==========

Web SmartDeviceMonitor Standard Version DM02.10.00

November 2011

==========

Introduction

This file contains additional information that may be useful in using Web SmartDeviceMonitor Standard.

Please read this information and Setup Guide before you install the program.

Please refer to the Manuals and Help for more details and other contents of Web SmartDeviceMonitor Standard.

---

(1) Requirements

<Server>

Computer:	PC-AT compatible machine
CPU:	1GHz Pentium compatible or higher (Pentium4 2.8GHz or higher recommended)
Main memory:	1GB minimum
Hard disk:	
- Program:	800MB
Monitor:	1024x768 pixels or better
OS:	Windows XP Professional + SP2 or later Windows 2000 Professional + SP4 or later Windows 2000 Server + SP4 or later Windows 2000 Advanced Server + SP4 or later Windows Server 2003 Standard + SP1 or later Windows Server 2003 Enterprise + SP1 or later Windows Server 2003 R2 Standard + SP1 or later Windows Server 2003 R2 Enterprise + SP1 or later (Excluding x64 edition) Windows Server2008 Standard Edition/Enterprise Edition (Excluding x64 edition)
DB:	MSDE 2000 SP4(Excluding Windows Server2008)

SQL Server 2005 Express Edition SP1 or later

Network Connection: TCP/IP must be installed.

Browser: Internet Explorer 6.0 + SP1 or later
Internet Explorer 7.0
Internet Explorer 8.0

The product cannot be installed or run on a computer on which ScanRouter DocumentServer, ScanRouter Web Navigator, or ScanRouter EX Professional/ Enterprise is installed.

<Client>

Computer: PC-AT compatible machine
CPU: 500MHz Pentium compatible or higher
Main memory: 128MB minimum
Hard disk: Equal to or more than the recommended hard disk space for operating system
Monitor: 1024x768 pixels or better
OS: Windows XP Home + SP2 or later
Windows XP Professional + SP2 or later
Windows 2000 Professional + SP4 or later
Windows 2000 Server + SP4 or later
Windows 2000 Advanced Server + SP4 or later
Windows Server 2003 Standard Edition + SP1 or later
Windows Server 2003 Enterprise Edition + SP1 or later
Windows Server 2003 R2 Standard + SP1 or later
Windows Server 2003 R2 Enterprise + SP1 or later
(Excluding x64 edition)
Windows Vista Ultimate/Enterprise/Business/Home Premium/Home Basic
Windows Server2008 Standard Edition/Enterprise Edition
Windows 7 Ultimate/Enterprise/Professional/Home Premium/Home Basic
Browser: Internet Explorer 6.0 + SP1 or later

Internet Explorer 7.0
Internet Explorer 8.0

Network Connection: TCP/IP must be installed

(2) Limitations on installation

- For instructions on how to install the product, please read Setup Guide provided with the product. Also please read this file (readme) carefully before you install the product since it contains up-to-date information on the product.

- To install the product, you must have administrator privileges, which means you must belong to the Administrators group.

- Do not install Web SmartDeviceMonitor from a remote computer connected via Remote Desktop Connection. Web SmartDeviceMonitor should be installed locally. Note that this excludes the cases where a precreated SQL Server 2005 DB is used.

- If Windows Firewall is set to ON on your computer, you may receive an alert message when installing the product. If this is the case, click the Unblock button in the message dialog to proceed.

- When you install the product, some important files are installed on the following locations in addition to the folder you specified for the installation. These files are essential for the product to work, so please be careful not to delete them accidentally.

  <S>:¥Program Files¥Common Files¥RDH Shared2
  <X>:¥Program Files¥Common Files¥RDH Shared2

  * <S> is the Windows system drive
    <X> is the drive you specified for the installation of the program

  * Please note that the folder names, "Program Files" and "Common Files" differ depending on the OS being used.

- MSDE 2000, which will be installed with the product, cannot be used with Windows 2008 Server. If you wish to use Windows 2008 Server, please be sure to install SQL Server 2005 before installing Web SmartDeviceMonitor.

- If you are going to use IIS 7.x, make sure that all the IIS extended options bellow are installed. Otherwise, you may not be able to select IIS when installing
  Web SmartDeviceMonitor.

    * ISAPI Extension
    * ISAPI Filters
    * Static Content
    * Default Document
    * HTTP Redirection
    * Directory Browsing
    * ASP.Net
    * Windows Authentication
    * IIS Metabase
    * IIS 6 WMI

- If User Access Control (UAC) is enabled on Windows 2008 Server, you must run the follwing tool as an administrator. To do this, right-click it and select [Run as Administrator]. If UAC is enabled and you do not run it as an administrator, some functions will not run correctly.

    * ManagementTool
    * Activation Tool
    * Authentication Manager

- Note for McAfee VirusScan Enterprise 8.0 (and later) users
  Apply the latest patch of VirusScan Enterprise before installing Web SmartDeviceMonitor. The latest patch is available to download from McAfee's website. See McAfee's website for details.
  Please also note that the following settings must be made in order to get Web SmartDeviceMonitor to work properly:

* In the VirusScan On-Access Scan Properties dialog box, add mdf and ldf as "What not to scan" items so that they will be excluded for scan. Mdf and ldf files are some of the files of the database that is used by Web SmartDeviceMonitor.

- Please note that when you have an antivirus program installed and running on the target PC, installing/uninstalling WSDM may take long. (This problem has been identified with McAfee/NetShield.)

- If McAfee PrivacyService is installed on the target computer, you must add the URL for Web SmartDeviceMonitor to McAfee PrivacyService "Allow List" and "Cookie."

- After you install Web SmartDeviceMonitor, the install program may require you to restart the PC. In some cases, however, the PC will not be restarted even though you accepted to restart. In this case, you must restart the PC manually.

(3) Limitations on uninstallation

- To uninstall the product from your computer, you must have administrator privileges. Please make sure to use the same account that was used when the product was installed.

(4) Notice / Limitations

- To reinstall this product after OS upgrade, a clean install is recommended.

- If you change OS administrator account and password after the product is installed, you must update account information as follows:

(1) Select Control Panels > Administrative Tools > Services.
(2) Open the Properties dialog box of the following services.

(3) Choose the Log On tab and enter the current user name and password correctly.

* DmComSc
* ServerAgentService

- The "admin" user is a built-in account that will not be listed in the User list. Therefore you cannot specify it as a notification destination.

- To backup your data files, you must use both ManagementTool and Authentication Manager.
Likewise, to restore your data files, use ManagementTool and Authentication Manager.

- The port number cannot be changed while the server is in operation.
Please note that if you make a backup of the data, uninstall the program, and then install the program again to rebuild the environment so that you can change the port number, the backup data cannot be restored on the environment where the port number has been changed. In this case, all you can migrate is information on devices, users, and groups, which can be done by using the Export/Import function of ManagementTool.

- To edit the User authentication settings using the Batch Configuration function, you must first set User administrator authentication to ON for the target printers. Follow the steps below:

1. Choose the printers that you want to change the settings and select Batch Configuration from the menu. Select Administrator settings and under the <Administrator authentication management> section, check the Administrator authentication management checkbox and select "On" for User administrator authentication. Click the OK button.
Do not proceed with the User authentication settings but click Next and then OK to finish the Batch Configuration.

2. Choose the printers again and select the Batch configuration menu item. Select User authentication settings and edit the settings as needed.

Click OK, Next, and OK to complete the Batch Configuration.

- If you select IIS as Web server, the product uses an anonymous user account (IUSR_<computer name>) for IIS. Therefore, do not disable IUSR account.
  To change the password for IUSR account, refer to the following URL for instructions:

  http://support.microsoft.com/kb/297989/EN-US/

- It is necessary to setup with IIS for restricting the HTTP access when utilizing this application enabling HTTPS (SSL) with IIS. Please refer IIS help titled "SSL (Secure Sockets Layer)" to setup as follow:
  - -- When this application is installed on the same port number as "Default Web Site" of IIS, setup with property of "Default Web Site".
  - -- When this application is installed on the different port number as "Default Web Site" of IIS, setup with property of "RDH Common2".

  1. Select the "Default Web Site" or "RDH Common2", and then click [Properties] from [Action] menu.
  2. Click [Edit] from [Secure Communications] on the [Directry Security] tab.
  3. Add the check mark to [Require secure channel (SSL)] in the [Secure Communications] window.

- Depending on the device model being used, configuring Date and time in Batch Configuration may fail. Configure one device at a time using WebImageMonitor.

- Depending on the device model being used, configuring LPR, DIPRINT, and IPP all at once in Batch Configuration may fail. Perform Batch Configuration to configure each item (LPR, DIPRINT, IPP) individually.

- Before running Window Update on the computer where Web SmartDeviceMonitor server is running, be sure to stop the service of ManagementTool. If you run Windows Update while the service is running, you must restart the service from

Management Tool when Windows Update is finished.

- You may see a phishing alert when you open the following e-mail sent from Web SmartDeviceMonitor using the Windows mail software on Windows Vista:

  * Device error notification
  * Batch configuration completion

  This is because such e-mail messages include the URL of Web SmartDeviceMonitor. To refer to the URL, you must turn off the Phishing Filter function manually.

- When you access Web SmartDeviceMonitor from Windows Vista x64 Internet Explorer,
  some of the characters may not be displayed correctly. It can be fixed by resizing the window.

- This product uses Web server of Apache or IIS and Tomcat.
  Web server, as well as Tomcat, generates access log files, which can be easily increased in size depending on the amount of time and frequency the server is used. We recommend you to periodically check these files and delete or move them to prevent them from taking over your server's disk space.

  A sample batch file that can be used to delete old Apache/Tomcat log files will be installed along with the product.
  For information about using the batch file, please refer to the later section of this document, "(3) Apache/Tomcat log deletion tool."

  Log files will be created in the following location:
  (1) Web Server
    (a) Apache Web Server
      If you choose Apache when installing the product, Apache Web Server is installed by the installer.
      Access log files of Apache Web Server is created in the following directory:

X:¥Program Files¥Common Files¥RDH Shared2¥Apache¥logs

Note: These files are named using the following format containing date information:

Http access log:	accessYYYY-MM-DD.log
Https access log:	accessYYYY-MM-DD_log
Action / Error log:	errorYYYY-MM-DD.log
	error_logYYYY-MM-DD.log

Do not delete any files other than the above names.

(b) IIS

IIS access log files are created in the location specified in the IIS settings. To find where the log files will be stored, check your IIS settings. By default, they will be created in the following directory:

X:¥WINNT¥system32¥LogFiles¥W3C

(2) Tomcat Log

Tomcat generates log files in the following directory no matter which Web Server is being used:

X:¥Program Files¥Common Files¥RDH Shared2¥Tomcat¥logs

Note: These files are named using the following format containing date information:

Action / Error log:	localhost_admin_log.YYYY-MM-DD.txt
	localhost_log.YYYY-MM-DD.txt

Do not erase any files other than the above names.

(3) Apache / Tomcat log deletion tool

There is a tool that can be used to delete Apache / Tomcat log files. The tool is installed in the following location:

Directory:

Installation folder¥apps¥doc

Files:

ApacheLog.bat: Starts Apache/Tomcat log deletion tool

ApLogDel.vbs: Contains a set of scripts for deleting Apache/Tomcat log

By default, the tool will erase all log files that are older than 30 days. This setting can be modified to meet specific needs. For information about the commands, refer to ApacheLog.bat.

* These files may be used for access analysis. Please determine how long you keep these files after careful consideration.

* IIS log files cannot be deleted by this tool. Please delete them manually as necessary.

(5) Using the product on Windows Server 2003 or later

The security features in Windows Server 2003 SP1 or later have been enhanced in many ways. If you are going to install and use the product as the server on such operating systems, please note that the following settings must be done before the users can use Authentication Manager from their client PCs:

a. DCOM settings

1. Select [Start] - [Administrative Tools] - [Component Services] or start dcomcnfg from [Run]
2. Open the properties of My Computer from [Component Services] - [Computers] - [My Computer]
3. Select the [COM Securities] tab and click the [Edit Limits] button in the [Access Permissions] section
4. Allow [Local Access] and [Remote Access] for ANONYMOUS LOGON
5. Click the [Edit Limits] button in the [Launch and Activation Permissions]
6. Add ANONYMOUS LOGON and allow Local Launch, Remote Launch, Local

Activation and Remote Activation for it

7. If you enable Windows Firewall, the following settings are also needed:
   7-1. Select [Connection-oriented TCP/IP] in the [Default Protocols] tab and click the [Properties] button
   7-2. Click the Add button of Port range and enter DCOM port range

   * Please specify successive port numbers that are not used
     (Example: 6001-6010)
     In most cases, 10 ports are enough. However, you can add more ports in case of need. Please keep in mind that these ports are used by not only the product but also any DCOM-using applications on the server.
8. Click [OK] and restart the server.

b. Exceptions ports of Windows Firewall
   This setting is required if you want to set Windows Firewall to on

   1. Launch [Windows Firewall] from [Control Panel]
   2. Select the [General] tab and click to select [On]
   3. Select the [Exceptions] tab and follow the instructions below:
      - Check [File and Printer Sharing]
      - Add the following ports:

Name	Prot number	TCP/UDP	
RPC	135	TCP	
RSI	50304	UDP	
WebHTTP	8080 or 80 (default)	TCP	(*1)
WebHTTPS	8443 or 443 (default)	TCP	(*1)
DCOMPort01	6001 (*2)	TCP	
:	:	:	
:	:	:	
DCOMPort10	6010	TCP	

(*1) HTTP port that Apache or IIS will use (the one specified when the product is installed)
Default for Apache: 8080
Default for IIS: 80
When SSL communication is enabled, HTTPS port must also be added
Default for Apache: 8443
Default for IIS: 443

(*2) If the OS is Windows Server 2003 SP1 or later, please add every DCOM port you have specified in 7-2 of "a. DCOM settings" above. The port numbers shown here are examples. You must specify the actual port numbers.

4. Click OK and restart the server.

<<<NOTICE>>>

Third Party Software; Copyrights and License Agreements

Certain third party software may be distributed, embedded, or bundled with Ricoh products, or recommended for use in conjunction with the installation and operation of this Ricoh product. Such third party software is separately licensed by its copyright holder. All third party software is governed by and must be used only in accordance with the terms of its license agreement. This section identifies the third party software contained in this Ricoh product; the copyright holder's proprietary notices and the license agreements which govern the use of each third party component.

Ricoh makes no representations or warranties of any kind whatsoever regarding any third party software, nor does Ricoh offer any support or maintenance for such third party software.

Notwithstanding anything herein to the contrary, all Third Party Software are furnished by Ricoh 'AS IS' AND WITHOUT ANY WARRANTIES OF ANY KIND, EXPRESS OR IMPLIED.

The third party software used in connection with this Ricoh product is as follows:

- Apache Software Foundation Components

  This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

  + Apache Axis
  + Apache Commons
  + Apache HTTP Server
  + Apache Log4cxx
  + Apache Log4j
  + Apache Tomcat
  + Apache Xerces

Copyright (c) 1999-2008 The Apache Software Foundation

Components from the Apache Software Foundation are licensed
under the terms of the Apache License version 2.0. A copy
of this license can be found in the "licenses" folder.

- deczip.exe

DECZIP.EXE (c) by pon software 2002-2007

- Expat

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd

These components are licensed under the terms of the
MIT License. A copy of this license can be found
in the "licenses" folder.

- Hibernate

profile.jar is db access module by using Hibernate library.
Copyright (C) 2005-2008 Ricoh Corp.

This library is licensed under the terms of the GNU Lesser
General Public License. A copy of this license can be found
in the "licenses" folder.

- Info-Zip

This product includes software developed by the Info-Zip
workgroup (http://www.info-zip.org).

+ Unzip32.dll
+ Zip32.dll 1.1

These components are licensed under the terms of the

Info-Zip License. A copy of this license can be found
in the "licenses" folder.

- Net-SNMP

Various copyrights apply to this package:

Copyright 1989, 1991, 1992 by Carnegie Mellon University
Derivative Work - 1996, 1998-2000
Copyright 1996, 1998-2000 The Regents of the University of California
All Rights Reserved

Copyright (c) 2001-2003, Networks Associates Technology, Inc
All rights reserved.

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.
All rights reserved.

A copy of this license can be found in the "licenses" folder.

- Openssl

Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

This software includes a Blowfish implementation that is
Copyright (C) 1995-1997 Eric Young.

A copy of this license can be found in the "licenses" folder.

- STLport

Copyright 1999,2000 Boris Fomitchev

Portions of this software have copyrights held by the following
organizations:

Copyright 1994 Hewlett-Packard Company
Copyright 1996,97 Silicon Graphics Computer Systems, Inc.
Copyright 1997 Moscow Center for SPARC Technology.

These components are licensed under the terms of the
STLport License. A copy of this license can be found
in the "licenses" folder.

- Zlib

Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler

A copy of this license can be found in the "licenses" folder.