



Sentinel User Guide



Version 2.70



Smart Printing Solutions

November 2010

All rights reserved. Neither this documentation nor any part of it may be reproduced, stored in a retrieval system, translated into another language, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, or otherwise, without the prior written permission of Smart Printing Solutions (SPS) LTD.

While every precaution has been taken in the preparation of this manual, SPS assumes no responsibility for errors or omissions, nor is any liability assumed for damages resulting from the use of the information contained herein. The information contained in this document is subject to change without notice. SPS reserves the rights to make any such changes without obligation to notify any person of such revision or changes. SPS makes no commitment to keep the information contained herein up to date.

Copyright © 2001–2010 Smart Printing Solutions (SPS) LTD.

Address: P.O. Box 30, Misgav Industrial Park
20179, ISRAEL

Tel: +972-4-990-9357
Fax: +972-4-999-0068
Email: info@smartprinter.co.il
Web: www.smartprinter.co.il

Contents

Welcome to Sentinel	1
What is Sentinel?	1
How does Sentinel work?	1
Using This Document	2
Installation	3
System Requirements	3
Preparing the System.....	3
Installing Sentinel Server Software on Windows Server 2003	3
Installing on Windows 7.....	9
Installing on Windows Server 2008	12
Installing on x64 Platforms.....	17
Registry Permissions in Windows 2000/XP.....	17
Checking the Installation	18
Configuring the Firewall for Sentinel.....	18
Installing Device Controllers	19
Configuring the Sentinel Server	21
Configuration Guidelines	21
Card Reader	21
Document	23
Auto Sync.....	24
Printing	25
Monitor	26
Quota Policy	27
Interface.....	27
Email.....	27
License.....	28
TCP/IP.....	28
Billing Code.....	28
Cluster and Other Settings.....	29
Senti-Mail Scan Control.....	30
Basic Functions	32
Adding a New Device.....	32
Upgrading a Device's Network Firmware.....	36
Adding New Users	37

- Databases..... 40**
 - Changing the Access Database into SQL Database 40
 - Upgrading the Database from Older Versions of Sentinel..... 41

- Sentinel Monitoring Screens..... 42**
 - Print Jobs..... 42
 - History and Archive 43
 - Logging and Errors..... 44
 - Reports 44
 - Printer Reports (Summary and Detailed)..... 46
 - User Reports (Summary and Detailed)..... 47
 - Billing Code Reports (Summary and Detailed) 48
 - Billing Code Reports (By User and By User Table) 49
 - Group, Department, Organization, and Company Reports..... 50
 - Other Reports..... 51

- External Utilities..... 52**
 - Maintenance Utilities 52
 - Identifying Print Jobs Sent from a Shared Workstation..... 53
 - Running Sentinel with Advanced Printing Features 58

- Troubleshooting..... 61**
 - Failed to Add Sentinel Service 61
 - Failed to Access IIS Metabase..... 61
 - Wrong username appears in the Web interface 62
 - HTTP Error 404: File or Directory not found 62
 - Could not use "; file already in use 63
 - Configuration Error 67
 - Service Unavailable Error 68
 - Job ID number is inconsistent or not advancing 69
 - Error in file C:\WINDOWS\TEMP when trying to make reports..... 70
 - The 'Microsoft.Jet.OLEDB.4.0' provider is not registered 71
 - The process cannot access the file..... 71
 - An error occurs when trying to load Crystal Reports 72
 - The Reports toolbar buttons are missing 72
 - Error when issuing a report 73
 - Default website is used by another application on the server 73
 - New print jobs don't appear in the Waiting Jobs list 76
 - Left-hand menu appears with strange spacing 77
 - Unknown User 79

Welcome to Sentinel

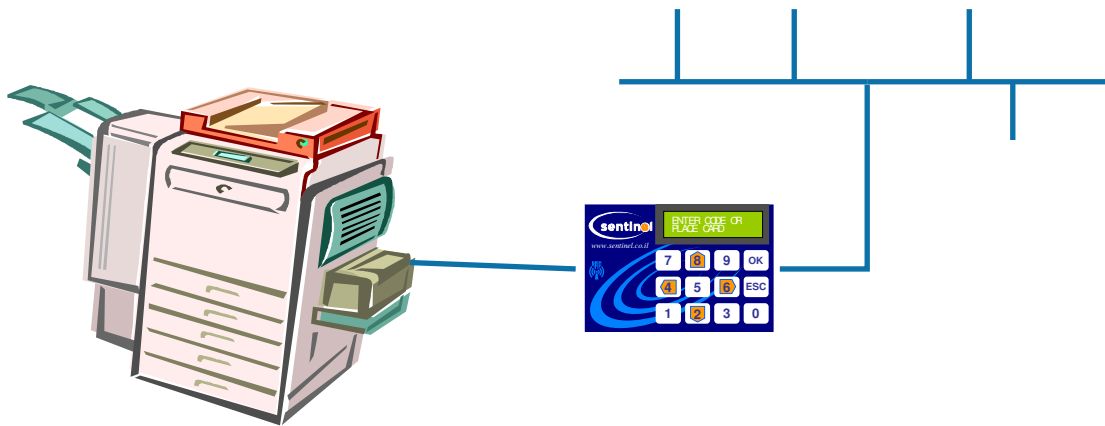
What is Sentinel?

Sentinel is a printing management and control system. Sentinel provides three critical features for your network printers:

- Improved security. Sensitive documents are collected only by the user who sent them, and are not lost or left unattended. Sentinel gives you control over who can print to which devices, and times that devices can be available.
- Reduced waste. Cut down on expensive, wasteful printing and copying.
- Powerful reporting. You can monitor and track all device usage by individuals or groups, or by device.

Sentinel does this by enabling printing only after identification has been established in a device connected to each printer.

Sentinel is made up of physical device controllers and software installed on the server. Each device controller has two network connections and is located between the printer and the network.



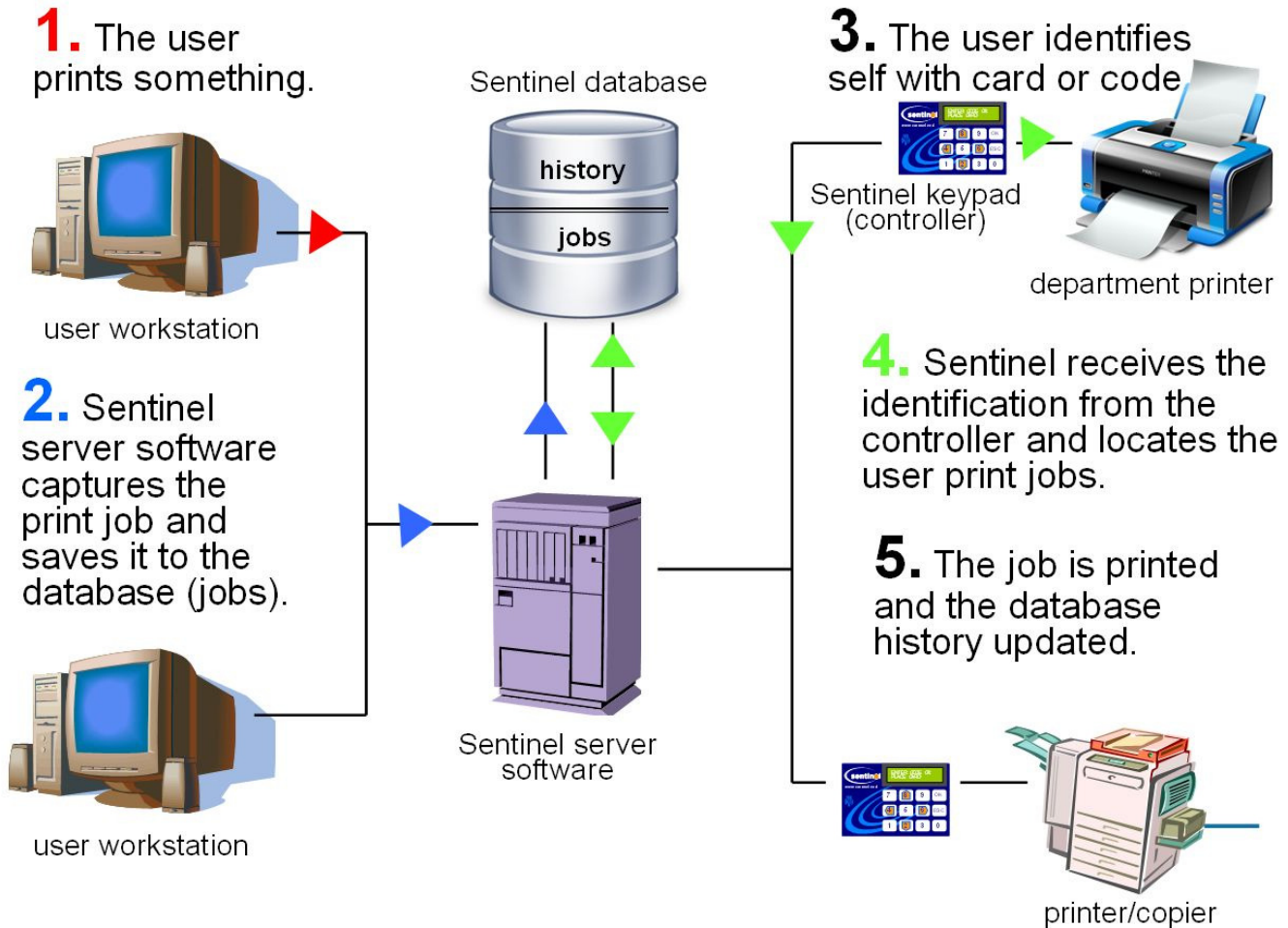
How does Sentinel work?

Sentinel has three main components:

- **Sentinel server:** software that sits on a PC (preferable Windows Server 2003). The server software includes the interface for you (the administrator), including all monitoring screens, all settings (Sentinel configuration definitions), user information, and report generation.
- **Sentinel database:** while database usually sits on the same PC as the server, it is a separate entity and can be located on a different computer in the network. The database has two parts:
 - **current jobs:** this is an area in which all current job requests are written.
 - **history:** this is an area where information about a print job is stored after a job is completed. This information is what is used for Sentinel reports.
- **Sentinel device controller:** the device controller is a small electronic unit with a keypad that is mounted next to each physical printer, copier, or scanner to be included in the Sentinel system. The device controller is connected between the network and to the printer. There are several different device controller models and different mounting options, but all have the same function. Jobs directed to that physical printer are only released when a user ID card (a magnetic card) is swiped or scanned at the device controller mounted next to that

printer. (Depending on the Sentinel configuration for that device and that user, jobs may also be released by entering a code at the device controller, or even printed automatically with no device controller activity.)

Here is a simplified diagram of the workflow in Sentinel:



Using This Document

This user guide is for the Sentinel administrator (usually the system administrator or network administrator). It contains installation and configuration instructions, as well as a description of all parameters, and some troubleshooting tips.

User documentation is provided as a template that can be modified with your company's logo, printed, and posted next to each Sentinel device controller. (After installation, sample templates are located in the folder `c:\Inetpub\wwwroot\Sentinel`. The templates have the file extension `.png`.)

Additional information about the Web interface for users (non-administrators) will be available in a later release.

Installation

System Requirements

Sentinel's software is based on the IIS Web server, so it will only run on computers that can run IIS.

Operating System

Microsoft Windows Server 2003	Strongly recommended
Microsoft Windows 2000 Microsoft XP Professional Windows 7 Windows Server 2008	Restrictions apply; does not support all features or capabilities and requires special configuration (see: <ul style="list-style-type: none">• <i>Registry Permissions in Windows 2000/XP</i> on p. 17• <i>Installing on Windows 7</i> on p. 9• <i>Installing on Windows Server 2008</i> on p. 12Error! Bookmark not defined.
x64 (64-bit) platforms	Restrictions apply; Sentinel must be configured specifically for this platform (see <i>Installing on x64 Platforms</i> on p. 9).

Browser

IE 6 or later

IE 7 or later

Recommended for best viewing

Preparing the System

Before installing the Sentinel software, make sure that the server is properly configured:

1. Install IIS (Internet Information Services) on the server system. For details, refer to Microsoft (<http://www.microsoft.com/resources/documentation/windows/xp/all/proddocs/en-us/iiiisin2.msp?mfr=true>).
2. Install Dot.Net framework 2.0 (<http://www.microsoft.com/downloads/details.aspx?FamilyID=0856EACB-4362-4B0D-8EDD-AAB15C5E04F5&displaylang=en>).

Installing Sentinel Server Software on Windows Server 2003



Caution!

These instructions are for installing Sentinel server software on a PC running Windows Server 2003 only.

- If you must install Sentinel on a Windows XP, Windows 2000, Windows 7, or windows Server 2008 platform, be aware that Sentinel will not be fully functional. You will also have to manually edit the Windows Registry to set certain permissions. See:
 - *Registry Permissions in Windows 2000/XP* on p. 17
 - *Installing on Windows 7* on p. 9
 - *Installing on Windows Server 2008* on p. 12
- If you must install on 64-bit platforms, be aware that there may be some limitations, and Sentinel requires special configuration. See *Installing on x64 Platforms* on p. 9.

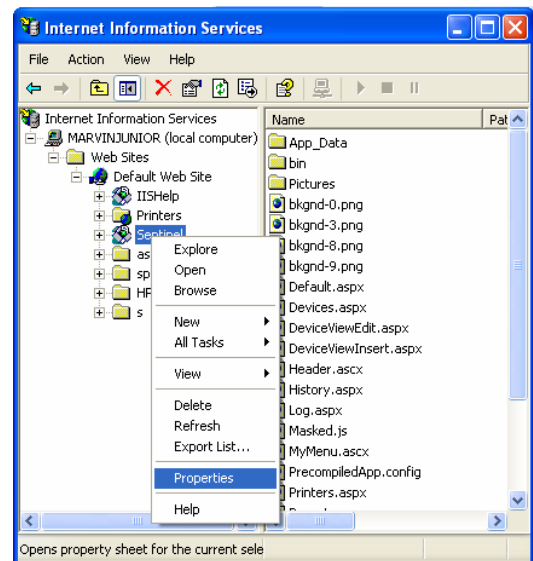
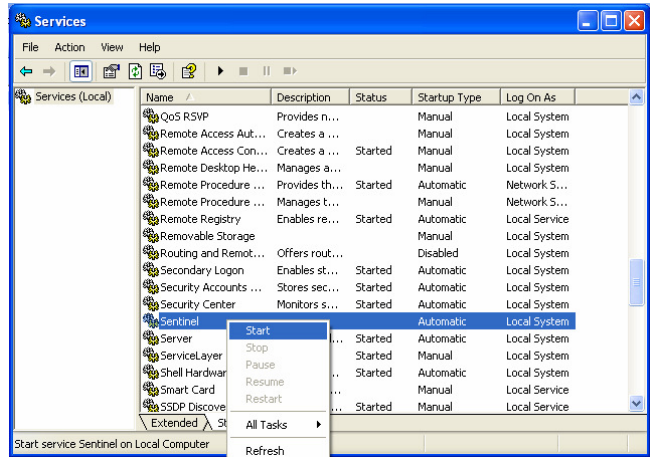
1. Run **SETUP.EXE** from the Sentinel installation directory or CD-ROM and follow the directions on screen. Use the default directories during the installation process.

2. Go to Services (Start → Settings → Control Panel → Administrative Tools → Services).

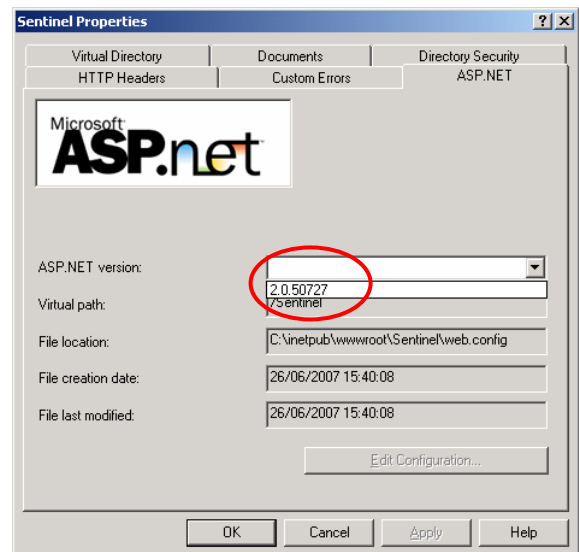
If you don't see these options in the Control Panel, make sure that you are in Classic View, rather than Category View.

3. To start the Sentinel service, scroll down to **Sentinel**, right-clicking it, and select **Start**. If the Sentinel service doesn't exist, see *Failed to add Sentinel Service* on p. 61.

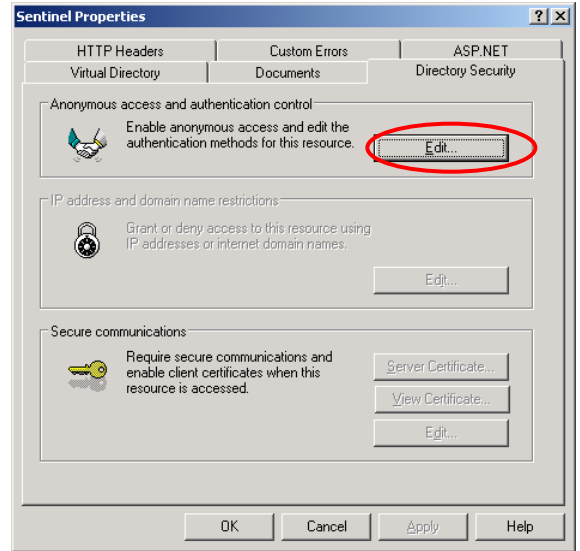
4. Go to IIS Settings (Start → Settings → Control Panel → Administrative Tools → Internet Information Services). Expand **Local Computer\Web Sites\Default Web Site**. Right-click **Sentinel** and select **Properties**.



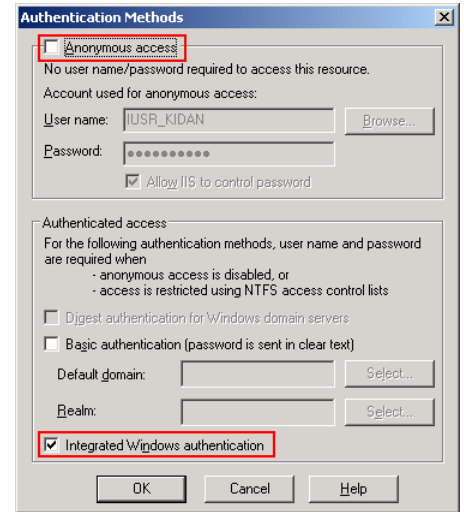
5. In the ASP.NET tab, make sure that the ASP.Net Version is 2.X.



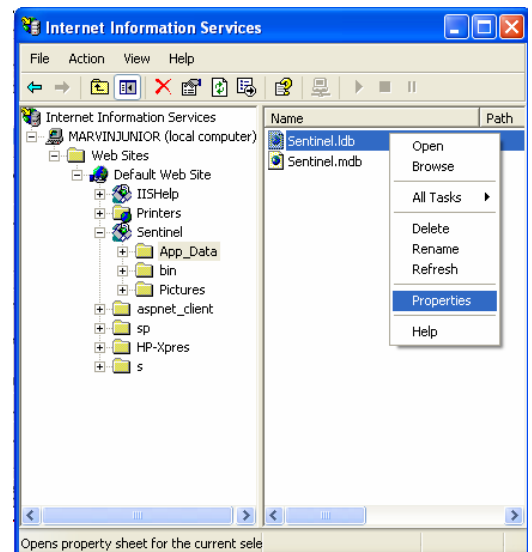
- In the Directory Security tab, click **Edit**. This opens the Authentication Methods dialog box.



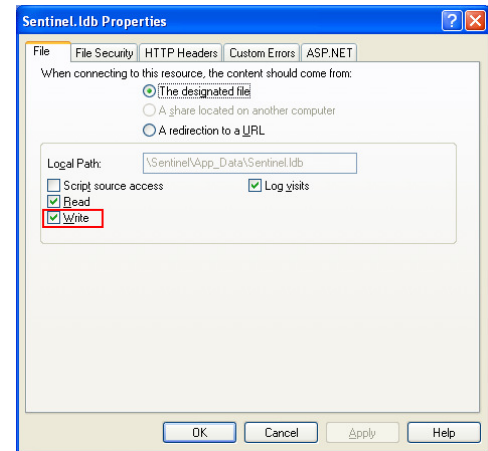
- Make sure that **Anonymous access** is not selected and that **Integrated Windows Authentication** is selected, and click **OK**.
- Click **OK** again to exit from Sentinel Properties.



- Expand **Sentinel** and select **App_Data**. Right-click **Sentinel.mdb** and select **Properties**.

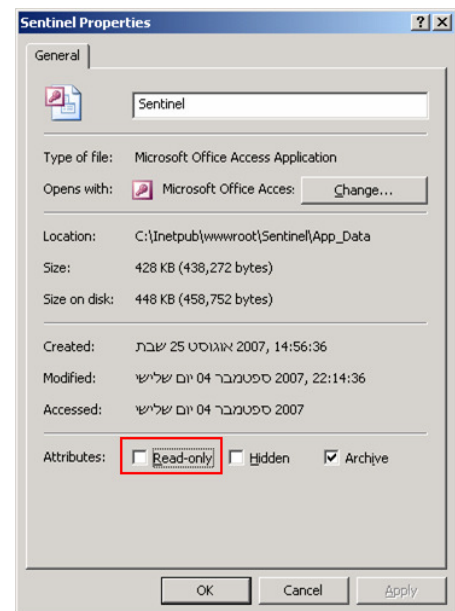


10. In the File tab, select the **Write** checkbox and click **OK**.

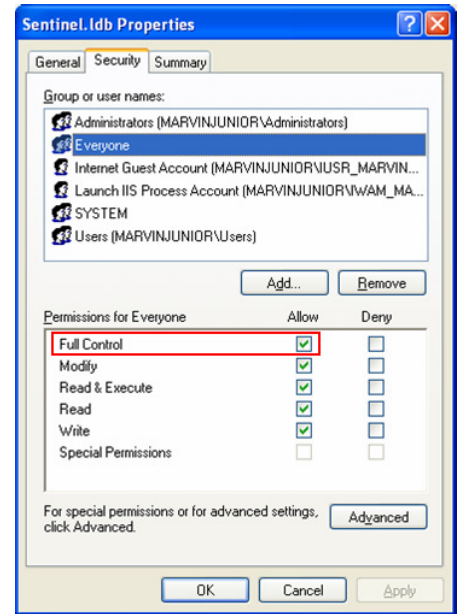


11. Repeat this process (from step 8) with **Sentinel.Idb**.
If the file **Sentinel.Idb** doesn't exist:
- a) Start the Web Sentinel (Start → Programs → Sentinel → Web Sentinel).
 - b) Ignore any errors and close the browser window. The file **Sentinel.Idb** should appear now.
 - c) If **Sentinel.Idb** still doesn't exist, collapse **App_Data** and then expand it again.
 - d) If **Sentinel.Idb** still doesn't exist, skip it perform the changes only to **Sentinel.mdb**.

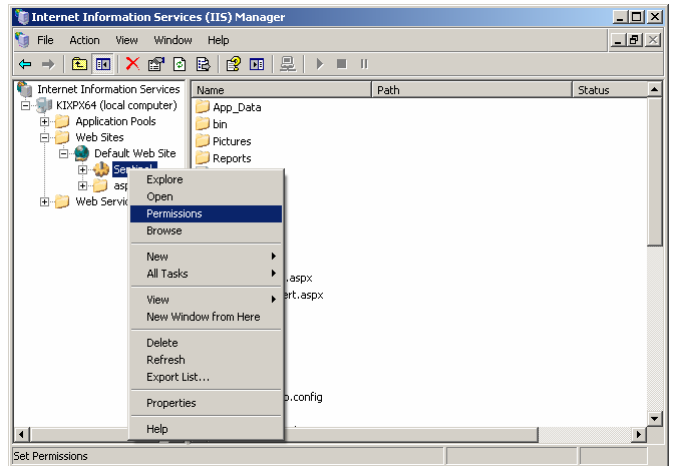
12. Go to the IIS Sentinel folder (default directory is **c:\inetpub\wwwroot\Sentinel**) and enter the **App_Data** folder.
13. Right-click **Senitnel.mdb** and select **Properties**.
14. Make sure that the **Read-Only** checkbox is not selected.



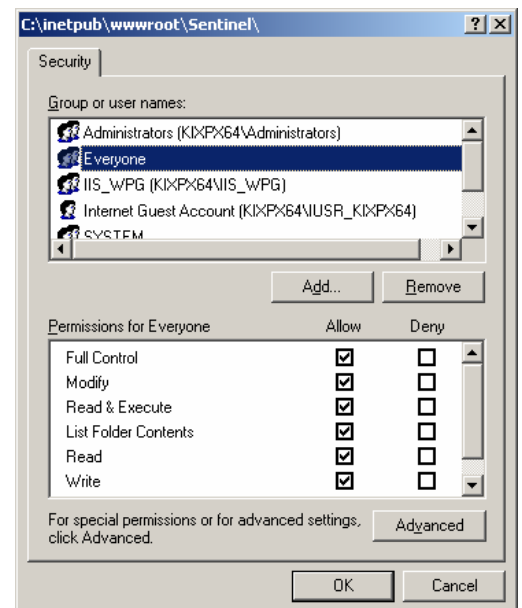
- In the Windows Security tab (if exists in your version of Windows), click **Everyone** and select the **Full Control** checkbox.



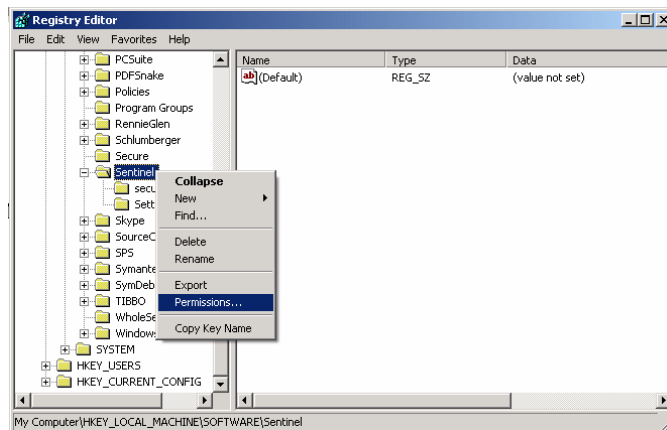
- Repeat the process (from step 12) for the file **Sentinel.Idb**.
- In the IIS Manager, expand the master server node (the Servername node). Under **Web Sites** → **Default Web Site**, right-click **Sentinel** and select **Permissions**.



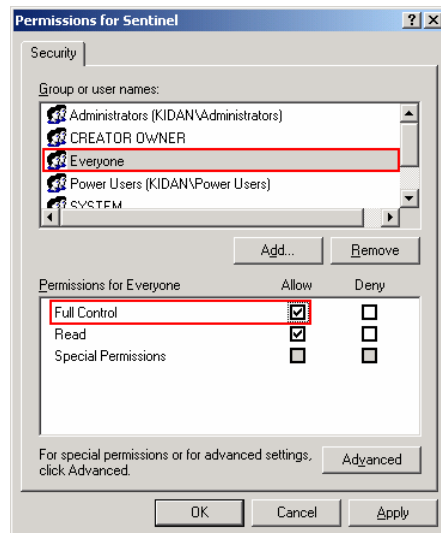
- Click **Everyone** and select **Full Control** (under the Allow column).



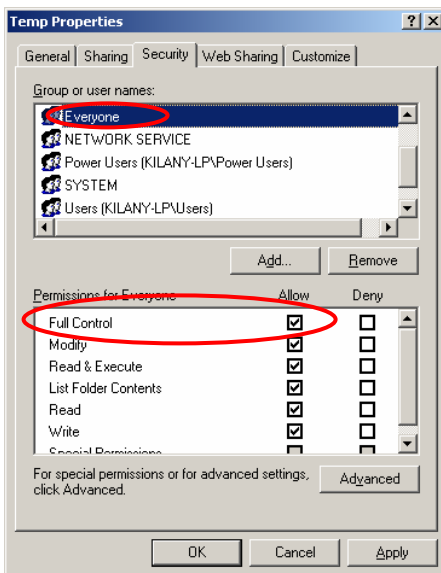
19. Start the Registry Editor (Start → Run and type the command **REGEDIT**). Right-click the Registry key **HKEY_LOCAL_MACHINE\SOFTWARE\Sentinel** and select **Permissions**.



20. Allow all users (**Everyone**) Full Control over this Registry key.



21. Right-click the Windows temporary directory (usually **C:\Windows\Temp**) and select **Properties**.
22. In the Security tab, select **Everyone** and select **Full Control** (under the Allow heading).



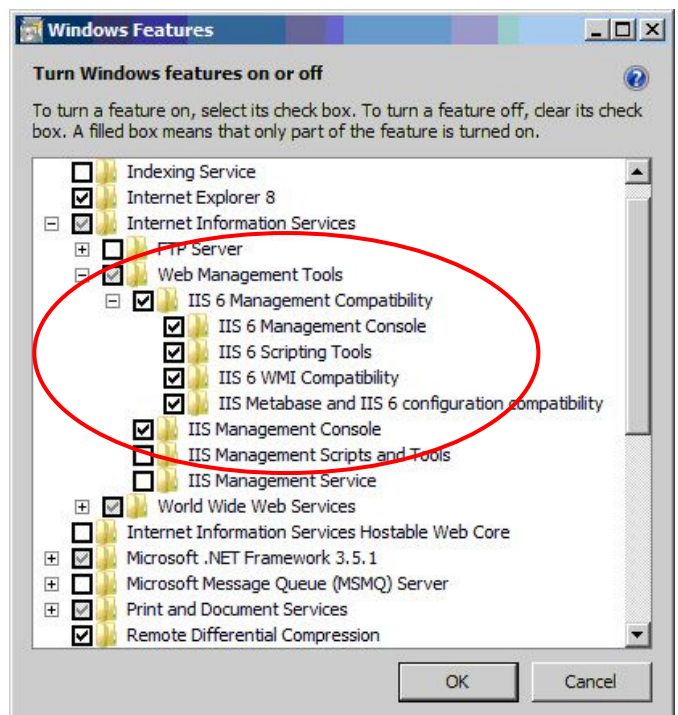
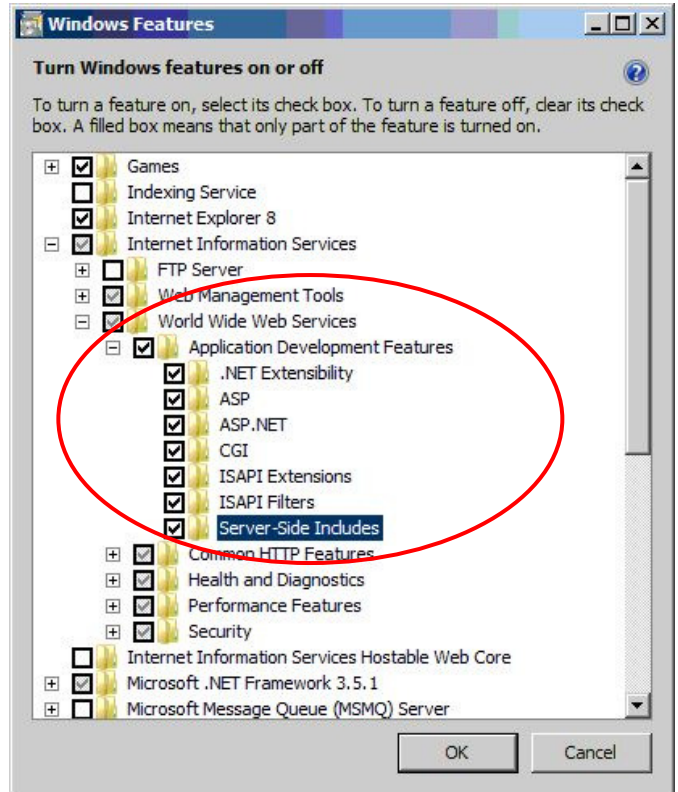
You can now proceed to *Checking the Installation* on p. 18.

Installing on Windows 7

When installing Sentinel on Windows 7, there are certain Windows settings and permissions that you must set manually before and after installing the Sentinel software.

Part 1: Set Windows permissions.

23. Add the IIS service (Control Panel → Programs and Features → Turn Windows features on or off).
24. Locate **Internet Information Services** in the list and expand it.
25. Make sure that all the checkboxes under **Application Development Features** are selected.
26. Expand **Web Management Tools** and make sure that all the checkboxes under **IIS 6 Management Compatibility** are selected.



- Under **World Wide Web Services**, expand **Security** and make sure that **Windows Authentication** is selected.

! .Net Framework 2.0 comes with Windows 7 and does not need to be installed.

- Click **OK** to close the Windows Features dialog box.

Part 2: Install the Sentinel software.

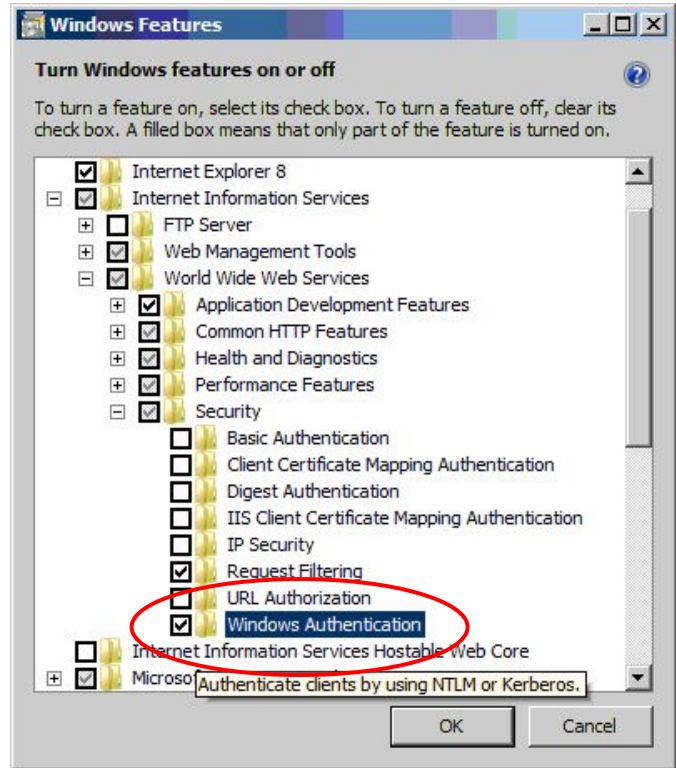
- Run **SETUP.EXE** from the Sentinel installation directory or CD-ROM.
- Follow the directions on screen. Use the default directories during the installation process

Part 3: Configure Windows 7 for Sentinel.

- Under IIS, set permissions for the Sentinel website at **Full Control** for all users (**Everyone**).
- Select **Application Pools** and click **DefaultAppPool**. Click **Edit Application Pool** (under **Actions** on the right side of the screen).

The **Edit Application Pool** dialog box appears.

- Set the .NET Framework version to **2.0** and set **Managed pipeline mode** to **Classic** and click **OK**.

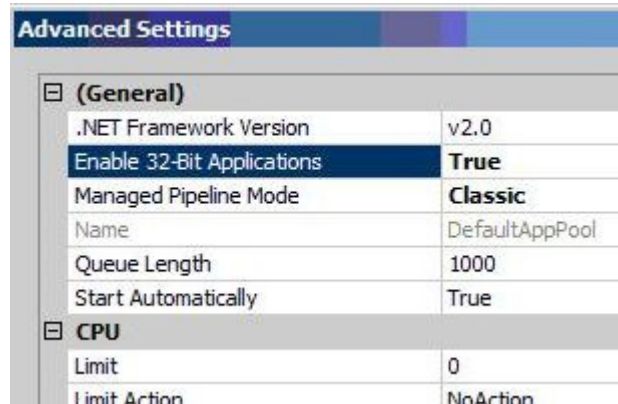
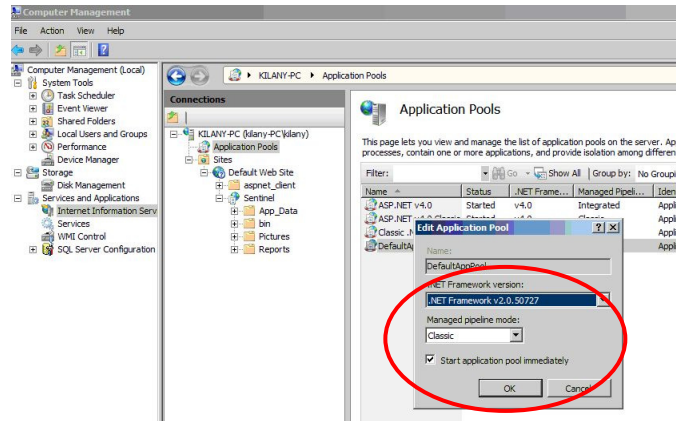


- Under **Actions** on the right side of the screen, click **Advanced Settings**.

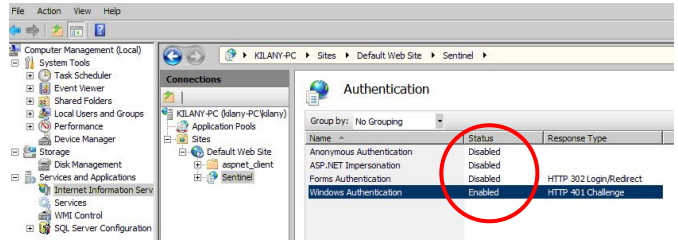
The **Advanced Settings** dialog box appears.

- Set **Enable 32-Bit Applications** to **True**.

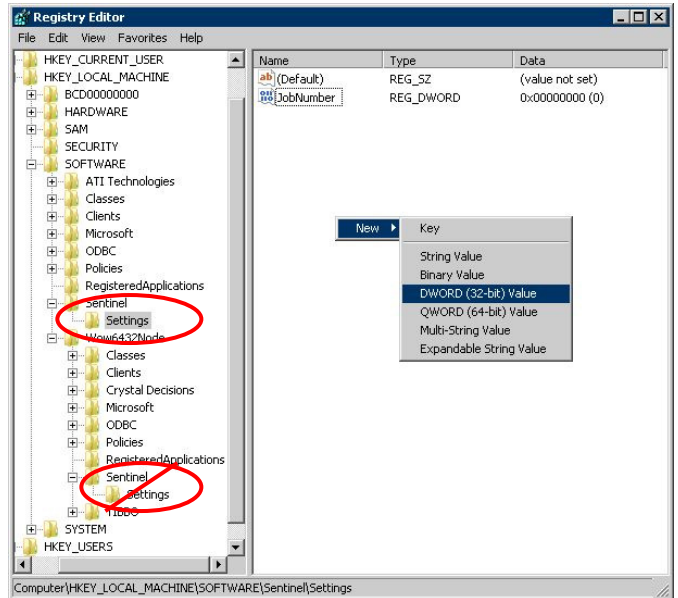
! This is only needed if the operating system is 64-bit.



6. Under IIS → Default Web Site → Sentinel → Authentication, make sure that only **Windows Authentication** is **Enabled** and that all the rest of the settings are **Disabled**.



7. Add permissions to the Sentinel key in the Windows Registry (HKEY_LOCAL_MACHINE\SOFTWARE\Sentinel).
- In 32-bit systems, this key is created automatically.
 - In 64-bit systems, you must create the key manually (right-click HKEY_LOCAL_MACHINE\SOFTWARE and select New → Key).

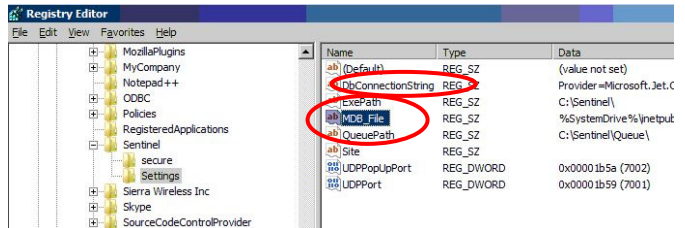


Right-click this key, select New → DWORD (32-bit) Value, and give it the name **JobNumber**.

Right-click Settings and select **Permissions**. Set permissions for all users (**Everyone**) to **Full Control** for this key.

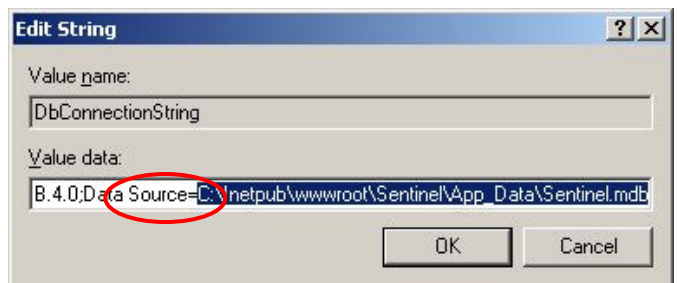
! If you are on a 64-bit system, the key you need is the Sentinel key directly under the SOFTWARE key, **not** the one under Wow6432Node.

8. Correct the full path of the file Sentinel.mdb. If you used the default directories when installing Sentinel, the file should be at C:\inetpub\wwwroot\Sentinel\App_Data



Windows 7 may corrupt the path within several internal settings. Correct the path as follows:

- In the Windows Registry, expand HKEY_LOCAL_MACHINE and locate Sentinel. Expand Sentinel and click Settings.
- Right-click **DbConnectionString** to open the Edit String dialog box. Change the path (everything after "Source=") to **C:\inetpub\wwwroot\Sentinel\App_Data\Sentinel.mdb**
- Right-click **MDB_File** and do the same thing and close Regedit.



- d) Open the file `C:\Inetpub\wwwroot\Sentinel\web.config` in Notepad. Search for `Sentinel.mdb`. The path may start with `%` or `|Datadirectory|`. Replace it with the correct path: `C:\Inetpub\wwwroot\Sentinel\App_Data\Sentinel.mdb`

You can now proceed to *Checking the Installation* on p. 18.

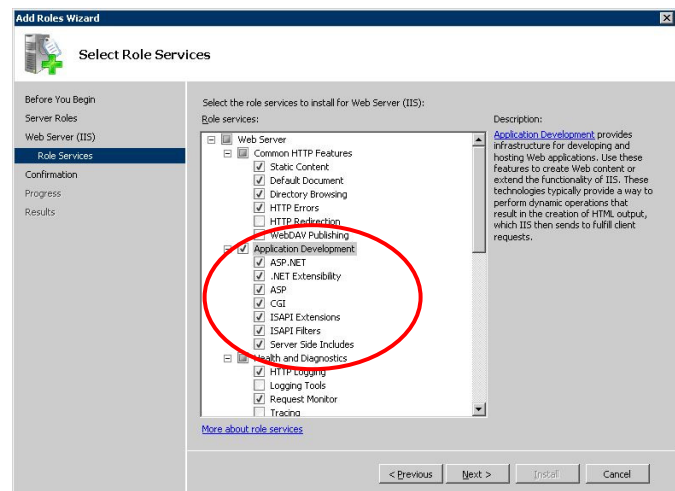
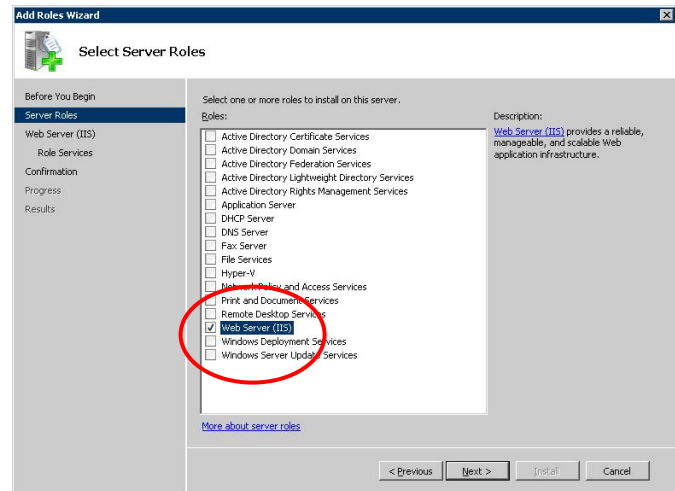
Installing on Windows Server 2008

In Windows Server 2008, *workloads* are general server functions, such as a database server or an application server. *Roles* are very specific things that the server has to do, such as acting as a print server. Most of the tools needed to define and manage the server have been bundled into a single tool—the Server Manager. To learn more about working with the Server Manager, see [Microsoft's TechNet blog](#).

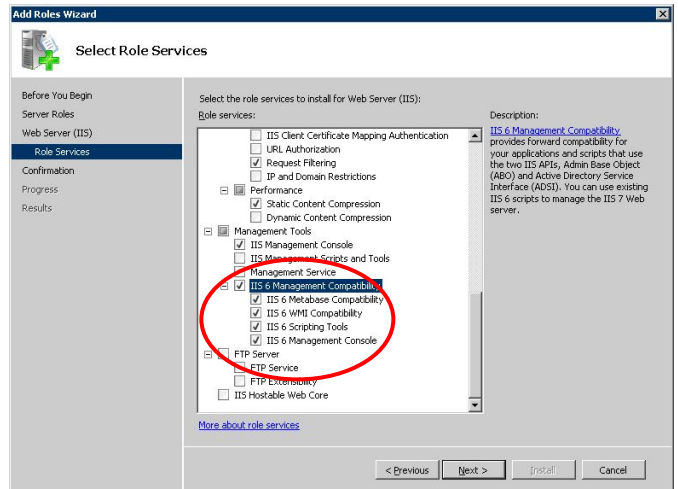
To run Sentinel on a Windows Server 2008, you need to define the correct *workload role* for Sentinel as follows:

Part 1: Create the role.

1. Open the Server Manager.
2. Right-click **Roles** and select **Add Role**.
This starts the Add Roles Wizard.
3. Select **Web Server (IIS)**.
4. Click **Role Services** and select **Application Development** and all of its sub-options.

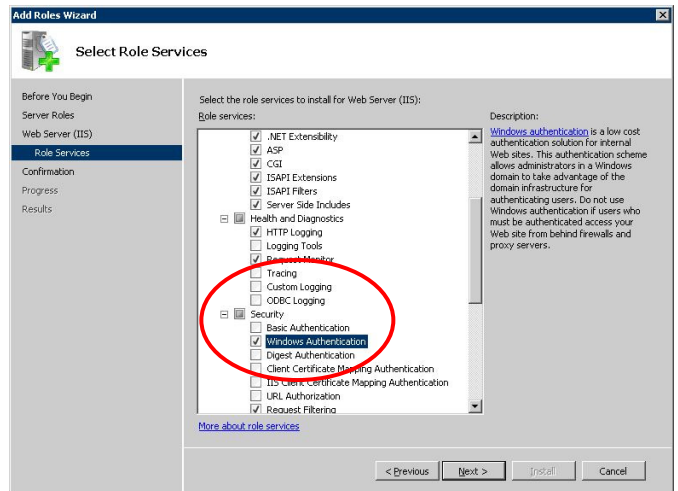


5. Select **IIS 6 Management Compatibility** and all of its sub-options.



6. Under **Security**, select **Windows Authentication**.

! .Net Framework 2.0 is included in the Windows Server 2008 operating system, so there is no need to install it.

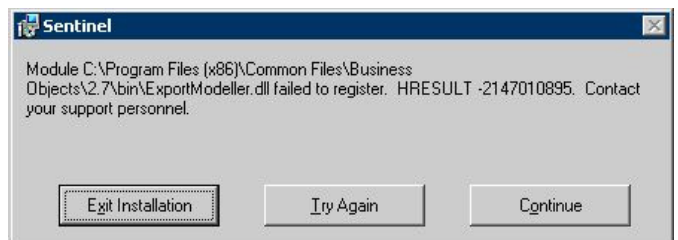


Part 2: Install the Sentinel software.

1. Run Setup.exe from the Sentinel CD-ROM or installation drive to install the Sentinel software.

If the this error occurs during installation, click **Continue** and after installation, proceed with *Part 3: Configure Windows Server 2008 for Sentinel*.

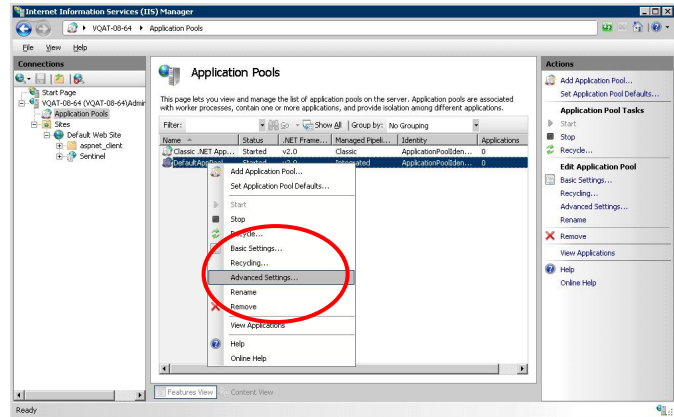
2. If the error does not occur, complete the installation, then skip to *Part 4: Correct the Registry entries*.



Part 3: Configure Windows Server 2008 for Sentinel.

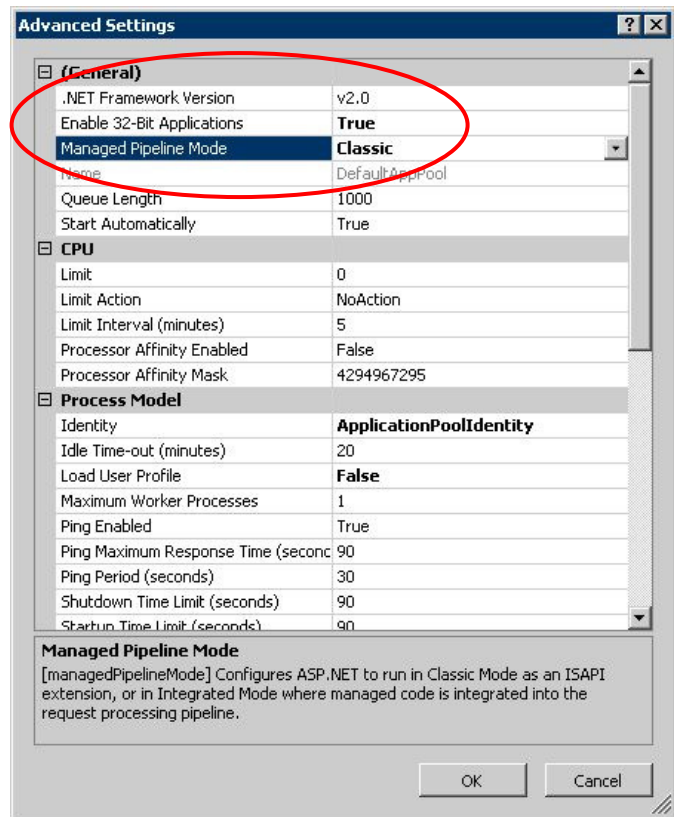
1. Open the IIS Manager. Under Application Pools, right-click **DefaultAppPool**, and select **Advanced Settings**.

This opens the Advanced Settings dialog box.



2. Set these options:
 - .NET Framework Version: v2.0
 - Enable 32-Bit Applications: True (this is only needed if you are running the 64-bit version of Windows Server 2008).
 - Managed Pipeline Mode: Classic
3. Click **OK** to save the changes and close the Advanced Settings dialog box.

This returns you to the main IIS Manager screen.

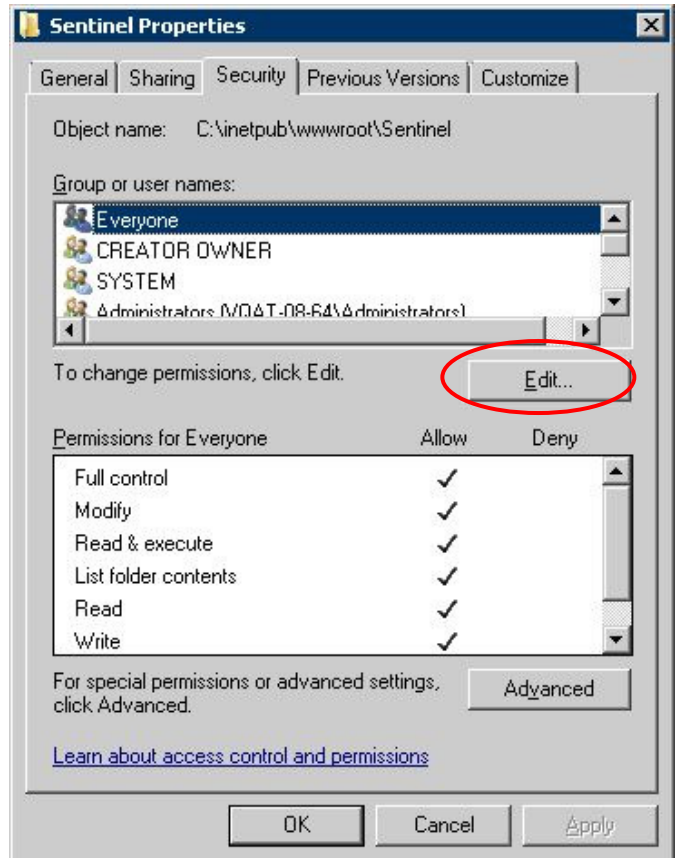


- Under Sites → Default Web Site, right-click **Sentinel** and select **Edit Permissions**.

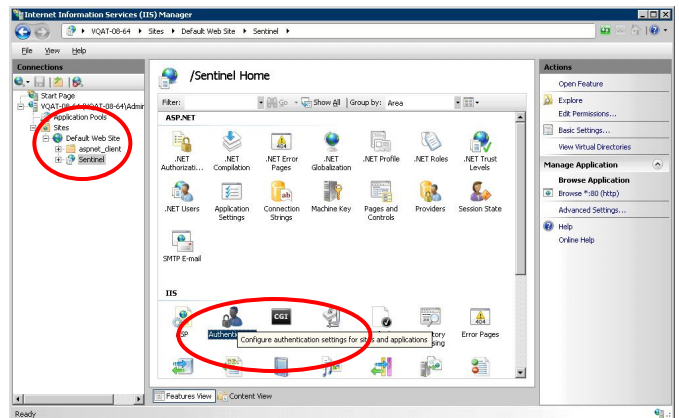
This opens the Sentinel Properties dialog box.

- Select the Security tab.
- Click **Edit** and set permissions for all users (**Everyone**) to **Full control**.
- Click **OK** to save the permissions and close the Sentinel Properties dialog box.

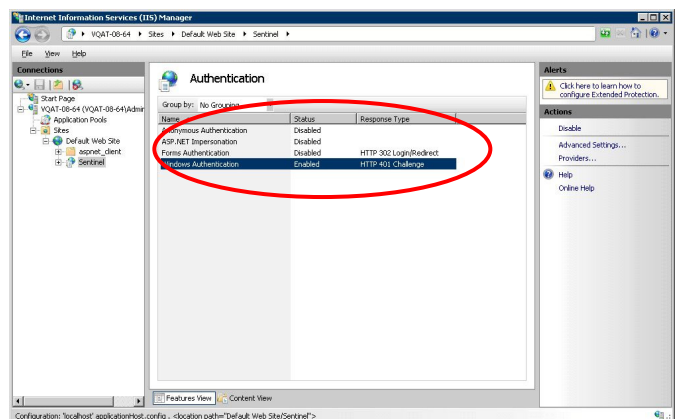
This returns you to the main IIS Manager screen.



- Under Sites, select **Sentinel**. Double-click the **Authentication** icon.



- Make sure that only **Windows Authentication** is enabled; all other authentication methods must be disabled.

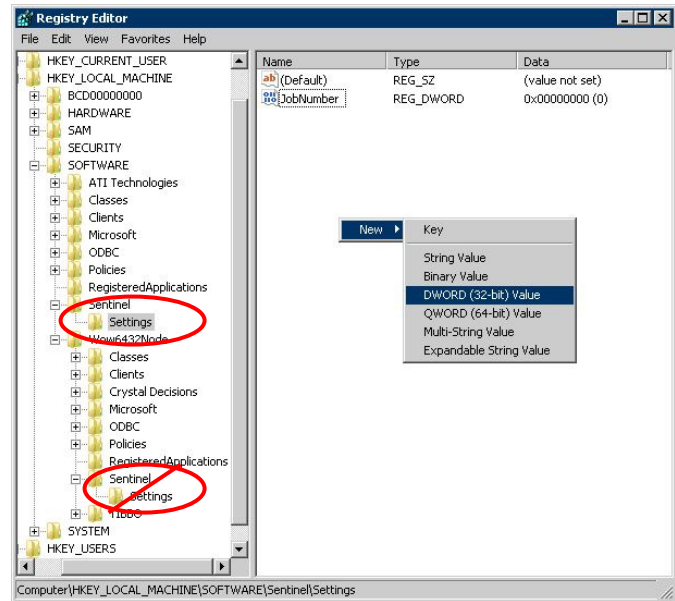


Part 4: Correct the Registry entries.

1. Add permissions to the Sentinel key in the Windows Registry (HKEY_LOCAL_MACHINE\SOFTWARE\Sentinel).
 - In 32-bit systems, this key is created automatically.
 - In 64-bit systems, you must create the key manually (right-click HKEY_LOCAL_MACHINE\SOFTWARE and select New → Key).

Right-click this key, select New → DWORD (32-bit) Value, and give it the name **JobNumber**.

Right-click Settings and select **Permissions**. Set permissions for all users (**Everyone**) to **Full Control** for this key.

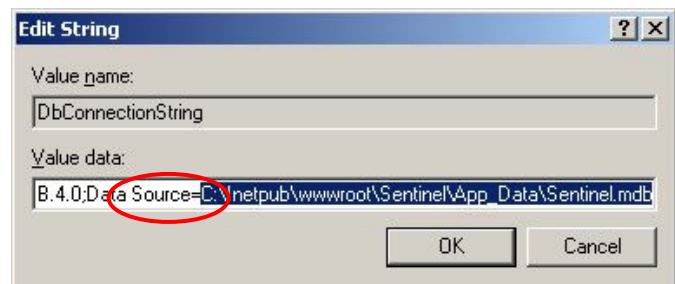
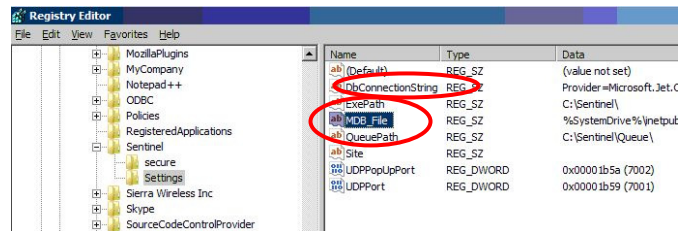


If you are on a 64-bit system, the key you need is the Sentinel key directly under the SOFTWARE key, **not** the one under Wow6432Node.

2. Correct the full path of the file Sentinel.mdb. If you used the default directories when installing Sentinel, the file should be at C:\Inetpub\wwwroot\Sentinel\App_Data

Windows 7 may corrupt the path within several internal settings. Correct the path as follows:

- a) In the Windows Registry, expand HKEY_LOCAL_MACHINE and locate Sentinel. Expand Sentinel and click Settings.
- b) Right-click **DbConnectionString** to open the Edit String dialog box. Change the path (everything after "Source=") to **C:\Inetpub\wwwroot\Sentinel\App_Data\Sentinel.mdb**
- c) Right-click **MDB_File** and do the same thing and close Regedit.
- d) Open the file C:\Inetpub\wwwroot\Sentinel\web.config in Notepad. Search for **Sentinel.mdb**. The path may start with % or [Datadirectory]. Replace it with the correct path: **C:\Inetpub\wwwroot\Sentinel\App_Data\Sentinel.mdb**



You can now proceed to *Checking the Installation* on p. 18.

Installing on x64 Platforms

On x64 platforms (64-bit operating systems), Sentinel can't work with an Access database. This limitation is because there is no Microsoft Jet 4.0 OLE DB Provider for the ODBC connection to the Access database under x64 platforms. (For details, refer to Microsoft's explanation at <http://support.microsoft.com/kb/957570>.)

This limitation means that if you want to install the Sentinel database on a 64-bit platform, you must use an SQL server for the Sentinel database. If you don't have a license for a standard SQL server database, you can use the Microsoft SQL Express 2008 database (prior versions of the SQL express don't support x64 OS).

1. Before installing Sentinel on an x64 OS with SQL Express 2008, you must install the following software:
 - Internet Information Services (IIS)
 - .Net Framework 2.0 SP2 for x64
 - Windows Installer 4.5
 - .Net Framework 3.5 SP1 for x64
 - Windows Power Shell 1.0
 - Microsoft SQL Server Express 2008 for x64
 - Crystal Reports x64
2. After installing all of these, install Sentinel as described in *Installing Sentinel Server Software on Windows Server 2003* on p. 3.
3. After installing Sentinel, proceed to *Checking the Installation* on p. 18

Registry Permissions in Windows 2000/XP

The Sentinel installation requires you to change the permissions of some Registry entries, and enable **Everyone** to read/write to it. The reason is that the last job number is stored in the Registry. Setting permissions is different in Windows 2000/XP than in Windows 2003.

To edit the Registry permissions in Windows 2000 or Windows XP:

1. Press **Start** → **Run**, and then type **regedt32**.
2. Go to **HKEY_LOCAL_MACHINE\SOFTWARE\Sentinel**.
3. Access Permissions:
 - For Windows XP, from the Edit menu, select **Permissions**.
 - For Windows 2000, from the Security menu, select **Permissions**.
4. Verify that **Everyone** appears in the list. **If not, skip to step 5.** If **Everyone** appears:
 - a) Select **Everyone**, and then select the **Full Control** and **Read** checkboxes in the Allow column.
 - b) Click **Apply** and **OK**.
 - c) Exit the Registry editor and restart your computer.
5. If **Everyone** doesn't appear in the list, proceed as follows:
 - a) Click **Add**.
 - b) For Windows XP: in the **Enter the object names** box, type **Everyone**.
For Windows 2000: in the **Look in** box, select the local network.

- c) For Windows XP: click **Check Names**, and wait until **Everyone** is underlined. For Windows 2000, select **Everyone** and click **Add**.
- d) Click **OK**.
- e) Select **Everyone**, and then select the **Full Control** and **Read** checkboxes in the Allow column.
- f) Click **Apply** and **OK**.
- g) Exit the Registry editor and restart your computer.

Checking the Installation

Once Sentinel is installed, verify that it is running.

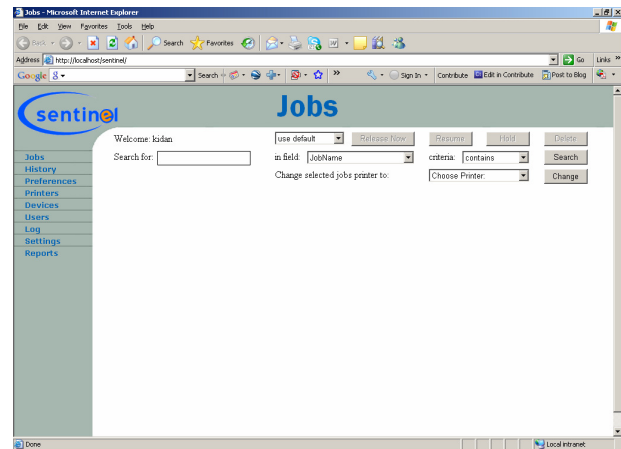
1. Select **Start → Programs → Sentinel → Web Sentinel**.
You can also go to **http://localhost/Sentinel** in your Web browser.

If you see this main screen, congratulations! Sentinel is up and running!



It may take up to 30 seconds to appear.

2. If the Sentinel main screen doesn't appear, see *Troubleshooting* on p. 61.



Configuring the Firewall for Sentinel

Some operating systems, such as Windows XP, have built-in firewall software that blocks Sentinel's communication. If a firewall is installed on the server, it must be configured properly before use. If you are planning on using the Sentinel popup feature on user workstations, the firewall on those PCs must be configured, as well.

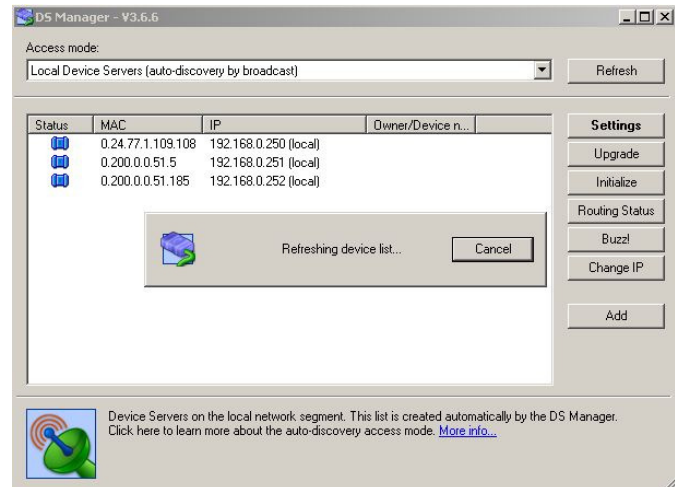
The server and clients (workstations and devices) needs ports 7001/7002 UDP/TCP open for correct communication.

To connect to the Web server from a remote machine, you must also open the IIS server port (usually 80/TCP).

You can automate the port-opening process with a provided script, Firewall.bat, located in the installation directory (default **C:\Sentinel**).

- Configure device controllers with the DS Manager application (**Start → Programs → Sentinel → DS Manager**).

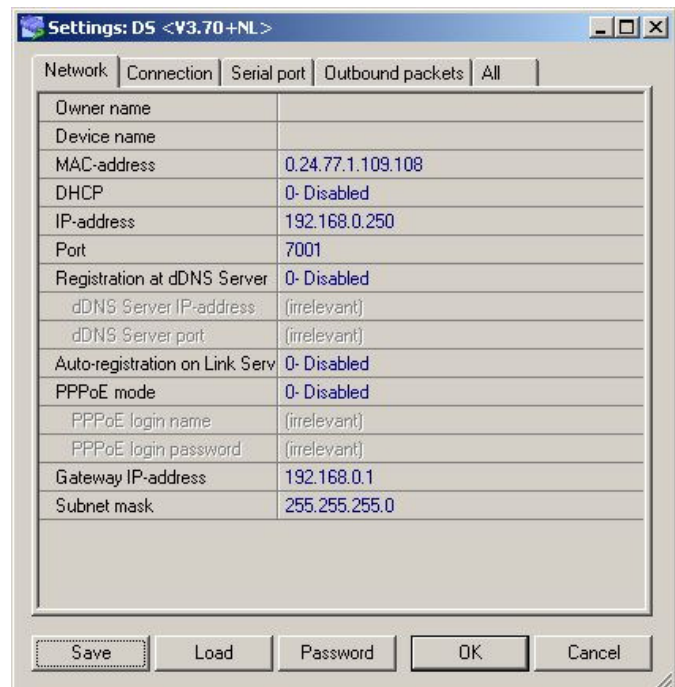
When launched, the DS Manager automatically searches for all connected device controllers and refreshes the list.



- To change the settings of a device controller, click it on the list and click **Settings**.

The Settings dialog box appears.

For more information about the DS Manager, see http://docs.tibbo.com/soism/index.html?ds_manager.htm.

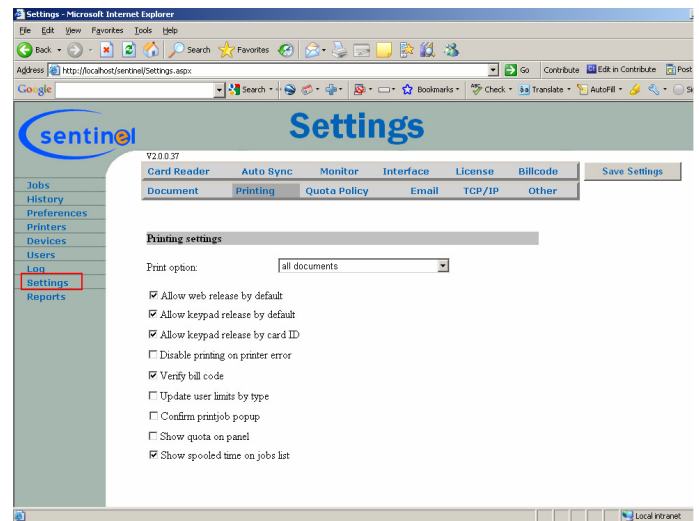


Configuring the Sentinel Server

This section describes the Settings screens in the Sentinel server. These are the screens which are usually configured immediately after installing Sentinel. Other screens are described with their specific procedures (see *Basic Functions* on p. 32).

Configuration Guidelines

1. Make sure that you are signed on as a local administrator of the computer on which Sentinel is installed.
2. Log on to Sentinel (**Start → Programs → Sentinel → Web Sentinel** or go to **http://localhost/Sentinel** in your browser).
3. Select **Settings** from the left-hand menu. If the menu only contains **Jobs** and **History**, the system didn't identify you as an administrator.
4. Configuration settings are grouped by tabs (explained below).
5. After making changes, click **Save Settings**.



Card Reader

These settings relate to the decoding of the card number read by the RFID reader, plus other options related to timeouts of the messages sent from the server to the device.

Parameter	Explanation
Timeouts	The period (in seconds) that the device will display messages on the screen before it will reset back to the default Enter Code or Place Card message.
• Information	Time period to display information messages (such as no jobs waiting for user).
• Error	Time period to display error messages (such as unidentified card was used).
• Selection	Time period to display the selection of print jobs to be released when the print option for the user is select by keypad .
• Copy	Time period that the device will open the copier and allow the user to make copies. This timeout renews after each copy is made.

Parameter	Explanation
Card Number Conversion	<p>This causes Sentinel to convert the card number read by the RFID reader at the device from one representation to another. This is used to verify that the correct card number is matched against the number in the User Table.</p> <p>These settings are particularly useful for large organizations that already use magnetic cards for employees (such as door access, time card machines, etc.). Since many of these devices interpret card data differently (as Hex, binary, etc.), and since you certainly don't want to have to manually add each user's card ID to Sentinel's database, these settings are needed to allow you to correctly interpret existing card data.</p>
<ul style="list-style-type: none"> • Use ISO 7Bit 	This causes Sentinel to convert the information arriving from the card using the ISO 7Bit protocol. This is usually used only with magnetic Track 1 cards.
<ul style="list-style-type: none"> • Convert Decimal to Hex 	Converts the card number from decimal to hexadecimal representation.
<ul style="list-style-type: none"> • Read characters from card (Right) 	Takes only the X rightmost characters of the card number.
<ul style="list-style-type: none"> • Read characters from card (Left) 	Takes only the X leftmost characters of the card number.
<ul style="list-style-type: none"> • Convert Hex to Decimal. 	Converts the card number from hexadecimal to decimal representation.
<ul style="list-style-type: none"> • Ignore card leading zero 	Ignores all leading zeros read by the card reader.
<ul style="list-style-type: none"> • Increment constant number 	Mathematically adds the card number that was read to this number.
<ul style="list-style-type: none"> • Complete Card ID to [X] digits 	Fills in leading zeros to the card number received by the server to the selected number of digits.

Example of card number conversion: In this scenario, none of the Card Number Conversion parameters are selected, and that a user's ID card has 15 digits. To match the card numbers with the existing numbers in the active directory, Sentinel needs only the middle nine digits. We can set **Read characters from card (Right)** to 12 and **Read characters from card (Left)** to 9. This leaves us with only the middle nine characters of the card.

Here is the original card number:	123456789012345
Sentinel reads the first 12 characters starting at the right...	456789012345
...and then reads the first 9 starting from the left...	456789012

Document

These settings determine how long unprinted jobs and job history data remain. They also contain timeouts and other settings.

Parameter	Explanation
<ul style="list-style-type: none">• Delete unprinted jobs after [X] hours	How long Sentinel keeps a print job in its queue when a print request is made by a user but not released. After this period of time, the job is cleared but an entry is made in the log.
<ul style="list-style-type: none">• Clear history after [X] days	How long Sentinel keeps print jobs on the History screen.
<ul style="list-style-type: none">• Clear log after [X] days	How long Sentinel keeps entries in the log.
<ul style="list-style-type: none">• Device active from time• Device active to time	Defines the default activity time for all devices. If empty, the devices always remain active. To set an activity time, enter the desired <i>from</i> and <i>to</i> times as HH:MM using a 24-hour syntax. For example, to set the default activity time from 8AM to 5:30PM, enter 08:00 and 17:30 , respectively.
<ul style="list-style-type: none">• AutoPrint TimeOut	<p>This is only relevant when AutoPrint is allowed on a device (usually a virtual device "0.0.0.0"), or if a user is allowed to print automatically (AutoPrint enabled for that user in Settings).</p> <p>Normally, when a user wants to print, the print job request is picked up by the Sentinel server and sent to the database. When the user is correctly identified at the device controller, the server retrieves the print job from the database and releases it.</p> <p>AutoPrint jobs, however, bypass the device controller. The server sends the print job request to the database and immediately tries to release it.</p> <p>If the Sentinel database is on the same computer as the Sentinel server, there is no problem. But if the database and server are on two computers that are far apart, the database may not have time to receive the information about the print job that the server is already trying to release.</p> <p>To avoid this problem, use this parameter to create a delay (for example, three seconds). This allows the database time to receive print job information before the server releases the job.</p>
<ul style="list-style-type: none">• SNMP TimeOut	<p>This is only relevant when SNMP Count (see p. 32) is selected on a device.</p> <p>SNMP continually monitors printer status, completion of jobs, number of pages printed, etc. Since Sentinel adds an additional communication chain to the process (<i>print request</i> → <i>Sentinel server</i> → <i>Sentinel database</i>, then <i>user recognition at device controller</i> → <i>Sentinel server</i> → <i>Sentinel database</i> → <i>release job</i>), there can be a delay between actual printing activity and what is in the Sentinel database. For example, if a user sends a 100 page printout, the job is recorded in the Sentinel database. But the user decides to cancel the job physically at the printer after only three pages were printed. From Sentinel's perspective, 100 pages were printed.</p> <p>To avoid this problem, use this parameter to create a delay (for example, two seconds) after the SNMP status request. This is the amount of time the server will wait before checking the printer to see how many pages were actually printed.</p>

Auto Sync

The Auto Sync settings control options related to synchronizing the User Table (Sentinel's own internal database of users) with external resources, such as the AD (Active Directory) or external SQL databases.

Rather than having to manually enter information for each user, you can easily synchronize with existing information. This is particularly useful as many organizations maintain detailed user information in their Windows AD.

For most activities, synchronization is one way: from the LDAP to the Sentinel database, particularly when adding users to the Sentinel database. Bidirectional synchronization usually occurs once a day when a script is run. For example, if a user has been deleted from LDAP, the script deletes them from the Sentinel database as well.



Caution!

Sentinel is designed specifically to work with LDAP settings. While you can synchronize the Sentinel database with an SQL database, this may require some trial and error to get the correct results. SPS and your Sentinel vendor are not responsible for the results.

To use any of these settings, first select the **Enable** checkbox, then one of the four Auto Sync options:

Parameter	Explanation
Use LDAP to get users from active directory	This option causes Sentinel to connect to the Active Directory (AD) using LDAP for each new user printing through the system. The user's card number is retrieved from a specific field in the AD. To use this feature, you must complete the other parameters within this group (Domain Name, Card ID Field Name, etc.).
<ul style="list-style-type: none">• Domain Name	The domain name that has permission to access the AD.
<ul style="list-style-type: none">• Card ID Field Name	You can use any LDAP field; for example, if your organization doesn't use pagers, the Pager field (from AD) can be used as a Card ID field. You would type Pager here. If Use LADP Server to get users from active directory is selected, this field is the minimal required setting.
<ul style="list-style-type: none">• AD User	The username with permission to access the AD.
<ul style="list-style-type: none">• AD Password	The password associated with this username.
<ul style="list-style-type: none">• From LDAP Field and To Field	You can synchronize more AD fields with fields from the User Table in Sentinel. For example, you can synchronize the Department field of the user in the AD with the field Department in Sentinel. To do so, specify the LDAP field to use in the From text box, and the Sentinel field to which it will be mapped in the To text box.
Use SQL Server to get users	If selected, Sentinel compares the username retrieved from the metadata of the print job with the one specified in User Field Name . If they match, the data in Card ID, First Name, and Last Name is updated in the internal User Table SQL Server.



Caution!

Using SQL data may require some trial and error to get the desired results.

Parameter	Explanation
<ul style="list-style-type: none"> User Field Name 	If Use SQL Server to get users is selected, this is the minimal required field. This is name of the field in the SQL database that contains the username used for matching.
<ul style="list-style-type: none"> Card ID Field Name 	The name of the field in the SQL database that contains data to be mapped to the card ID.
<ul style="list-style-type: none"> First Name Field 	The name of the field in the SQL database that contains data to be mapped to the user's first name.
<ul style="list-style-type: none"> Last Name Field 	The name of the field in the SQL database that contains data to be mapped to the user's last name.
<ul style="list-style-type: none"> Table Field Name 	The name of the table in which the users are listed.
<ul style="list-style-type: none"> Connection String 	The connection string to the SQL server.
Use complex sync (AD, SQL) to get users	This allows you to make more complex synchronizations with a call to an external DLL. For details and assistance, contact your Sentinel vendor.
Use random Sync to get users and Card IDs	If selected, each new user printing request is added automatically to the User Table, and a random card ID is issued to each user. This is useful when Sentinel is installed without any physical devices (with virtual 0.0.0.0 devices intended only for monitoring purposes without physical release).

Printing


These settings determine how printing is handled in general (not on a specific device). Settings for a specific device override the same settings here.

Parameter	Explanation
<ul style="list-style-type: none"> Print Option 	<p>If several print jobs are waiting for the user, you can select one of the following options:</p> <ul style="list-style-type: none"> All Documents: The user receives all of requested jobs at once. Last Document: Each time a user card is swiped, the user receives the last job requested. The order is LIFO (last in, first out). Select by Keypad: After a card swipe, if there are more then two jobs waiting for the user, they appear on the device's LCD and the user can select which jobs to release. If there is just one print job waiting for the user, it is printed automatically.
<ul style="list-style-type: none"> Allow Web release by default 	If selected, users are able to release print jobs from the Web interface.
<ul style="list-style-type: none"> Allow keypad release by default 	If selected, users are able to release print jobs by entering their keypad code on the device controller.
<ul style="list-style-type: none"> Allow keypad release by card ID 	If selected, users are able to release print jobs by entering their card ID number (not keypad code) on the device controller.
<ul style="list-style-type: none"> Disable printing on printer error 	If selected, the Sentinel server checks the status of the destination printer before releasing print jobs to it. If the printer status is error, then the print jobs are not released.

Parameter	Explanation
<ul style="list-style-type: none"> Verify Billing Code 	If selected, only billing codes that exist in the Billing Code Table are allowed; otherwise, any billing code, even if it doesn't exist yet, is accepted. This option is applicable when using a popup to select a billing code.
<ul style="list-style-type: none"> Update user limits by type 	If selected, all limits are updated at the same time. For example, if a user printed one B/W page, all limits are decreased by 1, not just the B/W limit.
<ul style="list-style-type: none"> Confirm print job popup 	When using a popup to select a billing code, this causes a second (confirmation) popup to appear after the initial popup selection. This allows the user to confirm the billing code.
<ul style="list-style-type: none"> Show quota on panel 	If selected, after user identification, the user's quota (and remaining pages) is shown on the device's display.
<ul style="list-style-type: none"> Show spooled time on job list 	When using the Select by keypad print option, all print jobs appear on the device's display and the user can select which print jobs to release. On the device controller with buttons (that is, <i>not</i> the touch screen version), print jobs are described with only 16 characters. This parameter, if selected, uses the first 5 characters of this description to display the time the print job was spooled.

Monitor

The screen contains settings that determine how Sentinel monitors devices, queues, and the overall system.

Parameter	Explanation
<ul style="list-style-type: none"> Monitor jobs on printers with error status 	If selected, Sentinel monitors printers with error status, looking for print jobs that are not spooled and therefore are not submitted yet to Sentinel. This checkbox causes those print jobs to be submitted despite the printer error status.
<ul style="list-style-type: none"> Monitor and activate the Sentinel service 	<p>If selected, Sentinel starts another process, SNTMON.EXE, which sends a UDP message to the standard Sentinel process (COMTCP.EXE) every several seconds. If the standard process doesn't response to three consecutive messages, the monitor process kills the standard process and restarts it.</p> <p>If this checkbox is selected, you must specify the IP address of the Sentinel server.</p> <div style="background-color: #f0f0f0; padding: 10px; margin-top: 10px;"> <p> This field is not kept in the Sentinel database, but in the file C:\Sentinel\Service.ini on the local server that runs the IIS. This is because there may be several Sentinel servers writing to the same database. If the IIS is not installed on the same server that runs the Sentinel service, you can edit this file manually and add the IP address of the server on each server separately.</p> </div>
<ul style="list-style-type: none"> IP Address 	The IP address of the Sentinel server (required if using Monitor and activate the Sentinel service).

Quota Policy


Quota policy allows you to increment or set the quota limit of each page type (B/W, color, and copies) automatically at defined intervals. You can define several quota policies, and for each user select a different policy.

Parameter	Explanation
<ul style="list-style-type: none">Default Quota Policy	The quota policy automatically assigned to new users.
<ul style="list-style-type: none">(policy to edit/delete)	Select the policy from the list. Click Add Policy to create a new policy. <ul style="list-style-type: none">For each policy, select the day of the month and the frequency (every X months that the policy rules are to be performed).For each policy and page type, select the number of pages the system will increment, or specify a set amount for the quota.

Interface

These settings refer to how information appears on the Sentinel screens.

Parameter	Explanation
<ul style="list-style-type: none">Seconds before AutoRefresh (0 for never)	If selected, the Web interface refreshes automatically every X seconds.
<ul style="list-style-type: none">(policy to edit/delete)	Select the policy from the list. Click Add Policy to create a new policy. <ul style="list-style-type: none">For each policy, select the day of the month and the frequency (every X months that the policy rules are to be performed).For each policy and page type, select the number of pages the system will increment, or specify a set amount for the quota.
<ul style="list-style-type: none">Send Hebrew text	If selected, the Sentinel screen and reports will allow Hebrew characters.

 Other languages and character sets will be supported in future releases of Sentinel.

Email

These settings define how Sentinel system messages and alerts can be sent via email to the appropriate person (system or network administrator, security administrator, etc.).

Parameter	Explanation
<ul style="list-style-type: none">From Email Address	This is the email address that the messages will come from; for example, sentinel@yourcompany.com.
<ul style="list-style-type: none">Email Address	The email address of the person to receive the messages.
<ul style="list-style-type: none">SMTP Server	The SMTP server for this person's email.
Send email notification when the following event types occur	Select any combination of these events.

Parameter	Explanation
• Error	These are errors that occur in the Sentinel system (server, database, etc.).
• System Error	These are errors in Windows that affect devices in the Sentinel system.
• Security	These are Sentinel events, such as users reaching their quotas.
• Warning	These are Sentinel interface events, such as the Monitor freezing or not refreshing.
• Information	These are all normal activity events in Sentinel, such as jobs printed.

License

This screen contains your current license for Sentinel. When this license expires, you can update it by entering your new license (from your Sentinel vendor) and clicking **License Now**.

The new license appears after you reset the Sentinel service.

To confirm that the license was successfully updated, look at the Sentinel Log screen for the event that indicates that a new license code was inserted.

TCP/IP

This screen allows you to change the working communication port of the system and the LPR printing settings.

The UDP ports must be open in both directions between the server and the devices or stations running popup.



Caution!

Changing these settings may prevent the system from functioning properly.

Parameter	Explanation
• UDP port	This is the main port between the Sentinel database and the device. Normally, it is set at 7001.
• UPD Popup Port	If using the Sentinel popup feature on user workstations, you must define the port between the Sentinel database and the user workstation. This is usually 7002.
• Ignore IP after Username	When using a shared printer, LPR communication often displays a user with the IP address of the computer from which the print job was sent. To Sentinel, Bob_K and Bob_K 192.41.87.123 are not the same thing. By selecting this option, Sentinel ignores any IP address that appears after a username, and can therefore correctly enter the event in the Sentinel database.

Billing Code

The system can assign to each print job a billing code. This code can then be used to issue reports according to document “owner,” rather than by who printed the jobs.

Cluster and Other Settings

Sentinel supports clustering. To enable clustering, you must identify the cluster name in the appropriate textbox and define the following parameters.

- The Sentinel database that can be accessed from all nodes of the cluster.
- The Sentinel queue directory (by default **C:\Sentinel\Queue**) that is common to all cluster nodes.
- The Sentinel print processor, which needs to be manually added to the cluster virtual printing. (Copy the file Sentinel.dll to the proper print processor DLL folder, and add the print processor Registry keys.)

Parameter	Explanation
<ul style="list-style-type: none">• Cluster Name	Any name used to identify the cluster.
<ul style="list-style-type: none">• Application System User	<p>Sometimes, when working with a non-Windows application, print jobs arrive with the same user name. For example, when working with Oracle applications, the print jobs will always arrive as if from user APPLMGR, rather than from the correct username. This is a problem when trying to release the print job, since Sentinel doesn't know which user actually sent the job.</p> <p>To work around this problem, some applications allow the implementers of the application to change the job name:</p> <ol style="list-style-type: none">1. Change the job name to username@jobname.2. Enter the special application username (for example, APPLMGR) in the textbox <p>Then when Sentinel receives a job from this special username, Sentinel searches for the @ character in the username and interprets any string before @ as the real username.</p>
<ul style="list-style-type: none">• Remove symbols from user name (left)	If selected, Sentinel searches for special characters in the username. These characters are "at" (@), colon (:), underscore (_), hyphen (-), and slash (/). If Sentinel finds any of those characters, it removes everything before the character. This is useful in systems where the username arrives with a prefix; for example, APP_USERNAME becomes USERNAME.
<ul style="list-style-type: none">• Support multiple users	Select this if you have several print servers working with one database.
<ul style="list-style-type: none">• Generate Temp Card ID by External DLL	This allows you to make more complex card ID generation scenarios with a call to an external DLL. To enable this option, contact your Sentinel vendor for assistance.

Senti-Mail Scan Control

Data from scan activities within the Sentinel system (that is, from scanners connected to a Sentinel device controller) can be processed based on scripts. This is done through a utility called Senti-Mail.

When a scanned document (.PDF or .TIF file) arrives in the incoming folder, Senti-Mail looks for a file called **CurrentUser.ini** in the same folder. The .INI file is a unique script for the scan; it identifies the user whose ID card was used at the scanner and the user settings that determine what to do with the scanned file (for example, forwarded the scan to another folder or send it as an email attachment).

In addition, Connection strings, taken from Sentinel settings, determine how the scan activity is stored in the Sentinel database.

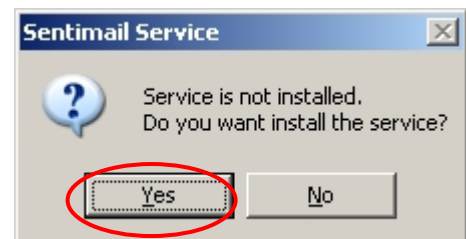
Install Senti-Mail:

1. In C:\Sentinel, locate the file **Senti-Mail_setup.msi**. Run it and follow the prompts.
2. Make sure that the scanners (or multi-function printers) are entered in Sentinel. (In the Devices screen, select the desired printer and click **Edit**. Set the Print or Copy field to **Copy** or to **Multifunction**. Make sure that **Support FTP Mail** is selected.)
3. Create an incoming folder.
4. In the incoming folder, create a subfolder for each scanner. The name of the subfolder must be exactly the same as the scanner device name as it appears in the Sentinel Devices screen.
5. Set the scanner to scan to the subfolder that matches its name. (This is done from the printer's Web application. Refer to your printer's documentation for details.)
6. In the Sentinel Users screen, click **Edit** for a user. Define either an email address (Mail) or a folder (Scan to Folder) for each user. (If both are defined, Senti-Mail will do both actions.) Do this for each user.
7. Run the Senti-Mail service (**Start → Programs → Senti-Mail → Service**). Click **Yes** to install the service.

Support FTP Mail



Edit User	
User	AB Test
AlternateUser	<input type="text"/>
Description	<input type="text" value="policy test"/>
Card ID	<input type="text" value="12345"/>
Group	<input type="text" value="test"/>
Department	<input type="text" value="Sales"/>
Organization	<input type="text" value="ABC"/>
Company	<input type="text" value="DEF"/>
Mail	<input type="text" value="ab@def.com"/>
Scan to Folder	<input type="text"/>



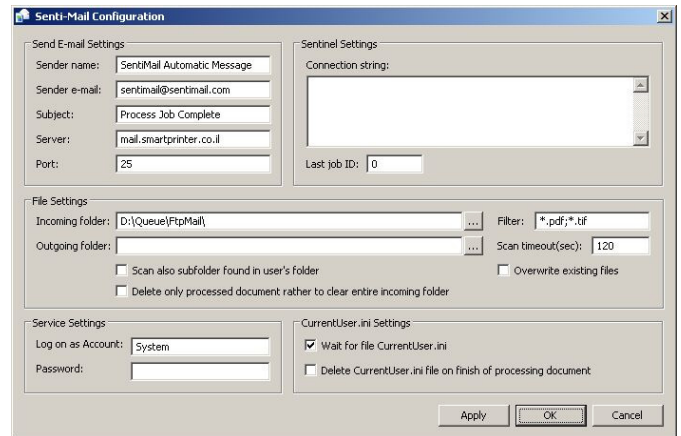
Configure Senti-Mail:

1. Select **Start → Programs → Senti-Mail → Settings**.

The Senti-Mail Configuration dialog box appears.

2. If you are using the email feature, define the following fields in **Send E-mail Settings**.

- **Sender name:** the name that appears as sender in the emails.
- **Sender e-mail:** the email address.
- **Subject:** the text to appear in the subject line of the emails.
- **Server:** the name of the mail server.
- **Port:** the fixed port of the mail server.



3. In **Sentinel Settings**, enter the connection string for the Sentinel database. This must be the same connection string defined in the Registry under the key: **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432 Node\Sentinel\secure\DbConnectionString**.

You can specify the starting number for job IDs by entering the number of the last job ID (for example, if you enter 10, the next job will be 11, and so on).

4. In **File Settings**, set:

- **Incoming folder:** This must be the name of the folder you created in step 3 of Senti-Mail installation (see p. 30).
- **Outgoing folder:** This is the folder to use as a default if nothing is specified in **CurrentUser.ini**.
- **Filter:** You can filter files (that is, specify which kinds of files are accepted). The default is to accept both .PDF and .TIF files.
- **Validation timeout:** This is the time (in seconds) that Senti-Mail will look in the incoming folder.
- **Look in second-level subfolders:** If not selected, Senti-Mail looks in the incoming folder and immediate subfolders. (Remember, each scanner has a subfolder in incoming folder.) If selected, Senti-Mail looks at three levels (the incoming folder, the immediate subfolders, and the next level of subfolders).
- **Delete processed document only:** If not selected, Senti-Mail deletes all files in the folder at the successful completion of processing. If selected, only the processed document.
- **Overwrite existing files:** If selected, a documents with the same file name as one already in the incoming folder overwrites the existing one.

5. In **Service Settings**, enter the account and password for the account used for this service. This is normally a system administration account.

6. In **CurrentUser.ini Settings**, determine how the .INI file is handled:

- **Wait for .INI file:** If selected, Senti-Mail will not proceed unless the file CurrentUser.ini is found in the incoming folder and subfolders (and second-level subfolders, if selected).
- **Delete .INI file on completion:** If selected, the file CurrentUser.ini is deleted after Senti-Mail processes the document.

7. Click **Apply** and then **OK** to close the dialog box.

Basic Functions

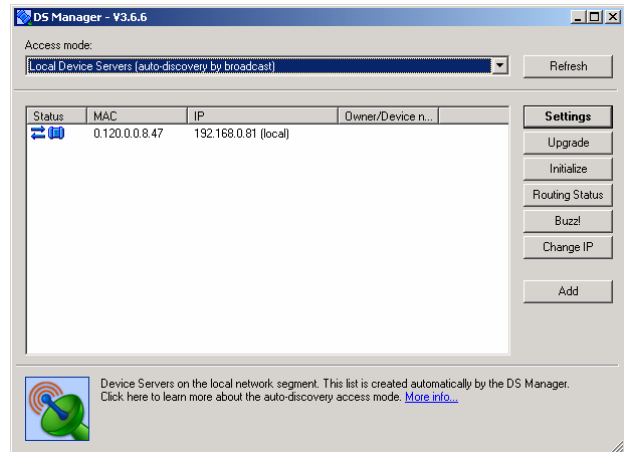
Once you have performed the initial configuration of the system, you can begin to add devices and users to the system.

Adding a New Device

Before using a new device, it must be configured properly.

1. Attach the new device to the network.
2. Select **Start → Programs → Sentinel → DS Manager**.

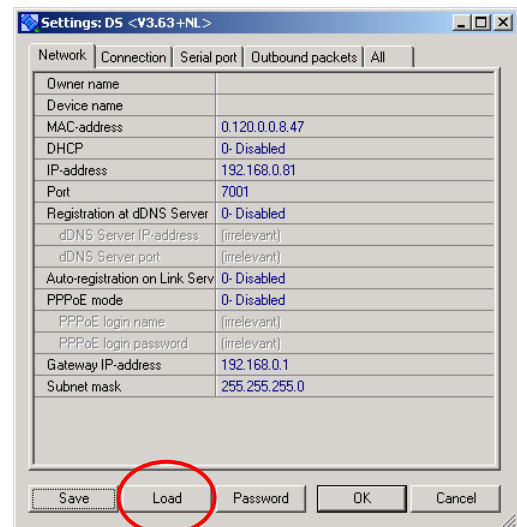
The DS Manager launches and begins looking for new devices.



3. From the device list, double-click the device you want to configure.

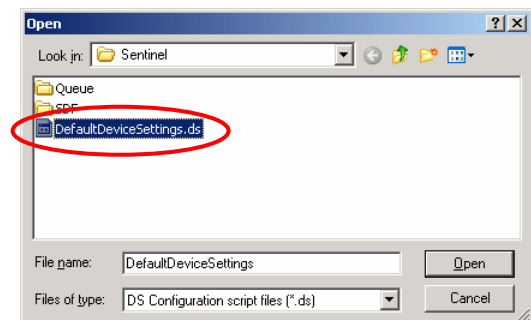
The device's settings window appears.

4. Click **Load**.



5. Select the predefined settings file from the Sentinel path.

This loads all the standard settings for the device.



6. Set up the specific definitions to match your network environment and your Sentinel system. These settings include:

- IP Address
- Gateway IP Address
- Subnet Mask
- Destination IP Address

7. Log in to Sentinel (**Start → Programs → Sentinel → Web Sentinel** or go to **http://localhost/Sentinel** in your Web browser).

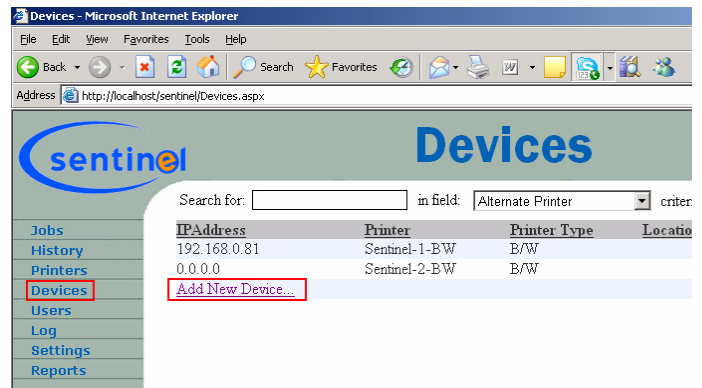
8. From the left-hand menu, click **Devices**.

9. From the list of all currently configured devices, select the device that you just added and click **Edit**.

10. To add a new device, click **Add New Device**.


This opens the Add Device screen. All parameters are described below.

11. When done with all parameters, click **Insert**.



Parameter	Explanation
• IP Address	The fixed IP address of the new device.
• Location	A short description of where the device is located (for example, by floor or room or department area).
• Description	A short description of the device (for example, "high-quality printer for marketing material").
• Site	This is usually a physical site. For example, if your organization has offices in two different cities, and both locations use the same Sentinel database.
• Print or Copy	Specify the device type: printer, copier, or a multifunction machine: <ul style="list-style-type: none"> • If the device is defined as a printer, when a successful identification is made, the waiting print job is released according to the print option defined and the user or the default print option. • If the device is defined as a copier, it requires a unique identifying name. Then, when a successful identification is made, the copier machine is opened for a predefined period of time (see Timeout Copy, below) in which the user can perform copies in the machine. When the time period ends, or after the user presses the <ESC> button at the device, the machine is locked again and the number of copied made is written to the server's database. • If the device is defined as multifunction, when a successful identification is made, the device shows a selection (usually print and copy). Specify the default value for the device.
• Printer	Select the printer from the list of printers attached to the device.

Parameter	Explanation
• Copier	If the device is attached to a copier machine that is not a printer, you must give it an identification name since it doesn't appear in the Windows printers list.
• Port Name	If you are using the SNMP option, you must verify that this textbox contains the IP address of the physical printer. Sentinel will attempt to figure out this information from the Windows port, but it is not 100% accurate. If you are not using the SNMP option, then this information is not used.
• Alternate Printer	Select an alternate printer to print jobs if the main printer is failing. (This is only for jobs that are printed automatically without the use of a card.)
• Heavy-duty Printer	If the value of Maximum Pages to Change Printer is lower than the number of pages in the current job, the job is printed on this heavy-duty printer. (This is only for jobs that are printed automatically without the use of a card.)
• Printer Type	Select the type of the printer (B&W, Color, Cheques, Copy, Color Copy, Scanner, or undefined).
• Activity Time	Select the time in which the device is active (for example, a device might be made available only during office hours). If the fields are left empty, the activity time is taken from the default value in Settings. If the activity time in Settings is also empty, the device is always available.
• Default Printer Permission	Select whether Sentinel should allow or deny printing from everyone (with exceptions).
• Printer Group	You can add a printer group name. This field is used only as an informative field in reports.
• Fixed Monthly Rental Cost	This field is used only in the reports as an informative field.
• Adjust Copy	Some printers report back, via the foreign interface cable, an incorrect number of copies (for example, a printer may consistently report back that one extra copy was made). Using this field, you can adjust for these errors and solve the reporting problem.
• Time-out Copy	This field is used to override the default value set in Timeout showing copy for this specific device. An empty value causes Sentinel to use the default value defined in Settings.
• Minimum Pages Requiring Confirmation	This is used only for virtual devices (non-physical devices that are defined as IP 0.0.0.0). Set the number of pages to trigger a confirmation popup on the user's workstation before releasing the print job.
• Minimum Pages to Change Printer	Set the number of pages to cause Sentinel to switch the printer to the Heavy-duty printer.
• Force Billing Code	When using the popup client, this defines the maximum number of pages that can be printed without entering a billing code.

Parameter	Explanation
<ul style="list-style-type: none"> Count PS/PCL 	<p>This setting defines the way Sentinel counts pages. Usually when printing from Windows applications, the amount of pages and copies in the print job is reported by the Windows spooler subsystem. However, this system sometimes reports incorrect results, especially when dealing with collated copies and print jobs arriving from non-standard applications. Incorrect reporting can also occur when printing from non-Windows applications, such as printing from Unix, DOS, AS/400, Mac OS, etc. In such cases, Sentinel can be instructed to try to count the amount of pages and copies in the print job by parsing the actual print job. This is only possible if the print job is in PostScript or PCL5 languages. Leave this box unchecked unless a different counting method is required by the system.</p>
<div style="background-color: #f0f0f0; padding: 10px; border: 1px solid #ccc;"> <div style="display: flex; align-items: center;">  <div> <p>Caution!</p> <p>Using this checkbox with a printer driver that is not PCL5 or PostScript (that is, PCL6 or GDI) can lead to extremely inaccurate page counts!</p> </div> </div> </div>	
<ul style="list-style-type: none"> Printer Supports Duplex 	<p>Select this checkbox if the printer supports duplex printing. This allows more accurate logging of the pages and papers printed in the history and reports.</p>
<ul style="list-style-type: none"> Support FTP Mail 	<p>This feature allows you to scan documents to a specific user folder or email. To set up this feature:</p> <ol style="list-style-type: none"> Select this checkbox. A new subfolder is created in the Sentinel Queue folder (for example, C:\Sentinel\Queue\printer). If the folder is not created, create it manually. Redirect the multifunction device to scan into this folder. Under each user (Settings → Users → Edit User), enter the appropriate values in the fields Mail and Scan to Folder. <p>For these users, their card usage triggers Sentinel to take the file in the printer subfolder and send it to the user email or copy it to the user folder.</p>
<ul style="list-style-type: none"> Auto Open Copier 	<p>If selected, the multifunction will be opened for copy. If the user has print jobs waiting, they will be released, and if not, the copier function is automatically available. This eliminates the user's need to select print or copy function each time.</p>
<ul style="list-style-type: none"> SNMP Count 	<p>If selected, the Sentinel server communicates with the printer to verify exactly how many pages were actually printed (even if the user cancelled the job in the middle). For more details, see SNMP Timeout on p. 23.</p> <p>When using this feature, make sure that the field Port Name has the correct IP address value of the machine; otherwise, the server can receive unexpected results.</p>
<ul style="list-style-type: none"> Delete Job on Error 	<p>If selected, Sentinel checks if the printer has an error during printing (using SNMP, so SNMP communications must be defined properly first). If an error is discovered, Sentinel deletes the job from the printer queue and sends the printer HTTP messages to cause the printer to purge the rest of the print job. This means that no additional pages of old print jobs will be printed until the malfunction in the printer is fixed.</p> <p>This feature only works with specific printer models. Consult your Sentinel vendor.</p>

Parameter	Explanation
<ul style="list-style-type: none"> Printer Exception Users 	Whatever you select Allow all or Deny all (Default Printer Permission), you can add exceptions here. Select a user from the user list and click Add User to add that user to the exception list. To remove a user, select from the exception list and click Remove .
<ul style="list-style-type: none"> Prices 	In this grouping, you can define prices per page for each of the page types. These prices are then used in Sentinel reports.

Upgrading a Device's Network Firmware

Sometimes there is a need to upgrade the device's network firmware.



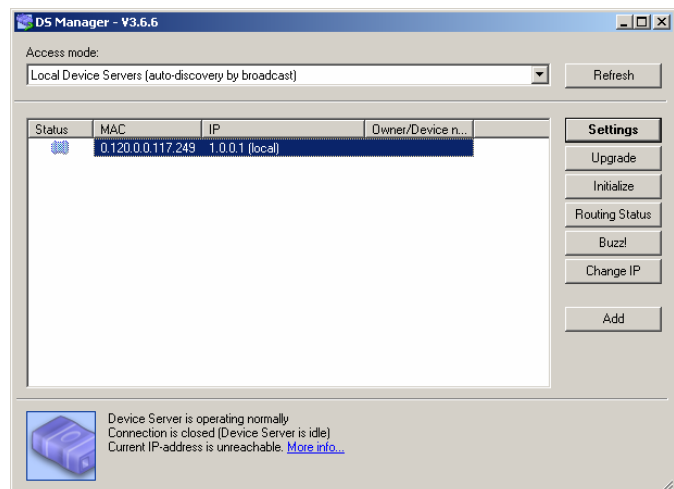
Caution!

Only do this if you have been specifically advised to do so by the device vendor!

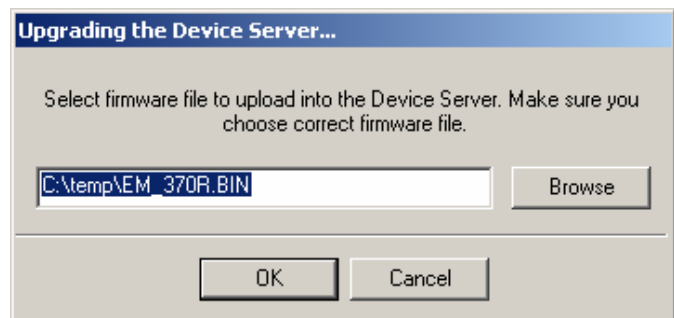
To upgrade the device's network firmware (Tibbo unit) you first need a firmware file (*.bin).

1. Attach the device you want to upgrade to the network.
2. Select **Start → Programs → Sentinel → DS Manager**.

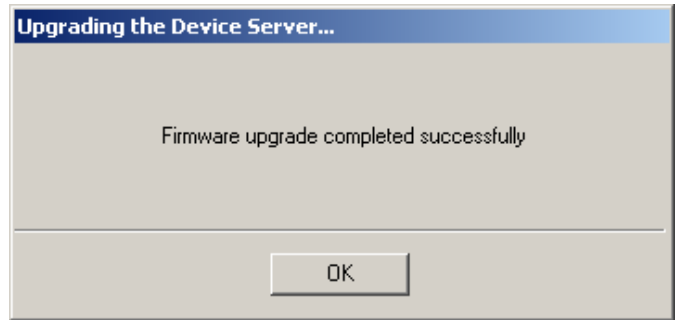
The DS Manager launches and begins searching for new devices.



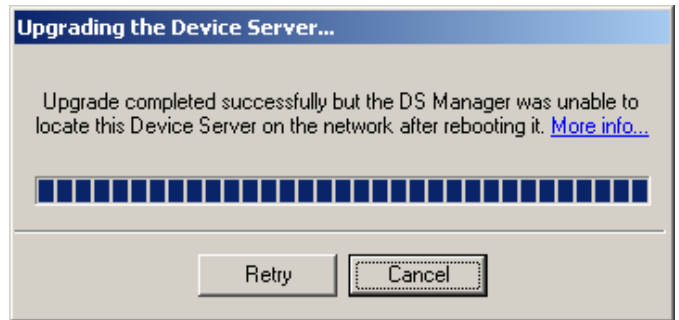
3. Browse for *.bin file supplied to you and click **OK**.



- The new device firmware is loaded into the device and this message appears. Click **OK**.



- If this message appears, click **Retry** and wait for the process to finish.



Adding New Users

To be able to print using Sentinel, a user must first be added to the system.



There are several options to instruct the system to automatically synchronize with external sources such as the Active Directory or an SQL server. For details, see *Auto Sync* on p. 24.

You can also add users to the system manually as follows:

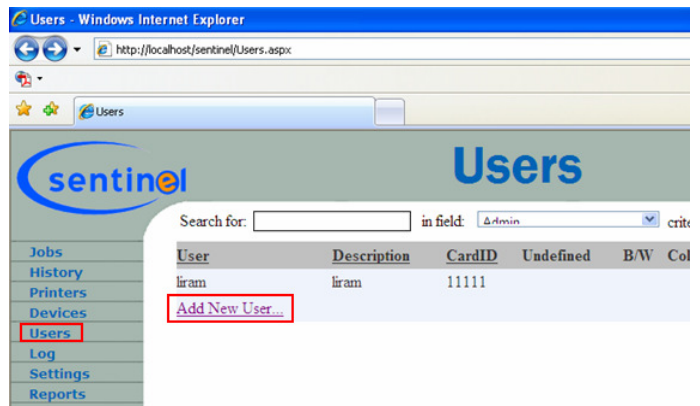
- From the left-hand menu on the Sentinel server, click **Users**.

All currently defined users appear in this table.

- To add create a new user, click **Add New User**.

This opens the Add User screen.

- Complete all fields as needed (described below).
- Click **Add**.



Parameter	Explanation
<ul style="list-style-type: none"> User 	Enter the name of the user. This name must be the same as the user login name on the Windows system.
<ul style="list-style-type: none"> Alternate User 	This is an alternate username that is used for the same user. This is common in ERP systems where the ERP username is different than the Network username.

Parameter	Explanation
• Description	Enter any text description of the user.
• Card ID	Enter the card ID of the user.
• Group • Department • Organization • Company	If you want to use Sentinel reports to track print activity within groups, departments, etc., you need to define each user as belonging to a group, a department, an organization, and a company. You can synchronize these with fields in the Active director. For details, see <i>Auto Sync</i> on p. 24.
• Mail	Enter the user's email address. This field is also used to receive scanned documents (see Support FTP Mail in the Add New Device screen).
• Scan to Folder	This is the path (local or network) of the folder to which scanned documents for this user are sent.
• Print Options	This setting overrides the same settings as defined on the General Settings page. To retain the default settings, select Use Default . For details of each of the options, see <i>Printing</i> on p. 25.
• Administrator	Select this checkbox to define the user as an administrator for Sentinel. An administrator can connect to the Sentinel Web interface from remote machines and see the full administrator menu (non-administrators only see their own print jobs).
• Exception User	This is an informative field in the database that can be used for external purposes.
• Allow Web Release	Select Allow to the user to log on to the Sentinel server Web interface and release jobs without using the reader device.
• Allow Keypad Release	Select Allow to the user to release print jobs by entering the keypad code or by entering the user card ID in the device controller. Select Deny to restrict device use by user card only.
• Manager	You can select another user whose jobs can be released by this user. (For example, if you have a manager with has several assistants, you can put the manager's username in this field for each of the assistants, and then all of them can release print jobs for the manager.
• Secretary	You can select another user name (hereafter: second user), and the first user can release the print jobs for the second user as well. For example if you have several managers who share a secretary, you can put the secretary's username in this field for each of the managers, and then this secretary can release print jobs for all of the managers.
• Keypad Code	You can define a keypad code, different from the card ID. Since card IDs can be very long, this makes it more convenient for users who want to enter a code at the device controller rather than using a card.
• Temp Card ID	This is an alternate card ID for this user. This allows you to assign another card ID for this user (for example, to give the user a temporary card to replace a lost card) without having to delete the original card ID.
• Quota Policy	Select one of the predefined quota policies. See <i>Quota Policy</i> on p. 27.
• Update Limits Now	After selecting a quota policy, you can force Sentinel to update the user's limits according to that quota policy. The default value for a new user is to update the quota, and the default value when editing an existing user is not to update the quota.

Parameter	Explanation
<ul style="list-style-type: none"> Force Billing Code 	<p>When using the popup client, this defines the maximum number of pages that can be printed without entering a billing code. This definition overrides the definition selected in the Device.</p>
<ul style="list-style-type: none"> Minimum Pages Requiring Confirmation 	<p>This is used only for virtual devices (non-physical devices that are defined as IP 0.0.0.0). Set the number of pages to trigger a confirmation popup on the user's workstation before releasing the print job. This definition overrides the definition selected in the Device.</p>
<ul style="list-style-type: none"> Message 	<p>Enter any text. This appears on the Web interface (below the left-hand menu) for that user.</p>
<ul style="list-style-type: none"> Limits 	<p>These fields allow you to set a printing limit for each type of printing. Setting a field to 0 (zero) disables all printing for that type. To allow unlimited printing, leave the field blank (empty).</p>

Databases

The standard installation of the Sentinel server uses the Microsoft Access database to store all data related to Sentinel activity. Microsoft Access itself is not required to be installed on the computer, as Sentinel uses the MDB file directly. However, if you choose to, you can install Microsoft Access and use it to open the Sentinel database file (usually located at **C:\Inetpub\wwwroot\Sentinel\App_Data\Sentinel.MDB**). This allows you to make additional reports and further use the data collected in the system.

Changing the Access Database into SQL Database

If you don't want to use the Microsoft Access database, you can set the Sentinel server to work with an SQL server database. To do so:

1. Edit the file `C:\inetpub\wwwroot\sentinel\web.config` according to the following scheme:

```
<add name="DatabaseConnection"
connectionString="Provider=SQLOLEDB.1;Server=<SERVER_NAME>;Database=Sentinel;U
id=<USER_ID>;Pwd=<PASSWORD>;"
providerName="System.Data.OleDb" />
```



There is usually a line starting with:

```
<add name="DatabaseConnection1..."
```

This line is intended for the SQL connection string. You can remove the "1" from this line, add the "1" to the line above that was without it and edit only the <Server Name> <User ID> <Password> fields.

2. Start the Registry Editor (**Start → Run**, and type the command **REGEDIT**).
3. Go to Registry key **HKEY_LOCAL_MACHINE\SOFTWARE\Sentinel\Settings** and edit the value **"DbConnectionString"** to be the same as the value you typed in the web.config file.
4. Add the database to the SQL Server as follows:
 - a. Build a new database with the name **Sentinel**.
 - b. Right-click the new database and select **Tasks → Import**.
 - c. Select the MDB file under `C:\Inetpub\wwwroot\Sentinel\App_Data\Sentinel.MDB` and select a destination – SQL.
 - d. Select the **Copy Data** option (not **Write**) and select **Select All**.
 - e. Select the **Execute immediately** option.
5. Go to **Sentinel → Tables** and right-click the first table. Select the **Modify** option (in SQL 2005) or the **Open Design** option (in SQL 2000). Then make the following modifications to each of the tables:
 - a. In each ID field, verify that the **Identity Specification** = YES.
 - b. Make sure that the function **Allow Null** is *not* selected (unchecked).
 - c. Verify in all tables that no field is defined as **Float** field type; use **Integer** field type instead.

Upgrading the Database from Older Versions of Sentinel

When upgrading Sentinel from older version to new version, you cannot simply replace all files, as some contain your specific definitions, such as the connection string to the database.

In addition, the new version may include new fields added to the database. If you upgrade the software files only but leave the database as it is, the software may encounter errors.

To prevent these problems, upgrade Sentinel as follows:

1. Back up all Sentinel files, including the database:
 - i) In the PC where the Sentinel server is installed, make a backup of the folders **c:\sentinel** and **c:\inetpub\wwwroot\sentinel**, including all files and subfolders. The second one is where the Sentinel website is located; if you selected a different path for this during installation, use that path.
 - j) If you are using anything other than the default Sentinel database (such as a different Access file or an SQL database), back it up. (If you are using the default database, **c:\inetpub\wwwroot\sentinel\App_Data\Sentinel.mdb**, it was included in the previous step.)
2. Copy and extra files:
 - a) Extract the upgrade package (usually a .zip file) to a temporary location. It contains three subfolders:
 - \PrecompiledWeb\
 - \Sentinel\
 - \UpdateTbl\
 - b) Select all the files in \Sentinel\ **except for service.ini**. Copy them to c:\sentinel\ (that is, overwrite the existing files).
 - c) Select all the files in \PrecompiledWeb\ **except for web.config** and **\PrecompiledWeb\App_Data\Sentinel.mdb**. Copy them to c:\inetpub\wwwroot\sentinel\ (that is, overwrite the existing files).
 - d) Select all the files in \UpdateTables\ and copy them to c:\sentinel\UpdateTables\ (that is, overwrite the existing files).
3. Update the Sentinel database:
 - a) Open a command line in the DOS box.
 - b) Go to the folder **c:\sentinel\updatetables**.
 - c) Make sure that the files **Access.ini** and **SQL.ini** exist in the same folder as the file **updatetbl.exe**.
 - d) Run the file **updatetbl.exe**. This runs a script that looks in the existing database for all missing fields and adds them. An output showing which fields were added appears on the screen.

Sentinel Monitoring Screens

In addition to all the Setting screens described previously, there are several screens that allow you to monitor print activities.

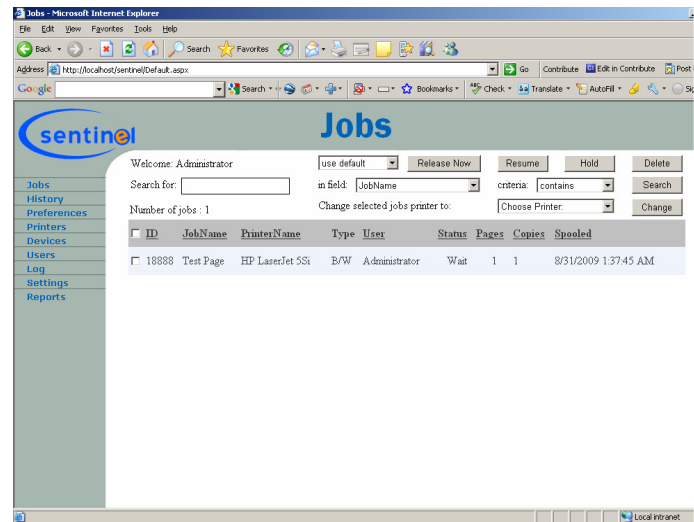
Print Jobs

This screen lists print jobs that were sent to Sentinel, but have not yet been picked up.

The information displayed here depends on the level of permission you have. If you are defined as an administrator of the system, you can see everyone's print jobs. Non-administrators can only see their own jobs.

You can use the search options to narrow the display to only print jobs answering specific criteria.

Each print job shows the job ID number, the print job name, the user who sent it, the printer it was sent to, the type of job it is (B/W, Color, etc.), the current job status, the number of pages and copies, and the time it was spooled.



The available job statuses are:

Status	Explanation
• Wait	The job was sent and is waiting for a user to release it.
• Held	The job is held at the queue and will not be released, even when the Delete unprinted jobs time period expires.
• Resumed	Same as Wait, but this print job was held once.

The following buttons provide control over these print jobs:

Parameter	Explanation
Release Now	Selecting some print jobs and clicking Release Now causes those print jobs to be released to the printer immediately. This is useful if there is a very large print job that was sent and the user doesn't want to go to the printer.
Change selected jobs printer to:	This causes the print job to change the destination printer to a different printer than the one to which it was sent. Since this action is performed automatically when identifying with an ID card in a different device than the one to which the print job was sent, this option is only useful when planning to release a print job with the Release Now to a different printer.

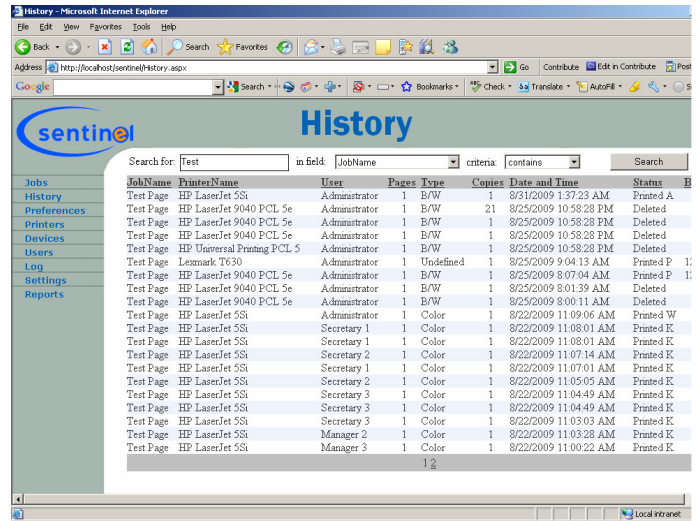
History and Archive

This screen displays the all events that occurred in the system within the defined period of time (defined in **Settings**).

The information displayed here depends on the level of permission you have. If you are defined as an administrator of the system, you can see everyone's print jobs. Non-administrators can only see their own jobs.

You can use the search options to narrow the display to only print jobs answering specific criteria.

Each print job shows the job ID number, the print job name, the user who sent it, the printer it was sent to, the type of job it is (B/W, Color, etc.), the current job status, the number of pages and copies, and the time it was spooled.

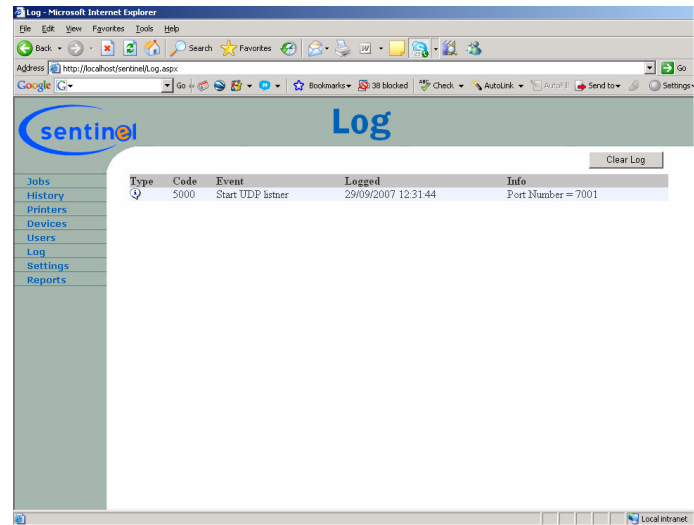


The available job statuses are:

Status	Explanation
• Printed C	The job was released by a user placing a real ID card at a device.
• Printed K	The job was released by a user typing a keypad code at a device
• Printed W	The job was released by selecting the job and releasing it from the Web interface.
• Printed A	The job was released automatically either because the job was sent to a virtual device (IP = 0.0.0.0) or the user sent this print job is defined as Auto Print.
• Printed P	The job was released after a popup window was used in the user station and confirmed the printing of the job or supplying a bill code.
• Printed T	The job was released by a user placing a temporary ID card at a device.
• Copied	This is a report from a copier or a multifunction device about an amount of copies made by a user.
• Scanned	This is a report from a scanning station about some pages scanned by a user.
• Deleted	The job was sent and manually deleted from the jobs menu.
• Deleted	The job was sent and was not released when the Delete unprinted jobs time period expired, and therefore was automatically cleared from the system.

Logging and Errors

This screen displays the all events, errors, and warnings that occur in the system.



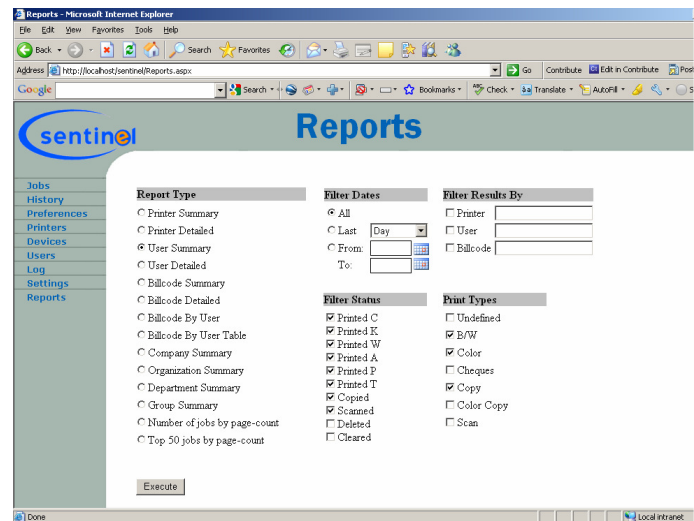
Reports

Once the system has been running for a while, you can generate reports to better understand and improve your organization's printing resources.

There are several types of reports that can be generated. Each report can be filtered according to dates, job status, and additional data fields, such as printer, user, and billing code.

After selecting the report type and the filters, click **Execute** to generate and view the selected report.

The report filters are described below.



Parameter	Explanation
Filter Dates	This allows you to select a range of dates for the report.
<ul style="list-style-type: none"> All From To 	This takes all information from the database with no date limitations. Specifies a date range for the data (either from a starting point or to an ending point).
Filter Results By	Filter the desired report only to a specific parameter (or a combination of parameters). The parameters include:
<ul style="list-style-type: none"> Printer 	Generates data only for a specific printer. To specify more than one printer, use a semicolon (;) between printer names, without any spaces before or after.

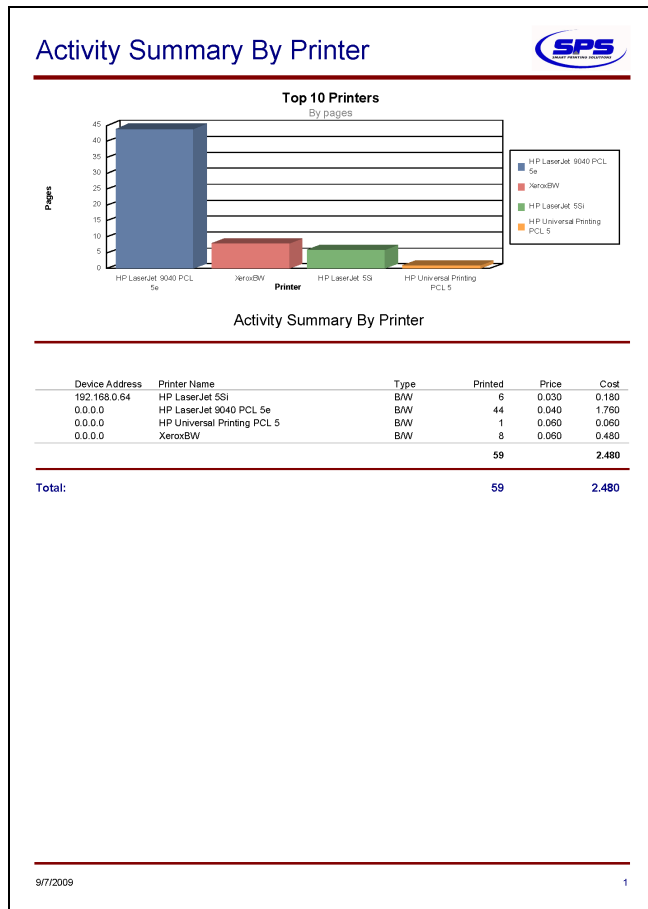
Parameter	Explanation
<ul style="list-style-type: none"> User 	Generates data only for a specific user. To specify more than one user, use a semicolon (;) between usernames, without any spaces before or after.
<ul style="list-style-type: none"> Billing Code 	Generates data only for a specific billing code. To specify more than one billing code, use a semicolon (;) between billing codes, without any spaces before or after.
Filter Status	<p>Generates data only for specific statuses. See <i>History and Archive</i> on p. 43 for an explanation of all statuses.</p> <p>For example, a very useful report is one showing only Deleted and Cleared jobs. This allows you to see how many pages are sent to the printer but not picked up or deleted before they are released.</p>
Filter Print Types	<p>Generates data only for specific printer types. See <i>Adding a New Device</i> on p. 32 for a description of the different printer types.</p> <p>The print type filter is enabled only if you select one of these reports:</p> <ul style="list-style-type: none"> User Summary Billing Code by User Billing Code by User Table Company Summary Organization Summary Department Summary Group Summary

Examples of reports are shown below.

Printer Reports (Summary and Detailed)

The printer summary report shows you the total amount of pages printed in a specific printer. The printer detailed report also gives you more detailed information about each of the print jobs printed to each printer.

Activity Details By Printer									
Activity Details By Printer									
HP LaserJet 9040 PCL 5e (1)									
Date	User	Job Name	Type	BitCode	Status	Printed	Price	Cost	
07/09/2009 10:48	Administrator	Test Page	B/W		Printed W	1	0.040	0.040	
07/09/2009 11:46	Employee4	File\JC\Documents and Settings\Adminis	B/W	111	Printed W	2	0.040	0.080	
07/09/2009 11:46	Employee8	outbind#343-00000000E8A9C4355E7EA94480	B/W		Printed W	1	0.040	0.040	
07/09/2009 11:46	Employee7	Microsoft Office Outlook - Weekly Style	B/W	222	Printed W	1	0.040	0.040	
07/09/2009 11:46	Employee1	xPress codes.xls	B/W		Printed W	18	0.040	0.840	
07/09/2009 11:48	Manager 1	xPress codes.xls	B/W	333	Printed W	2	0.040	0.080	
07/09/2009 11:48	Manager 3	Microsoft Word - Simadar Hebrew.doc	B/W	333	Printed W	21	0.040	0.840	
						44		1.760	
HP Universal Printing PCL 5 (1)									
Date	User	Job Name	Type	BitCode	Status	Printed	Price	Cost	
07/09/2009 10:45	Administrator	Test Page	B/W		Printed W	1	0.050	0.050	
						1		0.050	
XeroxBW (1)									
Date	User	Job Name	Type	BitCode	Status	Printed	Price	Cost	
07/09/2009 10:42	Administrator	Test Page	B/W		Printed A	1	0.090	0.090	
07/09/2009 11:46	Employee1	Test Page	B/W	333	Printed W	1	0.090	0.090	
07/09/2009 11:46	Employee2	http://localhost/sentinel/Default.aspx	B/W	222	Printed W	2	0.090	0.180	
07/09/2009 11:48	Secretary 2	xPress codes.xls	B/W	333	Printed W	4	0.090	0.360	
						8		0.690	
HP LaserJet 551 (1)									
Date	User	Job Name	Type	BitCode	Status	Printed	Price	Cost	
07/09/2009 11:46	Employee3	ink @MSFT\store C:\Program%20Files%20(x86)	B/W		Printed W	1	0.030	0.030	
07/09/2009 11:46	Employee5	Document1	B/W	222	Printed W	1	0.030	0.030	
07/09/2009 11:46	Secretary 1	Untitled	B/W		Printed W	1	0.030	0.030	
07/09/2009 11:48	Secretary 3	xPress codes.xls	B/W		Printed W	2	0.030	0.060	
07/09/2009 11:48	Manager 2	outbind#343-00000000E8A9C4355E7EA94480	B/W		Printed W	1	0.030	0.030	
						6		0.180	
9/7/2009									1

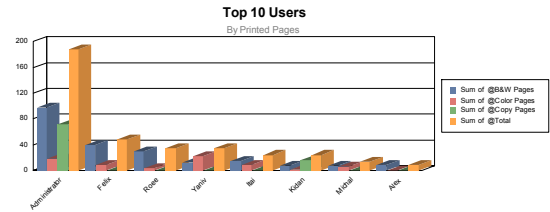


User Reports (Summary and Detailed)

The user summary report shows you the total amount of pages a specific user printed. The user detailed report also gives you more detailed information about each of the print jobs printed by each user.

Activity Details By User									
Administrators - Administrator ()									
Date	Printer	Job Name	Type	BillCode	Status	Printed	Price	Cost	
2/10/2009 10:00	HP4345	PDF-C-Sentinel-Hebrew 2.pdf	B/W		Printed C	2	0.05	0.10	
2/10/2009 09:45	Printer2	PDF-C-y3hn 12345.pdf	Color		Printed W	1	0.15	0.15	
2/10/2009 10:24	HP4345	Copy			Copied	1	0.08	0.08	
2/10/2009 10:22	HP4345	Copy			Copied	3	0.08	0.24	
2/10/2009 10:07	HP LaserJet M27	Microsoft Word - Reports	B/W		Printed A	1	0.05	0.05	
2/10/2009 10:07	HP LaserJet M27	Microsoft Word - Reports	B/W		Printed A	1	0.05	0.05	
2/10/2009 10:06	HP4345	Microsoft Word - Reports	B/W		Printed C	1	0.05	0.05	
2/10/2009 10:22	HP4345	Microsoft Word - Reports	B/W		Printed C	1	0.05	0.05	
2/10/2009 10:04	HP LaserJet M27	http://localhost/sentinel/Devices.a	B/W		Printed A	2	0.05	0.10	
2/10/2009 09:45	Printer1	PDF-C-y3hn 12345.pdf	B/W		Printed W	23	0.05	1.15	
2/10/2009 10:00	HP4345	Copy			Copied	2	0.08	0.16	
2/10/2009 10:00	HP4345	Microsoft Word - Reports	B/W		Printed C	1	0.05	0.05	
2/10/2009 09:57	HP4345	Copy			Copied	3	0.08	0.24	
2/10/2009 09:41	HP4345	PDF-C-neuron 22222.pdf	B/W		Printed W	1	0.05	0.05	
2/10/2009 09:45	HP4345	PDF-C-y3hn 12345.pdf	B/W		Printed W	2	0.05	0.10	
2/10/2009 09:32	HP4345	Copy			Copied	5	0.08	0.40	
2/10/2009 09:32	HP4345	PDF-C-neuron 22222.pdf	B/W		Printed C	2	0.05	0.10	
2/10/2009 09:32	HP4345	PDF-C-neuron 22222.pdf	B/W		Printed C	1	0.05	0.05	
2/10/2009 09:41	Printer1	PDF-C-y3hn 12345.pdf	B/W		Printed W	3	0.05	0.15	
2/10/2009 09:45	Printer2	PDF-C-y3hn 12345.pdf	Color		Printed W	14	0.15	2.10	
2/10/2009 09:45	Printer1	PDF-C-y3hn 12345.pdf	B/W		Printed W	28	0.05	1.40	
2/10/2009 10:02	HP4345	Copy			Copied	2	0.08	0.16	
2/10/2009 10:48	HP4345	Microsoft Word - Reports	B/W		Printed C	1	0.05	0.05	
2/10/2009 10:21	HP4345	Copy			Copied	20	0.08	1.60	
2/10/2009 14:41	HP4345	Copy			Copied	22	0.08	1.76	
2/10/2009 09:45	Printer1	http://localhost/sentinel/Devices.a	B/W		Printed W	2	0.05	0.10	
2/10/2009 14:29	HP4345	Copy			Copied	10	0.08	0.80	
2/10/2009 12:54	HP4345	Copy			Copied	1	0.08	0.08	
2/10/2009 09:52	HP4345	PDF-C-Sentinel-Hebrew 2.pdf	B/W		Printed W	2	0.05	0.10	
2/10/2009 09:45	Printer1	PDF-C-y3hn 12345.pdf	B/W		Printed W	14	0.05	0.70	
2/10/2009 09:45	Printer5	PDF-C-y3hn 12345.pdf	B/W		Printed W	2	0.05	0.10	
2/10/2009 10:26	HP LaserJet M27	Microsoft Word - Reports	B/W		Printed A	1	0.05	0.05	
2/10/2009 10:31	HP4345	Copy			Copied	2	0.08	0.16	

Activity Summary By User



Activity Summary By User

Administrators					
User	User Description	B/W	Color	Copy	Total
Administrator		98	18	72	188
Total: 98 18 72 188					
Sales					
User	User Description	B/W	Color	Copy	Total
Felix		39	9	0	48
Michal		7	6	0	13
Yaniv		12	22	0	34
Total: 58 37 0 95					
SPS					
User	User Description	B/W	Color	Copy	Total
Alex		8	0	0	8
Itai		15	9	0	24
Kidan		7	1	16	24
Roni		30	4	0	34
Total: 60 14 16 90					
Total:		216	69	88	373

2/3/2009

1

Billing Code Reports (By User and By User Table)

The billing code by user and billing code by user table reports shows both show you the total amount of pages a specific user printed for specific billing code, but in two different types of presentation.

Activity Details By Billcode And User									
Billcode	Billcode Description	User	CreditID	User Description	BW	Color	Copy	Printed	Cost
		Administrator	103		3.00	0.00	0.00	3	0.160
		Employee1	8		16.00	0.00	0.00	16	0.640
		Employee3	10		1.00	0.00	0.00	1	0.030
		Employee5	13		1.00	0.00	0.00	1	0.040
		Manager 2	3		1.00	0.00	0.00	1	0.030
		Secretary 1	5		1.00	0.00	0.00	1	0.030
		Secretary 2	7		2.00	0.00	0.00	2	0.060
		Employee4	11		2.00	0.00	0.00	2	0.060
		Employee2	9		2.00	0.00	0.00	2	0.120
111	Customer 1	Employee4	11		1.00	0.00	0.00	1	0.030
222	Customer 2	Employee2	9		1.00	0.00	0.00	1	0.040
222	Customer 2	Employee5	12		1.00	0.00	0.00	1	0.030
222	Customer 2	Employee5	13		1.00	0.00	0.00	1	0.040
333	Customer 3	Employee1	8		1.00	0.00	0.00	1	0.060
333	Customer 3	Manager 1	2		2.00	0.00	0.00	2	0.080
333	Customer 3	Manager 3	4		21.00	0.00	0.00	21	0.840
333	Customer 3	Secretary 2	6		4.00	0.00	0.00	4	0.240

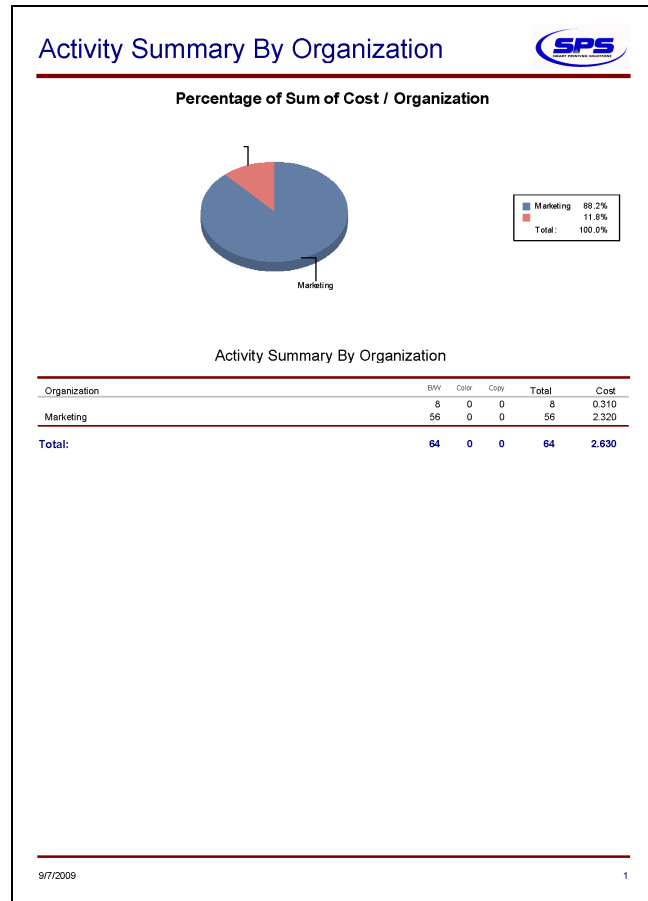
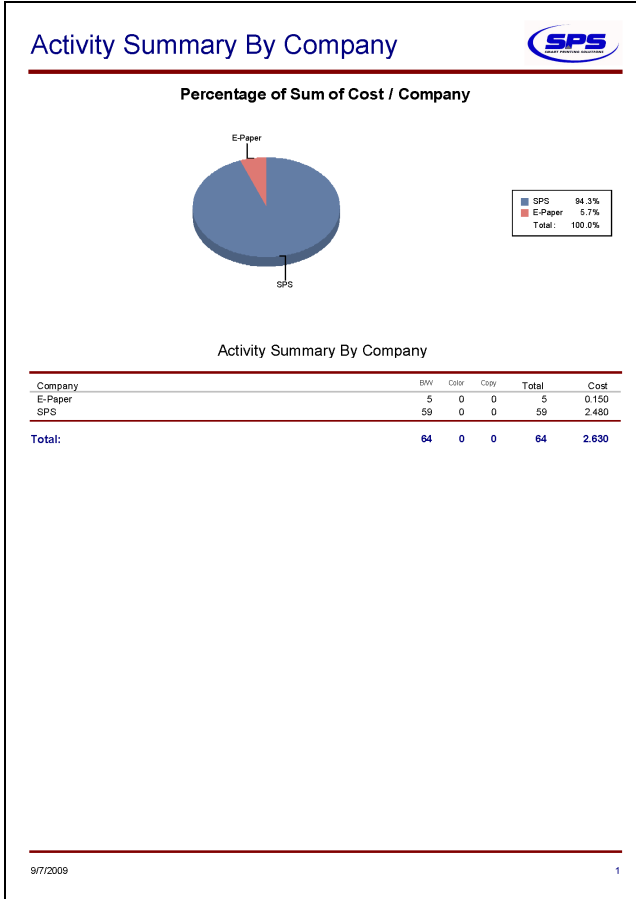
9/7/2009 1

Activity Summary By Billcode and User						
Activity Summary By Billcode and User						
User	User Description	BW	Color	Copy	Total	Cost
Administrator		3	0	0	3	0.160
Employee1		16	0	0	16	0.640
Employee3		1	0	0	1	0.030
Employee6		1	0	0	1	0.040
Manager 2		1	0	0	1	0.030
Secretary 1		1	0	0	1	0.030
Secretary 3		2	0	0	2	0.060
		25	0	0	25	0.990
111 - Customer 1						
User	User Description	BW	Color	Copy	Total	Cost
Employee4		2	0	0	2	0.080
		2	0	0	2	0.080
222 - Customer 2						
User	User Description	BW	Color	Copy	Total	Cost
Employee2		2	0	0	2	0.120
Employee5		1	0	0	1	0.030
Employee6		1	0	0	1	0.040
		4	0	0	4	0.190
333 - Customer 3						
User	User Description	BW	Color	Copy	Total	Cost
Employee1		1	0	0	1	0.060
Manager 1		2	0	0	2	0.080
Manager 3		21	0	0	21	0.840
Secretary 2		4	0	0	4	0.240
		28	0	0	28	1.220
Total:		59	0	0	59	2.480

9/7/2009 1

Group, Department, Organization, and Company Reports

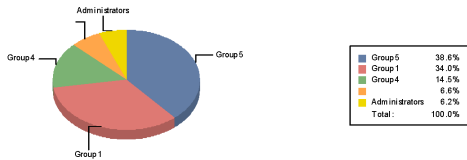
These reports show the distribution of usage between groups, departments, organizations and companies.



Activity Summary By Group



Percentage of Sum of Cost / Group



Activity Summary By Group

Group	BW	Color	Copy	Total	Cost
Administrators	3	0	0	3	0.160
Group 1	5	0	0	5	0.150
Group 2	19	0	0	19	0.820
Group 3	3	0	0	3	0.110
Group 4	7	0	0	7	0.350
Group 5	24	0	0	24	0.930
Total:	64	0	0	64	2.630

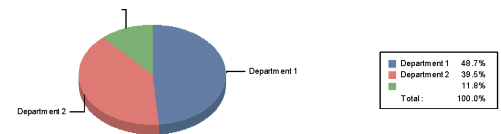
9/7/2009

1

Activity Summary By Department



Percentage of Sum of Cost / Department



Activity Summary By Department

Department	BW	Color	Copy	Total	Cost
Department 1	8	0	0	8	0.310
Department 2	29	0	0	29	1.280
Total:	64	0	0	64	2.630

9/7/2009

1

Other Reports

These reports show how many pages in average are printed on each print job, and the print jobs with the largest amount of pages, respectively.

Top 50 Jobs By Page Count



Top 50 Jobs By Page Count

Date	User	Printer	Job Name	Type	BillCode	Status	Printed	Price	Cost
07/09/2009 11:48	Manager 3	HP LaserJet 904	Microsoft Word - Smadar Hebrew.doc	BW	333	Customer 3	Printed W	21	0.940
07/09/2009 11:46	Employee1	HP LaserJet 904	sPhess codes.xls	BW			Printed W	16	0.640
07/09/2009 11:48	Secretary	XeroxBW	sPhess codes.xls	BW	333	Customer 3	Printed W	4	0.060
07/09/2009 11:48	Secretary	HP LaserJet 550	sPhess codes.xls	BW			Printed W	2	0.030
07/09/2009 11:48	Manager 1	HP LaserJet 904	sPhess codes.xls	BW	333	Customer 3	Printed W	2	0.040
07/09/2009 11:46	Employee2	XeroxBW	http://doccentral03.net/Default.a	BW	222	Customer 2	Printed W	2	0.090
07/09/2009 11:48	Employee1	HP LaserJet 904	hw.doc (Documents and Settings\Ad	BW	111	Customer 1	Printed W	2	0.010
07/09/2009 11:48	Employee5	HP LaserJet 550	Document1	BW	222	Customer 2	Printed W	1	0.030
07/09/2009 11:46	Employee6	HP LaserJet 904	subintl\J243-0000000EBARC435SE7EA	BW			Printed W	1	0.040
07/09/2009 11:46	Employee6	HP LaserJet 904	Microsoft Office Outlook - Weekly S	BW	222	Customer 2	Printed W	1	0.040
07/09/2009 10:42	Administra	XeroxBW	Test Page	BW			Printed A	1	0.060
07/09/2009 10:45	Administra	HP Universal P	Test Page	BW			Printed W	1	0.090
07/09/2009 10:48	Administra	HP LaserJet 904	Test Page	BW			Printed W	1	0.040
07/09/2009 11:46	Employee1	XeroxBW	Test Page	BW	333	Customer 3	Printed W	1	0.060
07/09/2009 11:46	Employee3	HP LaserJet 550	mk.QM8IT Store-C:\Program%20files%20	BW			Printed W	1	0.030
07/09/2009 11:46	Secretary	HP LaserJet 550	Untitled	BW			Printed W	1	0.030
07/09/2009 11:48	Manager 2	HP LaserJet 550	subintl\J243-0000000EBARC435SE7EA	BW			Printed W	1	0.030
07/09/2009 14:45	Admin	HP LaserJet 550	Test Page	BW			Printed W	1	0.030
07/09/2009 14:45	Admin	HP LaserJet 550	Test Page	BW			Printed W	1	0.030
07/09/2009 14:45	Admin	HP LaserJet 550	Test Page	BW			Printed W	1	0.030
07/09/2009 14:45	Admin	HP LaserJet 550	Test Page	BW			Printed W	1	0.030
07/09/2009 14:45	Admin	HP LaserJet 550	Test Page	BW			Printed W	1	0.030
Total:							64	2.630	

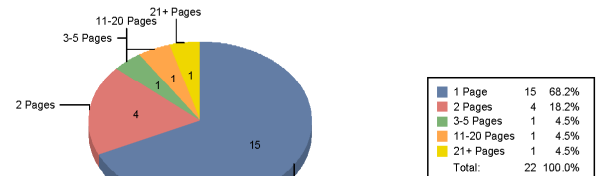
9/7/2009

1

Job Count By Number of Pages



Job Count By Number Of Pages



External Utilities

Maintenance Utilities

Sentinel supports various external tools that perform different maintenance tasks. These tools are usually used inside scripts or as scheduled tasks.

Utility	Explanation
DelKeypad.exe	<p>This tool is used to delete the values of the fields Temporary Card and Keypad Code from the user table. The syntax of usage is:</p> <ul style="list-style-type: none">• <code>DelKeypad.exe -dt</code> Deletes the Temporary Card field values for all users.• <code>DelKeypad.exe -dk</code> Deletes the Keypad code field values for all users. <p>For example, putting DelKeypad.exe -dt in a scheduler that runs each night deletes all temporary cards assigned during the day.</p>
ADUserSync.exe SQLUserSync.exe	<p>These tools are used to delete users that exists in the Sentinel database, but don't exist in the Active Directory/SQL server from which the automatic synchronization is performed. For more information about automatic synchronization, see <i>Auto Sync</i> on p. 24. The utility to be used is according to the synchronization type you use.</p> <p>If you want some users not to be deleted from the Sentinel database even though they don't exist in the Active Directory/SQL server, select the Exception User checkbox in the User Properties screen.</p>

Identifying Print Jobs Sent from a Shared Workstation

In situations where many users share a common account (username) on a centralized workstation, Sentinel may not be able to identify the correct user for print jobs. This is because when print jobs appear on the Sentinel port, they seem to come from the same user, even though each user has a unique ID card or code at the Sentinel device controller.

The solution is to run a special utility at the workstation. This utility provides an additional user identification window in which users must identify themselves before the print job can be released. This way, when print jobs appear on the Sentinel port, they are correctly recognized.

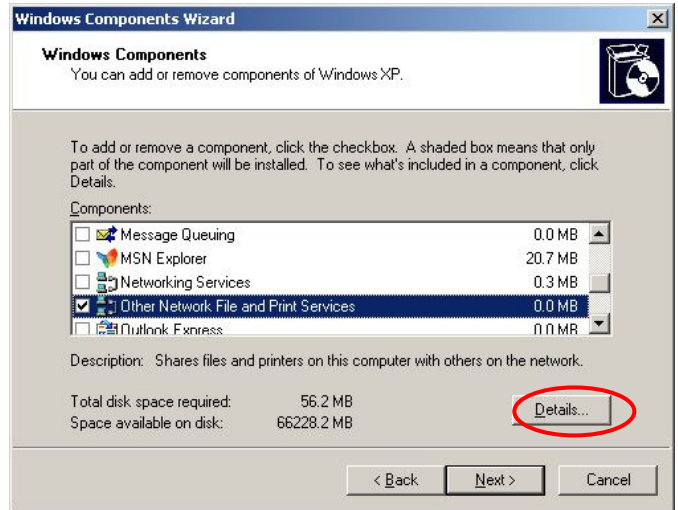
To configure this feature:

1. Make sure that the Sentinel server is running the LPD service (sometimes referred to as Print Services for Unix or the TCP/IP Print Server):

For Windows 2003 Server or Windows XP: Go to **Control Panel → Add or Remove Programs → Add/Remove Windows Components**. Select **Other Network File and Print Services** and click **Details**. Make sure that **Print Services for Unix** is selected.



The location of these Windows settings is slightly different in Windows Vista and Windows 2008. Refer to your Windows documentation for more information.

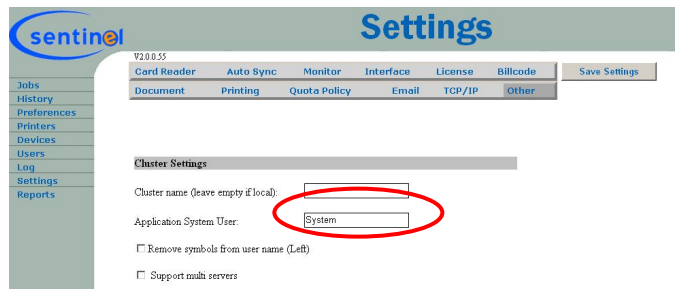


2. After running the service, make sure that there is no active firewall. If there is, open TCP port 515.



There is no need to share printers from the server; printing is done by LPD-LPR.

3. Log on to Sentinel (**Start → Programs → Sentinel → Web Sentinel**). Select **Settings** from the left-hand menu.
4. Select the **Other** tab.
5. In **Application System User**, enter the general username used when logging in from a shared workstation.

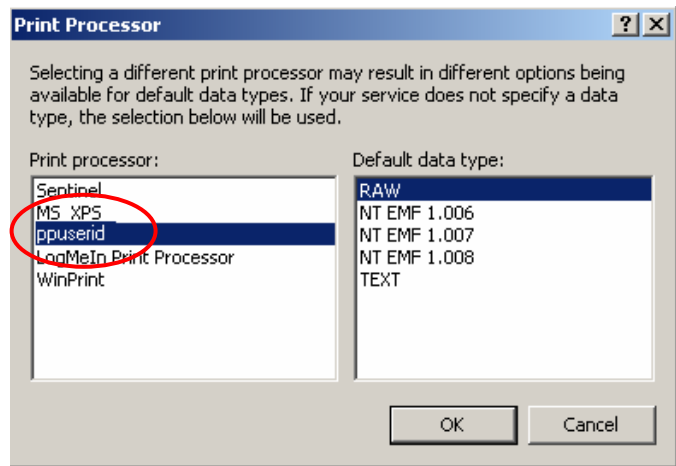
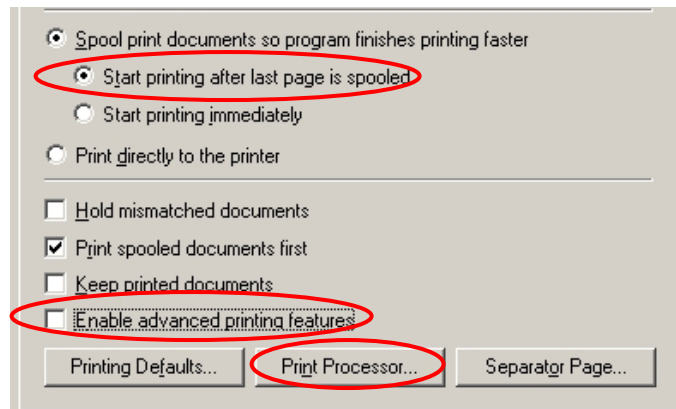
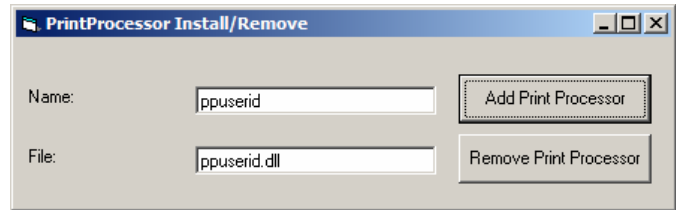


6. The following three files are located in C:\Sentinel\ppuserid. Copy them to each workstation where you want the user identification window to appear:
 - Ppuserid.dll: copy to c:\windows\system32\spool\prtprocs\w32x86\
 - Userid.dll: copy to c:\windows\system32
 - Ppuserid.exe: copy to the workstation (the location doesn't matter; this file can be deleted after this installation process)

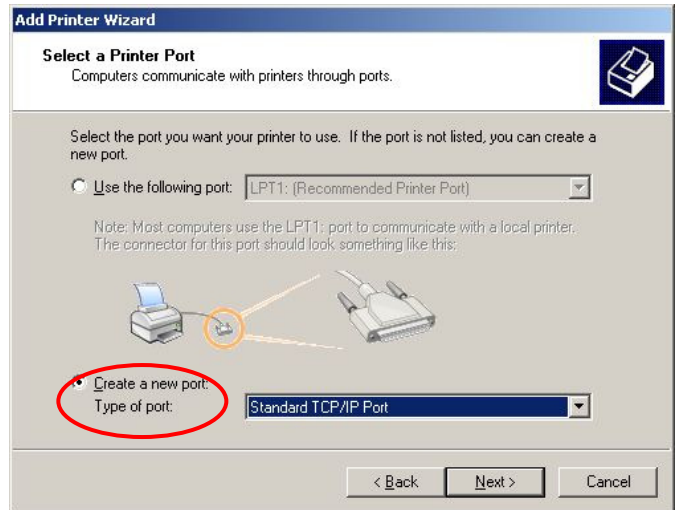
7. Run **Ppuserid.exe** on the workstation, make sure that the **Name** and **File** are correct, and click **Add Print Processor**.

! If you receive an error message at this point, contact your Sentinel provider.

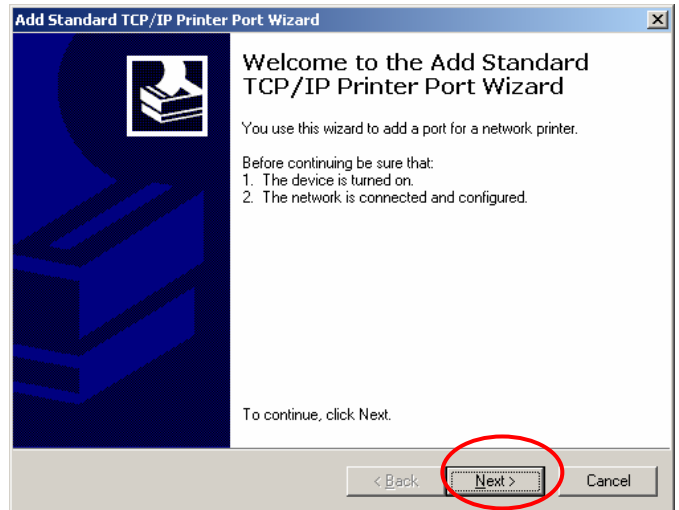
8. When the Add Print Processor utility finishes, install it as follows: Go to **Control Panel → Printers and Faxes**. Right-click the ppuserid printer and select **Properties**. Select the **Advanced** tab. Make sure that **Start printing after last page is spooled** is selected, and that **Enable advanced printing features** is *not* selected.
9. Click **Print Processor**. The printer appears in the list.



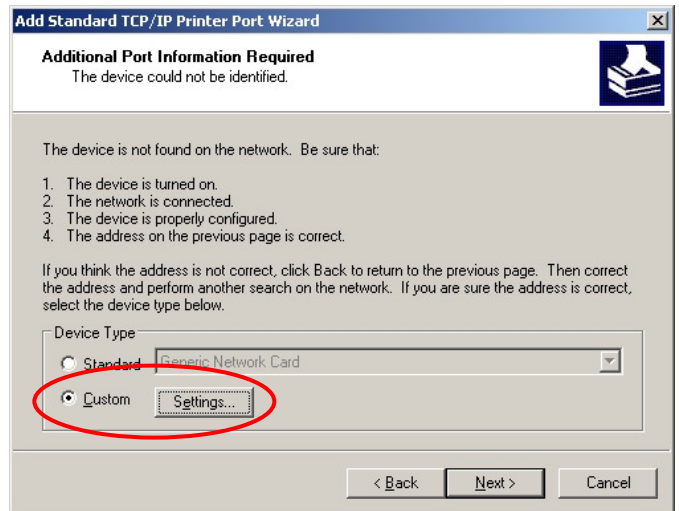
10. Add a local printer to the workstation (**Control Panel → Printers and Faxes → Add a printer**). In the Add Printer wizard, select **Local Printer** and click **Next**. Select **Create a new port** and set the port type to **Standard TCP/IP Port**. Click **Next**.



11. The Add Standard TCP/IP Port Printer wizard opens. Click **Next**.



12. Select **Custom** and click **Settings**.



13. Enter the IP address of the Sentinel server.

The **Port Name** is created automatically; it is the IP address with “IP_” in front. Do not change this.

Click **Next**.



It may take the wizard up to a minute to proceed.

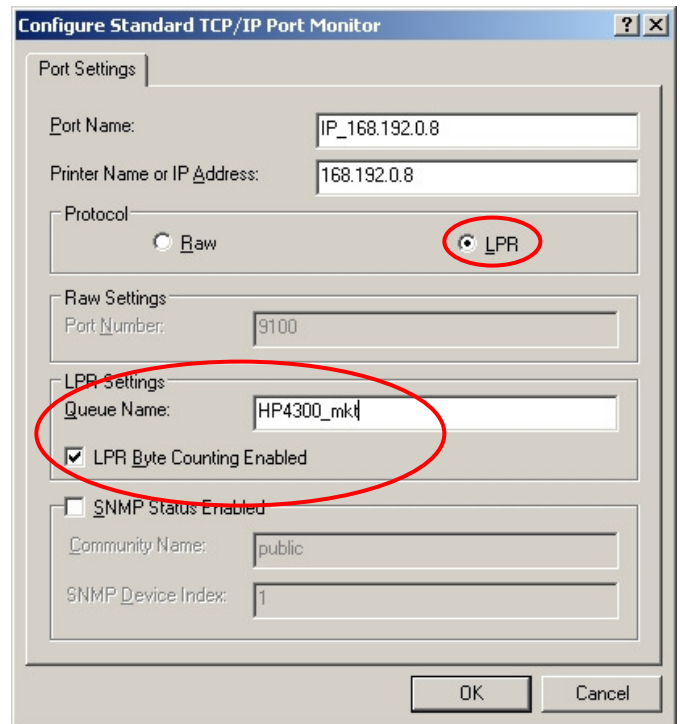
The screenshot shows the 'Add Standard TCP/IP Printer Port Wizard' dialog box. The title bar reads 'Add Standard TCP/IP Printer Port Wizard'. The main heading is 'Add Port' with the question 'For which device do you want to add a port?'. Below this, it says 'Enter the Printer Name or IP address, and a port name for the desired device.' There are two input fields: 'Printer Name or IP Address:' containing '168.192.0.8' and 'Port Name:' containing 'IP_168.192.0.8'. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

14. In **Device Type**, select **Custom** and click **Settings..**

The screenshot shows the 'Add Standard TCP/IP Printer Port Wizard' dialog box. The title bar reads 'Add Standard TCP/IP Printer Port Wizard'. The main heading is 'Additional Port Information Required' with the message 'The device could not be identified.' Below this, it says 'The device is not found on the network. Be sure that:' followed by a numbered list: 1. The device is turned on. 2. The network is connected. 3. The device is properly configured. 4. The address on the previous page is correct. Below the list, it says 'If you think the address is not correct, click Back to return to the previous page. Then correct the address and perform another search on the network. If you are sure the address is correct, select the device type below.' There is a 'Device Type' section with a dropdown menu set to 'Generic Network Card'. Below this are two radio buttons: 'Standard' (unselected) and 'Custom' (selected). A red oval highlights the 'Custom' radio button and the 'Settings...' button next to it. At the bottom right, there are three buttons: '< Back', 'Next >', and 'Cancel'.

15. Set **Protocol** to **LPR**.
16. In **Queue Name**, enter the name of the printer as it appears on the Sentinel server (the printer name itself, and not the name of the shared service).
17. Make sure that **LPR Byte Counting Enabled** is selected and click **OK**.

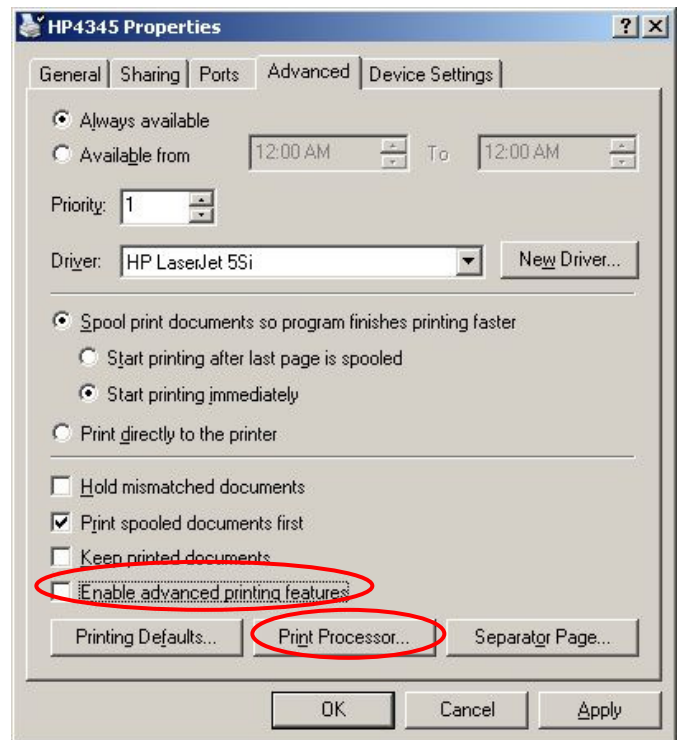
The printer is created and now should appear on in the Control Panel's Printers and Faxes area.



18. Right-click the printer and select **Properties**.
19. In the Advanced tab, make sure that **Enable advanced printing features** is **not** selected.
20. Click **Print Processor**.

The Print Processor dialog box appears. Select **ppuserid** from the list.

Users can now print from the workstation. After sending a print request, a user identification window appears. A user must enter a username or user ID number to proceed.



Running Sentinel with Advanced Printing Features

Usual configuration of Sentinel requires that **Enable advanced printing features** is *not* selected. This is because if **Enable advanced printing features** is selected, you can't run Sentinel as a print processor. This means that advanced features, such as being able to print multiple pages on a single page, are not available.

The solution is to run Sentinel as a port monitor instead of a print processor. This allows you to use **Enable advanced printing features**.



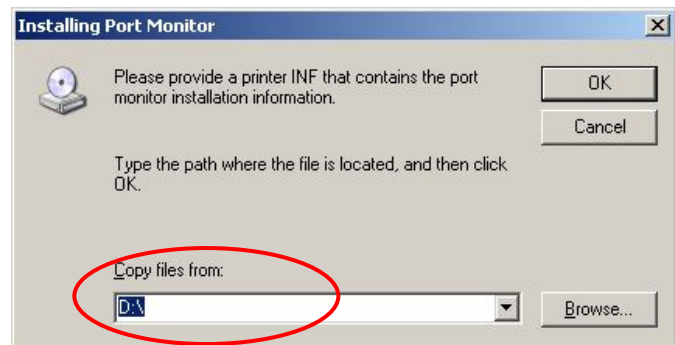
This solution currently works only with a virtual networked printer; that is, sharing a single printer for all users and using **Follow Me** when users place their ID cards at a Sentinel device controller. This is because Sentinel port monitor can't move print jobs after releasing them to a real printer; it can only capture print job information for the database.

This configuration process is only for Windows XP and Windows 2003 Server (both 32- and 64-bit). Other operating systems may require different settings.

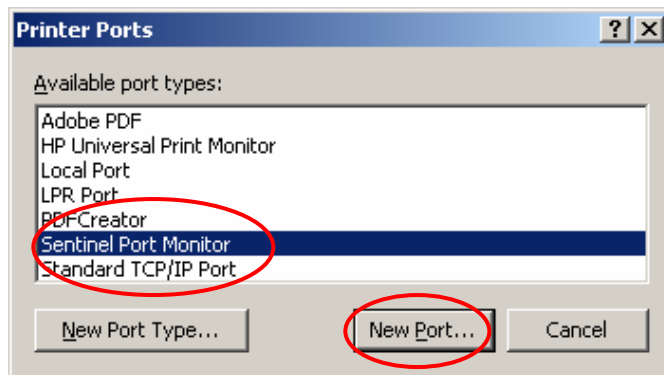
1. Create the following folders:
 - c:\Sentinel\port_mon\w32\
 - c:\Sentinel\port_mon\w64\
 - monitor.inf
 - sentinel_local_mon.dll
 - sentinel_local_mon_ui.dll
2. Copy the following files into each OS type (32- and 64-bit) folder:
3. Open the virtual's printer Properties (in the Control Panel's Printers and Faxes area, right-click the printer and select **Properties**).
4. Select the **Ports** tab and click **Add Port**.
5. Click **New Port Type**.

The Installing Port Monitor dialog box appears.

6. Select the folder to which you copied the three files (in step 2, above) and click **OK**.



7. The new port type now appears on the list. Select it and click **New Port**.

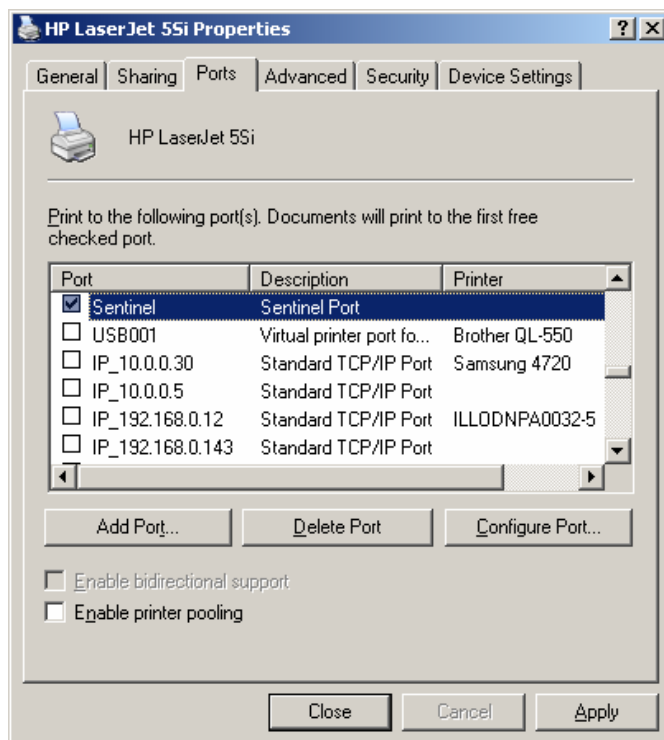


8. Enter **Sentinel** as the port name and click **OK**.

9. Click **Close**.



10. Select the Sentinel port from the list and click **Apply**.



11. In the Advanced tab, click **Print Processor** .

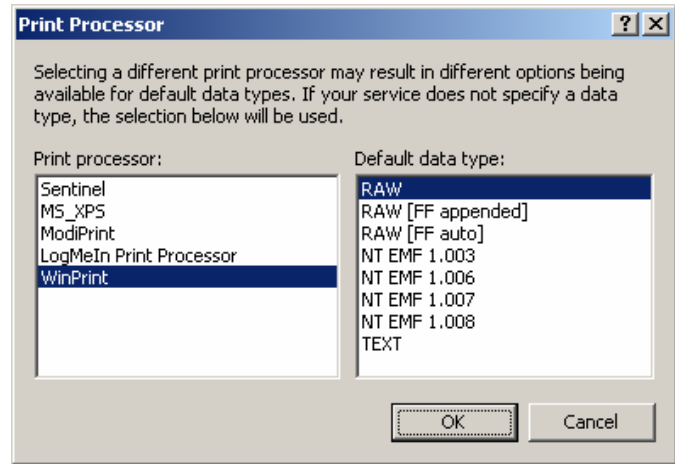
The Print Processor dialog box appears.

12. Select **WinPrint** from the list of Print processors and click **OK**. (You are resetting the print processor from Sentinel to WinPrint.)



This is very important because if the Print Processor is not changed to WinPrint, then all print jobs sent through this port will appear in Sentinel twice!

You can now work with Advanced Printing features enabled, allowing you to collate or print multiple pages per page.



Troubleshooting

This section covers errors or problems that can occur during installation, configuration, and daily operation of Sentinel. If the suggested solution does not solve the problem, or if you experience a problem not listed here, contact your Sentinel technical support provider.

Failed to Add Sentinel Service

Symptoms	When trying to start the Sentinel service, you see that no such service is added to the system. In the file <code>c:\sentinel\service.log</code> , the error Failed to create service Sentinel, error code = 1073 appears.
Cause	There may be other services that use the name "Sentinel"; when the installation program tries to install the service, it fails.
Resolution	Change the name of the service and add it manually as follows: <ol style="list-style-type: none">1. Open the file <code>c:\sentinel\service.ini</code> in Notepad.2. Under the section [Settings], change the key ServiceName to something else; for example, change it to ServiceName = SPSSentinel.3. Save the file.4. Open a DOS box command line and change the directory to <code>c:\sentinel</code>.5. Type the command service -i.6. In the Services screen, check to see if the Sentinel service was added in the new name.

Failed to Access IIS Metabase

Symptoms When trying to start the Sentinel Web page, you get the following error:
Server Error in '/ Sentinel ' Application.

Failed to access IIS metabase.

Description: An unhandled exception occurred during the execution of the current web request. Please review the stack trace for more information about the error and where it originated in the code.

Exception Details: System.Web.Hosting.HostingEnvironmentException: Failed to access IIS metabase.

The process account used to run ASP.NET must have read access to the IIS metabase (e.g. IIS://servername/W3SVC). For information on modifying metabase permissions, please see <http://support.microsoft.com/?kbid=267904>.

Source Error:

An unhandled exception was generated during the execution of the current web request. Information regarding the origin and location of the exception can be identified using the exception stack trace below.

Stack Trace:

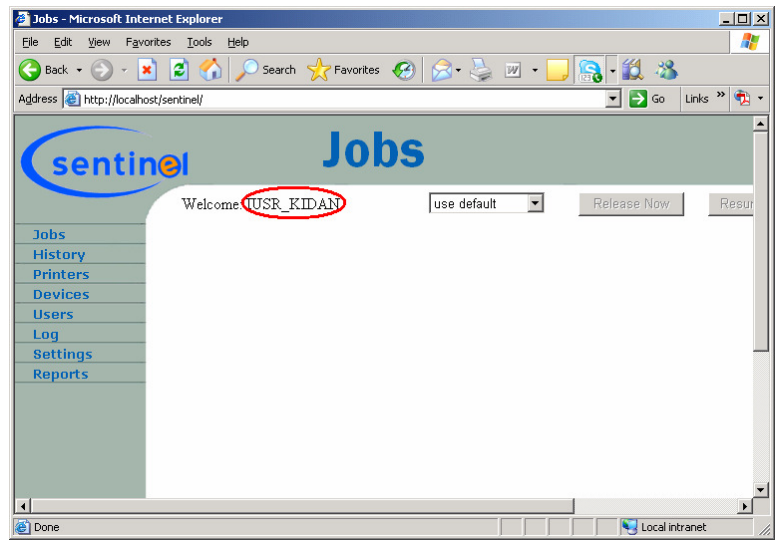
```
[HostingEnvironmentException: Failed to access IIS metabase.]
System.Web.Configuration.MetabaseServerConfig.MapPathCaching(String siteID, VirtualPath path) +3492122
System.Web.Configuration.MetabaseServerConfig.MapPathCaching(String siteID, VirtualPath vpath) +9
System.Web.Hosting.HostingEnvironment.MapPathActual(VirtualPath virtualPath, Boolean permitNull) +163
System.Web.CachedPathData.GetConfigPathData(String configPath) +382
System.Web.CachedPathData.GetConfigPathData(String configPath) +243
System.Web.CachedPathData.GetConfigPathData(String configPath) +243
System.Web.CachedPathData.GetApplicationPathData() +68
System.Web.CachedPathData.GetVirtualPathData(VirtualPath virtualPath, Boolean permitPathsOutsideApp) +3385631
System.Web.Configuration.RuntimeConfig.GetLKGRuntimeConfig(VirtualPath path) +189
```

Version Information: Microsoft .NET Framework Version:2.0.50727.42; ASP.NET Version:2.0.50727.42

Cause	This error usually occurs when the IIS was installed after the DotNet Framework 2.0 was already installed. Then the rights to the ASPNET user are not set correctly. The DotNet Framework must be installed after the IIS.
Resolution	Run the command C:\WINDOWS\Microsoft.NET\Framework\v2.0.50727\aspnet_regiis -i If it fails, try this: <ol style="list-style-type: none"> 1. Uninstall Sentinel, DotNet Framework 2.0 and IIS. 2. Install IIS. 3. Install DotNet Framework 2.0. 4. Install Sentinel.

Wrong username appears in the Web interface

Symptoms When running the Web interface, the same user name always appears (usually starts with the prefix "IUSR_").



Cause	This error occurs when the IIS is using Anonymous access instead of Integrated Windows authentication .
Resolution	Follow step 7 on p. 5 to set the proper settings.

HTTP Error 404: File or Directory not found

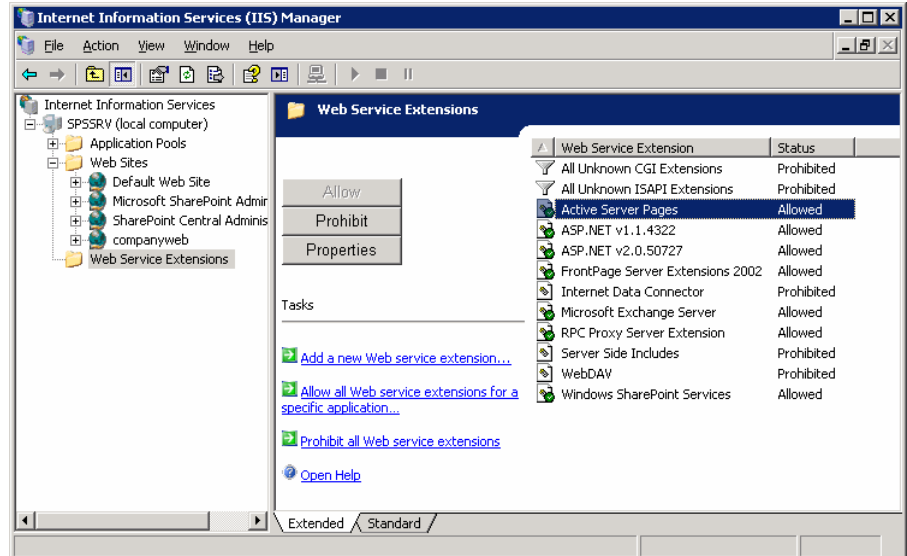
Symptoms When trying to start the Sentinel web page, you get the following error: **HTTP Error 404: File or Directory not found**.

Cause By default, when IIS is installed on any version of the Windows Server 2003 family, IIS only serves static content (HTML).

Resolution

First check that IIS is running, and **Default Web Site** is not stopped. If it is running, and you need to permit IIS to serve content that requires a specific ISAPI or CGI extension that is already listed in the Web service extensions list, follow these steps:

1. Open IIS Manager, expand the master server node (that is, the Servername node), and then select the Web service extensions node.

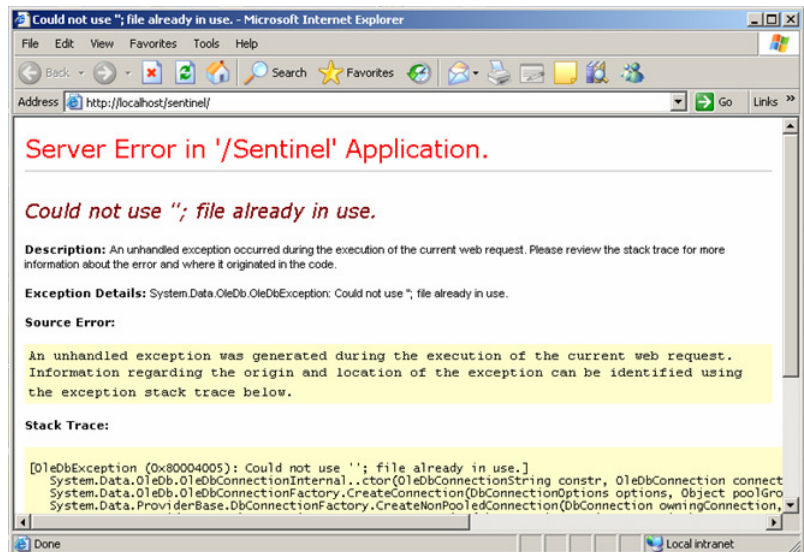


2. In the right pane of IIS Manager, make sure that the **Active Server Pages** extension is allowed and that the ASP.NET v2.0.50727 is allowed.
3. Reset the IIS service by typing **IISRESET** in the command line.

Could not use "; file already in use

Symptoms

When trying to start the Sentinel Web page, you get the following error:



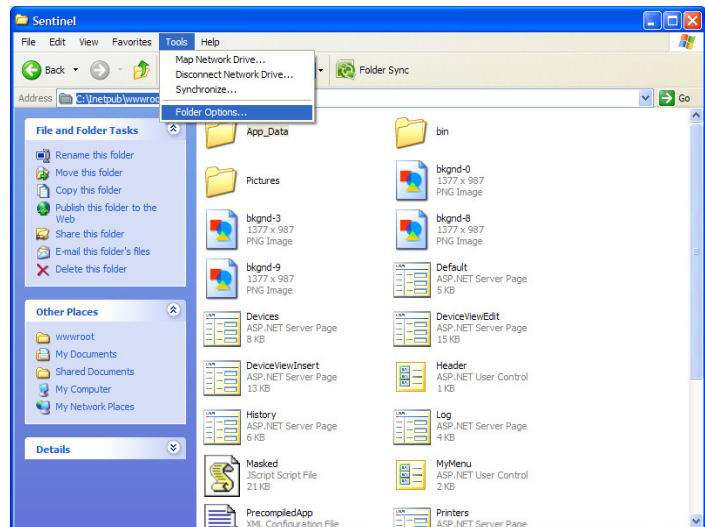
Cause

The database is currently locked by the Sentinel service because the right permissions haven't been set for it. Verify this by stopping Sentinel as follows:

1. Go to Windows Services (**Start → Settings → Control Panel → Administrative Tools → Services**).
2. Stop the Sentinel service by right-clicking **Sentinel** and selecting the **Stop** option.
3. Go back and refresh the Web Sentinel page. It should load without the problem.

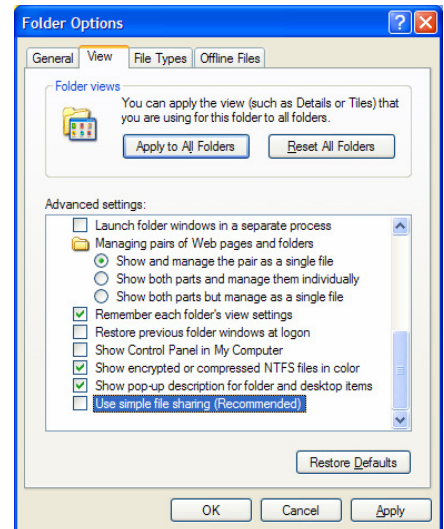
Resolution 1

1. Make sure the service is running. If you stopped it, start it again (in Windows Services, select **Sentinel** and click **Start**)
2. Open File Explorer and navigate to **C:\inetpub\wwwroot\Sentinel\App_Data**
3. Right-click the file **Sentinel.mdb** and click **Properties**.
4. Click the Security tab. If you don't see a Security tab, close the Properties window, and from the Tools menu, select **Folder Options**.

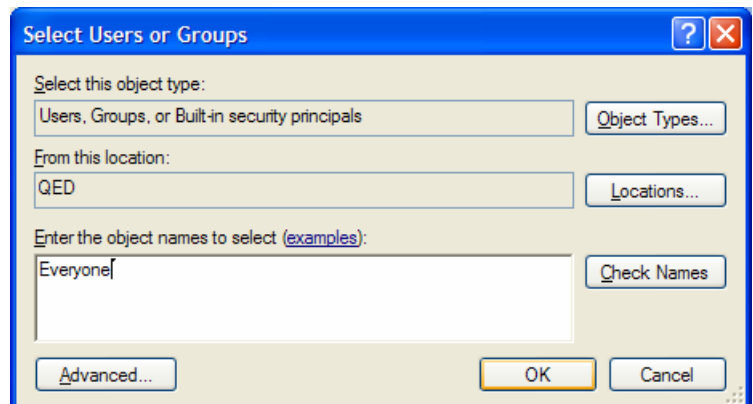


Resolution 1, cont.

5. Click **OK**, confirm, and go back to the folder.



6. Right-click the file **Sentinel.mdb** and select Properties. This time, you should see a Security tab. Select it and click **Add**.
7. In the Textbox, type **Everyone** and click **OK**.



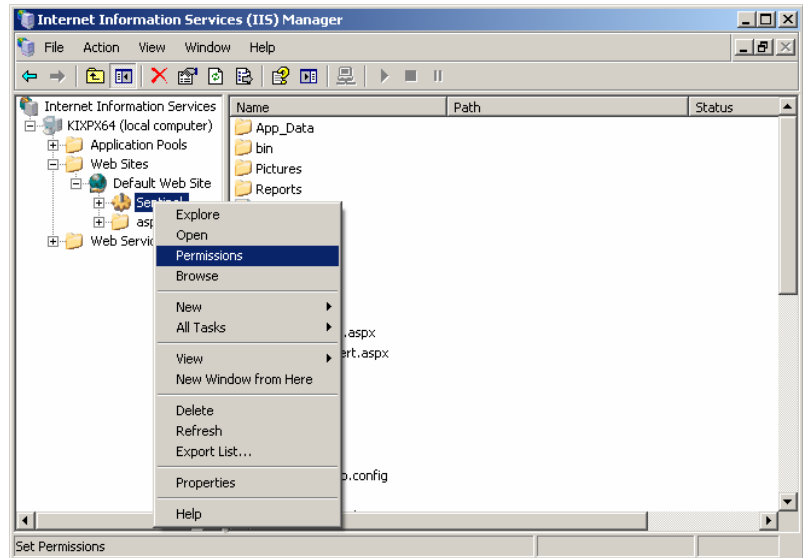
8. Click **Everyone** and select the checkbox **Full Control** under **Allow**. It automatically marks all other checkboxes under **Allow**. Click **OK**.
9. Repeat these actions with the file **Sentinel.ldb**.

Now you can access the Web interface of Sentinel with the service running.

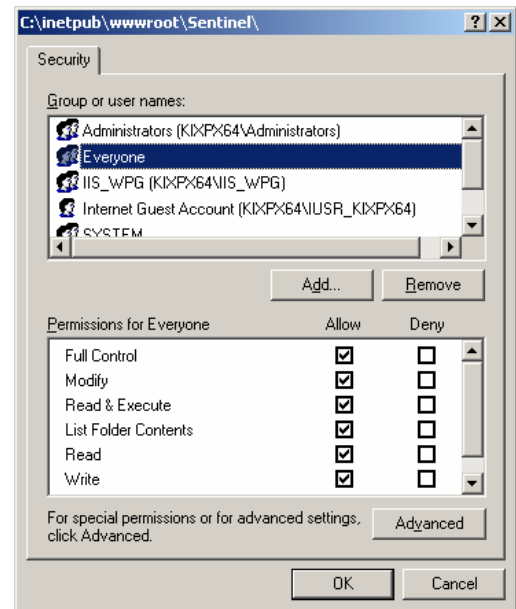
Resolution 2

If the previous steps did not resolve the problem, try this:

1. Open IIS Manager and expand the master server node (the Servername node).
2. Under Web Sites → Default Web Site, right-click **Sentinel** and select **Permissions**.



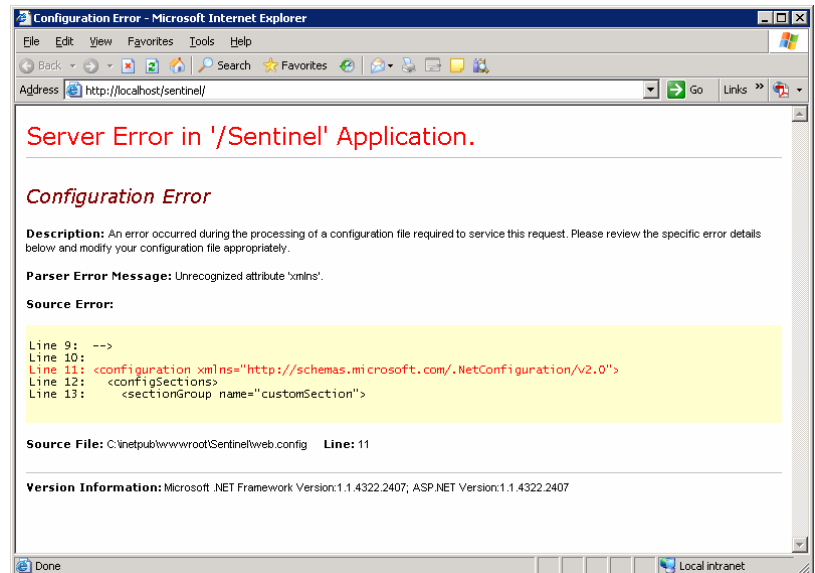
3. Click **Everyone** and select the checkbox **Full Control** under **Allow**.



Configuration Error

Symptoms

When trying to start the Sentinel web page, you get the following error:

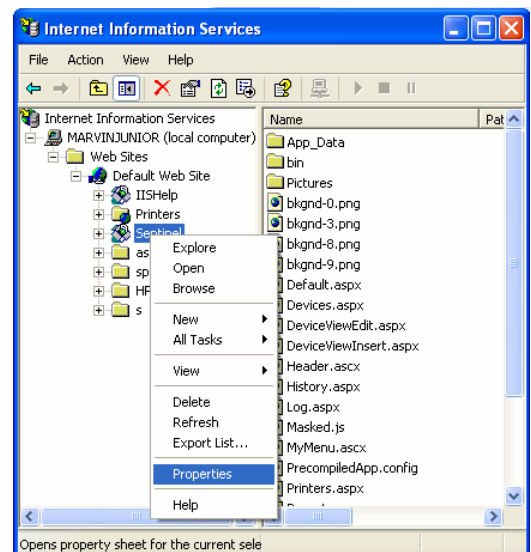


Cause

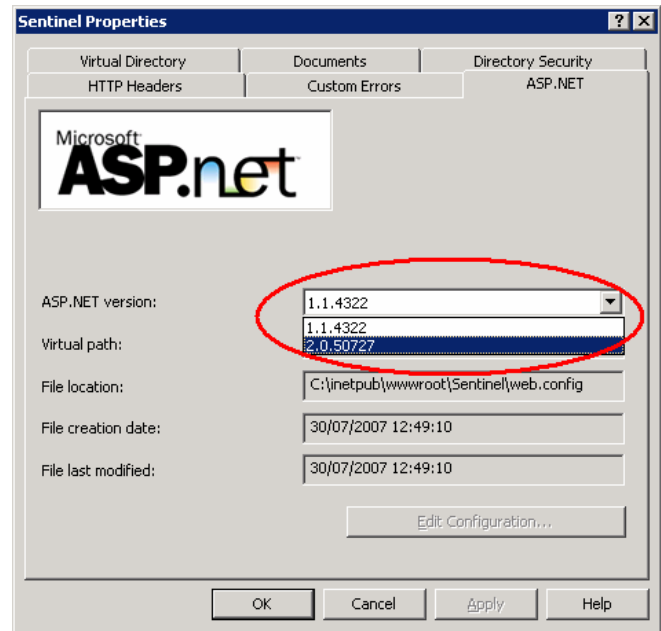
This error occurs when the Sentinel is using after the DotNet Framework 1.4 instead of the DotNet Framework 2.0.

Resolution

1. Go to IIS Settings (Start → Settings → Control Panel → Administrative Tools → Internet Information Services).
2. Expand **Local Computer\Web Sites\Default Web Site**. Right-click **Sentinel** and select Properties.



3. Go to ASP.NET tab and make sure that the ASP.Net Version is 2.X.



Service Unavailable Error

Symptoms	When trying to start the Sentinel web page, you get the error: Service Unavailable .
Cause	This issue may occur if the server that is running Microsoft Internet Information Services (IIS) 6.0 is also a domain controller. The problem occurs because the Application pool is using the NT Authority\Network Service account, and the NT Authority\Network Service account may not have permissions to access the required folders.
Resolution	<p>To resolve this problem, manually set permissions on the folders for the IIS_WPG group, and then set permissions on the folders for the NT Authority\Network Service account.</p> <p>To set permissions on the folders for the IIS_WPG group and the NT Authority\Network Service account:</p> <ol style="list-style-type: none">1. Start Windows Explorer, and then open the folder %systemroot%\Help\iisHelp.2. In the right pane, right-click the Common folder, and then click Sharing and Security.3. Click the Security tab, click Add, type IIS_WPG, and then click OK.4. With IIS_WPG selected, select the following checkboxes under the Allow column, and then click OK:<ul style="list-style-type: none">• Read and Execute• List Folder Contents• Read

5. Repeat the above step with **NETWORK SERVICE** instead of IIS_WPG.
6. Open the folder %systemroot%\system32\inetsrv.
7. In the right pane, right-click the ASP Compiled Templates folder, and then click **Sharing and Security**.
8. Click the Security tab, click the **IIS_WPG** group, and then select the **Full Control** checkbox under the **Allow** column. Click **OK**.
9. Repeat the above step with **NETWORK SERVICE** instead of IIS_WPG.
10. Open the folder %systemroot%.
11. In the right pane, right-click the IIS Temporary Compressed folder, and then click **Sharing and Security**.
12. Click the Security tab, click the **IIS_WPG** group, and then select the **Full Control** checkbox under the **Allow** column. Click **OK**.
13. Repeat the above step with **NETWORK SERVICE** instead of IIS_WPG.
14. After you have completed these steps, restart the IIS Admin service from the Services snap-in or from the Computer Management snap-in.

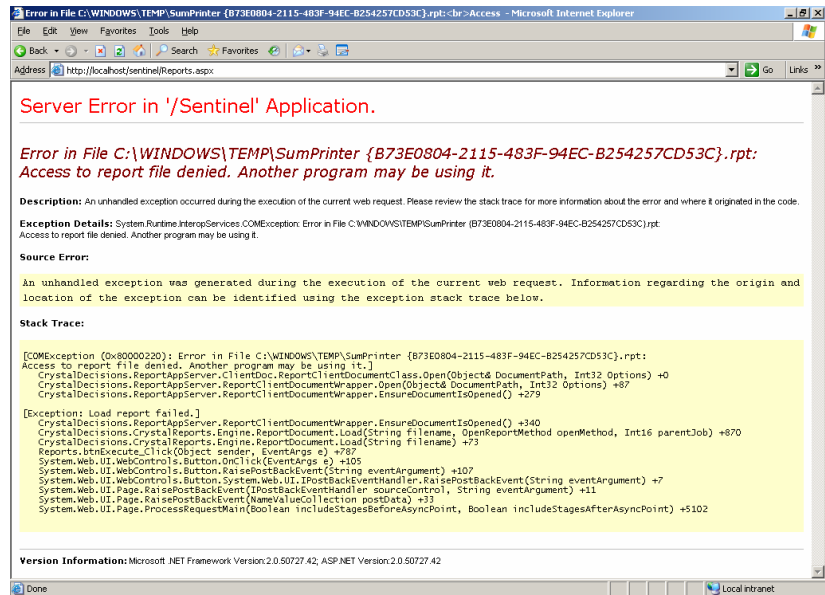
Job ID number is inconsistent or not advancing

Symptoms	Job IDs appear incorrect or the same for several jobs.
Cause	<p>Sentinel saves the last job number as a key in the Registry. This key must have write access permission to all the users using the system. If you forgot to allow writing access for all users (usually full control for everyone for this specific Registry key), then Sentinel can't advance the last job ID and the job numbers remain the same.</p> <p>Another possibility is that Sentinel can't access the Registry key at all. In this case, Sentinel assigns a random number as a job ID, but if there are many jobs, the numbers can sometimes collide.</p>
Resolution	Add a writing permission to the Sentinel Registry key as described in the installation process.

Error in file C:\WINDOWS\TEMP when trying to make reports

Symptoms

When trying to make any report from the sentinel system, the following error is received:



Cause

Sentinel is using Crystal Reports to create its reports, and it requires access to the Windows temp folder to make some temporary calculations before generating the reports. This error occurs when Crystal Reports doesn't have access to the Windows temporary folder (usually **c:\windows\temp**).

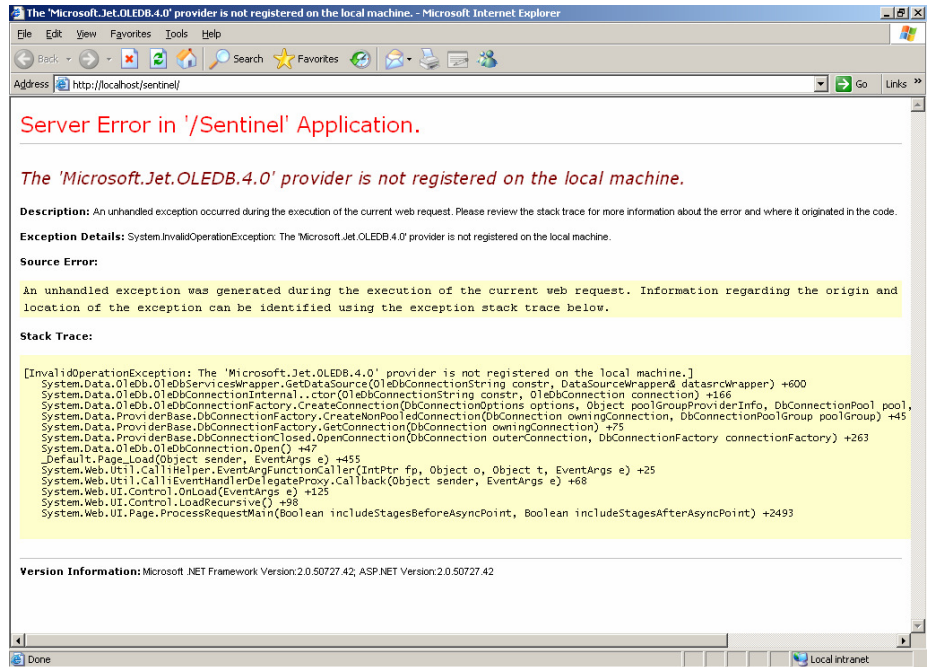
Resolution

Add a writing permission to the Windows temp folder as described in the installation process.

The 'Microsoft.Jet.OLEDB.4.0' provider is not registered

Symptoms

When running the Web interface, the following error appears in the browser:



Cause

This error occurs if there is no correct ODBC driver installed that Sentinel can use to reach the Access database. This usually occurs if you are running x64 operating system that has no such ODBC driver.

Resolution

Follow the installation instructions for x64 operating systems in order to configure Sentinel to work with SQL express database instead of with Access.

The process cannot access the file

Symptoms

You can't use the Web interface since the default website is stopped, but when you go to the IIS Manager and try to start the website, you get the following message:

The process cannot access the file because it is being used by another process.

Cause

This error usually occurs when the Web port (usually port 80) is taken by another application.

Resolution

Refer to the following article for assistance:

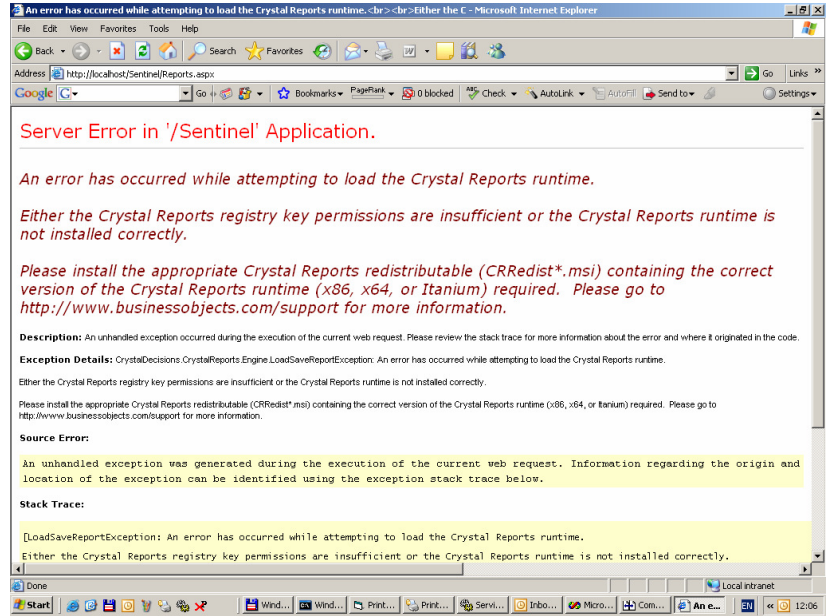
<http://support.microsoft.com/kb/890015>.

Look for applications that may use the Web port (such as Skype) and close them.

An error occurs when trying to load Crystal Reports

Symptoms

When trying to generate any Sentinel report, the following error occurs:



Cause

This error usually occurs when the wrong Crystal Reports runtime is installed, usually when your operating system is x64 and the installed Crystal Reports runtime is the 32-bit version.

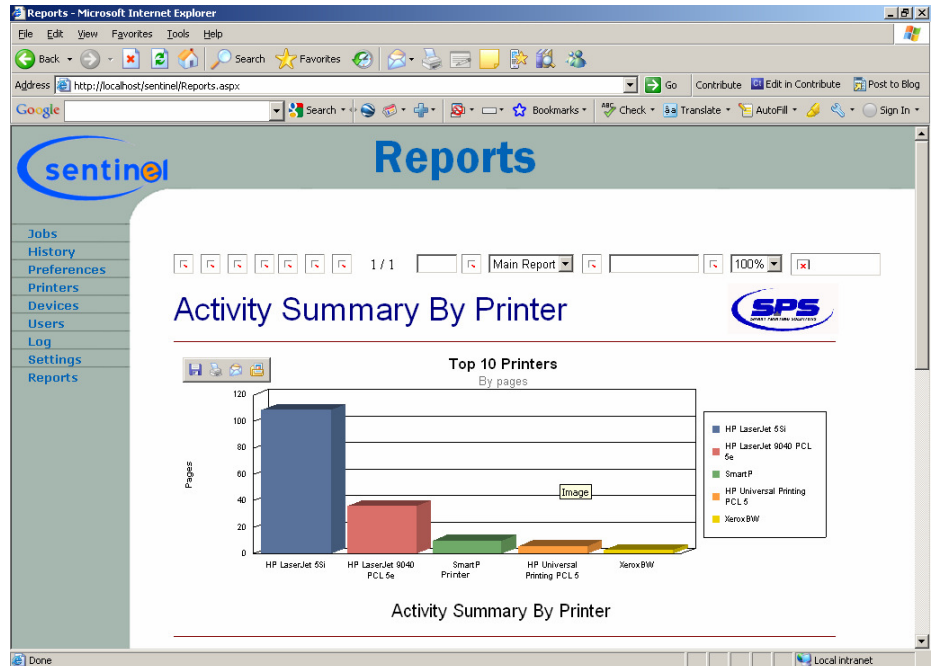
Resolution

Follow the installation instructions (*Installing on x64 Platforms* on p. 9), and install the 64 bit version of Crystal Reports runtime.

The Reports toolbar buttons are missing

Symptoms

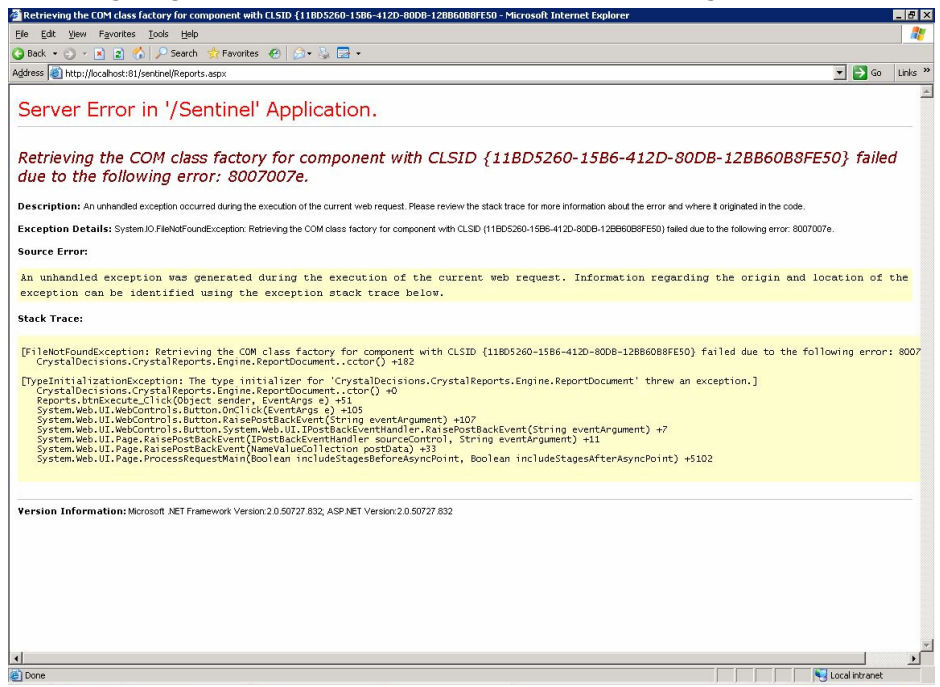
When trying to generate any Sentinel report, the report appears, but the control buttons of the toolbar are missing:



Cause	This error occurs when the virtual directory "aspnet_client" is missing.
Resolution	Under the folder c:\inetpub\wwwroot\ , there should be a folder called aspnet_client . If the folder exists physically but doesn't exist in the IIS manager under the Default Web Site, add it by selecting New → Virtual Directory . If the folder is missing physically, contact your software vendor to receive the content of the folder and create it.

Error when issuing a report

Symptoms When trying to generate any Sentinel report, the following error appears:



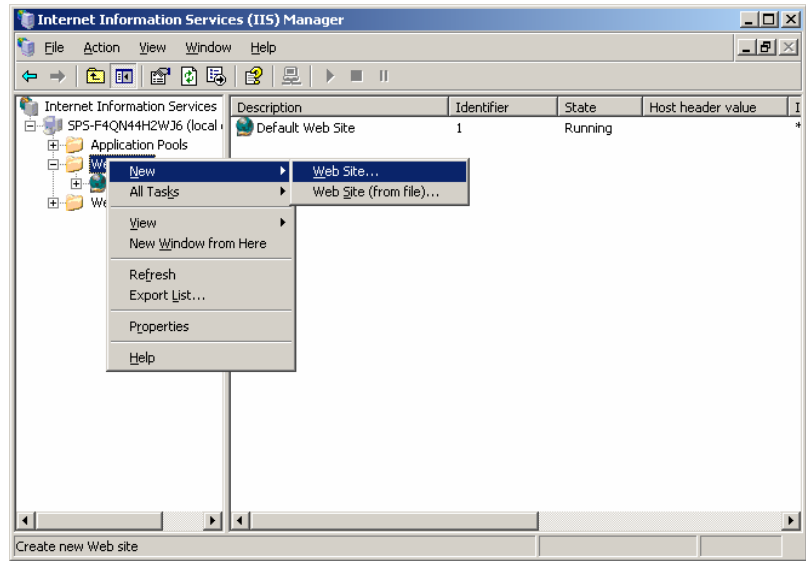
Cause	This error occurs when the Crystal Reports installation is corrupted.
Resolution	You need to reinstall Crystal Reports. The MSI file can be downloaded from: http://www.smartprinter.co.il/files/CrystalReportsRedist2005_x86.zip If you are using 64-bit version, make sure to install the appropriate file.

Default website is used by another application on the server

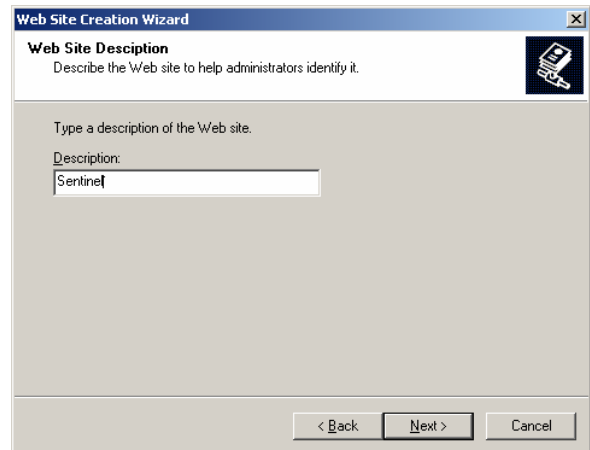
Symptoms	When logging in to the Sentinel Web page, you receive another application, or an error related to other application.
Cause	When installing Sentinel, the default installation option is to the Default Web Site, and the default port is 80 (the standard Web port). If this website or port is already in use by another application, there may be a collision between the applications and Sentinel Web page will not be presented.

Install Sentinel on a new website with a different port number as follows:

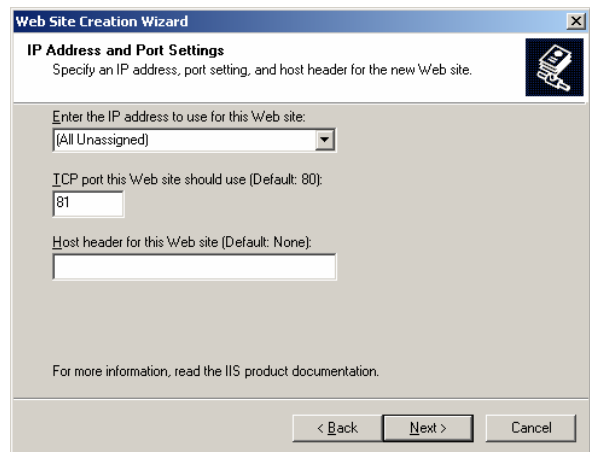
1. Open the IIS Manager and add a new website.



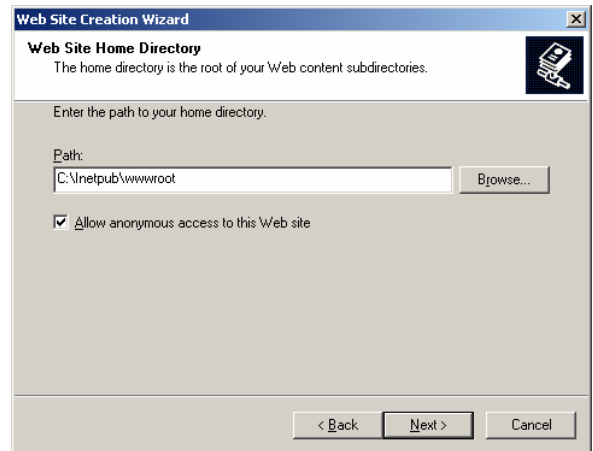
2. Click **Next** and in the following screen type the name of the site (**Sentinel**) and click **Next** again.



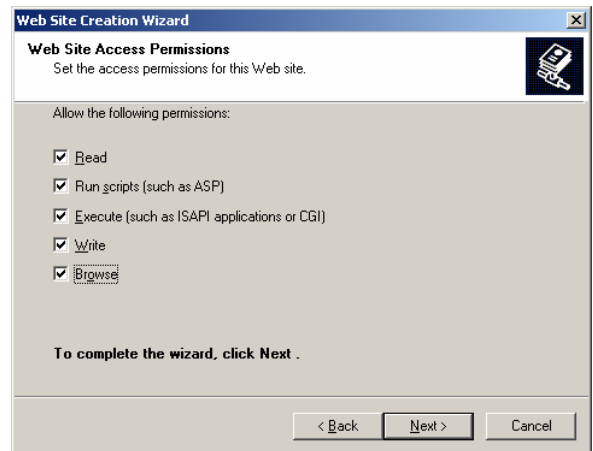
3. Change the port number for the new website to a new port (for example, 81), and click **Next** again.



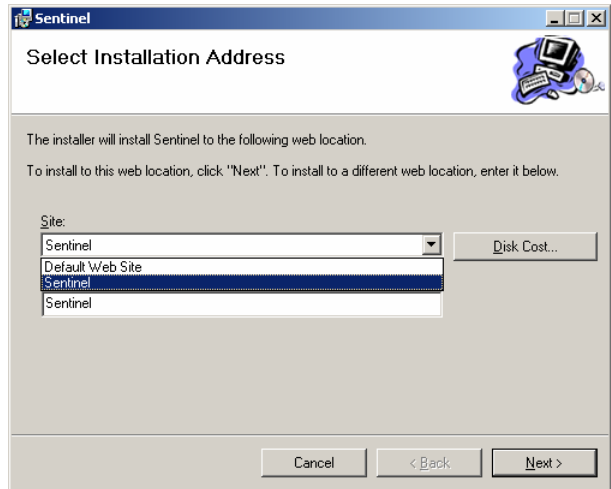
4. Type the path to the root of the new website (**c:\inetpub\wwwroot**) and click **Next** again.



5. Allow all Access permissions and click **Next** again.



6. Confirm the warning message and click **Finish** to close the wizard.
 7. Uninstall Sentinel from the Add/Remove Programs dialog box.
 8. Start the Sentinel setup program to reinstall it. In the Select Installation Address dialog box, from the Site list, select **Sentinel (not the Default Web Site)**.
-



9. Continue with the installation instructions as described in *Installing Sentinel Server Software on Windows Server 2003* on p. 3 until successfully completing all installation steps.
10. When trying to open the Web interface of Sentinel in a browser, make sure you are using the correct port to the website; for example: **http://localhost:81/sentinel**

New print jobs don't appear in the Waiting Jobs list

Symptoms When printing from the server on which Sentinel is installed, the new print jobs appears in the Web interface, but when printing from other workstations using other user logins, the jobs don't appear in the waiting Jobs screen.

Cause When printing from other workstations to Sentinel, two actions are performed:

- F and H files are created in the folder **c:\sentinel\queue**.
- A process (Submitter.exe) is run on these files. The process inserts the information about these files into the database.

There are two variations for this error: either the files don't appear in the queue folder at all, or the files appear in the queue folder but the information is not recorded into the database.

Resolution

1. If the files don't appear in the queue folder, add permissions for this folder to **Everyone** and give Full Control to the folder (usually **c:\sentinel\queue**).
2. If the files appear in the queue folder but are not recorded into the database, try to manually record them into the database using the command:

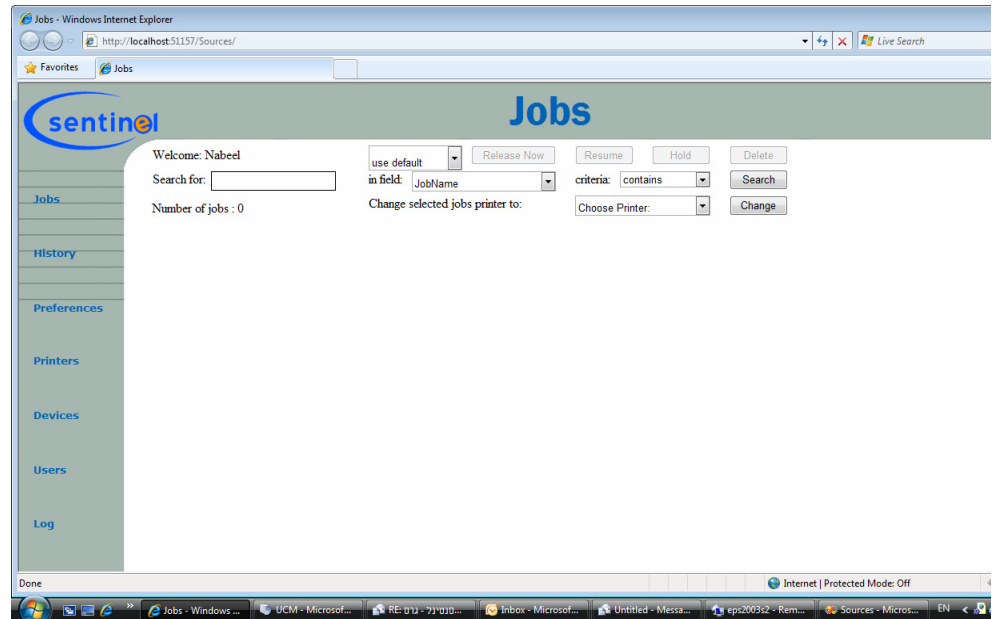
```
c:\sentinel\submitter.exe c:\sentinel\queue\Hxxx
```

(where **xxx** is the file number). If the file is recorded now, then it means that the print process which runs under the user's login name don't have permissions to run the submitter process, try to give permissions for **Everyone** as Full Control in the folder **c:\sentinel**.

3. If the manual submission of the file (running the DOS command as described above) fails as well, check that the connection string to the database is correct in the Registry (under the Registry key: **HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Sentinel\secure\DbConnectionString**).

Left-hand menu appears with strange spacing**Symptoms**

When starting the Web interface of Sentinel in some versions of Internet Explorer, the spacing of the left-hand menu is excessive:



Cause

Internet Explorer is misinterpreting the Sentinel interface.

Resolution 1

For small installations (limited number of users), you can correct the problem at each user workstation as follows:

From the browser **Tools** menu, select **Compatibility View**.

For larger installations with many users, it is more efficient to make the changes centrally (on the Sentinel server). You can add a custom HTTP response header at the website level, at the folder level, or at the virtual director level in IIS.

For IIS 7 on Windows Server 2008:

1. Start IIS Manager (Start → Run, type **inetmgr**, and click **OK**).
2. Under **Connections**, double-click the server you want, then double-click **Sites**.
3. Select the website, folder, or virtual directory where you want to add the custom HTTP response header.
4. Under *<website name> Home*, in the **IIS** section, double-click **HTTP Response Headers**.
(where *<website name>* is the placeholder for the actual name of the selected website)
5. Under **Actions**, click **Add**.
6. In the **Name** box, type **X-UA-Compatible**.
7. In the **Values** box, type **IE=EmulateIE7** and click **OK**.

For IIS 6 and Earlier Versions:

1. Access IIS settings (Start → Run, type **inetmgr.exe** in the Run dialog box, and click **OK**).
2. Expand the server that you want, then expand **Web Sites**.
3. Right-click the website, the folder, or the virtual directory where you want to add the custom HTTP response header, and click **Properties**.
4. Select the HTTP Headers tab. Under **Custom HTTP Headers**, click **Add**.
5. In the Add/Edit Custom HTTP Header dialog box, type **X-UA-Compatible** for the custom header name and **IE=EmulateIE7** for the custom header value and click **OK**.



6. Click **OK** again to close the IIS settings.

Unknown User

Symptoms	When a user places a card or enters a code at a device controller, the error unknown user is displayed on the device controller LCD.
Cause	This occurs if a new user attempts to use a card before actually sending a print job.
Resolution	Have the user send a print job.