WebSpy Sentinel 3.2
Planning and Installation Guide

This document will assist you in setting up and configuring WebSpy Sentinel to record your network information as logged data.

Please send all issues or queries to WebSpy Support (support@webspy.com)

This document is intended as a guide only. It aims to introduce the reader to issues that may be relevant to their organization, and to point out sources from which more detailed information may be obtained. It is **NOT** a substitute for professional legal advice.

Table of Contents

Table of Contents 1
Introduction 2
New Features 2
Getting Help 2
Before you start... 3
Hardware Requirements 3
Software Requirements 3
Network Structure Questions 3
Sentinel Usage Questions 4
Deploying Sentinel 5
Determining your Optimum Installation Point 5
Connecting Sentinel to the Optimum Installation Point 6
Network Diagrams 7
Case Study One: Hub Installation 7
Case Study Two: Unmanaged Switch 7
Case Study Three: Managed Switch 'Monitoring Port' 8
Case Study Four: Multiple Subnets 9
Case Study Five: Multiple Subnets – Gateway Solution 9
Case Study Six: Hub and Gateway Solution 10
User Name Resolution 11
Windows NT® 4 11
Windows® 2000 and Windows® XP 13
Windows Server 2003 16
Definitions 19
WebSpy North America 21
WebSpy Europe 21
WebSpy Australia 21
WebSpy Support 21

Introduction

WebSpy Sentinel is a program that enables you to record all web, mail, newsgroup, telnet and FTP traffic on your network without the need for proxy server software. The logged data is stored in a log file format that can subsequently be imported into WebSpy's Analyzer, Live and Vantage ranges and examined to identify Internet usage patterns of your employees or departments.

WebSpy Sentinel captures all traffic passing through the network on which it is installed but only keeps (or logs) the protocols that you choose. You can log just the basic information about the Internet traffic you are seeing (i.e. source, destination, URL etc.) or you can capture all of the content of that traffic. See Sentinel's Getting Started Guide for more information.

WebSpy Sentinel is made up of two parts: Sentinel Service, and Sentinel Management. Sentinel Service is the driver, which connects to your Network Card, and the service, which logs the data. The driver and the service are always installed together, so that the driver can 'see' all Internet traffic. Sentinel Management is used to configure the Sentinel Service running on multiple computers on the same network. You can install Sentinel Management on any computer on your network with access to all of the computers running Sentinel Service. This guide will help you to determine where to install. Therefore it is essential that the point of installation for the Service is planned and implemented correctly.

Please see page 11 for an explanation of terms used in this guide.

New Features

- POP3 and Secure Web
  Sentinel 3.2 can now capture data from the POP3 and Secure Web (HTTPS) protocols.

- Selective name resolution
  Improve Sentinel's performance and efficiency by specifying the networks you want Sentinel to resolve usernames for (defined by network and subnet masks)

- Extended log files
  Sentinel now logs bytes sent and received, browser, query and status.

- Automatically restarts capture
  When you make changes to Sentinel's data capture settings, you no longer need to manually stop and start the service.

- Log per-protocol
  You can now configure Sentinel to create one log file per protocol.

- Improved performance
  Sentinel 3.2 has been optimized to improve capture speed and accuracy.

Getting Help

For more information, press F1 to open Sentinel's help at the most appropriate topic.

Support is available by contacting WebSpy support at support@webspy.com. Please provide full details about your network structure and software, including the types and manufacturers of hardware.

Before you start...

This guide is intended to help you decide how many installations of Sentinel you will require, where to put them, and what computers to install Sentinel on.

Hardware Requirements

A computer that has Sentinel installed on it is referred to as a Sentinel Server. This Sentinel Server must have the following hardware:

Item	Minimum	Recommended
CPU	Pentium III	Pentium 4 or Higher
RAM	128 MB	512 MB or Higher
Disk Space	6 MB for program, and approximately 1MB per monitored PC per day.	6 MB for program, and approximately 5MB per monitored PC per day.
Network Device	Ethernet network card	Ethernet network card

Note: The storage space required for your Sentinel Log files is not related to the amount of data you download. For example, a 2 GB download may create only one entry in your log file, where as a news or weather service may create an entry every 5 seconds.

Software Requirements

Your Sentinel Server will install and run on Windows ® NT 4 SP5, Windows 2000, Windows Server 2003, Windows XP, Windows Vista, or Windows Server 2008. Optimally, your Sentinel Server will have Windows Server® 2003, Windows® XP or Windows® Vista, Windows Server 2008.

Additional applications may be run on the same machine that Sentinel is installed onto. However, if you use an application similar to Sentinel, you must install it on a different computer.

Network Structure Questions

You will need to know what hardware and software you have on your network to decide where to install WebSpy Sentinel. If you do not have this information, consult your network administrator.

Alternatively you can forward your questions to WebSpy support at support@webspy.com. Please remember to collate as much information on your network as possible including the Internet connection, operating systems, server applications and network hardware before sending in your query.

Sentinel Usage Questions

Is Sentinel going to be used to capture full content?

For most effective content capture, ensure that the Sentinel Server has additional RAM and CPU – like most applications, Sentinel works best with a faster CPU and more RAM. The CPU usage and RAM requirements will be dependent on the amount of traffic and whether you choose to capture content or not. Capture of HTTP is not recommended, unless for a specific purpose as this will greatly affect computer performance. Please see the WebSpy Sentinel Integration Guide, which explains the effects of capturing content.

Is Sentinel going to resolve usernames?

There are currently issues preventing the username resolution feature working correctly when your domain controller is running Windows Server 2003 and above. There may also be issues logging usernames for the client machines running Windows Vista and above. This feature will be improved in a future version of Sentinel. For more information see User Name Resolution on page 11.

Which protocols should be captured?

You can choose which protocols you want to capture. As different protocols are affected by other applications on the network, you may need to install Sentinel in more than one position i.e. one server to capture Web and one to capture SMTP. A good example of this situation is if you use Microsoft® Exchange server. Microsoft Outlook communicates with Exchange server using a proprietary protocol that Sentinel cannot capture.

Hint: If you want to see your internal email usage, and you use Microsoft® Exchange Server, you can import your Exchange tracking logs into WebSpy Analyzer Premium, Analyzer Giga or any of the WebSpy Vantage range. You can also monitor them in real time using WebSpy Live.

If I have to install Sentinel in more than one location, how do I administer the software?

After installing the software on one or more computers, you can use Sentinel Management to configure and monitor each Sentinel Server. You can install Sentinel Management on any convenient computer that has access to the Sentinel Servers.

Deploying Sentinel

When you choose to install WebSpy Sentinel, there are a few preliminary steps you will need to go through to ensure Sentinel will work most effectively. These steps are:

- Determine your optimum installation point or points, where all the Internet traffic on you network passes in a form that Sentinel can use.
- Decide on the most efficient way for you to tap into the installation point(s).
- Remove any existing WebSpy Sentinel components from the computer that will be running WebSpy Sentinel 3.2.

Once you have completed these steps, you can install WebSpy Sentinel.

Usually, you will only need one, or perhaps two, computers running Sentinel Service to capture all the Internet traffic on your network. You can install Sentinel Management on any computer with access to the computer(s) running Sentinel Service.

Determining your Optimum Installation Point

The optimum installation point for Sentinel Service will depend on your network topology. It may be possible that no one point is optimal; in these cases you will need two or more copies of Sentinel Service, depending on the network. You can install Sentinel Management on any computer with access to the computer(s) running Sentinel Service.

Please refer to the table below to determine your optimum installation point.

I have…	**The optimum installation position for Sentinel is…**
A proxy server	On the same side of the proxy server as your users to capture web traffic
Multiple proxy servers	On the same side of each proxy server as your users to capture web traffic
A firewall	On the same side of the firewall as your users
A router connecting my network to the Internet	On the same side of the router as your users
Multiple Subnets	Between all the subnets' routers and your Internet gateway or router OR One computer running Sentinel on the same side of each subnet's router as that subnet's users
Network Address Translation software	Between the software and your users

A Microsoft® Exchange Server	Between the server and your Internet gateway to capture external email traffic. To log internal email traffic, enable your Microsoft® Exchange tracking logs.
Multiple Microsoft® Exchange Servers	On the same side of each server as your Internet gateway to capture external email traffic
Multiple Domains	One computer running Sentinel in each domain. Follow the points above to work out the optimum installation point for each domain.
A computer with two network cards acting as my Internet gateway	On the Internet gateway itself if the gateway is a computer running Microsoft® Windows

Connecting Sentinel to the Optimum Installation Point

Once you have determined where to install WebSpy Sentinel, you will have to determine how to connect the computer running Sentinel to that point. The different installation points are graphically displayed in the Diagrams section of this document.

Please refer to the table below for installation instructions.

My Optimum Installation Point is…	**Install Sentinel Service…**
A hub	On any computer connected to that hub that has all of the internet traffic passing through it
A managed switch	On a computer attached to the switch's monitoring port
An unmanaged switch	On a computer connected to a hub connecting the unmanaged switch and the Internet gateway OR On a computer connected to the monitoring port of a managed switch connecting the unmanaged switch and the Internet gateway OR On the Internet gateway itself if the gateway is a computer running Microsoft® Windows OR On each computer connected to the switch
A network cable	By replacing the single cable with two cables and a device (hub, managed switch or computer with

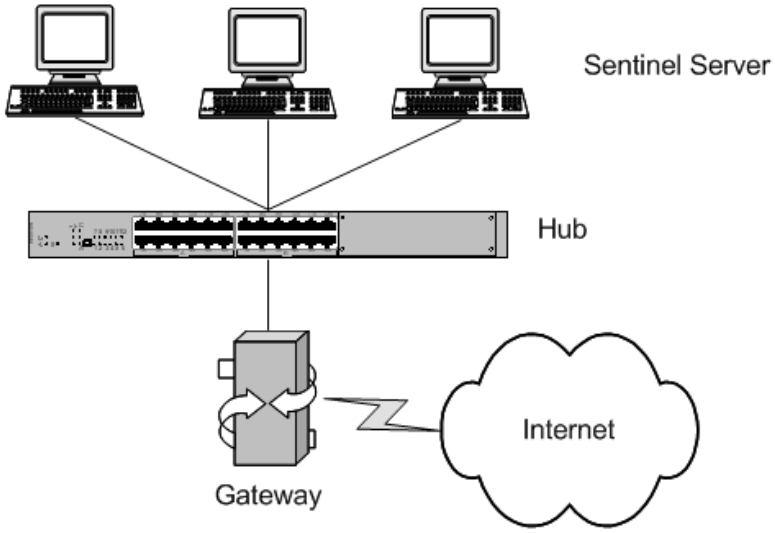
two network cards) between them. You can then install Sentinel in a position appropriate for the connecting device (see above).

Network Diagrams

Case Study One: Hub Installation

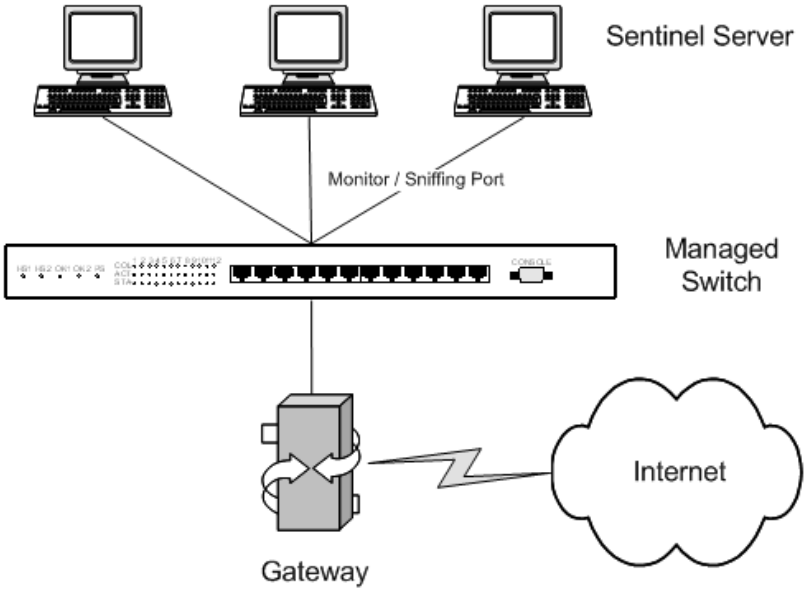
Sentinel can be installed on any computer connected to a hub, whether a workstation or a gateway or firewall.

If Sentinel is installed on the gateway or firewall, please make sure that it is monitoring the internal network card and not the external network card.



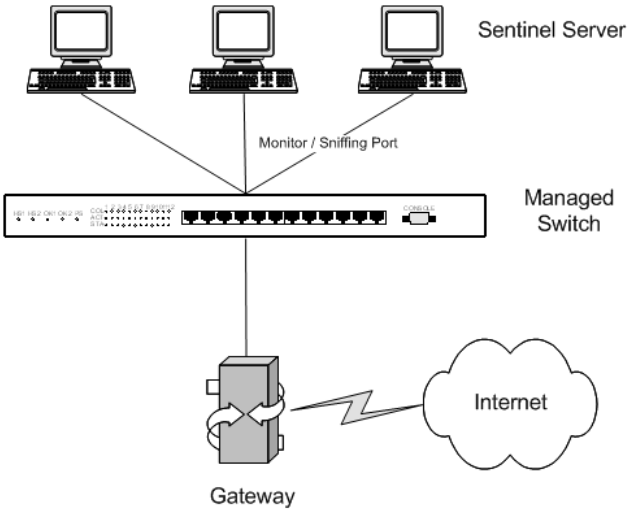
Case Study Two: Unmanaged Switch

None of these computers can listen to the others' traffic because of the switch, and since it is an unmanaged switch, no monitoring port is available. Therefore, WebSpy Sentinel must be installed on either the existing gateway or on an additional computer with dual network cards. Alternatively, see Case Study Six for another way of managing this situation.



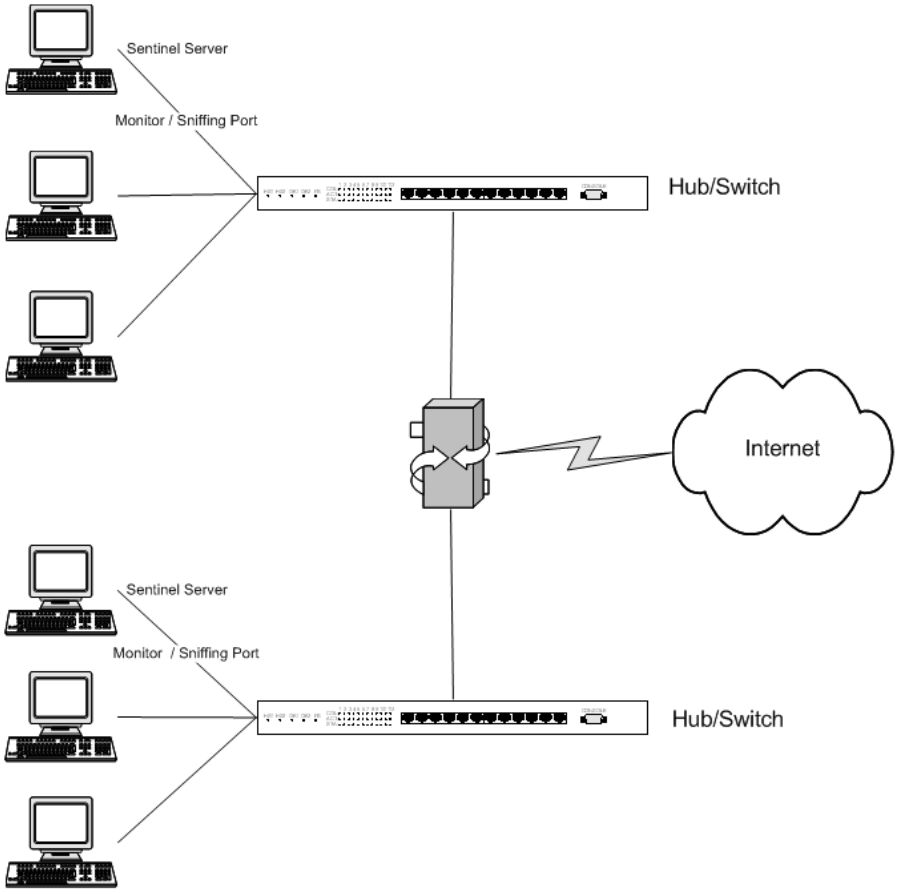
Case Study Three: Managed Switch 'Monitoring Port'

A hub is effectively a broadcaster of information while a switch directs information directly to the port that the information is intended for. Some switches (managed switch) have what is known as a monitoring port. This can 'listen' to all the other ports on the switch if it is enabled. Alternatively, see Case Study Six for another way of managing this situation.



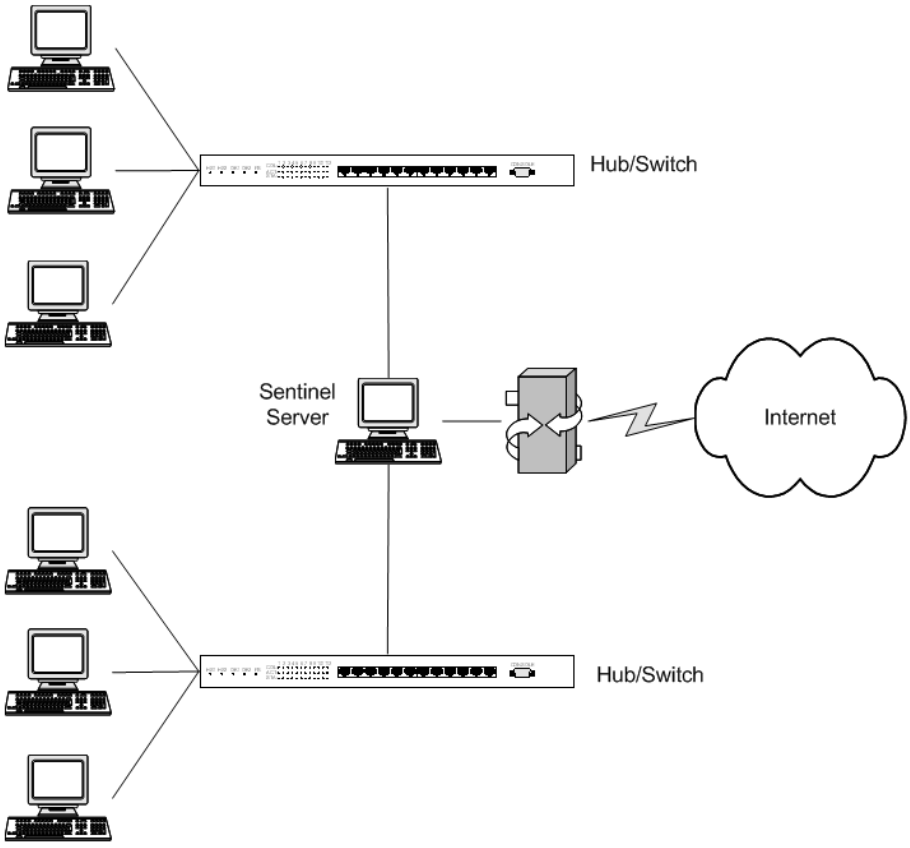
Case Study Four: Multiple Subnets

When working with multiple subnets, you can place a Sentinel Server on each subnet to capture that subnet's data. This will also distributes the load between the servers and will provide more efficient data capture.



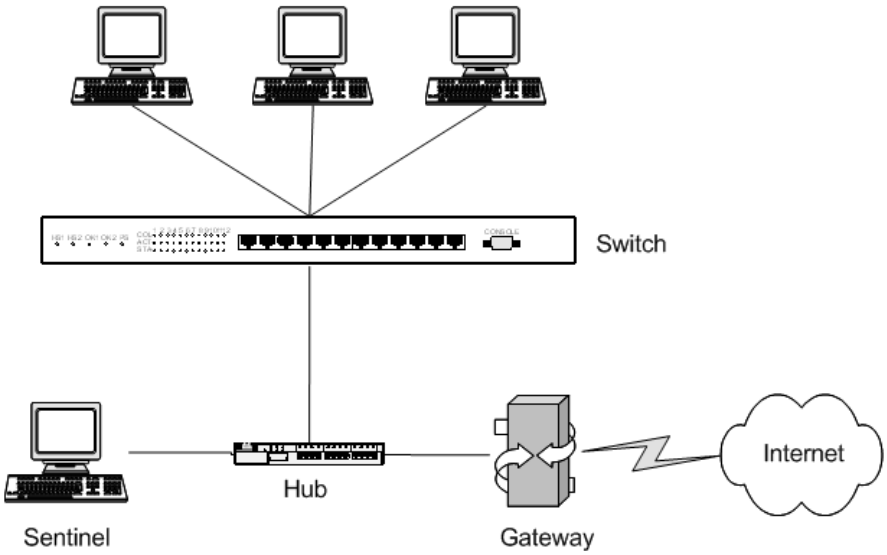
Case Study Five: Multiple Subnets – Gateway Solution

When working with multiple subnets you can also place a Sentinel Server in front of the gateway to capture your entire organization's traffic. This is the best solution if you have unmanaged switches, or if you do not want a Sentinel Server on each subnet.



Case Study Six: Hub and Gateway Solution

This solution will prove effective when you can't install Sentinel onto your gateway. This may be because you are running Unix, Linux or a hardware device. The installation point will allow all traffic that is entering or exiting your network to be captured by the Sentinel Server.



User Name Resolution

To find out the actual user name for each person on your network accessing the Internet, you must install WebSpy Sentinel on a computer that has access to a Windows Primary or Backup Domain Controller.

To use a domain controller to get the information Sentinel needs, you must configure the Sentinel Service so that it has permission to audit the security logs. See the section below for the instructions appropriate to your operating system.

For Sentinel to be able to resolve usernames, there are five things you will need to do. **These actions must be performed by a domain administrator:**

- Create a new user account belonging to the Domain Admins group for Sentinel Service to run as
- Ensure that the security logs are created with the appropriate information about users logging on and off
- Give the Sentinel user permission to audit security logs
- Make sure the Sentinel user has permission to log on as a service
- Make Sentinel Service run using the Sentinel user account you created

Note: (Sentinel Build 3.2.2.3074) There are currently issues preventing the username resolution feature working correctly when your domain controller is running Windows Server 2003 and above. There may also be issues logging usernames for the client machines running Windows Vista and above. This feature will be improved in a future version of Sentinel.

Windows NT® 4

The following instructions are a guide to setting up Sentinel to be able to resolve usernames with Windows NT® 4. You will need to perform these tasks on your primary domain controller.

Create a new user account for Sentinel:

On your Windows NT domain controller, go to **Start | Programs | Administrative Tools (Common) | User Manager for Domains**. The User Manager dialog is opened for you.

Select **User | New User** from the main menu of the User Manager dialog to open the New User dialog.

In the New User dialog:

- Type a name for the Sentinel user in the Username edit box.
- Enter a password for the Sentinel user
- Confirm that password
- Select any other password options in accordance with your organization's password policy

Click on the **Groups** button at the bottom of the New User dialog to open the Group Memberships dialog.

In the Group Memberships dialog:

- Select the Domain Admins group from the right-hand list
- Click on the **Add** button to add the Sentinel User to the Domain Admins group
- Click **OK** to close the Group Memberships dialog

In the New User dialog click on the Add button to create the user account. Click Close to return to the User Manager dialog. The new Sentinel user you just created will be in the list of users at the top of the dialog.

Create domain security logs with the appropriate information for Sentinel

1. In the User Manager dialog, select **Policies | Audit** from the main menu to open the Audit Policy dialog.
2. Select the 'Audit These Events' radio button to enable the checkboxes in the dialog.
3. Check the Logon and Logoff 'Success' and 'Failure' checkboxes.
4. Click **OK** to return to the User Manager dialog.

Give Sentinel user permission to audit domain security logs:

1. In the User Manager dialog, select **Policies | User Rights** to open the User Rights Policy dialog.
2. Check the 'Show Advanced User Rights' checkbox at the bottom of the dialog.
3. Select 'Generate security audits' from the right drop down list.
4. Click on the **Add** button to open the Add Users and Groups dialog.
5. In the Add Users and Groups dialog:
   - Click on the **Show Users** button
   - Select the Sentinel user in the Names List
   - Click on the **Add** button. The Sentinel user will appear in the Add Names list
   - Click **OK** to add the Sentinel user to the list of users with permission to audit domain security logs and close the dialog.
6. Click **OK** to close the User Rights Policy dialog and return to the User Manager dialog.

Ensure that the Sentinel user logs on as a service:

1. In the User Manager dialog, select **Policies | User Rights** from the main menu to open the User Rights Policy dialog.

2. Check the 'Show Advanced User Rights' checkbox at the bottom of the dialog.
3. Select 'Log on as a service' from the Right drop down list.
4. Click on the **Add** button to open the Add Users and Groups dialog.
5. In the Add Users and Groups dialog:
   - Click on the **Show Users** button
   - Select the Sentinel user in the Names List
   - Click on the **Add** button. The Sentinel user will appear in the Add Names list
   - Click **OK** to add the Sentinel user to the list of users that log on as a service
6. Click **OK** to close the User Rights Policy dialog and return to the User Manager dialog.

Set Sentinel Service to run as the Sentinel user:

1. On the machine running WebSpy Sentinel, go to **Start | Settings | Control Panel | Services** to open the Services dialog.
2. Select Sentinel from the Service list.
3. Click on the **Stop** button and wait until your computer says the service has been successfully stopped.
4. Double click on Sentinel in the Service list to open the Service dialog.
5. Select the 'This Account' radio button in the Log on as section of the dialog.
6. Click on the **…** button to the right of the Account Name edit box to open the Add User dialog, then:
   - Select the Sentinel user from the Names list
   - Click on the **Add** button, then click **OK** to return to the Service dialog
7. Enter the password you chose for the Sentinel user.
8. Click **OK** to return to the Services dialog.
9. Click on the **Start** button to restart Sentinel Service.
10. Click **Close** to close the Services dialog.

Windows® 2000 and Windows® XP

Create a new user account for Sentinel:

1. On your domain controller, go to **Start | Control Panel | Administrative Tools | Active Directory Users and Computers** to open the Active Directory Users and Computers dialog.

2. In the Tree section, expand your domain and click on the Users folder.
3. Click on the **New User** button on the toolbar to open the New Object – User dialog.
4. In the New Object – User dialog:
    - Type an appropriate name for the Sentinel user into the Full name and User logon name edit boxes, and click **Next**
    - Enter a password for the Sentinel user, confirm that password, and select any other password options in accordance with your organization's password policy, and click **Next**
    - Check the summary for the Sentinel user is correct, and click **Finish** to close the New Object – User dialog. The new user will be added to the User list on the right hand side of the Active Directory Users and Computers dialog
5. Make sure the Sentinel user is selected, and then click on the **Add user to group** button on the toolbar of the Active Directory Users and Computers dialog to open the Select Group dialog.
6. In the Select Group dialog:
    - Select the Domain Admins group from the list
    - Click **OK** to close the Select Group dialog

Create domain security logs with the appropriate information for Sentinel:

1. Go to **Start | Settings | Control Panel | Administrative Tools | Domain Controller Security Policy** to open the Domain Controller Security Policy dialog.
2. In the Tree section, expand the 'Security Settings' item.
3. Expand the 'Local Policies' item, and select the 'Audit Policy item'.
4. Double click the 'Audit account logon events' item in the right-hand list to open the Security Policy Setting dialog.
5. Check all the checkboxes in the dialog.
6. Click **OK** to return to the Domain Controller Security Policy dialog. The Computer Setting information for the 'Audit account logon events' item will change to Success, Failure.
7. Double click the 'Audit logon events' item in the right-hand list to open the Security Policy Setting dialog.
8. Check all the checkboxes in the dialog.
9. Click **OK** to return to the Domain Controller Security Policy dialog. The Computer Setting information for the 'Audit account logon events' and 'Audit logon events' items should be Success, Failure.

Give Sentinel user permission to audit security logs:

1. In the Domain Controller Security Policy dialog, expand the 'Security Settings' item in the Tree section.
2. Expand the 'Local Policies' item, and select the 'User Rights' Assignment item.
3. Double click the 'Generate security audits' item in the right-hand list to open the Security Policy Setting dialog.
4. In the Security Policy Setting dialog, ensure the checkbox is checked and then click on the **Add** button to open the Add user or group dialog.
5. In the Add user or group dialog:
   - Click on the **Browse** button to open the Select Users or Groups dialog
   - Select the Sentinel user from the Names list
   - Click on the **Add** button.
     The Sentinel user will appear in the Add Names list
   - Click **OK** to close the Select Users or Groups dialog
   - Click **OK** to close the Add user or group dialog
6. Click **OK** to close the Security Policy Setting dialog and return to the Domain Controller Security Policy dialog.

Ensure that the Sentinel user logs on as a service:

1. In the Domain Controller Security Policy dialog, expand the 'Security Settings' item in the Tree section.
2. Expand the 'Local Policies' item, and select the 'User Rights Assignment' item.
3. Double click the 'Log on as a service' item in the right-hand list to open the Security Policy Setting dialog.
4. In the Security Policy Setting dialog, ensure the checkbox is checked and then click on the **Add** button to open the Add user or group dialog.
5. In the Add user or group dialog:
   - Click on the **Browse** button to open the Select Users or Groups dialog
   - Select the Sentinel user from the Names list
   - Click on the **Add** button.
     The Sentinel user will appear in the Add Names list
   - Click **OK** to close the Select Users or Groups dialog
   - Click **OK** to close the Add user or group dialog

6. Click **OK** to close the Security Policy Setting dialog and return to the Domain Controller Security Policy dialog.

Set Sentinel Service to run as the Sentinel user:

1. On the machine running WebSpy Sentinel, go to Start **| Settings | Control Panel | Administrative Tools | Services** to open the Services dialog.
2. Select Sentinel from the list on the right of the dialog.
3. Click on the **Stop** button on the toolbar.
4. Double click on Sentinel to open the Sentinel Properties dialog.
5. Select the 'Log on' tab.
6. Select the 'This account' radio button and click on the **Browse** button to open the Select User dialog.
7. In the Select User dialog:
   - Select the name of the user in the list
   - Click **OK** to return to the Sentinel Properties dialog
8. Type the password for the Sentinel user in the appropriate edit boxes and click **OK** to close the Sentinel Properties dialog.
9. Click on the **Start** button on the toolbar of the Services dialog to restart Sentinel Service.

Windows Server 2003

Note: (Sentinel Build 3.2.2.3074) There are currently issues preventing the username resolution feature working correctly when your domain controller is running Windows Server 2003 and above. There may also be issues logging usernames for client machines is running Windows Vista and above.

The instructions below are provided on an as-is basis, but there may still be issues preventing the successful logging of usernames. This feature will be improved in a future version of Sentinel.

Create a new user account for Sentinel:

1. On your Windows Server 2003 domain controller, go to **Start | Control Panel | Administrative Tools | Active Directory Users and Computers** to open the Active Directory Users and Computers dialog.
2. Create a new user at the appropriate location in your directory (such as a folder that holds system or application accounts):
   - Type an appropriate name for the Sentinel user into the Full name and User logon name edit boxes
   - Enter a password for the Sentinel user, confirm that password, and select any other password options in accordance with your organization's password policy

- Check the summary for the Sentinel user is correct, and click **Create** then **Close**.

3. Right-click the newly added Sentinel user and select **Properties**.
4. Go to the 'Member of' tab and click the **Add** button:

- Type *Domain Admins* and click the **Check Names** button
- Click **OK** to close the Select Group dialog

Create domain security logs with the appropriate information for Sentinel:

1. Go to **Start | Settings | Control Panel | Administrative Tools | Domain Controller Security Policy** to open the Domain Controller Security Policy dialog.
2. In the Tree section, expand the 'Security Settings' item.
3. Expand the 'Local Policies' item, and select the 'Audit Policy item'.
4. Double click the 'Audit account logon events' item in the right-hand list to open the Security Policy Setting dialog.
5. Check all the checkboxes in the dialog.
6. Click **OK** to return to the Domain Controller Security Policy dialog. The Computer Setting information for the 'Audit account logon events' item will change to Success, Failure.
7. Double click the 'Audit logon events' item in the right-hand list to open the Security Policy Setting dialog.
8. Check all the checkboxes in the dialog.
9. Click **OK** to return to the Domain Controller Security Policy dialog. The Computer Setting information for the 'Audit account logon events' and 'Audit logon events' items should be Success, Failure.

Give Sentinel user permission to audit security logs:

For Windows Server 2003 you must modify registry entries to grant access to the security event logs.

To allow authenticated users read access to the security event log:

1. Open the registry editor by selecting **Start | Run**, typing 'regedit' (without the quotes) and clicking **OK**.
2. Find the following key:
   HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Eventlog\Security
3. Append (A;;0x1;;;AU) to the CustomSD value

For more information on this registry change, please view Microsoft's article "How to set event log security locally or by using Group Policy in Windows Server 2003" http://support.microsoft.com/kb/323076.

Ensure that the Sentinel user logs on as a service:

1. In the Domain Controller Security Policy dialog, expand the 'Security Settings' item in the Tree section.
2. Expand the 'Local Policies' item, and select the 'User Rights Assignment' item.
3. Double click the 'Log on as a service' item in the right-hand list to open the Security Policy Setting dialog.
4. In the Security Policy Setting dialog, ensure the 'Define these policy settings' checkbox is checked and then click on the **Add user or Group...** button to open the Add user or group dialog.
5. In the Add user or group dialog:
   - Click on the **Browse** button to open the Select Users or Groups dialog
   - Enter the name of the Sentinel user and click **Check Names**
   - Click **OK** to close the Select Users or Groups dialog
   - Click **OK** to close the Add user or group dialog
6. Click **OK** to close the Security Policy Setting dialog and return to the Domain Controller Security Policy dialog.

Set Sentinel Service to run as the Sentinel user:

1. On the machine running WebSpy Sentinel, go to Start **| Settings | Control Panel | Administrative Tools | Services** to open the Services dialog.
2. Right-click the WebSpy Sentinel Service and select **Stop** from the popup menu
3. Double click the WebSpy Sentinel service to open the Sentinel Properties dialog.
4. Select the 'Log on' tab.
5. Select the 'This account' radio button and click on the **Browse** button to open the Select User dialog.
6. In the Select User dialog:
   - Select the name of the user in the list
   - Click **OK** to return to the Sentinel Properties dialog
7. Type the password for the Sentinel user in the appropriate edit boxes and click **OK** to close the Sentinel Properties dialog.

Right-click the WebSpy Sentinel Service and select **Start** from the popup menu to restart Sentinel Service.

Definitions

Domain Controller

A domain controller is the computer that logs users on to domain accounts in a Windows NT® Server domain. The primary domain controller keeps track of any changes to the domain accounts, and will log users on to domain accounts. By default, Sentinel uses the primary domain controller to resolve user names. A backup domain controller is kept up to date with changes by the primary domain controller, and can be used to provide the information Sentinel needs, if the primary domain controller is not available.

Firewall

A system of hardware and/or software designed to prevent unauthorized access to or from a private network. All items entering or leaving your network have to pass through the firewall, which examines each item and blocks those that do not meet its specified security criteria. Firewalls are a form of Gateway.

Gateway (Internet)

A gateway is a combination of hardware and software that links two different types of networks. Internet gateways connect an organization's LAN to the Internet. It is therefore important that Sentinel is installed on the inside of a Gateway.

Hub

A hub is a common connection point for devices in a network. Hubs are commonly used to connect segments of a LAN. A hub contains multiple ports. When a packet arrives at one port, it is copied to the other ports so that all segments of the LAN can see all packets. Therefore, if Internet traffic is going through a hub and Sentinel is installed onto the hub, Sentinel will see the traffic.

LAN

A local area network (LAN) is a group of computers and associated devices that share a common communications line and typically share the resources of a single processor or server within a small geographic area (for example, within an office building). Usually, the server has applications and data storage that are shared in common by multiple computer users. A local area network may serve as few as two or three users (for example, in a home network) or many thousands of users (for example, in a large corporation).

Mail

For WebSpy Sentinel's purposes, this is Internet traffic received via SMTP (Simple Mail Transfer Protocol), not POP3 or IMAP. SMTP is a TCP/IP protocol used in sending and receiving e-mail. POP3 or IMAP are protocols that let the user save messages in a server mailbox and download them periodically from the server. Users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving messages that have been stored for them at their local server.

Newsgroups

A newsgroup is a discussion about a particular subject consisting of e-mails or notes written to a central Internet site and redistributed through Usenet, a worldwide network of news discussion groups. The protocol used is Network News Transfer Protocol (NNTP).

Packet

A packet is the unit of data that is routed between an origin and a destination on the Internet or any other packet-switched network. When any file (e-mail message, HTML file, GIF file, URL request, and so forth) is sent from one place to another on the Internet, the file is divided into "chunks" or packets of a suitable size for efficient routing. Each of these packets is separately numbered and includes the Internet address of the destination.

Protocol

A protocol is a special set of rules or conventions for communication between two computers, both of which must recognize and observe the protocol. Different types of Internet traffic use different protocols. Protocols are often described in an industry or international standard.

Switch/Managed Switch

A switch is a network device that selects a path or circuit for sending a unit of data to its next destination.

Telnet

Telnet enables you to access another computer across the Internet, assuming they have given you permission. Such a computer is known as a 'host' computer. With Telnet, you log on as a regular user with whatever privileges you may have been granted to the specific application on that computer.

Web

For WebSpy Sentinel's purpose, this is any Internet traffic received via HTTP (Hypertext Transfer Protocol). HTTP is the set of rules for exchanging files (text, graphics, sound, video, and other multimedia files) on the World Wide Web (WWW).Contact WebSpy

WebSpy North America

(Servicing North and South America)

Columbia Center
701 5th Ave, Suite 4200
Seattle, Washington 98104

Toll free: 888-862-4403
Phone: +1 206-575-7763
Fax: +1 206-575-7809
Email: sales@webspy.com

WebSpy Europe

(Servicing Europe, Middle East and Africa)

3rd Floor, Unit 19
Angel Gate
326 City Road
London, EC1V 2PT

Phone: +44 (0) 207 239 7500
Fax: +44 (0) 207 239 7539
Email: europesales@webspy.com

WebSpy Australia

(Servicing Australia, Asia and the Pacific)

Level 3
9 Colin Street
West Perth, Western Australia 6005

Toll Free: 1800 801 121
Phone: +61 8 9321 3322
Fax: +61 8 9321 3377
Email: sales@webspy.com.au

WebSpy Support

To contact WebSpy Support, please visit our support page at
http://www.webspy.com.au/contact/support.aspx