86 Ultimate / Enterprise / Business / Home Premium/Home Basic Windows Server 2003 Standard Edition / Enterprise Edition: Service Pack 1 or later Windows Server 2003 R2 Standard Edition / Enterprise Edition: Service Pack 1 or later **Note** ❒ You cannot use this application under Windows Vista x64 Edition.
Language of the operating system	Dutch, English, French, German, Italian, Spanish [*1]
Network	TCP/IP must be installed and configured correctly.

[*1] You can install in the language selected on the corresponding operating system. When you install this application software in an operating system other than the corresponding operating systems, English is set.

Device Requirements

The product requirements of the printers and machines that you can monitor using Web SmartDeviceMonitor Standard are as follows:

Item	Description
Network Protocol	TCP/IP
Supported MIB	Printer MIB v2 (RFC 3805) / Printer MIB (RFC 1759), MIB-II (RFC 1213), and Host Resource MIB (RFC 2790)

Protocols

Item	TCP/IP *1
Device Information Acquisition	SNMP, SNMPv3, or HTTP
Device Setting	SNMP, SNMPv3, or HTTP
Display on Browser	HTTP (by default, port number 8080 or 80 is used.) HTTPS (by default, port number 8443 or 443 is used.)

*1 It is not compatible with IPv6 and is only compatible with IPv4.

Deciding the Installation Type

You can install Web SmartDeviceMonitor Standard using one of the following two procedures:

❖ **New installation**

Select this installation type if you are installing Web SmartDeviceMonitor Standard on a server that does not have an earlier version of this product installed on it. This installation type is the best choice if you do not want to inherit data from an earlier version of this product. If the server does have an earlier version installed but you do not want to retain its data, be sure to uninstall the earlier version, and then install the present version.

Note

❒ If an earlier version of a product that uses the authentication management service (such as Web SmartDeviceMonitor/ScanRouter System) has been installed on the server, the authentication information of the earlier version can be retained through the uninstallation, and inherited by the new installation.

Reference

See p.11 “New Installation” for installing this product as new.

See p.69 “Uninstallation” for uninstalling the earlier version.

❖ **Overwriting installation**

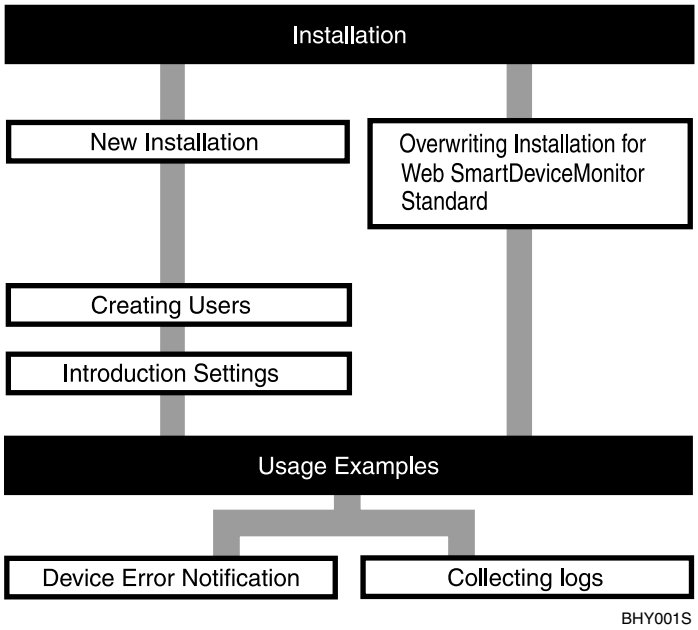
Select this installation type if you are installing Web SmartDeviceMonitor Standard on a server that already has Web SmartDeviceMonitor Standard installed on it. This installation type is the best choice if the server already has Web SmartDeviceMonitor Standard installed and you want to retain its data.

Limitation

❒ Only the device management component of Web SmartDeviceMonitor Professional IS cannot be installed by overwriting.

Setup Flow

The following diagram represents the flow of Web SmartDeviceMonitor Standard setup.



❖ Installation references

Reference

- p.11 “New Installation” for information regarding "New installation".
- p.22 “Overwriting Installation of Web SmartDeviceMonitor Standard” for information regarding "Overwriting Installation for Web SmartDeviceMonitor Standard".
- p.25 “Creating Users” for information regarding "Creating Users".
- p.38 “Quick Setup” for information regarding "Quick setup".

❖ Usage example references

Reference

- p.53 “Device Error Notification” for information regarding "Device error notification".
- p.60 “Collecting Logs” for information regarding "Collecting logs".

Required Settings when Using a Firewall

If you are installing Web SmartDeviceMonitor Standard in a firewall-protected Windows environment, you must open the required ports.

Log on to Windows as an Administrators group member, and then free the following ports:

- Port used as HTTP port
  Web SmartDeviceMonitor Standard uses the following default port numbers for unencrypted communication:
  - When running on an Apache Web server: 8080
  - When running on an Internet Information Service (IIS) Web server: 80
- Port used as HTTPS port
  Open this port if communication paths are encrypted. Web SmartDeviceMonitor Standard uses the following default port numbers for encrypted communication:
  - When running on an Apache Web server: 8443
  - When running on an Internet Information Service (IIS) Web server: 443

Reference

For details about communication channel encryption, see "Encrypting Communication Channels", *Web SmartDeviceMonitor Standard Operation Guide*.

Settings When Using Windows Server 2003

If the computer used to log on to Web SmartDeviceMonitor Standard is Windows Server 2003, execute the security settings in Internet Options in the sequence given below.

1 Activate Internet Explorer.

2 Select [Internet Options...] on the [Tools] menu.

The **[Internet Options]** dialog box appears.

3 Click the [Security] tab.

4 Select [Local intranet] and click [Sites...].

The **[Local intranet]** dialog box appears.

5 Enter the URL below in [Add this Web site to the zone].

http://*Web SmartDeviceMonitor Standard host name or IP address*

6 Click [Add].

7 **Click [Close].**

The **[Local intranet]** dialog box closes.

8 **Click [OK].**

The **[Internet Options]** dialog box closes.

This completes the settings.

Settings When Using SQL Server 2005

You can use SQL Server 2005 as a database server for Web SmartDeviceMonitor Standard.

To use SQL Server 2005 as your database server, configure the following settings.

Limitation

❒ Only the Express Edition of SQL Server 2005 can be used as a database server for Web SmartDeviceMonitor Standard.

Settings When Installing SQL Server 2005

Perform the following steps when installing SQL Server 2005:

1. **On the [Instance Name] screen, select [Named instance], and then enter "RDHWEBSERVICE".**
2. **On the [Service Account] screen, select [Use the built-in System account], and then click [Local system] in the list.**
3. **On the [Authentication Mode] screen, select [Mixed Mode (Windows Authentication and SQL Server Authentication)], and then enter the database administrator's password (SA password).**

Limitation

❒ Spaces, \(back slash), and "(double quotes) cannot be used in the SA password.

Setting a TCP/IP Connection to SQL Server 2005

Enable a TCP/IP connection to SQL Server 2005.

1. **On the [Start] menu, point to [All Programs], point to [Microsoft SQL Server 2005], point to [Configuration Tools], and then click [SQL Server Configuration Manager].**
2. **In [SQL Server 2005 Network Configuration], select [Protocols for RDHWEBSERVICE].**
3. **Enable [TCP/IP].**

Overwriting an MSDE Installation

If you are running Web SmartDeviceMonitor Standard with MSDE, perform the following steps to overwrite MSDE with SQL Server 2005:

When overwriting, select **[Named instance]** on the **[Instance Name]** screen, and then enter "RDHWEBSERVICE".

1. **Overwrite MSDE with SQL Server 2005.**
2. **Restart the computer.**

New Installation

Installation Procedure

Preparation

During installation, you are asked to log on to Windows again. Log on as the same user who installed Web SmartDeviceMonitor Standard.

If IIS is selected as Web server type in step 9, install IIS and launch web service before starting the installation of Web SmartDeviceMonitor Standard. See Windows Help for the IIS installation method.

Step 11 requires the administrator password (SA password) to install MSDE. Obtain the SA password for the database beforehand.

To use SQL Server 2005 as your database server, you must first install SQL Server 2005, and then configure the necessary settings *before* installing Web SmartDeviceMonitor Standard.

If IIS is specified for the Web server, this product will run using an anonymous user account for IIS (IUSR_<Computer name>). For this reason, do not disable the IUSR account.

Access the following URL for details about changing the IUSR account password:

http://support.microsoft.com/default.aspx?scid=kb%3Ben%3B297989

Reference

For details about the settings you must configure to use SQL Server 2005, see p.10 “Settings When Using SQL Server 2005”.

The following user information is necessary for installation:

❖ **Administrators group user information**

This refers to information about users who have administrator privileges on the computer.

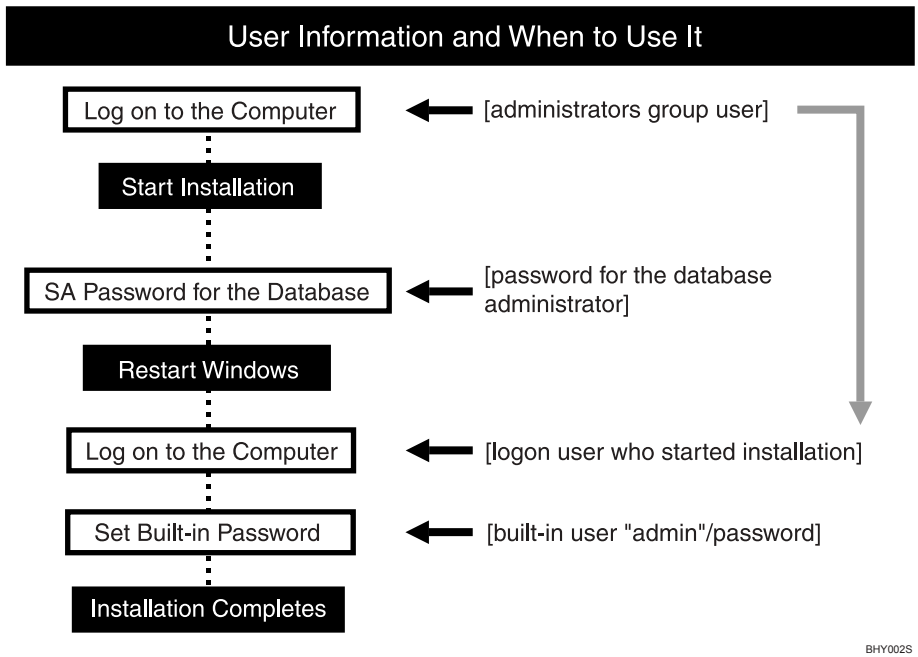
❖ **SA password for the database**

This refers to the administrator password, which is required when installing the database.

❖ **Built-in password**

This refers to information about users who have total authority to manage Web SmartDeviceMonitor Standard. The user name is "Admin".

Enter the required user information in the order shown below.



Important

❒ Before beginning the installation, log on to Windows as an Administrators group member and close all applications that are currently running.

Note

❒ The server must be connected to the network.

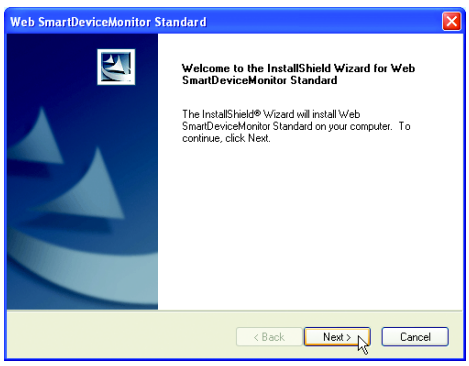
1 **Double-click Setup.exe.**

A warning about the installation appears.

2 **Read the warning, and then click [OK].**

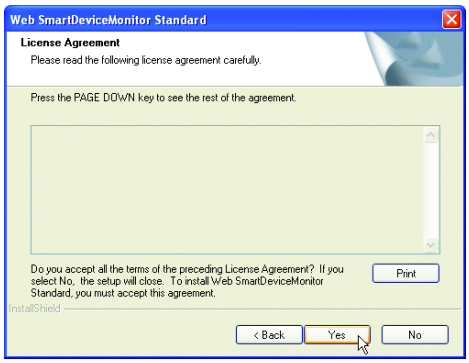
The **[Welcome to the InstallShield Wizard for Web SmartDeviceMonitor Standard]** dialog box appears.

3 **Click [Next>].**



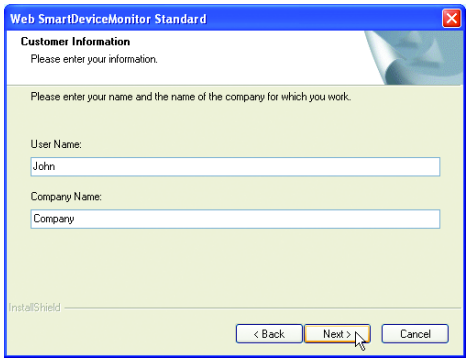
The **[License Agreement]** dialog box is displayed.

4 **Read all of the terms of the license agreement, and if you agree, click [Yes].**



The **[Customer Information]** dialog box appears.

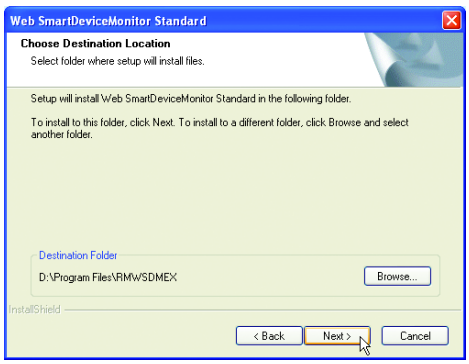
5 **Enter your [User Name] and [Company Name], and then click [Next>].**



For **[User Name]** and **[Company Name]**, enter the user name and company name registered in the product.

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

6 **Check the folder for the installation is the correct folder, and then click [Next>]. To change the folder, click [Browse...]. Select a different folder, and then click [Next>].**

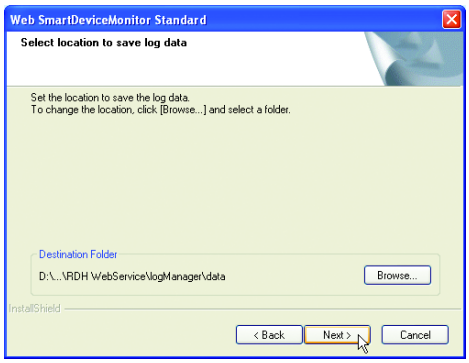


Limitation

❒ Double-byte characters cannot be used in the destination folder name.

The **[Select location to save log data]** dialog box appears.

7 **Check the folder where log data is to be saved is the correct folder, and then click [Next>]. To change the folder, click [Browse...]. Select a different folder, and then click [Next>].**



Note

❒ Log data refers to JobLog and AccessLog collected by the Log Management function from the device.

Reference

For details about Log Management, see *Web SmartDeviceMonitor Professional IS/Standard Operation Guide*, and Log Management help.

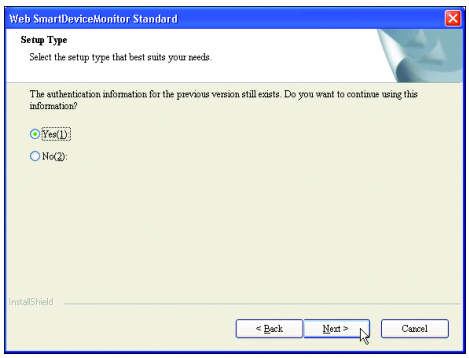
❖ **If the authentication information of a product that uses the authentication management service was retained after uninstallation**

A dialog box prompting you to select whether to inherit the authentication information appears. Proceed to **8**.

❖ **If the authentication information of a product that uses the authentication management service was not retained after uninstallation**

A dialog box prompting you to select a Web server appears. Proceed to **9**.

8 **Select whether to inherit the authentication information, and then click [Next>].**

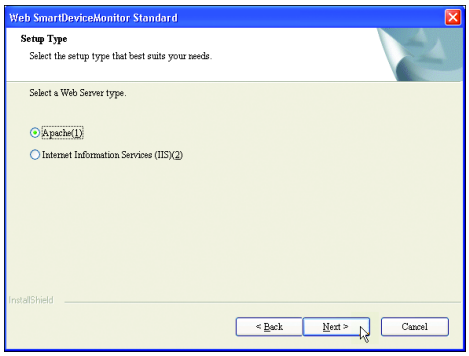


Note

❒ Select **[Yes]** to inherit the authentication information to Web SmartDeviceMonitor Standard.

A dialog box prompting you to select a Web server appears.

9 **Select either [Apache] or [Internet Information Services (IIS)] as the Web server type in use and click [Next>].**



Note

❒ You can only choose Apache in the following cases:

- IIS is not installed.
- Your operating system is Windows 2000 Professional or Windows XP Professional.

❒ If Apache is selected as the Web server type, regular maintenance of the server's access logs is required.

❒ To use IIS, install IIS first, and then launch the Web service.

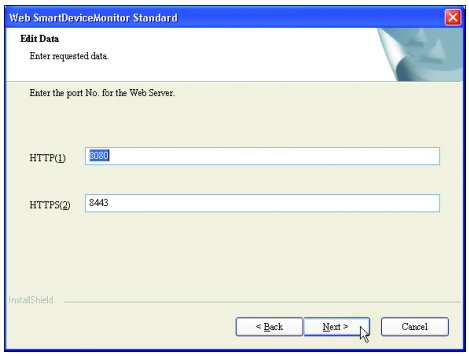
Reference

For details about Managing Web Server Log Files, see "Managing Web Server Log Files", *Web SmartDeviceMonitor Professional IS/Standard Operation Guide*.

It may be possible to select IIS depending on the OS in use. See Windows Help for the IIS installation method.

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

10 **Enter each Port number for [HTTP] and [HTTPS] that the Web server will use, and then click [Next>].**



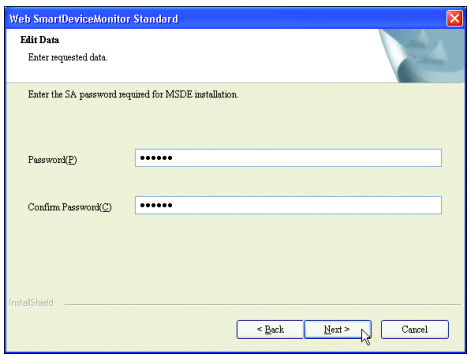
Important

❒ Port numbers cannot be changed after the installation. To change the port numbers, you must first uninstall and then reinstall Web SmartDevice-Monitor Standard.

❒ When moving Web SmartDeviceMonitor Standard to another server, the Authentication Manager backup must be restored on the new server. To do this, you must specify the same port number as was used to save the backup data on the original server. The Authentication Manager backup can be restored only if the same port number is specified.

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

11 Obtain the database administrator password (SA password). Enter the SA password in the [Password] and [Confirm Password] boxes, and then click [Next>].



Limitation

❒ Spaces, \(back slash), and "(double quotes) cannot be used in the SA password.

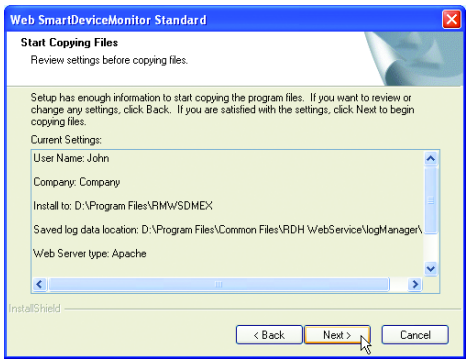
Note

❒ 1-128 characters can be entered.

❒ If you are using SQL Server 2005 for the database, a dialog box prompting you to enter the SA password appears. Enter the password set when SQL Server 2005 was installed, and then click **[Next>]**.

The **[Start Copying Files]** dialog box appears.

12 Check your Setup, and then click [Next>].



Installation of Web SmartDeviceMonitor Standard is started.

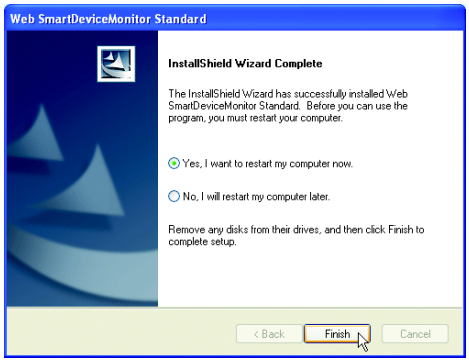
Important

❒ If you are running one of the following systems, the **[Windows Security Alert]** dialog box may appear:

- Windows Server 2003 R2 Standard Edition / Enterprise Edition: Service Pack 1 or later
- Windows Server 2003 Standard Edition / Enterprise Edition: Service Pack 1 or later
- Windows XP Professional Service Pack 2 or later
  Click **[Unblock]** and continue installation.

When installation is complete, the **[InstallShield Wizard Complete]** dialog box appears.

13 Make sure you select [Yes, I want to restart my computer now.], and then click [Finish].



Windows restarts and logon window appears.

14 Log on to Windows with the logon user that executed Web SmartDeviceMonitor Standard installation.

Important

❒ Installation will not continue if the logon user is different.

The **[Authorization for Server Access]** dialog box appears.

15 Enter the Windows logon password in the [Password:] and [Confirm password:] text boxes and click [OK].

The **[Authentication Method Settings]** dialog box is displayed.

In subsequent operations, authentication method is confirmed and the built-in password is set. Settings differ according to the conditions of the server computer in which Web SmartDeviceMonitor Standard is installed. See p.19 “Setting Authentication Method”.

Setting Authentication Method

The displayed screen differs according to the conditions of the server computer in which Web SmartDeviceMonitor Standard is installed.

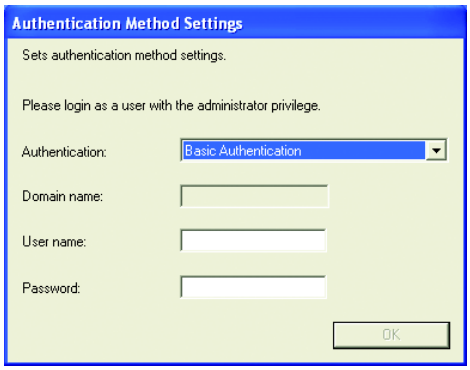
If Authentication Manager is already installed, See p.19 “Confirmation of authentication method”.

In case of either of the following, set device authentication while referring to p.20 “Setting product authentication”.

- If Authentication Manager is not installed.
- If Authentication Manager is installed but no built-in user password has been set for Authentication Manager and Authentication Manager administrator authority has been assigned to built-in users.

Confirmation of authentication method

[Basic Authentication] is selected as the authentication method.



Note

❒ **[Basic Authentication]** is the only authentication method that is compatible with Web SmartDeviceMonitor Standard.

Enter **[User name:]** and **[Password:]** as Authentication Manager administrator information and click **[OK]**.

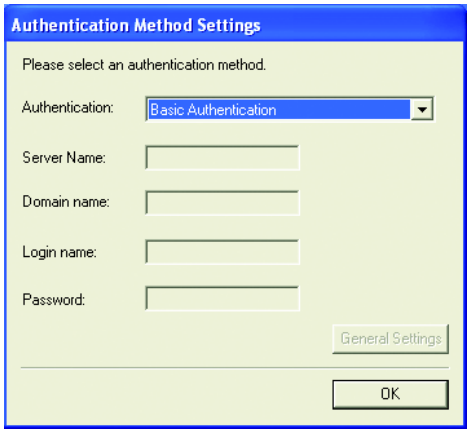
After clicking **[OK]**, a dialog box is displayed confirming Web SmartDeviceMonitor Standard product authentication.

Reference

See p.20 “Setting product authentication” to continue setting product authentication.

Setting product authentication

The **[Authentication Method Settings]** dialog box is displayed.



Confirm that **[Basic Authentication]** is selected as the authentication method and click **[OK]**.

Note

❒ **[Basic Authentication]** is the only authentication method that is compatible with Web SmartDeviceMonitor Standard.

The dialog box for setting built-in passwords is displayed in either of the following cases:

- If Authentication Manager is not installed.
- If Authentication Manager is installed but no built-in user password has been set.

After completing the setting of product authentication, set the built-in password while referring to p.21 “Setting Built-in Password”. If Authentication Manager is already installed and the built-in password has been set, Web SmartDeviceMonitor Standard installation is completed.

Setting Built-in Password

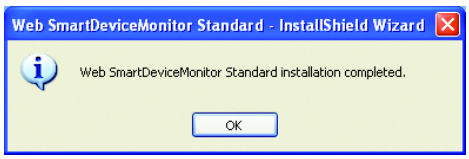
In the **[Set Built-in User Password]** dialog box, enter the password of the administrator with special authority to develop Web SmartDeviceMonitor Standard. The administrator's user name is "Admin". The administrator has authority for all management operations including Authentication Manager.

Important

❒ You will no longer be able to log on with Admin if you forget the built-in password. If that happens, you must reinstall Web SmartDeviceMonitor Standard since it is not possible to recover the password. Take care to avoid forgetting the built-in password.

This completes the installation of Web SmartDeviceMonitor Standard.

If the installation completes normally, a dialog box indicating that Web SmartDeviceMonitor Standard was successfully installed appears.



See p.25 "Creating Users and Quick Setup", and then continue creating users and executing installation settings.

Overwriting Installation

If Web SmartDeviceMonitor Standard is already installed on the server, Update Installation (Overwriting Installation) is performed.

This form of installation overwrites previously installed Web SmartDeviceMonitor Standard and related information. If you do not want to overwrite, first uninstall the product, and then perform the new installation.

Limitation

❒ Only the device management component of Web SmartDeviceMonitor Professional IS cannot be installed by overwriting.

Overwriting Installation of Web SmartDeviceMonitor Standard

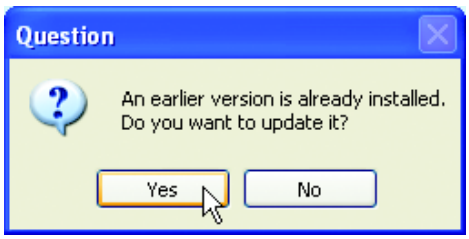
Important

❒ Before beginning the installation, log on to Windows as an Administrators group member and close all applications that are currently running.

1 **Double-click Setup.exe.**

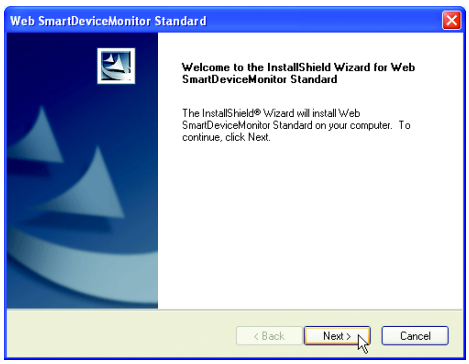
The **[Question]** dialog box appears.

2 **Check the content of the dialog box, and then click [Yes].**



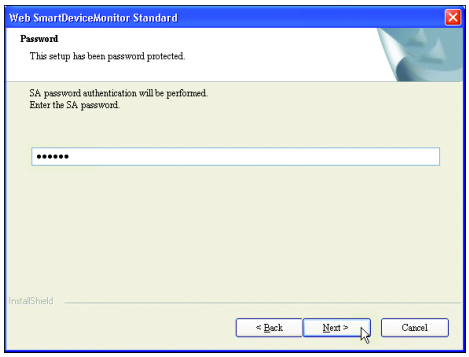
The **[Welcome to the InstallShield Wizard for Web SmartDeviceMonitor Standard]** dialog box appears.

3 **Click [Next>].**



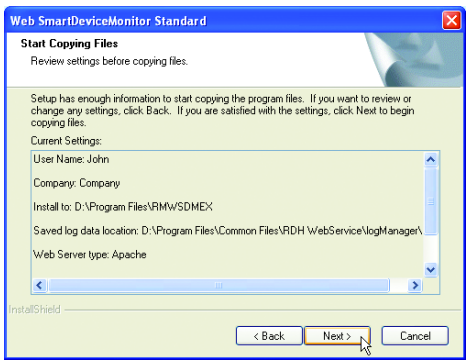
The **[Password]** dialog box appears.

4 **Enter the SA password, and then click [Next>].**



The **[Start Copying Files]** dialog box appears.

5 **Check your setup, and then click [Next>].**



Installation of Web SmartDeviceMonitor Standard starts.

Important

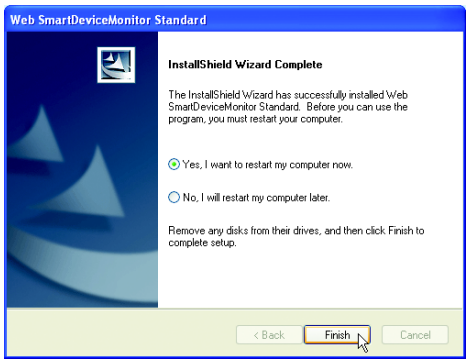
❒ If you are running one of the following systems, the **[Windows Security Alert]** dialog box may appear:

- Windows XP Professional Service Pack 2 or later
- Windows Server 2003 Standard Edition / Enterprise Edition: Service Pack 1 or later
- Windows Server 2003 R2 Standard Edition / Enterprise Edition: Service Pack 1 or later

  Click **[Unblock]** and continue installation.

When installation is complete, the **[InstallShield Wizard Complete]** dialog box appears.

6 **Make sure you select [Yes, I want to restart my computer now.], and then click [Finish].**



Windows restarts.

7 **Log on to Windows with the logon user that executed Web SmartDeviceMonitor Standard installation.**

Important

❒ Installation will not continue if the logon user is different.

The **[Authorization for Server Access]** dialog box appears.

8 **Enter the Windows logon password in the [Password:] and [Confirm password:] text boxes and click [OK].**

The **[Authentication Method Settings]** dialog box appears.

Set the authentication method and built-in password in the subsequent steps. Settings differ according to the conditions of the server PC in which Web SmartDeviceMonitor Standard is installed. See p.19 “Setting Authentication Method”.

3. Creating Users and Quick Setup

Creating Users

When Web SmartDeviceMonitor Standard is first installed, there is only one built-in user. After logging in as Admin, the following users with access authority are created:

Reference

For details about each access privilege, see "Security" and "Accounts", *Web SmartDeviceMonitor Professional IS/Standard Operation Guide*.

- Web SmartDeviceMonitor administrator
- Device/Network administrator
- User

Web SmartDeviceMonitor administrators are created here for subsequent operations.

Note

❒ Authentication Manager can also be downloaded for use on the administrator computer.

Downloading Authentication Manager

Authentication Manager can be downloaded from the Web SmartDeviceMonitor server computer to the administrator computer.

Limitation

❒ Only the Web SmartDeviceMonitor administrator can download Authentication Manager.

1 **Start Internet Explorer.**

2 **Enter the following URL in the address bar, and then press the 【Enter】 key on the keyboard.**

http://*{host name.domain name}*:*{port number}*/wsdm/pc/basic.Login

or

http://*{IP address}*:*{port number}*/wsdm/pc/basic.Login

- Specify the host name or IP address of the computer on which Web SmartDeviceMonitor Standard is installed.

- Specify the name of the domain that contains the computer on which Web SmartDeviceMonitor Standard is installed.

  Note

  ❒ The domain name is required only if the computer on which Web SmartDeviceMonitor Standard is installed belongs to a domain.

- Specify the port number designated when Web SmartDeviceMonitor Standard was installed.

The login screen appears.

3 Enter the built-in user information.

- In **[User name:]**, enter "Admin".
- In **[Password:]**, enter the built-in user password .

4 Click [Login].

The Top Page appears.

5 Click [Setting Menu].

The **[Settings]** screen appears.

6 Click [User Account Settings].

The **[User Account Settings]** screen appears.

7 On the [Tools] menu, select [Download Authentication Manager].

The **[File Download]** dialog box appears.

8 Click [Save].

The **[Save As]** dialog box appears.

9 Specify a storage destination, and then click [Save].

The download starts.

When the download is complete, the **[Download complete]** dialog box appears.

10 Click [Close].

Downloading of Authentication Manager is now complete.

Installing Authentication Manager

Install Authentication Manager (downloaded from the Web SmartDeviceMonitor server) onto an administrator computer.

Important

❒ Before beginning the installation, log on to Windows as an Administrators group member and close all applications that are currently running.

1. **Double-click *AuthMngToolInstaller.exe*, which you downloaded.**

   The **[Web SmartDeviceMonitor – Authentication Manager]** dialog box appears.

2. **Click [Next>].**

   The **[License Agreement]** dialog box appears.

3. **Read the terms of the license agreement, and if you agree, click [Yes].**

   The **[Customer Information]** dialog box appears.

4. **Enter your [User Name] and [Company Name], and then click [Next>].**

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

5. **Check the folder for the installation is the correct folder, and then click [Next>]. To change the folder, click [Browse...]. Select a different folder, and then click [Next>].**

   Important

   ❒ Double-byte characters cannot be used in the destination folder name.

   The **[Start Copying Files]** dialog box appears.

6. **Check your Setup, and then click [Next>].**

   Installation of Authentication Manager is begins.

   When the installation is complete, the **[InstallShield Wizard Complete]** dialog box appears.

7. **Click [Finish].**

   Windows restarts.

Server Settings for Authentication Manager

When Web SmartDeviceMonitor Standard is introduced into Windows Server 2003/R2 SP1 or later, or Windows XP SP2 or later, for server use, make the following settings on the server, so that Authentication Manager can be operated from the administrator computer.

❖ **DCOM Settings**

Display the properties from **[Component Services]** - **[Computers]** - **[My Computer]**, and make the following settings:

- **[Local Access]** or **[Remote Access]** for ANONYMOUS LOGON is permitted.
- ANONYMOUS LOGON is added to the startup permissions.
- **[Local Launch]**, **[Remote Launch]**, **[Local Activation]**, and **[Remote Activation]** for ANONYMOUS LOGON are permitted.

Make the following settings to enable Windows Firewall:

- Adding a port range
  Specify a range of unused port numbers that can be secured contiguously (for example: 6000-6010).

Note

❒ Specify about ten ports. If connection does not succeed with the specified port range, increase the number of ports.

After specifying the port range, click **[OK]**, and then restart the server.

❖ **Setting Windows Firewall-excepted**

Make the following settings to enable Windows Firewall:

- Select **[General]**, and then set it to **[On]**.
- Select the **[Exceptions]** tab, and then select **[File and Printer Sharing]**.
- Add of the following ports:

Name	Port Number	TCP/UDP
RPC	135	TCP
RSI	50304	UDP
WebHTTP	8080 or 80 (Default)	TCP
WebHTTPS	8443 or 443 (Default)	TCP
DCOMPort01	6001 (example only)	TCP
DCOMPort10	6010 (example only)	TCP

Note

❒ If SSL communication is running, add HTTPS ports.

❒ For WebHTTP and WebHTTPS port numbers, enter the port numbers of HTTP and HTTPS that were specified when Web SmartDeviceMonitor Standard was installed.

❒ If Web SmartDeviceMonitor Standard is introduced into Windows Sever 2003 SP1 or later for server use, add all the DCOM ports that were added in the setup of DCOM.

After making all the necessary settings, click **[OK]**, and then restart the server.

Settings under Windows Vista

If your computer is running Windows Vista, perform the following steps before starting Authentication Manager.

1. **On the [Start] menu, click [Control Panel], click [Security], and then click [Windows Firewall].**

   The **[Windows Firewall]** dialog box appears.

2. **Click [Allow a program through Windows Firewall].**

   The **[User Account Control]** dialog box appears.

3. **If you logged on as an Administrators group member, click [Continue]. If you did not log on as an Administrators group member, enter the administrator password, and then click [OK].**

   The **[Windows Firewall Settings]** dialog box appears.

4. **Click the [Exceptions] tab, and then click [Add program ...].**

   The **[Add a Program]** dialog box appears.

5. **Select [Authentication Manager], and then click [OK].**

   The **[Windows Firewall Settings]** dialog box reappears. Check that **[Authentication Manager]** is added.

Using Authentication Manager to add Users

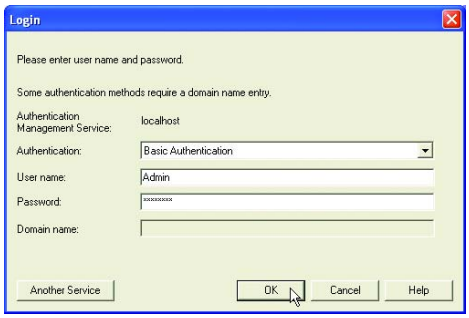
1 **Select [Start] - [All programs] - [Web SmartDeviceMonitor] - [Authentication Manager] on the computer in which Web SmartDeviceMonitor Standard is installed.**

Authentication Manager **[Login]** screen appears.

2 **Enter the setting items.**

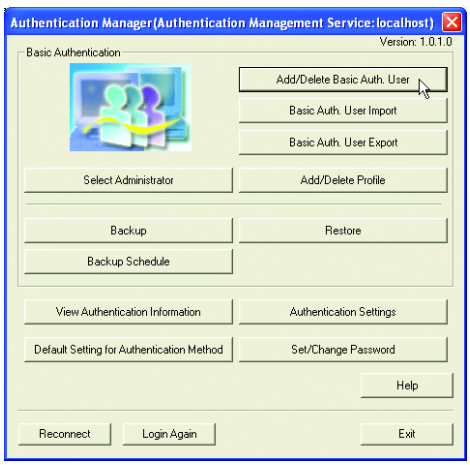
- User name
  Enter "Admin".
- Password
  Enter the built-in user password.

3 **Click [OK].**



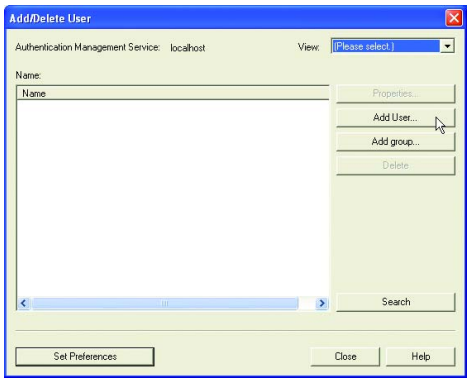
The **[Authentication Manager]** screen appears.

4 **Click [Add/Delete Basic Auth. User].**



The **[Add/Delete User]** screen appears.

5 Click [Add User...].



The **[User Property]** screen appears.

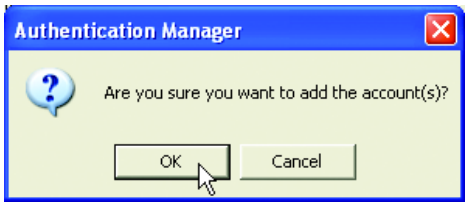
6 Enter each of the items.

- User name:
  Decide and enter the name of the user to be added.
- New password:
  Decide and enter the password of the user to be added.
- Confirm password:
  Enter the password entered as the new password for confirmation purposes.

7 Click [OK].

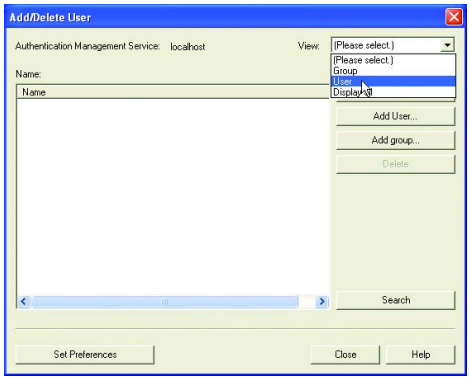
The **[Authentication Manager]** screen appears.

8 **Click [OK].**



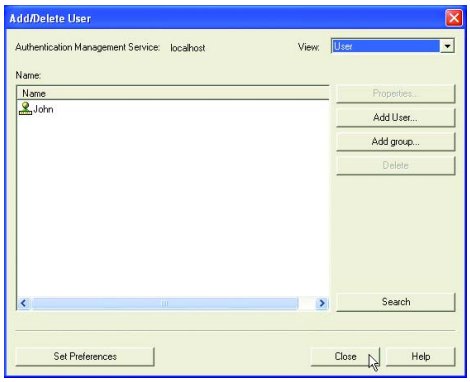
The **[Add/Delete User]** screen appears.

9 **In the [View:] list, click [User].**



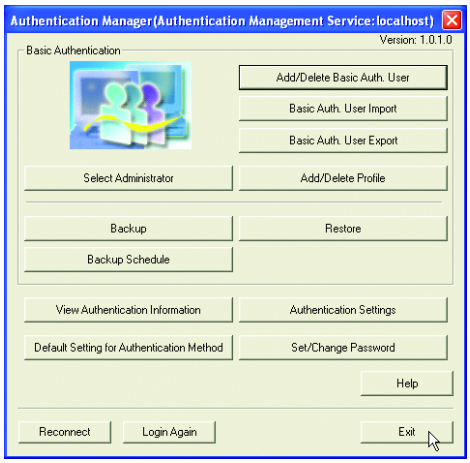
Registered users are displayed. The added user is also displayed.

10 **Click [Close].**



The **[Authentication Manager]** screen appears.

11 **Click [Exit].**



The **[Authentication Manager]** screen appears.

12 **Click [OK].**

Authentication Manager closes.

Continue to set up user accounts using Web SmartDeviceMonitor Standard.

Setting User Accounts

Preparation

If using Windows Server 2003, there are settings that must be made before logging on to Web SmartDeviceMonitor Standard. Execute the settings while referring to p.8 “Settings When Using Windows Server 2003”.

Web SmartDeviceMonitor Standard user accounts are set.

1 **Start Internet Explorer.**

2 **Enter the following URL in the address bar, and then press the [Enter] key on the keyboard.**

http:// *{host name.domain name}*:*{port number}*/wsdm/pc/basic.Login

or

http:// *{IP address}*:*{port number}*/wsdm/pc/basic.Login

- Specify the host name or IP address of the computer on which Web SmartDeviceMonitor Standard is installed.
- Specify the name of the domain that contains the computer on which Web SmartDeviceMonitor Standard is installed.

Note

❒ The domain name is required only if the computer on which Web SmartDeviceMonitor Standard is installed belongs to a domain.

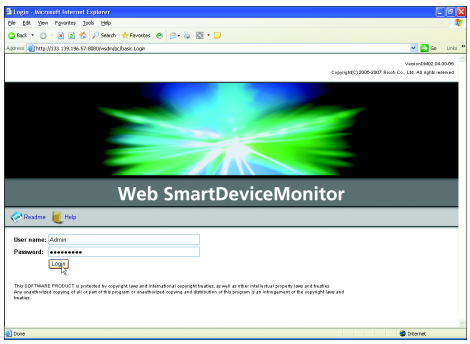
- Specify the port number designated when Web SmartDeviceMonitor Standard was installed.

The login dialog box appears.

3 **Enter the built-in user information.**

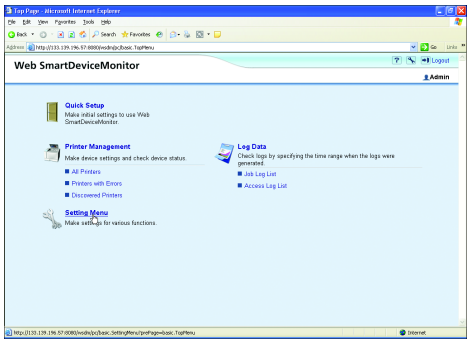
- In **[User name:]**, enter "Admin".
- In **[Password:]**, enter the built-in user password.

4 **Click [Login].**



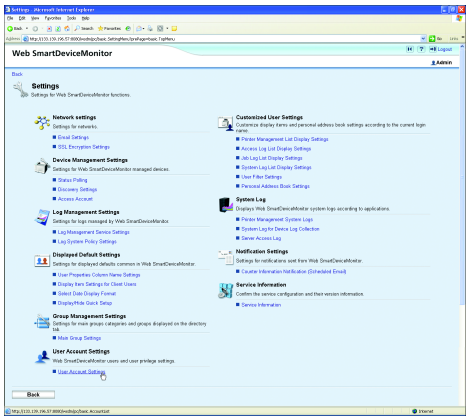
The Top Page is displayed.

5 Click **[Setting Menu]**.



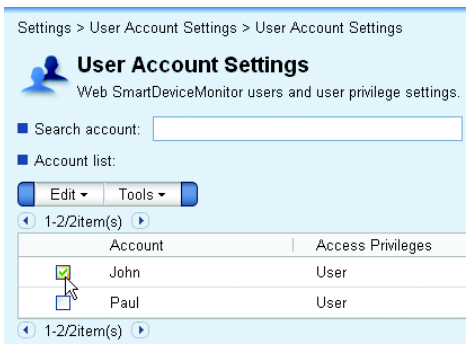
The **[Settings]** screen is displayed.

6 Click **[User Account Settings]**.

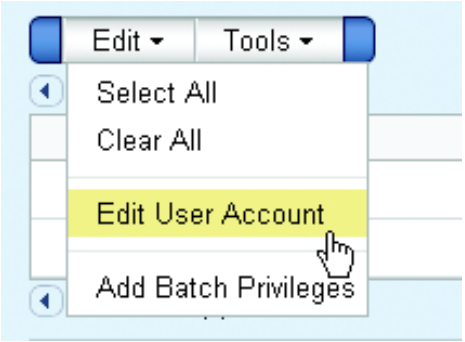


The **[User Account Settings]** screen appears.

7 **Users added using the procedure shown on p.30 “Using Authentication Manager to add Users” are displayed in the [Account list:]. Check the check boxes of the accounts.**



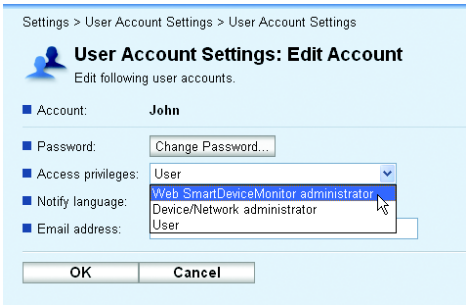
8 **Select [Edit User Account] on the [Edit] menu.**



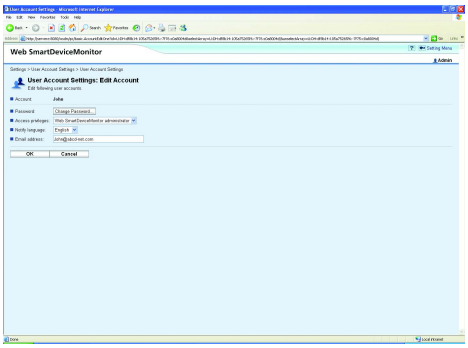
The **[User Account Settings: Edit Account]** screen appears.

9 **Confirm that the selected account is displayed in [Account:].**

10 **In the [Access privileges:] list, click [Web SmartDeviceMonitor administrator].**



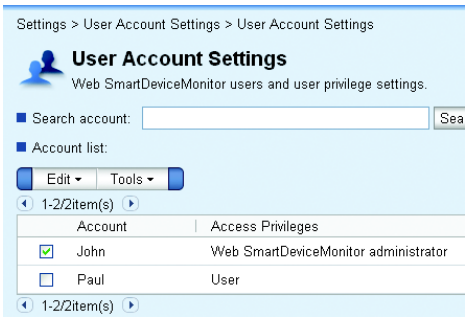
11 **Enter the e-mail address in [Email address:].**



12 Click [OK].

The screen returns to the **[User Account Settings]** screen.

The access authority of the selected account is displayed as **[Web SmartDevice-Monitor administrator]**.



13 Click [Back].

The **[Settings]** screen appears.

14 Click .

The top page is displayed.

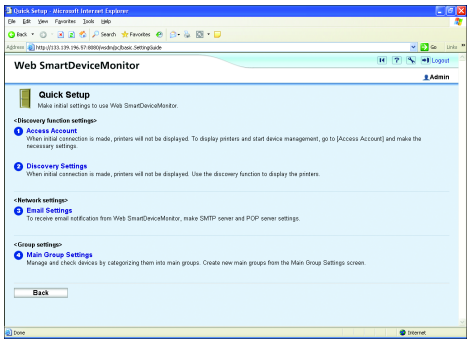
This completes user creation. Continue to execute installation settings.

Quick Setup

For new installations, installation settings are made after completing the installation of the Web SmartDeviceMonitor Standard and creating users. Web SmartDeviceMonitor Standard is accessed using the account of the created Web SmartDeviceMonitor Standard administrator and the installation settings are executed.

- Access Account
  Access accounts for devices are established in order to start device management.
- Discovery Settings
  Set the method for Discovery, and perform Discovery.
- Email Settings
  Set the SMTP server and the POP server in order that Web SmartDeviceMonitor Standard can send notice mails.
- Main Group Settings
  Create new main groups and groups for the management of groups.

The **[Quick Setup]** screen appears by clicking **[Quick Setup]** with the top page displayed.



Access Account

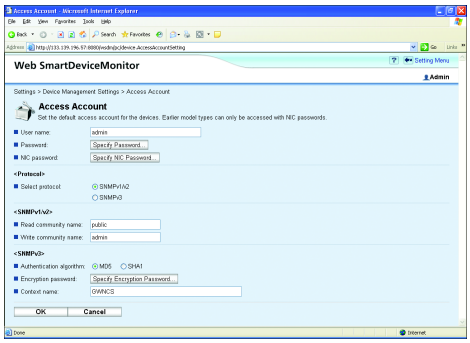
Access accounts for devices are established in order to start device management.

Important

❒ Only one access account can be set here. First integrate device administrator user names, passwords, and NIC passwords, and then set them in each device.

1 **Click [❶ Access Account] in the [<Discovery function settings>] area.**

The **[Access Account]** screen appears.



2 **Set each item.**

Important

❒ Be sure to set the access account. If you execute discovery without setting the access account, you will no longer be able to execute batch settings, etc.

Note

❒ In **[SNMPv3]**, entry is required when gaining access to an SNMPv3-compatible model.

Item	Explanation
User name	Enter the user name of a device administrator set in the device. **Note** ❒ This item is required as a security function for certain models. ❒ Default: admin

Item	Explanation
Password	Enter the password of a device administrator set in the device. Click **[Specify Password...]**. The **[Access Account: Specify Password]** window is displayed. Passwords are changed by entering the new password in **[Password]** and **[Confirm password:]**, and then click **[OK]**. **Note** ❒ This item is required as a security function for certain models.
NIC password:	Enter the NIC password set in the device. Click **[Specify NIC Password...]**. The **[Access Account: Specify NIC Password]** window is displayed. Passwords are changed by entering the new password in **[NIC password:]** and **[Confirm NIC password:]**, and then click **[OK]**.

❖ Protocol

Item	Explanation
Select protocol:	Select the protocol to use for Discovery. • SNMPv1/v2 • SNMPv3 **Note** ❒ Default: SNMPv1/v2

❖ SNMPv1/v2

Item	Explanation
Read community name:	Specify when gaining access to a device using SNMPv1 or SNMPv2. Enter a community name that can read only device information. **Note** ❒ Default: public
Write community name:	Specify when gaining access to a device using SNMPv1 or SNMPv2. Enter a community name that can read and write device information. **Note** ❒ Default: admin ❒ Batch settings and other device settings may malfunction if this is not properly set.

❖ **SNMPv3**

Item	Explanation
Authentication algorithm:	Select an authentication algorithm. ❖ **MD5** Select when specifying authentication algorithm for MD5 using a device. ❖ **SHA1** Select when specifying authentication algorithm for SHA1 using a device. **Note** ❒ Default: MD5
Encryption password:	Enter the encryption password set in the device. Click **[Specify Encryption Password...]**. The **[Access Account: Specify Encryption Password]** window is displayed. Encryption passwords are changed by entering the new encryption password in **[Encryption password:]** and **[Confirm encryption password:]**, and then click **[OK]**.
Context name:	Enter the context name set in the device. **Note** ❒ Default: GWNCS

3 **Click [OK].**

The **[Quick Setup]** screen appears.

Discovery Settings

Set the method for Discovery, and perform Discovery.

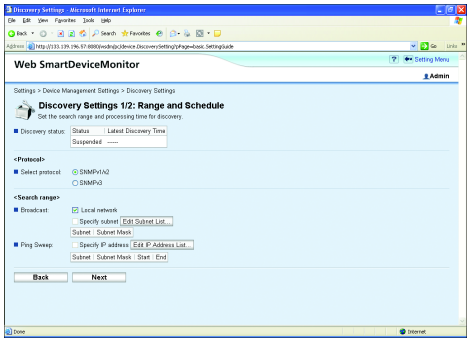
Note

❒ You cannot change Discovery function settings while Discovery is running.

❒ Click **[Cancel]** to cancel editing of the Discovery settings.

1 **Click [❷ Discovery Settings] on the [<Discovery function settings>] section.**

The **[Discovery Settings 1/2: Range and Schedule]** screen appears.



2 Set each items.

Item	Explanation
Discovery status:	The state while discovery is in progress is displayed.

❖ Protocol

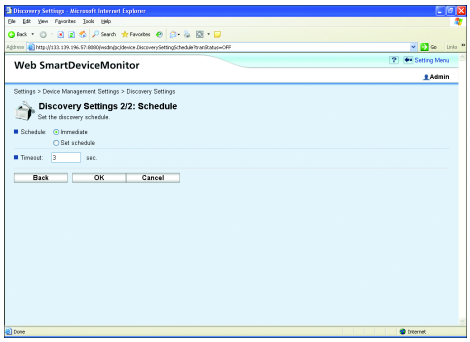
Item	Explanation
Select protocol:	Select the protocol to use for Discovery. • SNMPv1/v2 • SNMPv3 **Note** ❒ Default: SNMPv1/v2

❖ <Search range>

Item	Explanation
Broadcast:	Specify whether to set a local network and a specified subnet as the search range. The local network and a subnet can be set at the same time. ❖ **[Local network]** Select this check box to specify a local network as the search range. ❖ **[Specify subnet]** Select this check box to specify a subnet as the search range. Edit the range of the subnet specified for a search range on the **[Discovery Settings: Edit Subnet List]** window displayed when you click **[Edit Subnet List...]**. **Reference** For details, see "Discovery Settings" in the *Web SmartDeviceMonitor Professional IS/Standard Operation Guide*. **Note** ❒ Default: Local network
Ping Sweep:	Select **[Specify IP address]** when performing discovery by Ping Sweep. Edit the range of an IP address specified for a search range on the **[Discovery Settings: Edit IP Address List]** window displayed when you click **[Edit IP Address List...]**. **Reference** For details, see "Discovery Settings" in *Web SmartDeviceMonitor Professional IS/Standard Operation Guide*.

3 **Click [Next].**

The **[Discovery Settings 2/2: Schedule]** screen appears.



4 **Select [Immediate] on [Schedule:].**

Note

❒ You can configure discovery to be automatically performed on a periodic basis. For details, see "Discovery Settings" *Web SmartDeviceMonitor Professional IS/Standard Operation Guide*.

5 **Click [OK].**

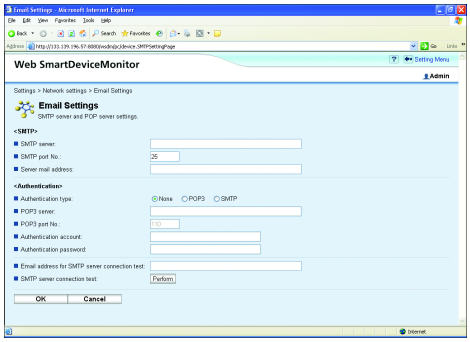
The **[Quick Setup]** screen appears.

Email Settings

Set the SMTP server and the POP server in order that Web SmartDeviceMonitor Standard can send notice mails.

1 **Click [❸ Email Settings] on the [<Network settings>] section.**

The **[Email Settings]** screen appears.



2 Set each item.

❖ SMTP

Item	Explanation
SMTP server:	Enter the SMTP server host name or IP address.
SMTP port No.:	Enter the port number used for SMTP.
Server mail address:	Enter mail address of an SMTP server.

❖ Authentication

Item	Explanation
Authentication type:	Either POP3 or SMTP is designated for authentication. ❖ **[None]** Not authenticate. ❖ **[POP3]** Authenticate by POP3 server. ❖ **[SMTP]** Authenticate by SMTP server. **Note** ❒ Default: **[None]**
POP3 server:	Enter the POP3 server host name or IP address.
POP3 port No.:	Enter the port number used in a POP3 protocol.
Authentication account:	Enter the authentication account.
Authentication password:	Enter the authentication password.
Email address for SMTP server connection test:	Enter the destination mail address, to which a test mail is sent, to confirm whether the system is connected to the SMTP server.
SMTP server connection test:	Click **[Perform]**. A test mail is then sent to the destination mail address specified in **[Email address for SMTP server connection test:]**.

3 Click [OK].

The **[Quick Setup]** screen appears.

Setting Main Groups and Groups

Create new main groups and groups for the management of groups.

Main groups and groups

You can register devices in groups and manage them. Devices can be easily managed by registering them in groups by office, location, use, etc.

❖ **Main Group**

In order to execute group management, it is necessary to create main groups in the group management route. You can create a maximum of 3 main groups. You can consolidate groups into preferred categories such as by department, by floor, etc. You can realize management reflecting various perspectives by creating multiple main groups and registering groups and devices to match the categorization.

Note

❒ You cannot register devices directly in main groups.

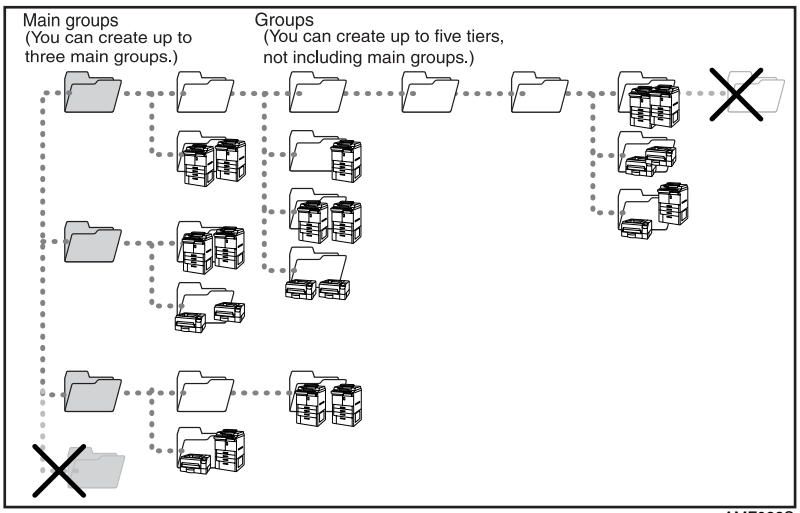
❖ **Group**

Groups are added to main groups. You can also create groups in other groups to create a nested structure. You can create up to five group tiers, not including the main groups, can be created.

You can manage devices by group by registering them in groups. For a group, you can specify a recipient to be notified when a device error occurs.

Note

❒ A device cannot be registered to multiple groups within the same main group, but it can be registered to a group in another main group.

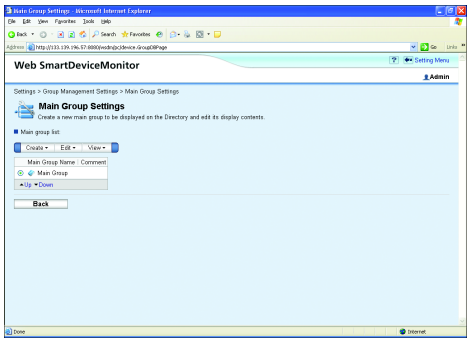


Creating main groups

Creating main groups

1 **Click [❹ Main Group Settings] on the [<Group settings>] section.**

The **[Main Group Settings]** screen appears.



2 **Select [New Main Group] on the [Create] menu.**

The **[Main Group Settings: Create New Main Group]** screen appears.

3 **Set each item.**

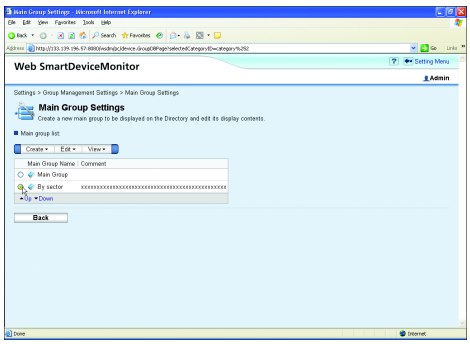
Item	Explanation
Main group name:	Enter the name of newly created main group.
Icon color:	Select an icon color for a newly created group database • **[Blue]** • **[Green]** • **[Yellow]** **Note** ❒ Default: **[Blue]**
Comment	In the text box, enter any relevant comments to append to newly created main group.

4 **Click [OK].**

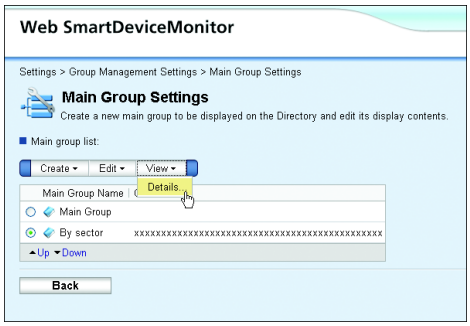
Creating groups

Creating groups.

1. **Select the main group for registering new groups on the [Main Group Settings] screen.**



2. **Select [Details...] on the [View] menu.**



The **[Group Settings]** screen appears.

3. **Select [New Group] on the [Create] menu on the [Group Settings] screen.**

The **[Group Settings: Create New Group 1/2]** screen appears.

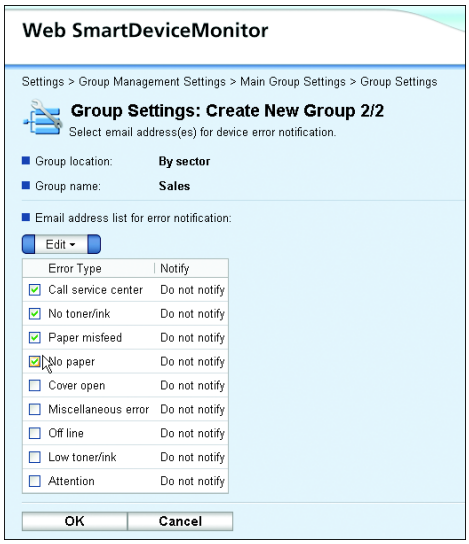
4 Set each of the items.

Item	Explanation
Group location:	The location where the new group is created appears.
Group name:	Enter the name of newly created group.
Comment:	In the text box, enter any relevant comments to append to newly created main group.

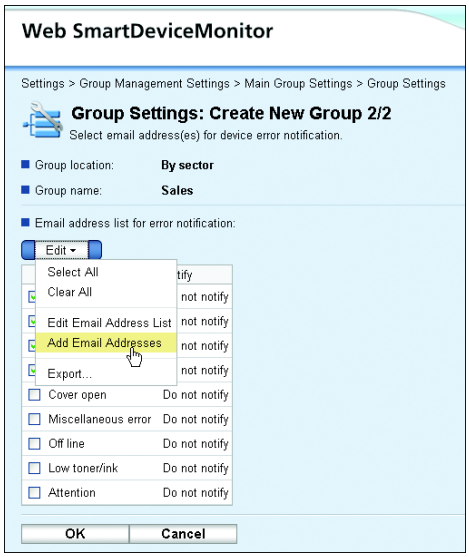
5 Click [Next].

The **[Group Settings: Create New Group 2/2]** screen appears.

6 Check the check boxes of errors that are to be notified upon occurrence on the [Email address list for error notification:].



7 **Select [Add Email Addresses] on the [Edit] menu.**

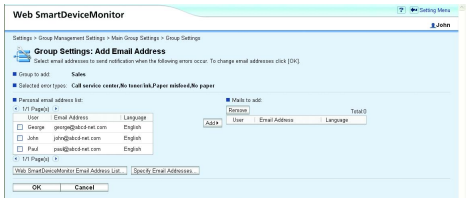


The **[Group Settings: Add Email Address]** screen appears.

8 **Set notification e-mail addresses.**

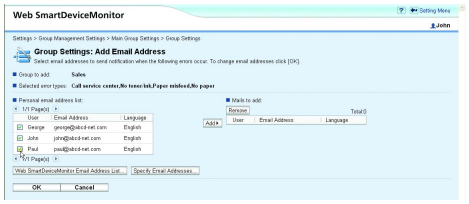
Note

❒ You can set multiple addresses.

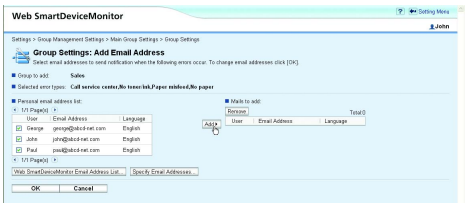


Setting E-mail notification addresses from the personal address book

❶ **Check the check boxes of users to be added to notification e-mail addresses in the [Personal email address list:].**



❷ **Click [Add].**



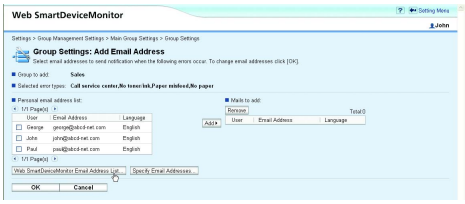
User names appear in the **[Mails to add:]**.

Reference

For details about personal address books, see "Personal Address Book Settings", *Web SmartDeviceMonitor Professional IS/Standard Operation Guide*.

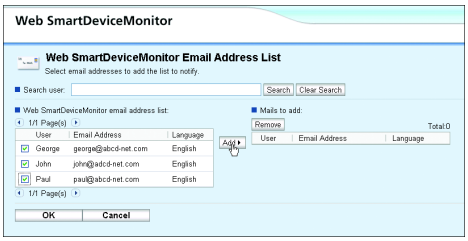
Setting E-mail notification addresses from the server address book

❶ **Click [Web SmartDeviceMonitor Email Address List...].**



The server address book appears.

❷ **Check the check boxes of users to receive notifications and click [Add].**

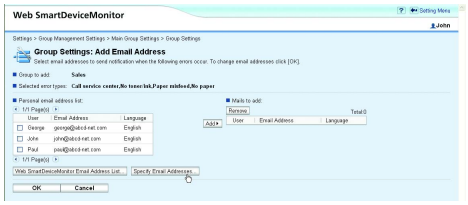


The selected users appear in the add address list.

❸ **Click[OK].**

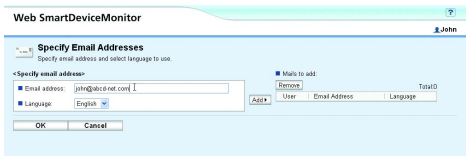
Entering E-mail addresses and setting E-mail notification destinations

❶ **Click [Specify Email Addresses...].**

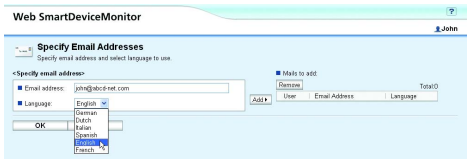


The **[Specify Email Addresses]** screen appears.

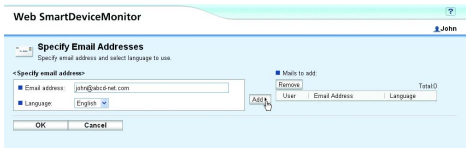
❷ **Enter e-mail addresses in [Email address:].**



❸ **Select the language to be used in e-mail notifications on the [Language:] menu.**

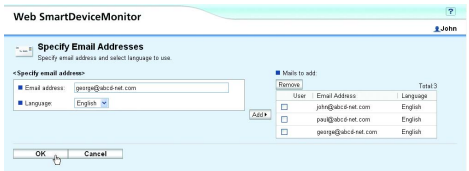


❹ **Click [Add].**

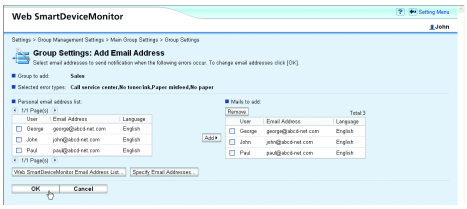


E-mail notification addresses appear in the **[Mails to add:]**.

❺ **Click [OK].**

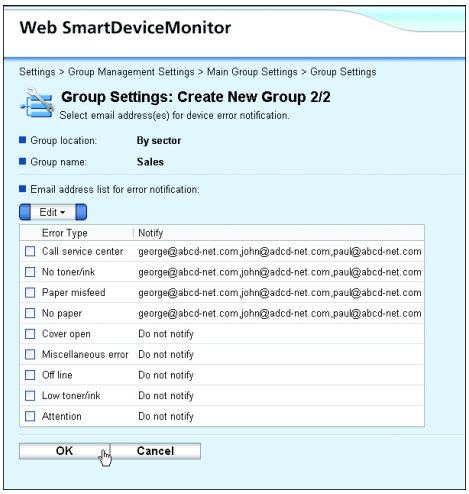


9 **Click [OK].**



Return to the **[Group Settings: Create New Group 2/2]** screen.

10 **Click [OK].**



Quick Setup is now complete.

4. Usage Examples and Settings

This chapter provides examples of Web SmartDeviceMonitor Standard use and required settings.

Note

❒ It is necessary to execute discovery of the devices in advance. Execute discovery settings and execute discovery of network devices while referring to p.41 "Discovery Settings".

❒ If using Windows Server 2003, there are settings that must be made before logging on to Web SmartDeviceMonitor Standard. Execute the settings while referring to p.8 "Settings When Using Windows Server 2003".

❒ Time out is executed if no action is taken for thirty minutes after logging on to Web SmartDeviceMonitor Standard. The screen returns to the login screen if operations are executed after the elapse of thirty minutes. Login again at this time.

Device Error Notification

If a device error is detected by device checking during status polling, notification of the error can be automatically sent.

1 Start the browser on the administrator's computer, and access Web SmartDeviceMonitor Standard. The URL is as follows:

http://*{host name.domain name}*:*{port number}*/wsdm/pc/basic.Login

or

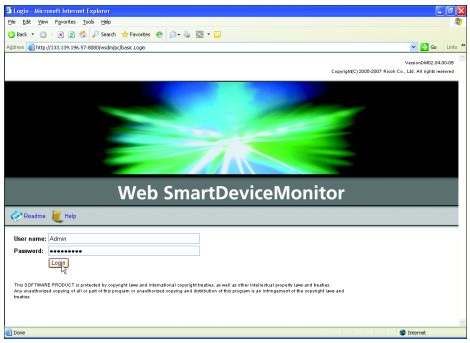
http://*{IP address}*:*{port number}*/wsdm/pc/basic.Login

- Specify the host name or IP address of the computer on which Web SmartDeviceMonitor Standard is installed.
- Specify the name of the domain that contains the computer on which Web SmartDeviceMonitor Standard is installed.

  Note

  ❒ The domain name is required only if the computer on which Web SmartDeviceMonitor Standard is installed belongs to a domain.
- Specify the port number designated when Web SmartDeviceMonitor Standard was installed.

The login screen appears.

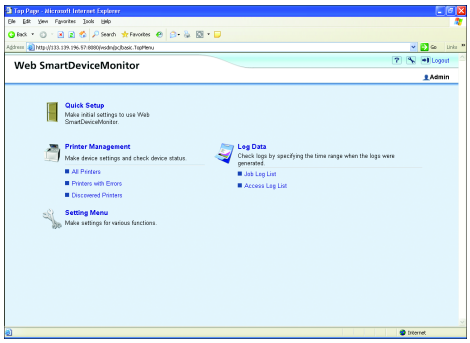


2 **Enter Web SmartDeviceMonitor Standard administrator data.**

- In **[User name:]**, enter the name of the account user with Web SmartDeviceMonitor Standard administrator authority.
- In **[Password:]**, enter the account password entered in **[User name:]**.

3 **Click [Login].**

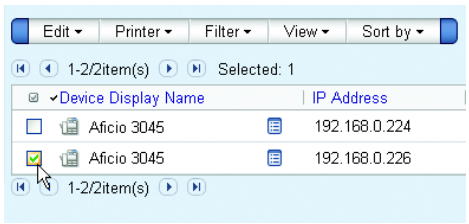
The top page appears.



4 **Click [Printer Management].**

The **[All Printers]** screen appears.

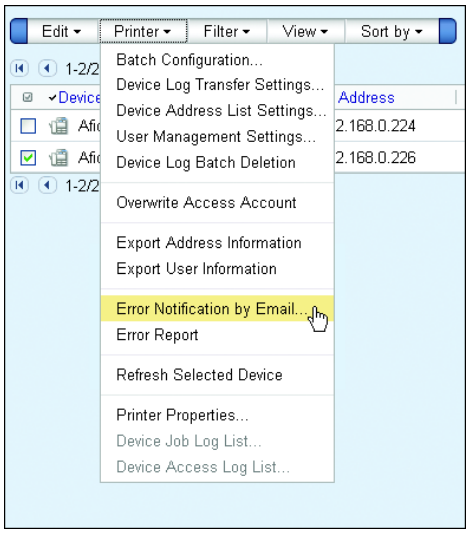
5 **Select the check box of the device for which error notification is to be enabled.**



Note

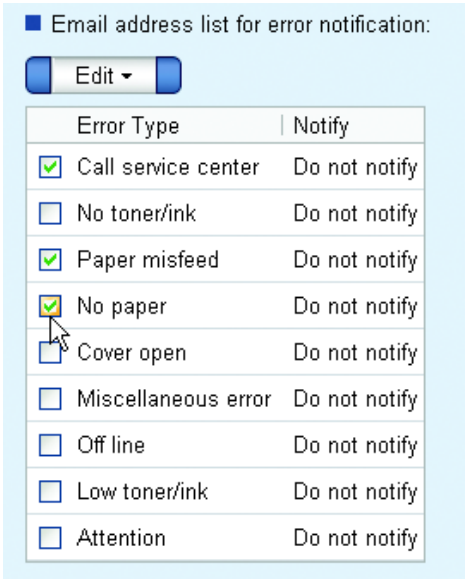
❒ Multiple devices can be selected.

6 **Select [Error Notification by Email...] on the [Printer] menu.**

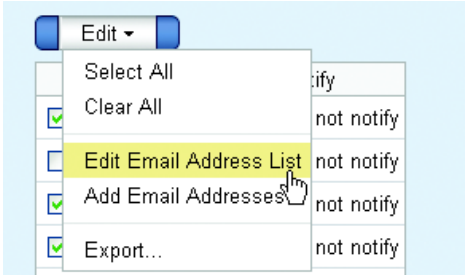


The **[Error Notification by Email]** screen appears.

7 **Under [Email address list for error notification:], select the check boxes of errors that you want to send notification of to selected users.**



8 **Select [Edit Email Address List] on the [Edit] menu.**

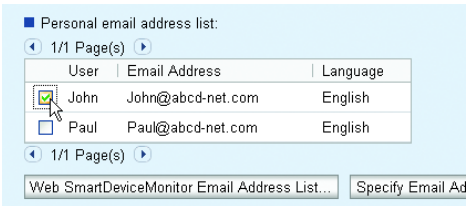


The **[Error Notification by Email: Edit Email Addresses]** screen appears.

9 **Specify the e-mail addresses of notification recipients.**

Specifying addresses from personal address books

❶ **Check the check boxes of users set as notification recipients from the displayed [Personal email address list:].**



❷ **Click [Add].**

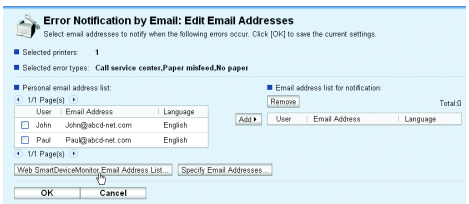
Users set as notification recipients are added to the **[Email address list for notification:]**.

Reference

For details about personal address books, see "Personal Address Book Settings", *Web SmartDeviceMonitor Professional IS/Standard Operation Guide*.

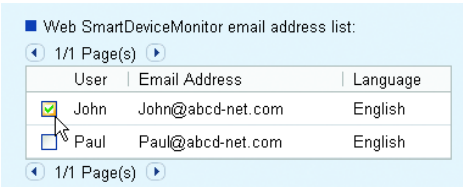
Specifying addresses from the server address book

❶ **If the server address book is to be selected, click [Web SmartDeviceMonitor Email Address List...].**



The **[Web SmartDeviceMonitor Email Address List]** screen appears.

❷ **Check the check boxes of users to receive notifications.**



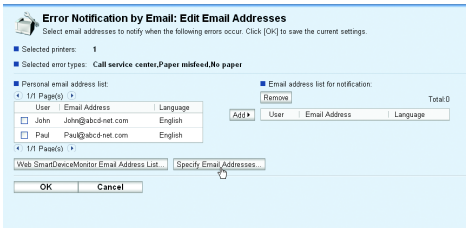
❸ **Click [Add].**

Users set as notification recipients are added to the **[Email address list for notification:]**.

❹ **Click [OK].**

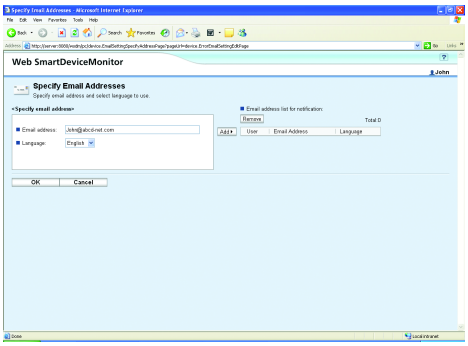
Entering addresses directly

❶ **Click [Specify Email Addresses...].**



The **[Specify Email Addresses]** screen appears.

❷ **Enter the e-mail addresses set as notification recipients in [Email address:].**



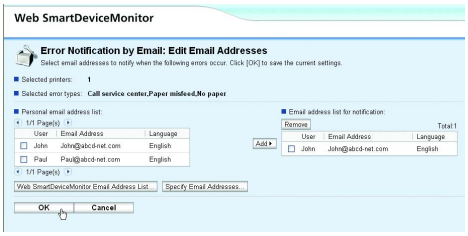
❸ **Select the language to be used in e-mail notifications from [Language:].**

❹ **Click [Add].**

Users set as notification recipients are added to the **[Email address list for notification:]**.

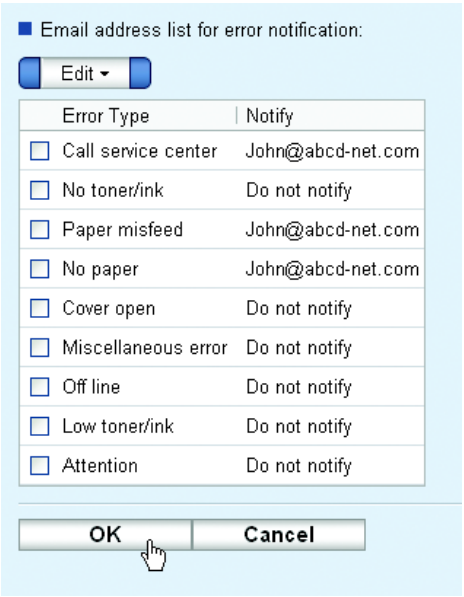
❺ **Click [OK].**

⑩ Click [OK].



The **[Error Notification by Email]** screen appears.

E-mail addresses set as notification recipients are displayed next to the error selected on the **[Email address list for error notification:]**.



⑪ Click [OK].

The **[All Printers]** screen appears.

This completes the setting of error notification recipients. Error notification is now enabled for the selected device.

Note

❒ If multiple errors occur in a single incident, the error with the highest priority will be displayed in the subject line of the notification e-mail sent to recipients who have been selected to receive notice of multiple errors. Details of the other errors will be provided in the body of the e-mail message.

❖ **Priority order of device error notifications**

- Call service center
- No toner/ink
- Paper misfeed

- No paper
- Cover open
- Miscellaneous error
- Off line
- Low toner/ink
- Attention

Collecting Logs

It is possible with Web SmartDeviceMonitor Standard to collect and display job logs and access logs of discovered devices.

Note

❒ It is necessary first for the devices to be discovered. Execute the discovery setting while referring to p.41 “Discovery Settings” and discover the devices on the network.

Log Collection Settings

With log retrieval settings, log system policy is first set with Web SmartDeviceMonitor Standard. Log transfer settings are then made in the devices.

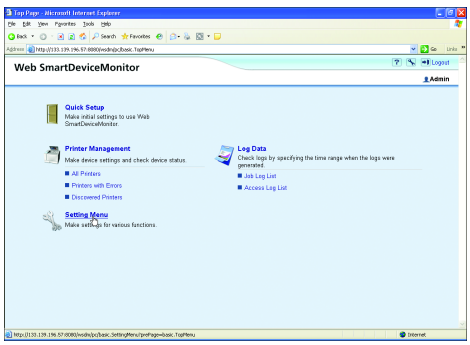
Log System Policy settings

1 Log in on Web SmartDeviceMonitor Standard.

See steps 1 and 3 of p.53 “Device Error Notification” for the login method.

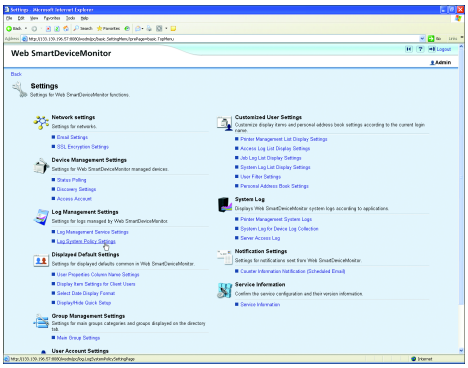
The top menu is displayed.

2 Click the [Setting Menu].



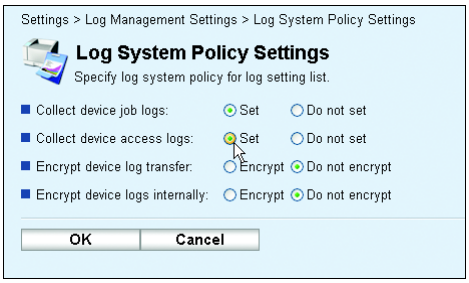
The **[Settings]** screen appears.

3 Under **[Log Management Settings]**, click **[Log System Policy Settings]**.

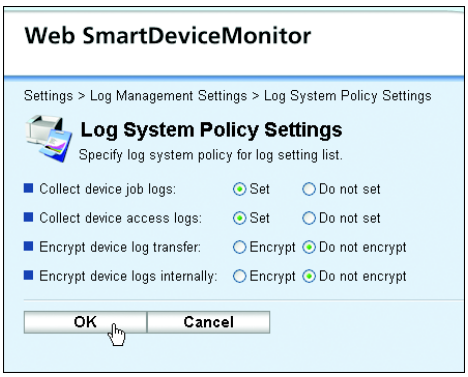


The **[Log System Policy Settings]** screen appears.

4 Select **[Set]** for **[Collect device access logs:]** and **[Collect device job logs:]**.



5 Click **[OK]**.



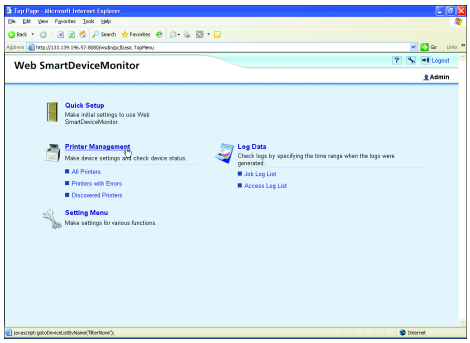
The **[Settings]** screen appears.

6 Click .

The top page is displayed.

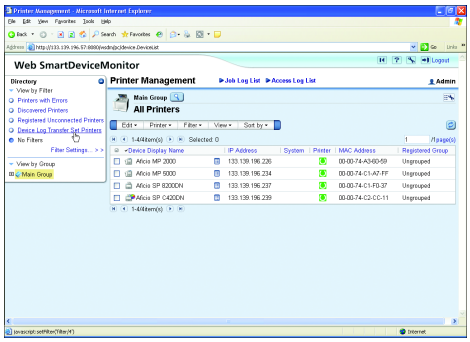
Device log transfer settings

1 **Click [Printer Management].**



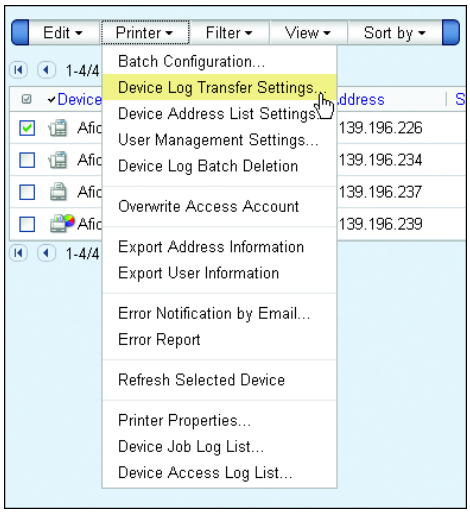
The **[All Printers]** screen is displayed and a list of discovered devices is displayed.

2 **On the [Directory] tab, click [Device Log Transfer Set Printers].**



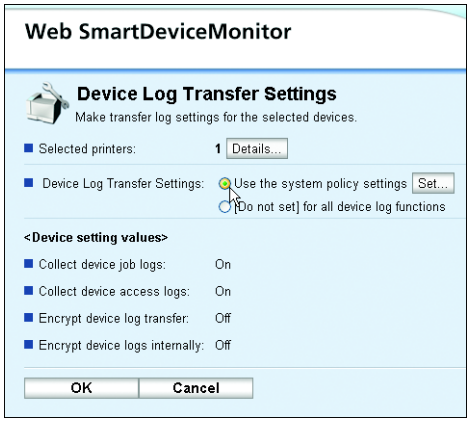
Only devices from which device logs can be transferred will be listed.

3 **Select the check box of the devices whose logs you want to retrieve, and then click [Device Log Transfer Settings...] on the [Printer] menu.**

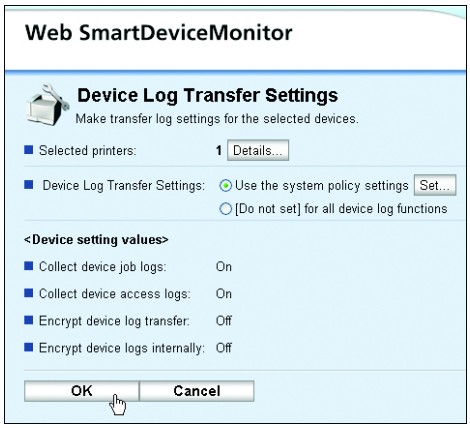


The **[Device Log Transfer Settings]** screen appears.

4 **In [Device Log Transfer Settings], click [Use the system policy settings].**



5 Click **[OK]**.



The **[Device Log Transfer Set Printers]** screen appears.

See the printer management system logs for results of device log transfer settings.

Retrieving device logs

Use the following procedure to retrieve device logs.

1 **On a device for which log transfer was specified, perform a print or copy job.**

Note

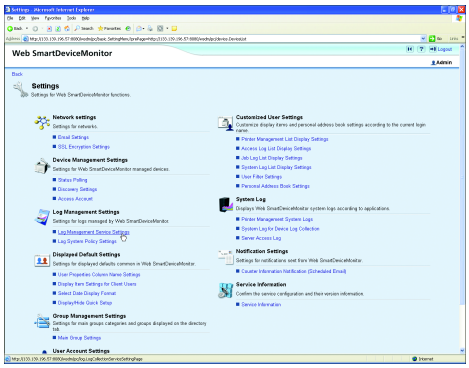
❒ Job logs are generated only if the device has performed at least one job. To view a job log, you must first perform a job on the device.

❒ The following procedure updates the database in real time to confirm retrieval of the device logs. Normally, device logs are automatically retrieved without the user having to perform this procedure.

2 Click .

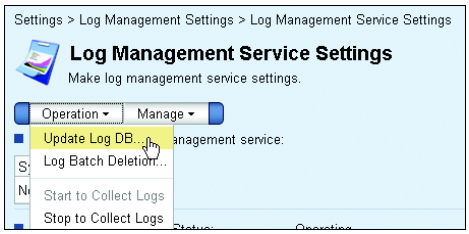
The **[Settings]** screen is displayed.

3 In [Log Management Settings], click [Log Management Service Settings].



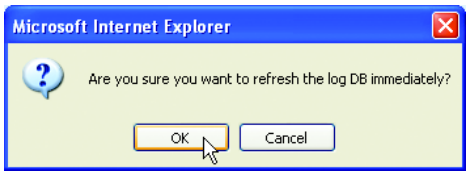
The **[Log Management Service Settings]** screen appears.

4 On the [Operation], click [Update Log DB...].

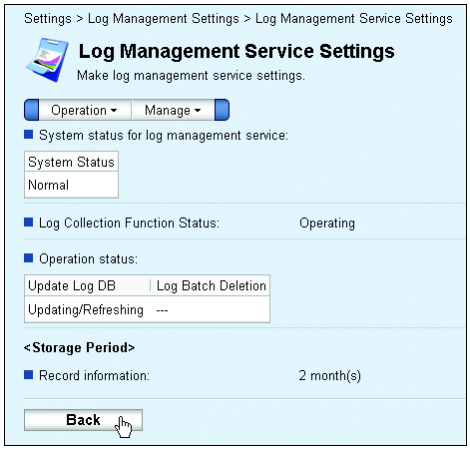


The confirmation dialog box appears.

5 Click [OK].



6 Click [Back].



The **[Settings]** screen appears.

7 Click .

The top page is displayed.

The settings for device log retrieval are complete.

Continue displaying logs.

Displaying Logs

You can view retrieved logs. This section explains how to display a log list by log type and how to display logs by device.

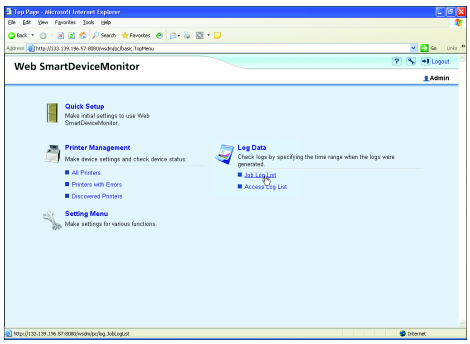
Reference

For details about display items and menus, see "Log Data", *Web SmartDeviceMonitor Professional IS/Standard Operation Guide*.

Displaying a log list by type

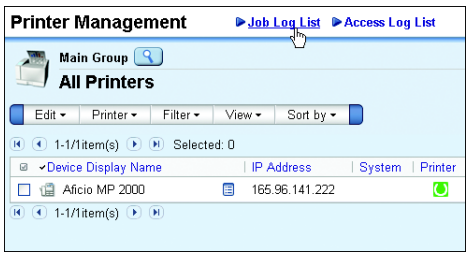
❖ Displaying from the Top Page

Click a log list in **[Log Data]** from the Top Page.



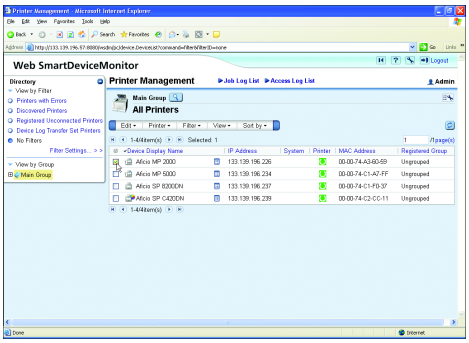
❖ Displaying from the Printer Management screen

Click a log list from the Printer Management screen.

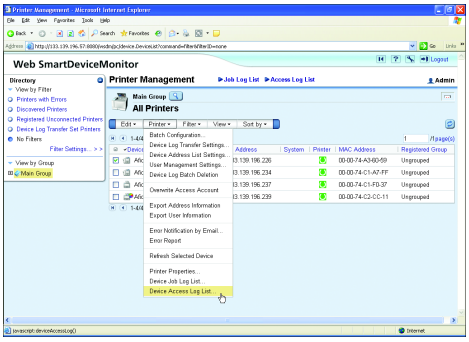


Displaying logs of selected devices

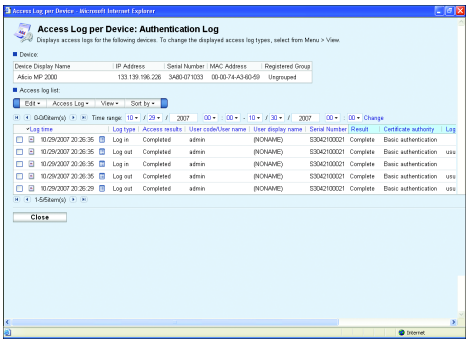
1 **Check the check boxes of devices to display logs.**



2 **On the [Printer] menu, click the log list you want to display.**



The logs of the selected device are displayed in another window.



Uninstallation

The procedure for uninstalling Web SmartDeviceMonitor Standard is explained below.

Uninstalling Web SmartDeviceMonitor Standard

When you remove Web SmartDeviceMonitor Standard, use the Windows **[Add or Remove Applications (or Add or Remove Programs)]** function in the **[Control Panel]**.

Reference

For details about backup using ManagementTool, see "Backup" in "Server Operations", *Web SmartDeviceMonitor Professional IS/Standard Operation Guide*.

Important

- ❒ If there are devices with log transfer enabled, log transfer must be disabled for the devices before uninstalling Web SmartDeviceMonitor Standard.
- ❒ To uninstall Web SmartDeviceMonitor Standard, log on to Windows as the same administrator who performed the installation.

1 If Web SmartDeviceMonitor Standard is running, start ManagementTool.

2 Stop Web SmartDeviceMonitor Standard service using ManagementTool.

3 From the Windows [Start] menu, click [Control Panel].

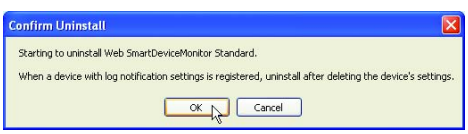
4 Click [Add or Remove Programs].

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

5 Select [Web SmartDeviceMonitor Standard], and then click [Remove].

The **[Confirm Uninstall]** dialog box appears.

6 Click [OK].



The **[Setup Type]** dialog box appears.

Note

- ❒ If you are using an SQL Server 2005 database, a dialog box prompting you to enter the database administrator password (SA password) appears. Enter the SA password set when SQL Server 2005 was installed.

7 **Select whether or not to retain the authentication information, and then click [Next>].**

Note

❒ Select **[Yes]** to retain the authentication information. After uninstallation, the authentication information can be migrated if a product that uses the authentication management service (Web SmartDeviceMonitor/Scan-Router System) is installed.

Uninstallation starts.

When uninstallation is complete, the **[Uninstall Complete]** dialog box appears.

8 **Make sure you select [Yes, I want to restart my computer now.], and then click [Finish].**

Windows restarts.

Uninstallation of Web SmartDeviceMonitor Standard is now complete.

Files remaining after uninstallation

The folders listed below and some of the files they contain remain stored in the computer after Web SmartDeviceMonitor Standard is uninstalled (assuming Web SmartDeviceMonitor Standard is installed in drive C):

- A log file in C:\Program Files\Common Files\RDH Shared2
- Files in C:\Program Files\Common Files\RDH Shared2\bin
- Files in C:\Program Files\Common Files\RDH Shared2\bin\log
- Log files in C:\Program Files\Common Files\RDH Shared2\reg
- Log files in C:\Program Files\RMWSDMEX\bin

Troubleshooting

If problems occur during setup of Web SmartDeviceMonitor Standard, take the remedial actions indicated in the following table.

Problem	Possible cause and solution
Web SmartDeviceMonitor Standard has not been installed correctly.	To install Web SmartDeviceMonitor Standard, you must log on to Windows as an Administrators group member.
	Stop the Web SmartDeviceMonitor Standard service before you update Web SmartDeviceMonitor Standard.
	Uninstall any earlier version of Web SmartDeviceMonitor Standard before installing a 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.
A message is displayed indicating that the designated port cannot be used during Web SmartDeviceMonitor Standard installation.	If Web SmartDeviceMonitor Standard, previously used on a PC operating Web SmartDeviceMonitor Standard using IIS, is uninstalled and reinstalled, it is not possible to use IIS because the previous port is reserved. Take either of the following two steps. • Specify a port number different from that previously used. • Activate Internet Service Manager and delete sites that use the port. **Reference** For details about Internet Service Manager, see Windows help.
An error message "Failed to connect to the authentication management service." appears during Web SmartDeviceMonitor Standard installation.	If your Web server is using IIS, check that the appropriate IIS Service Pack is installed. If the appropriate IIS Service Pack is not installed, install it, and then reinstall Web SmartDeviceMonitor Standard.
Web SmartDeviceMonitor Standard has not been uninstalled correctly.	Stop the Web SmartDeviceMonitor Standard service before you uninstall.
	To uninstall Web SmartDeviceMonitor Standard, you must log on to Windows as an Administrators group member.
The Web SmartDeviceMonitor Standard 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 Standard server. The default port number is 8080 or 80.

Problem	Possible cause and solution
Immediately after Web SmartDeviceMonitor Standard update (overwrite) installation, the device information inherited (preserved) from the earlier version (Web SmartDeviceMonitor) appears gray.	If Web SmartDeviceMonitor Standard detects the device, device information appears grayed. Wait until the device is detected.
Only one account: "Admin" is provided after update (overwrite) installation of the earlier version (Web SmartDeviceMonitor).	Account settings are not preserved, unlike device information. Add accounts as required.
You cannot execute batch settings or remote firmware updates.	The device search access account was not set before executing discovery. Perform one of the following procedures: ① Overwrite the device access account with the system default access account configured using **[Access Account]** on the **[Setting Menu]**: On the **[Printer Management]** screen, select the device whose an access account is to be overwritten, and then click **[Overwrite Access Account]** on the **[Printer]** menu. Click **[OK]** in the confirmation dialog box that appears. ② On the **[Printer Management]** screen, select the device for which you want to set an access account, and then click **[Printer Properties...]** on the **[Printer]** menu. If **[Device Access Account]** is selected on the **[Printer]** menu on the **[Printer Properties]** screen, the **[Access Account]** screen appears. Setup an access account on the **[Access Account]** screen.

Limitations under Windows Vista

Note the following if your computer is running Windows Vista:

❖ **Displaying Help**
"WinHlp32.exe" is required to display Help. If this program is not installed on your computer, download it from the Microsoft Web site and install it.

INDEX

R

S

T

U

W

Due to product development, illustrations and explanations in this guide may differ slightly from your product.

Notes

1. The contents of this documents are subject to change without notice.
2. No part of this document may be duplicated, replicated, reproduced in any form, modified or quoted without prior consent of the supplier.
3. THE SUPPLIER SHALL NOT BE LIABLE FOR THE RESULT OF THE OPERATION OF THIS SOFTWARE OR THE USE OF THIS DOCUMENT.

Important

- ❒ Documents and data stored in the computer can be damaged or lost as a result of user or software error. Be sure to back up all important data frequently.
- ❒ Do not remove or insert any disks 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 SmartDeviceMonitorStandard Setup Guide

GB (GB)
EN (USA) G842-8603D