Sentinel
User Guide

Version 2.63

Smart Printing Solutions

July 2010

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

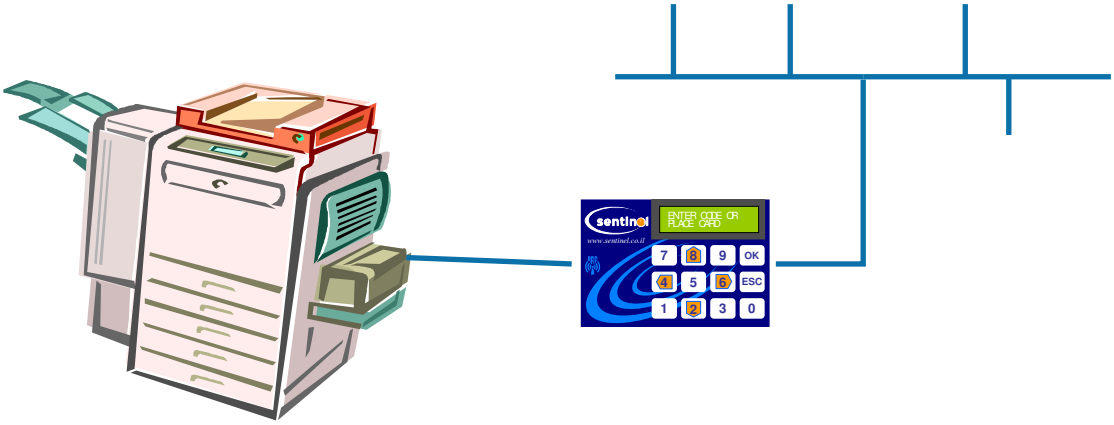
What is Sentinel?

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.



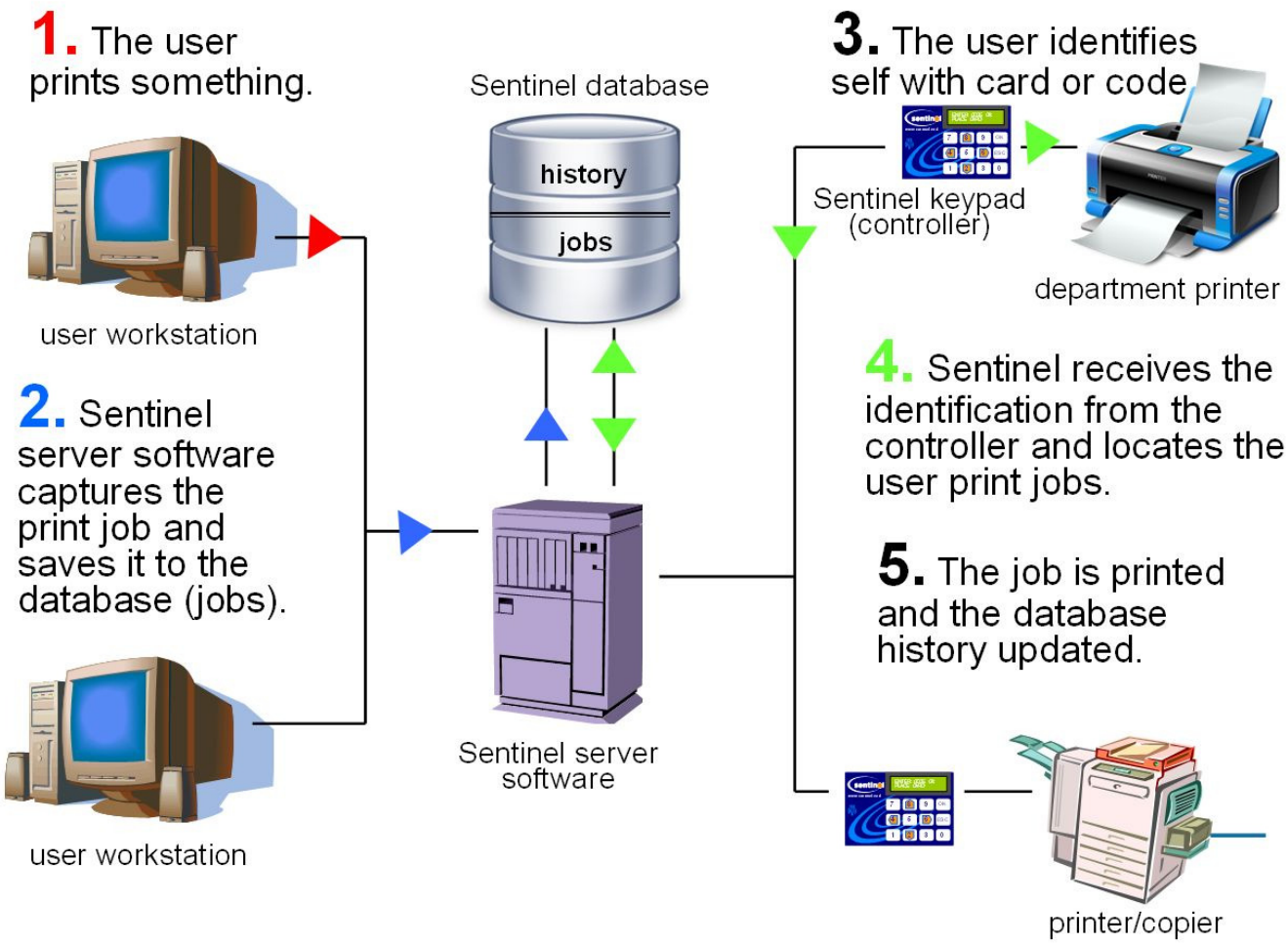
How does Sentinel work?

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:\Inetpup\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	Restrictions apply; does not support all features or capabilities and requires special configuration (see *Registry Permissions in Windows 2000/XP* on p. 10).
x64 (64-bit) platforms	Restrictions apply; Sentinel must be configured specifically for this platform (see *Installing on x64 Platforms* 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.mspx?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.

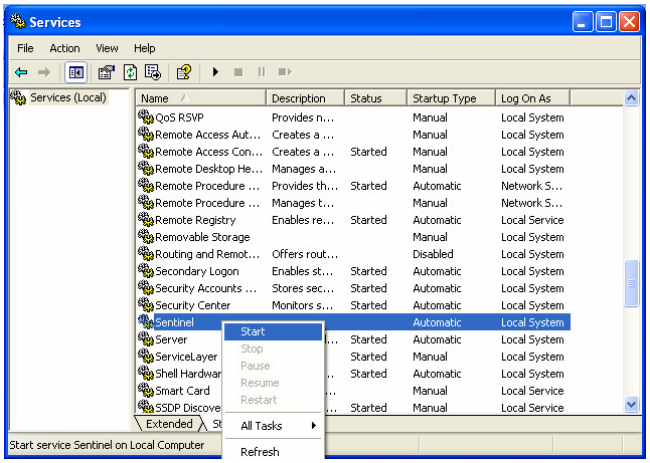
- If you must install Sentinel on a Windows XP or Windows 2000 platform, be aware that Sentinel will not be fully functional. You will also have to manually edit the Windows Registry to set certain permissions. See *Registry Permissions in Windows 2000/XP* on p. 10.
- If you must install on 64-bit platforms, 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 and follow the directions on screen. Use the default directories during the installation process.

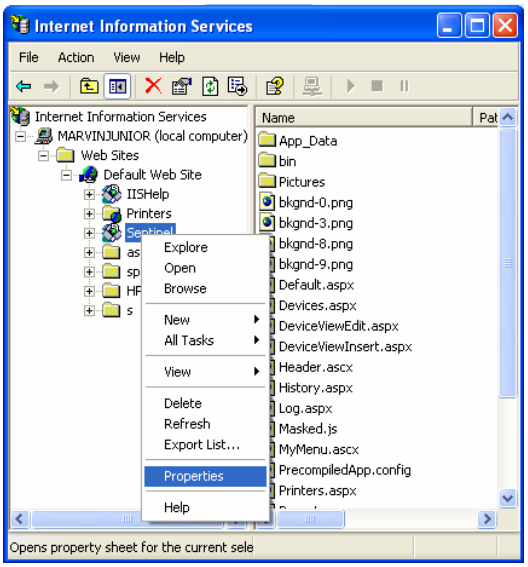
2. Go to Services (**Start → Settings → Control Panel → Administrative Tools → Services**).

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

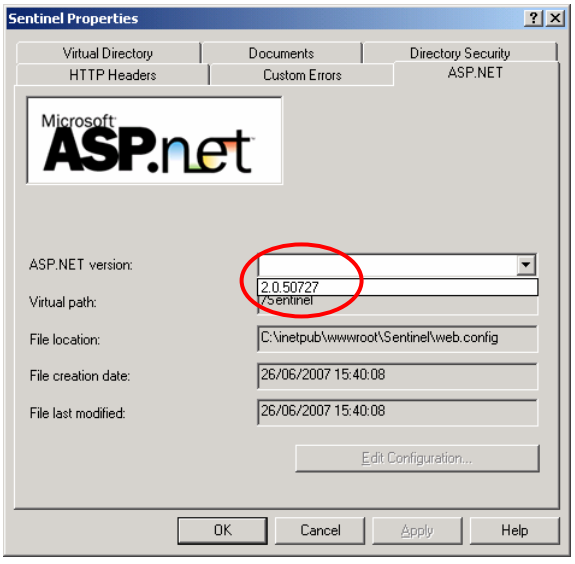
3. To start the Sentinel service, scroll down to **Sentinel**, right-clicking it, and select **Start**. If the Sentinel service doesn't exist, see *Failed to add Sentinel Service* on p. 44.



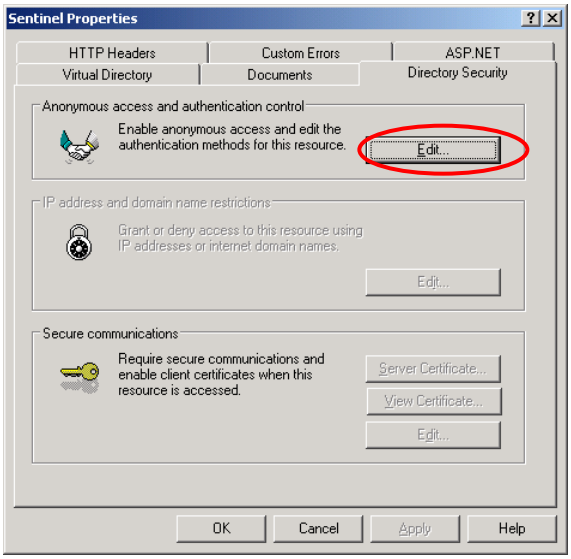
4. Go to IIS Settings (Start → Settings → Control Panel → Administrative Tools → Internet Information Services). Expand **Local Computer\Web Sites\Default Web Site**. Right-click **Sentinel** and select **Properties**.



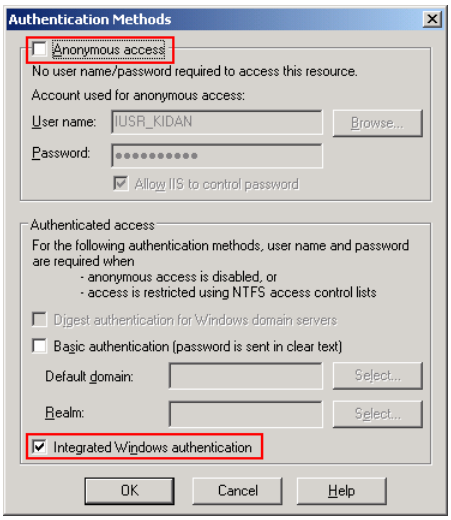
5. In the ASP.NET tab, make sure that the ASP.Net Version is 2.X.



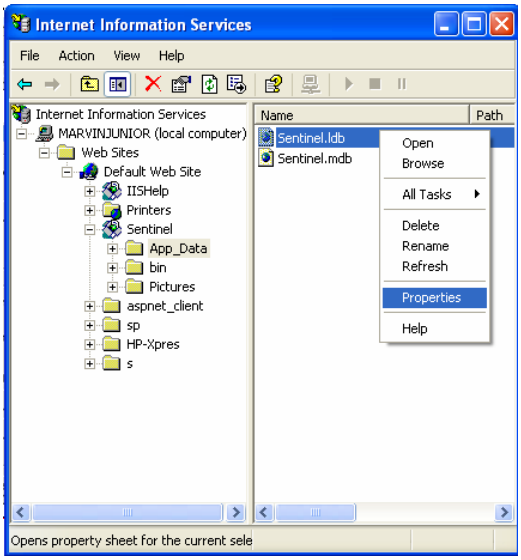
6. In the Directory Security tab, click **Edit**. This opens the Authentication Methods dialog box.



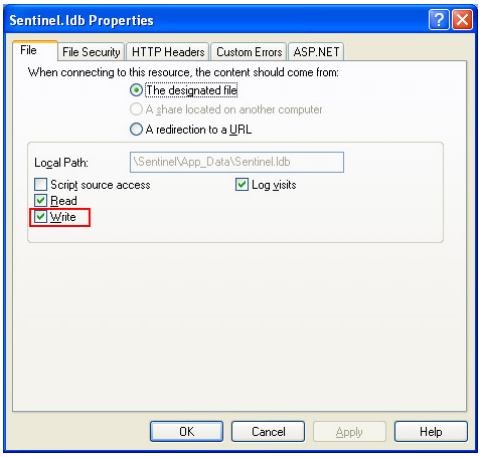
7. Make sure that **Anonymous access** is not selected and that **Integrated Windows Authentication** is selected, and click **OK**.
8. Click **OK** again to exit from Sentinel Properties.



9. 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**.

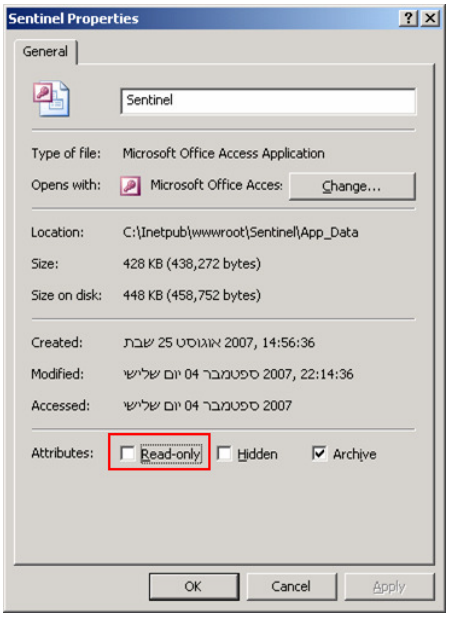


11. Repeat this process (from step 8) with **Sentinel.ldb**.
    If the file **Sentinel.ldb** doesn't exist:
    a) Start the Web Sentinel (Start → Programs → Sentinel → Web Sentinel).
    b) Ignore any errors and close the browser window. The file **Sentinel.ldb** should appear now.
    c) If **Sentinel.ldb**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

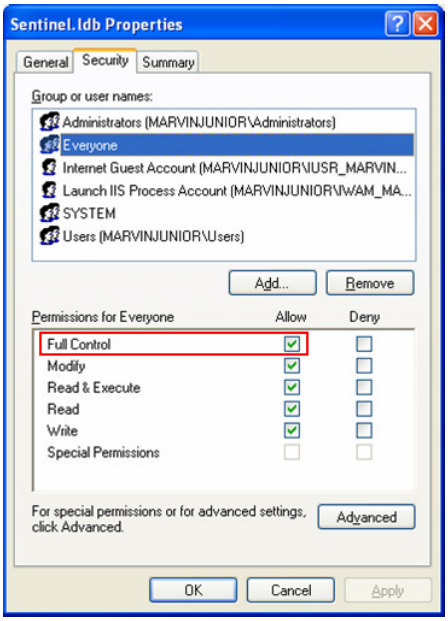
12. Go to the IIS Sentinel folder (default directory is **c:\Inetpub\wwwroot\Sentinel**) and enter the App_Data folder.

13. Right-click **Senitnel.mdb** and select **Properties**.

14. Make sure that the **Read-Only** checkbox is not selected.

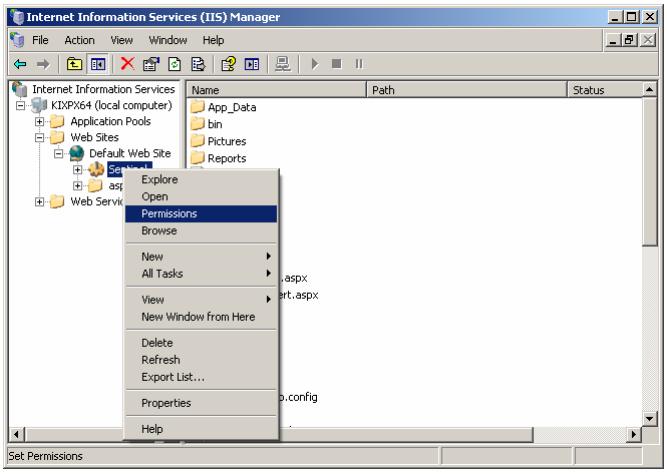


15. In the Windows Security tab (if exists in your version of Windows), click **Everyone** and select the **Full Control** checkbox.

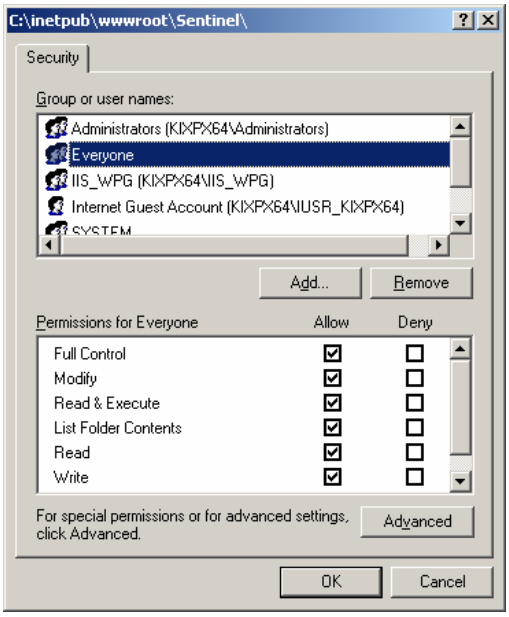


16. Repeat the process (from step 12) for the file **Sentinel.ldb**.

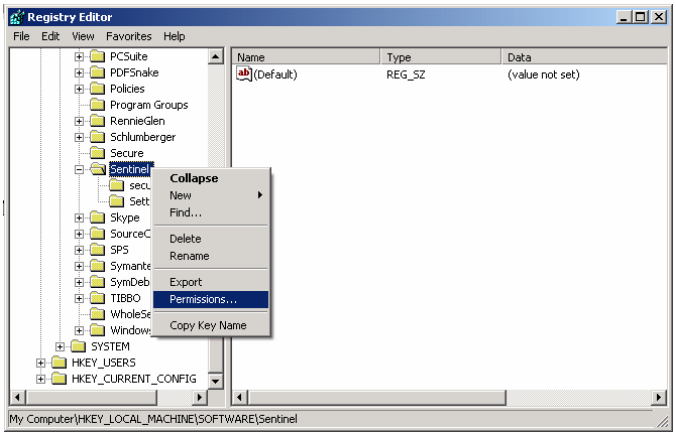
17. In the IIS Manager, expand the master server node (the Servername node). Under **Web Sites → Default Web Site**, right-click **Sentinel** and select **Permissions**.



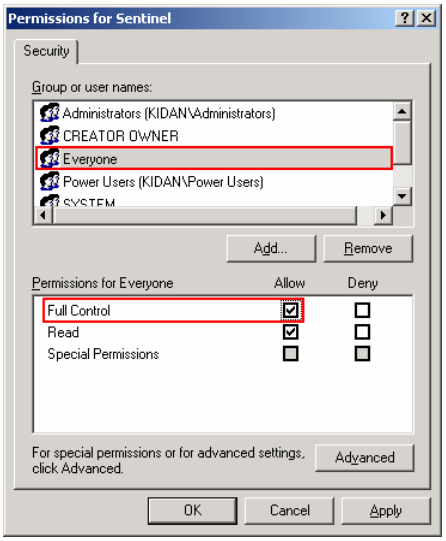
18. Click **Everyone** and select **Full Control** (under the Allow column).



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**.

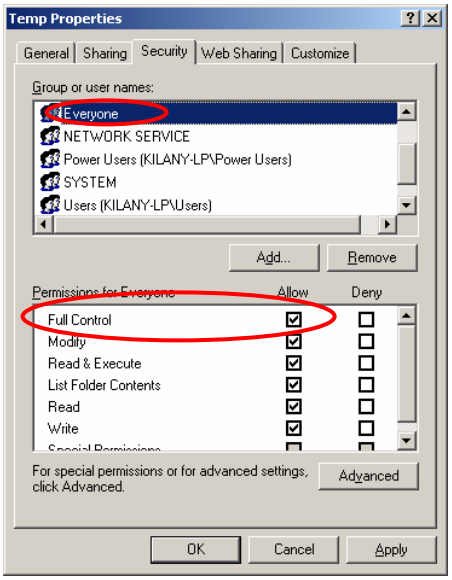


20. Allow all users (**Everyone**) Full Control over this Registry key.



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. 11.

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)
    - DotNet Framework 2.0 SP2 for x64
    - Windows Installer 4.5
    - DotNet 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. 11

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

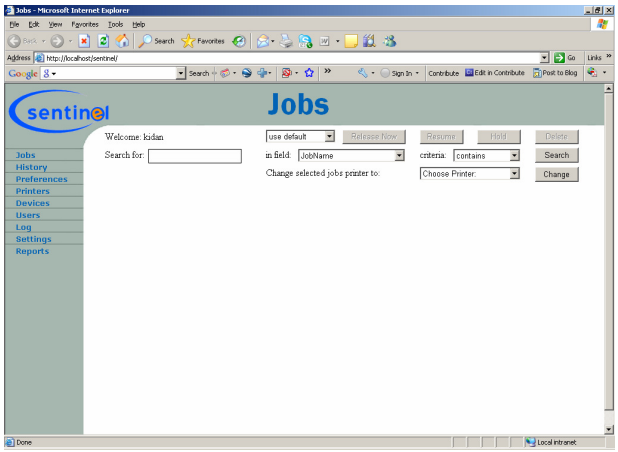
Once Sentinel is installed, verify that it is running.

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

2. If you see a main screen similar to this, congratulations! Sentinel is up and running!

   Note! It may take up to 30 seconds to appear.

   If the Sentinel main screen doesn't appear, see *Troubleshooting* on p. Troubleshooting44.



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**).

The script creates four additional rules for Sentinel on the firewall.

If you are using a third-party firewall, contact your system administrator or security administrator.

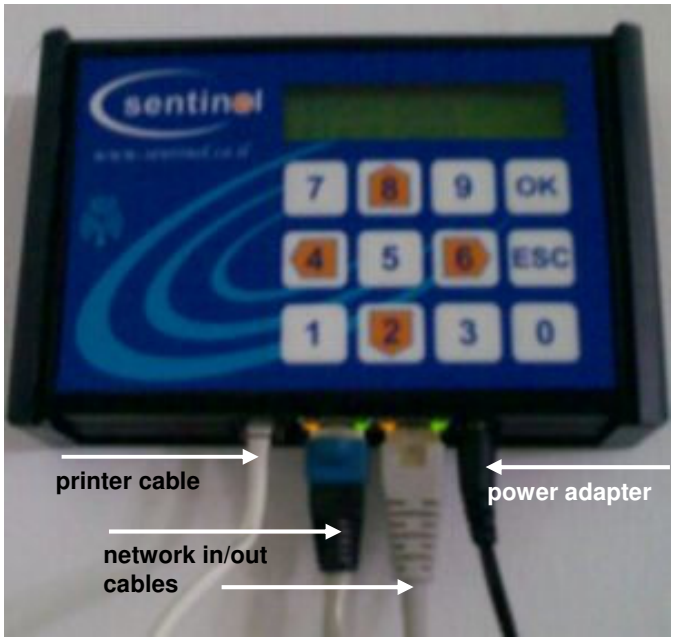
Installing Device Controllers

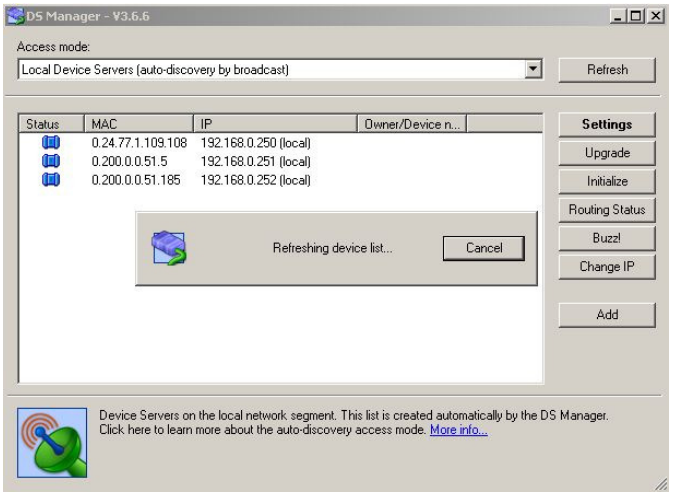
Each physical printer, copier, scanner, or combination unit, needs to be connected to a device controller to be part of the Sentinel system.

1. Find a position for the device controller that will allow convenient access for everyone (for example, don't place it too high on the wall, or in a place that requires people to lean across a large printer).
2. Make sure that you have the correct mounting option (contact your Sentinel vendor for details; there are several different wall-mount and desk-mount options).
3. Make sure that you have the correct printer cable (contact your Sentinel vendor for details).
4. Connect the network in/out cables to the two standard RJ-45 ports. These ports are interchangeable, so it doesn't matter which you use for *in* and which for *out*.
5. Attach the 9v power adapter to the device controller and plug it in to a power source.

   When the device controller is plugged in, the message "Enter Code or Place Card" appears on the LCD.
6. 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.

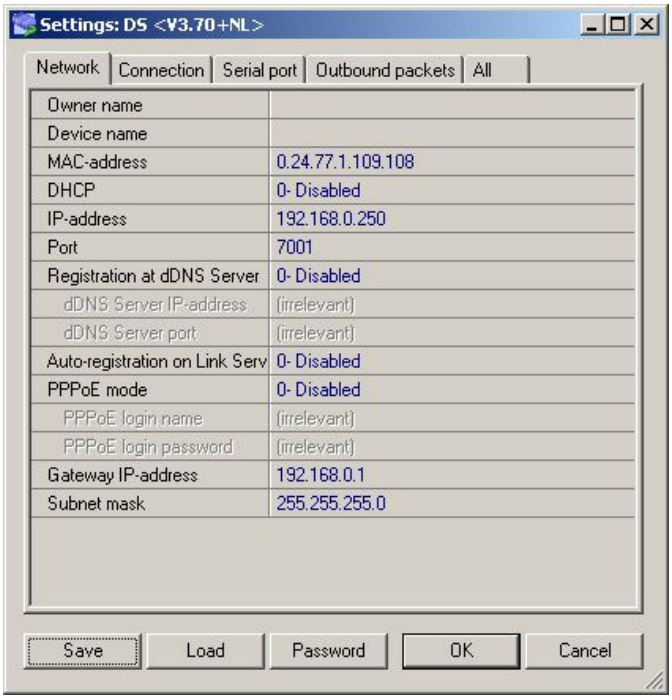




7. To change the settings of a device controller, click it on the list and click **Settings**.

   The Settings dialog box appears.

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

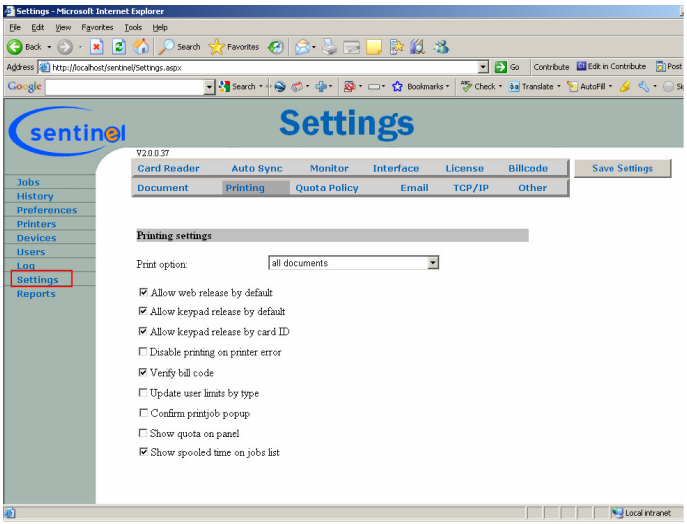


Configuring the Sentinel Server

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. 23).

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	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. 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.
• 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.
• Convert Decimal to Hex	Converts the card number from decimal to hexadecimal representation.
• Read characters from card (Right)	Takes only the X rightmost characters of the card number.
• Read characters from card (Left)	Takes only the X leftmost characters of the card number.
• Convert Hex to Decimal.	Converts the card number from hexadecimal to decimal representation.
• Ignore card leading zero	Ignores all leading zeros read by the card reader.
• Increment constant number	Mathematically adds the card number that was read to this number.
• 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
• 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.
• Clear history after [X] days	How long Sentinel keeps print jobs on the History screen.
• Clear log after [X] days	How long Sentinel keeps entries in the log.
• 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 *from* and *to* 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.
• AutoPrint TimeOut	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). 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. AutoPrint jobs, however, bypass the device controller. The server sends the print job request to the database and immediately tries to release it. 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. 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.
• SNMP TimeOut	This is only relevant when SNMP Count (see p. 23) is selected on a device. SNMP continually monitors printer status, completion of jobs, number of pages printed, etc. Since Sentinel adds an additional communication chain to the process (*print request → Sentinel server → Sentinel database*, then *user recognition at device controller → Sentinel server → Sentinel database → release job*), 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. 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.

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.).
• Domain Name	The domain name that has permission to access the AD.
• 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.
• AD User	The username with permission to access the AD.
• AD Password	The password associated with this username.
• 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
• 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.
• Card ID Field Name	The name of the field in the SQL database that contains data to be mapped to the card ID.
• First Name Field	The name of the field in the SQL database that contains data to be mapped to the user's first name.
• Last Name Field	The name of the field in the SQL database that contains data to be mapped to the user's last name.
• Table Field Name	The name of the table in which the users are listed.
• 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
• Print Option	If several print jobs are waiting for the user, you can select one of the following options: • 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.
• Allow Web release by default	If selected, users are able to release print jobs from the Web interface.
• Allow keypad release by default	If selected, users are able to release print jobs by entering their keypad code on the device controller.
• 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.
• 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
• 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.
• 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.
• 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.
• Show quota on panel	If selected, after user identification, the user's quota (and remaining pages) is shown on the device's display.
• 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, ***not*** 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
• 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.
• Monitor and activate the Sentinel service	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. If this checkbox is selected, you must specify the IP address of the Sentinel server. **Note!** 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.
• 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
• Default Quota Policy	The quota policy automatically assigned to new users.
• (policy to edit/delete)	Select the policy from the list. Click Add Policy to create a new policy. • 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
• Seconds before AutoRefresh (0 for never)	If selected, the Web interface refreshes automatically every X seconds.
• (policy to edit/delete)	Select the policy from the list. Click Add Policy to create a new policy. • 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.
• Send Hebrew text	If selected, the Sentinel screen and reports will allow Hebrew characters. **Note!** 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
• From Email Address	This is the email address that the messages will come from; for example, sentinel@yourcompany.com.
• Email Address	The email address of the person to receive the messages.
• 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.
• Error	These are errors that occur in the Sentinel system (server, database, etc.).

Parameter	Explanation
• 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
• Cluster Name	Any name used to identify the cluster.
• Application System User	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. To work around this problem, some applications allow the implementers of the application to change the job name: 1. Change the job name to **username@jobaname**. 2. Enter the special application username (for example, APPLMGR) in the textbox 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.
• 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.
• Support multiple users	Select this if you have several print servers working with one database.
• 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.

Basic Functions

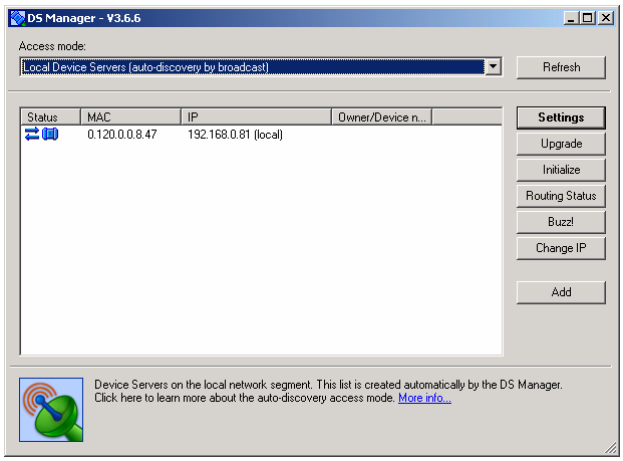
Once you have performed the initial configuration of the system, you can begin to add devices and users to the system.

Adding a New Device

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

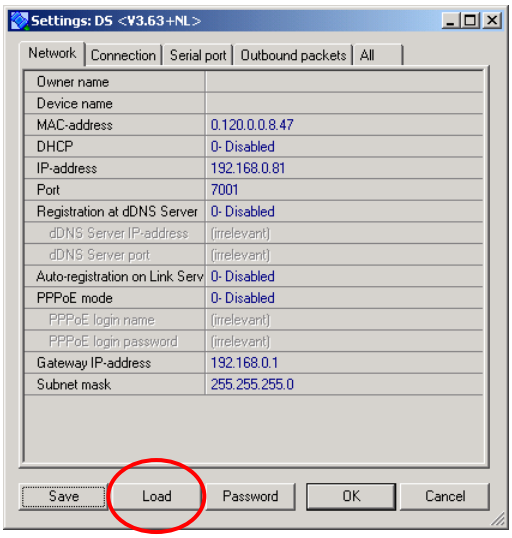
1. Attach the new device to the network.
2. Select **Start → Programs → Sentinel → DS Manager**.

   The DS Manager launches and begins looking for new devices.



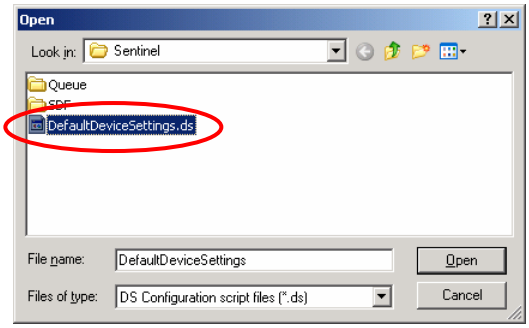
3. From the device list, double-click the device you want to configure.

   The device's settings window appears.
4. Click **Load**.



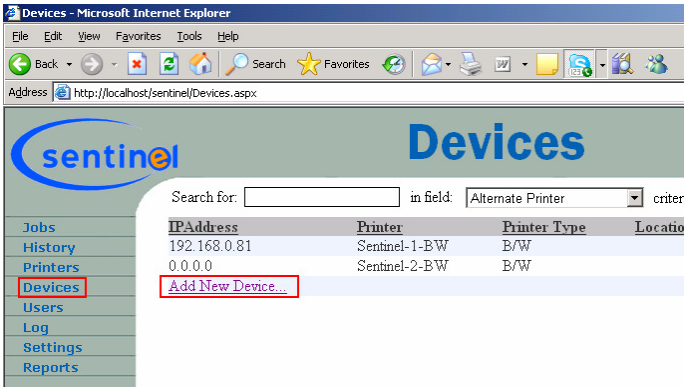
5. Select the predefined settings file from the Sentinel path.

   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: • 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
• Count PS/PCL	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.  **Caution!** 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!
• Printer Supports Duplex	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.
• Support FTP Mail	This feature allows you to scan documents to a specific user folder or email. To set up this feature: 1. Select this checkbox. A new subfolder is created in the Sentinel Queue folder (for example, **C:\Sentinel\Queue\printer**). 2. If the folder is not created, create it manually. 3. Redirect the multifunction device to scan into this folder. 4. Under each user (**Settings → Users → Edit User**), enter the appropriate values in the fields **Mail** and **Scan to Folder**. For these users, their card usage triggers Sentinel to takes the file in the printer subfolder and send it to the user email or copy it to the user folder.
• Auto Open Copier	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.
• SNMP Count	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. 16. 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.
• Delete Job on Error	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. This feature only works with specific printer models. Consult your Sentinel vendor.

Parameter	Explanation
• 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**.
• 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.

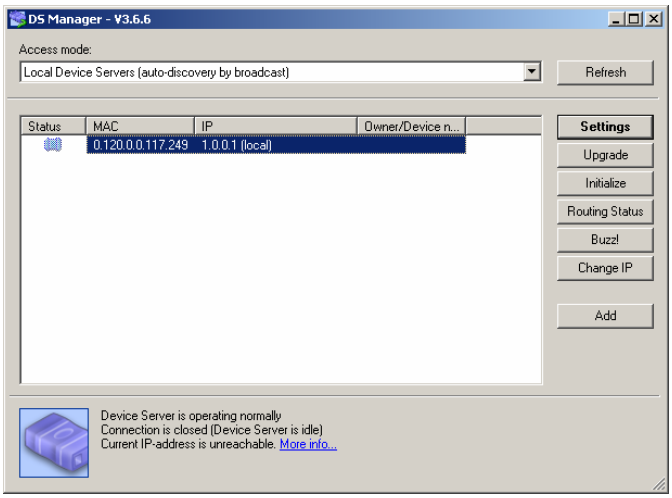
Caution!

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).

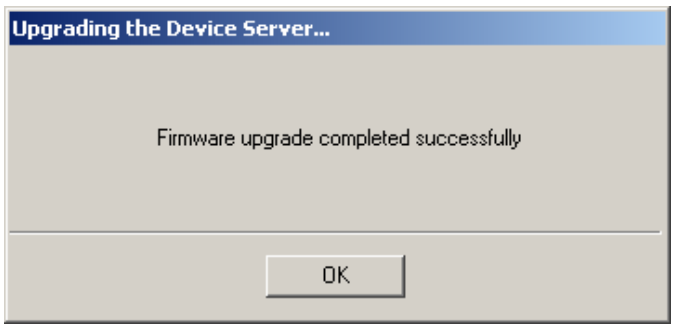
1. Attach the device you want to upgrade to the network.
2. Select **Start → Programs → Sentinel → DS Manager**.

   The DS Manager launches and begins searching for new devices.



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

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



5. 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.

Note! 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. 17.

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

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

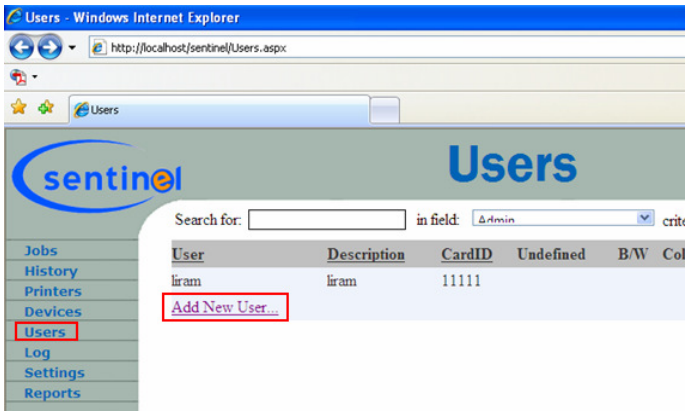
   All currently defined users appear in this table.

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

   This opens the Add User screen.

3. Complete all fields as needed (described below).

4. Click **Add**.



Parameter	Explanation
• User	Enter the name of the user. This name must be the same as the user login name on the Windows system.
• 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 *Auto Sync* on p. 17.
• 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 *Printing* on p. 18.
• 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 *Quota Policy* on p. 20.
• 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
• Force Billing Code	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.
• 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. This definition overrides the definition selected in the Device.
• Message	Enter any text. This appears on the Web interface (below the left-hand menu) for that user.
• Limits	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).

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" />
```

Note!

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, often there are fields added to the database. If you upgrade the software files only but leave the database as it is, the software may encounter errors when it searches for fields that don't exist in the older database.

To upgrade the fields of an existing database:

1. Open a command line in the DOS box.
2. Go to the folder **c:\sentinel\updatetables**.
3. Run the file **updatetbl.ex**e.

   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.
4. Make sure that the files Access.ini and **SQL.ini** exist in the same folder as the file **updatetbl.ex**e.

Sentinel Monitoring Screens

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

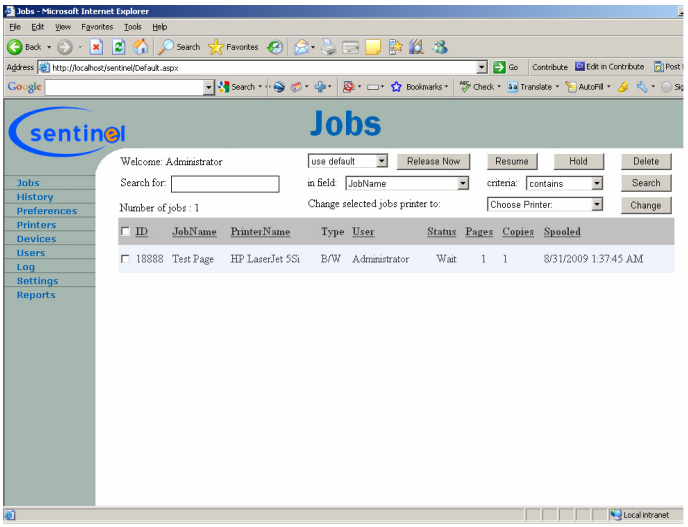
Print Jobs

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 then 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.

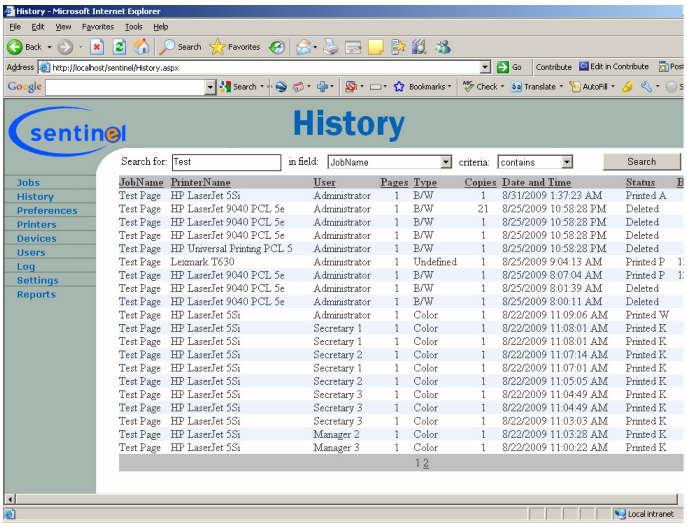
History and Archive

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.

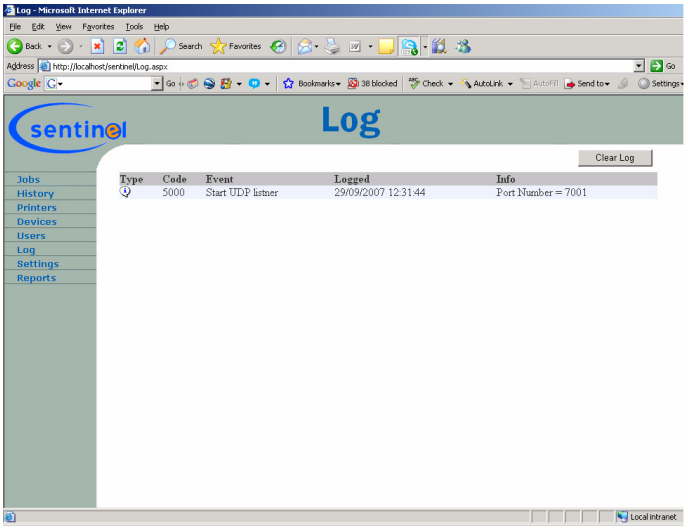


The available job statuses are:

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.



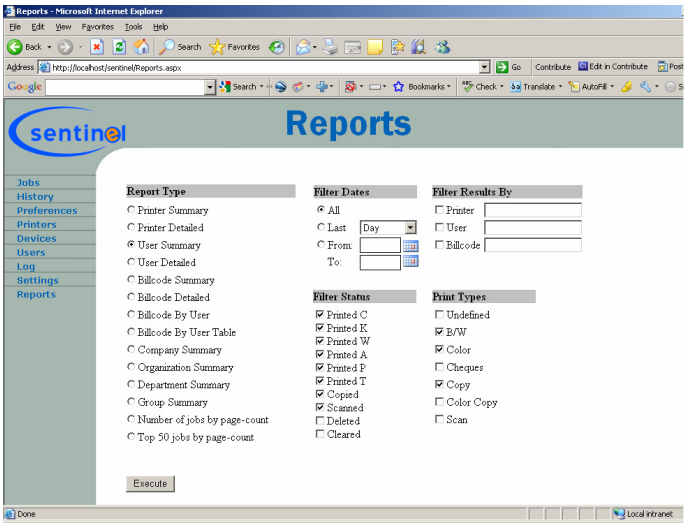
Reports

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.



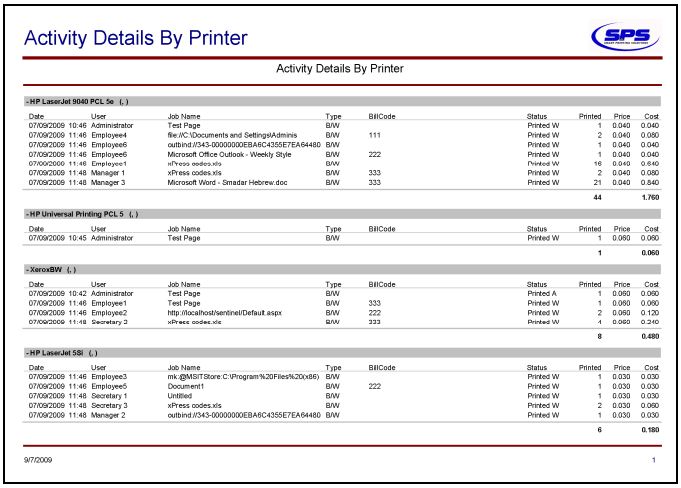
Parameter	Explanation
Filter Dates	This allows you to select a range of dates for the report.
• All	This takes all information from the database with no date limitations.
• From • To	Specifies a date range for the data (either from a starting point or to an ending point).
Filter Results By	Filter the desired report only to a specific parameter (or a combination of parameters). The parameters include:
• Printer	Generates data only for a specific printer. To specify more then one printer, use a semicolon (;) between printer names, without any spaces before or after.

Parameter	Explanation
• User	Generates data only for a specific user. To specify more then one user, use a semicolon (;) between usernames, without any spaces before or after.
• Billing Code	Generates data only for a specific billing code. To specify more then one billing code, use a semicolon (;) between billing codes, without any spaces before or after.
Filter Status	Generates data only for specific statuses. See *History and Archive* on p. 34 for an explanation of all statuses. 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.
Filter Print Types	Generates data only for specific printer types. See *Adding a New Device* on p. 23 for a description of the different printer types. The print type filter is enabled only if you select one of these reports: • 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 mode 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 (,)

Date	User	Job Name	Type	BillCode	Status	Printed	Price	Cost
07/09/2009 10:46	Administrator	Test Page	B/W		Printed W	1	0.040	0.040
07/09/2009 11:46	Employee4	file://C:\Documents and Settings\Adminis	B/W	111	Printed W	2	0.040	0.080
07/09/2009 11:46	Employee6	outbind://343-00000000EBA6C4355E7EA64480	B/W		Printed W	1	0.040	0.040
07/09/2009 11:46	Employee6	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	16	0.040	0.640
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 - Smadar Hebrew.doc	B/W	333	Printed W	21	0.040	0.840
						44		**1.760**

- HP Universal Printing PCL 5 (,)

Date	User	Job Name	Type	BillCode	Status	Printed	Price	Cost
07/09/2009 10:45	Administrator	Test Page	B/W		Printed W	1	0.060	0.060
						1		**0.060**

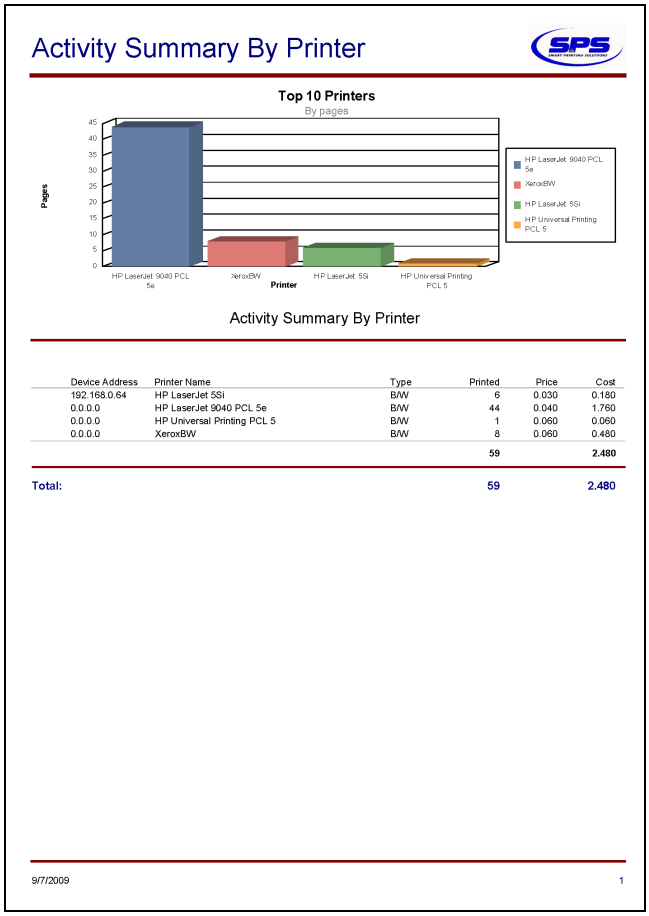
- XeroxBW (,)

Date	User	Job Name	Type	BillCode	Status	Printed	Price	Cost
07/09/2009 10:42	Administrator	Test Page	B/W		Printed A	1	0.060	0.060
07/09/2009 11:46	Employee1	Test Page	B/W	333	Printed W	1	0.060	0.060
07/09/2009 11:46	Employee2	http://localhost/sentinel/Default.aspx	B/W	222	Printed W	2	0.060	0.120
07/09/2009 11:48	Secretary 2	xPress codes.xls	B/W	333	Printed W	4	0.060	0.240
						8		**0.480**

- HP LaserJet 5Si (,)

Date	User	Job Name	Type	BillCode	Status	Printed	Price	Cost
07/09/2009 11:46	Employee3	mk:@MSITStore: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 11:48	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://343-00000000EBA6C4355E7EA64480	B/W		Printed W	1	0.030	0.030
						6		**0.180**

9/7/2009 1



Activity Summary By Printer

Activity Summary By Printer

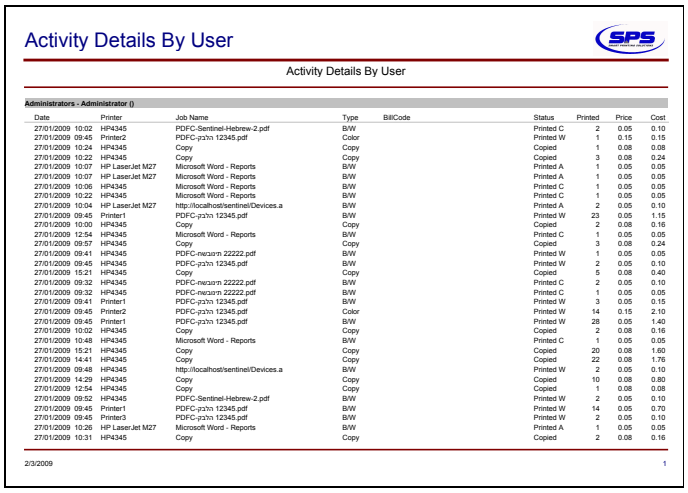
Device Address	Printer Name	Type	Printed	Price	Cost
192.168.0.64	HP LaserJet 5Si	B/W	6	0.030	0.180
0.0.0.0	HP LaserJet 9040 PCL 5e	B/W	44	0.040	1.760
0.0.0.0	HP Universal Printing PCL 5	B/W	1	0.060	0.060
0.0.0.0	XeroxBW	B/W	8	0.060	0.480
			59		**2.480**

Total: **59** **2.480**

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 mode detailed information about each of the print jobs printed by each user.



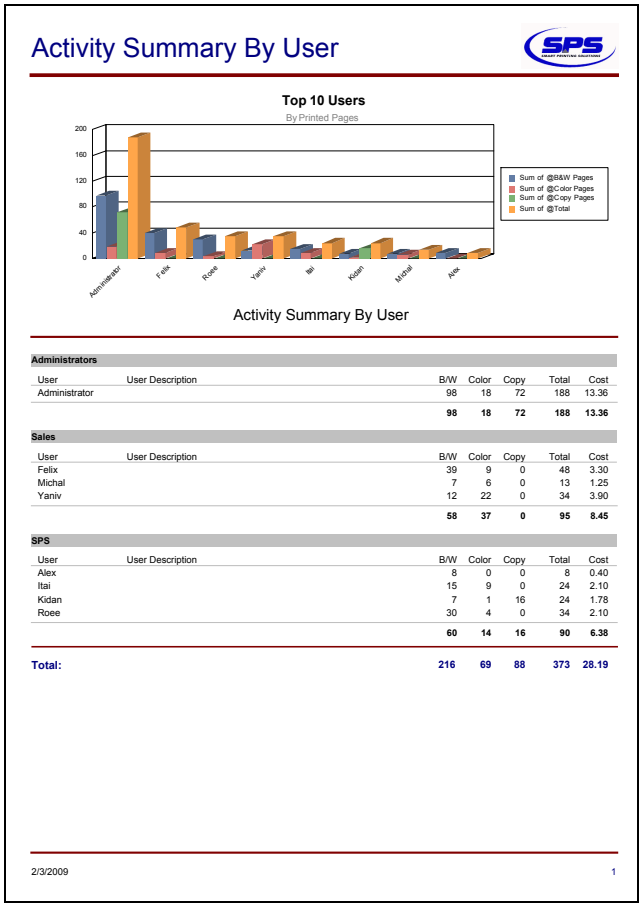
Activity Details By User

Activity Details By User

Administrators - Administrator ()

Date	Printer	Job Name	Type	BillCode	Status	Printed	Price	Cost
27/01/2009 10:02	HP4345	PDFC-Sentinel-Hebrew-2.pdf	B/W		Printed C	2	0.05	0.10
27/01/2009 09:45	Printer2	PDFC-הלבן 12345.pdf	Color		Printed W	1	0.15	0.15
27/01/2009 10:24	HP4345	Copy	Copy		Copied	1	0.08	0.08
27/01/2009 10:22	HP4345	Copy	Copy		Copied	3	0.08	0.24
27/01/2009 10:07	HP LaserJet M27	Microsoft Word - Reports	B/W		Printed A	1	0.05	0.05
27/01/2009 10:07	HP LaserJet M27	Microsoft Word - Reports	B/W		Printed A	1	0.05	0.05
27/01/2009 10:06	HP4345	Microsoft Word - Reports	B/W		Printed C	1	0.05	0.05
27/01/2009 10:22	HP4345	Microsoft Word - Reports	B/W		Printed C	1	0.05	0.05
27/01/2009 10:04	HP LaserJet M27	http://localhost/sentinel/Devices.a	B/W		Printed A	2	0.05	0.10
27/01/2009 09:45	Printer1	PDFC-הלבן 12345.pdf	B/W		Printed W	23	0.05	1.15
27/01/2009 10:00	HP4345	Copy	Copy		Copied	2	0.08	0.16
27/01/2009 12:54	HP4345	Microsoft Word - Reports	B/W		Printed C	1	0.05	0.05
27/01/2009 09:57	HP4345	Copy	Copy		Copied	3	0.08	0.24
27/01/2009 09:41	HP4345	PDFC-תיבואה 22222.pdf	B/W		Printed W	1	0.05	0.05
27/01/2009 09:45	HP4345	PDFC-הלבן 12345.pdf	B/W		Printed W	2	0.05	0.10
27/01/2009 15:21	HP4345	Copy	Copy		Copied	5	0.08	0.40
27/01/2009 09:32	HP4345	PDFC-תיבואה 22222.pdf	B/W		Printed C	2	0.05	0.10
27/01/2009 09:32	HP4345	PDFC-תיבואה 22222.pdf	B/W		Printed C	1	0.05	0.05
27/01/2009 09:41	Printer1	PDFC-הלבן 12345.pdf	B/W		Printed W	3	0.05	0.15
27/01/2009 09:45	Printer2	PDFC-הלבן 12345.pdf	Color		Printed W	14	0.15	2.10
27/01/2009 09:45	Printer1	PDFC-הלבן 12345.pdf	B/W		Printed W	28	0.05	1.40
27/01/2009 10:02	HP4345	Copy	Copy		Copied	2	0.08	0.16
27/01/2009 10:48	HP4345	Microsoft Word - Reports	B/W		Printed C	1	0.05	0.05
27/01/2009 15:21	HP4345	Copy	Copy		Copied	20	0.08	1.60
27/01/2009 14:41	HP4345	Copy	Copy		Copied	22	0.08	1.76
27/01/2009 09:48	HP4345	http://localhost/sentinel/Devices.a	B/W		Printed W	2	0.05	0.10
27/01/2009 14:29	HP4345	Copy	Copy		Copied	10	0.08	0.80
27/01/2009 12:54	HP4345	Copy	Copy		Copied	1	0.08	0.08
27/01/2009 09:52	HP4345	PDFC-Sentinel-Hebrew-2.pdf	B/W		Printed W	2	0.05	0.10
27/01/2009 09:45	Printer1	PDFC-הלבן 12345.pdf	B/W		Printed W	14	0.05	0.70
27/01/2009 09:45	Printer3	PDFC-הלבן 12345.pdf	B/W		Printed W	2	0.05	0.10
27/01/2009 10:26	HP LaserJet M27	Microsoft Word - Reports	B/W		Printed A	1	0.05	0.05
27/01/2009 10:31	HP4345	Copy	Copy		Copied	2	0.08	0.16

2/3/2009 1



Activity Summary By User

Top 10 Users

By Printed Pages

Activity Summary By User

Administrators

User	User Description	B/W	Color	Copy	Total	Cost
Administrator		98	18	72	188	13.36
		98	**18**	**72**	**188**	**13.36**

Sales

User	User Description	B/W	Color	Copy	Total	Cost
Felix		39	9	0	48	3.30
Michal		7	6	0	13	1.25
Yaniv		12	22	0	34	3.90
		58	**37**	**0**	**95**	**8.45**

SPS

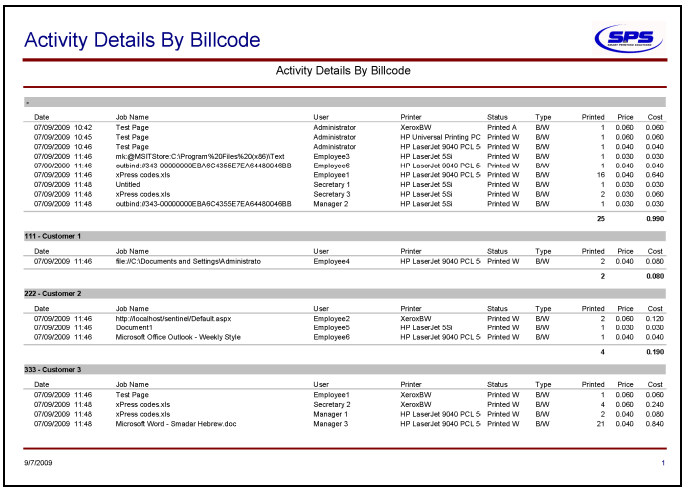
User	User Description	B/W	Color	Copy	Total	Cost
Alex		8	0	0	8	0.40
Itai		15	9	0	24	2.10
Kidan		7	1	16	24	1.78
Roee		30	4	0	34	2.10
		60	**14**	**16**	**90**	**6.38**

Total:		**216**	**69**	**88**	**373**	**28.19**

2/3/2009 1

Billing Code Reports (Summary and Detailed)

The billing code summary report shows the total amount of pages printed for a specific billing code. The billing code detailed report gives more detailed information about each of the print jobs printed for each billing code.



Activity Details By Billcode

Activity Details By Billcode

-

Date	Job Name	User	Printer	Status	Type	Printed	Price	Cost
07/09/2009 10:42	Test Page	Administrator	XeroxBW	Printed A	B/W	1	0.060	0.060
07/09/2009 10:45	Test Page	Administrator	HP Universal Printing PC	Printed W	B/W	1	0.060	0.060
07/09/2009 10:46	Test Page	Administrator	HP LaserJet 9040 PCL 5	Printed W	B/W	1	0.040	0.040
07/09/2009 11:46	mk:@MSITStore:C:\Program%20Files%20(x86)\Text	Employee3	HP LaserJet 5Si	Printed W	B/W	1	0.030	0.030
07/09/2009 11:46	outbind://343-00000000EBA6C4366E7EA64480046BB	Employee6	HP LaserJet 9040 PCL 6	Printed W	B/W	1	0.040	0.040
07/09/2009 11:46	xPress codes.xls	Employee1	HP LaserJet 9040 PCL 5	Printed W	B/W	16	0.040	0.640
07/09/2009 11:48	Untitled	Secretary 1	HP LaserJet 5Si	Printed W	B/W	1	0.030	0.030
07/09/2009 11:48	xPress codes.xls	Secretary 3	HP LaserJet 5Si	Printed W	B/W	2	0.030	0.060
07/09/2009 11:48	outbind://343-00000000EBA6C4355E7EA64480046BB	Manager 2	HP LaserJet 5Si	Printed W	B/W	1	0.030	0.030
						25		0.990

111 - Customer 1

Date	Job Name	User	Printer	Status	Type	Printed	Price	Cost
07/09/2009 11:46	file://C:\Documents and Settings\Administrato	Employee4	HP LaserJet 9040 PCL 5	Printed W	B/W	2	0.040	0.080
						2		0.080

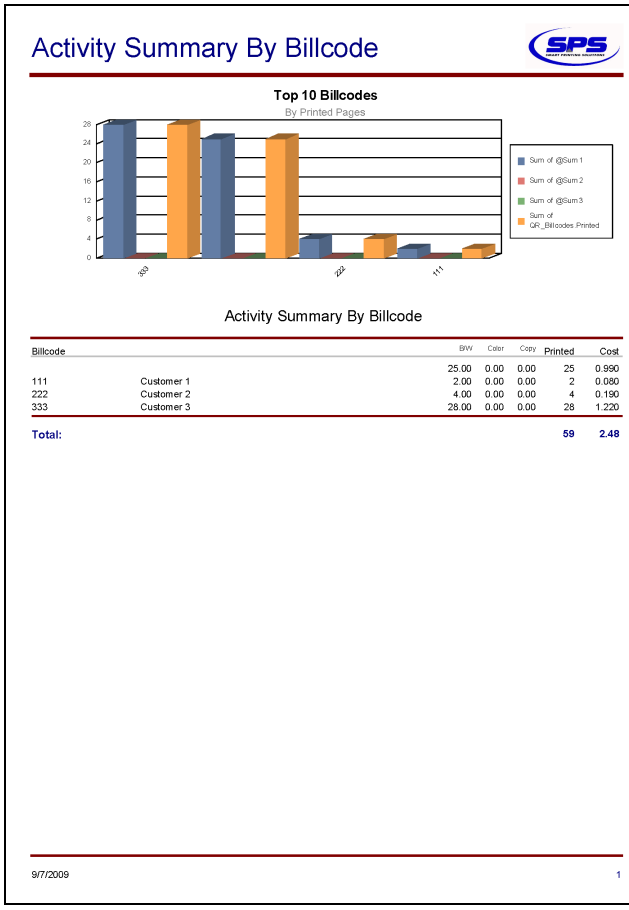
222 - Customer 2

Date	Job Name	User	Printer	Status	Type	Printed	Price	Cost
07/09/2009 11:46	http://localhost/sentinel/Default.aspx	Employee2	XeroxBW	Printed W	B/W	2	0.060	0.120
07/09/2009 11:46	Document1	Employee5	HP LaserJet 5Si	Printed W	B/W	1	0.030	0.030
07/09/2009 11:46	Microsoft Office Outlook - Weekly Style	Employee6	HP LaserJet 9040 PCL 5	Printed W	B/W	1	0.040	0.040
						4		0.190

333 - Customer 3

Date	Job Name	User	Printer	Status	Type	Printed	Price	Cost
07/09/2009 11:46	Test Page	Employee1	XeroxBW	Printed W	B/W	1	0.060	0.060
07/09/2009 11:48	xPress codes.xls	Secretary 2	XeroxBW	Printed W	B/W	4	0.060	0.240
07/09/2009 11:48	xPress codes.xls	Manager 1	HP LaserJet 9040 PCL 5	Printed W	B/W	2	0.040	0.080
07/09/2009 11:48	Microsoft Word - Smadar Hebrew.doc	Manager 3	HP LaserJet 9040 PCL 5	Printed W	B/W	21	0.040	0.840

9/7/2009 1



Activity Summary By Billcode

Top 10 Billcodes

By Printed Pages

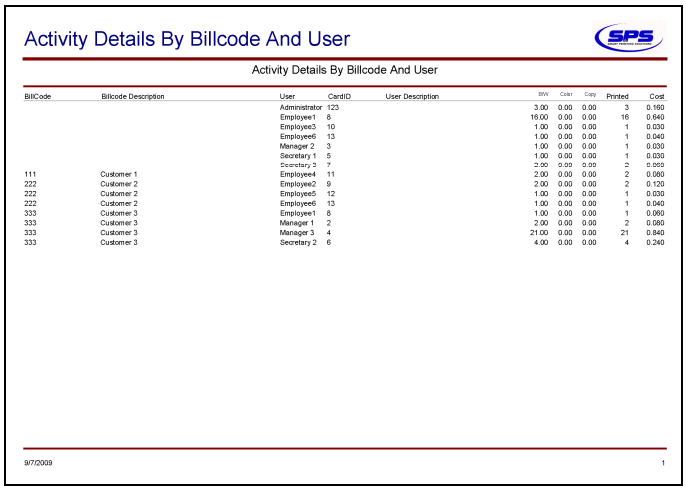
Activity Summary By Billcode

Billcode		B/W	Color	Copy	Printed	Cost
		25.00	0.00	0.00	25	0.990
111	Customer 1	2.00	0.00	0.00	2	0.080
222	Customer 2	4.00	0.00	0.00	4	0.190
333	Customer 3	28.00	0.00	0.00	28	1.220
Total:					**59**	**2.48**

9/7/2009 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.

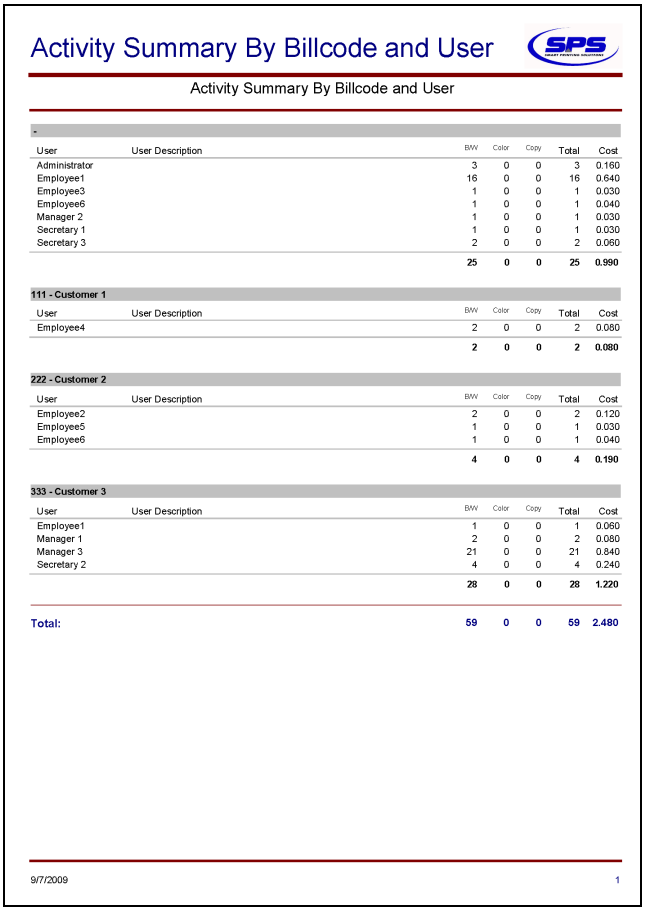


Activity Details By Billcode And User

Activity Details By Billcode And User

BillCode	Billcode Description	User	CardID	User Description	BW	Color	Copy	Printed	Cost
		Administrator	123		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
		Employee6	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 3	7		2.00	0.00	0.00	2	0.060
111	Customer 1	Employee4	11		2.00	0.00	0.00	2	0.080
222	Customer 2	Employee2	9		2.00	0.00	0.00	2	0.120
222	Customer 2	Employee5	12		1.00	0.00	0.00	1	0.030
222	Customer 2	Employee6	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

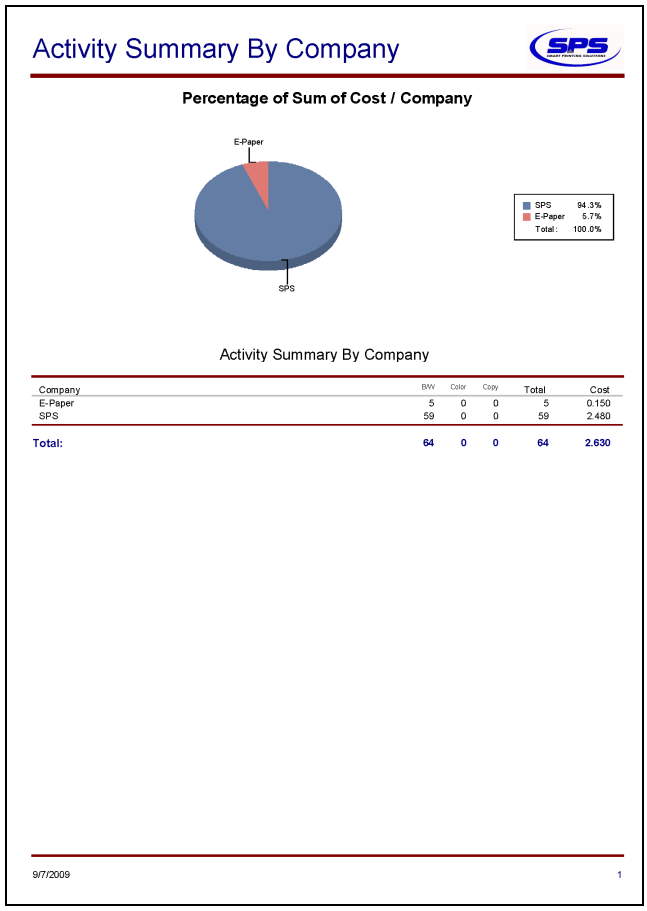
User	User Description	BW	Color	Copy	Total	Cost
Employee1		1	0	0	1	0.060
Manager 1		2	0	0	2	0.080
Manager 3		21	0	0	21	0.840
Secretary 2		4	0	0	4	0.240
		28	**0**	**0**	**28**	**1.220**

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.



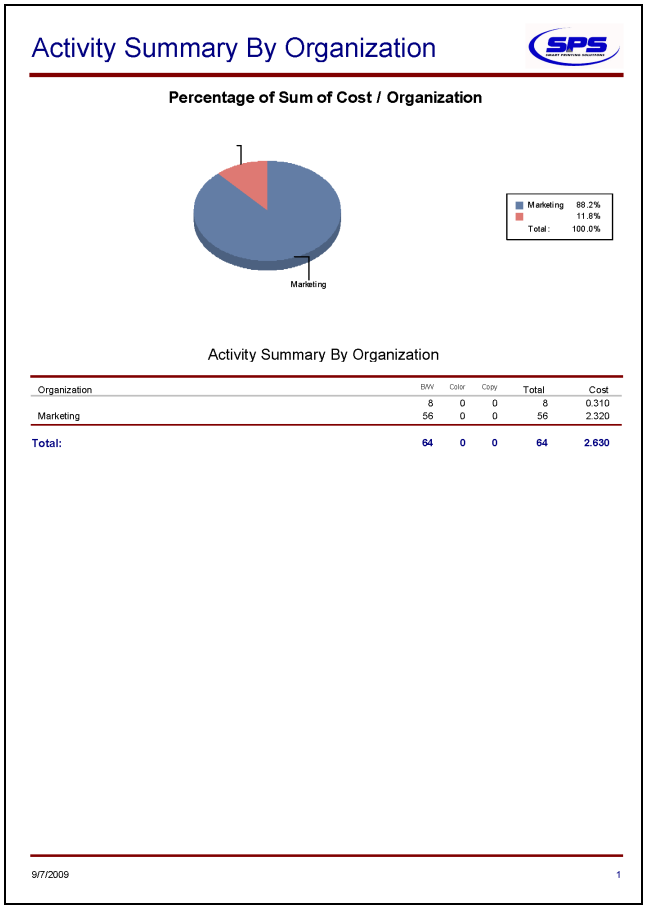
Activity Summary By Company

Percentage of Sum of Cost / Company

Activity Summary By Company

Company	B/W	Color	Copy	Total	Cost
E-Paper	5	0	0	5	0.150
SPS	59	0	0	59	2.480
Total:	**64**	**0**	**0**	**64**	**2.630**

9/7/2009 1



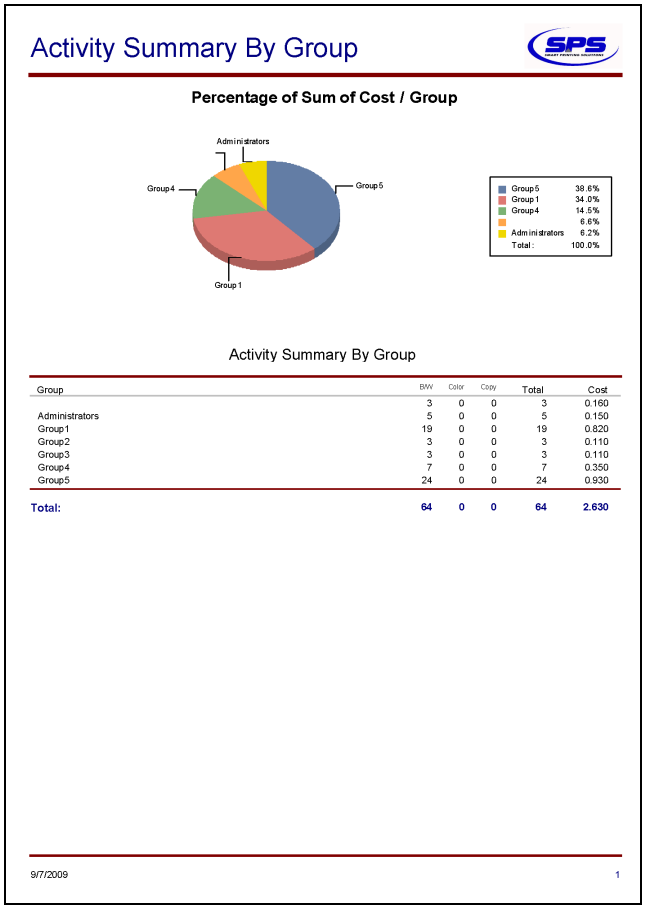
Activity Summary By Organization

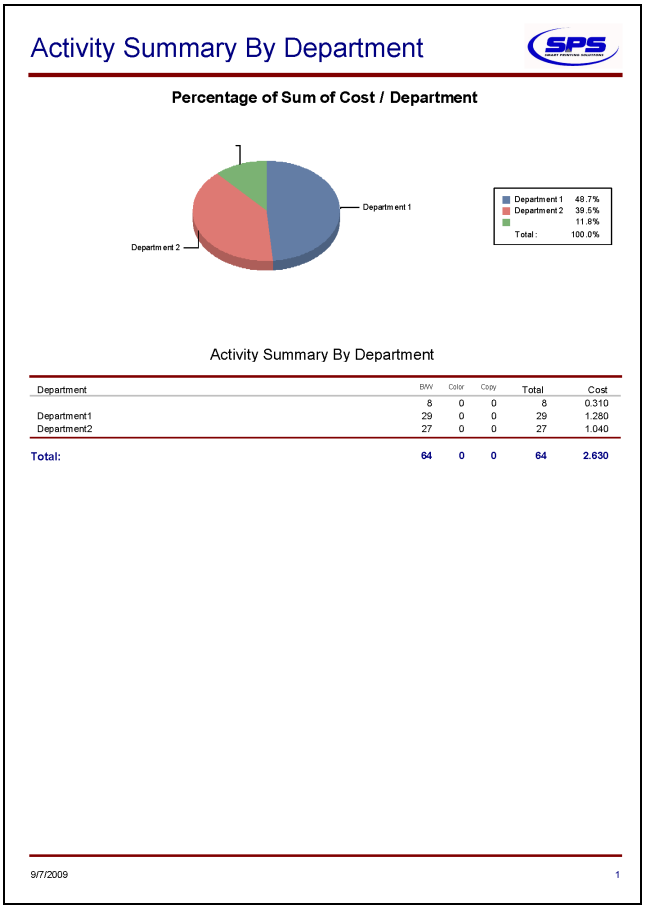
Percentage of Sum of Cost / Organization

Activity Summary By Organization

Organization	B/W	Color	Copy	Total	Cost
	8	0	0	8	0.310
Marketing	56	0	0	56	2.320
Total:	**64**	**0**	**0**	**64**	**2.630**

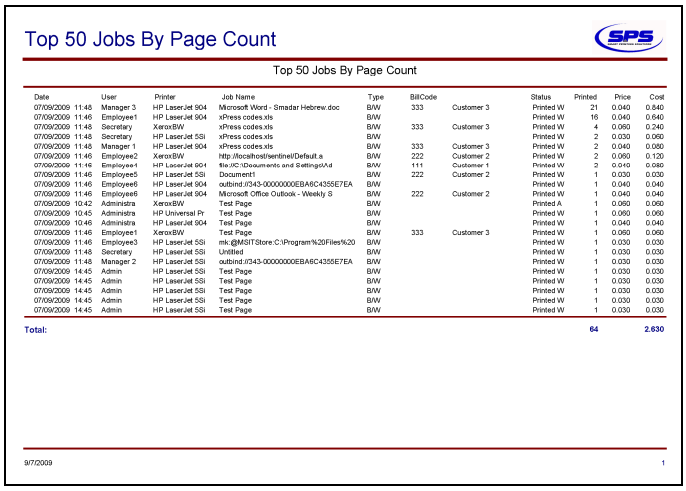
9/7/2009 1

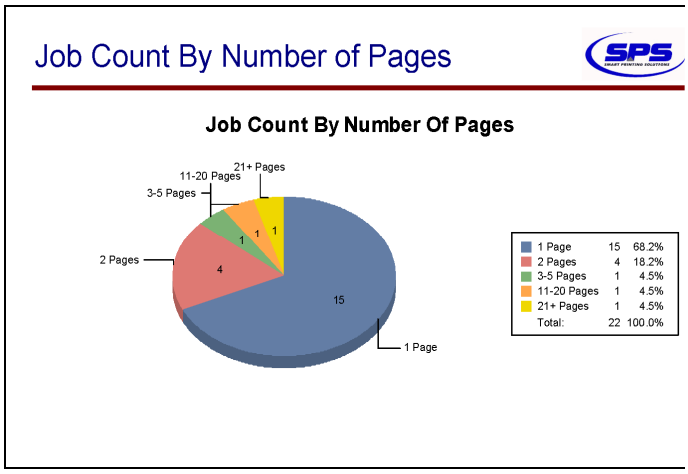




Other Reports

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.





External Utilities

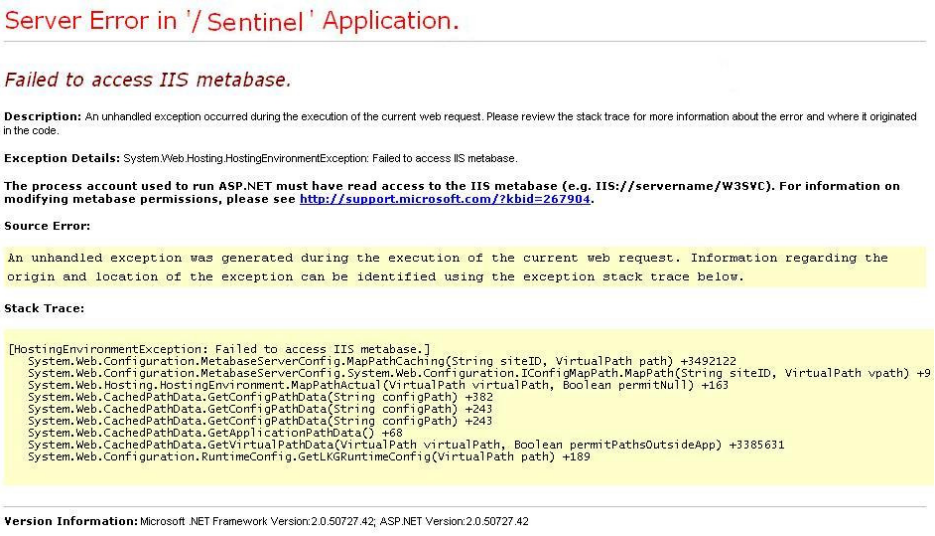
External utilities are tools that are used to perform different maintenance tasks. These tools are usually used inside scripts or as scheduled tasks.

Utility	Explanation
DelKeypad.exe	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: • `DelKeypad.exe -dt` Deletes the Temporary Card field values for all users. • `DelKeypad.exe -dk` Deletes the Keypad code field values for all users. For example, putting **DelKeypad.exe -dt** in a scheduler that runs each night deletes all temporary cards assigned during the day.
ADUserSync.exe SQLUserSync.exe	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 *Auto Sync* on p. 17. The utility to be used is according to the synchronization type you use. 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.

Troubleshooting

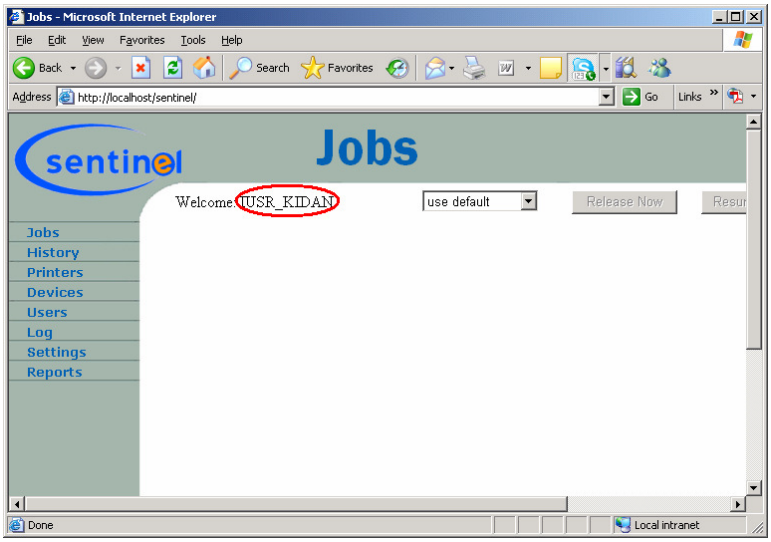
This section covers errors or problems that can during installation, configuration, and daily operation of Sentinel. If the suggested solution does not solve the problem, or if you experience a problem not listed here, contact your Sentinel technical support provider.

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 **c:\sentinel\service.log**, 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: 1. Open the file **c:\sentinel\service.ini** 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 **c:\sentinel**. 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.System.Web.Configuration.IConfigMapPath.MapPath(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: 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.

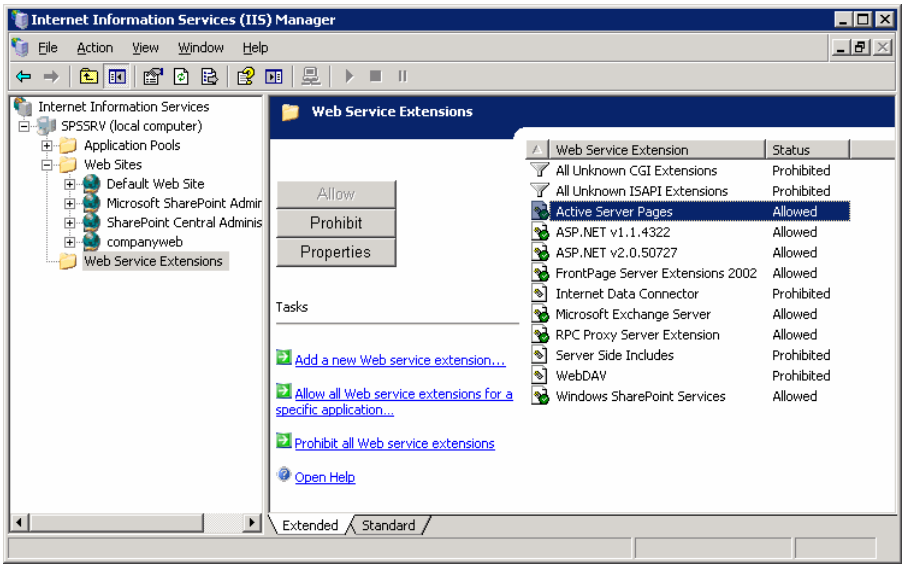
HTTP Error 404: File or Directory not found

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.



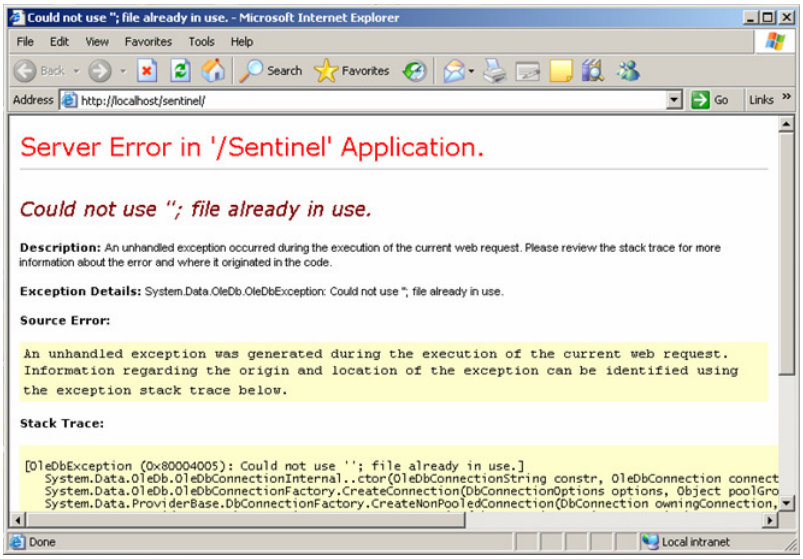
2. In the right pane of IIS Manager, make sure that the **Active Server Pages** extension is allowed and that the ASP.NET v2.0.50727 is allowed.

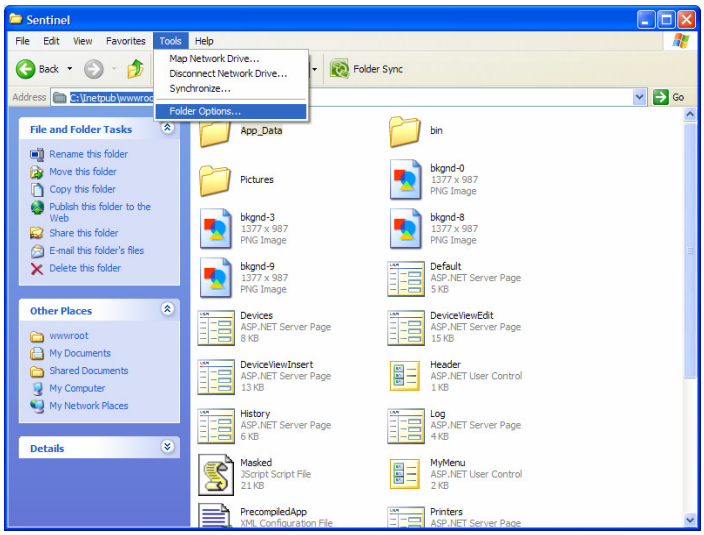
3. Reset the IIS service by typing **IISRESET** in the command line.

Could not use ''; file already in use

Symptoms

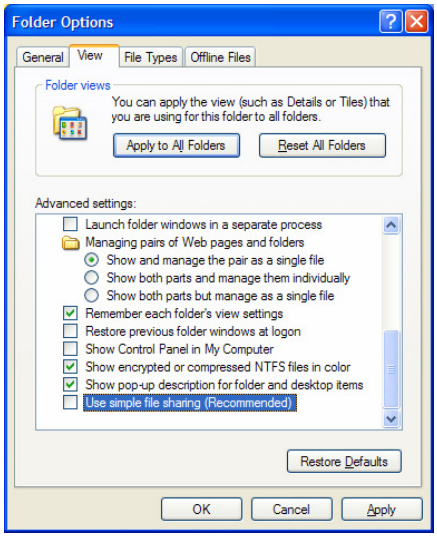
When trying to start the Sentinel Web page, you get the following error:



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**. 

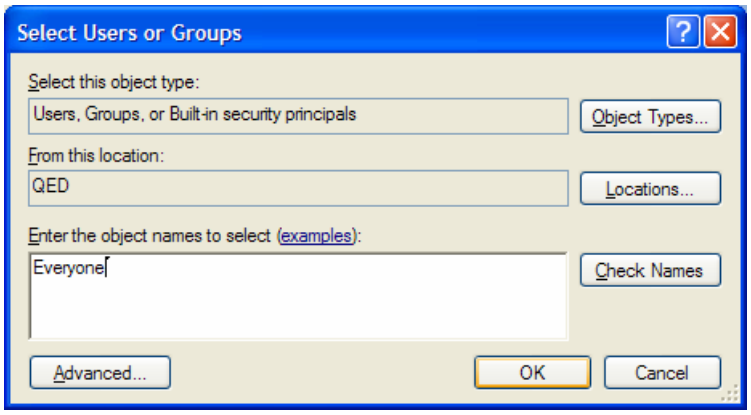
Resolution 1, cont.

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**.

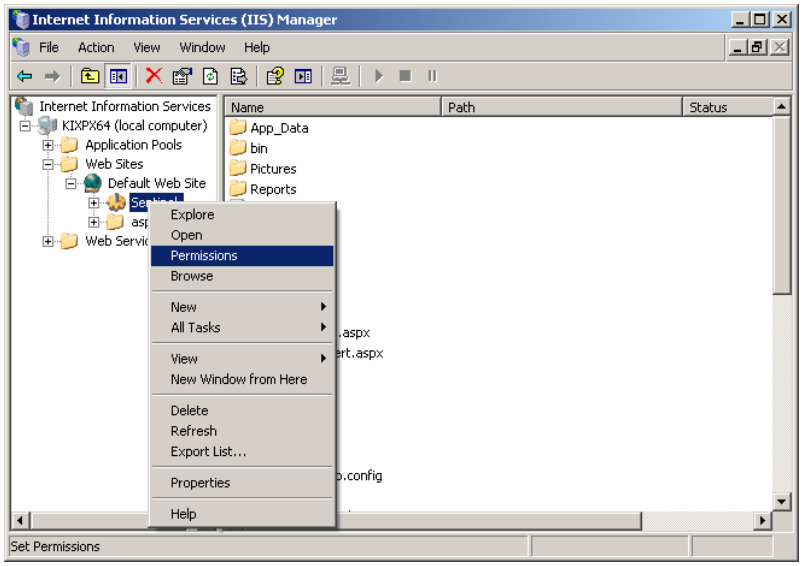
9. Repeat these actions with the file **Sentinel.ldb**.

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

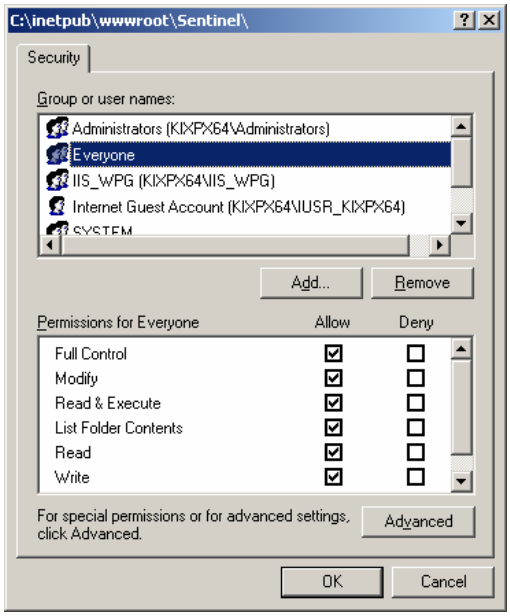
Resolution 2

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**.



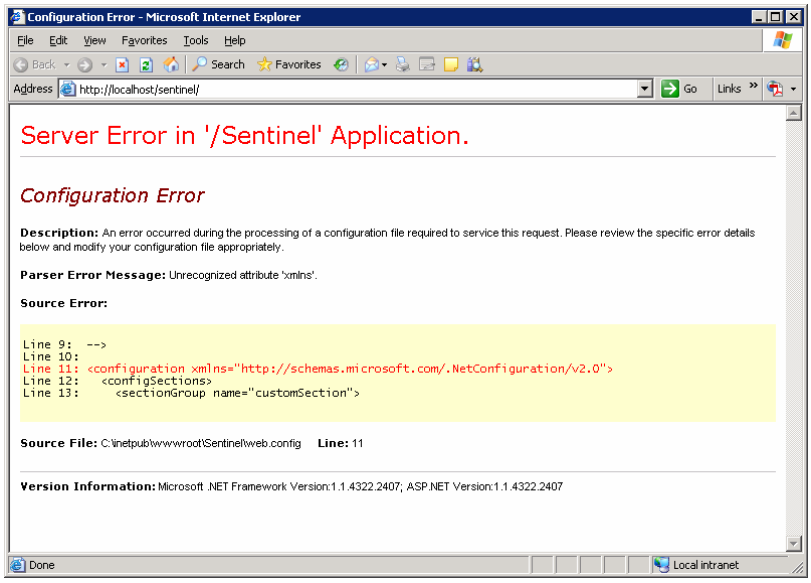
3. Click **Everyone** and select the checkbox **Full Control** under **Allow**.



Configuration Error

Symptoms

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



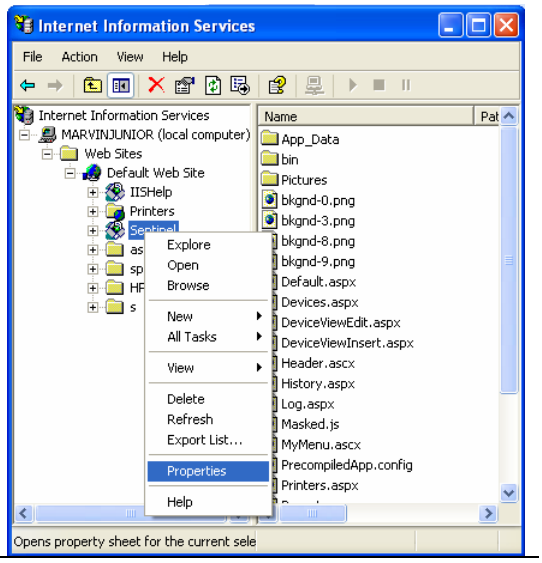
Cause

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

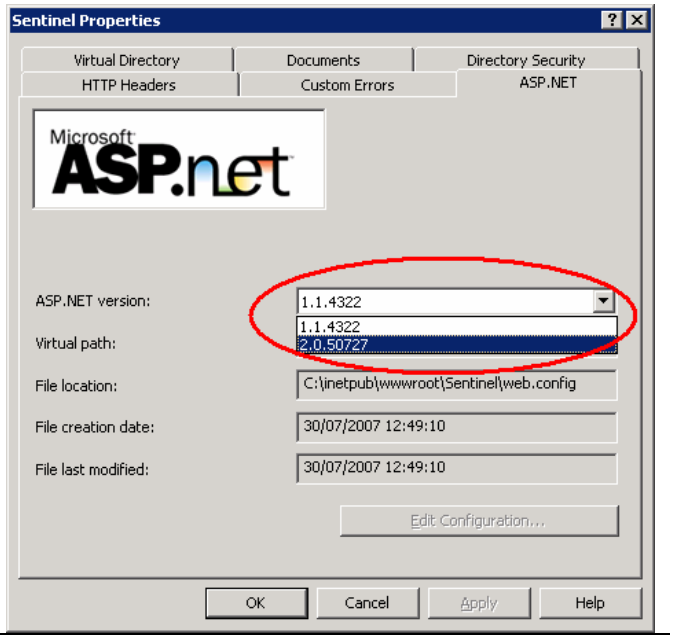
Resolution

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.

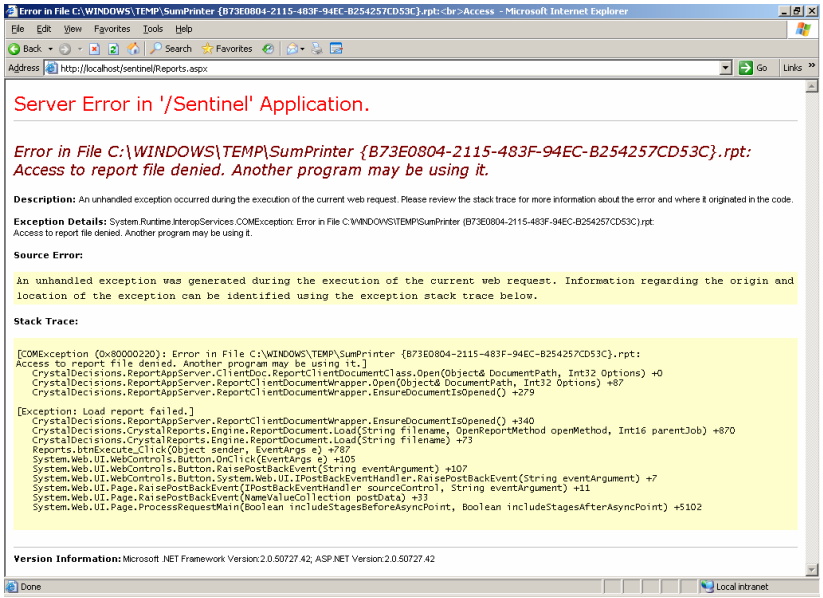


Service Unavailable Error	
Symptoms	When trying to start the Sentinel web page, you get the error: "Service Unavailable".
Cause	This issue may occur if the server that is running Microsoft Internet Information Services (IIS) 6.0 is also a domain controller. The problem occurs because the Application 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	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. To set permissions on the folders for the IIS_WPG group and the NT Authority\Network Service account: 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**: • Read and Execute • List Folder Contents • Read

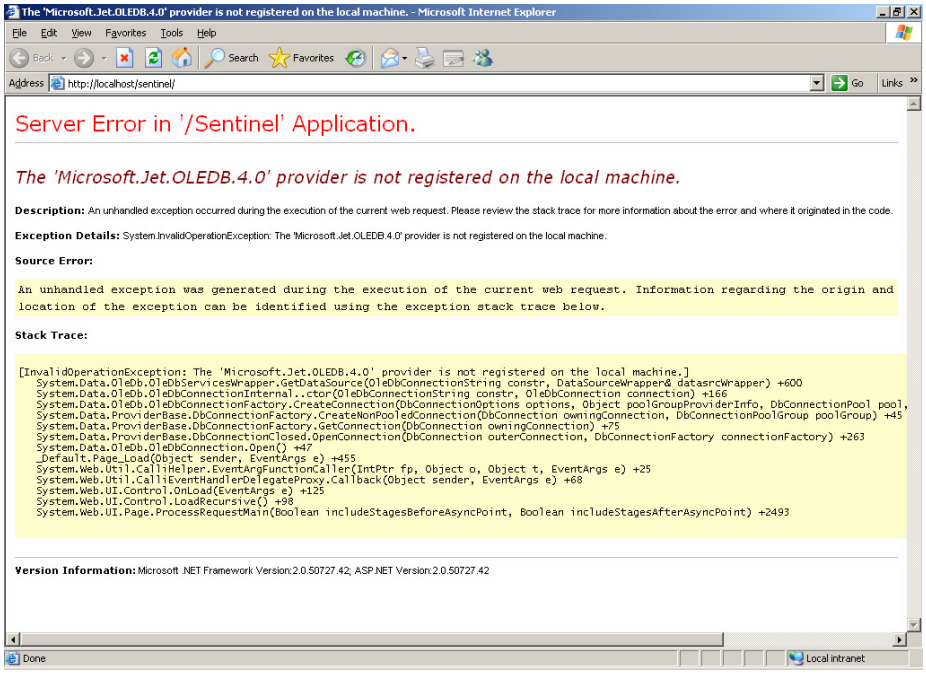
5. Repeat the above step with **NETWORK SERVICE** instead of IIS_WPG.
6. Open the folder **%systemroot%\system32\inetsrv**.
7. In the right pane, right-click the ASP Compiled Templates folder, and then click **Sharing and Security**.
8. Click the Security tab, click the **IIS_WPG** group, and then select 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	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. 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.
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.

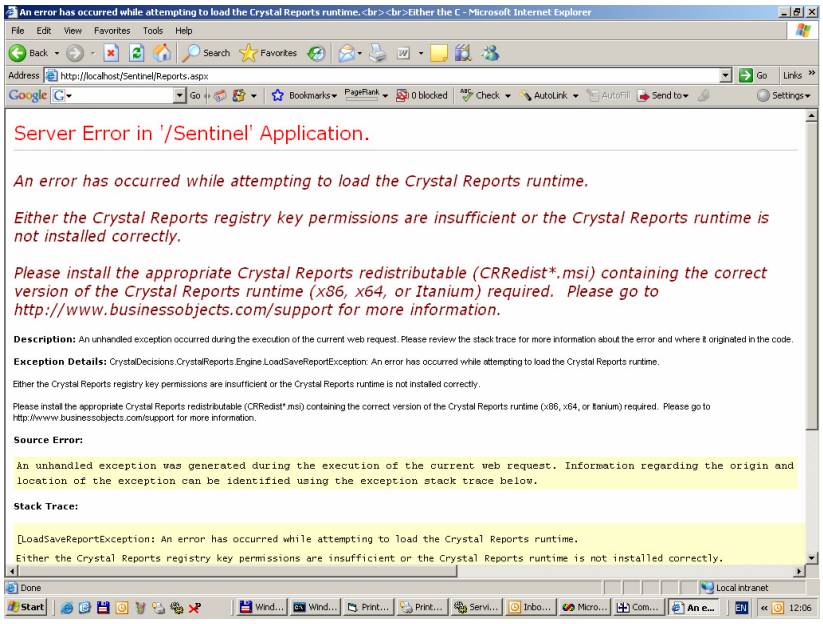
The 'Microsoft.Jet.OLEDB.4.0' provider is not registered

Symptoms	When running the Web interface, the following error appears in the browser: 
Cause	This error occurs if there is no corrects 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.

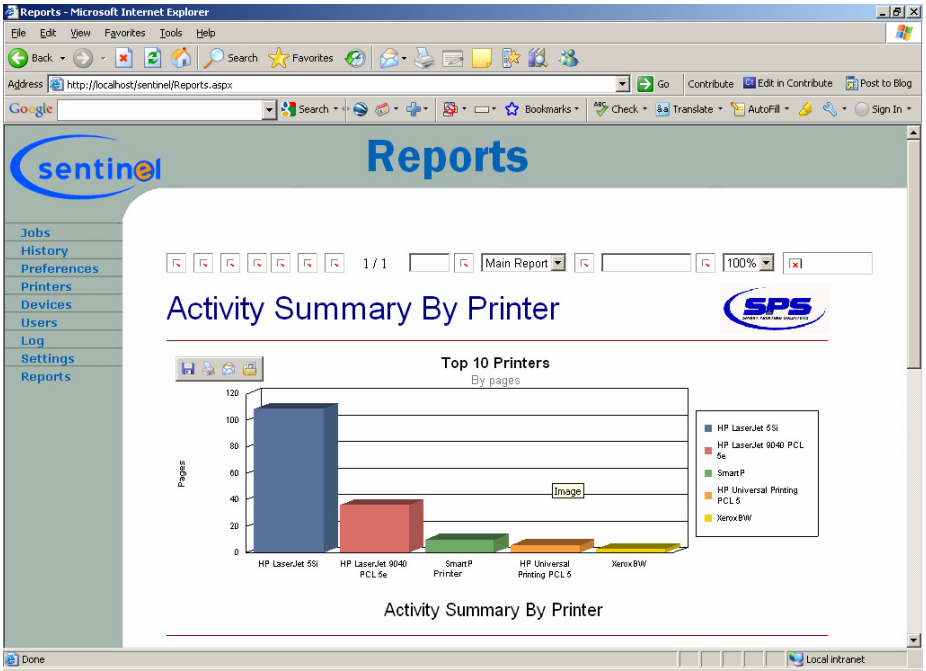
The process cannot access the file

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

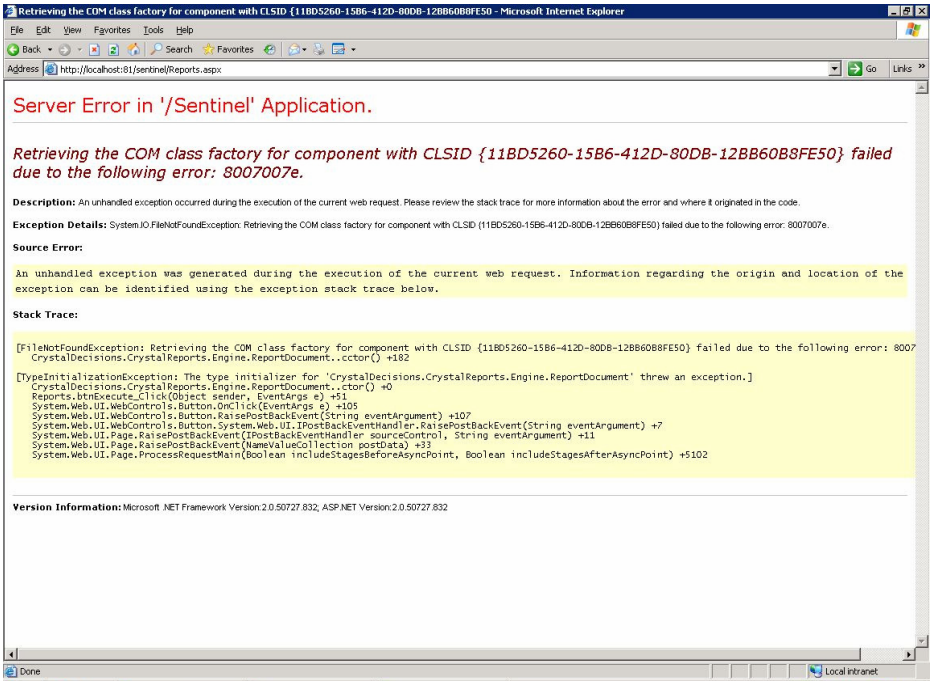
Symptoms	When trying to generate any Sentinel report, the following error occurs: 
Cause	This error usually occurs when the wrong Crystal Reports runtime is installed, usually when your operating system is x64 and the installed Crystal Reports runtime is the 32-bit version.
Resolution	Follow the installation 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.

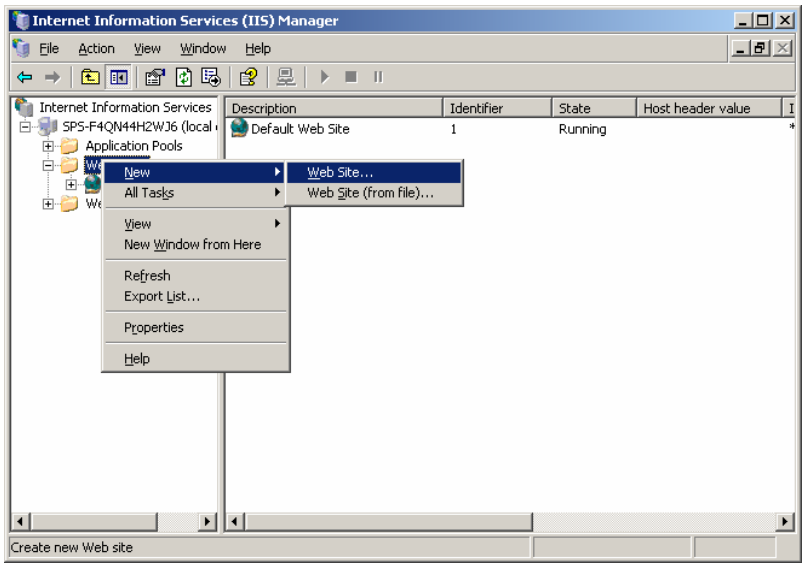
Default website is used by another application on the server

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.

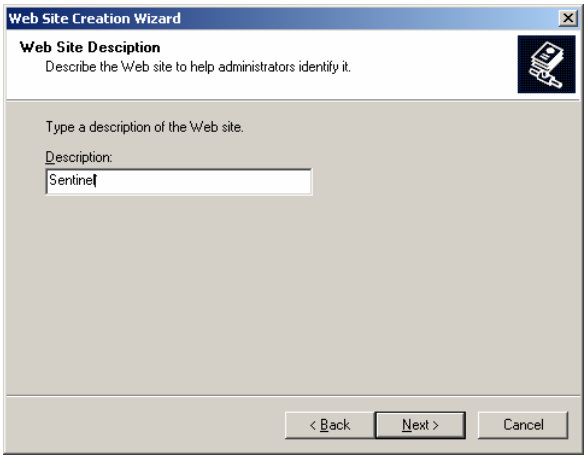
Resolution

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

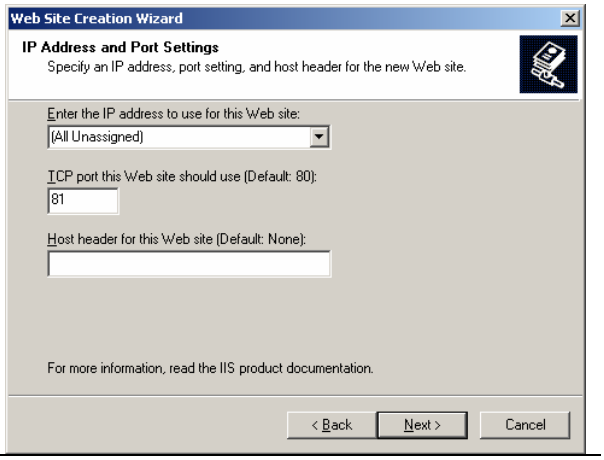
1. Open the IIS Manager and add a new website.



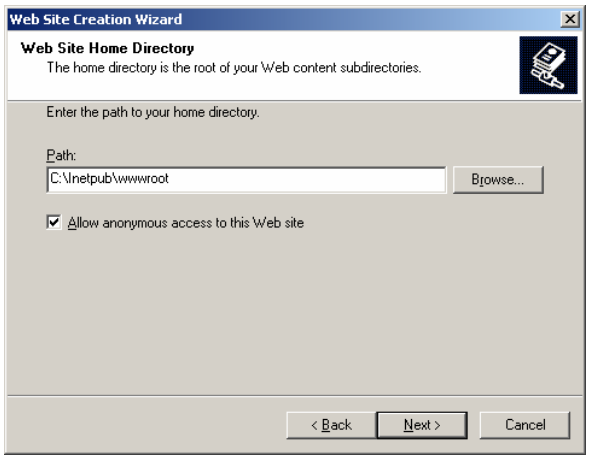
2. Click **Next** and in the following screen type the name of the site (**Sentinel**) and click **Next** again.



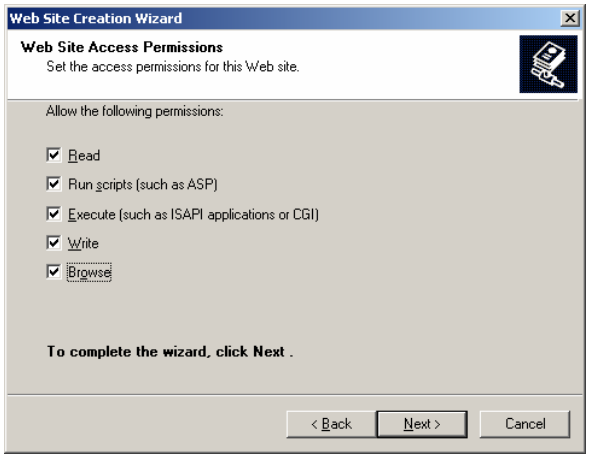
3. Change the port number for the new website to a new port (for example, 81), and click **Next** again.



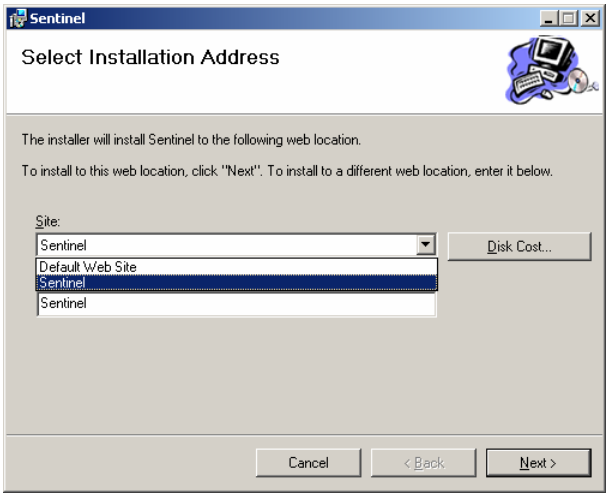
4. Type the path to the root of the new website (**c:\inetpub\wwwroot**) and click **Next** again.



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).



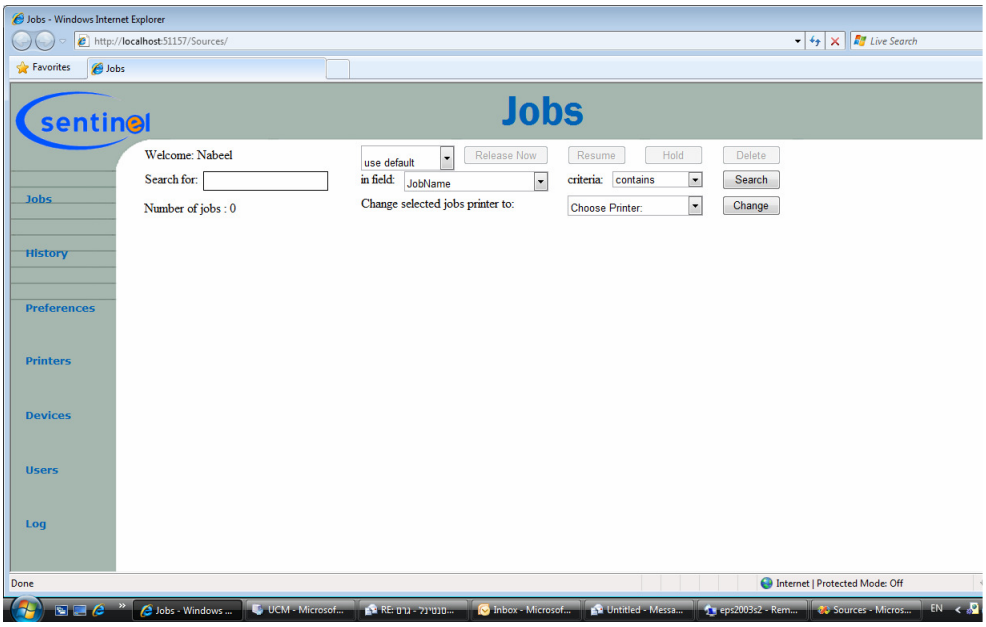
9. Continue with the installation instructions as described in *Installing Sentinel Server Software on Windows Server 2003* on p. 3until successfully completing all installation steps.

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

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.