

By Debra Littlejohn Shinder, MCSE, MVP

Like it or not, network administrators these days must take on the added task of playing Big Brother—monitoring employees' use of the computers and network. Even if the company's management philosophy allows for some private use of company equipment, you often need to know what Web sites employees are visiting, what files they're sending and receiving, and even what they're saying in their e-mail. That's because employee actions can subject the company to monetary loss, civil lawsuits, and even criminal charges if they involve deliberate or accidental disclosure of confidential company information, transmission of pornography, or exposure to malicious code. According to the July 2005 issue of *HR Focus*, more than 60 percent of employers monitor all workers' Internet usage. This list covers 10 ways you can keep tabs on what your users are doing with the company's computers.

1 Use auditing to monitor access to files

On a Windows network, you can keep tabs on which files employees open—or even failed attempts to access files—by using the audit policy feature that's built into the operating systems. In Windows 2000 and above, auditing is enabled via Group Policy. Setting up auditing of access to files and folders is a two-step process: First, you must enable auditing in the Group Policy interface; then, you must set auditing in the properties of the particular network objects (files or folders) you want to audit. For detailed instructions on how to set up auditing of access to files, folders, and printers on a Windows XP computer, see [KB article 310399](#).

2 Examine cached Web files

If you have only a few computers and want to find out what Web sites their users are visiting, you may be able to do it without buying any special software if you examine the Web browser's cache (called Temporary Internet Files in Internet Explorer). Copies of the pages and graphics that a user downloads are stored here so they can be more quickly displayed if the user wants to go back to the same page. However, savvy users who visit sites they don't want you to know about may clear the cache to prevent you from seeing these files.

You can make this circumvention more difficult on Windows XP computers by using the User Restrictions Tool in Microsoft's free [Shared Computer Toolkit](#) to deny users access to the Internet Options selection on the Tools menu, which is the interface for accessing and clearing the History and Temporary Internet Files.

3 Monitor Web access at the firewall

Another way to monitor which Internet Web sites users are visiting is to configure your firewall to report on Web sites accessed according to user name and/or computer name. Enterprise-level perimeter firewalls, such as Microsoft's ISA Server, Cisco PIX, and CheckPoint Firewall-1, either have built-in reporting features or have add-ons available that can provide reports of all Web sites accessed through the firewall and from what account and computer they were accessed.

See your firewall's documentation on how to set up reporting or check out these add-on products:

- [SurfControl](#)
- [Websense](#)
- [GFI WebMonitor](#)

4 Filter Web access by URL

You can go a step further. Rather than just monitoring which Web sites employees visit, actually block undesirable sites. This is an especially good tactic in the case of pornographic sites that could subject your company to sexual harassment lawsuits or sites that are known to contain malicious software downloads, such as some hacker sites. You might also want to block certain “recreational” sites (entertainment topics, chat sites, etc.) to prevent employees from wasting time when they should be working.

There are hundreds of blocking programs available, ranging from those intended for home users (NetNanny, Cybersitter) to powerful enterprise-level packages such as those made by SurfControl, Websense, and GFI referenced above.

5 Filter Web access by keywords

The problem with URL or domain name filtering is that you have to know the URLs of the sites you want to monitor or block. Many companies maintain blacklists of Web sites that have been determined to be undesirable according to particular criteria (including the vendors of most Web-blocking software). However, even if these lists are updated frequently, it's doubtful they'll contain all undesirable Web sites.

Instead of blocking sites just by address, some application filtering firewalls and add-on Web-blocking programs can filter sites by keywords.

6 Monitor incoming and outgoing e-mail messages

You can monitor employees' e-mail messages using programs such as [Spector CNE](#) from SpectorSoft. It combines the features of its Spector Pro monitoring software for consumers with installation, configuration, and deployment capabilities for corporate networks. You can automatically capture and review both sent and received messages and set up alerts to notify you instantly if particular words or phrases are detected. CNE also monitors IM communications, Web browsing, and other Internet activity and includes keystroke logging and snapshot recording.

7 Monitor instant messages (IMs)

Because they're exchanged in real time and users sometimes type before they think, instant messages are often a source of security breaches. You can block instant messaging altogether by configuring your firewall to block the ports used by IM programs or by using software such as [Akonix Enterprise](#) or [IMlogic IM Manager](#). However, since instant messaging can actually be useful in the business environment, assisting customers and enabling instantaneous communications with co-workers, vendors, etc., you may prefer to control it rather than block it. The Akonix and IMlogic programs can also be used to control and monitor IM communications by applying policies to specific groups and users and capturing usage statistics and other information. You can, for example, allow chat but prohibit file-sharing features of IM programs.

8 Use keyloggers to capture typed data

Keyloggers record all information that's typed on a computer's keyboard and come in two types: hardware- and software-based. The hardware devices, such as KeyGhost, are small devices that install between the keyboard's connector and the PS2 or USB port on the computer. Software keyloggers can be configured to send the captured keystrokes to you on a remote computer and are often included as part of the functionality of a more broad-based monitoring program, such as CNE, or less expensive, consumer-oriented programs, such as SpyRecon.

9 Use screen capture tools to find out what users are doing

Like keyloggers, screen capture utilities are often included in monitoring packages. Unlike keyloggers, they enable you to monitor what your employees read on their screens, not just information they type in. So in addition to finding out the URL of a Web site an employee visited, you can actually see the site that was displayed on his or her screen, an opened Word document or graphics file, the contents of a dialog box, a video game being played by the employee.

10 Control what software employees can install or run

You can use built-in tools in Windows XP and Server 2003 to control employees' installation and running of software. Prevent users from installing programs via Group Policy's User Rights and use the Software Installation feature to manage the distribution of software throughout the organization. Then, you can use Group Policy's Software Restriction Policies to identify software running on your network's computers and to control whether those programs can run.

Additional resources

- TechRepublic's [Downloads RSS Feed](#) **XML**
- Sign up for our [Downloads Weekly Update](#) newsletter
- Sign up for our [Network Security NetNote](#)
- Check out all of TechRepublic's [free newsletters](#)
- ["Web filtering software is just one piece of the Internet usage policy"](#) (TechRepublic article)
- ["Top 10 valuable \(but underused\) Microsoft security technologies"](#) (TechRepublic download)
- ["Information Security Policy"](#) (TechRepublic download)

Version history

Version: 1.0

Published: January 23, 2006

Tell us what you think

TechRepublic downloads are designed to help you get your job done as painlessly and effectively as possible. Because we're continually looking for ways to improve the usefulness of these tools, we need your feedback. Please take a minute to [drop us a line](#) and tell us how well this download worked for you and offer your suggestions for improvement.

Thanks!

—The TechRepublic Downloads Team