Echo•Suite™ User Guide

Version 7.0

Table of Contents

Chapter 1

Getting Started

Welcome

Introducing Echo•Suite™®, a comprehensive employee Internet management package from Pearl Software. This premier tracking utility is the industry model for employee Internet access management and represents the most significant step available today in promoting responsible Internet use in the workplace. Featuring Pearl Software's Mobility Monitor™ technology, Echo•Suite can effectively block inappropriate sites or set time restrictions on Internet use, regardless of where end-users reside. But what makes Echo•Suite most unique is its intrinsic ability to monitor email, chat/instant messaging (IM) and news group postings and provide detailed access profiles to your network administrator. Echo•Suite's Quick-Link feature allows automatic links to visited web sites, and Echo•Suite can restore all text from outbound and inbound communications. Echo•Suite is a powerful application, offering dynamic filtering, reporting and knowledge management functions to assist you in fulfilling your regulatory compliance and corporate governance requirements.

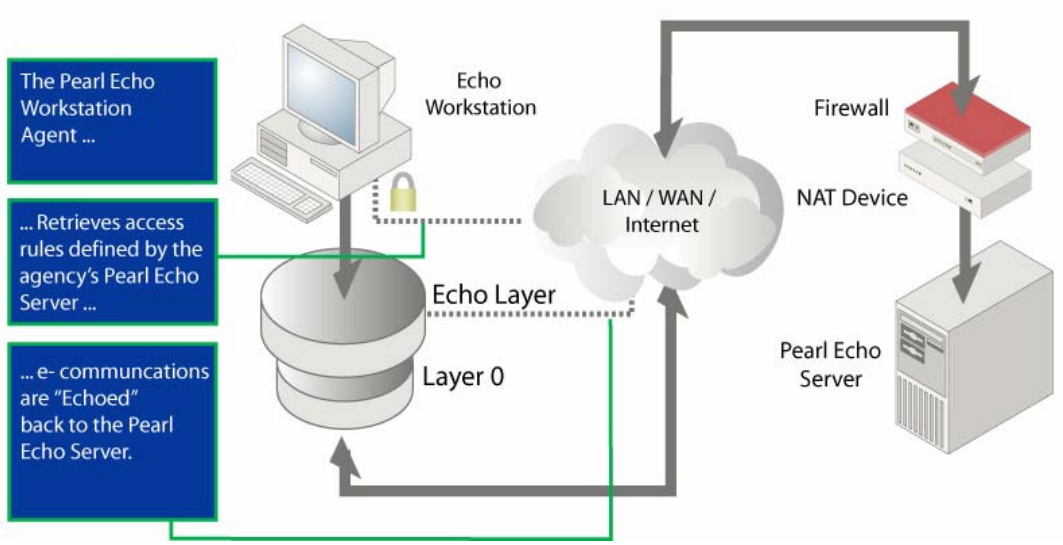
About this User Guide

The Echo•Suite User Guide describes Echo•Suite's features and functions as well as installation instructions and deployment strategies. It is assumed that the reader has a general understanding of TCP/IP networking concepts as well as Microsoft Windows® operating systems. This guide is supplemental to Echo•Suite's context sensitive help found in the Echo•Suite Administration Console under the program's Help menu.

Echo•Suite Architecture

Echo•Suite's Employee Internet Management technology is based on an independent agent-server architecture. By creating an independent service, Echo•Suite is not affected by high traffic volumes, how users access the Internet, or where your end users are physically located. Echo•Suite's Employee Internet Management technology does not suffer from the performance and security problems of proxy monitoring solutions or from the overload and network dependency limitations of network sniffer solutions.

The Echo•Suite Server software runs as an independent service resident on one of your Windows Domain or Stand Alone Servers or on a Windows Workstation. The Internet access rules you create at the Echo•Suite server are retrieved by your managed workstations through a secure, zero-maintenance agent loaded on your Windows workstations.



The same secure, zero-maintenance agent is responsible for sending -- or echoing -- actual or attempted Internet transactions back to the Echo•Suite server. For ultimate efficiency, Internet access decisions are made at the client agent. Data to be logged is first compressed by the agent before being sent back to the server on a path that is not dependent upon the path the workstation uses to access the Internet. The Echo•Suite Workstation agent can be installed from the Echo•Suite CD or automatically deployed by the Windows Installer files provided with Echo•Suite. Once deployed, the Echo•Suite Workstation agent is self-updating; the Workstation agent automatically gathers any updates or upgrades to Echo•Suite when you update your Echo•Suite server.

With Echo•Suite's Mobility Monitor™ technology, managed workstations can be connected to your local area network, wide area network or completely detached from your private network. The Echo•Suite Workstation agent does its job no matter how or where your users connect to the Internet.

Echo•Suite's Employee Internet Management technology is extremely efficient, adds negligible network traffic and scales well due to its client-server architecture. Depending on the size of your network, loads can be balanced by running multiple Echo•Suite services and pointing workstations to the appropriate server.

Because Echo•Suite runs as its own service, Echo has no dependences on legacy Proxy Servers or Firewalls.

Installing Echo•Suite

☑ **You can automate workstation installation using the included Windows Installer Service files.**

Step 1: Echo Server Installation

The Echo•Suite Server Software can be installed on any supported Microsoft Windows platform whose IP address can be directly or indirectly (NAT) accessed by your managed workstations. The Echo•Suite Server Software is typically installed on a shared or dedicated Windows Server platform but can even be installed on a Windows Workstation platform. If you would like to set Internet access privileges based on existing Active Directory User or Group names, you should install Echo•Suite Server Software on a machine that is a member of your Domain. The machine can be a Windows Domain Controller but need not be as the Echo•Suite service is Domain-Aware and will automatically find your database of Active Directory Users and Groups[1]. If you have not yet migrated to Active Directory, Echo•Suite will automatically revert to the machine's local list of Users and Groups. Echo•Suite will even accommodate smaller peer-to-peer installations and allow you to set Internet access profiles based on local login names. Regardless of your environment, there are no complicated setup steps for you to worry about. The Echo•Suite Server Software will automatically sense its environment and will configure itself accordingly.

Follow these steps to install the Echo Administration Console and Monitoring Service:

1. Turn off Anti-virus & Spyware Removal applications prior to beginning installation.
2. Run setup.exe from the program installation folder or from the installation CD.
3. On the Startup screen, "click" the **Server Setup** Button.
4. The InstallShield Wizard will walk you through the initial installation procedures and prompt you to confirm the default installation settings.

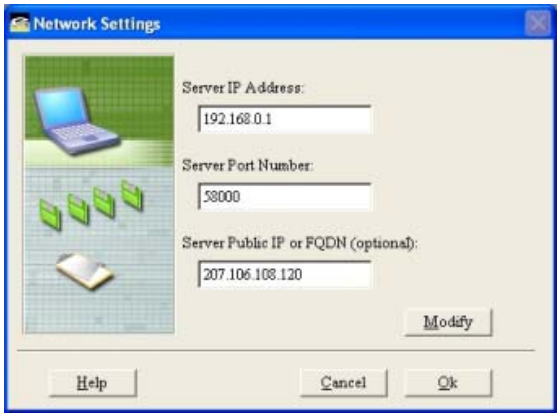
TIP
Please note the destination location for your installation as you will need to exempt this folder from your antivirus & antispyware applications.

The default location for this installation is C:\Program Files\Echo 7.0 or you can specify a different location to install the application.

5. Configure your antivirus and antispyware applications to **exclude the Echo•Suite program file directory folder that you created in step 4** (e.g. c:\Program Files\Echo 7.0) from being scanned.

[1] The Active Directory container(s) of your Users and Group members, resident on your domain computer(s), are mapped by the Echo Server. It is recommended that the computer running the Echo•Suite Server be explicitly added to the list of security objects for your User and Groups containers and the computer be given read permissions on those containers.

6. Launch the Echo•Suite Administration Console from the Programs section of the Windows Start button.
7. Confirm/Enter your IP configuration
   a) When prompted, confirm or enter the **fixed IP address your machine** (IP address cannot be assigned through DHCP or through any other means).
   b) We recommend that you use the default Port number 58000.
   c) Enter the Public IP or FQDN of the Echo Administrative machine if any of the managed end-user machines will roam outside of your local network. To manage users while they roam outside of your local network, you will need to configure your firewall to allow the roaming Echo•Suite Workstation agent to make a connection back to the Echo•Suite server. Please refer to the Echo Suite 7 User Guide's Advanced Installation instructions for additional information on managing your remote users.



8. Confirm the environment that will be managed through this application. We recommend selecting PC's with Updated applications as your default environment.
   a) If you would also like to evaluate Echo•Suite™ 7 on your Terminal Server, Citrix Server or other thin clients, include this environment in your setup options. Please refer to the Echo•Suite™ 7 User Guide for detailed instructions on managing server-centric installations.
9. Enter a password to use when connecting to the Echo Administration Console.
10. Confirm that you wish to turn Echo•Suite Internet Management on now. This setting must be **ON** to begin the Echo Workstation Installation.
11. We recommend that you ***Accept Defaults*** from the Profile Wizard interface. Please refer to the *Echo Suite User Guide* for detailed configuration settings.

☑If your installation machine has multiple IP addresses or NIC Cards, the IP address entered during Echo Server Setup will serve your local network workstations and must match the IP address that will be entered during the Workstation Installation.

☑When installing the Pearl Echo Workstation software on Exchange Server, from the setup screen select "Options" and "This Machine is an Exchange Server". Refer to Chapter 2 detailed information on advanced installation topics.

Step 2: Echo•Suite Workstation Installation

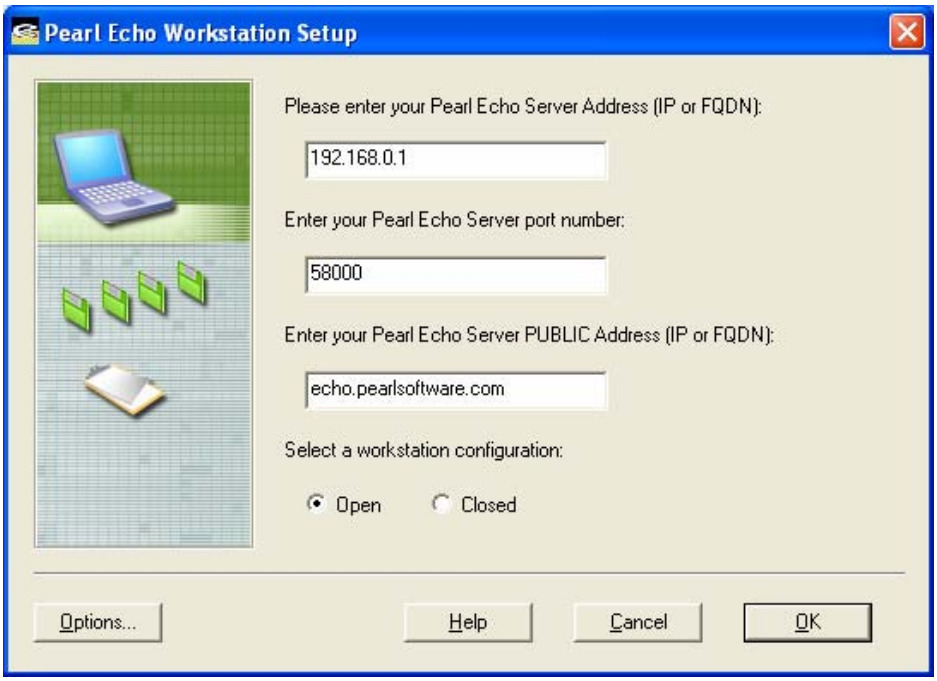
The Echo•Suite Server Software must be installed and running to install the Echo•Suite workstation agent.

Note: Before installing Echo•Suite workstation components on Windows 95, verify that the workstation is running the latest version of Microsoft's Winsock2 (available in the Utilities directory on the installation media).

You can configure your managed workstations to have either full (Open) or restricted (Closed) access to the Internet if the Echo•Suite Service is not available on your server. Please note, if you are running an evaluation version of Echo•Suite, the Echo service will not be available once your trial period has expired. After expiration, a closed workstation's Internet access will be interrupted. The Echo Service may also be unavailable due to server maintenance, network problems, etc.

Follow these steps to manually install the Echo Workstation Agent:

1. Login to the workstation using an account with Administrator privileges.
2. **Turn Off** all antivirus, antispyware and disk utility applications before beginning workstation installation.
3. Run setup.exe from the program installation folder or from the installation CD.
4. Click ***Workstation Setup*** from the startup screen.
5. Enter the Echo Server FQDN or IP address entered in step 7(a) of the Echo Server Software Installation above.
6. Enter the Port number that you specified during the Echo Server Installation in Step 7(b) above.
7. If the workstation will roam outside of your private network, enter the Public IP or FQDN of your Echo Server entered in Step 7(c) above. To manage users while they roam outside of your private network, you will need to configure your firewall to allow the roaming Echo•Suite Workstation agent to make a connection back to the Echo•Suite server. Please refer to the Echo Suite 7 User Guide's Advanced Installation instructions.



8. Select a workstation configuration. **Open** configuration is recommended during evaluation.

TIP

Pearl Echo provides fail-safe operation if connectivity between a workstation and the Pearl Echo Server is interrupted. You can configure your managed workstations to have either full access (open configuration) or restricted access (closed configuration) to the Internet if the Pearl Echo Monitoring Service is not available due to maintenance, network problems, etc.

If you are running an evaluation version of Echo, the Echo Monitoring Service will not be available once your trial period has expired. After expiration, Internet access will be interrupted on a workstation installed with the closed configuration.

9. The workstation will perform a test communication with the Echo•Suite Service and will display the results. If a link can be established, reboot your Echo workstation to complete the installation.

TIP

During your initial installation, if your workstation does not communicate with your Pearl Echo server, the following are common issues that may need to be addressed:

- **Make sure you have correctly identified and set your Administration machine's FIXED IP address in the Pearl Echo server software under the Options->Network Configuration menu.**
- **Test visibility of your server from your workstation by pinging the machine on which you installed the Pearl Echo Server software.**
- **If a firewall is installed on or between your Pearl Echo Server and managed Workstations, please be sure to make the firewall port assignments as detailed in Chapter 2 of the Echo•Suite™ 7 User Guide.**
- **Make sure your Pearl Echo management is On in the Pearl Echo server software under the Security->Set Security Status menu.**

Additional troubleshooting tips are available in the Appendix of this User Guide.

10. Configure your antivirus and antispyware applications to **exclude the Echo•Suite Workstation program file directory folder.** You will also need to configure anti-virus and antispyware applications to not disturb the Echo•Suite Workstation Agent or its components. Refer to this Guide's Appendix for detailed guidelines.
11. Now that you have installed the Echo workstation monitoring agent, begin browsing the Internet from this workstation or, if applicable, send IM and/or email messages from this workstation to test your initial setup.

12. Return to your Administration Machine and launch the Echo•Suite Administration Console to view the monitored activity. You should see the workstation's Internet activity presented in the Echo•Suite Activity Log.

    - If you do not see the workstation activity, you might need to refresh your Echo•Suite Server activity log from the File menu or by hitting the F5 key.

13. **Congratulations!** You have successfully completed the initial installation Echo•Suite™ 7.

TIP

Within your Echo Software is a context sensitive Help Menu with deployment procedures and tips to help you continue a successful implementation using more advanced deployment options such as: creating unique user profiles, setting security and time controls, configuring automated Workstation installations and scheduling automated activity reports.

For detailed information on these tips, please refer to the section titled *Advanced Installation* in this document.

Upgrading from a Previous Version of Echo•Suite

Echo•Suite Version 7.0 will automatically gather your existing settings from previous installations.

Server Upgrade

Before installing and activating the Version 7.0 Server Software,

1. Login to the Administration Console of your previous version of Echo•Suite and turn monitoring OFF from the Set Security Status menu.
2. Make note of your network settings in the Options->Network Settings menu. You will need these settings if you would like to monitor existing Echo•Suite Workstation installations with your Version 7.0 Server.
3. Close the Echo•Suite Administration Console.

Install and activate Echo•Suite Version 7.0 in a new program directory. When prompted, use the same IP and Port settings as your previous installation. Your pervious version's access control profiles, controls lists and report settings will automatically appear in your new installation.

Workstation Upgrade

Previous versions of the Echo•Suite Workstation software are fully compatible with the new Echo•Suite 7.0 Server. It is recommended, however, that you upgrade your Echo•Suite Workstation software in order to take advantage of the added benefits available in this latest version.

If you are upgrading your workstations to Version 7.0, you will need to uninstall your previous version of the Echo•Suite Workstation software before installing Echo•Suite 7.0 Workstation components. This can be accomplished by removing the software from the Workstation's Add/Remove Programs applet or automated with use of scripts provided by Pearl Software support. Because the Echo•Suite Workstation software is a secure installation, it cannot be removed with a Group Policy Object.

Once deployed, the Echo•Suite 7.0 Workstation agent is self-updating; the Workstation agent automatically gathers any updates or upgrades to Echo•Suite when you update your Echo•Suite server.

Starting Echo•Suite for the First Time

When you run the Echo•Suite Administration Console for the first time:

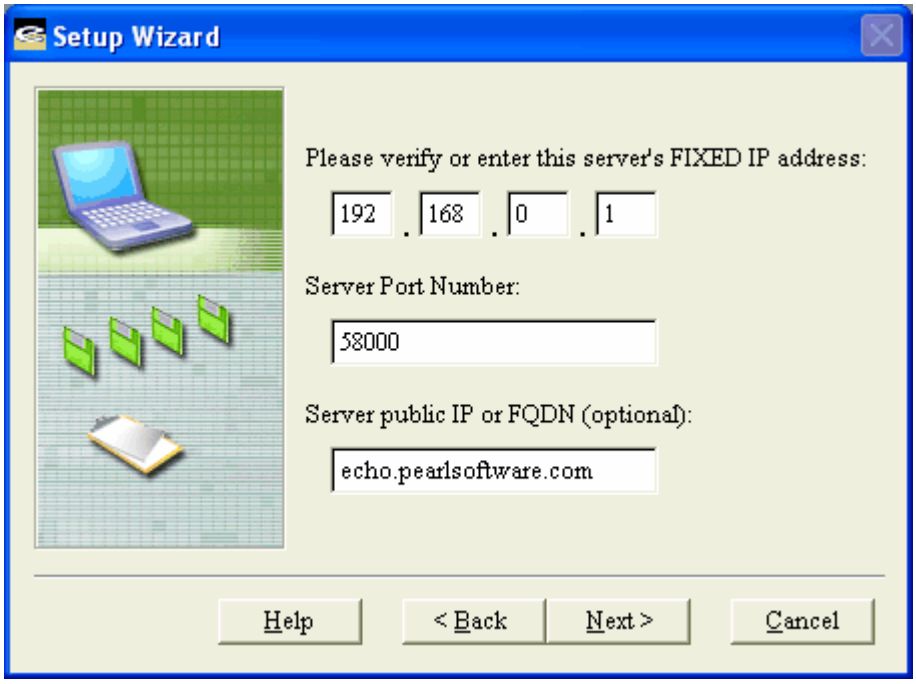
Step 1: Setup Wizard will ask you to register your name and serial number.

1. Enter your name as you would like it to appear on the Echo•Suite startup welcome screen.
2. Enter your product serial number exactly as provided with the distribution media or sales confirmation documentation. If you are evaluating Echo•Suite, enter the evaluation code in the Name field and leave the serial number blank. Your evaluation code was emailed to you when you registered for your trial software.

Step 2: Setup Wizard will ask you to confirm or enter your network settings.

☑**Your Pearl Echo Server can be set to operate through a NAT or Firewall device. More on this in Chapter 2.**

Setup Wizard will ask you to verify or enter the IP address of your server and a service port number. If you would like to monitor users that roam beyond the perimeter of your private network, enter the Public IP or FQDN of your Echo•Suite Server.



Note: For detailed information on configuring Echo•Suite to work with Network Address Translation (NAT) or through a Firewall, please refer to Chapter 2, *Advanced Installation.*

Step 3: Setup Wizard will ask you to describe your computing environment.

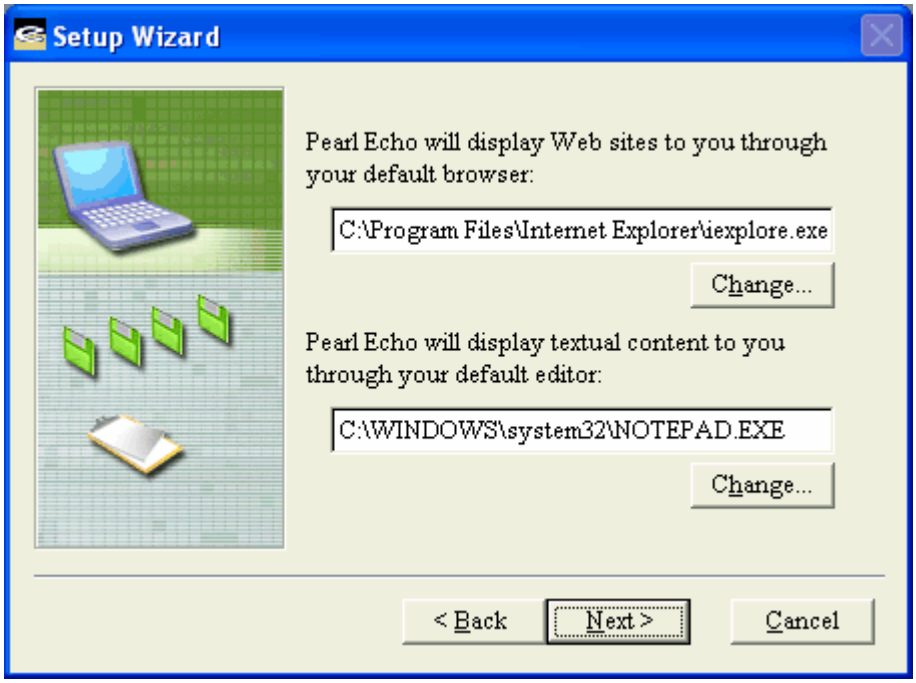
Setup Wizard will ask you about your computer environment. By default, Echo•Suite will automatically detect Internet applications running on your managed workstations. To reduce resource overhead and to accommodate legacy applications that don't conform to Microsoft's Winsock2 specifications, Echo•Suite can be configured to monitor only applications that you specify.

Step 4: Setup Wizard will ask you to enter and confirm your administrative password.

Your password can be any combination of numbers and letters. Upper and lower case letters are not treated the same. Passwords are limited to less than twenty characters.

Step 5: Setup Wizard will automatically configure your default browser and your default text editor.

These defaults are determined by your current system configuration. This enables Echo•Suite's Quick Link™ feature and the restoration of Email, News, Chat and Instant Messaging text.



You can change the default values if you have a preference for applications other than your system defaults.

Step 6: Setup Wizard will ask you if you want to begin monitoring Internet activity.

When Setup Wizard finishes, Echo•Suite will start the Profile Wizard.

The Profile Wizard will walk you through selecting Echo•Suite's most common settings. Any settings you make in the Profile Wizard can be changed later from within the Echo•Suite Administration Console. When the Configuration Wizard finishes, the Echo•Suite Administration Console will prompt you to log in for the first time.

Uninstalling Echo•Suite

The Echo•Suite Service authenticates Echo•Suite Workstation uninstall requests. The Echo•Suite Service must be running to securely uninstall workstation components. To run the Echo•Suite Service, set the Internet Management State to "ON" in the Echo•Suite Administration Console.

To Uninstall Echo•Suite Workstation Software

1. From the workstation taskbar, click on Start and select Settings.
2. Select the Windows Control Panel.
3. Select Add/Remove Programs.
4. From the Install/Uninstall tab, click on ec70ws.
5. Select the Add/Remove button.
6. Enter your Echo•Suite password and follow the instructions as they appear on the screen.

Echo•Suite will log successful and unsuccessful attempts at uninstalling the Echo•Suite Workstation software. Echo•Suite will also log when the Workstation's network configuration has been altered.

To Uninstall Echo•Suite Server Software

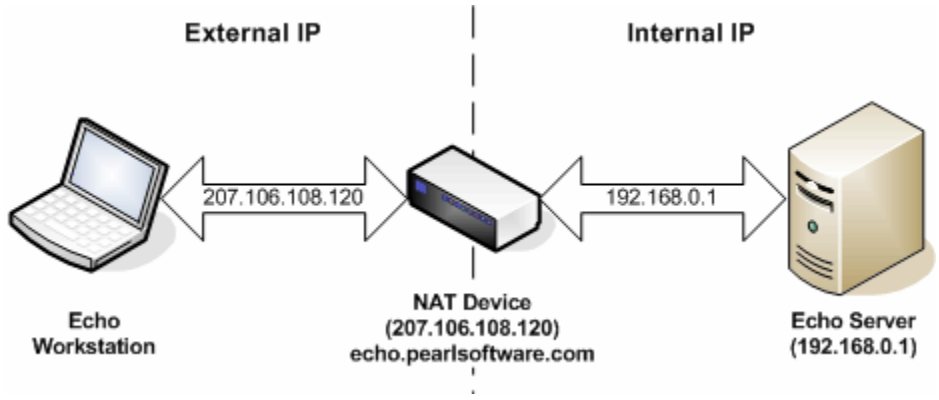
1. Run the Echo•Suite Administration Console.
2. From the Security Menu, select Set Security Status.
3. Turn the Echo•Suite Management State "OFF" and exit Echo•Suite.
4. Select the Windows Control Panel.
5. Select Add/Remove Programs.
6. From the Install/Uninstall tab, click on EC7.0.
7. Select the Add/Remove button.

Chapter 2

Advanced Installation

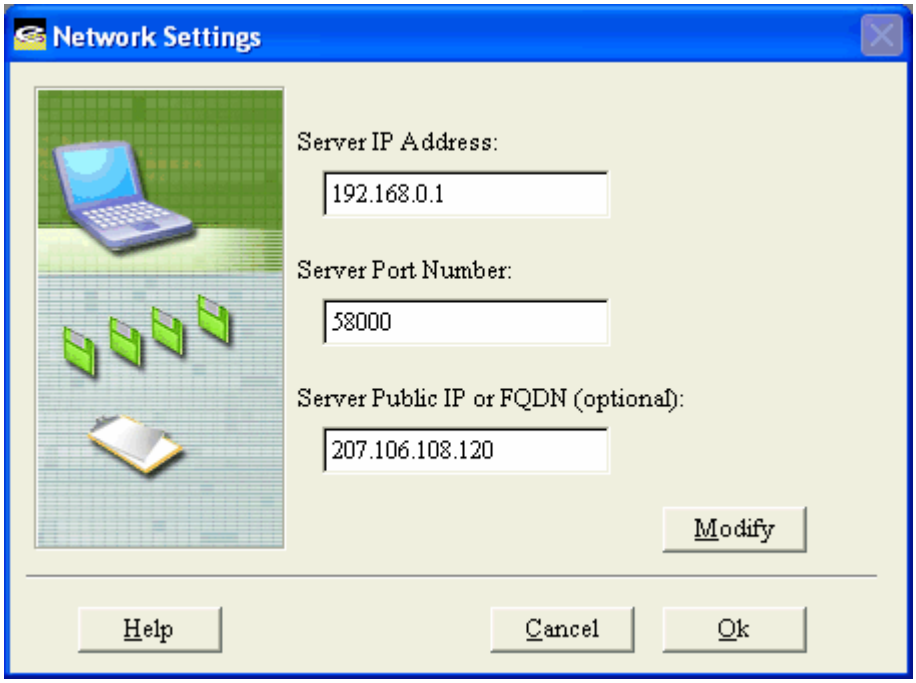
Network Address Translation

Echo•Suite can be configured to work with Network Address Translation (NAT). Use this configuration if the NAT device provides IP and PORT translation between the internal Echo•Suite Server and external or roaming Echo•Suite Workstations.



1. Start the Echo•Suite Administration Console.
2. From the Security Menu select Set Security Status.
3. Turn Echo•Suite Internet Management OFF.
4. From the Options Menu select Network Settings.
5. Enter the External IP address or Fully Qualified Domain Name (FQDN) of the NAT device in the "Server Public IP or FQDN" box.
6. From the Security Menu select Set Security Status.
7. Turn Echo•Suite Internet Management ON.

NOTE: A Fully Qualified Domain Name provides greater flexibility if your server IP address changes due to server upgrade or network architecture changes.

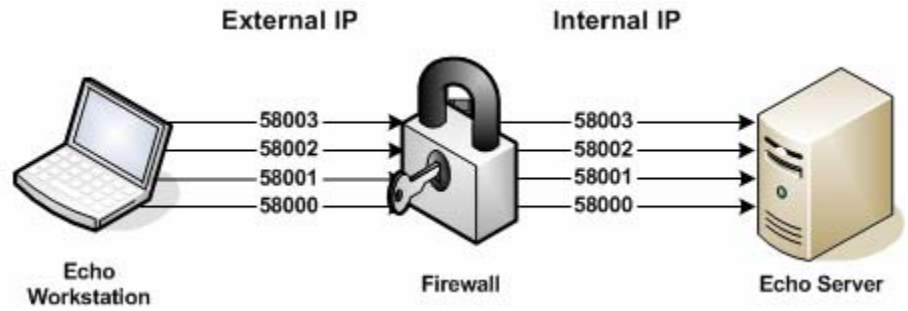


Firewall Settings

Echo•Suite's Mobility Monitor™ connects through a Firewall device utilizing a specified group of ports. Echo•Suite workstations establish an initial connection with the Echo•Suite Server on a Control Port (Server Port Number). Additional command and control communications occur on three supplemental IP ports. The Server Port Number (e.g. 58000) and three additional IP ports (e.g. 58001, 58002 and 58003) will need to be opened for direct pass-thru on your Firewall device.

Public IP: Server Port Number + **0** ↔ Private IP: Server Port Number + **0**
Public IP: Server Port Number + **1** ↔ Private IP: Server Port Number + **1**
Public IP: Server Port Number + **2** ↔ Private IP: Server Port Number + **2**
Public IP: Server Port Number + **3** ↔ Private IP: Server Port Number + **3**

Example:



The Echo•Suite Monitoring Service residing the Echo Server communicates with the Echo•Suite Workstation Agent through a proprietary protocol. Connections to the Echo•Suite Monitoring Service that don't communicate with the Echo•Suite protocol are dismissed.

The Echo•Suite Server Port Number setting is accessed from Network Settings in the Echo•Suite Administration Console's Options Menu.

Terminal/Citrix Server Setup

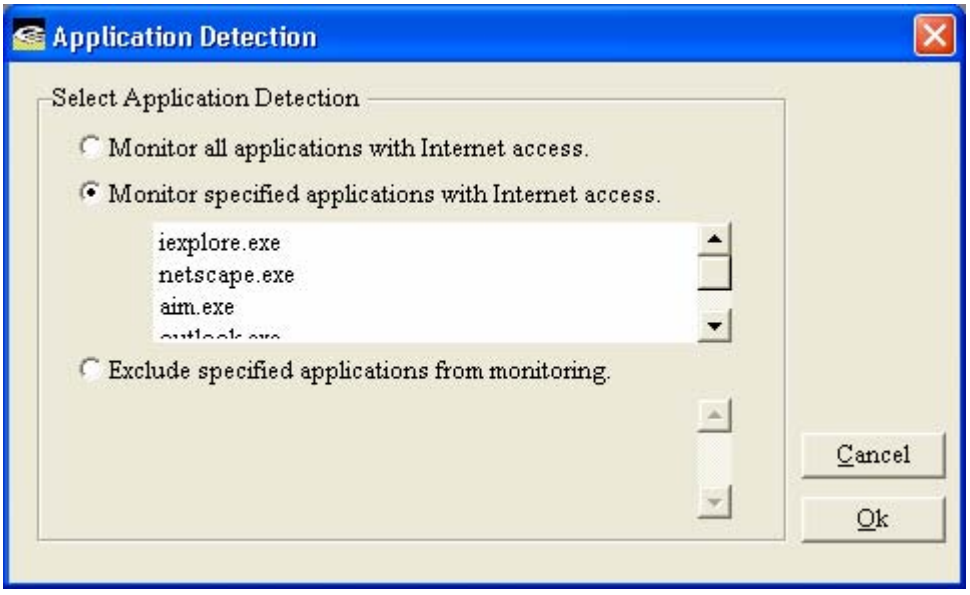
Echo•Suite is fully functional in a Terminal/Citrix Server environment. To operate in a Terminal/Citrix Server environment, install the Echo•Suite Server Software as described in *Echo•Suite Server Installation* above, on any Windows platform other than your Terminal/Citrix Sever.

Next, install the Echo•Suite Workstation software on your Terminal/Citrix server as detailed above in *Echo•Suite Workstation Installation*. Once installed, each Terminal/Citrix desktop session will run its own instance of the Echo•Suite Workstation agent and will be fully managed by settings you specify in the Echo•Suite Administration Console.

Echo•Suite will also monitor each user's session, even if the session is run as a *published* application. For more information on managing published applications, please refer to the online article, "Using Echo•Suite to Monitor Published Applications on Citrix and Windows Terminal Server" located at www.pearlsw.com/support.

Echo•Suite has been optimized for a server-centric multi-user environment. The Echo•Suite Agent is extremely efficient, has a small memory footprint and adds negligible network traffic. To further optimize performance of your Terminal/Citrix sessions, it is recommended that you specify the applications you would like to manage using Echo•Suite.

☑Administrators can define the applications to be managed through Echo by selecting "Application Detection" in the Options menu.



Managing Exchange E-mail at the Exchange Server

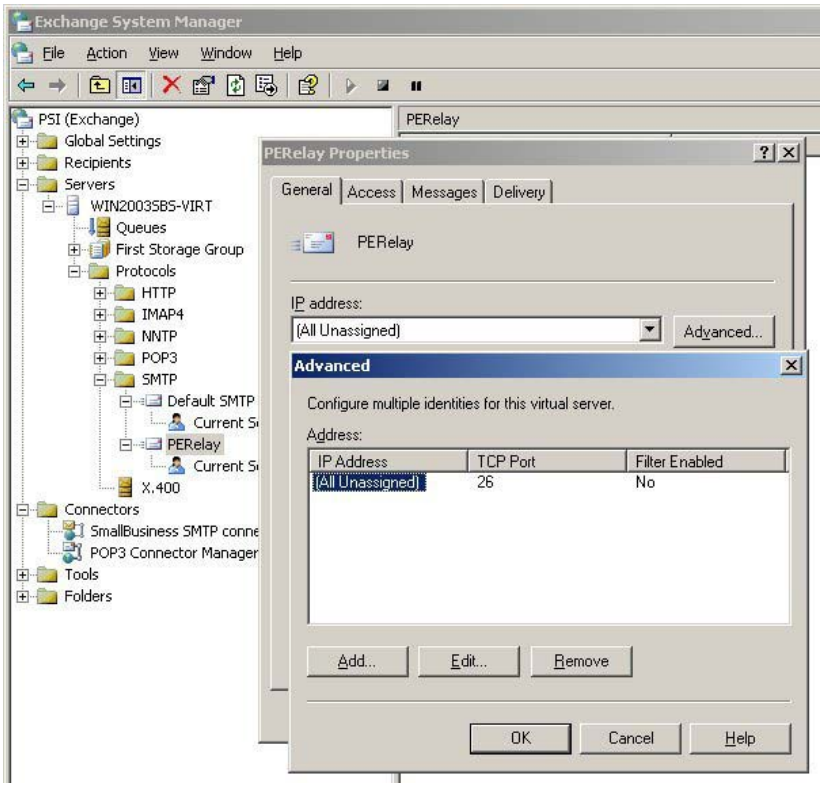
Echo•Suite monitors Microsoft Exchange Mail activity at the Exchange Server through the SMTP service without requiring modification to the Exchange Mail clients. By default, the Exchange service and the SMTP service are closely coupled and communicate using a proprietary protocol. In order for Echo•Suite to monitor the Exchange Mail this protocol needs to be set to SMTP.

Step 1: Configuring your Exchange Server

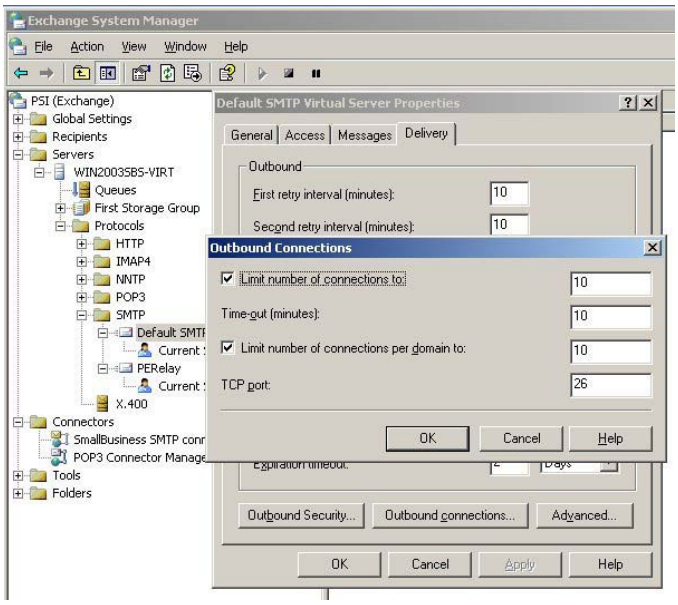
The following two scenarios outline the procedure for configuring the SMTP protocol in your Exchange Server.

Scenario 1: Configuring Your Standalone Exchange Server

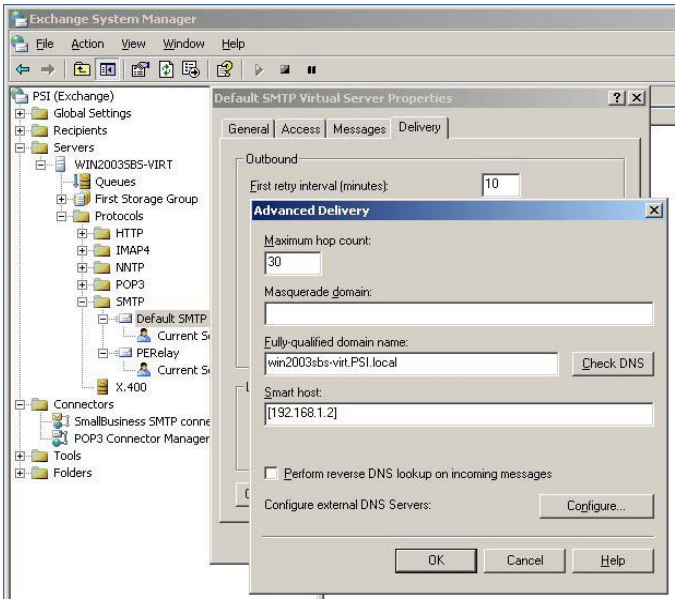
1. Run the Exchange System Manger.
2. Create a **new** SMTP Virtual Server
    a. Under server **Protocols**, create a new SMTP Virtual Server named "**PERelay**".
    b. Under **General Properties** of the PERelay SMTP Virtual Server, select **Advanced** and change the default TCP Port to **26**.
    c. Apply the changes and close the Properties for the PERelay SMTP Virtual Server.



3. Modify the **existing** Default SMTP Virtual Server
    a. Select **Delivery Properties** of the Default SMTP Virtual Server.
    b. Select **Outbound Connections** and set the TCP port to **26** and select **OK**.

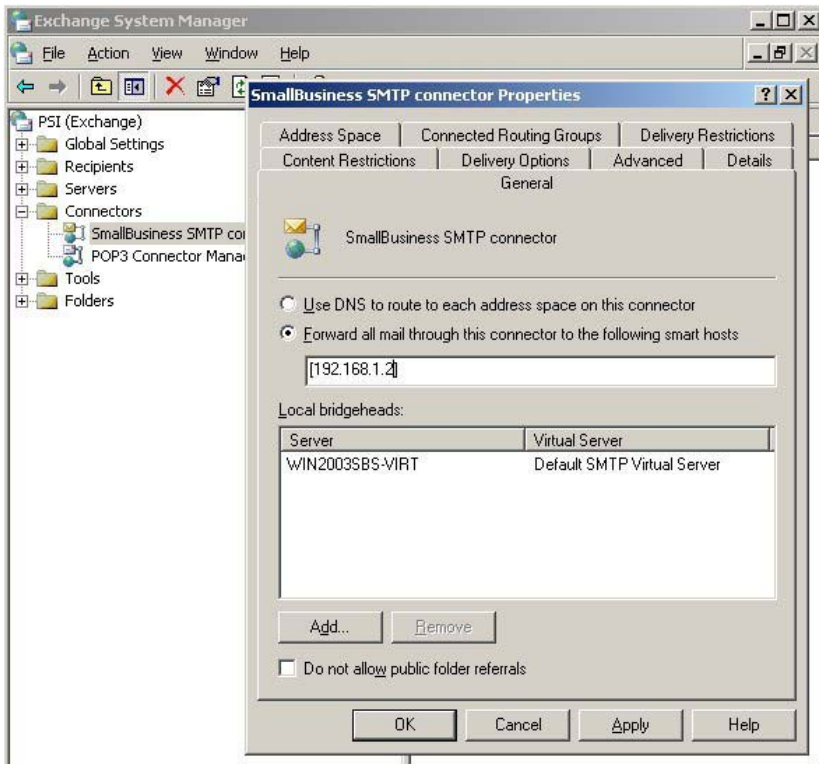


    c. On the same **Delivery Properties** tab, select **Advanced** and set the **Smart host** to the IP address of the standalone Exchange server using the bracketed IP notation [xxx.xxx.xxx.xxx].



    d. Select **OK** and **Apply** the changes.

4. Modify the existing SMTP **Connector**
    a. Under **Connectors**, select **General Properties** of the SMTP connector.
    b. Set the Internet mail connector to **foreword** mail through a **smart host** and specify the IP address of the stand alone server using the bracketed IP notation [xxx.xxx.xxx.xxx].



5. Test your changes by restarting your SMTP Virtual Servers and sending an email from an internal email account to an external email recipient.

Scenario 2: Configuring Your Border Exchange Server or Smart Host

Force outbound and inbound messages through a border Exchange server or smart host by using an SMTP connector. Place the Echo•Suite Exchange client on the border Exchange server or smart host. Because Exchange 2003 and Exchange 2000 servers communicate with each other through SMTP, all messages to a border server or to a smart host will be in the expected SMTP format.

Step 2: Install the Pearl Echo Workstation Software as a Service

To install the Echo•Suite Workstation Service for Exchange:

1. Run setup.exe from the installation media or download directory.
2. Select Workstation Setup.
3. When prompted by the setup wizard, enter the IP address and Port number you assigned when installing the Echo•Suite server software.
4. Select the **'Options'** button and then select **"This Machine is an Exchange Server"**.
5. Select OK.
6. The workstation will perform a test communication with the Echo•Suite Monitoring Service and will display the results. If a link is successfully established, your Echo workstation installation is complete. If you are unable to establish a link, please review the Troubleshooting Tips section of this User Guide.

Managing Exchange E-mail at the Exchange Client

Echo•Suite is designed to monitor any e-mail client using the POP3, SMTP or IMAP e-mail protocol. By default, Exchange e-mail clients communicate with the Exchange server via Exchange's native Remote Procedure Call (RPC) protocol. By making the following simple modification, Exchange e-mail clients can be configuring to communicate via the IMAP protocol without affecting Exchange's e-mail synchronization ability or any of Exchange's additional RPC functionality. In this configuration, no changes need to be made to your Exchange Server.

On the Exchange e-mail client:

1. Create an additional IMAP/SMTP e-mail account (Options->Accounts, in Outlook).
2. Specify the required information including your Exchange server as the IMAP and SMTP servers.
3. Set your new account as the Default mail account.

E-mail will now be received and sent through the Exchange server using the IMAP/SMTP protocol.

Automated Workstation Setup

Echo•Suite supports automating the Echo•Suite Workstation installation using the Windows Installer Service. When you assign an application to a computer, the application installation is performed when it is safe to do so. Typically this happens when the computer starts so that there are no competing processes on the computer.

Preparation

☑**Software Installation through Group Policy is available on Windows 2000 and later Operating Systems.**

Remote Software Installation is performed in conjunction with your settings in the configuration file, *servset.ini*, and the Windows Installer package supplied with Echo•Suite.

The first step is creating a network share, called a software distribution point, which contains the packages and the program and configuration files. Next you need to make sure that Domain Computers can read from the software distribution point and write to the target of the installation. Finally, you need to modify the configuration file, *servset.ini*, with settings that you entered during the Echo•Suite Server software installation.

1. Create a shared directory that contains the Echo•Suite Workstation installation files. Share the directory as *echows*
2. Assign the 'Read' NTFS permission for 'Domain Computers' on *echows* (Winlogon is the privileged agent that applies software installation policy when each computer starts. Winlogon requires read permissions to the source files to complete the installation).
3. Edit the file servset.ini in the new directory and specify the server IP and Port that you entered during the Echo•Suite Server Software installation. In addition you will need to specify your configuration preference - open or closed. If you have users that will roam outside of your private network, you can optionally enter the public address (FWIP) of your Echo•Suite server.

   Example:
   [Echo 7.0 settings]
   IP=192.168.0.1
   FWIP=echoservername.mycompany.com
   Port=58000
   Configuration=open

Setting Group Policy

Software Installation works in conjunction with Group Policy and Active Directory. In order to ensure that the Echo•Suite Workstation software does not get installed on your Domain Controller(s), the Group Policy Object that is created should have the appropriate security filters set.

1. Open Active Directory Users and Computers from Administrative Tools.

2. In the console tree, right-click the domain or organizational unit for which you want to set Group Policy.
3. Click **Properties**, and then click the **Group Policy** tab.
4. Click **New** to create a new Group Policy object and rename the object *echows_gpo*.
5. Click **Properties** of *echows_gpo*.
6. Click **Security**
7. Remove **'Authenticated Users'** from the ACL
8. Add **'Domain Computers'** to the ACL and assign **'Read'** and **'Apply Group Policy'** permissions.
9. Verify that **'Domain Controllers'** is not part of the ACL.
10. Click OK

To set the Software Installation Group Policy in the *echows* Group Policy object:

1. Click **Edit** *echows_gpo*.
2. Double-click Computer Configuration.
3. Double-click Software Settings.
4. In the console tree, right-click Software Installation and select **New Package**.
5. Enter the UNC name of the Echo•Suite Workstation installer file(e.g. *servername*\echows\Echo 7.0 Workstation.msi)
6. Select Assigned.

If you prefer to mask the software title from appearing during installation on Domain Computers, you can edit the properties of the new Software Installation entry. The next time a workstation in the domain starts, it will automatically install the Echo•Suite 7.0 Workstation software and configure the installation to access the Echo•Suite Server specified in *serverset.ini*.

Important Note: Because the Echo•Suite Workstation software is a secure installation, it cannot be removed with Group Policy Object. Removing the software can only be accomplished from the Workstation's Add/Remove Programs applet or automated with scripts provided by Pearl Software support.

Automated Workstation Setup using Logon Scripts

Echo•Suite supports automating the Echo•Suite Workstation installation using Windows Logon Scripts. To silently deploy the Echo•Suite Workstation agent:

1. Create a shared directory that contains the Echo•Suite Workstation installation files. Share the directory as *echows*
2. Create a blank file called firsttime.txt in the new directory.
3. Edit the file servset.ini in the new directory and specify the server IP and Port that you entered during the Echo•Suite Server Software installation. In addition you will need to specify your configuration preference - open or closed. If you have users that will roam outside of your private network, you can optionally enter the public address (FWIP) of your Echo•Suite server.

   Example:
   [Echo 7.0 settings]
   IP=192.168.0.1
   FWIP=echoservername.mycompany.com
   Port=58000
   Configuration=open

At login, the workstation will need to run the command

```
<path>\Setup.exe /s /v"/qn"
```

where <path> is the file path to the new directory (note: do not change spacing format around quotation marks)

The following is an example of running a silent install from a user's login script. Installation is run one time for each machine.

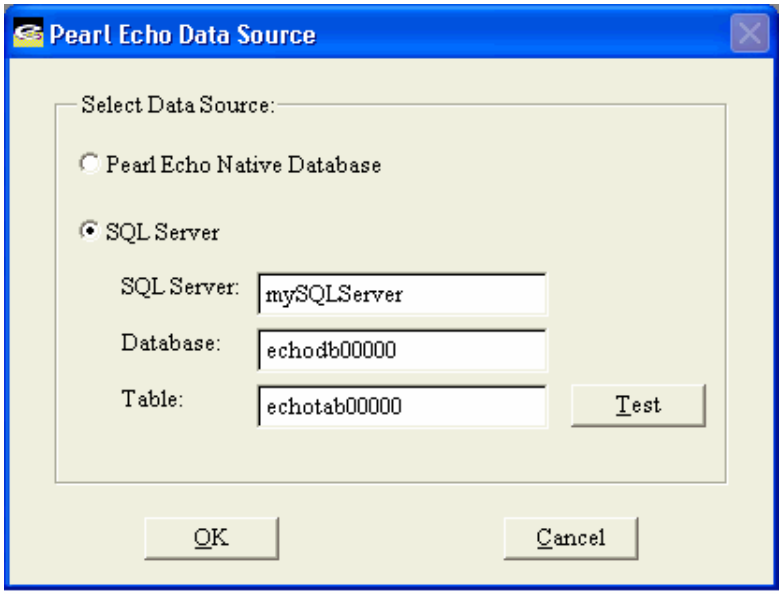
```
@echo off
'Checking for first time on target machine
if exist c:\firsttime.txt goto vend
copy \\servername\echows\firsttime.txt c:\firsttime.txt
\\servername\ echows \Setup.exe /s /v"/qn"
:vend
```

Integration with Microsoft SQL Server

Echo•Suite stores monitored Internet activity in its native Microsoft xBase database format. For installations with high volume monitoring loads and large storage requirements, Echo•Suite can be configured to store monitored Internet activity to a Microsoft SQL Server (version 2000 or later). The Echo•Suite Server Software can be loaded on the same server that is running Microsoft SQL Server or any other machine that resides in a trusted Domain. Data stored on Microsoft SQL Server can be viewed and reported upon from the Echo•Suite Administration Console. To configure Microsoft SQL Server:

1. Copy the Echo•Suite database (echodb00000) files located in the Utilities directory of the product CD to your SQL Server.
2. Remove the files' Read Only attribute.
3. Create a SQL Server user called echouser with password echopassword.
4. Attach to the Echo•Suite database by right clicking on Databases and selecting All Tasks->Attach Database in the SQL Server Console.
    a. SQL Server 2000: *While* attaching to the database, specify echouser as the database owner.
    b. SQL Server 2005: *After* attaching to the database, select Users for the echodb00000 database, add the username "echouser" with login name "echouser", and assign the role db_owner.
5. Create a network share named cache0000000000 and apply read and write permissions to the domain computer on which the Echo•Suite Server software resides. This share will be the location where Echo•Suite will store additional cached content.

To configure the Echo•Suite Server to store monitored Internet activity to the Echo database on Microsoft SQL Server, enter the Echo•Suite Administration Console and select Data Source Selection from the Options menu. Specify the name of the Microsoft SQL server and the database (echodb00000) and table (echotab00000) where Echo•Suite should log activity.



Chapter 3

Feature Overview

Echo•Suite tracks Internet activity by looking at content as it travels to and from a workstation computer via the computer's built in Winsock networking components. This approach enables Echo•Suite to run reliably and silently in the background. The only indication that Echo•Suite is running is the display of an optional warning message on the Workstation that can be configured in the Echo•Suite Administration Console.

Echo•Suite's Administration Console allows you to customize how you monitor and manage access to Internet Web, Email, Chat, Instant Messaging, News and FTP. Access Control Profiles are used to control the Internet access of individual users or groups of users. If you install Echo•Suite Server Software on a machine in a Windows Domain, User names and Group names are gathered from your Active Directory database. This enables better administration by eliminating the need to maintain separate profile accounts in the Echo•Suite Administration Console.

Monitoring Employee Internet Access

Echo•Suite allows you to retrace nearly every step an Internet user makes, by creating a complete audit trail of Internet activity, including site visits, file transfers, news group activity, chat, instant messaging, and email. Echo•Suite's Quick Link™ feature allows the password holder to automatically link back to the actual World Wide Web and FTP sites the user visited, or to restore the text of incoming and outgoing News, Email, Chat and Instant Messaging items. As a monitoring tool, Echo•Suite watches Internet activity and reports it back to you.

Managing Employee Internet Access

For managing Internet access, Echo•Suite provides fully customizable Allow and Block Control lists that are categorized into Web sites, FTP resources, Email addresses, newsgroups and chat/instant messaging. Internet Security control can be set to allow varying levels of access. Each segment of the Internet can be set independently with the default being set to allow and monitor all sites. Within the Echo•Suite Administration Console you can create Internet access Profiles in order to set varying levels of restrictions based on existing Windows User and Group definitions.

Echo•Suite can also be configured to block incoming and outgoing content based on an administrator-defined set of keywords. The primary focus of this feature is to protect against the dissemination of private information. This feature can also be used to block content that contains offensive material.

In addition to the above modes of control, Echo•Suite includes a set of categorized Echo Filters™ based on an automatically updating database of Internet domains. Using Echo•Filters you can provide access to Web content based on content type. There are over 40 Echo•Filters categories from which to choose include shopping, job search, adult, and web-mail portals to name a few.

Echo•Suite also supports the PICs rating standard. There are various rating systems that have been developed and are currently being used on the Internet. PICs rating systems attempt to characterize the nature of Web pages and other Internet content. Echo•Suite's PICs rating support allows you to control access to Internet content that has been rated by the content provider. While this content is self-rated, there are various third party organizations that strive to audit the validity of the content's rating.

Echo•Suite's comprehensive approach to managing employee Internet access provides you with the ability to customize access modes and immediately override and update blocked material.

Echo•Suite Security

Echo•Suite Server

Echo•Suite logs Internet activity to files on your Echo•Suite server. Since Echo•Suite runs as a network service, all Echo•Suite server files and configuration settings are well protected by your server's built in security. In order to function, the Echo•Suite server installation directory need not be accessible by users on your network.

Echo•Suite Workstation

Echo•Suite workstation files are protected by Echo•Suite's built in security. The workstation uninstall is password protected and file tampering will cause Internet access to be terminated. Additional security is provided via Windows ACL permissions on applicable Windows platforms.

Chapter 4

Using Echo•Suite

Signing In

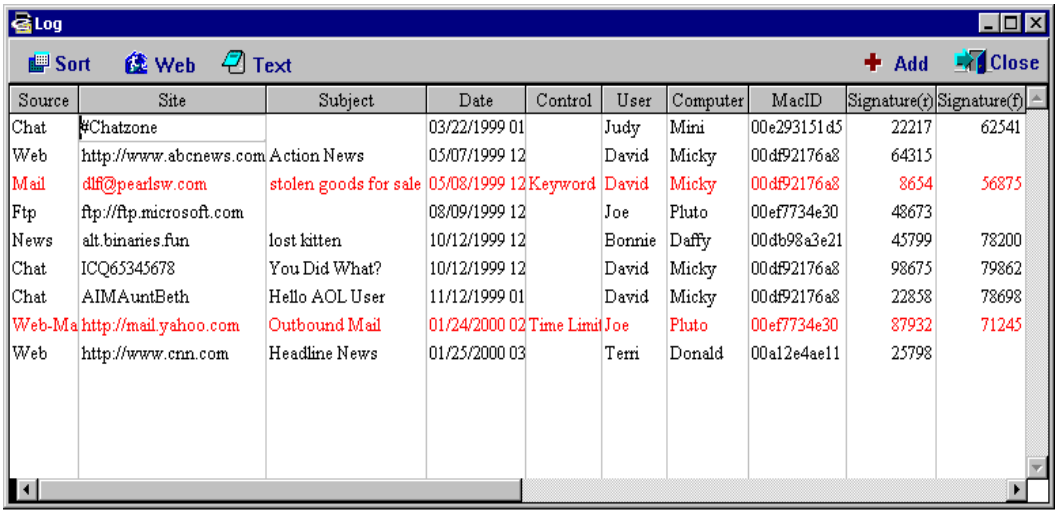
Each time you start the Echo•Suite Administration Console, you will be prompted for your login password.

After your password is confirmed, you will be presented with the most current copy of the Echo•Suite Activity Log. You can perform any file operation on your copy of the log without altering the integrity of the original Echo•Suite log.

The Echo•Suite Administration Console supports an Administrative and User level login. The User Level password allows users other than the administrator to view the Echo•Suite Activity Log and run Echo•Suite reports. All Echo•Suite features are available in the User Level except features that control Echo•Suite security configurations. The Administrative Level login allows access to all Echo•Suite features and settings.

Viewing the Activity Log

The Echo•Suite Administration Console automatically displays a copy of monitored Internet activity in the Echo•Suite Activity Log Window.



Source	Site	Subject	Date	Control	User	Computer	MacID	Signature(r)	Signature(f)
Chat	#Chatzone		03/22/1999 01		Judy	Mini	00e293151d5	22217	62541
Web	http://www.abcnews.com	Action News	05/07/1999 12		David	Micky	00df92176a8	64315	
Mail	dlf@pearlsw.com	stolen goods for sale	05/08/1999 12	Keyword	David	Micky	00df92176a8	8654	56875
Ftp	ftp://ftp.microsoft.com		08/09/1999 12		Joe	Pluto	00ef7734e30	48673	
News	alt.binaries.fun	lost kitten	10/12/1999 12		Bonnie	Daffy	00db98a3e21	45799	78200
Chat	ICQ65345678	You Did What?	10/12/1999 12		David	Micky	00df92176a8	98675	79862
Chat	AIMAuntBeth	Hello AOL User	11/12/1999 01		David	Micky	00df92176a8	22858	78698
Web-Ma	http://mail.yahoo.com	Outbound Mail	01/24/2000 02	Time Limit	Joe	Pluto	00ef7734e30	87932	71245
Web	http://www.cnn.com	Headline News	01/25/2000 03		Terri	Donald	00a12e4ae11	25798	

The Echo•Suite Activity Log presents Internet Activity by the following categories:

Source: The type of Internet activity being logged. This can be Web, Ftp, Email, News, Chat/Instant Messaging, or Web-Mail. Web-Chat and Instant Messaging are logged as Chat.

Site: The address of the Internet activity being logged. This can be a Web or Ftp location. It can also be an Email address, News Group name, Chat channel or Instant Messaging ID.

Subject: The subject or title of the activity being logged. For Email and News this will be the text that appears in the message subject line. For Web activity, the Web page title will appear here. This entry will remain blank for Ftp.

Date: The date and time of the Internet activity being logged.

Control: Displays the Echo•Suite Control that has restricted access to Internet content. Examples include Keywords, Ratings, Block List and Allow List.

User: The Microsoft Windows™ login name of the user being monitored.

Computer: The Widows computer name associated with the computer being monitored.

MacID: The Media Access Controller ID (MacID) of the monitored workstation. The MacID is a unique ID associated with the network card within a workstation.

Signatures: Data verification is performed at the Echo•Suite Workstation on all data sent to the Echo•Suite Server. Individual check-sums are performed on the logged record data (Signature-r) as well as associated file attachments (Signature-f).

Remote Administration

☑ **You can remotely access the Activity Log through a built -in Terminal Server or Remote Desktop connection.**

Echo•Suite configuration settings can be remotely administered with Remote Desktop, Terminal Services or any third party remote connection software. Echo•Suite uses a global protection mechanism to guard against access of the Echo•Suite Administration Console from simultaneous user sessions.

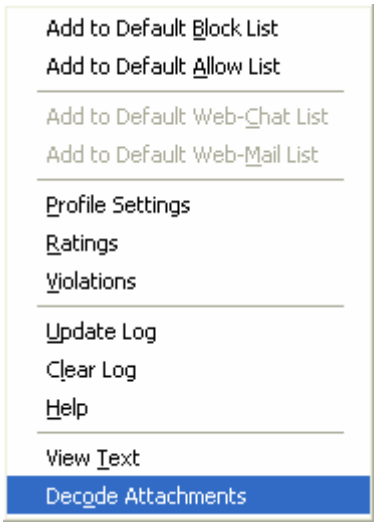
Viewing Logged Email, News, Chat & IM

Echo•Suite monitors and controls all Internet standard Email (Pop-3/SMTP/IMAP/Web-Mail), NNTP News, and Chat/Instant Messaging (IRC, AIM, MSN, Yahoo!, ICQ and Java™). Echo•Suite also monitors any Chat/Instant Messaging application that is based on the SIP protocol such as Microsoft Messenger for Communications Server. To view the content of incoming and outgoing Email, News, IM, and Chat:

1. Select the desired entry from the Echo•Suite Log Window.
2. Click on the Text Button or Double click on the desired entry.

You will be presented with the monitored text. Encoded attachments will also be referenced. You can decode and read any email and News attachment by

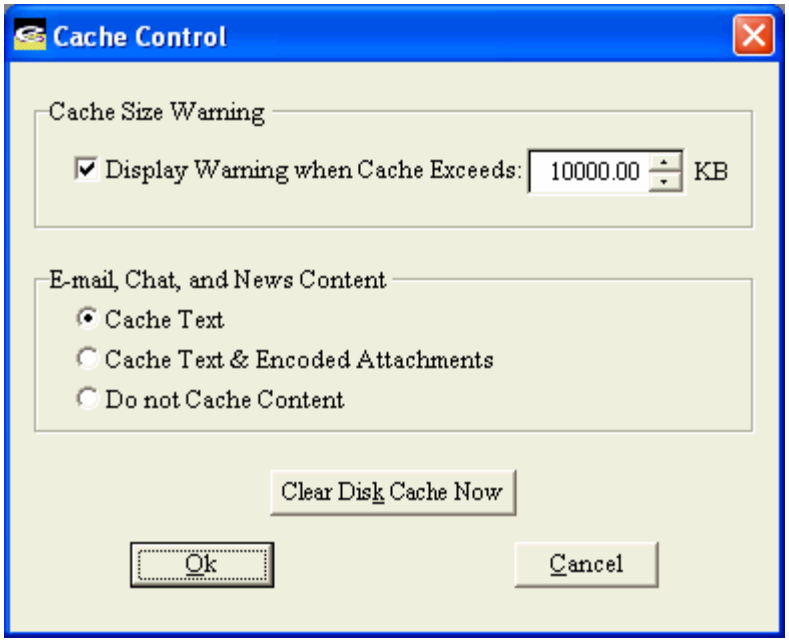
1. Right clicking on the desired entry from the Echo•Suite Log Window.
2. Selecting 'Decode Attachments' from the shortcut menu.



3. Selecting the destination folder in which to store the attachments.

The original decoded attachments will be available in the directory you specify. You will need the file's associated application or viewer to open or run the attachments.

To capture the text of Email, Chat, IM, and News postings, select "Cache Text" from the Cache Control menu. If you would like to log Email, News, Chat, and Instant Messaging activity without capturing content, select "Do not cache Content" from the Cache Control menu.



If you would like Echo to log a transaction's associated encoded attachments, select "Cache Text & Encoded Attachments" from the Cache Control menu in the Echo•Suite Administration Console.

Quick-Link™ to Logged Sites

You can use Echo•Suite's Quick Link feature to easily view the Web and FTP sites listed in your active Echo•Suite Activity Log.

1. To browse all sites, click the Web button on the active Echo•Suite Log Window. This will automatically start your default web browser with links generated from your Echo•Suite Activity Log.
2. To browse an individual site, double-click your mouse button on the log entry that you want to visit. You can also choose "Go to URL" from the shortcut menu. Your default web browser will automatically start and access the site of interest.
3. You can also generate a permanent copy of your web page by selecting the "Publish Browser Page…" item from the File Menu. This is useful if you would like to create an HTML version of your Echo•Suite Window in order

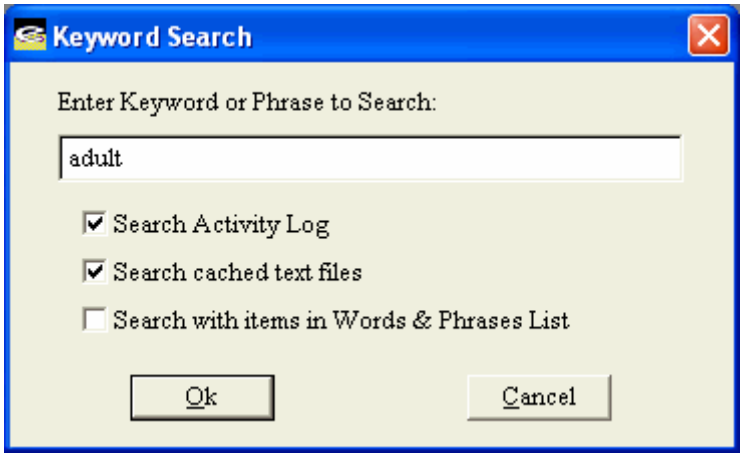
to provide a starting point for Internet users. Use this when you've logged your own research and would like to share the sites with a group.

Searching the Activity Log

The Echo•Suite Administration Console provides the ability to quickly sort through the entries displayed in the active Echo•Suite Log Window.

In order to identify specific information, sorting can be done by keyword, date, user, computer, MacID, violations or Internet content type.

The Keyword command in the Sort menu allows you to enter a word or phrase by which to sort the contents of the active Echo•Suite Log Window and associated text attachments. You can include the words in the Current Profile's Words & Phrases List during a keyword sort by selecting "Search with items in Words & Phrases List" in the keyword search screen.



Items in the Echo•Suite Log Window and any associated attachments that contain instances of the words or phrases in the Sort box or Words & Phrases List will be identified.

Clearing the Activity Log

☑ **You can automatically archive or purge aged data to maintain the current Pearl Echo Activity Log.**

The Echo•Suite log file contains the list of activity logged during all managed Internet sessions. The "Clear Activity Log" command in the Security menu is used to clear the contents of the secure Echo•Suite log file.

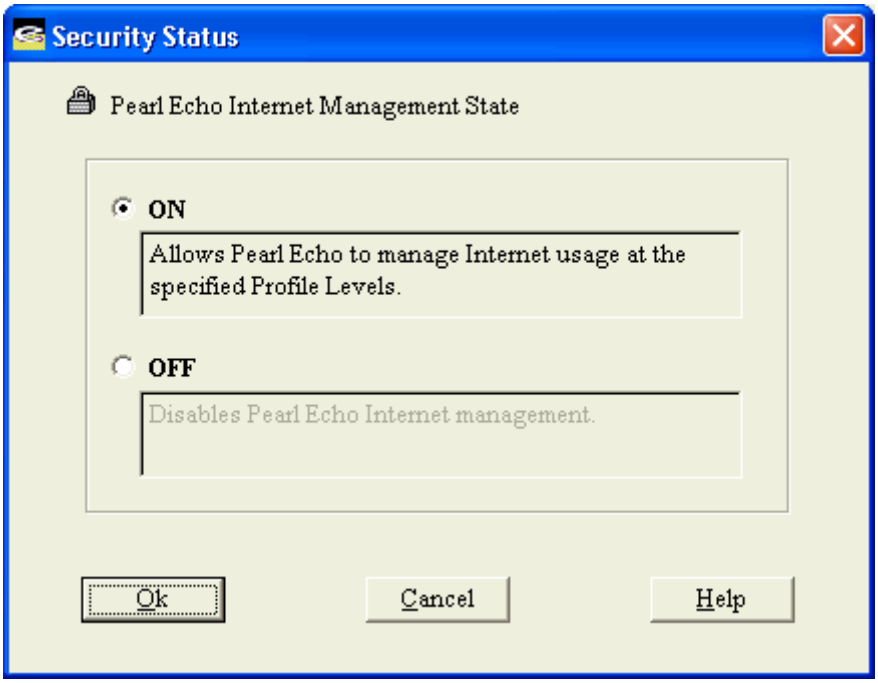
Clearing the activity log must occur from within the Echo•Suite Administration Console to maintain Echo•Suite's security.

Chapter 5

Setting Echo•Suite Security Levels

Turning Echo•Suite Management On and Off

You can turn the Echo•Suite Internet Management service On and Off in the "Set Security Status" command of the Security menu.

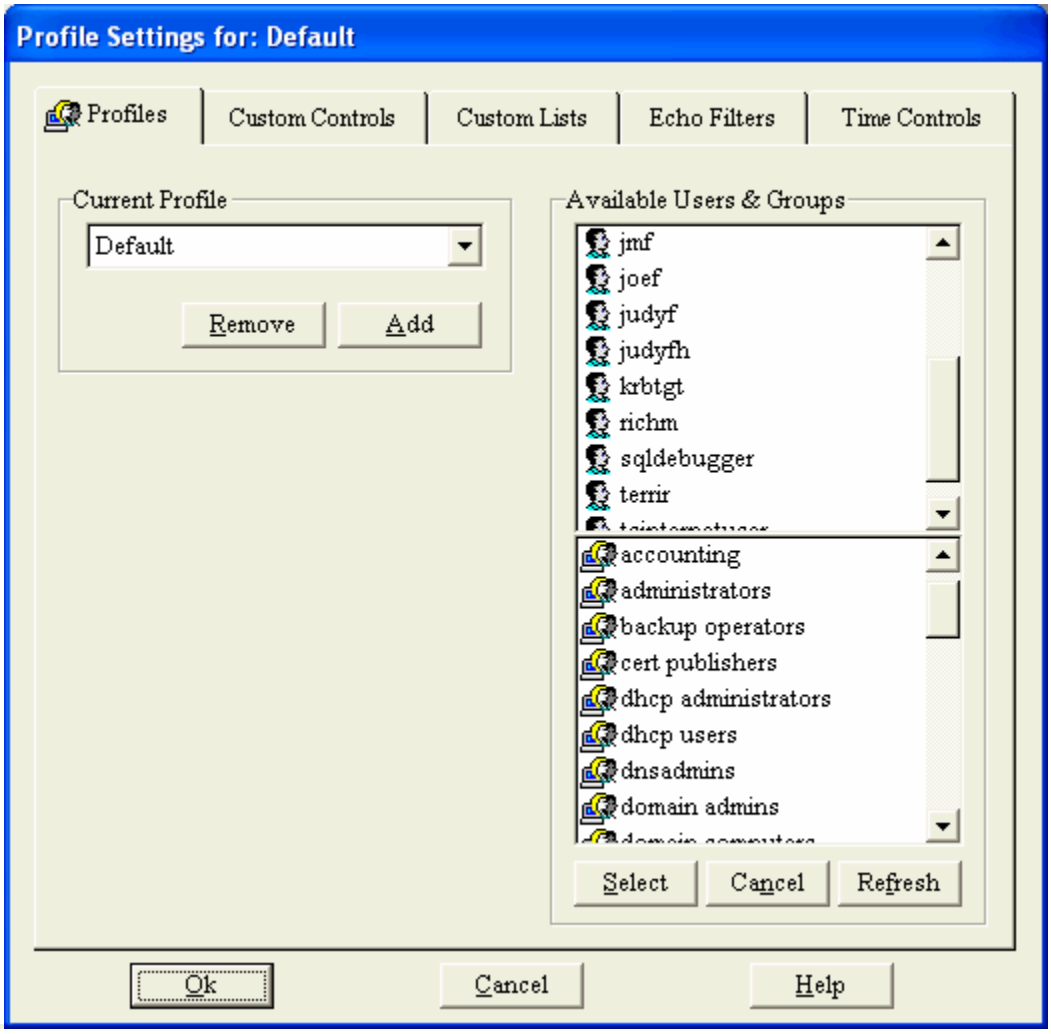


When the Echo•Suite Management Service is On, Echo•Suite is controlling Internet activity even after you exit the Echo•Suite Administration Console and log off of the Echo•Suite server.

It is recommended that you *not* start and stop the Echo•Suite Service from your system's Services Console.

Administering Echo•Suite Profiles

An Echo•Suite Profile is a group of settings you define to govern the Internet access permissions of your users. Access privileges are applied to individual users or groups of users. As such, your Echo•Suite Profile names are based on your existing Windows User and Group names. You can Add, Remove and Select the Current Profile in the "Profile Settings" command of the Security menu.



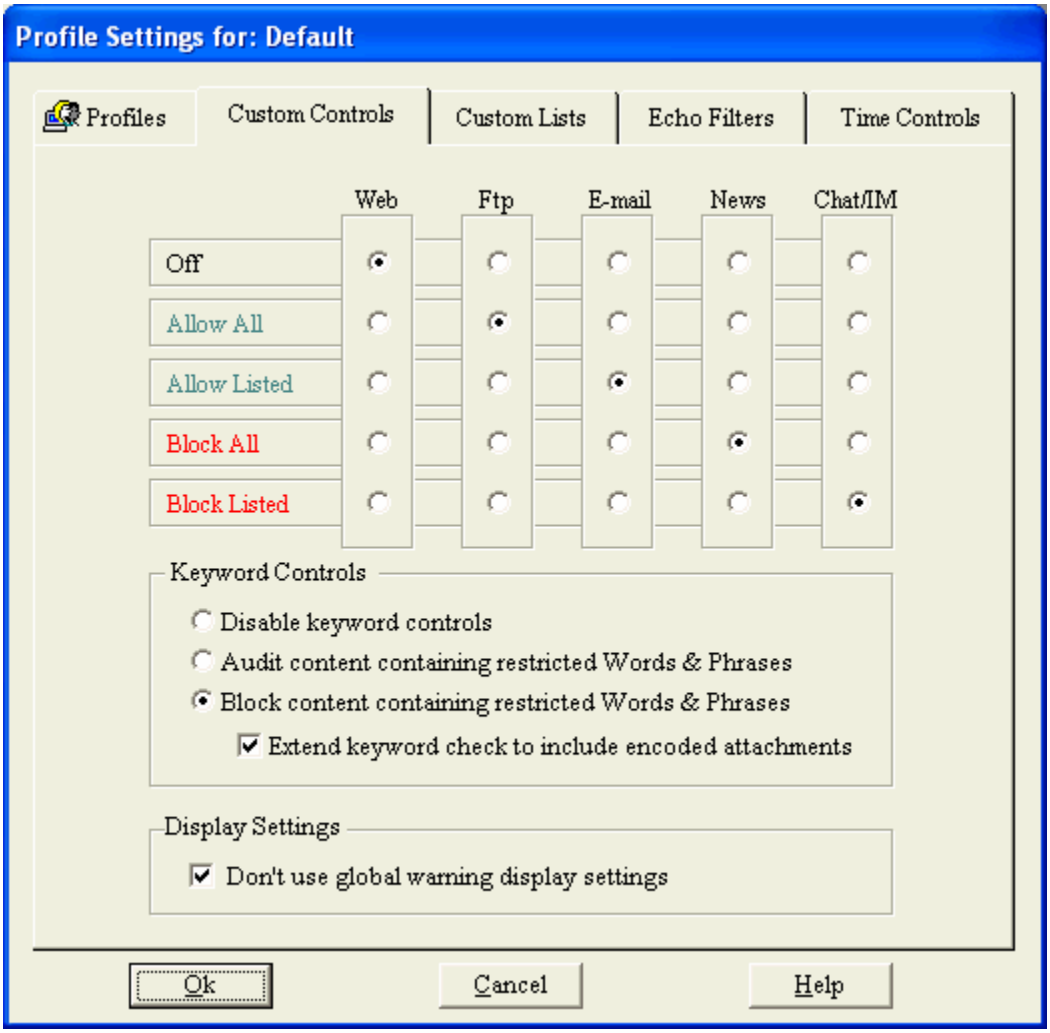
The Echo•Suite Administration Console will access and display the available User and Group names from the Active Directory database when Echo•Suite Server Software is installed on a machine that is part of a Domain using the Active Directory Service. If Active Directory Service is not available, the Echo•Suite Administration Console will access and display the available User and Group names from the server on which it is installed. If you have not installed the Echo•Suite Server software on a Windows server, the Echo•Suite Administration Console provides you with the ability to manually create the User names of Profiles that you would like to manage.

When a managed User attempts to access the Internet, their activity is governed by a Profile's configuration settings. Echo•Suite first looks for a matching User Profile. If no matching User Profile is found, Echo•Suite looks for a Group Profile to which the User belongs. If no matching Group Profiles are found, Echo•Suite uses the settings defined by your Echo•Suite Default Profile. If a User belongs to multiple groups, Echo•Suite selects the first matching Group (alphabetically) to govern Internet access.

For more information on this subject or to practice using this feature, please see the *Echo•Suite Tutorial* in the online help.

Setting Echo•Suite Control Levels

Internet access control is configured in the Profile's Custom Controls tab. Access levels are established by selecting the appropriate button under each Internet category in conjunction with entries in the Profile's Allow and Block Control Lists.



Off: Select Off to give the Current Profile full Internet access with no monitoring.

Allow All: Select Allow All to give the Current Profile full Internet access with monitoring. Unlike the Off level, all Internet activity will be logged. In this example, full Ftp access is granted and Ftp activity is logged.

Allow Listed: Select Allow Listed to have Echo•Suite block all Internet activity except for a list of permissible sites defined in the Current Profile's Allow Control lists. All Internet activity will be logged. In this example, Email access is granted to only the addresses listed in the Profile's Email Allow List.

Block All: Select Block All to have Echo•Suite block a Profile's Internet activity. All activity is logged. In this example, all NNTP News groups will be blocked.

Block Listed: Select Block Listed to have Echo•Suite allow all Internet activity except for a list of objectionable sites defined in the Current Profile's Block Control lists. All Internet activity will be logged. In this example, Chat/IM access is blocked to only the groups and "buddies" listed in the Current Profile's Chat Block List.

Auditing Words & Phrases

You can have Echo•Suite identify when specific content is transmitted in any segment of the Internet by selecting "Audit content containing restricted Words & Phrases." With this option set, Echo•Suite will allow all Internet activity to proceed but will highlight transactions containing words or phrases defined in the Profile's Words & Phrases Control list. The Words & Phrases List applies to all Web, Ftp, Email, News and Chat/IM content.

Blocking Content Based on Words & Phrases

You can have Echo•Suite block objectionable words and phrases in all segments of the Internet by selecting "Block content containing restricted Words & Phrases." With this option set, Echo•Suite will allow all Internet activity except for content containing words or phrases defined in the Profile's Words & Phrases Control list. The Words & Phrases List applies to all Web, Ftp, Email, Chat/IM, and News content.

When content is blocked based on a keyword or phrase, the user will not receive or transmit the blocked content but the content will be available for the administrator to review from within the Echo•Suite Administration Console.

For more information on this subject or to practice using this feature, please see the  *Echo•Suite Tutorial* in the online help.

Encoded Attachments

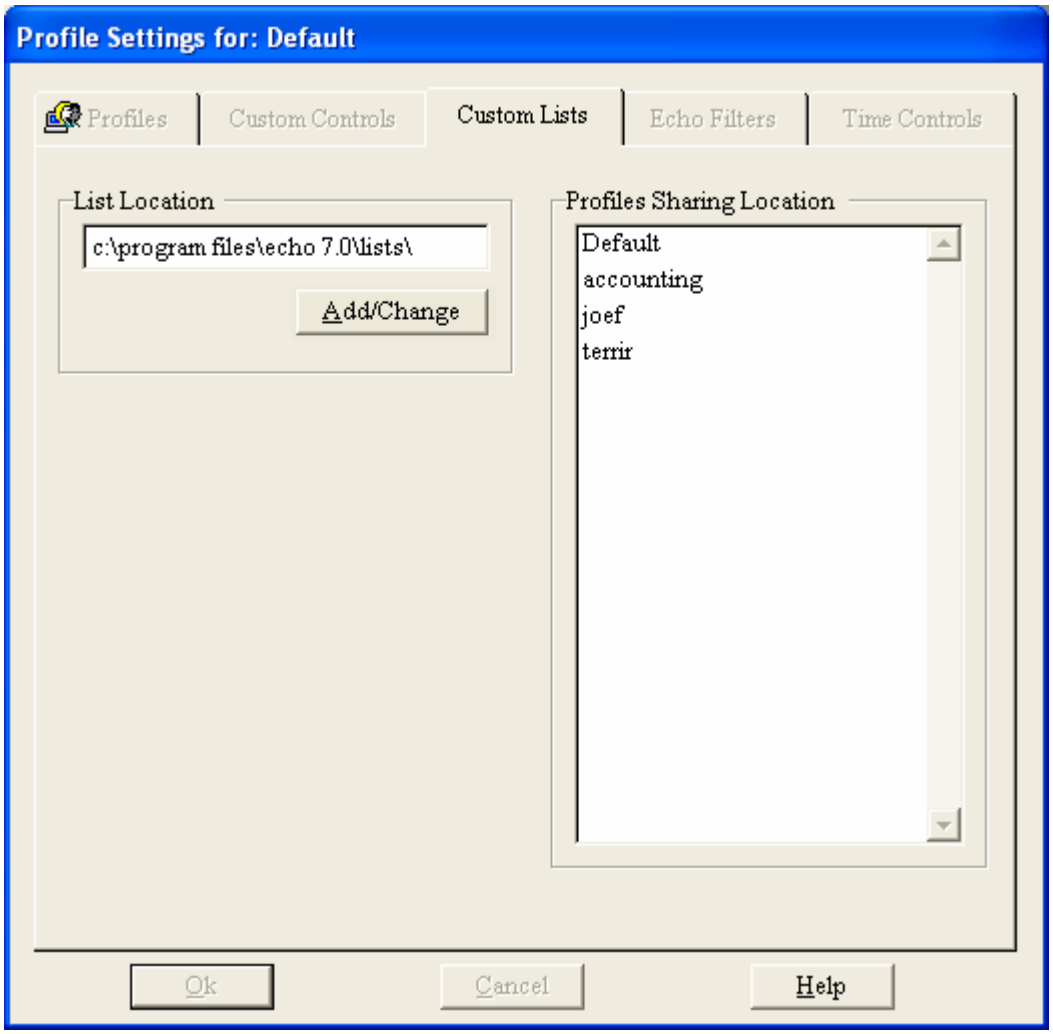
The audit and block keyword features can also be applied to encoded attachments in Email and News group postings. By selecting "Extend keyword check to include encoded attachments," Echo•Suite will decode attachments in real-time and search the attachment for textual data that matches words or phrases defined in the Profile's Words & Phrases Control list.

Global Warning Message

You can stop Echo•Suite from displaying your custom warning message for a specific Profile. This can be used if you have configured Echo•Suite to display a warning message to users but want to run Echo•Suite in silent mode for a particular user or group of users.

Assigning Echo•Suite Control Lists

You can assign a Profile's Control List location in the Custom Lists tab of the Profile window. When a new Profile is created, it shares the Default Profile's Control Lists. You can configure a Profile to share another Profile's Control Lists or to have its own Control Lists.



To create a separate set of Control Lists for a Profile:

1. Select the Add/Change Button in the Custom Lists tab of the Profile Window.
2. Type the new location or browse to a new folder that will contain the new set of Control Lists.
3. Select OK.

The selected Profile will have a new set of blank Control Lists which you can edit or import data.

To share an existing set of Control Lists for a Profile:

1. Select the Add/Change Button in the Custom Lists tab of the Profile Window.
2. Type the existing location or browse to the existing folder that contains the existing set of Control Lists.
3. Select OK.

The selected Profile will share the existing set of Control Lists.

Using Echo•Suite Allow and Block Control Lists

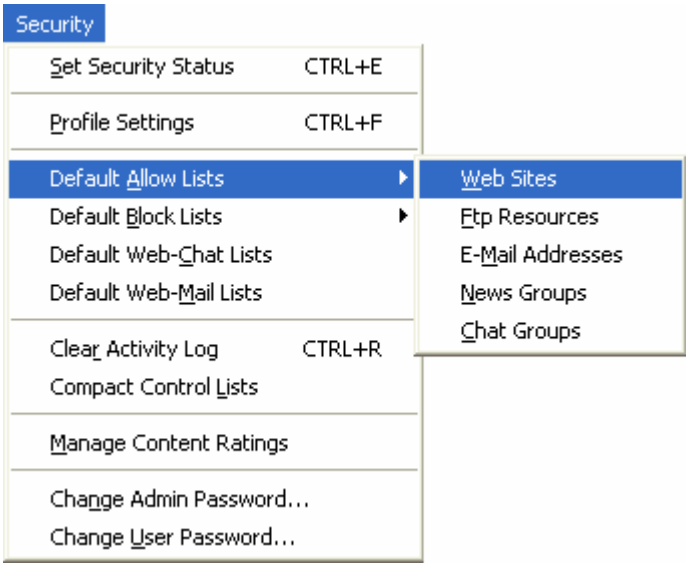
Echo•Suite's customizable Allow Lists are used to block all Internet activity except for a list of permissible Web Sites, Ftp Sites, Email contacts, News groups and Chat/IM groups. This is useful when a Profile's access needs to be limited to a defined list of web sites or Internet addresses.

Echo•Suite's customizable Block Lists are used to allow all Internet activity except for a list of unacceptable Web Sites, Ftp Sites, Email contacts, News groups and Chat/IM groups.

There are a number of ways to edit a Profile's Control Lists.

Manual Edit

To manually edit a Profile's Control List, select the desired list from the Security menu.

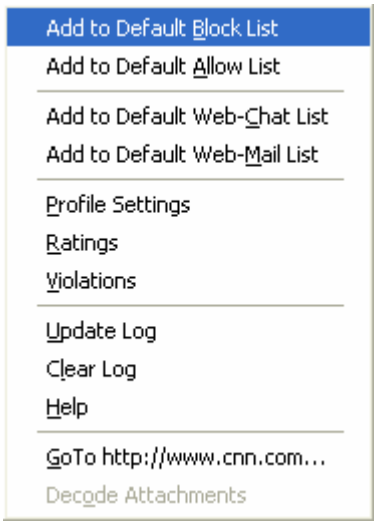


With the Profile's Control List active, you can add, remove and change entries. The format of the Control List entries must conform to Echo•Suite's standard Control List syntax. For more information on this subject or to

practice using this feature, please see the *Echo•Suite Tutorial* in the online help.

Automatic Add

You can automatically add an *individual* log entry to the Current Profile's Control Lists from the shortcut menu.

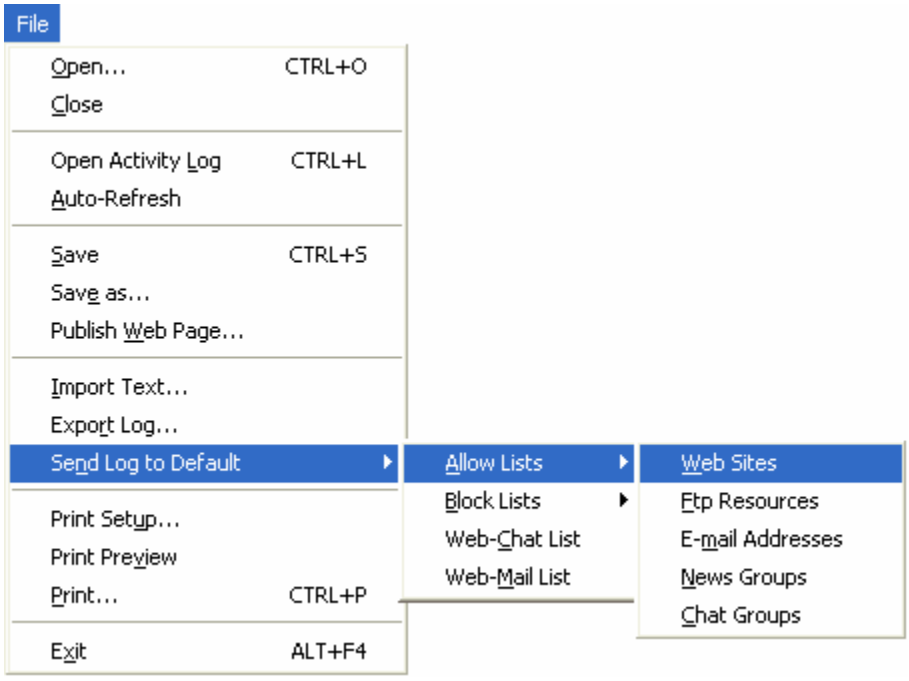


1. Right-Click your mouse button on the log entry that you want to add to a Profile's Control List.
2. Select "Add to Block/Allow List".

The selected entry will automatically be sent to the Current Profile's Block or Allow List.

Automatic Send

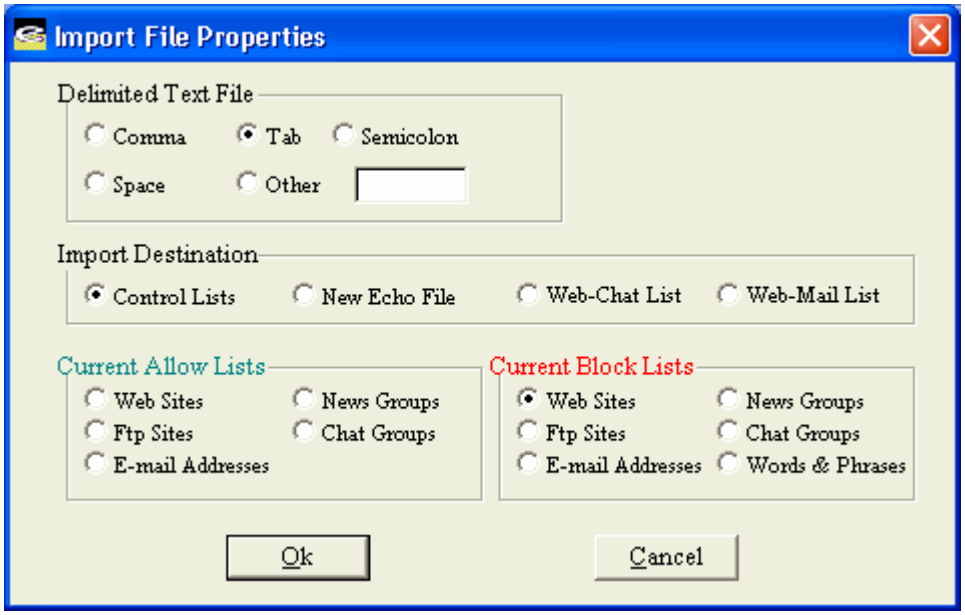
You can automatically send all entries from a sorted or unsorted log window to the Current Profile's control list by selecting "Send Log to" from the file menu.



The appropriate entries will automatically be sent to the selected Block or Allow list.

Import Text

You can import properly formatted text files into the Echo•Suite Administration Console by selecting "Import Text" from the File menu. Use this feature when sharing lists or restoring lists from backup.



The "*" Wildcard

The "*" Wildcard can be used in your Web and Email Allow and Block lists to simplify administration. The following examples illustrate how and when you might use the "*" wildcard:

To restrict a Profile's email to inter-company email, add *@yourcompany.com to the Profile's Email Allow List. Set the Profile's Custom Email Control to Allow Listed.

To block the receipt or sending of Hotmail™, add *@hotmail.com to the Profile's Email Block List. Set the Profile's Custom Email Control to Block Listed.

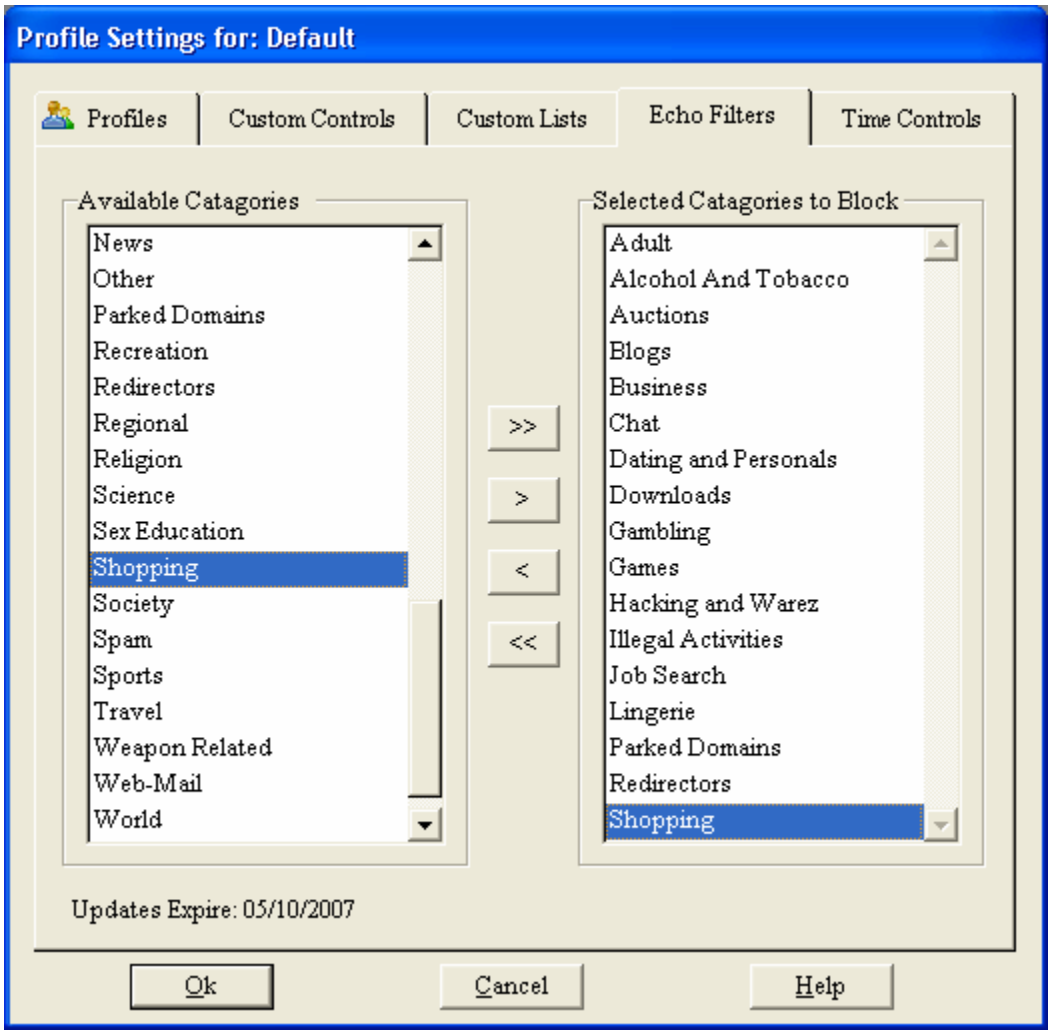
To allow access to all intranet servers in your company and add a level of security for internal sites, add http://*.yourcompany.com to the Profile's Web Allow List. Set the Profile's Custom Web Control to Allow Listed.

To block access to all Yahoo! content including mail and chat, add http://*.yahoo.com to the Profile's Web Block List. Set the Profile's Custom Web Control to Block Listed.

Blocking Web Content Using Echo•Filters

You can block access to Web sites based on categories of content in the Echo•Filters tab of the Profile window. This feature is an optional module available with Echo•Suite.

To block Web content based on categories, select the category to be blocked from the "Available Categories" list and select the right arrow button to move it to the "Selected Categories to Block" list. You can press the shift or ctrl keys to select multiple categories at once. To add or remove all categories, select the right or left double arrow button.



To block Web Content that is not found in one of the existing Echo Filter categories, add the "Other" category to the "Selected Categories to Block" list.

Echo Filters Updates

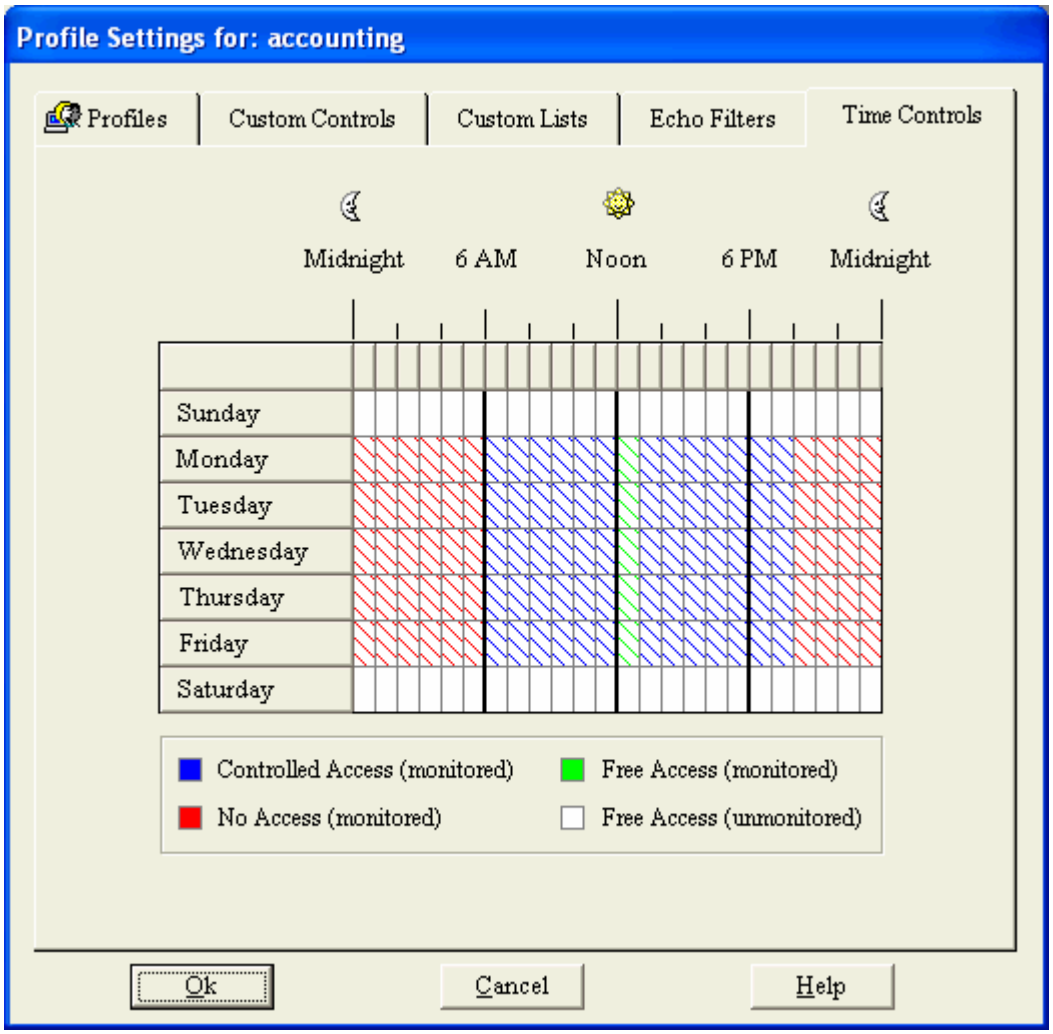
Echo•Suite will automatically update the Echo Filters database each day. The list of Echo Filter categories can be found in Appendix B of this document.

When you enter the Echo•Suite Administration Console, you will be notified when you are within two weeks of the expiration of your Category Updates. You may also receive an email notification from Pearl Software. If your Category Updates expire, the Echo Filters will continue to function however their effectiveness may diminish as the automated daily updates will not be available.

Note: Echo•Suite performs an outbound transaction on ports 80 and 443 when updating the Echo Filters database.

Setting Time Restrictions

You can use Echo•Suite to restrict the days and hours during which a Profile can access the Internet. You can also allow free access with or without monitoring during specified time periods. The default configuration is to allow a user to connect during all hours of all days of the week.



In the above example, the Accounting Profile is set to have

- No Internet access after hours from 8 p.m. to 6 a.m. (red)
- Uncontrolled access without monitoring on weekends (white)
- Uncontrolled access with monitoring during the lunch hour (green)
- Controlled access during all other time periods (blue)

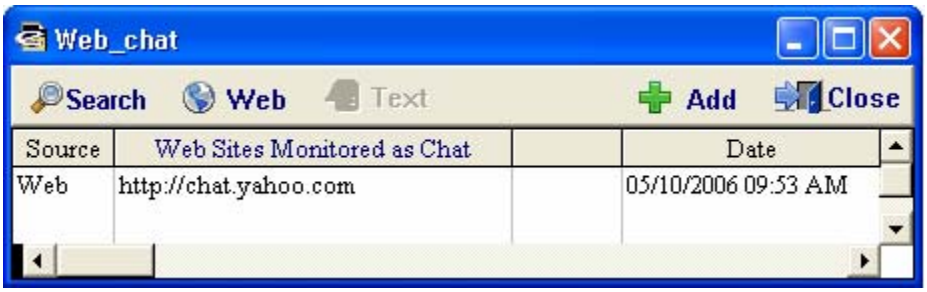
To manage login hours:

1. Select the hours to be administered:
   - To select one hour, click that hour.
   - To select a block of time, click the beginning hour and drag through the rows and columns to the ending hour.
   - To select an entire day, click that day in the left column.
   - To select one hour for all seven days, click the top of that column.
   - To select the entire week, click the upper-left box (above Sunday).
2. Select the type of access:
   - To allow controlled access during the selected hours, click "Controlled Access".
   - To deny connections during the selected hours, click "No Access".
   - To allow monitored connections without any controls you have set, click "Free Access (monitored)".
   - To allow unmonitored connections without any controls you have set, click "Free Access (unmonitored)".
3. Repeat steps 1 and 2, as necessary.

Suggestion: When using time controls, you may want to restrict users running Windows 95, 98 or ME from altering their workstation's clock. From the "Preferences…" command in the Options menu, you can select Lock System Clock to disable the Windows time settings program. Select Lock DOS Prompt to disable access to DOS and DOS time commands. Note: Restricting access to DOS may affect legacy programs that run in DOS mode.

Monitoring Web-Chat

Certain Web pages have non-standard Java chat applications (applets) built-in. Chatting through a Web browser is known as "Web-Chat". In order for Echo•Suite to treat these Web sites as Chat sessions, the Web site's address must be specified in a Profile's Web-Chat Control List.



When the Echo•Suite Workstation agent encounters a Web site that is listed in the Profile's Web-Chat Control List, the agent will be triggered to capture all data communicated to and from the site. Because the communicated data does not conform to an agreed-upon Chat standard, the presentation of the captured content in the Echo•Suite Administration Console may appear unorganized.

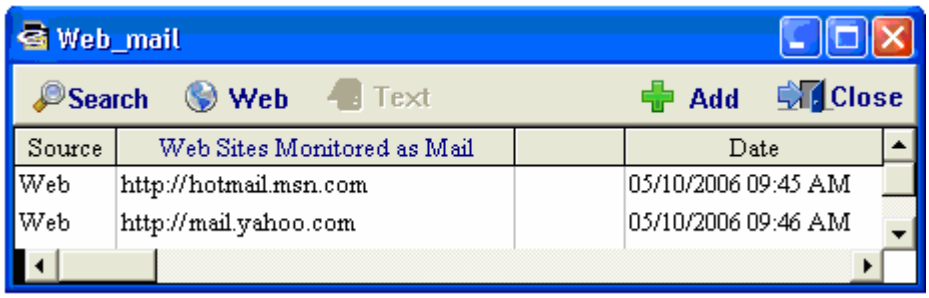
To edit entries in your Web-Chat list, select "Web-Chat List" from the Security menu.

The format of the Web-Chat list entries must conform to Echo•Suite's standard Control List syntax. For more information on this subject, please see the *List Syntax* topic in the online help. Like other Web sites, *controlling access to Web* sites containing chat applets is done through a Profile's *Web* Block & Allow Lists.

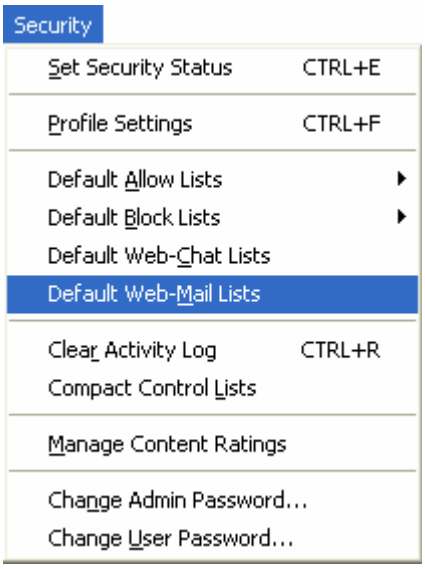
Monitoring Web-Mail

Certain Web sites have non-standard email applications built-in. These Web based email portals are usually free and allow users to easily send, receive and organize their email with a standard web browser. Web-Mail eliminates the need for specialized email software on your computer.

In order for Echo•Suite to treat these Web sites as email sessions, the Web site's address must be specified in your Web-Mail Control List. Echo•Suite will capture all the content presented at pages within the site you specify in your Web-Mail Control List.



To edit entries in your Web-Mail list, select "Web-Mail List" from the Security menu.



The format of the Web-Mail list entries must conform to Echo•Suite's standard Control List syntax. For more information on this subject, please see the *List Syntax* topic in the online help. Like all Web sites, controlling access to these Web-Mail sites is done through your Web Block & Allow Lists.

Suggestion: Some Web-Mail portals redirect users to various computers when retrieving and sending Web-Mail. For example, you may see something similar to http://by108fd.bay108.hotmail.msn.com when users access their Hotmail email. You can simply enter the root url, http://hotmail.msn.com, in the Web-Mail list to capture content at the site. The "*" wildcard is not needed when specifying Web-Mail or Web-Chat entries.

Using Keyword Blocking and Auditing

You can configure Echo•Suite to block or audit a Profile's inbound and outbound content containing words and phrases that you specify. The primary focus of this feature is to protect against the inappropriate dissemination of confidential information. This feature can also be used to block or warn of material that contains offensive language.

There are two methods to block or audit content based on words and phrases:

Default Method

Content that contains your specified words by themselves or as part of another word will be blocked or audited. For example, if your Block List contains the entry 'pain', content that contains the word 'pain' or 'Spain' will be blocked or audited. This is the default method.

Exact Method

Content that contains your specified words by themselves will be blocked or audited. For example, if a Profile's Block List contains the entry '!pain!', content that contains the word 'pain' will be blocked or audited. Content that contains the word 'Spain' will not be affected. You must place exclamation points (!) around the words you want to block or audit with the exact method. This allows you to use the Default and Exact methods simultaneously.

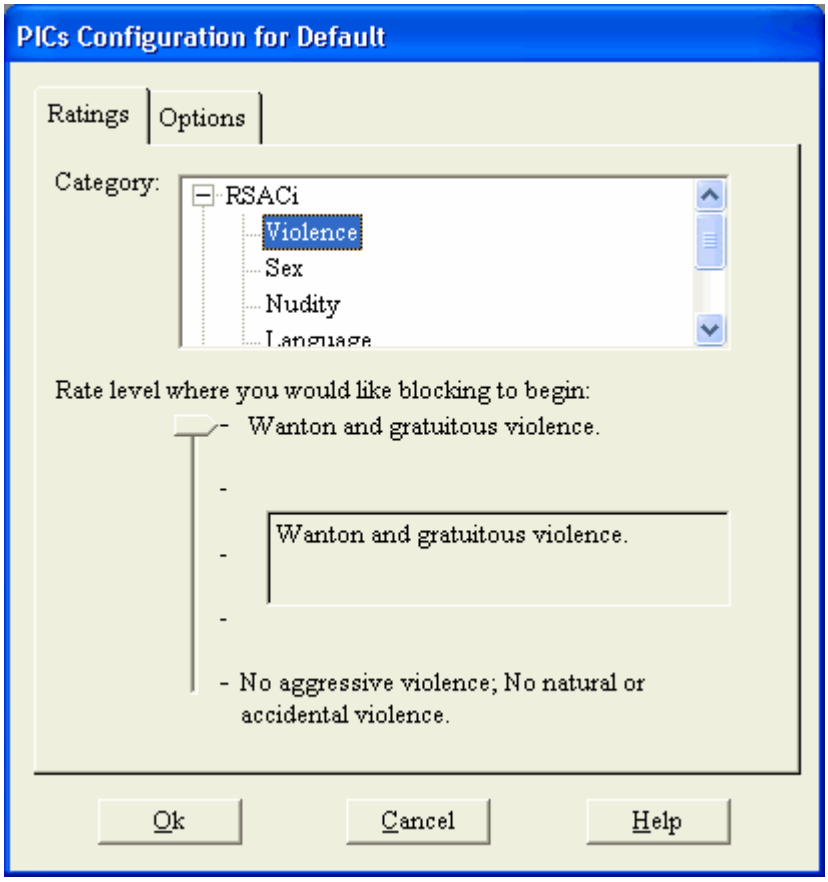
Entries in your Allow Control Lists will override other controls including entries in your Words & Phrases list. This is useful for allowing access to sites, emails, etc. that may occasionally present "iffy" material but do so in a manner that does not violate your Acceptable Use Policy.

Note: Time Controls will take precedence over all other controls including Allow List entries.

For more information on this subject or to practice using this feature, please see the  *Echo•Suite Tutorial* in the online help.

Controlling Access to Rated Content

The PICs rating system relies on content providers voluntarily rating the content they create and distribute. On Web pages, information exists in the header (hidden part) of the Web page that contains the rating code for that page. Echo•Suite looks at the page rating code and compares it to the Profile's levels you specify in the "Manage Content Ratings" section of the Security menu.



There are various rating systems that have been developed and are currently being used on the Internet. You use Echo•Suite to define acceptable rating levels for each rating system you want to use. For example, if the familiar Motion Picture Association of America (MPAA) rating system where used, you might set Echo•Suite to block all rated material that is rated "R" or above. As you browse to a Web page, Echo•Suite would check the rating of the page. If the page used the MPAA rating system, Echo•Suite would check the rating and block the page if it where rated "R" or above. Echo•Suite can be set to monitor multiple rating systems simultaneously. You can also set Echo•Suite to block any content that is not rated.

For more information on this subject or to practice using this feature, please see the *Echo•Suite Tutorial* in the online help.

Chapter 6

Additional Echo•Suite Features & Settings

Refreshing the Echo•Suite Activity Log

☑Pressing the F5 key will refresh the Echo•Suite™ Activity log.

The Echo•Suite Activity Log shows the most current Internet activity up to the moment that you open the Echo•Suite Administration Console. If Echo•Suite Workstations access the Internet while the Echo•Suite Administration Console is open, you will need to refresh the Activity log to view the latest Internet activity. To view updated Internet activity use the "Open Activity Log" command in the File menu.

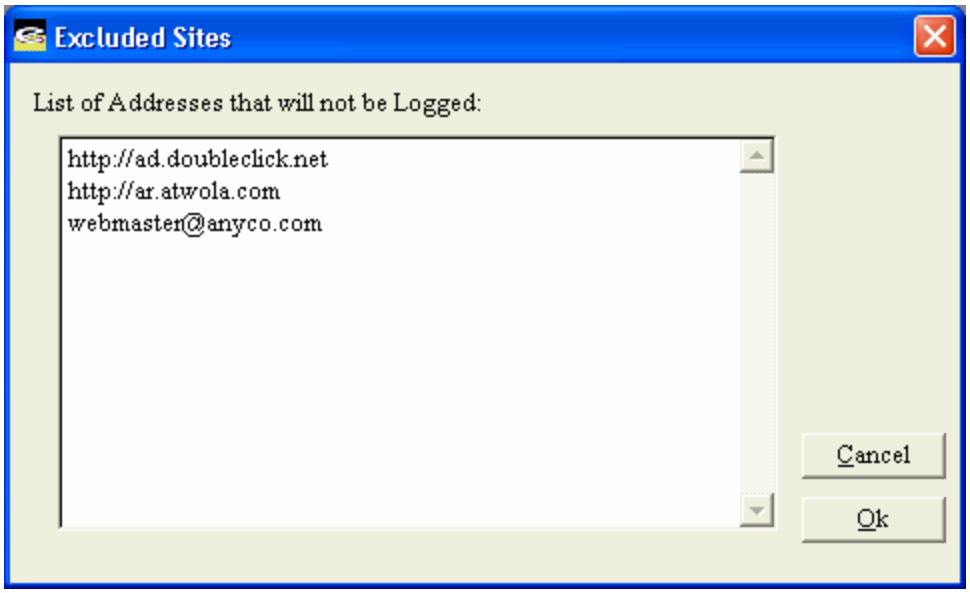
Pressing the F5 key or using the toolbar or shortcut menus can also be used to refresh the Activity Log.

To automatically update the Echo•Suite Activity Log, select "Auto-Refresh" from the File menu. While in Auto-Refresh mode other Echo•Suite Administration Console features are unavailable. Press Alt+F5 to escape Auto-Refresh mode.

Excluding Data from Being Saved in the Activity Log

Echo•Suite can be configured to exclude a list of Internet addresses from being logged. This is useful if frequented URL's or other addresses are not of particular interest or may be skewing the results of reports or other analysis. Examples include Web activity that pulls advertisements from advertising sites, web access to an organization's intranet sites, or communications that may be considered privileged or protected as confidential such as whistleblower or employee ethics hotlines.

To add Internet addresses that should not be saved in the Echo•Suite Activity Log, select "Exclude Sites from Log" in the Echo•Suite Options menu.



Web addresses must contain the http:// prefix and are applicable to the entire specified domain. Addresses from any source of Internet activity (web, ftp, email, news, chat, im) can be added to the list of excluded sites. Although the specified activity will not be saved in the Echo•Suite Activity Log, the listed Internet addresses may still be controlled based on restrictions you may have defined in your Echo•Suite control Profiles.

You can also use the "*" wildcard in the Excluded Sites list. For example, adding the entry http://*.js will exclude all sites from being logged that contain a java script suffix. The entry *@mycompany.com can be used to exclude all internal company emails from being logged.

The Echo•Suite Activity Log Database

☑**Pearl Echo can be configured to log directly to SQL Server.**

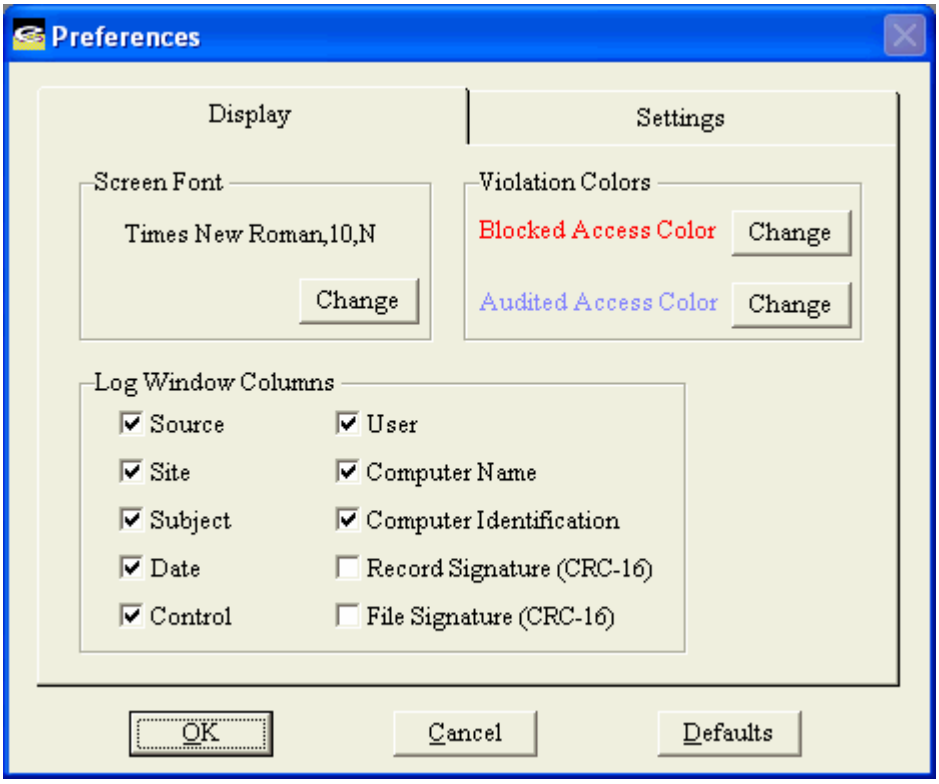
Echo•Suite stores data in an open xBase database format. You do not need to install a third party RDBMS when using Echo•Suite with its native database. The Echo•Suite native database size limit is 2GB. For installations with high volume monitoring loads and large storage requirements, Echo•Suite can easily be configured to store monitored Internet activity to a Microsoft SQL Server. Other database platforms can be supported with additional customization by Pearl Software's Professional Services group.

Configuring Echo•Suite to store data to Microsoft SQL Server provides additional flexibility to your organization: Echo•Suite Servers can be placed at various locations to provide distributed Employee Internet Monitoring and Control, yet all data can be centrally stored and managed for increased security, reliability and consolidated reporting.

Modifying How Echo•Suite Displays Information

The Preferences command in the Options menu allows you to set:

1. Screen Fonts.
2. Violation Colors.
3. Log Window Appearance.
4. Log Window Detail.



Screen Fonts

The screen font setting controls how text is displayed in the Echo•Suite Log windows.

Violation Colors

The violation colors are used to easily identify Activity Log entries where users have tried to access content that has been blocked or audited by your Echo•Suite control settings.

Log Window Columns

You can control how the Echo•Suite Administration Console displays monitored data. The Computer Identification check box is used to display the Media Access Controller ID (MacID) of the monitored workstation. The MacID is a unique ID associated with the network card within the workstation.

The Signature check boxes are used to display data integrity details. A verification check-sum is performed at the Echo•Suite Workstation on all data sent to the Echo•Suite Server. Individual check-sums are performed on the logged record data (Signature-r) as well as associated file content and attachments (Signature-f).

Log Window Detail

You can control how Echo•Suite displays and stores Web site activity. Since accessing one web page may actually reference many other pages in a web site, you can choose to compress this detail to one entry per web site. This also reduces the amount of data sent from the Echo•Suite Workstation to the Echo•Suite Server.

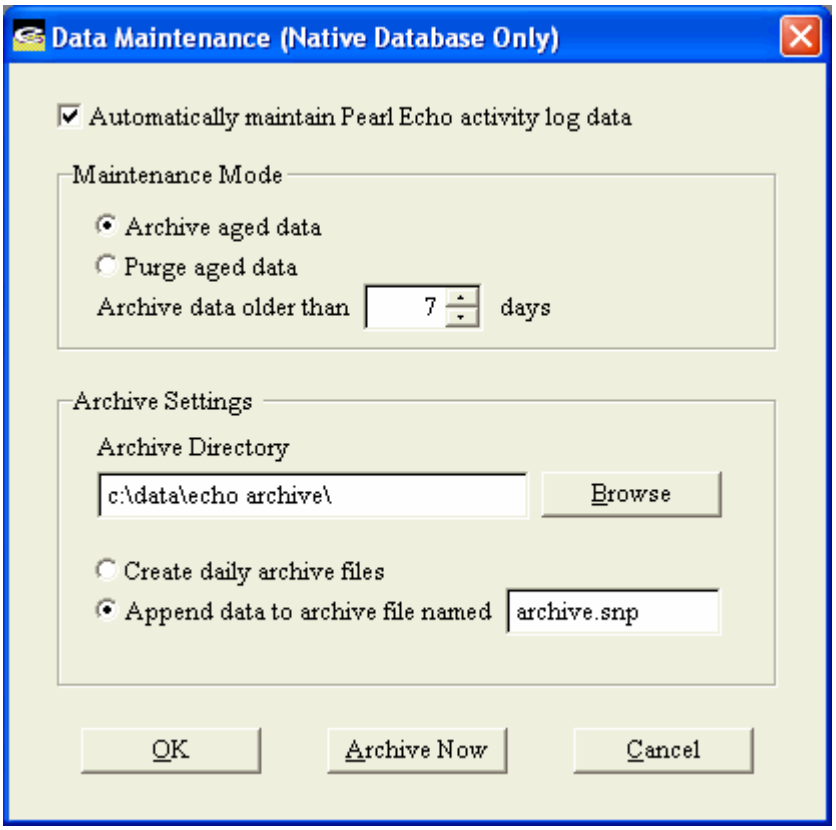
Changing the Echo•Suite Warning Message

You can inform users that Echo•Suite is monitoring their workstations. The message you display can be customized in the "Set Warning Message" command in the Options menu.

1. You can set Echo•Suite to periodically display your warning message by setting the display interval. To stop Echo•Suite from periodically displaying your warning message, set the warning interval to 0 minutes.
2. You can also set Echo•Suite to warn users when one of your Internet access rules is violated. To warn users when a violation occurs, select the "Warn on Violation" check box.

Data Maintenance

You can control the size of the native Echo•Suite Activity Log by archiving or purging your aged Echo•Suite data.



☑ **The maximum size of any *native* Pearl Echo log file is 2 gigabytes. The Pearl Echo SQL Server module does not have this limit.**

The Echo•Suite service can be set to automatically perform an archive or purge of the native Activity Log and its associated cache files. Archived data can be stored to individual daily archive files or appended to a single archive file. Data moved to individual daily archive files will be stored to a file named arcmmddyyyy.snp where mm is the current month, dd is the current day, and yyyy is the current year. The file will be stored in the local or network directory you specify in the text box above.

Archived data and your current data will remain available as data sources against which you can run reports.

If Echo•Suite is configured to log data to Microsoft SQL Server, data maintenance is performed through maintenance scripts created by the SQL Server DBA.

Compacting the Current Profile's Control Lists

The "Compact Lists" command in the Security menu is used to increase the efficiency of the Allow and Block operations. Wasted space and duplicate entries are purged from the Current Profile's Control Lists.

Changing the Admin Level Login Password

The "Change Admin Password" command in the Security menu is used to change the administrative password. Upper and lower case letters are not treated the same. Passwords are limited to less than twenty characters.

For security reasons, you must correctly enter your old password before creating a new one.

Changing the User Level Login Password

The "Change User Password" command in the Security menu is used to change the user level password. The User Level password allows users other than the Echo•Suite Administrator to view the Echo•Suite Activity Log and run reports. All Echo•Suite features are available when logged in with the User Level password except features that control Echo•Suite security configurations.

Managing Access to Data for Reporting

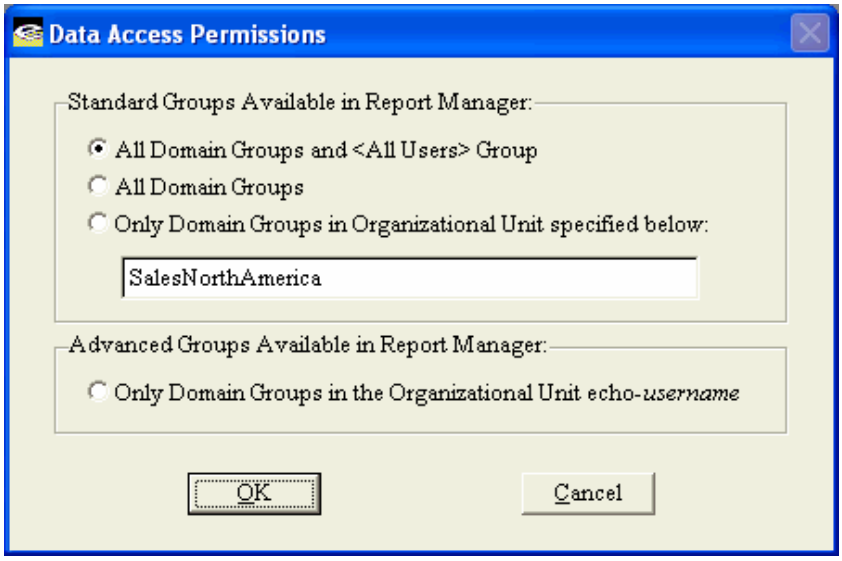
Echo•Suite provides you with the capability to distribute the Echo Administration Console configured as an Echo Reporting Console to other designated personnel in your enterprise. The Echo Reporting Console provides designated personnel access to end-user data based on Directory System Groups to which end users belong and to which the designated personnel have access. This allows administrators to use the inherent security and grouping capabilities of your Directory System to define the specific user level data accessible by the distributed Echo Reporting Consoles.

Administrators can utilize this feature to reduce the amount of administration time and effort needed to maintain multilayered reporting capabilities. The administrator can make changes to reporting privileges faster and benefit from the dynamic capabilities of their existing Directory System without requiring user intervention to invoke changes.

The use of data access permissions also allows the administrator to centrally manage enterprise-wide auditing and reporting activities in adherence with organizational or network policies.

In addition to standard Echo Reporting Console configurations based on existing Directory System Groups, the administrator can also create specialized types or groups of users (such as Executive, Human Resources, Management, Sales, etc.). These configurations can be used in combination with the Echo Reporting Console and Remote Installation Services to automate deployment to user workstations, reducing the amount of time required deploying reporting capabilities to a large number of users or to new workstations.

To configure Data Access Permissions, in the Echo•Suite Administration Console select "Data Access Permissions" from the Options menu. Select the Directory Groups that will appear in the Echo Administration Console.



Standard Access Permissions

Standard user level permissions are created by assigning one of three access levels. Based upon the access level, the data available within the Echo Administration Console or the Echo Reporting Console will be limited to the end-user activity logged for the specific group(s) of end-users in which the Console user has Directory System rights to view.

All Domain Groups and <All Users> Group

1. Select "All Domain Groups and <All Users> Group" to provide access to data from all users. The groups to which individuals belong that are available in the Echo Reporting Manager include all available Domain Groups, Custom Groups created in the Echo Report Manager and the Echo•Suite <All Users> Group. The available Domain Groups are based on the domain in which the user of the Echo Console is logged in and the credentials the user has to access Group Directory objects.

All Domain Groups

2. Select "All Domain Groups" to provide access to data from only those individuals that belong to Domain Groups and all Custom Groups created in the Echo Report Manager. The available Groups are based on the domain in which the user of the Echo Console is logged in and the credentials the user has to access Group Directory objects.

Only Domain Groups in a Specified Organization Unit

3. Select "Only Domain Groups in the Organizational Unit specified below" to specify a subset of Directory System Groups available to the Echo Report Manager. The available Groups are based on the domain in which the user of the Echo Console is logged in and the credentials the user has to access Group objects.

Advanced Access Permissions

☑ **Advanced Access Permissions can be used to create Echo specific reporting permissions within your Domain without requiring changes to existing Directory System policies.**

Administrators interested in implementing advanced access permissions within Echo•Suite must first create customized Directory Organizational Units using the **echo-*username*** fixed-variable naming convention. The fixed component of the name refers to an Organizational Unit used by the Echo Report Manager. The variable portion, *username,* is the Windows user name of the individual running the Echo Administration Console or the Echo Reporting Console. Utilizing this naming structure within your Domain will allow you to create customized reporting permissions that do not require changes to your existing Directory System policies.

The customized Organizational Units should contain the specific Groups that will be available to the user for reporting purposes within the Echo Console. Advanced user level access permissions are applied by selecting the fourth choice in the Data Access Permissions menu in the Echo Administration Console.

Only Domain Groups in the Organizational Unit echo-*username*

1. Select "Only Domain Groups in Organizational Unit named echo-*username*" to further restrict access to data from only those individuals that belong to Directory Groups in the Directory OU called echo-*username*.

Publishing a Web Page for your Users

You can generate a permanent copy of your active log window in HTML format. This file can then be opened directly by a user's Web Browser. You can use this feature to create a starter web page that is identical to a Profile's Web Allow list. This is an easy way to share research and keep users on track.

To publish the active log window in HTML format, select "Publish Web Page…" from the Echo•Suite File menu.

Importing and Exporting Data

Importing Text

You can import data into the Current Profile's Allow and Block Lists from the "Import text" command in the file menu.

The file you import must contain properly formatted text. The file format required is:Source <dl> Site <dl> Subject <dl> Date&Time <dl> Control <dl> User <dl> Computer <dl> MacID <dl> Signature(r) <dl> Signature(f) <dl> File Name <dl> Flag <dl> Text1 <dl> Text2 <dl> Text3

Field	Data Type
Source	Character
Site	Character
Subject	Character
Date&Time	DateTime Format (12/18/2002 03:00 PM)
Control	Character
User	Character
Computer	Character
MacID	Character
Signature(r)	Character
Signature(f)	Character
File Name	Character
Flag	Integer
Text1	Character
Text2	Character
Text3	Character
<dl>	Field Delimiter (tab, space, comma, other)

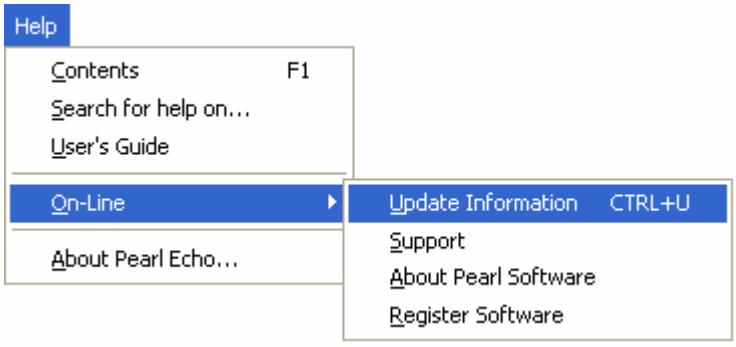
Use this feature when sharing lists or importing data from a backup.

Example: Mail,dlf@pearlsw.com,Confidential,05/08/1999 12:00 AM, Keyword,David,TestMachine,,,,NONE,0,,,

Exporting

You can export data from the Echo•Suite Administration Console with the "Export log" command in the file menu. The exported file will be a delimited text or spread sheet format. Use this feature for sharing sites or for custom data analysis.

Performing Product Updates



Periodically, Echo•Suite will automatically check Pearl Software's Internet Servers for available *program* updates. You can manually check for program updates by selecting "Update Information" from the Help Menu. If the Update Checker determines that you are using an older version of Echo•Suite, you will be automatically directed to Pearl Software's update Internet site.

You can disable Echo•Suite from automatically checking for program updates in the "Preferences…" command of the Options menu.

Update Instructions

Echo•Suite Server updates are accomplished by running the Server patch available from Pearl Software's update Internet site. The Echo•Suite Server software does not need to be removed or reconfigured when installing a Echo•Suite Server update. Before updating the Echo•Suite Server software, start the Echo•Suite Administration Console and set the Echo•Suite Management State to OFF in the program's Security menu.

To automatically update your Echo•Suite Workstation agents, place the available Workstation patch in the WS_Updates folder found in the directory where you installed the Echo•Suite Server software. The Echo•Suite service will automatically deliver the patch to Echo•Suite's self-updating agent. The self-updating agent will update itself the next time the workstation is started.

Note: Echo•Suite *program* updates differ from Echo Filter updates. Echo Filter updates are done daily with a current Echo•Suite Categories Module Agreement.

Activating Your Copy of Echo•Suite

If you are evaluating a demo version of Echo•Suite, you can activate your copy by purchasing a license from Pearl Software. To activate your copy of Echo•Suite, open the About dialog box in the Echo•Suite Administration Console and enter the Product Serial number that is supplied to you after purchasing the product. The About option is located under the Help menu.

Chapter 7

Report Manager

Overview

The Echo•Suite Administration Console contains an enterprise-class reporting module. You can use the Echo•Suite Report Manager to query up-to-date Activity Log files, directories of archived data, log files residing on a Microsoft SQL Server, as well as files that you have filtered and saved in Echo•Suite's native file format.

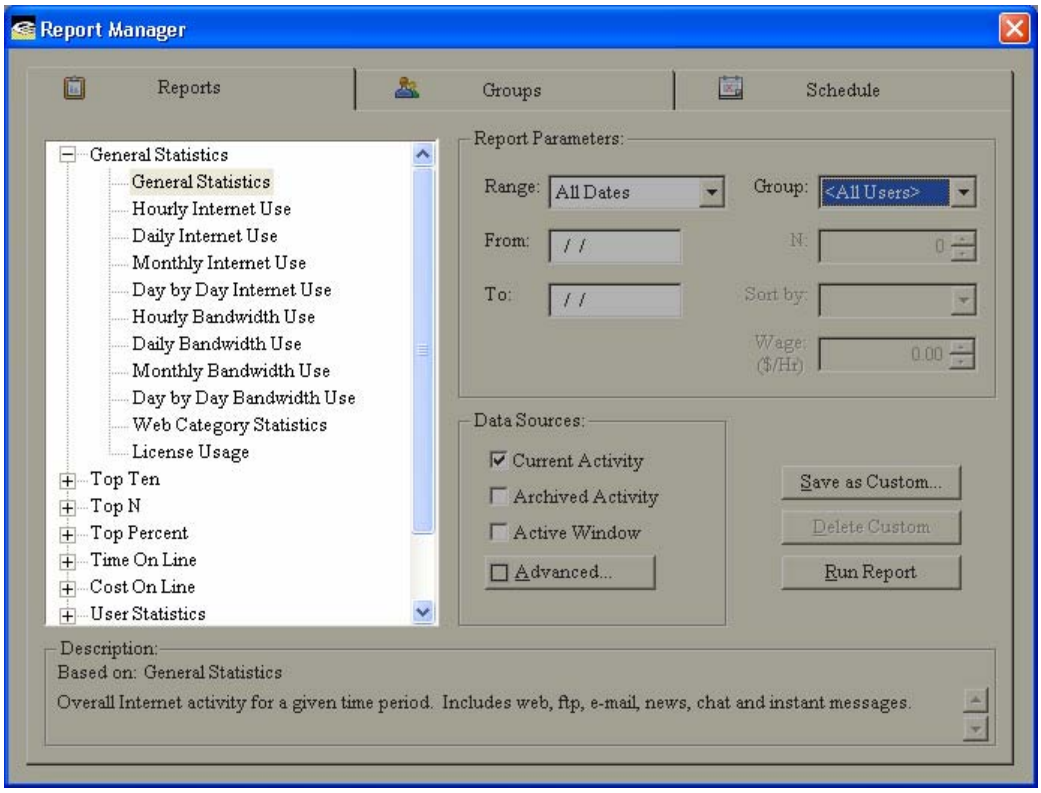
The Echo•Suite Report Manager provides more than seventy-five standard reports that can be customized and saved for future use. The Echo•Suite Report Manager allows you to run reports ad hoc or to schedule reports to be automatically generated and distributed. The Echo•Suite Report Manager allows you to save reports in a wide variety of file formats including Crystal Reports format for interactive reporting and drill down. You can even customize reports with your corporate logo.

Reports can be scheduled to be published to any accessible directory including your organization's intranet so users can easily access reports through their web browser. In addition, the Echo•Suite Report Manager can automatically distribute reports via e-mail using Echo•Suite's built-in SMTP email service. You can even customize the report email with your own disclaimer.

The Echo•Suite Report Manager consists of a single management console to handle all reporting activities. The Echo•Suite Report Manager is organized by Reports, Groups and Schedules.

Echo•Suite Reports

The Reports tab in the Echo•Suite Report Manager is where reports are selected to be generated and report parameters defined. The Reports tab is also where reports are run or saved for future use.



Report Selection

The available standard and custom reports are displayed in an expandable tree-view. Selecting any report reveals a detailed description about the report at the bottom of the Reports tab screen. Reports are organized by the following categories:

General Statistics

General Statistics reports provide an overall view of your organization's Internet activity. This information is displayed numerically and graphically. Overall activity is displayed along with bandwidth consumption on an hourly, daily and monthly basis. Day by day reports are also included for ongoing trend analysis. License usage reports are available for you to audit your Echo•Suite license consumption.

Top 10

Top 10 reports show the ten most active web sites, ftp sites, email address, news groups, chat rooms and instant messages. Activity is based on "Impressions" which is the number of occurrences of each activity. A single Impression corresponds to a single entry in the Echo•Suite Activity Log.

Top N

Top N reports show the most active web sites, ftp sites, email address, news groups, chat rooms and instant messages. Activity is based on the number of occurrences of each activity. N is a configurable parameter that you define. The top 15 addresses are listed graphically; all N addresses are listed numerically.

Top Percent

Top Percent reports show the highest percentage of web sites, ftp sites, email address, news groups, chat rooms and instant messages. Activity is based on the number of occurrences of each activity. P is a configurable parameter between 1 and 99 percent. The top 15 addresses are listed graphically; all top P percent addresses are listed numerically.

Time On Line

Time On Line reports estimate the total time users have spent accessing the web. A configurable Idle Time parameter determines the maximum amount of time a user is assessed for being on a single web page. Results are displayed by user or by total time on an hourly, daily or monthly basis.

Time On Line reports also include the amount of time individuals and all users spend at a particular site or domain. The Top-N sites are shown on the summary page. By drilling down on a specific user-name, you can view all data relevant to that user.

Cost On Line

Cost On Line reports estimate the total cost users have spent accessing the web. A configurable Wage parameter determines the dollar amount a group of users is assessed for being on the web. Results are displayed by user or by total cost on an hourly, daily or monthly basis.

Cost On Line reports also include the cost individuals and all users spend at a particular site or domain. The Top-N sites are shown on the summary page. By drilling down on a specific user-name, you can view all data relevant to that user.

User Statistics

User Statistics report on detailed activity for each user. User violations and bandwidth consumption are also reported. A "Total Activity with supporting

data" report exists in order for you to distribute a view of the raw data in the Echo•Suite Activity Log.

Machine Statistics

Machine Statistics report on detailed activity for each machine. Machine violations and bandwidth consumption are also reported. You can also run an "Installed Machines" report to easily determine which machines contain the Echo•Suite Workstation agent.

Custom

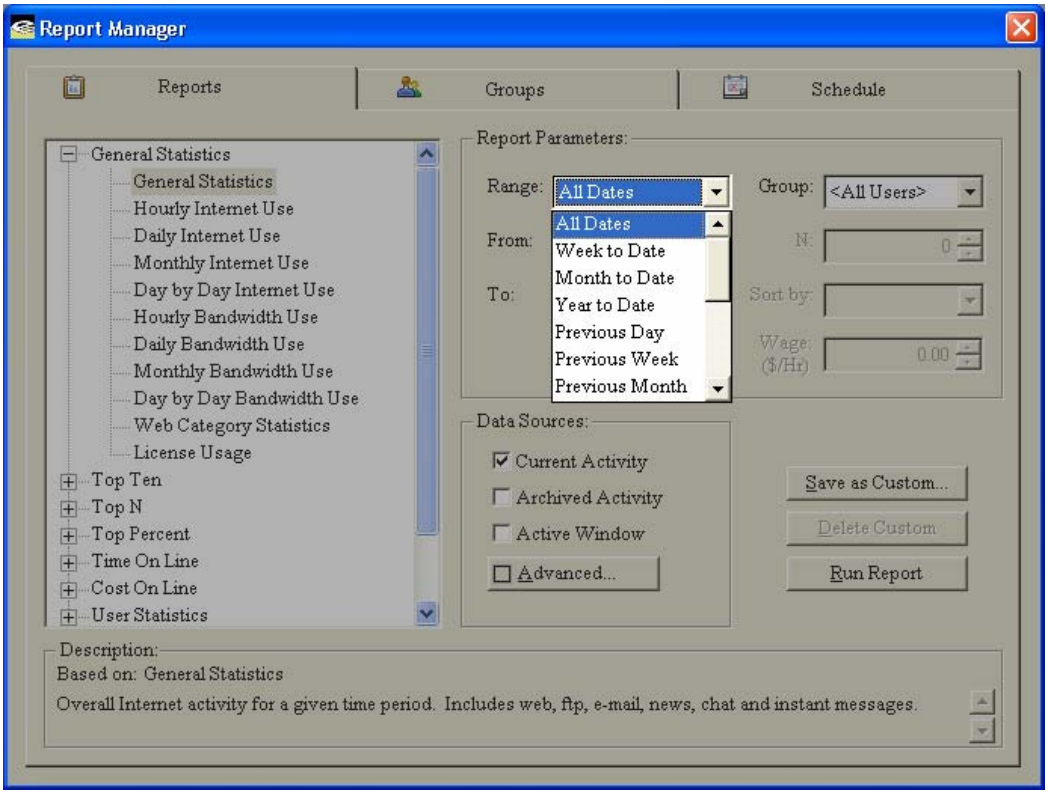
All reports can be customized and saved for future use. Your saved reports appear under the Custom Report section.

Categories

Many of the report sections above contain Category reports. Category reports are based on categorized web access available with Echo Filters™. The Echo•Suite Categories Module must be purchased for Echo•Suite to categorize web site activity.

Date Range

The Echo•Suite Report Manager allows you to specify a time period over which data is analyzed.



The time frames can be specified as follows:

All Dates

Reports on all data in the selected data source. The date range of the specified data is determined and presented in the Report Preview.

Week to Date

Reports on all data beginning with Sunday of the current week up to and including the current day.

Month to Date

Reports on all data beginning with the first day of the current month up to and including the current day.

Year to Date

Reports on all data beginning with the first day of the current year up to and including the current day.

Previous Day

Reports on all data from the day preceding the current day.

Previous Week

Reports on all data from Sunday to Saturday of the week preceding the current week.

Previous Month

Reports on all data from the month preceding the current month.

Previous Year

Reports on all data from the year preceding the current year.

Last 7 Days

Reports on the most recent seven days of data up to and including the current day.

Last 14 Days

Reports on the most recent fourteen days of data up to and including the current day.

Last 1 Month

Reports on all data over the last month beginning the day after the current day of the previous month up to and including the current day of the current month.

Last 3 Months

Reports on all data over the last three months beginning the day after the current day of the third prior month up to and including the current day of the current month.

Last 6 Months

Reports on all data over the last six months beginning the day after the current day of the sixth prior month up to and including the current day of the current month.

Last 12 Months

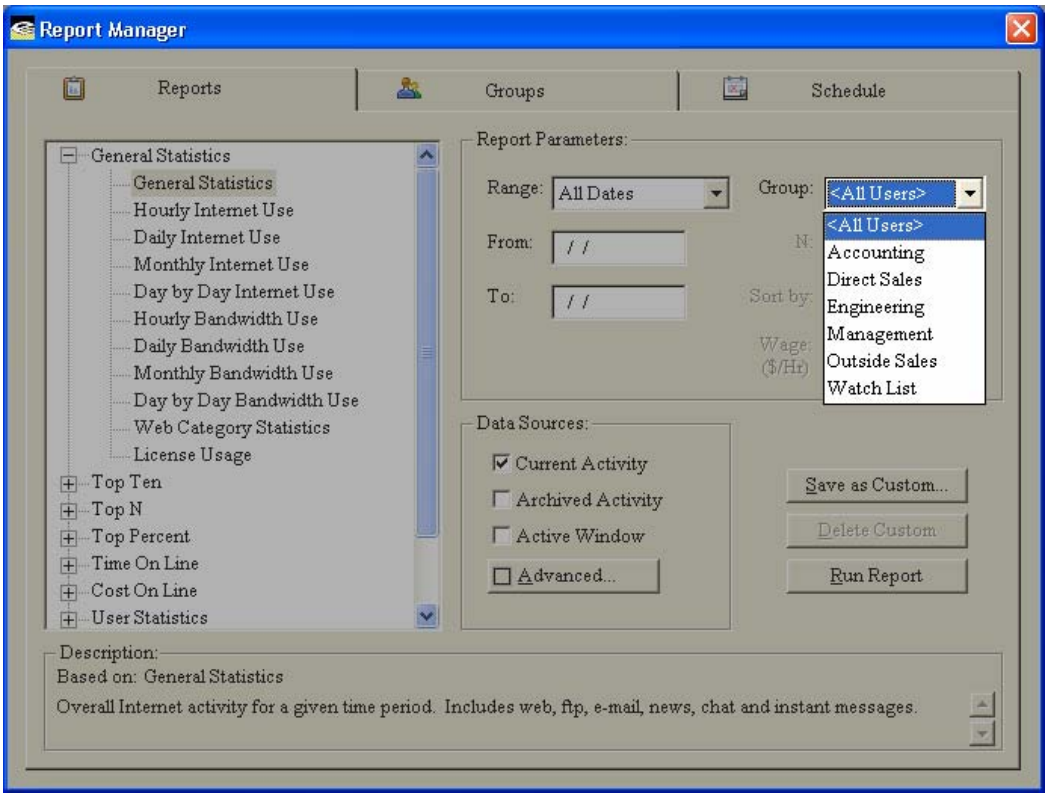
Reports on all data over the last twelve months beginning the day after the current day of the twelfth prior month up to and including the current day of the current month.

Custom

Reports on all data over a time frame that you specify.

Groups

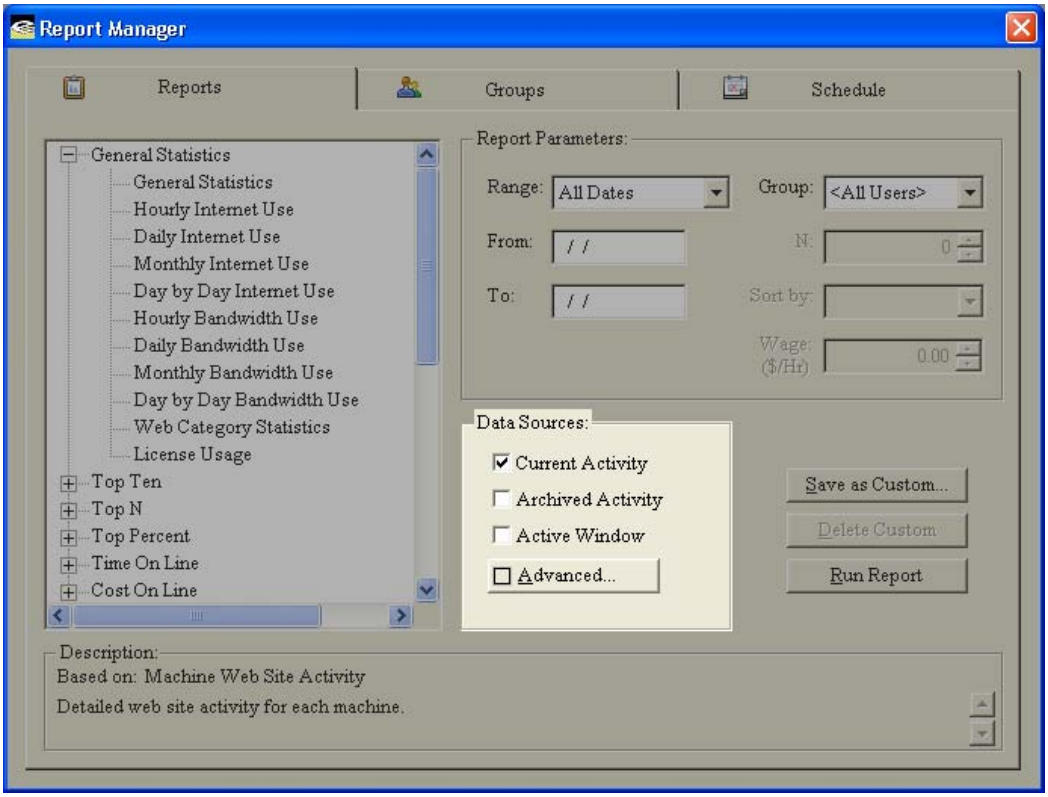
The Echo•Suite Report Manager allows you to specify a group of users to be included in the report results.



By narrowing reports based on specific users, reports can be run for managers of a specific group, department or division. Defining Report Groups is discussed in more detail later in this chapter.

Data Sources

The Echo•Suite Report Manager provides a number of data sources against which a report may be run.



The Reports tab provides access to the following data sources:

Current Activity

This option is used to report against the current *native* Echo•Suite Activity Log file. As the Echo•Suite Activity Log is dynamically changing and contains up-to-date data, this option is the most frequently used selection.

Archived Activity

This option is used to report against aged data that you have specified to be stored in your Echo•Suite archive directory. The directory containing your archived data is specified in the "Data Maintenance" selection of the Options menu. The Echo•Suite Report Manager can run reports against archived data stored to individual daily archive files or data appended to a single archive file.

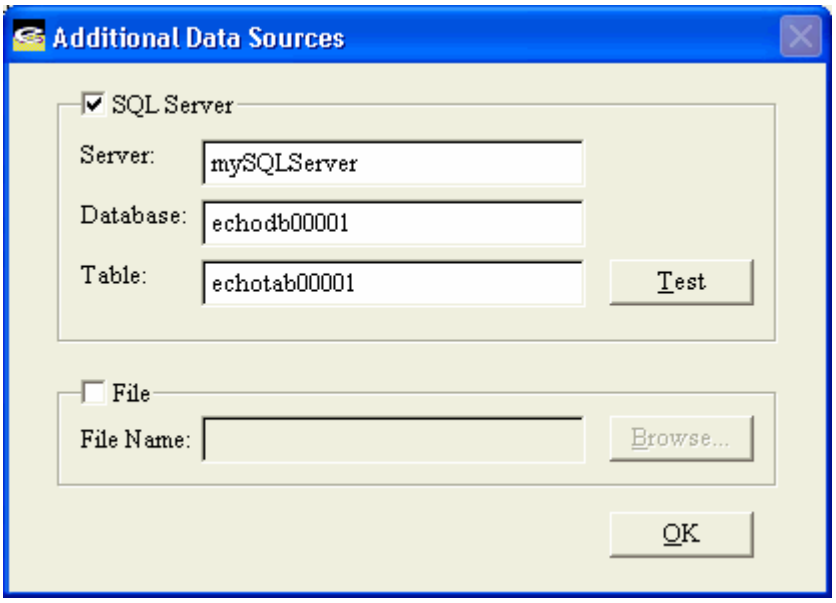
Active Window

When running reports interactively from the Reports tab, you can specify the active Echo•Suite window to be the data source against which reports are

run. This is useful for running reports against Activity Logs that you have filtered or sorted.

SQL Server

You can set the Echo•Suite Report Manager to report against data that has been logged to a Microsoft SQL Server. Under the Advanced button in the Reports tab, enter the SQL Server name, database and table where your Echo•Suite data resides.



Running reports on SQL Server allows data processing to be optimized on the SQL Server and is not constrained by a 2 GB data limit. When the SQL Server Data Source is selected, all other data sources in the report manager are cleared.

You can specify any database and table that contains Echo•Suite formatted data as your data source - including archive databases created by your SQL Server DBA.

File

You can specify a particular file against which a report will be run. The file you specify must be in Echo•Suite's native xBase file format. Echo•Suite files are created by saving filtered or sorted versions of the Echo•Suite Activity Log.

Saving a Report

Once a report's optional date range, parameters, group and data sources have been defined, the report can be saved for future use by selecting the Save as Custom button on the Reports tab. This feature allows you to create

reports for specific business units, divisions, groups, or individuals with limited access to data particular to each report.

When saving a custom report, you will be prompted for a report title and description, both of which will appear on your report when the report is run. This feature provides you with the ability to customize how the report header is displayed in order to fit your specific needs. Once saved, your new report will appear in the Custom section of the reports list. Selecting the custom report will reveal your report description as well as the standard report upon which your custom report is based.

Running a Report

Once a report's optional date range, parameters, group and data sources have been defined, the report can be run by selecting the Run Report button on the Reports tab. Running the report displays the Report Preview screen where you can view the report results, drill down through available data in the report, Quick-Link to reported web sites, print the report, save the report in a variety of file formats or e-mail the report through your existing e-mail software. E-mailing a report from the Report Preview screen uses the standard MAPI protocol to communicate with your default e-mail software. Some Microsoft security configurations may prompt you for input when sending mail though this MAPI interface. Reports that are e-mailed automatically through the Echo•Suite Report Scheduler do not use this MAPI interface.

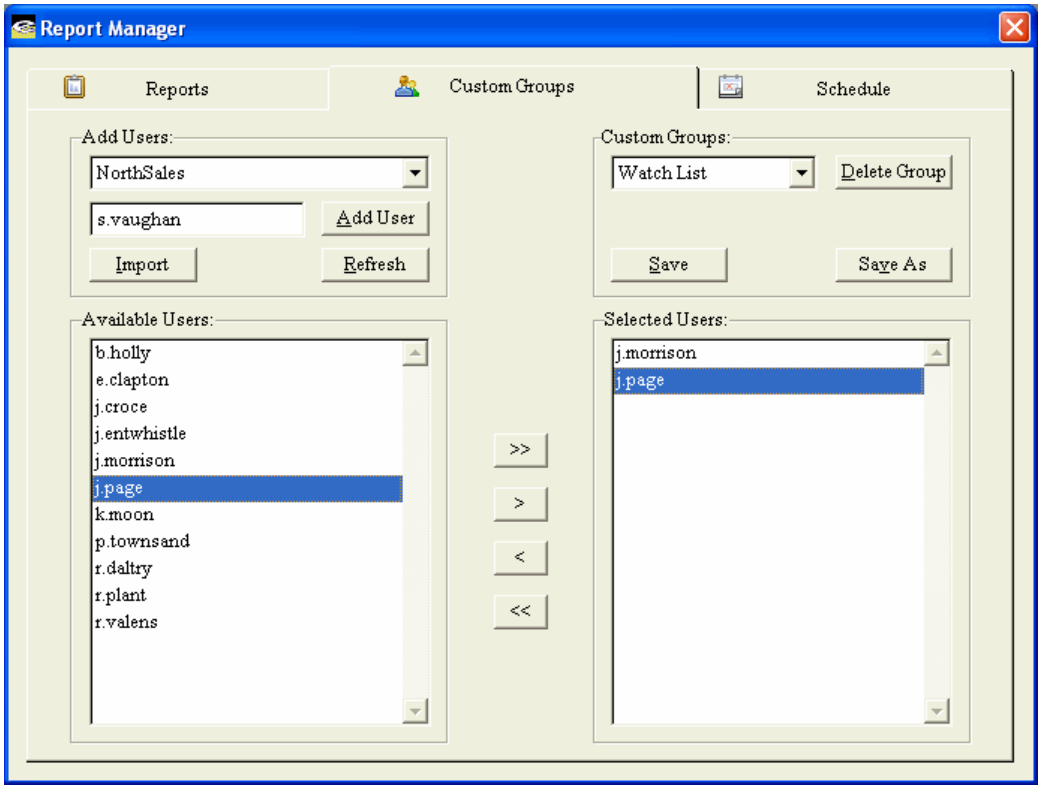
Echo•Suite Custom Report Groups

The group of users included in a report is selected on the Reports tab in the Echo•Suite Report Manager. Creating Custom Report Groups and defining users that belong to a Custom Report Group is done in the Groups tab in the Echo•Suite Report Manager. Only Groups specified in your Echo Data Access Permissions settings will be available for reporting.

Available Users

The names present in the Available Users list can be automatically or manually added. To automatically add users to the Available Users list, select the Domain Groups dropdown to present users that belong to the selected Domain Group.

Importing a list of names from a text file can also be used to populate the list of Available Users. The text file you import should be formatted to contain one user name on each line of the text file.



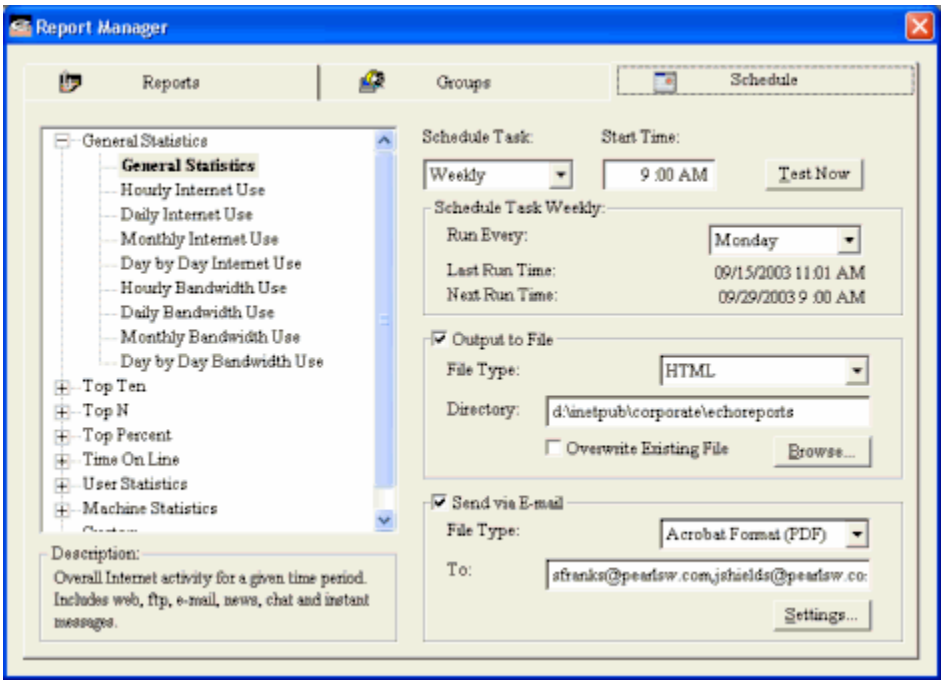
Lastly, you can manually add users to the Available Users list by typing a user name in the name box and selecting the Add User button. To delete a name from the Name list, select the name and then select the delete key.

Selected Users

To add users to a group, select the user in the Available Users list and select the right arrow button. You can press the shift or ctrl keys to select multiple users to be added to a group. To add all users to a group, select the right double arrow button. To remove users from a group, select the user in the Selected Users list and then select the left arrow button. You can press the shift or ctrl keys to select multiple users to be removed from a group. To remove all users from a group, select the left double arrow button. To save modifications to an existing group, select the Save button on the Groups tab. To save modifications as a new group, select the Save As button on the Group Tab. To delete a group from the Group list, select the Delete Group button next the selected group.

Report Scheduler

The Schedule tab in the Echo•Suite Report Manager provides you with the ability to schedule your standard and custom reports to be automatically created and distributed. Reports can be scheduled to be run once, daily, weekly or monthly. The Schedule tab informs you of the last time a scheduled report was run and, if applicable, the next time the report is due to be run. Reports that are scheduled to be run will appear in bold font in the report list tree-view.



File Output

The Schedule tab allows you to define how a scheduled report will be saved. Reports can be saved in any available location on your Echo•Suite server or network share. Echo•Suite reports can be saved in a variety of file standards including Adobe Acrobat, Crystal Reports, HTML, Microsoft Excel, Microsoft Word, Rich Text Format and Plain Text formats. Reports saved in Crystal Reports format will provide a dynamic report experience for users licensed to use Crystal Reports. Your Echo•Suite license provides you with Crystal Reports functionality within the Echo•Suite Report manager.

By saving scheduled reports to a shared location, users can conveniently access Echo•Suite reports on the network. If reports are saved in HTML format, reports can be automatically integrated into your organization's intranet.

When a report is saved to a location that you specify, the report can be saved with a unique identifier in order to retain the same report previously run or can be set to overwrite the same report previously run.

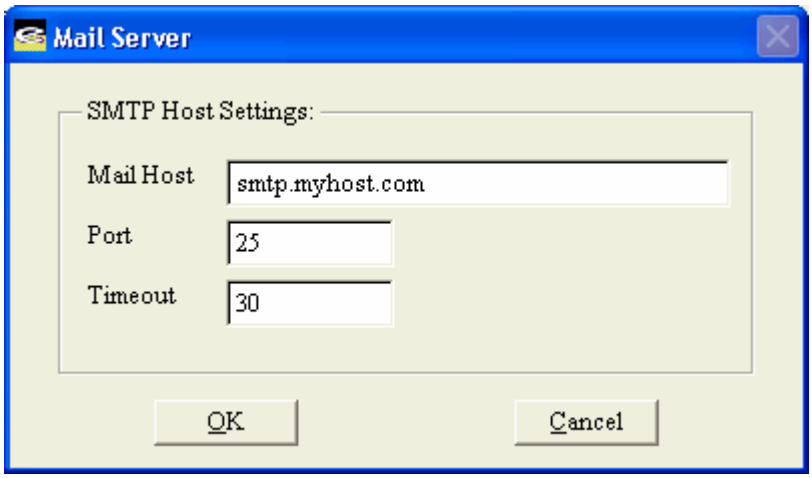
E-mail Output

The Schedule tab allows you to specify if a report is distributed via Echo•Suite's SMTP e-mail service. Reports are e-mailed as attachments in a variety of file standards including Adobe Acrobat, Crystal Reports, Microsoft Excel, Microsoft Word, Rich Text Format and Plain Text formats.

You can specify multiple email recipients in the "To" box on the Schedule tab by separating e-mail addresses with a comma.

Configuring the Report Manager Email Service

The Echo•Suite Report Manager e-mails reports by communicating with an available SMTP relay. To configure the Report Manager email service, select the Settings button on the Schedule tab and indicate the SMTP server and port with which the Echo•Suite Report Manger should communicate.



You can customize the appearance of the emailed report by modifying the email footer. This is done by selecting "Customize" from the Reports menu.

Distributing the Echo•Suite Reporting Console

A copy of the Echo•Suite Administration Console can be configured as an Echo Reporting Console and can be distributed to managers or supervisory personnel that want to run their own reports. By installing the Echo•Suite Server software on a user's workstation, you provide the user access to the Echo Report Manager and logged activity data. The Echo Report Manager will be the only function active in the console since your Echo•Suite workstation agents are not configured to communicate with the managers or supervisor's workstation.

There are a number of options to distributing the Echo Reporting Console:

Option 1: Administrator Install of Echo Reporting Console

1. Login to the user's workstation using an account with administrative privileges.
2. Run Setup.exe from the installation media or download directory.
3. Select Server Setup.
4. Run the Echo•Suite Administration Console and proceed through the Setup Wizard.
5. When prompted, enter your product serial number.
6. Set Data Access Permissions as required in the "Data Access Permissions" selection of the Options menu.
7. Create a User Level password in the "Change User Level Password" selection of the Security menu. Provide the User Level password to individuals that want to use the Reporting Console.

Option 2: User Install with Data Access Restricted to all Domain Groups

The Echo Reporting Console can also be distributed for individuals to install where access to user data is restricted to "All Domain Groups" in the "Data Access Permissions" selection of the Options menu.

Instruct users to:

1. Run setup.exe from the installation media or download directory.
2. Select Server Setup.
3. Run the Echo•Suite Administration Console and proceed through the Setup Wizard.
4. When prompted, enter your Domain Group Reporting Console serial number.

The Echo Reporting Console will be installed with restricted access to the Security and Options menu items - similar to a User Level login.

Option 3: User Install with Data Access Restricted to the echo-*username* Organizational Unit

The Echo Reporting Console can also be distributed for individuals to install where access to user data is restricted to "Only Domain Groups in Organizational Unit (OU) named echo-*username*" in the "Data Access Permissions" selection of the Options menu.

Instruct users to:

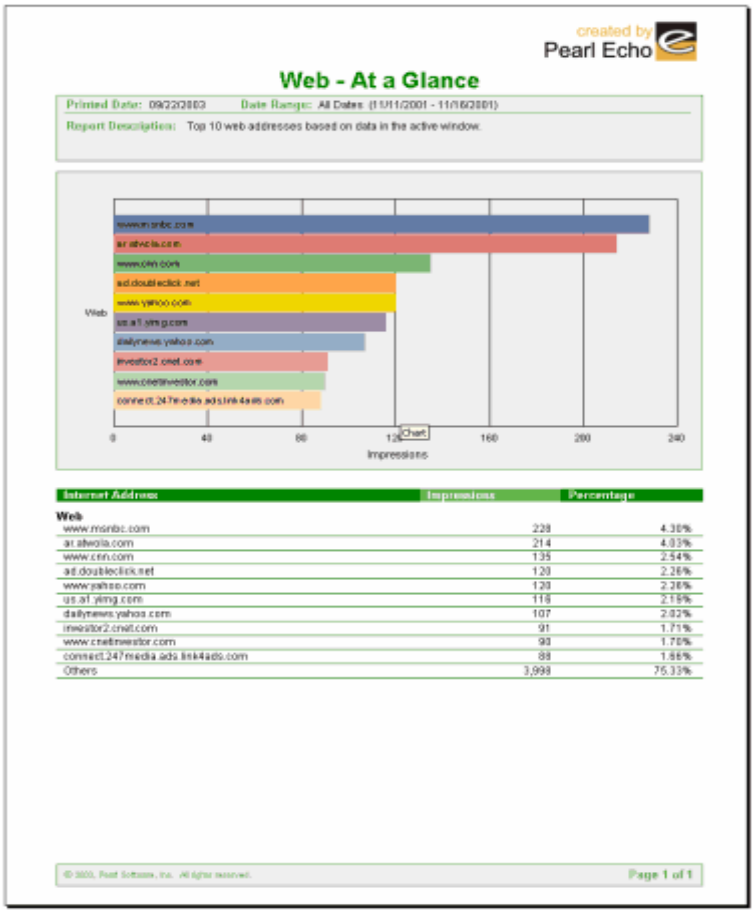
1. Run setup.exe from the installation media or download directory.
2. Select Server Setup.
3. Run the Echo•Suite Administration Console and proceed through the Setup Wizard.
4. When prompted, enter your Restricted OU Reporting Console serial number.

Chapter 8

Data Analysis

At-a-Glance Reports

Selecting an item in the Echo•Suite At-a-Glance Reports Menu will provide you with details on how the Internet is being used. Echo•Suite will report on the most frequented web sites, email transactions, news group postings, file transfers, and chat groups. Echo•Suite Reports will also show you the top Internet users and computers on your network.



Time on Web Reports

Echo•Suite can *estimate* the amount of time users spend on the World Wide Web. Echo•Suite calculates the duration of web activity by looking at successive log entries in the Echo•Suite Activity Log. Because Echo•Suite can not determine if users are actively reading a web page or just have left their browsers open while talking on the phone, eating lunch, etc., a configurable Idle Time parameter is used to determine the maximum amount of time a user is assessed for being on a single web page. To configure the Idle Time, select the Idle Time option in the "Settings" section of the Report Menu.

Idle Time = 2 minutes

☑ **The Time on Web value is actually calculated based on seconds; the final result rounded to the nearest minute.**

In the example above, Steven would be assessed 5 minutes of Web activity:

1 minute for being on cnn.com

2 minutes (the maximum amount of time charged) for being on abcnews.com

1 minute for being on espn.com and

1 minute (half of the Idle Time) for the final entry, monster.com.

When At-A-Glance and Time on Web reports are run from the Reports menu, Echo•Suite reports against data in the active Echo•Suite window. For more extensive reporting, refer to the Echo•Suite Report Manager section above.

Combining Echo•Suite & Spread Sheet Programs

You can export the active log window to a number of file formats for sharing or custom data analysis.

Echo•Suite allows you to combine the power of Echo•Suite monitoring with the power of popular data analysis tools. Export formats supported by Echo•Suite include:

- .TXT - Customized Delimited Text
- .XL5 - Excel Version 5.0
- .XLS - Excel
- .WK1 - Lotus 1-2-3 revision 2.x
- .WKS - Lotus 1-2-3 revision 1.a
- .WRK - Lotus Symphony version 1.10
- .WR1 - Lotus Symphony version 1.01
- .DIF – VisiCalc

Appendix

A

Echo•Suite Program Components

Echo•Suite's security is predicated upon Microsoft's Access Control settings and Microsoft's network provider chaining model. To function properly, Echo•Suite must have full access to its own files and network components. **Components of Echo•Suite should not be indiscriminately removed by third party applications such as antivirus and antispyware programs.**

The following is a list of Echo•Suite directories and components that must not be altered, scanned or opened by third party applications:

Echo•Suite Server	
All Files in Echo•Suite program directory	Typically c:\Program Files\Echo 7.0
Echo•Suite Workstation	
All files in the Echo•Suite program directory	Typically c:\Program Files\Common Files\Microsoft Shared\pse7
All files in the Echo•Suite user directory	Typically c:\Documents and Settings\<user name>\Local Settings\Application Data\pse7
Network Layer files in the Windows System directory	.Dll files having a prefix of lspent (e.g. lspent*.dll)
Network components in the Winsock 2 layered service provider chain	Echo 7 Layered Provider

Appendix B

Echo•Filters

The following is a list of available categories used by Echo•Filters:

Category	Description
Ad Services	Sites that are used for bulk or email advertising. Banner ads are included.
Adult	Discussion of adult topics, phone sex, adult chat rooms. Nudity may be included but not graphic sexual content. Hate, advocating of violence, Satanism and other subversive groups are included. Domains that sell adult novelty items or adult videos are included.
Alcohol and Tobacco	Alcohol or tobacco sales or discussion how to make alcohol and mix beverages.
Alternative Lifestyle	Gay, Lesbian, Nudist Colony, etc. No nudity appears on the site. Discussion about these alternative lifestyles only.
Anonymizer	Sites that are used for anonymizing Internet access.
Arts	Museums, art galleries, artist sites, photographers (artistic / tasteful nude allowed).
Auctions	Sites that allow auction / bidding on items.
Blogs	Sites that either offer blogging services or personal pages.
Business	Sites that are run by a business. They may or may not be selling products or services.
Chat	Sites that contain a chat area or are primarily dedicated to online chat.
Computers	Computer related sites. May discuss computer software, programming, repair, etc.
Dating and Personals	Online dating guides and matchmaking services.
Download Media	Streaming video, music, mp3, and other bandwidth intensive sites.

Downloads	Any type of application available for download from a site including sites that specialize in file downloads.
Education and Reference	Schools, universities, and sites dedicated to research.
Entertainment	Information about the entertainment industry or personal entertainment. Movies, television, and magazines are included.
Error or Blank	Domains that do not resolve to a valid server.
Finance and Investment	Stock trading, investment advice or online banking.
Free Hosting	Free webpage hosting sites.
Gambling	Online gambling, bookmaking, sports betting, dog tracks, horse race betting.
Games	Gaming and gaming related activities. Gambling related sites are not included.
Hacking and Warez	Sites that discuss or distribute tools for hacking, cracking, attacking, or phreaking systems. Contains keys, serial numbers, or cracked downloads for pirated programs.
Health	Health related sites that are legal in nature. Hospitals and medical related sites such as pharmacies.
Home	Home decorating, appliances and things that are purchased for homes. Real estate for homes is also included.
Illegal Activities	Illegal online pharmacies, weapons, bomb making, credit card fraud, illegal drugs and drug manufacturing or recreational drug usage.
Job Search	Resume posting and job-hunting sites.
Kids and Teen	Sites appropriate for children and teens. Some teen online help sites are included.
Lingerie	Sites that sell or promote lingerie. No graphic photos.
News	Sites for news agencies and outlets.
Parked Domains	Companies who hold domains and pay people for their usage.
Recreation	Includes both outdoor and indoor recreation. Sports are in a separate category.
Redirectors	Sites with the primary purpose to redirect users to another site to hide the identity of the destination site.
Regional	City, state, country, military, or government sites.

Religion	Religious discussion sites and sites for places of religious worship.
Science	Science and discussions of science related information. Biology, DNA, and science related companies.
Sex Education	Sexual education sites. No graphic adult material allowed. Sexual related topics may be included if presented in an educational manner.
Shopping	Sites that offer something for sale.
Society	Clubs, organizations for causes, social issues and politics.
Spam	Domains identified as spam traps.
Sports	College, amateur, and professional sporting events and activities.
Travel	Sites that sell, book and specialize in travel.
Weapon Related	Weapon related sites for guns and knives that are not illegal. Gun clubs, hunting, legal weapon sales, etc.
Webmail	Sites that offer Web-Mail from their domain.
World	If a domain contains no English it will be classified here.
XXX	Graphic adult material. Pornographic sites, and sites that sell pornographic materials.

Appendix C

Troubleshooting Tips

Issue	Resolution
Echo•Suite Workstation installation fails to connect to Echo•Suite server.	Verify that the Echo•Suite Management State is On in the Echo•Suite Administration Console. Verify that a firewall is not blocking communications on any of the Echo•Suite TCP/IP ports. Refer to Chapter 2 of this Guide for firewall configuration parameters.
Echo•Suite Administration Console hangs at startup every few weeks.	The Echo•Suite Administration Console optionally checks for product updates every two weeks. Verify that a firewall is not blocking ftp communication from echo70.exe or disable auto-updates from the Options->Preferences menu.
Echo•Suite Administration Console periodically stops updating the Activity Log. After rebooting, logging resumes and missing activity is present.	Echo•Suite requires exclusive access to the Echo•Suite database files. Exempt the Echo•Suite Program Directory from antivirus and antispyware scans.

Issue	Resolution
"Network components have been altered" appears in the Echo•Suite Activity Log,	Echo•Suite's Winsock 2 components have been modified, displaced, or removed by a third party program. Uninstall and reinstall the Echo•Suite Workstation software. See Appendix C of this Guide for details on configuring third party security utilities with Echo•Suite.
Echo•Suite Administration Console installed on Windows NT 4 does not show Active Directory Users or Groups.	Install Microsoft's Active Directory Client Extension, commonly referred to as the DSClient. There are two versions of the DSClient, one for Windows NT 4.0 and the other for Windows 95, Windows 98, and Windows Me. For more information about DSClient, see "How to install the Active Directory client extension" in the Microsoft Knowledge Base at support.microsoft.com/default.aspx?scid=kb;en-us;288358
Citrix Published Applications are not monitored.	The Echo•Suite workstation agent must be running for Pearl Echo to monitor applications running in desktop or published mode. For more information on monitoring published applications, see "Using Pearl Echo to Monitor Published Applications on Citrix and Windows Terminal Server" in the Pearl Software Knowledge Base at www.pearlsoftware.com/support/kbase.html
OLE Error appears when opening Report Manager.	One of Echo•Suite's active-x components has not been registered or its registration information has been corrupted. Issue the following two commands from a command prompt on the Pearl Echo server: c:\windows\system32\regsvr32 <Path to Pearl Echo Program Directory>\ChilkatMail.dll c:\windows\system32\regsvr32 <Path to Pearl Echo Program Directory>\ChilkatUtil.dll

Appendix D

Glossary

Activity Log: List of activity logged during past Internet sessions.

AIM: (America Online Instant Messenger) is a proprietary instant messaging program that informs users who's on-line at any time and enables users to contact each other at will. Using AIM, users can chat and send private messages to one another. AIM runs as a stand alone application or as an integrated component in the AOL user interface.

Applet: A small program or application. Web-Chat Java™ applets are small programs that download into your Web Browser to view and send chat text.

Cache: A data storage buffer.

Control Lists: Echo•Suite Block and Allow lists used to control access to Web, Ftp, News, Chat, and Email address.

Cookies: Data transmitted behind-the-scenes to and from Internet Web servers.

Current Profile: Configuration name selected in the Profile Settings screen and the name that appears in the menu toolbar. All configuration and Control List settings pertain to the Current Profile. See Profile.

Email: Electronic mail consists of a message header and message body. The header contains addresses of the mail sender and recipients. The header may also contain the message body subject matter. Addresses follow the form username@computer.something. The message body contains text and possibly images, sound, video, and file attachments.

FTP: File Transfer Protocol programs are used to send and retrieve files to and from file servers on the Internet. Files can be programs, pictures, movies, etc.

FQDN: Fully Qualified Domain Name (e.g. echoserver.company.com)

HTML: Hyper Text Markup Language is the code used by web pages to display text, graphics, tables etc.

ICQ: ICQ is a non-standard instant messaging program that informs users who's on-line at any time and enables users to contact each other at will. Using ICQ, users can chat and send private messages to one another.

IM: Instant Messengers are proprietary messaging programs that inform users who's on-line at any time and enables users to contact each other at will. Instant Messenger programs include AIM, Yahoo! Messenger, ICQ, and MSN Messenger Service

Impressions: Echo•Suite report activity is based on "Impressions" which is the number of occurrences of each activity. A single Impression corresponds to a single entry in the Echo•Suite Activity Log.

Internet: The Internet is a constantly growing group of international computers networked together by telephone lines. The Internet was created in the 1960's as a US Government endeavor to connect various computer systems in a fault-tolerant manner. The Internet is now used by millions of people, from commercial and educational institutions to individual consumers. The computers that are connected to the Internet are accessed through Internet software programs primarily to exchange email, news, chat with other users, transfer files, and browse the World Wide Web.

IRC Chat: Internet Relay Chat is an interactive electronic forum whereby users chat among themselves by typing messages to a global or private message board. Like News groups, Chat groups are arranged by subject. These subjects span an enormous range of topics. Messages posted to chat groups consist of a user id followed by a sentence or two of text. The format is similar to a playwright's script.

MacID: The Media Access Controller Identification is a unique ID associated with the network card within a workstation.

News: Network News Transfer Protocol (NNTP) is an electronic bulletin board where messages are posted in various groups. News groups are arranged by subject ranging from sports & music to sex & pornographic pictures. Messages posted to news groups consist of a message header and message body. The header contains the address of the news poster as well as the message body subject matter. The message body contains text and possibly images, sound, video, and file attachments.

NNTP: Network News Transfer Protocol (see News).

PICs: A rating system which relies on content providers voluntarily rating the content they create and distribute. There are various rating systems that have been developed and are currently being used on the Internet. PICs rating systems attempt to characterize the nature of Web pages and other Internet content.

Pop-3/SMTP: Post Office Protocol-3/Simple Mail Transfer Protocol are the dominant means for receiving and sending mail through the Internet. Email

applications like Microsoft Mail™, Netscape Mail™, Eudora™ as well as Email servers all conform to this standard.

Profile: An Internet access configuration assigned to a User name or Group name. The Internet access configuration includes Web, Ftp, Email, News and Chat Control Settings, Block and Allow Control List locations, Rating System Settings and other access control variables. When a network User attempts to access the Internet, their activity is governed by a Profile's configuration settings.

URL: Uniform Resource Locators are addresses used to find locations on the World Wide Web. Typical URL's begin with http:// or ftp://.

Web Browser: Web browsers are graphical software programs that allow users to search for and access world wide computer systems that exist on the Internet. Examples of Internet browsers include Netscape's Navigator™ and Microsoft's Internet Explorer™.

Web-Chat: Certain Web pages have non-standard chat applications (applets) built-in. Chatting through a Web browser is known as "Web-Chat".

World Wide Web: A portion of the Internet defined by Internet Web servers. Internet Web Servers are depositories of information accessed by Web Browser programs. This information is displayed graphically through the use of formatted text, images and sound.

Appendix

E

Contacting Pearl Software

By Email

- For sales questions: sales@pearlsw.com
- For support issues: support@pearlsw.com
- For general issues: information@pearlsw.com
- For reseller information: reseller.info@pearlsw.com

By the Web

- Echo•Suite Web: www.PearlEcho.com
- Corporate Web: www.PearlSoftware.com
- Purchase Web: www.PearlSoftware.com/Purchase
- Support Web: www.PearlSoftware.com/Support

By Telephone

- (800) 732-7596 (800-PEARL96)
- (610) 485-5160 (International)

By Mail

- Pearl Software, Inc.
  64 East Uwchlan Ave.
  Suite 230
  Exton, PA 19341
  USA