PearlEcho 12

Pearl Echo User's Guide

Version 12

Information in this document refers to features available in Version 12 of Pearl Software's Echo.Suite software. If you have purchased a module of Pearl Echo.Suite such as Website.Echo or IM.Echo, please refer to http://www.pearlsw.com/products/comparison.html for a list of features available with your product and described herein.

Information in this document, including URL and other Internet web site references, is subject to change without notice. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced or transmitted in any form without the express written consent of Pearl Software, Inc.

Pearl Software may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Pearl Software, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

TRADEMARKS: Pearl Software, Pearl Echo, Echo.Suite, Echo.Filters, Website.Echo, IM.Echo, and Mobility Monitor are either registered trademarks or trademarks of Pearl Software, Inc.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

PATENTS: Pearl Echo.Suite, Website.Echo and IM.Echo are protected by one or more patents including U.S. Patent Nos. 6,978,304; 7,634,571; 7,958,237; 8,930,535. For more information about our patents, please visit: Patent – http://www.pearlsoftware.com/about/patents.html

Table of Contents

Chapter 1

Getting Started

Welcome

Introducing Pearl Echo®, a comprehensive employee Internet management package from Pearl Software. This premier tracking utility is the industry model for employee Internet access monitoring, filtering and control and represents the most significant step available today in promoting responsible Internet use in the workplace and at school. Featuring Pearl Software's Mobility Monitor™ technology, Pearl Echo can effectively block inappropriate sites or set time restrictions on Internet use, regardless of where end-users reside. Pearl Echo provides real-time control and capture of communicated content through IM and e-mail and provides detailed access configurations for your organization. Pearl Echo's Quick-Link feature allows complete restoration of all text from outbound and inbound communications. Pearl Echo is a powerful application, offering dynamic filtering, reporting and knowledge management functions to assist you in fulfilling your regulatory compliance and governance requirements.

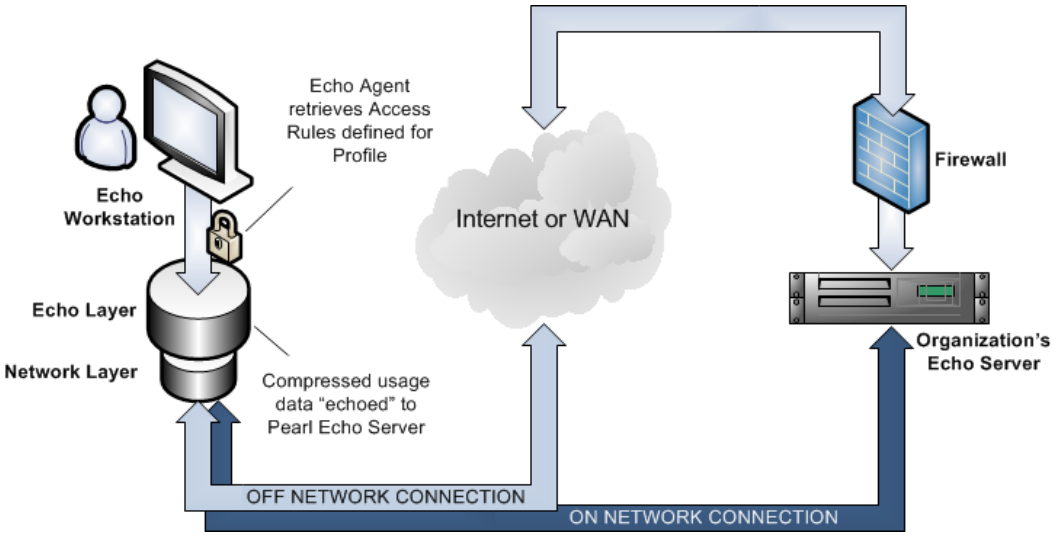
About this User's Guide

The Pearl Echo User's Guide describes Pearl Echo'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 Pearl Echo's context sensitive help found in the Pearl Echo Administration Console under the program's Help menu.

Pearl Echo Architecture

Pearl Echo's Employee Internet Management technology is based on an independent agent-server architecture. By creating an independent service, Pearl Echo is not affected by high traffic volumes, how users access the Internet, or where your end users are physically located. Pearl Echo'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 Pearl Echo 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 Pearl Echo Administration Machine 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 Pearl Echo Administration Machine. For ultimate efficiency, Internet access rules are applied at the workstation by the Pearl Echo agent. Data to be logged is first compressed by the agent in order to minimize network overhead. The Pearl Echo Workstation agent is deployed automatically from the Pearl Echo Administration Console or can be installed with a third party software management tool. Once deployed, the Pearl Echo Workstation agent is self-updating; the Workstation agent automatically retrieves any updates or upgrades to Pearl Echo when you update your Pearl Echo Server Software.

With Pearl Echo'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 Pearl Echo Workstation agent functions no matter how or where your users connect to the Internet.

Pearl Echo is not a Proxy Server. Users can have access to the Internet through any means - a direct connection, proxy connection, shared connection, etc. The Pearl Echo Administration Machine runs independently and is the point at which you define Internet access privileges as well as perform user Internet access analysis and reporting. Because Pearl Echo runs as its own service, Echo has no dependences on legacy Proxy Servers or Firewalls.

Installing Pearl Echo

Step 1: Echo Server Software Installation

☑ **You can automate workstation installation from the Pearl Echo Administration Console.**

The Pearl Echo 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 Pearl Echo 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 use Active Directory and would like to set Internet access privileges based on existing Active Directory User, Group or Computer names, you should install Pearl Echo 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 Pearl Echo service is Domain-Aware and will automatically find your database of Active Directory Users, Groups and Computers[1]. If you don't use Active Directory, Pearl Echo will automatically revert to the machine's local list of Users and Groups. Pearl Echo will even accommodate smaller peer-to-peer installations and allow you to set Internet access profiles based on local login names and computers. Regardless of your environment, there are no complicated setup steps for you to worry about. The Pearl Echo 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. Disable Antivirus & Antispyware applications prior to installation.
2. Run the secure setup.exe from the program installation folder or from the installation CD.
3. On the Startup screen, select 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
Note the destination location for your installation as you will need to exempt this folder from your antivirus & antispyware applications.

5. Configure your antivirus and antispyware applications to exclude from scanning the Pearl Echo program file directory that you created in number 4 (typically C:\Program Files (x86)\Pearl Echo).
6. Launch the Pearl Echo Administration Console from the Programs section of the Windows Start button.

[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 Pearl Echo 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.

7. Enter your Company name and purchased serial number. For demo installations
   a. Select the **Demo** button to generate a trial activation code. **Note: Stealth Mode is disabled in Demo mode.**
   b. Enter the trial activation code into the first "Serial Number:" field and select Next.

8. Confirm or Enter your IP settings:
   a. When prompted, confirm or enter the fixed IP address of the Pearl Echo Administration Machine (the server IP cannot be assigned via DHCP).
   b. We recommend that you use the default Port number 58000.
   c. Enter the Public IP or FQDN of the Pearl Echo Administration 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 Pearl Echo Workstation agent to make a connection back to the Pearl Echo Administration Machine. Please refer to the Advanced Installation chapter of this User's Guide for additional information on managing your remote users.

9. Enter a password to use when connecting to the Pearl Echo Administration Console. This password will also be used to securely uninstall the Pearl Echo Workstation Software, if needed.
10. Confirm that you wish to turn Pearl Echo Internet Management on Now. This setting starts the Echo Monitoring Services **and must be ON to begin the Pearl Echo Workstation Installation.**

Step 2: Automated Pearl Echo Workstation Installation

(Skip to the next Step if you choose to manually install the Echo Workstation Software or if you do not user Active Directory)

You can manage Echo Workstation installation and removal from your Echo Administration Console. After completing the Workstation Software installation, there will be no indication to a user that the Echo Workstation Software components are resident and running (licensed versions only).

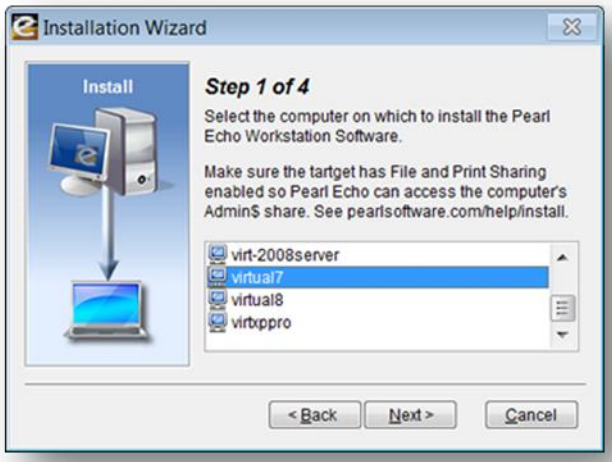
1. Create or open a network share and copy the Workstation folder from the Pearl Echo CD. The network share must be accessible to both the Echo Administration Machine as well as the target workstation.
2. Verify that the network share has *read and write* *share* permissions for your account on the Echo Administration Machine (preferably Domain Admin).
3. You must have login credentials permitting you to perform a software installation on the target workstation (preferably Domain Admin). Verify that the network share has *read and write* *share* permissions for this account as well (if different from the previous step).

TIP
Access to a folder on a file server can be determined through two sets of permission entries: the share permissions set on a folder and the NTFS permissions set on the folder. For the access permissions above, make sure you are working with *share* permissions.

4. Select the target workstation on which to install the Echo Workstation Software.

   The target workstation must have file and print sharing enabled.

   (You will be able to select multiple workstation targets for simultaneous deployment when you enter the Administration Console.)



TIP
Check File and Print sharing settings in the workstation's Control Panel | Network and Internet | Network and Sharing Center | Advanced Sharing settings. For help on easy methods to enable file and print sharing on your network, visit pearlsoftware.com/help/install.

5. Specify the UNC path to the Workstation installation files you copied to the network share in 1, above. The wizard will verify that the necessary share permissions exist for this directory. You must specify a UNC path as this path will also be referenced by the target workstation to access the Echo Workstation installation files.

6. The Echo Workstation installation requires a system reboot. Specify when the target workstation should restart. Note that forcing an immediate workstation restart from the Administration Console will reboot the target workstation without warning potentially active end-users.
7. Enter the login credentials permitted to perform a software installation on the target workstation.
8. Click 'Next>'. Once complete, a log file will be generated displaying installation results including any errors if they occurred.
9. Now that you have installed the Echo Workstation Software, begin browsing the Internet from the workstation in order to test your initial setup.

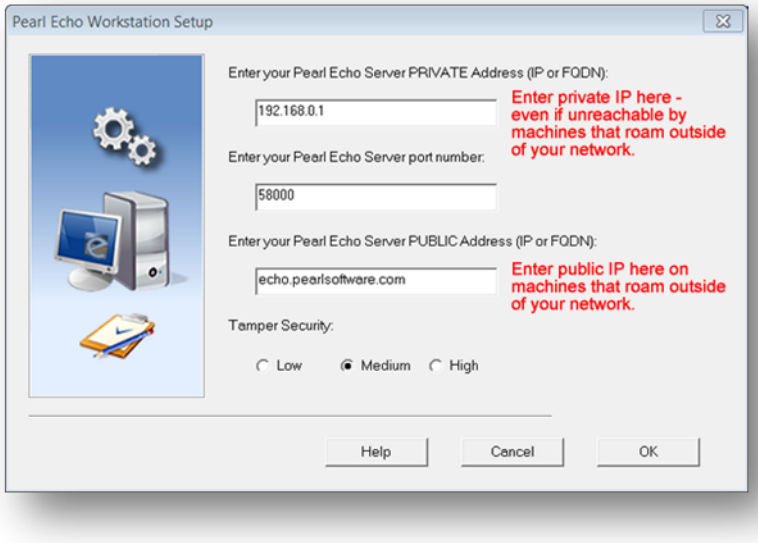
10. Return to the Echo Administration Console to view the monitored activity. You should see the workstation's Internet activity presented after opening or refreshing the Pearl Echo Activity Log.

Step 2 (Optional): Manual Pearl Echo Workstation Installation

The Echo Server Software must be **installed with Internet Management set to ON** prior to installing the Echo Workstation Software. To complete this installation, you will need the Echo Administration Machine IP address or FQDN, port and, if appropriate, the public Echo Administration Machine IP or FQDN entered in Step 1 point 8 above. After completing the Workstation Software installation, there will be no indication to a user that the Echo Workstation Software components are resident and running (licensed versions only).

Follow these steps to manually install the Echo Workstation Agent:

1. Login to the workstation using an account with Administrator privileges.
2. Disable antivirus and antispyware applications before beginning installation.
3. Run the secure setup.exe from the program installation folder or from the installation CD.
4. Select Workstation Setup from the startup screen.
5. Enter the Echo Administration Machine FQDN or IP address entered in Step 1 part 8a of the Echo Server Software Installation above. (Note: FQDN is recommended in case you later move or upgrade your Administration Machine to a new IP.)



6. Enter the Port number that you specified during the Echo Server Software Installation in Step 1 part 8b above (58000 by default).
7. If the workstation will roam outside of your private network, enter the Public IP or FQDN of your Echo Administration Machine entered in Step 1 part 8c, above. To manage users while they roam outside of your private network, you will need to configure your firewall to allow the roaming Echo Workstation Software to make a connection back to the Pearl Echo Administration Machine on four ports (58000-58003 by default). Please refer to Advanced Installation instructions in Chapter 2 of this User's Guide.
8. Select a Tamper Security level. The **Medium** setting is recommended during evaluation.

TIP
You can configure your managed workstations to provide a Low, Medium or High level of tamper security and prevention. Set to Low, Pearl Echo will not prevent users from accessing the Internet if Pearl Echo components have been altered manually or by third party applications such as antispyware or antivirus software. This is useful in environments where security tools cannot be configured to exempt Pearl Echo or on workstations that have become unstable due to viruses, unauthorized applications or neglect. With Tamper Security set to Medium, Pearl Echo will prevent access to the Internet if Pearl Echo components have been altered. This is the default setting and is targeted to well-managed environments. When Tamper Security is set to High, Pearl Echo will prevent access to the Internet if Pearl Echo components have been altered or if access to the Pearl Echo Services is not available on your server. The Echo Service may be unavailable due to server maintenance, network problems, trial expiration, etc.

Please note, if you are running an evaluation version of Pearl Echo, the Echo service will not be available once your trial period has expired. After expiration, a workstation with Tamper Security set to High will have Internet access blocked.

9. The workstation will perform a test communication with the Pearl Echo 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 Monitoring Services, here are some common issues that may need to be addressed:

- **Firewall. Firewall. Firewall.** If a software firewall is on the Pearl Echo Administration Machine, add the rule to allow the Pearl Echo process echoComm.exe. If a software firewall is on the managed Workstation, add the rule to allow the Pearl Echo processes rnappp7.exe and updater7.exe. (The installation software attempts to configure these settings automatically.) If a hardware firewall is installed between your Pearl Echo Administration Machine and managed Workstations, please be sure to make the firewall port assignments as detailed in Chapter 2 of this User's Guide.
- Make sure you have correctly identified and set your Administration Machine's FIXED IP address in the Pearl Echo Administration Console under the Options->Network Configuration menu.
- Make sure your Pearl Echo management is ON in the Pearl Echo Administration Console under the Security->Set Security Status menu.

10. Configure your antivirus and antispyware applications to **exclude the Pearl Echo Workstation program file directory folder.** You will also need to configure anti-virus and antispyware applications to not disturb the Pearl Echo Workstation Agent or its components. Refer to this Guide's Appendix for detailed guidelines.
11. Now that you have installed the Pearl Echo Workstation 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 Pearl Echo Administration Console to view the monitored activity. You should see the workstation's Internet activity presented in the Pearl Echo Activity Log.

TIP
If you do not see the workstation activity, you might need to refresh your Pearl Echo activity log from the File menu or by selecting the F5 key while in the Pearl Echo Administration Console.

13. Congratulations! You have successfully completed the initial installation. For detailed information on procedures and tips to help you continue a successful implementation using more advanced deployment options, please refer to the *Advanced Installation* chapter of this User's Guide.

Upgrading from a Previous Version of Pearl Echo

The instructions contained in this section are for major release upgrading only (e.g. **10**.09.0009 to **12**.03.0003). For minor release patching (e.g. 12.**01.0001** to 12.**03.0003**), follow the patching instructions at www.pearlsoftware.com/echo12/updates. Pearl Echo Version 12 will automatically gather your existing settings from Pearl Echo Version 5 or later. You must have a valid Version 12 serial number to successfully upgrade from a previous version.

Server Software Upgrade

Before installing and activating the Version 12 Server Software,

1. Login to the Administration Console of your previous version of Pearl Echo and turn Internet Management OFF from the Set Security Status menu.
2. Make note of your network settings in the Options->Network Settings menu.
3. Close the Pearl Echo Administration Console.
4. Make a backup copy of your Pearl Echo Server installation directory.

Server Software Upgrade from Version 8 and Later

Upgrading from Version 8 through Version 11 should be accomplished using the Pearl Echo 12 server installation software. A link to the full product download is emailed during trial registration and order confirmation. When run against your previous server software install, all settings and data will be maintained.

1. Run setup.exe from the downloaded Version 12 installation CD.
2. On the Startup screen, select the Server Setup Button.
3. The InstallShield Wizard will prompt you to confirm the default installation settings.
4. Once complete, login to the Administration Console and enter your Version 12 serial number in the Help->About Pearl Software menu.
5. Select "OK" and re-enable Internet Management when prompted.

Server Software Upgrade from Version 7 or Earlier

Install and run the full version of Pearl Echo Version 12 in a new program directory. A link to the full product download is emailed during trial registration and order confirmation. When prompted, use the same IP and Port settings as your previous installation. Your pervious version's profiles, lists, active data and report settings will automatically be migrated to your new installation. After you confirm migration of your previous version's settings, uninstall the previous version Pearl Echo Server Software from Add/Remove Programs.

Workstation Software Upgrade

It is recommended that you upgrade your Pearl Echo Workstation Software in order to take advantage of the added features and new filtering module changes available in this latest version.

Workstation Software Upgrade from Version 7 and Later

Previous versions of Pearl Echo Workstation must be patched to Version 10.099 or later to *automatically* upgrade your Pearl Echo Workstation agents to Version 12.

Part 1:

1. If Pearl Echo Workstation agents are not at version 10.099 or later, download the Version 10.099 Workstation patch from the Pearl Software website, www.pearlsoftware.com/echo10/updates.
2. Place the Version 10.099 Workstation patch in the WS_Updates folder found in the directory where you installed the Pearl Echo Version 12 Server Software.

The Pearl Echo Administration Machine will automatically deliver the *patch* to Pearl Echo's workstation agent. After delivery, the self-updating agent will *patch* itself the next time the machine on which the workstation agent resides is restarted.

Part 2:

1. To complete the Version 12 *upgrade*, place the Pearl Echo 12 Workstation upgrade file, Upgrade_120xx_WS.msi, in the WS_Updates folder found in the directory where you installed the Pearl Echo Version 12 Server Software. The upgrade file is found in the Workstation directory on the downloaded installation CD. Previous patches and this upgrade file can co-exist in the WS_Updates folder.

The Pearl Echo Administration Machine will automatically deliver the *upgrade* to Pearl Echo's workstation agent. After delivery, the self-updating agent will *upgrade* itself the next time the machine on which the workstation agent resides is restarted.

Version 6 or Earlier Workstation Upgrade

If you are upgrading your Version 6 or earlier workstations to Version 12, you will need to uninstall your previous version of the Pearl Echo Workstation Software before installing Pearl Echo 12 Workstation components. This can be accomplished by removing the software from the Workstation's Add/Remove Programs applet. **Because the Pearl Echo Workstation Software is a secure installation, it cannot be removed with a Group Policy Object.**

Uninstalling Pearl Echo

Pearl Echo provides a secure uninstaller for the Pearl Echo Workstation Agent. To reduce visibility, a Pearl Echo entry does not exist in the Workstation's Add Remove Programs window. The Pearl Echo Service is required to authenticate Pearl Echo Workstation uninstall requests. For this reason, the Pearl Echo Service must be running to securely uninstall workstation components. To run the Pearl Echo Service, set the Internet Management State to "ON" in the Pearl Echo Administration Console.

To Uninstall Pearl Echo Workstation Software

Option1: *Automated* Pearl Echo Workstation Software Uninstall

1. Run the Pearl Echo Administration Console.
2. From the Security Menu, select Manage Workstation Software.
3. Select the Remove tab.
4. Select the machine(s) targeted for software removal.
5. Enter your Pearl Echo password, domain credentials and follow the instructions as they appear on the screen.

Option2: *Manual* Pearl Echo Workstation Software Uninstall

1. From the workstation taskbar, click on Start and select Run.
2. Enter ec7unins.exe and select OK.
3. Enter your Pearl Echo password and follow the instructions as they appear on the screen.

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

Important Note: Because the Pearl Echo Workstation Software is a secure installation, it cannot be removed with Group Policy Object. Removing the software can only be accomplished from the Workstation as above or automated from the Echo Administration Console.

To Uninstall Pearl Echo Server Software

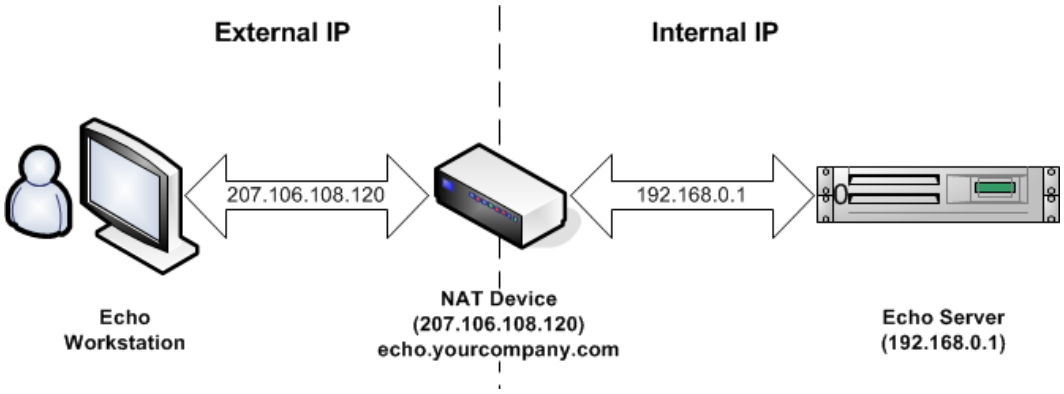
1. Run the Pearl Echo Administration Console.
2. From the Security Menu, select Set Security Status.
3. Turn the Pearl Echo Management State "OFF" and exit Pearl Echo.
4. Select the Windows Control Panel.
5. Select Add/Remove Programs.
6. From the Install/Uninstall tab, click on Pearl Echo.
7. Select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

Chapter 2

Advanced Installation

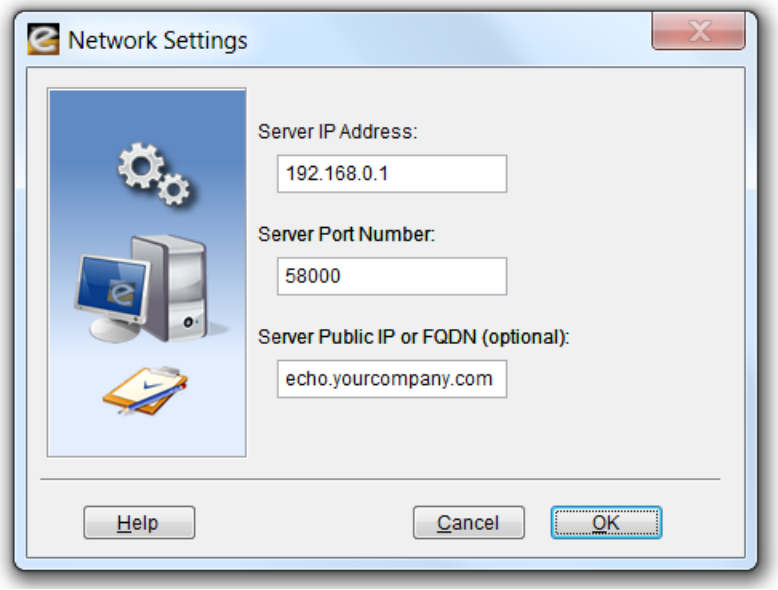
Network Address Translation

Pearl Echo 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 Pearl Echo Administration Machine and external or roaming Pearl Echo Workstations.



1. Start the Pearl Echo Administration Console.
2. From the Security Menu select Set Security Status.
3. Turn Pearl Echo 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 Pearl Echo Internet Management ON.

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

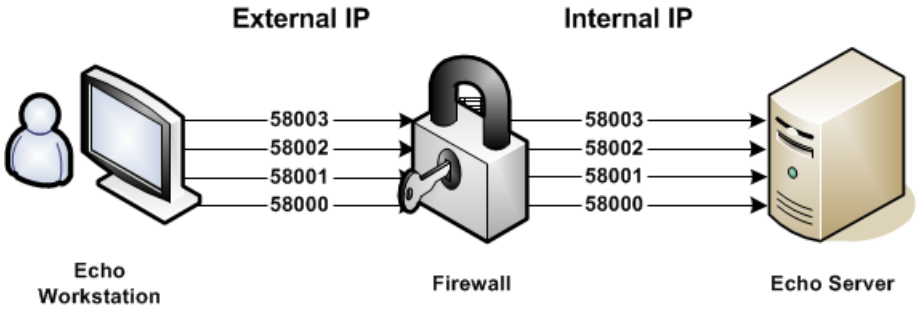


Firewall Settings

Pearl Echo's Mobility Monitor™ connects through a Firewall device utilizing a specified group of ports. Pearl Echo workstations establish an initial connection with the Pearl Echo Administration Machine 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 Pearl Echo Monitoring Service residing on the Echo Administration Machine communicates with the Pearl Echo Workstation Agent through a proprietary encoded protocol. Connections to the Pearl Echo Monitoring Service that don't communicate with the Pearl Echo protocol are dismissed.

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

Terminal/Citrix Server Setup

Pearl Echo is fully functional in a Terminal/Citrix Server environment. To operate in a Terminal/Citrix Server environment, install the Pearl Echo Server Software as described in Pearl Echo Server Software Installation, on any Windows platform. The Pearl Echo Server Software can be installed on a Domain Controller, a Domain Computer, a standalone machine or on the Terminal/Citrix Sever itself.

If using Citrix, correct Session Reliability issues as detailed in Knowledge Base Article 9 (www.pearlsw.com/support/kbase.html). Install the Pearl Echo Workstation Software on your Terminal/Citrix server as detailed above in *Pearl Echo Workstation Installation*. Once installed, each Terminal/Citrix desktop session will run its own instance of the Pearl Echo Workstation agent and **each user** will be fully managed by the specific settings you create in the Pearl Echo Administration Console.

Pearl Echo 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 Pearl Echo to Monitor Published Applications on Citrix and Windows Terminal Server" located at www.pearlsw.com/support.

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

Pearl Echo has been optimized for a server-centric multi-user environment. The Pearl Echo 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 Pearl Echo. This is done by selecting "Application Detection" in the Pearl Echo Administration Console's Options menu.

Workstation Setup with GPO

Pearl Echo supports automatically deploying the Pearl Echo Workstation installation from the Pearl Echo Administration Console as described in Chapter 1 of this User's Guide. The following describes the steps necessary to install the Pearl Echo Workstation Software using Microsoft's Group Policy Objects.

For additional details on using GPO to deploy software applications, *including trouble-shooting tips*, please refer to Microsoft's server and online documentation.

Preparation

☑ **For additional details on using GPO to deploy software applications, including trouble-shooting tips, please refer to Microsoft's server and online documentation.**

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

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 Pearl Echo Server Software installation.

1. Create a shared directory that contains all of the Pearl Echo 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 Administration Machine IP and Port that you entered during the Pearl Echo Server Software installation. In addition you will need to specify your Tamper Security configuration preference – low, medium or high. If you have users that will roam outside of your private network, you can optionally enter the public address (FWIP) of your Pearl Echo Administration Machine.

   Example:
   [Echo 12.0 settings]
   IP=192.168.0.1
   FWIP=echoservername.mycompany.com
   Port=58000
   Configuration=medium

Setting Group Policy

Software Installation works in conjunction with Group Policy and Active Directory. Installation is done on computer objects, not user objects. You can install to all computers in your domain or to specified computers in a

given organizational unit. In order to ensure that the Pearl Echo 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 that contains the computers 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 Pearl Echo Workstation installer file(e.g. *servername*\echows\Echo 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 Pearl Echo Workstation Software and configure the installation to access the Pearl Echo Administration Machine specified in *servset.ini*.

Important Note: Because the Pearl Echo Workstation Software is a secure installation, it cannot be removed with Group Policy Object. Removing the software can only be accomplished from the Workstation as above or automated from the Echo Administration Console.

Workstation Setup with 3rd Party Management Tools

Pearl Echo supports automatically deploying the Pearl Echo Workstation installation from the Pearl Echo Administration Console as described in Chapter 1 of this User's Guide. The following describes the steps necessary to install the Pearl Echo Workstation Software using third party software management tools that utilize the Windows Installer Service.

You will need to provide your software management tool with the Pearl Echo Workstation installation software, Pearl Echo Workstation.msi, as well as the installer "answer file", servset.ini.

1. Edit the file servset.ini to specify the Administration Machine IP and Port that you entered during the Pearl Echo Server Software installation. In addition you will need to specify your Tamper Security configuration preference – low, medium or high. If you have users that will roam outside of your private network, you can optionally enter the public address (FWIP) of your Pearl Echo Administration Machine.

   Example:
   [Echo 12.0 settings…]
   IP=192.168.0.1
   FWIP=echoservername.mycompany.com
   Port=58000
   Configuration=medium

Workstation Setup using Logon Scripts

Pearl Echo supports automatically deploying the Pearl Echo Workstation installation from the Pearl Echo Administration Console as described in Chapter 1 of this User's Guide. The following describes automating the Pearl Echo Workstation installation using Windows Logon Scripts. To silently deploy the Pearl Echo Workstation agent:

1. Create a shared directory that contains all of the Pearl Echo 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 Administration Machine IP and Port that you entered during the Pearl Echo Server Software installation. In addition you will need to specify your Tamper Security configuration preference – low, medium or high. If you have users that will roam outside of your private network, you can optionally enter the public address (FWIP) of your Pearl Echo Administration Machine.

   Example:
   [Echo 12.0 settings…]
   IP=192.168.0.1
   FWIP=echoservername.mycompany.com
   Port=58000
   Configuration=medium

At login, the workstation will need to run the command

msiexec.exe /i "<path>\Pearl Echo Workstation.msi" /q

where <path> is the file path to the new directory.

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
msiexec.exe /i "\\servername\echows\Pearl Echo Workstation.msi" /q
:vend
```

Note 1: The user under which the script is run must have Administrator privilege on the machine.

Note 2: The workstation installation modifies the machine's network settings. A forced reboot is included to ensure the stability of the workstation (processing running before and after installation will have different network settings until reboot). Though it is not recommended, you can suppress the forced reboot with the following command:

msiexec.exe /i "<path>\Pearl Echo Workstation.msi" /qn REBOOT=ReallySuppress

Integration with Microsoft SQL Server

Pearl Echo stores monitored Internet activity in its native Microsoft xBase database format. For installations with high volume monitoring loads and large storage requirements, Pearl Echo can be easily configured to store monitored Internet activity to a Microsoft SQL Server (version 2000 or later). The Pearl Echo 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 Pearl Echo Administration Console. To configure SQL Server:

☑ **Verify the Authentication Mode of the SQL server is "Mixed Mode (Windows Authentication and SQL Server Authentication)".**

Authentication Mode is found in SQL Server Management Studio: Right-click your server, and then click Properties and Security.

1. Copy the Pearl Echo database (echodb00000) files located in the Utilities directory of the product CD or installation folder to your SQL Server.
2. Create a *SQL Server Authenticated* user called echouser with password echopassword.
3. Attach to the Pearl Echo 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 and later: *After* attaching to the database, select Security->Users for the echodb00000 database, add the username "echouser" with login name "echouser", and assign **the role** db_owner.
4. Create a network share on the SQL Server named cache0000000000 and apply read and write permissions to the domain computer on which the Pearl Echo Server Software resides (verify the Share has read and write access under both the Share Permissions and NTFS Security tabs). This share will be the location where Echo will store additional cached content.

To configure the Pearl Echo Administration Machine to store monitored Internet activity to the Echo database on Microsoft SQL Server, enter the Pearl Echo 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 Pearl Echo should log activity.

NOTE: The above configuration requires that you have a licensed version of Microsoft SQL Server and the Pearl Echo SQL Server Module.

NOTE: Alternative SQL database products (e.g. SQL Server Express) may operate when substituted for a fully licensed version of Microsoft SQL Server, however Pearl Software is unable to support configurations other than its native Microsoft xBase or a fully licensed version of Microsoft SQL Server.

SQL Server Data Maintenance (Optional Sample)

Pearl Echo includes sample files to backup aged data* stored on your SQL Server primary Pearl Echo database to a backup database. To backup data stored from your primary Pearl Echo database, echodb00000:

Attach the Supplied Pearl Echo Backup Database

1. Copy the Pearl Echo backup database (echodbBackUp) files located in the Utilities directory of the product CD or installation folder to your SQL Server.
2. Attach to the Pearl Echo backup 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 and later: After attaching to the database, select Security->Users for the echodbBackUp database, add the username "echouser" with login name "echouser", and assign **the role** db_owner.

Schedule the Backup Job

1. Start the SQL Server Agent.
2. On the Jobs Folder, Right Click and select "New Job".
3. Enter **EchoBackup** as the job "Name".
4. Select "Steps" in the left hand window pane.
5. Click "New".
6. Enter **EchoBackupStep** as the "Step name".
7. In the Command Window, type **exec echodb00000.dbo.job_backup**
8. Click "OK".
9. Select Schedules in the left hand window pane.
10. Click "New".
11. Enter **EchoBackupSchedule** as the "Name".
12. Configure the schedule parameters as you require and click "OK".
13. Click "OK" to finalize the new scheduled job.

*The default value for aged data is 14 days. You can change this by modifying the stored procedure, dbo.job_Backup, located in echodb00000->Programmability->Stored Procedures.

1. Right click on dbo.job_Backup.
2. Select "Modify".
3. Modify the integer 14 in the line
    SET @start_log_date = dateadd(day,-**14**,getdate())
4. Select "Execute" from the Query tool bar

SQL Server Index Maintenance* (Optional Sample)

Pearl Echo includes sample files to tune fragmented index files in your SQL Server primary Pearl Echo database and your backup database. In addition, scripts are included to add index maintenance as scheduled jobs.

1. Start the SQL Server Agent.
2. *SQL Server 2000 or 2005*: Locate the index maintenance files in the Utilities\SQL Server Files\Index Maintenance**\2005** directory of the product CD or installation folder.
   SQL Server 2008 or later: Locate the index maintenance files in the Utilities\SQL Server Files\Index Maintenance**\2008** directory of the product CD or installation folder.
3. To *rebuild* the *primary* Pearl Echo indexes:
   a. Open the file **1-job_RebuildIndexes.sql**
   b. Execute the script
4. To *rebuild* the *backup* Pearl Echo indexes:
   a. Open the file **2-job_RebuildIndexes.sql**
   b. Execute the script
5. To *create* the *primary* Pearl Echo index job:
   a. Open the file **3-echodb00000_IndexMaintenance.sql**
   b. Execute the script
6. To *create* the *backup* Pearl Echo index job:
   a. Open the file **4-echodbbackup_IndexMaintenance.sql**
   b. Execute the script

By default, the index maintenance jobs will be scheduled to run each morning at 1:00 AM.

*Pearl Echo SQL Database Module 10.06.0006 or later must be attached prior to setting these index maintenance functions.

Chapter 3

Feature Overview

Pearl Echo tracks Internet activity by looking at content as it travels to and from a workstation computer via the computer's built in networking components. Pearl Echo adds security way-down-low to analyze network protocols so you have no worries about application choices, plug-in headaches or compatibility issues. This approach enables Pearl Echo to run reliably and silently in the background. The only indication that Pearl Echo is running is the display of an optional warning message or web page redirection on the Workstation that can be configured in the Pearl Echo Administration Console.

Pearl Echo's Administration Console allows you to customize how you monitor and manage access to Internet Web, Email, Chat, Instant Messaging, News and FTP. Controls can also be placed on non-Internet-specific applications like Word, Solitaire, iTunes etc. Access Control Profiles are used to set the access privileges of individual users, groups of users or computers. If you install Pearl Echo Server Software on a machine in a Windows Domain, User names, Group names and Computer names are gathered from your Active Directory database. This enables seamless administration by eliminating the need to maintain separate login accounts in the Pearl Echo Administration Console.

Monitoring Employee Internet Access

Pearl Echo 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. Pearl Echo's Quick Link™ feature allows the password holder to automatically link back to the actual Web and FTP sites the user visited, or to restore the content of incoming and outgoing postings, Email, Chat and Instant Messaging items. As a monitoring tool, Pearl Echo watches Internet activity and reports it back to you.

Managing Employee Internet Access

For managing Internet access, Pearl Echo 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 Pearl Echo Administration Console you can create Internet access Profiles in order to set varying levels of restrictions based on existing Windows User, Group and Computer definitions.

Pearl Echo can also be configured to block incoming and outgoing content based on an administrator-defined set of keywords and text patterns. 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.

Pearl Echo also supports bandwidth limits. With Pearl Echo you can allocate a daily allotment of bandwidth to users, groups or computers. Different levels of bandwidth can be assigned to different users and varied by Internet activity.

Pearl Echo 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 social media sites, to name a few.

In addition to the above modes of control, Pearl Echo allows you to control the daily time usage of non-Internet-specific applications. Specified programs can be completely blocked from running or allotted a specified number of minutes per day. Application blocking can be combined with Pearl Echo's powerful time controls to allow access to blocked applications during certain times of the day like lunch hours or after work hours.

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

Pearl Echo Security

Pearl Echo Administration Machine

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

Pearl Echo Workstation

Pearl Echo workstation files are protected by Pearl Echo's built in security. The workstation uninstall is password protected and file tampering will cause Internet access to be terminated if Security Tampering is set to Medium or High during the Pearl Echo Workstation installation. Additional security is provided via Windows ACL permissions.

Chapter 4

Using Pearl Echo

Signing In

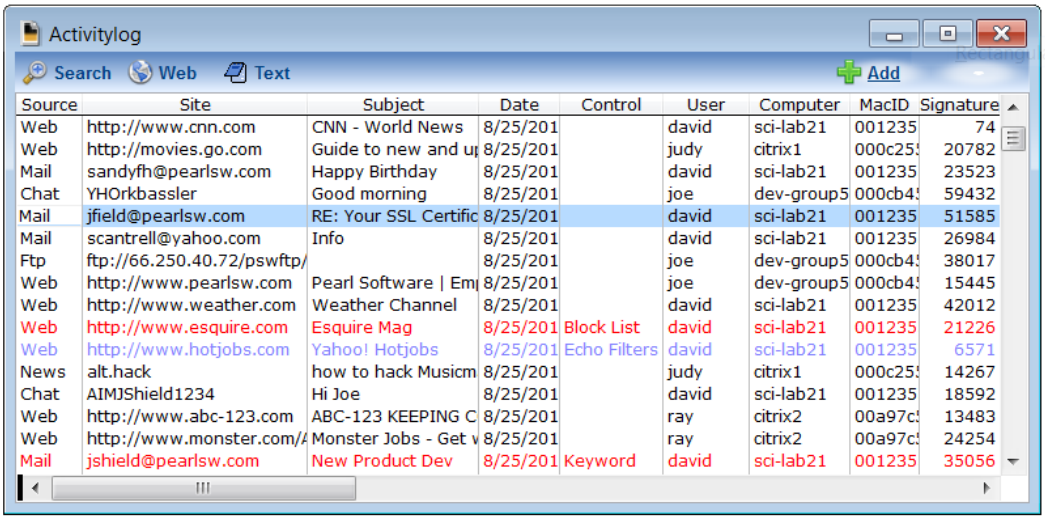
Each time you start the Pearl Echo Administration Console, you will be prompted for your login password.

After your password is confirmed, you will be presented with the Pearl Echo Navigator providing you access to the most common Pearl Echo features and administrative tasks including running reports as well as viewing the Pearl Echo Activity Log. While in the Pearl Echo Administration Console, you will have access to the most current copy of the Pearl Echo Activity Log. You can perform any file operation on your copy of the log without altering the integrity of the actual secure Pearl Echo log.

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

Viewing the Activity Log

The Pearl Echo Administration Console displays a copy of real-time monitored Internet activity in the Pearl Echo Activity Log Window. There are a number of ways to open and refresh the Pearl Echo Activity Log Window, the easiest being pressing the F5 function key or clicking the leftmost toolbar button.



Source	Site	Subject	Date	Control	User	Computer	MacID	Signature
Web	http://www.cnn.com	CNN - World News	8/25/201		david	sci-lab21	001235	74
Web	http://movies.go.com	Guide to new and u	8/25/201		judy	citrix1	000c25	20782
Mail	sandyfh@pearlsw.com	Happy Birthday	8/25/201		david	sci-lab21	001235	23523
Chat	YHOrkbassler	Good morning	8/25/201		joe	dev-group5	000cb4	59432
Mail	jfield@pearlsw.com	RE: Your SSL Certific	8/25/201		david	sci-lab21	001235	51585
Mail	scantrell@yahoo.com	Info	8/25/201		david	sci-lab21	001235	26984
Ftp	ftp://66.250.40.72/pswftp/		8/25/201		joe	dev-group5	000cb4	38017
Web	http://www.pearlsw.com	Pearl Software | Em	8/25/201		joe	dev-group5	000cb4	15445
Web	http://www.weather.com	Weather Channel	8/25/201		david	sci-lab21	001235	42012
Web	http://www.esquire.com	Esquire Mag	8/25/201	Block List	david	sci-lab21	001235	21226
Web	http://www.hotjobs.com	Yahoo! Hotjobs	8/25/201	Echo Filters	david	sci-lab21	001235	6571
News	alt.hack	how to hack Musicm	8/25/201		judy	citrix1	000c25	14267
Chat	AIMJShield1234	Hi Joe	8/25/201		david	sci-lab21	001235	18592
Web	http://www.abc-123.com	ABC-123 KEEPING C	8/25/201		ray	citrix2	00a97c	13483
Web	http://www.monster.com/	Monster Jobs - Get v	8/25/201		ray	citrix2	00a97c	24254
Mail	jshield@pearlsw.com	New Product Dev	8/25/201	Keyword	david	sci-lab21	001235	35056

The Pearl Echo 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. For Chat and IM, the first line of the conversation will be displayed. This entry will remain blank for Ftp.

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

Control: Displays the Pearl Echo Control that has restricted access to Internet content. Examples include Keywords, Ratings, Block List and Allow Lists, Time Limits and Bandwidth Limits.

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

Computer: The Windows 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 Pearl Echo Workstation on all data sent to the Pearl Echo Administration Machine. Individual check-sums are performed on the logged record data (Signature-r) as well as associated file attachments (Signature-f).

☑ **You can remotely access the Pearl Echo Administration Console through a built-in Terminal Server or Remote Desktop connection.**

Remote Administration

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

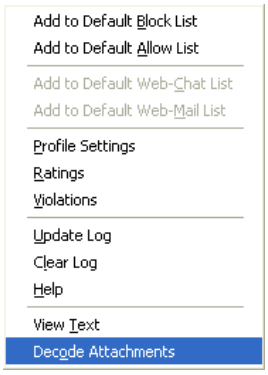
Viewing Logged Email, News, Chat & IM

Pearl Echo monitors and controls all Internet standard Email (Pop-3/SMTP/IMAP/GroupWise/Web-Mail), NNTP News, and Chat/Instant Messaging in Skype for Business. To view the content of incoming and outgoing Email, News, IM, and Chat:

1. Select the desired entry from the Pearl Echo 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

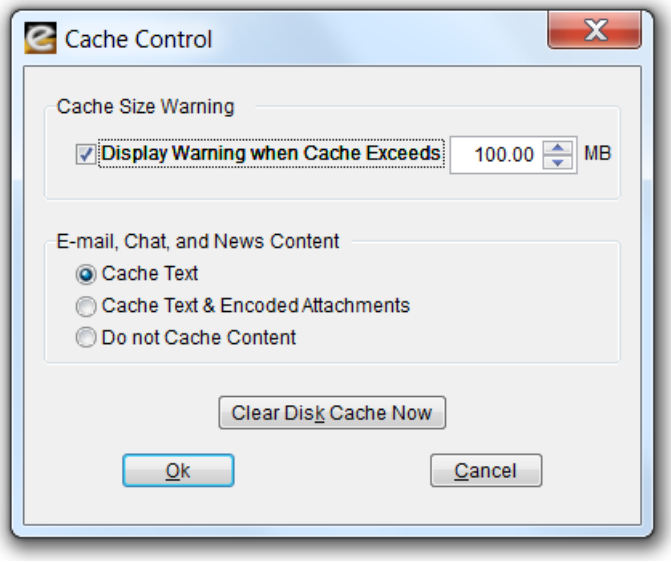
1. Right clicking on the desired entry from the Pearl Echo Log Window.
2. Selecting 'Decode Attachments' from the shortcut menu.



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 Pearl Echo Administration Console. Pearl Echo includes a built in attachment decoder in order for you to view captured documents, spread sheets, images, etc.

Quick-Link™ to Logged Sites

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

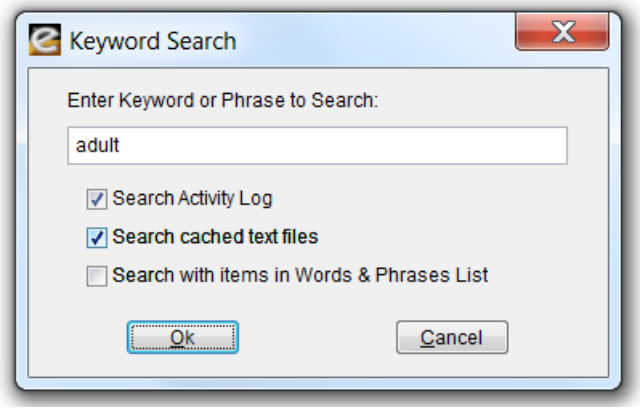
1. To browse all sites, click the Web button on the active Pearl Echo Log Window. This will automatically start your default web browser with links generated from your Pearl Echo Activity Log.
2. To browse an individual site, double-click your mouse button on the log entry that you want to visit. You can also choose "Go to URL" from the popup 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 Pearl Echo 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 Pearl Echo Administration Console provides the ability to quickly search through the entries displayed in the active Pearl Echo Log Window.

In order to identify specific information, searching 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 search the contents of the active Pearl Echo Log Window and associated text attachments. You can include the words in the current Profile's Words & Phrases List during a keyword search by selecting "Search with items in Words & Phrases List" in the keyword search screen.



Items in the Pearl Echo Log Window and any associated attachments that contain instances of the words or phrases in the Search 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 Pearl Echo secure 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 Pearl Echo log file.

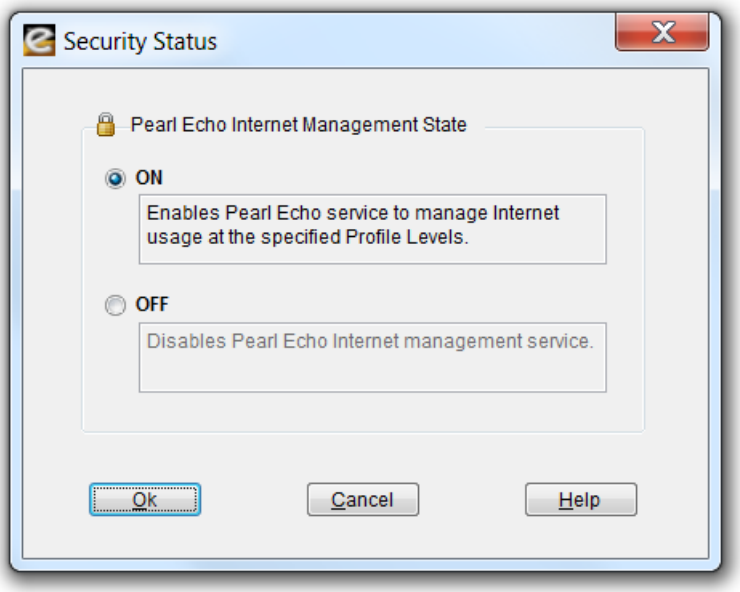
Data that you view in the Activity Log Window is a copy of the secure log. Modifying or deleting entries in any Activity Log Window has no effect on the actual secure log file.

Chapter 5

Setting Pearl Echo Security Levels

Turning Pearl Echo Management On and Off

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

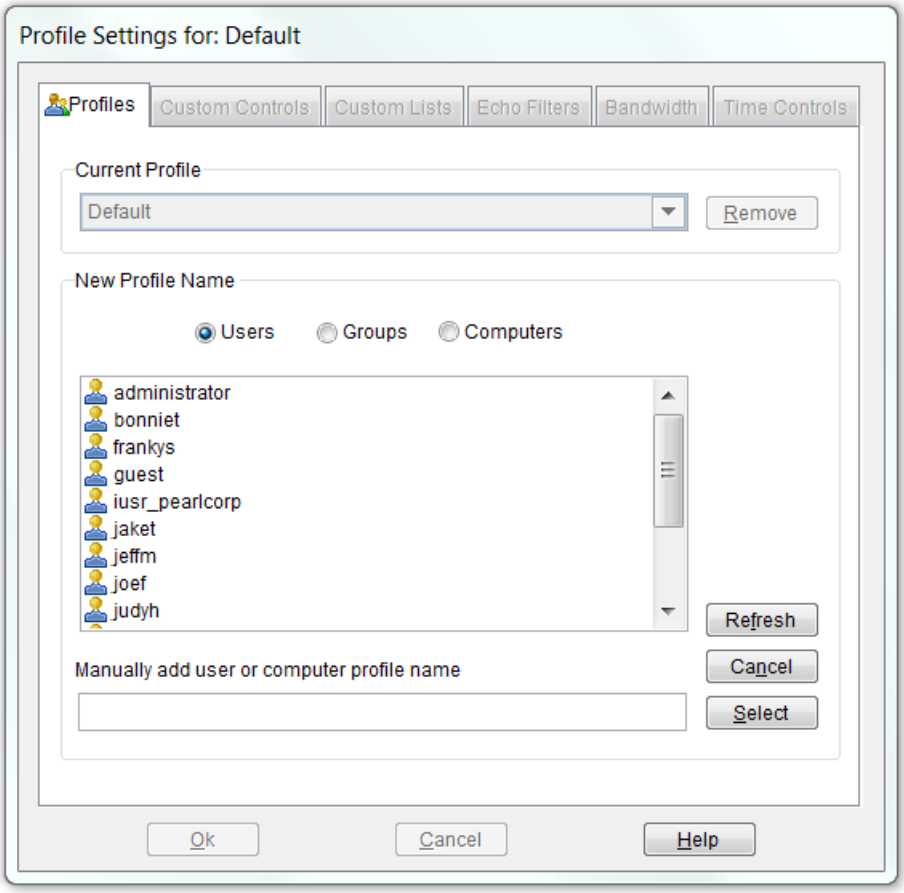


When the Pearl Echo Management Service is On, Pearl Echo is controlling Internet activity even after you exit the Pearl Echo Administration Console and log off of the Pearl Echo Administration Machine.

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

Administering Pearl Echo Profiles

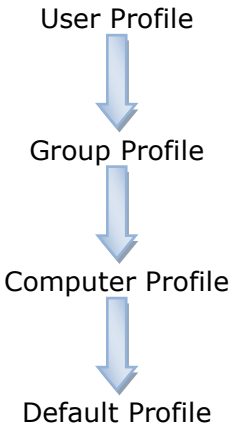
A Pearl Echo Profile is a group of settings you define to govern the Internet access permissions of your users. Initially, the Default Profile governs all users. Specific access privileges can be applied to individual users, groups of users or computers. Pearl Echo Profile names are based on your existing Windows User, Group and Computer names. You can Add, Remove and Select the Current Profile in the "Profile Settings" command of the Security menu.



The Pearl Echo Administration Console will access and display the available User, Group and Computer names from the Active Directory database when the Pearl Echo 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 Pearl Echo 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 Pearl Echo Server Software on a Windows server, the Pearl Echo Administration Console provides you with the ability to manually create the User and Computer names for Profiles that you would like to define.

When a managed User attempts to access the Internet, their activity is governed by one of your Profile's configuration settings. Pearl Echo first looks

for a matching User Profile. If no matching User Profile is found, Pearl Echo looks for a Group Profile to which the User belongs. If no matching Group Profiles are found, Pearl Echo looks for a Computer Profile based on the computer name being used. If no matching Computer Profiles are found, Pearl Echo uses the settings defined by your Pearl Echo Default Profile.

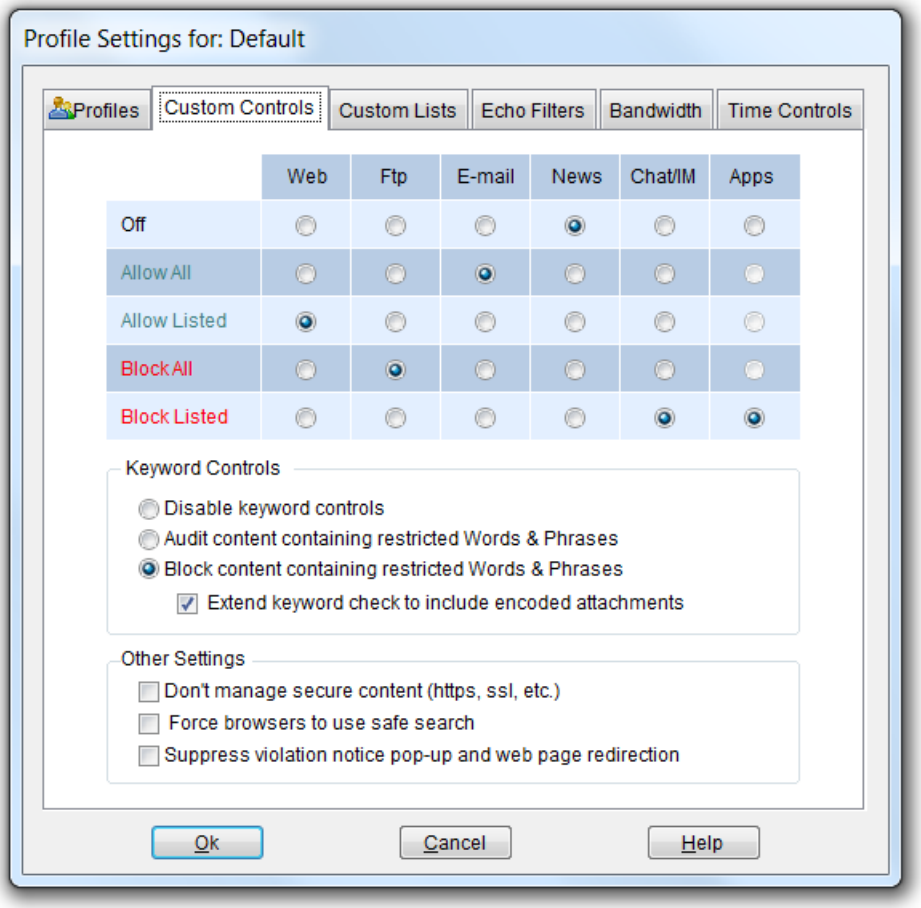


(Note: If a User belongs to multiple groups, Pearl Echo selects the first matching Group (alphabetically) to govern Internet access.)

For more information on this subject or to practice using this feature, please see the *Pearl Echo Tutorial* in the program's Help menu.

Setting Pearl Echo Control Levels

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



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

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

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

Block All: Select Block All to have Pearl Echo block the selected Profile's Internet activity. All activity is logged. In this example, all file uploads and downloads using FTP and Web browser programs will be blocked.

Block Listed: Select Block Listed to have Pearl Echo allow all Internet activity except for a list of objectionable sites defined in the selected Profile's Block Control lists. All Internet activity will be logged. In this example, Chat/IM access is blocked to only the chat groups and contacts listed in the selected Profile's Chat Block List. This example also shows that Applications listed in the selected Profile's Application Block List will be blocked after a configurable amount of daily usage.

Auditing Words & Phrases

You can have Pearl Echo identify when specific content is transmitted in any segment of the Internet by selecting "Audit content containing restricted Words & Phrases." With this option set, Pearl Echo will allow all Internet activity to proceed but will highlight transactions containing words, phrases or text patterns defined in the selected Profile's Words & Phrases Control list. The Words & Phrases List applies to all Internet content.

Blocking Content Based on Words & Phrases

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

For more information on this subject or to practice using this feature, please see the *Pearl Echo Tutorial* in the program's Help menu.

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," Pearl Echo will decode attachments in real-time and search the attachment for textual data that matches words, phrases or text patterns defined in the selected Profile's Words & Phrases Control list.

Secure Web Site Control[2]

Pearl Echo provides full visibility into encrypted data while it resides on the managed workstation (Note: Encrypted data remains encrypted as it travels to and from the managed workstation). The custom access rules that you assign to the current Profile are automatically applied to encrypted communications. If your organization dictates that you not manage encrypted data, you can have Pearl Echo ignore this content by selecting "Don't manage secure content (https, ssl, etc.)."

Safe Search

You can restrict the current Profile's web searches to use a search engine's "safe search" setting. Safe search is a search engine feature that acts as an automated filter to potentially offensive content. This setting is controlled by the user but can be overridden by Pearl Echo. Pearl Echo enforces the safe search feature of the following major search engines: Google, Bing and Yahoo.

Global Warning Message

You can prevent Pearl Echo from displaying your custom warning message for a specific Profile. This can be used if you have configured Pearl Echo to display a warning message to users or redirect a blocked web page but want to run Pearl Echo in silent mode for a particular user, group of users or computer.

Blocking Applications

You can block access to any application a user may run. This is accomplished by setting Apps to Block Listed in the current Profile's Custom Controls tab. The applications blocked are listed in the current Profile's Applications Block Control List. Applications can be set to be blocked immediately or after a period of daily usage. Users will be warned five minutes before an application is terminated due to expiration of an allocated allotment of time.

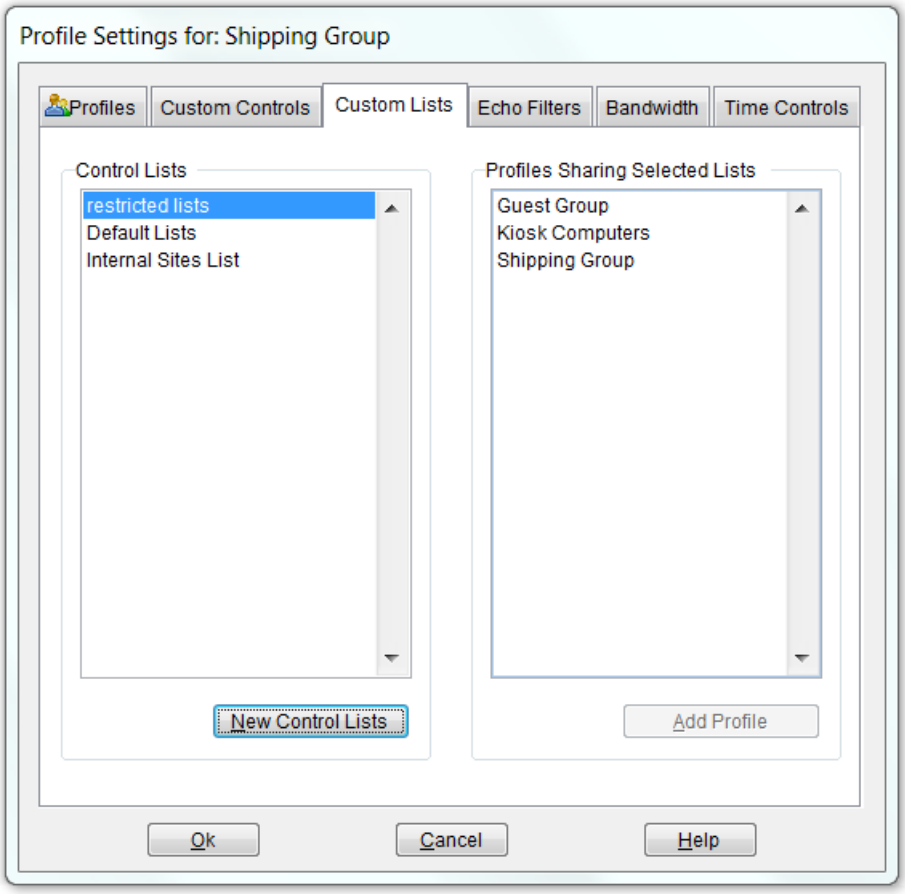
Applications are considered active when they consume CPU cycles. For example, Notepad, while minimized, is inactive - it uses no CPU cycles. If notepad.exe is in a user's Applications Block Control List, the user does not get charged for Notepad being open and minimized. iTunes, while minimized, is active - it uses CPU cycles. If itunes.exe is in a user's Applications Block Control List, the user does get charged for iTunes being open and minimized.

Application restrictions can be overridden with the Profile's Time Control settings. In addition, the default warning message can be suppressed by selecting, "Don't use global warning display settings" in the Profile's Custom Controls tab.

[2] Applies to Windows 7 and later.

Assigning Pearl Echo Control Lists

You can assign the Control Lists that a Profile uses in the Custom Lists tab of the Profile window. A Profile can share Control Lists with other Profiles in order to reduce administration. A Profile can also have its own set of custom Control Lists if you need to define specific access lists for specific Profiles. When a new Profile is created, it automatically shares the Default Profile's Control Lists.



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

1. Select the New Control Lists button in the Custom Lists tab of the Profile Window.
2. Assign a name to the new set of Control Lists.
3. Select OK.

The selected Profile will have a new set of blank Control Lists into which you can add or import entries.

To share an existing set of Control Lists with the selected Profile:

1. From the Profile tab, select the desired Profile in the Current Profile box.
2. Select the existing Control List name in the Custom Lists tab for the selected Profile.
3. Select the Add Profile button.

The list of Profiles that share the selected Control Lists appear in the adjacent display.

Using Pearl Echo Allow and Block Control Lists

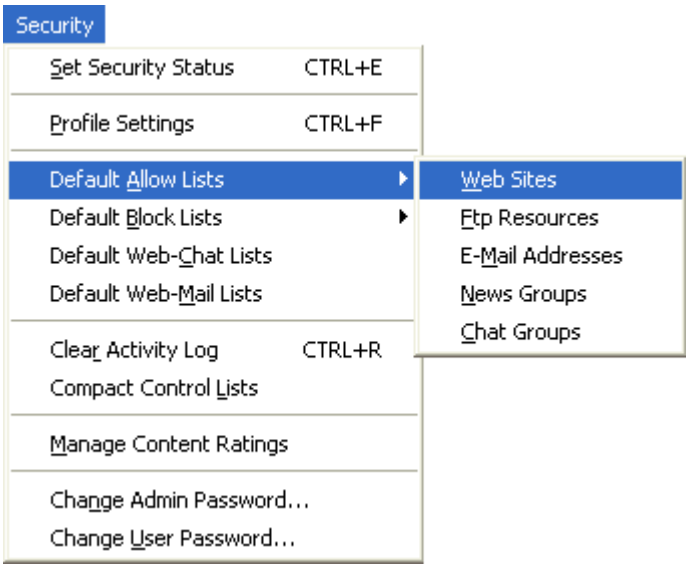
Pearl Echo's customizable Allow Lists are used to block all Internet activity except for a list of permissible Web Sites, Ftp Sites, Email contacts, News groups and Chat/IM groups. This is useful when a Profile's access needs to be limited to a defined list of web sites or Internet addresses.

Pearl Echo'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. Pearl Echo also allows you to block access to applications after they have been used for a specified period of time.

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

Manual Edit

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

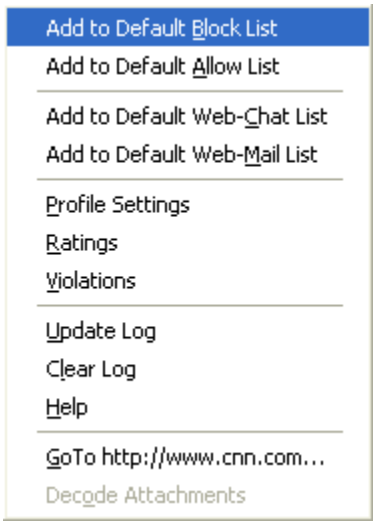


Within the selected Profile's Control List, you can add, remove and change entries. The format of the Control List entries must conform to Pearl Echo's

standard Control List syntax. For more information on Control List formats or to practice using this feature, please see the *Pearl Echo Tutorial* in the program's Help menu.

Automatic Add

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

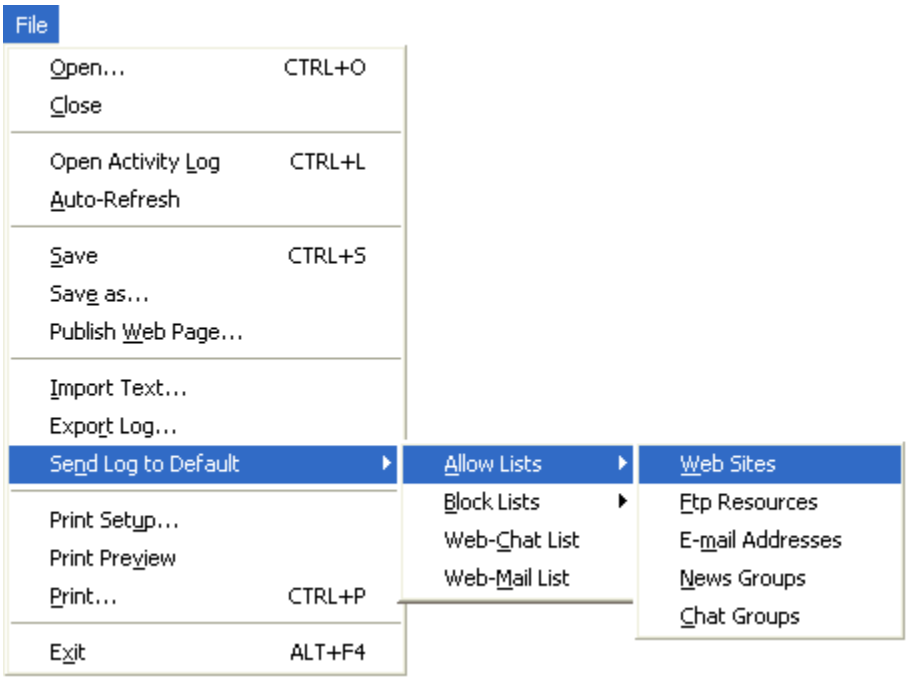


1. Right-Click your mouse button on the log entry that you want to add to the current Profile's Control List.
2. Select "Add to Block/Allow List".

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

Automatic Send

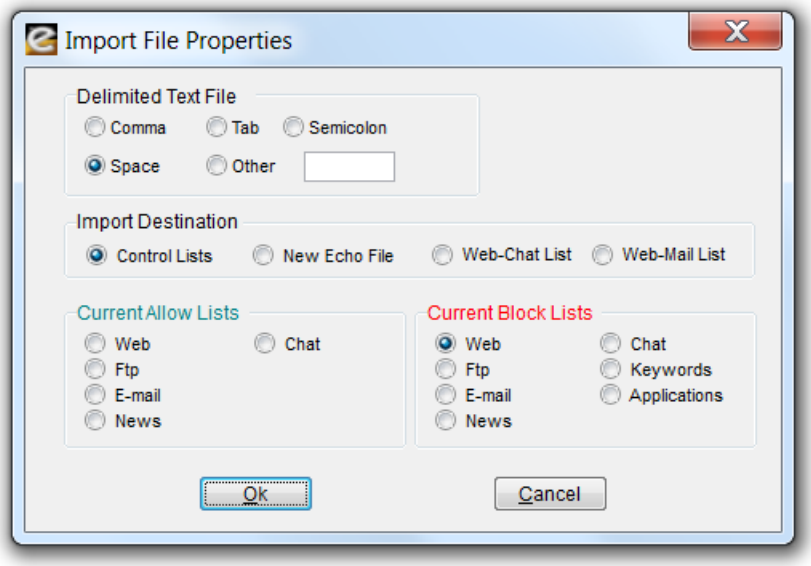
You can automatically send all entries from a sorted or unsorted activity log window to the current Profile's control list by selecting "Send Log to" from the file menu.



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 Pearl Echo Administration Console by selecting "Import Text" from the File menu. Use this feature when copying control lists or restoring lists from backup.



Formatting Control List Entries

Entries in Pearl Echo's Block and Allow Lists must contain valid address to insure proper functioning of the Control Lists.

The following demonstrates the format of entries in the site column of Pearl Echo's Control Lists:

Web Address:	Hypertext Transfer Protocol (HTTP)
Example:	http://www.abc.com/news
Secure Web:	Secure Hypertext Transfer Protocol (HTTPS)
Example:	https://www.facebook.com
Ftp Address:	File Transfer Protocol (FTP)
Example:	ftp://ftp.microcenter.com
E-mail Address:	Mail Transport Protocols (SMTP/POP-3/IMAP/GroupWise)
Example:	rsmith@usda.gov
News Group:	Network News Transfer Protocol (NNTP)
Example:	alt.binaries.pictures

Skype Chat: Skype for Business/Skype for Office 365 Protocol
Example: skypeUserName

The "*" Wildcard

The "*" Wildcard can be used in your Web, FTP and Email Allow and Block lists to simplify administration.

You can use one wild card per URL and it must:

1. Be the leftmost character in the URL
2. Completely occupy a base grouping in the URL

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 Yahoo! mail, add *@yahoo.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 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.

Proper use of the "*" wild card:

Example: http://*.abc.com/

Effect: Manages access to all servers at the domain abc.com (e.g. www.abc.com, www.machine1.abc.com, mail.abc.com, etc.)

Example: http://*.au

Effect: Manages access to all domains with an au (Australia) suffix.

Improper use of the * wild card:

Example: http://www.*.abc.com/

Reason: Wild card is not the leftmost character in the URL.

Example: http://www.a*c.com.com/

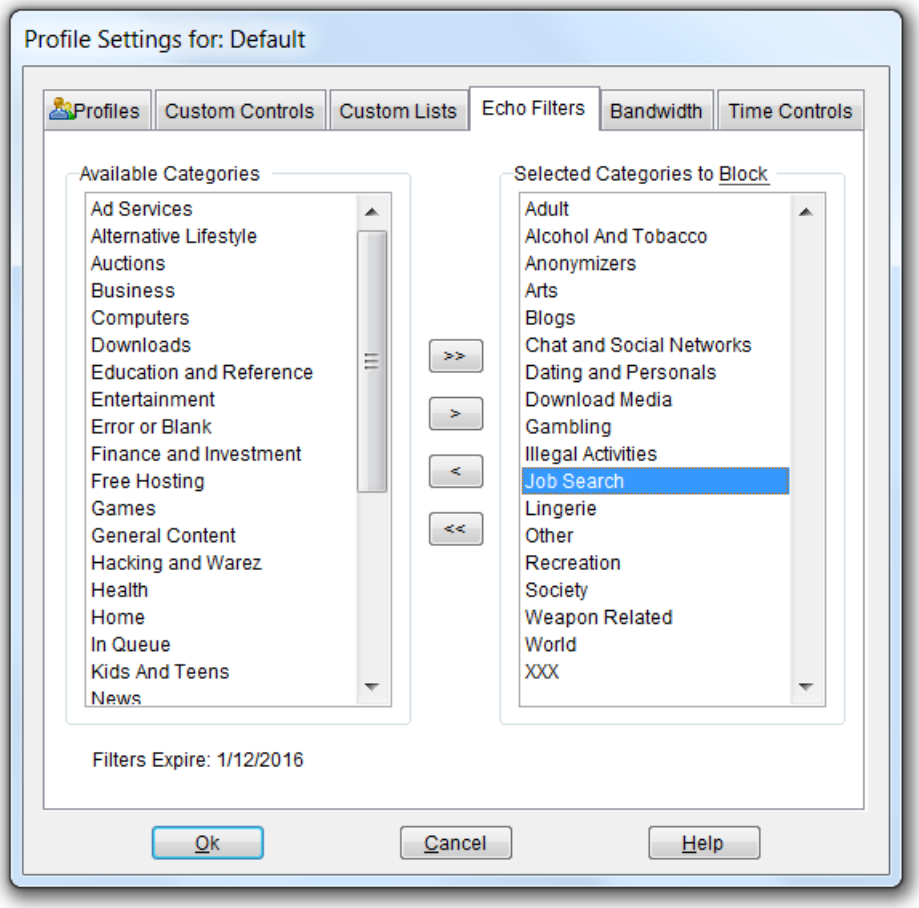
Reason: Wild card does not occupy a base grouping in the URL

The "*" wild card can also be used as any octet in an IP address (e.g. http://212.148.*.*).

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 Pearl Echo.

To block Web content based on categories, select the category to be blocked from the "Available Categories" list on the left and select the right arrow button to move it to the "Selected Categories to Block" list on the right. 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.Filters categories, add the "Other" category to the "Selected Categories to Block" list. To block Web Content that is not yet categorized by Echo.Filters, add the "In Queue" category to the "Selected Categories to Block" list. Uncategorized web sites are anonymously added to the Echo.Filters update database for future review.

When a URL is blocked due to a category selection, the control in the Pearl Echo Activity Log will display, "Echo Filters". You can right-click on an entry in the Pearl Echo Activity Log to display the category which caused the web site to be blocked.

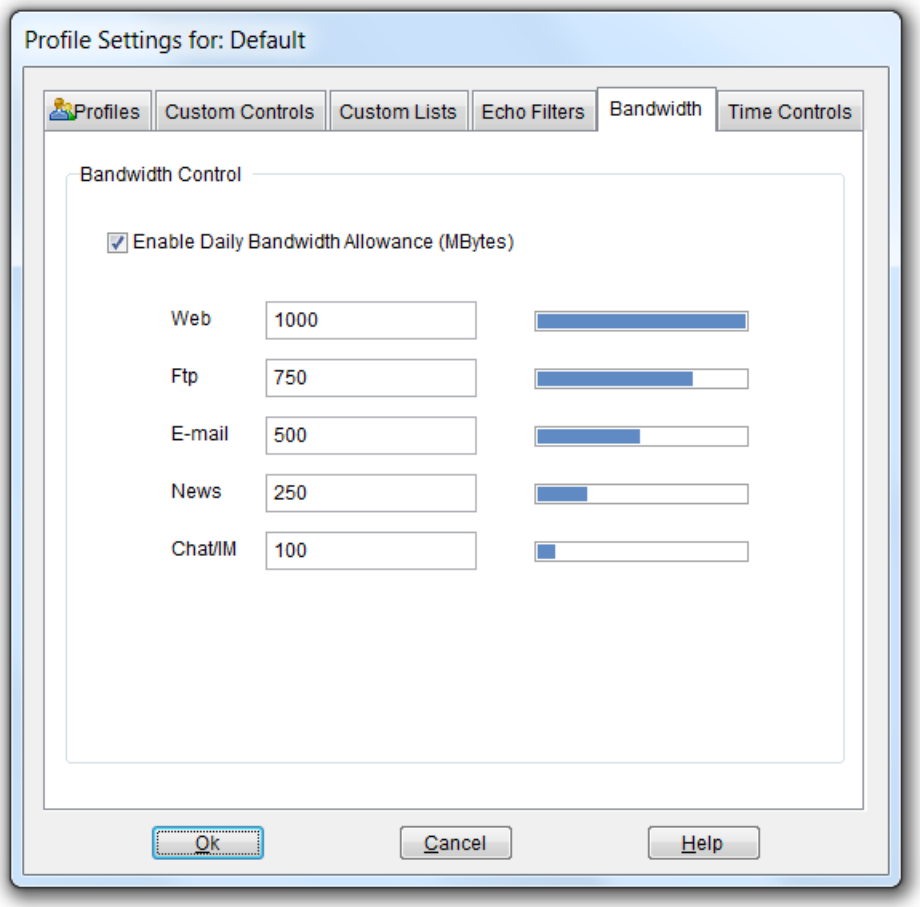
Echo.Filters Updates

Pearl Echo will automatically update the Echo.Filters database throughout the day. Sites that have not yet been categorized are automatically and anonymously submitted to our categorization queue for human review. The list of Echo.Filters categories can be found in Appendix B of this User's Guide.

When you enter the Pearl Echo 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, Echo.Filters category lookups will cease to function which may affect access privileges if so defined as well as any reports that contain category information.

Setting Bandwidth Restrictions

You can use Pearl Echo to allocate a daily allowance of bandwidth for a Profile. Bandwidth is specified in Megabytes (1 million bytes). Separate allocations can be set for each of Web, Ftp, E-mail, News and Chat/IM.



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

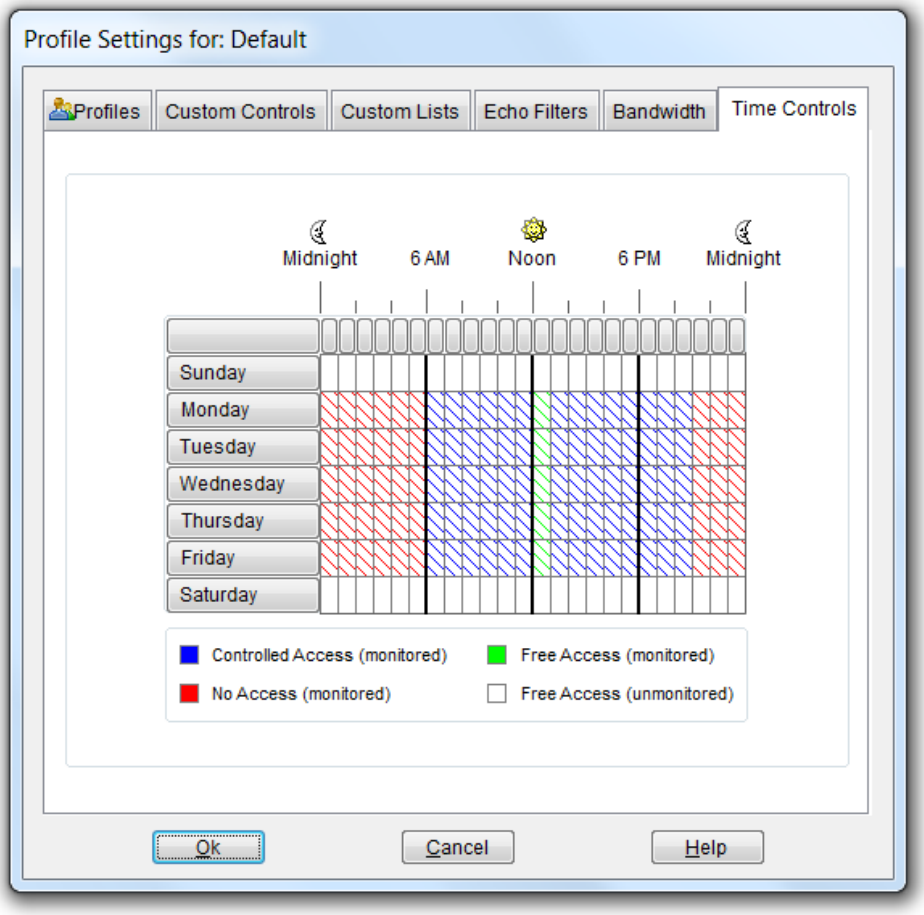
- 1 Gigabyte (1000 Megabytes) of daily Web activity
- 750 Megabytes of daily Ftp activity
- 500 Megabytes of daily E-mail activity
- 250 Megabytes of daily News activity
- 100 Megabytes of daily Chat/IM

Users will be warned when they are within five percent of their daily allotment. Bandwidth restrictions can be overridden with the Profile's Time Control and Allow List settings. In addition, the default warning message can be suppressed by selecting, "Don't use global warning display settings" in the Profile's Custom Controls tab.

If a bandwidth limit is reached in the middle of a communication, the communication will complete before the bandwidth restriction goes into effect.

Setting Time Restrictions

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



In the above example, the Default 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 from altering their workstation's clock. This is accomplished with Windows Group Policy.

Pearl Echo Time Controls take precedence over all other forms of access controls.

Using Keyword Blocking and Auditing

You can configure Pearl Echo to block or audit a Profile's inbound and outbound content containing words, phrases and text patterns 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 content.

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 for different words and phrases.

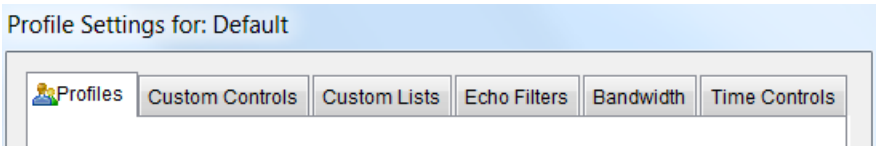
Pearl Echo can also be configured to block or audit content based on character patterns that you specify. You can use the pound character (#) to represent digits and the question mark character (?) to represent letters. For example, to block or audit any inbound and outbound transmission of social security numbers, you could use the following pattern in your Keyword Control List: ###-##-####. Patterns can be specified in the Default or Exact Method as described above.

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  *Pearl Echo Tutorial* in the program's Help menu.

Combining Security Features



A profile's Custom Controls, Echo.Filters, Bandwidth and Time Controls can all be used simultaneously and in concert with one another. For example, if a site is not contained in an Echo.Filters category, you can block the site by adding it to the Profile's Web Block Control list and setting the Custom Controls level to "Block Listed."

Similarly, you can add keyword controls for a profile to block content not specified in your Block Control Lists and not contained in the Echo.Filters database.

Entries in your Allow Control Lists will override blocks of content specified in all other controls with the exception of time controls. This is useful for allowing access to sites, e-mails, etc. that may occasionally present "iffy" material but do so in a manner that does not violate your Acceptable Use Policy. This is also useful to immediately unblock a site that you feel does not belong in an Echo.Filters category. Entries in your Allow Control Lists are in effect, even if Custom Controls are not explicitly set to "Allow Listed."

Time Controls work across all segments of the Internet and take precedence over all other forms of Pearl Echo Controls. For example, you can block specified applications like games and file sharing programs but override the block during lunch. Similarly, you can override Bandwidth blocks after normal working hours.

The following questions are frequently asked about combining security features:

Q. Do I need to set Web controls to 'Block Listed' for Echo.Filters to work?
A. No. Any filter category selected to be blocked will do so regardless of your Custom Control settings. The Echo.Filters module must be purchased and must not be expired in order to control and report web activity by content category.

Q. How do I allow access to only specific sites?
A. The quickest way to accomplish this is to monitor yourself browsing to the allowable sites. You will see the sites you accessed in the Pearl Echo Activity Log. Add the allowed sites to the Profiles Web Allow List. Do this by right clicking on the logged entries and selecting 'Add to Allow List.' Alternatively you can use the 'Automatic Send' feature combined with Pearl Echo's search capability to quickly add all logged sites to a Profile's Web Allow List. Once added to the Web Allow List, you should edit the list to use wild cards. For instance, sites like yahoo.com have multiple hosts that provide content: www.yahoo.com, finance.yahoo.com,

f11.yahoo.com, etc. You can quickly cover this scenario by using the '*' wildcard, like http://*.yahoo.com.

Q. Why do my new Profiles have entries in their Block and Allow Control Lists?

A. By design, new profiles inherent the Default Profile's control settings and *share* the Default Profile's Block and Allow Control lists. Once the new Profile is created, you can easily create a unique set of Allow and Block lists for the new profile. Do this by selecting 'New Control Lists' in the Custom Lists tab. The new Control Lists that you create can be specific to a single Profile or be shared amongst multiple profiles.

Chapter 6

Additional Pearl Echo Features & Settings

Refreshing the Pearl Echo Activity Log

☑ **Pressing the F5 key will refresh an open Pearl Echo Activity log.**

Pearl Echo captures Internet activity in real-time. The Pearl Echo Activity Log shows a copy of the most current Internet activity up to the moment that you open the Pearl Echo Activity Log. If Pearl Echo Workstations access the Internet while the Pearl Echo 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.

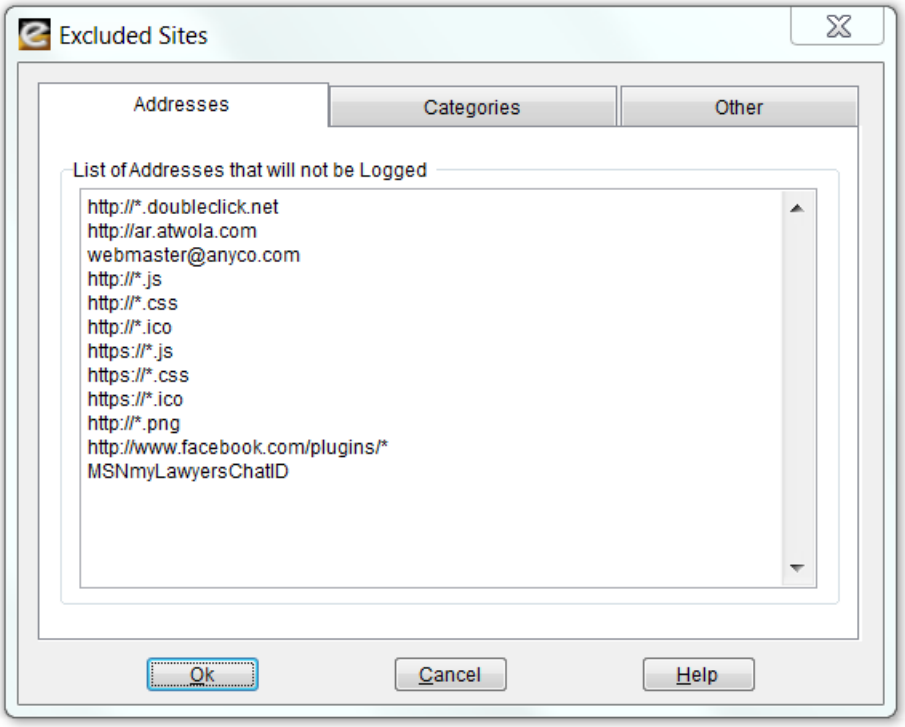
The Navigator, toolbar and shortcut menus can also be used to open a new copy of the Activity Log. Each time you open the Activity Log, a new window is created which can eventually clutter the Administration Console. Using the F5 key will refresh an open Activity Log.

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

Excluding Data from Being Saved in the Activity Log

Pearl Echo 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.

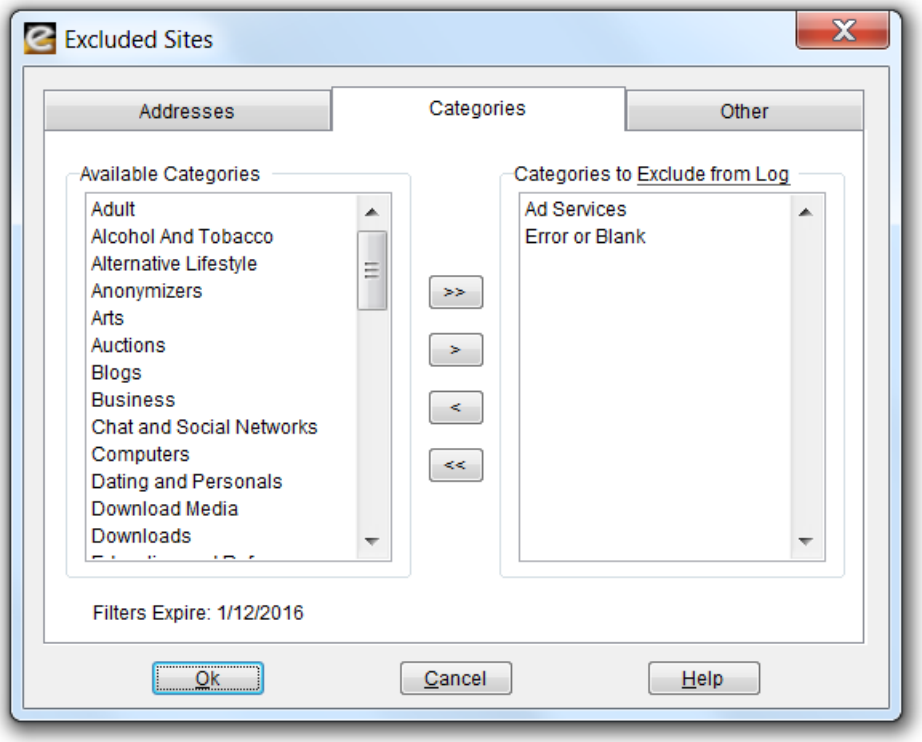
To add Internet addresses that should not be saved in the Pearl Echo Activity Log, select "Exclude Sites from Log" in the Pearl Echo Options menu.



Web addresses must contain the http:// or https:// 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 Pearl Echo Activity Log, the listed Internet addresses may still be controlled based on restrictions you may have defined in your Pearl Echo 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.

When using the Echo.Filters subscription, Pearl Echo will log Web activity based on content category. Internet addresses can also be excluded from being logged based on these categorized transactions.



Web activity may occur even when a computer is idle; web pages may refresh or applications like antivirus programs may automatically "phone home". You can suppress the logging of web activity that occurs when a machine is idle by selecting "Exclude all web site entries when computer is idle for *n* minutes."

The Pearl Echo Activity Log Database

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

Pearl Echo stores data in an open xBase database format. You do not need to install a third party RDBMS when using Pearl Echo with its native database. The Pearl Echo native database size limit is 2GB. For installations with high volume monitoring loads and large storage requirements, Pearl Echo can easily be configured to store monitored Internet activity to a Microsoft SQL Server.

Configuring Pearl Echo to store data to Microsoft SQL Server will enable reporting over larger data sets and expanded time frames. Report processing is done by the SQL Server engine so it is extremely efficient. Configuring Pearl Echo to store data to Microsoft SQL Server provides additional flexibility to your organization: Pearl Echo Administration Machines 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.

Integration with Microsoft SQL Server requires that you have both a licensed version of Microsoft SQL Server and the Pearl Echo SQL Server Module. Refer to the section "Integration with Microsoft SQL Server" in Chapter 2 of this User's Guide for additional instructions on this topic.

Modifying How Pearl Echo Displays Information

The Preferences command in the Options menu allows you to modify program features and appearance.

Screen Fonts

The screen font setting controls how text is displayed in the Pearl Echo Activty Log windows.

Violation Colors

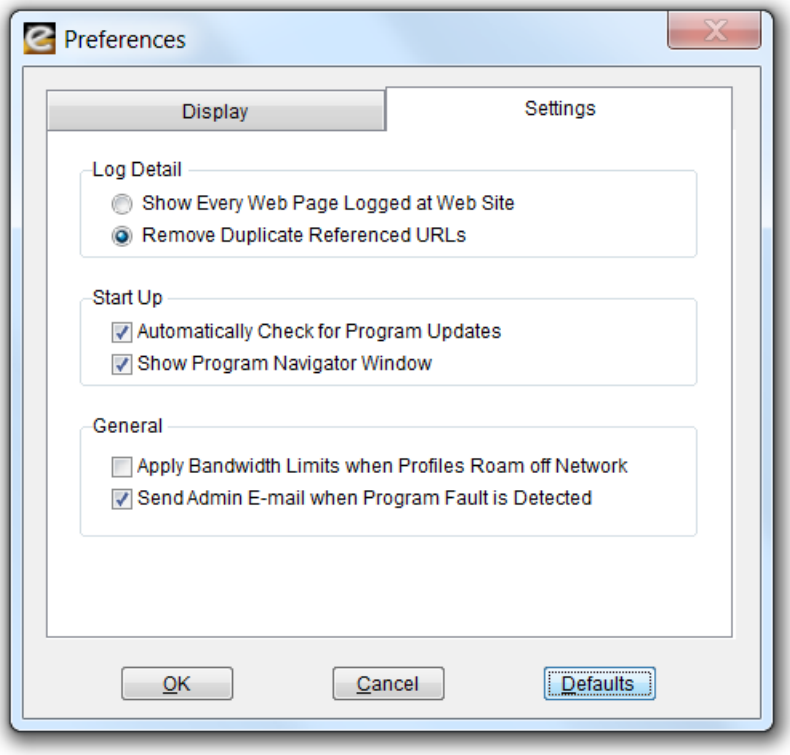
The violation colors are used to easily identify Activity Log entries where users have tried to access content that has been blocked or set to audit by your Pearl Echo control settings.

Log Window Columns

You can control how the Pearl Echo 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 Pearl Echo Workstation on all data sent to the Pearl Echo Server. Individual check-sums are performed on the logged record data (Signature-r) as well as associated file content and attachments (Signature-f).

Settings



Log Window Detail

You can control how Pearl Echo displays and stores Web site activity. Since accessing one web page may actually reference many other pages on the site or across the Internet, you can choose to compress this detail to one entry per page plus associated unique referenced URL requests. This also reduces the amount of data sent from the Pearl Echo Workstation to the Pearl Echo Administration Machine.

Startup

When you start the Pearl Echo Administration Console, the program can be set to automatically check for program updates. Updates are checked every two weeks. If an update is available, you will be notified how to access the program update.

The Startup box also lets you control if the Pearl Echo Program Navigator launches when you enter the Pearl Echo Administration Console.

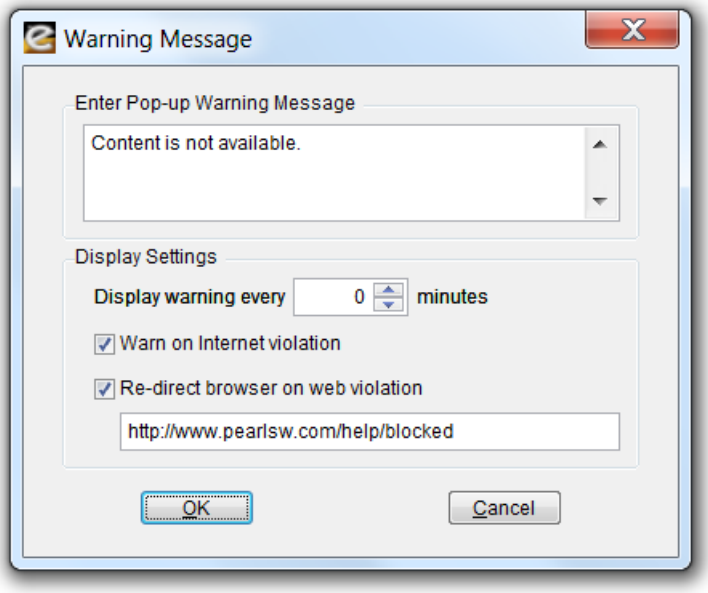
General

Bandwidth Controls can be disabled when users roam off your private network or work remotely. This is the default setting.

Pearl Echo monitors its own program functionality. If faults are detected, an email stating the problem along with possible solutions is emailed to the system administrator. The e-mail settings defined in the Pearl Echo Report Manager are used for communicating discovered faults.

Changing the Pearl Echo Warning Message

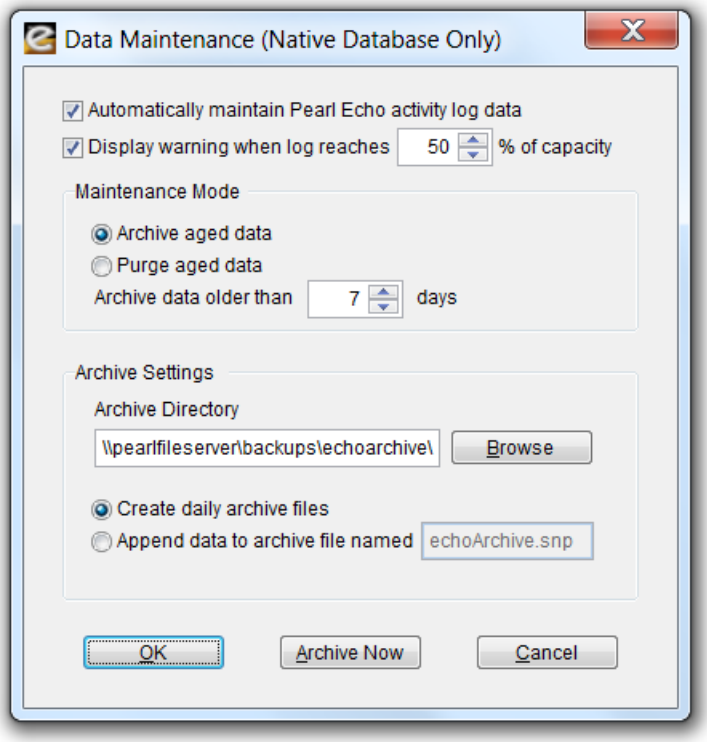
By default, Pearl Echo runs in stealth mode. You may inform users that Pearl Echo is monitoring their workstations. The message you display can be customized in the "Set Warning Message" command in the Options menu.



1. You may set Pearl Echo to periodically display your warning message by setting the display interval. To stop Pearl Echo from periodically displaying your popup warning message, set the warning interval to 0 minutes.
2. You may set Pearl Echo 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.
3. You may also have Pearl Echo redirect users' Web browsers to a web page that you specify. The web page can be Pearl Software's generic block page (www.pearlsoftware.com/help/blocked) or contain any URL with content that you design. The redirection URL will automatically be exempted from any block rules you may have in place. If you would prefer that the redirection URL not be logged in the Pearl Echo Activity Log, you may add the URL to the "Exclude Sites from Log" list located in the Options menu.

Data Maintenance

You can control the size of the native secure Pearl Echo Activity Log by archiving or purging your aged Pearl Echo.



☑ **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 Pearl Echo 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 (suggested) or appended to a single archive file (2GB limit). 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 Pearl Echo is configured to log data to Microsoft SQL Server, data maintenance is performed through procedures setup by the SQL Server DBA. Pearl Echo includes sample files and scripts to backup aged data stored on your SQL Server. Refer to the section "Integration with Microsoft SQL Server" in Chapter 2 of this User's Guide for additional instructions on this topic.

Compacting and Repairing Files

The "Compact/Repair 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.

This feature is also used when files become corrupt due to third party file modifications or abnormal system shutdowns.

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 Pearl Echo Administrator to view the Pearl Echo Activity Log and run reports. All Pearl Echo features are available when logged in with the User Level password except features that control Pearl Echo security configurations.

Managing Access to Data for Reporting

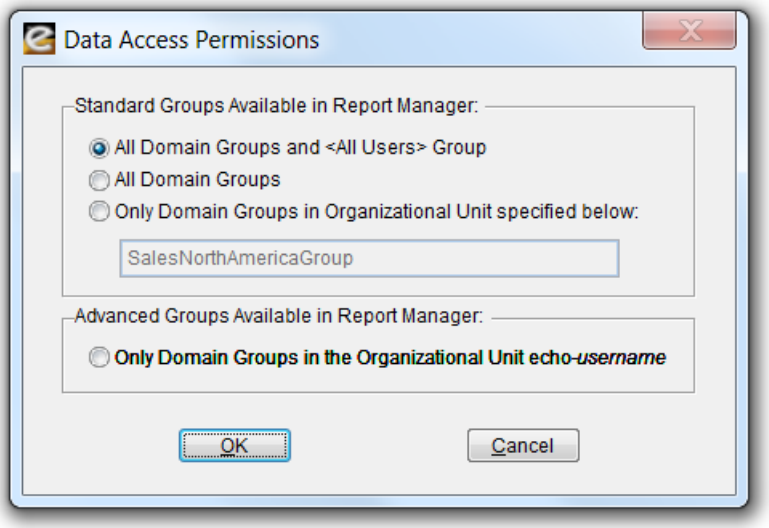
Pearl Echo provides you with the capability to distribute the Echo Administration Console configured as an Echo Reporting Console to other designated personnel in your enterprise. The Echo Reporting Console provides designated personnel access to end-user data based on Directory System Groups to which 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 Pearl Echo 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 Pearl Echo <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 Pearl Echo 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 Pearl Echo 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 (12/18/2015 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)

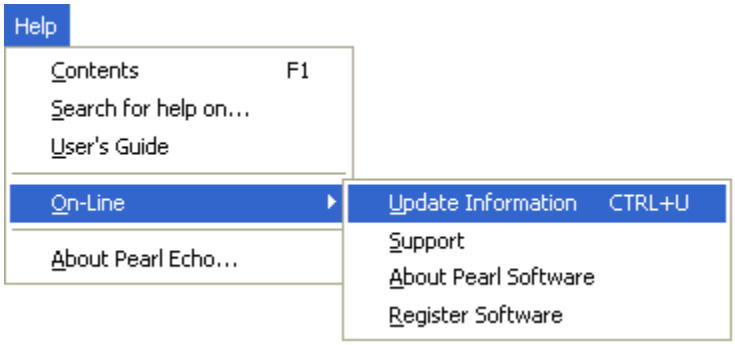
Use this feature when sharing lists or importing data from a backup.

Example: Mail,dlf@pearlsw.com,Confidential,05/08/2015 12:00 AM, Keyword,David,TestMachine,,,,NONE,0,,,

Exporting

You can export data from the Pearl Echo Administration Console with the "Export" command in the file menu. The exported file will be a delimited text or spread sheet format. If exporting to Excel, you can export a maximum of 65,535 rows. Use the exporting feature to copy Control Lists or for custom data analysis.

Performing Product Updates



Periodically, Pearl Echo 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 Pearl Echo, you will be automatically directed to Pearl Software's update Internet site.

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

Update Instructions

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

To automatically update your Pearl Echo Workstation agents, place the available Workstation patch in the WS_Updates folder found in the directory where you installed the Pearl Echo Server Software. The Pearl Echo service will automatically deliver the patch to Pearl Echo's self-updating agents. The self-updating agents will update themselves the next time the workstations are started.

Note: Pearl Echo *program* updates differ from Echo.Filters updates. Echo.Filters updates are done throughout the day with a current Echo.Filters subscription.

Activating Your Copy of Pearl Echo

If you are evaluating a demonstration version of Pearl Echo, you can activate your copy by purchasing a license from Pearl Software. To activate your copy of Pearl Echo, turn Pearl Echo Monitoring OFF from the Set Security Status menu, open the About dialog box in the Pearl Echo 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 Pearl Echo Administration Console contains an enterprise-class reporting module. You can use the Pearl Echo 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 modified and saved in Pearl Echo's native file format.

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

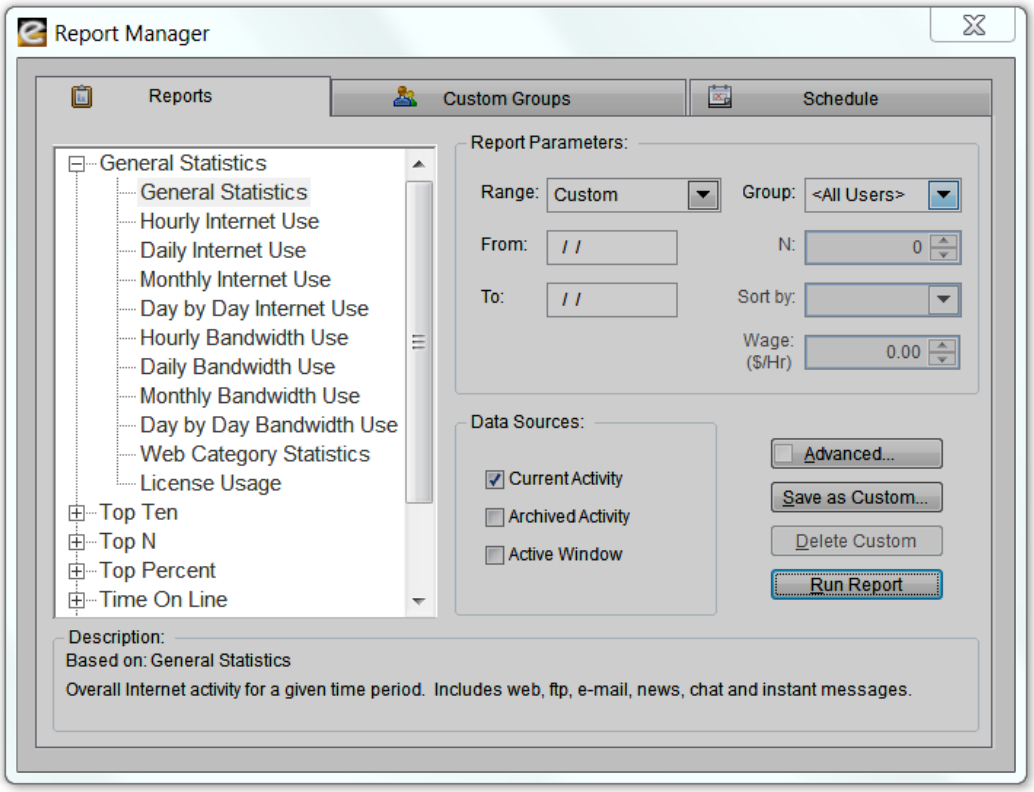
Reports can be scheduled to be published to any accessible directory including your organization's intranet so users can easily access reports through their web browser. In addition, the Pearl Echo Report Manager can automatically distribute reports via e-mail using Pearl Echo's built-in SMTP email service.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

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

Data is presented and analyzed by "impressions" which is the occurrences of each activity. A single Impression corresponds to a single entry in the Pearl Echo Activity Log.

Pearl Echo Reports

The Reports tab in the Pearl Echo 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 Pearl Echo license consumption. (Note: Real-time license consumption is displayed in the Navigator on the Administration Console's desktop.)

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 Pearl Echo 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 Pearl Echo 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 Pearl Echo Workstation agent.

Custom

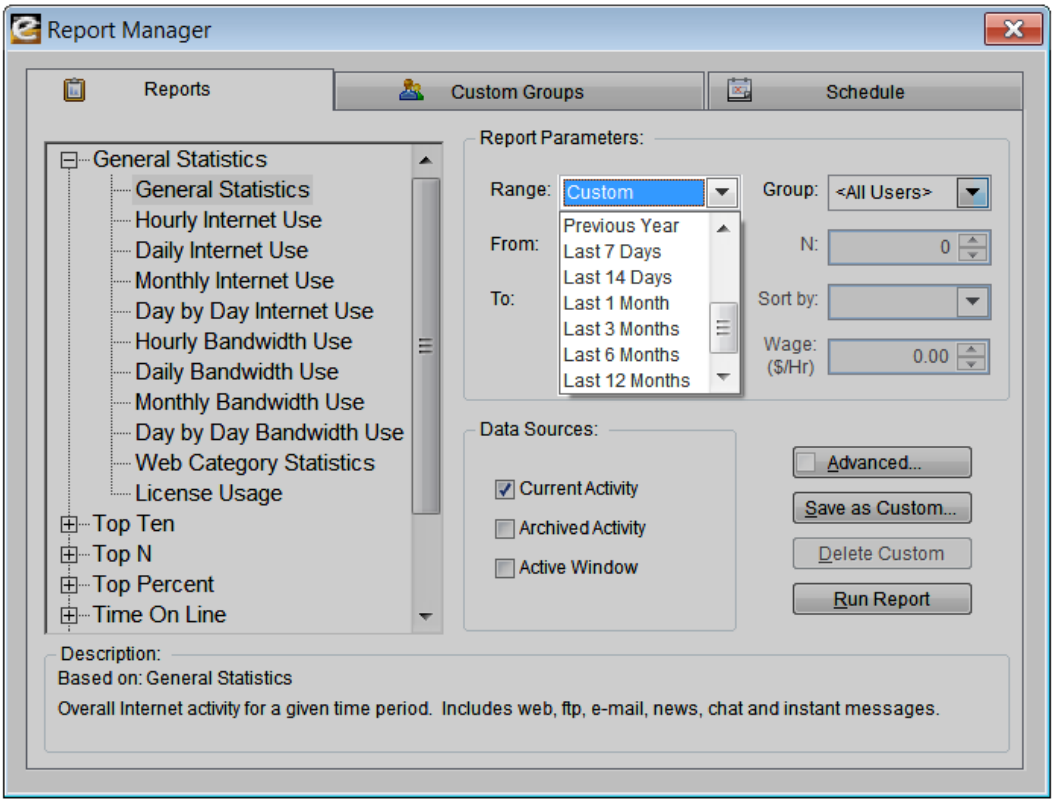
All reports can be customized and saved for future use. Your saved reports appear under the Custom Report section.

Categories

Many of the report sections above contain Category reports. Category reports are based on categorized web access available with Echo.Filters. The Echo.Filters category module must be purchased for Pearl Echo to categorize web site activity.

Date Range

The Pearl Echo 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.

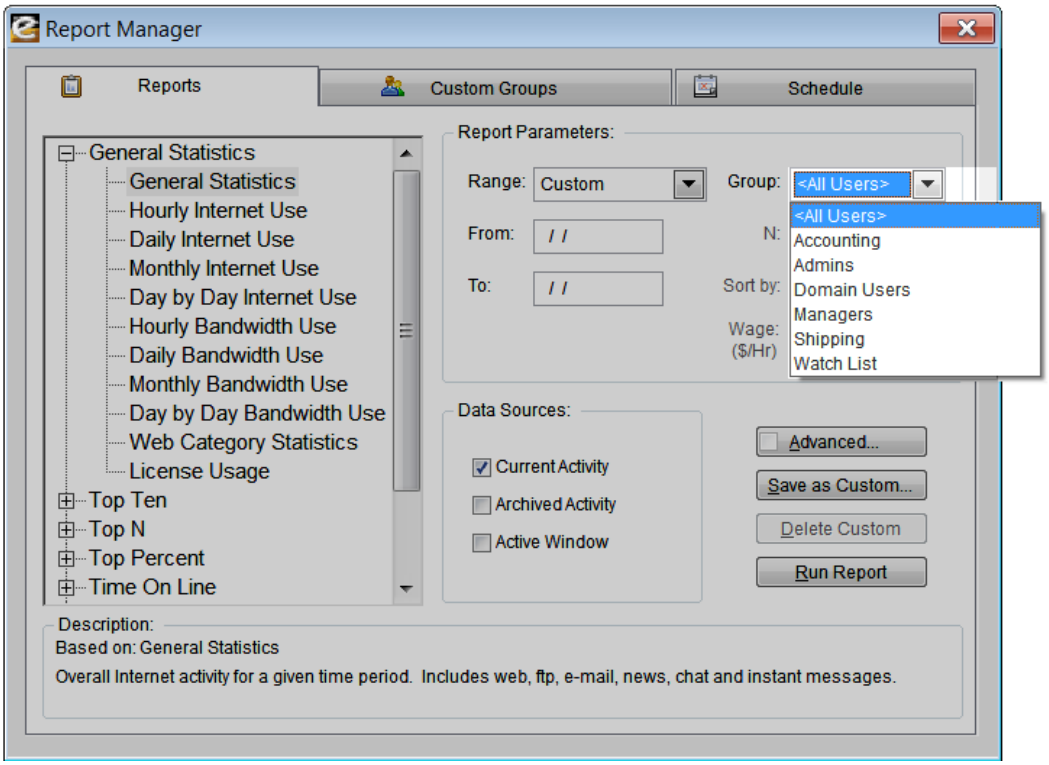
Custom

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

Groups

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

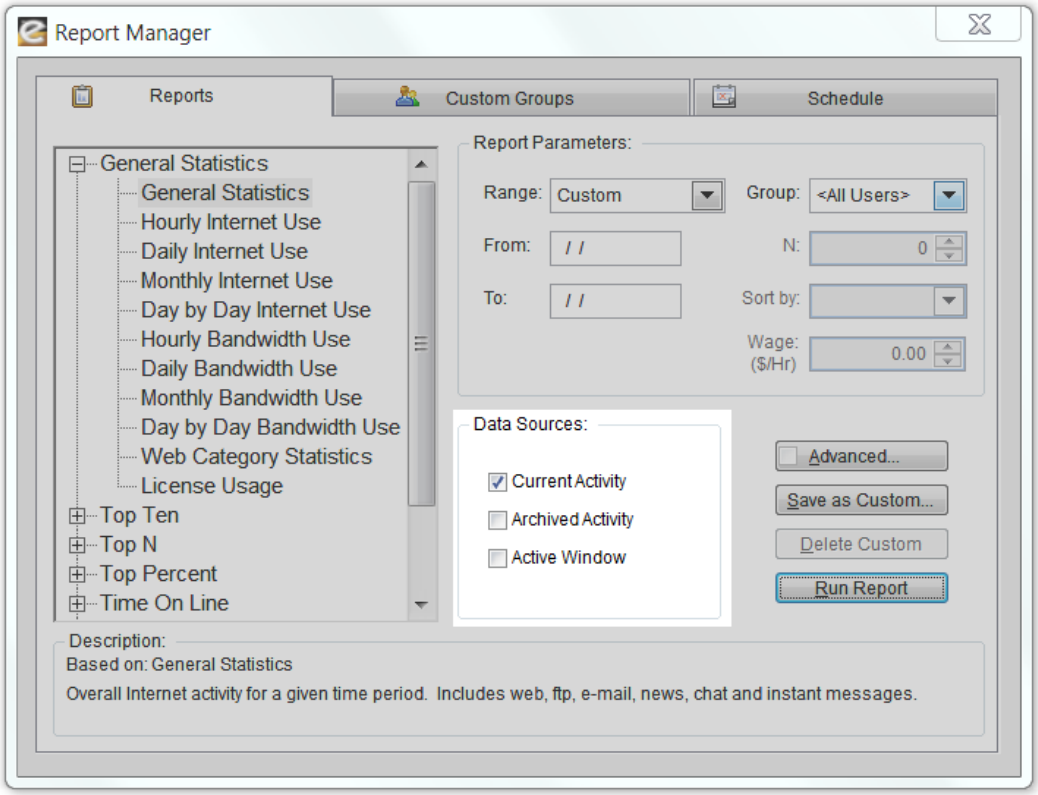
☑ **The Group dropdown includes your existing Windows Groups as well as custom groups you may choose to define in the Custom Groups tab in the Report Manager.**



By narrowing reports based on specific users, reports can be run for managers of a specific group, department or division. The groups displayed include your Active Directory groups (if available) as well as custom groups you define in the Report Manger Groups tab. Defining custom Report Groups is discussed in more detail later in this chapter.

Data Sources

The Pearl Echo 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* Pearl Echo Activity Log file. As the Pearl Echo Activity Log is dynamically changing and contains up-to-date data, this option is the most frequently used selection.

Archived Activity

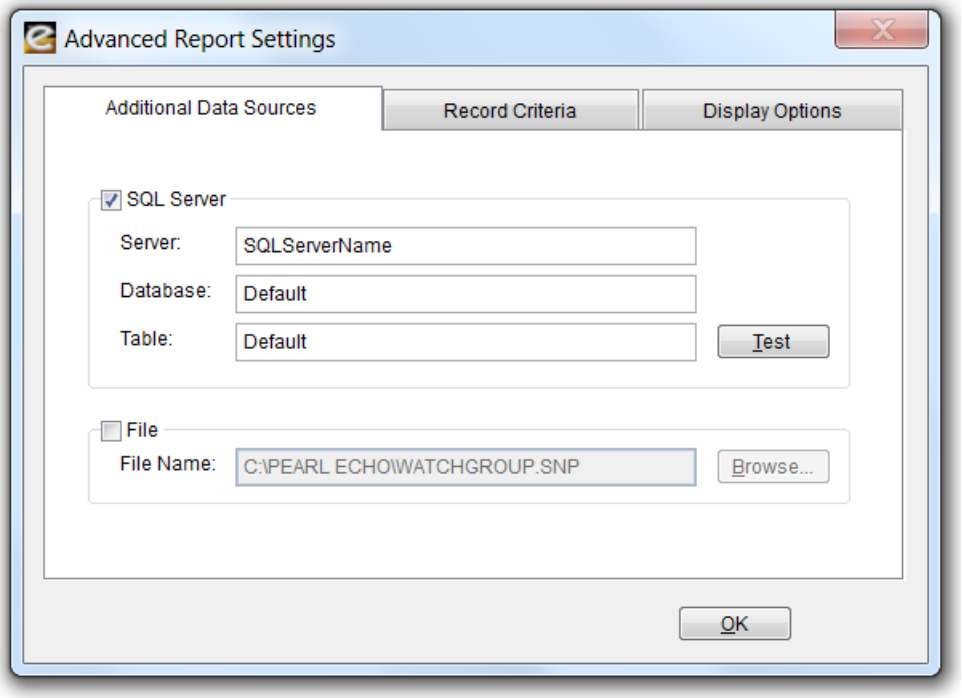
This option is used to report against aged data that you have specified to be stored in your Pearl Echo archive directory. The directory containing your archived data is specified in the "Data Maintenance" selection of the Options menu. The Pearl Echo Report Manager can run reports against archived data 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 Pearl Echo 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. Note: The active window should not be the Program Navigator window as this contains no activity data.

SQL Server

You can set the Pearl Echo 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 Pearl Echo 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 Pearl Echo 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 Pearl Echo's native xBase file format. Pearl Echo files

are created by saving filtered or sorted versions of the Pearl Echo Activity Log.

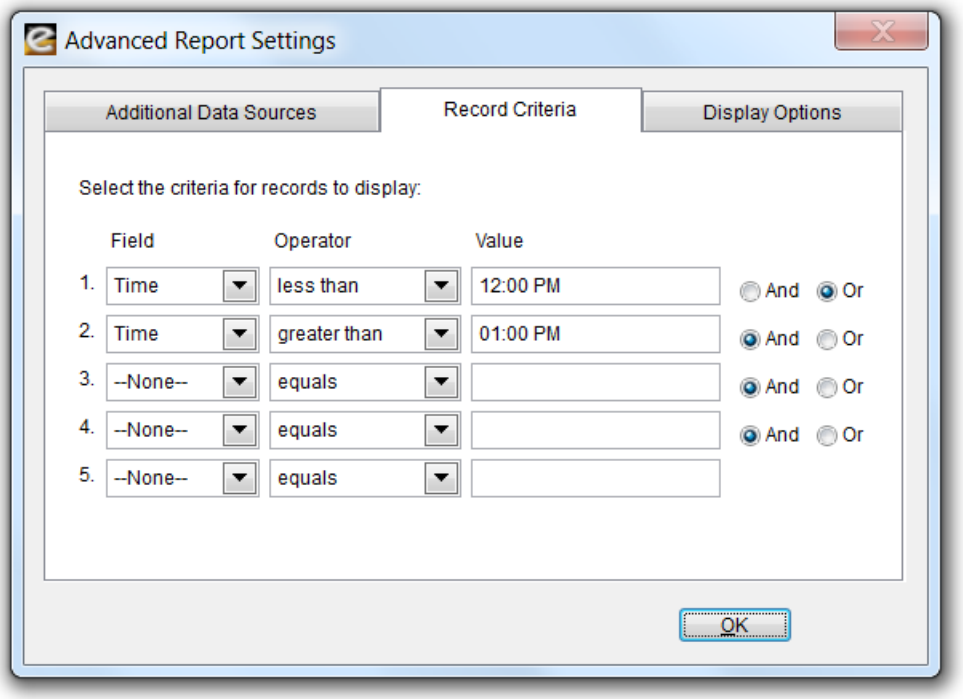
Advanced Settings

Record Criteria

You can limit the results displayed in your reports by specifying custom criteria in the Advanced Report Settings.

To enter record criteria:

1. Choose a field from the first drop-down list.
2. Choose an operator. For descriptions of each operator, see Criteria Operators below.
3. In the third field, enter the value to match.
4. To combine additional criteria select the logical "And" or "Or" condition and enter additional criteria on a subsequent line.



Use the following tips for entering record criteria:

- Create one condition per line.
- To limit records to a group of users, use the Group drop down box on the Report Manager's Reports tab.
- To limit records to a range of dates, use the Range drop down box on the Report Manager's Reports tab.
- To create a filter that includes more than one value, enter your search terms on multiple lines and join the criteria with the logical "And" or "Or" option. For example, to report on activity from only two

computers, machine1 or machine2, enter the first criteria "Computer equals machine1 *or*" followed by the second criteria "Computer equals machine2".

- If entering a time value, use the 12-hour (e.g. 01:00 PM) or 24-hour (e.g. 13:00) time format. For example, to report on Internet activity that excludes web browsing during the lunch hour, set the criteria "Time less then 12:00 PM Or" followed by the second criteria "Time greater then 1:00 PM".
- To limit report results to records that do not contain blank or "null" values for a particular field, choose the field and the "not equal to" operator; leave the third field blank. For example, to limit records to only those with violations, set the criteria to "Control not equal to ".
- Use the "contains" operator to broaden your results. For example, to run a report showing the time spent at a specific *domain* such as espn.com, add the criteria "Site *contains* espn.com". This will return all *pages* in the domain and also eliminate the need to use the http:// and hostname prefixes.

You can use the following operators when entering conditions for search criteria:

Operator	Use
equals	Use for an exact match; for example, "Site equals http://www.pearlsoftware.com"
not equal	Shows records that don't have the value you enter. This is especially useful for eliminating empty fields; for example, "Control not equal to <blank>".
less than	Use for results that are less than the value you enter; for example, "User less than n" returns records where user names are alphabetically in the range "a" through and including "m".
greater than	Use when you want results that exceed the value you enter; for example, "Time greater than 7:30 PM" returns activity that begins at 7:31 PM.
less or equal	Use for results that match or are less than the value you enter.
greater or equal	Use for results that match or exceed the value you enter.
contains	Use for fields that include your search string but might also include other information. For example, "Subject contains California" would find California Travel, California Pro Shop, and Surf California.
does not contain	Eliminates records that do not contain the value you enter; for example, "site does not contain @mycompany.com" eliminates inter-company mail from results.

Display Options

The Pearl Echo Report Manager allows you to save and e-mail reports in a wide variety of file formats including Crystal Reports format for interactive reporting and drill down. For instances where report recipients do not have a Crystal Report viewer, you can specify that all data visible in the drill down pages of the report be visible on the top summary pages. You can accomplish this by selecting "Include details from drill down pages with top summary report" in the Display Options tab found under Advanced Settings. Note: A free Crystal Report viewer is available in the Utilities directory of the Pearl Echo CD.

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 Pearl Echo Report Scheduler do not use this MAPI interface.

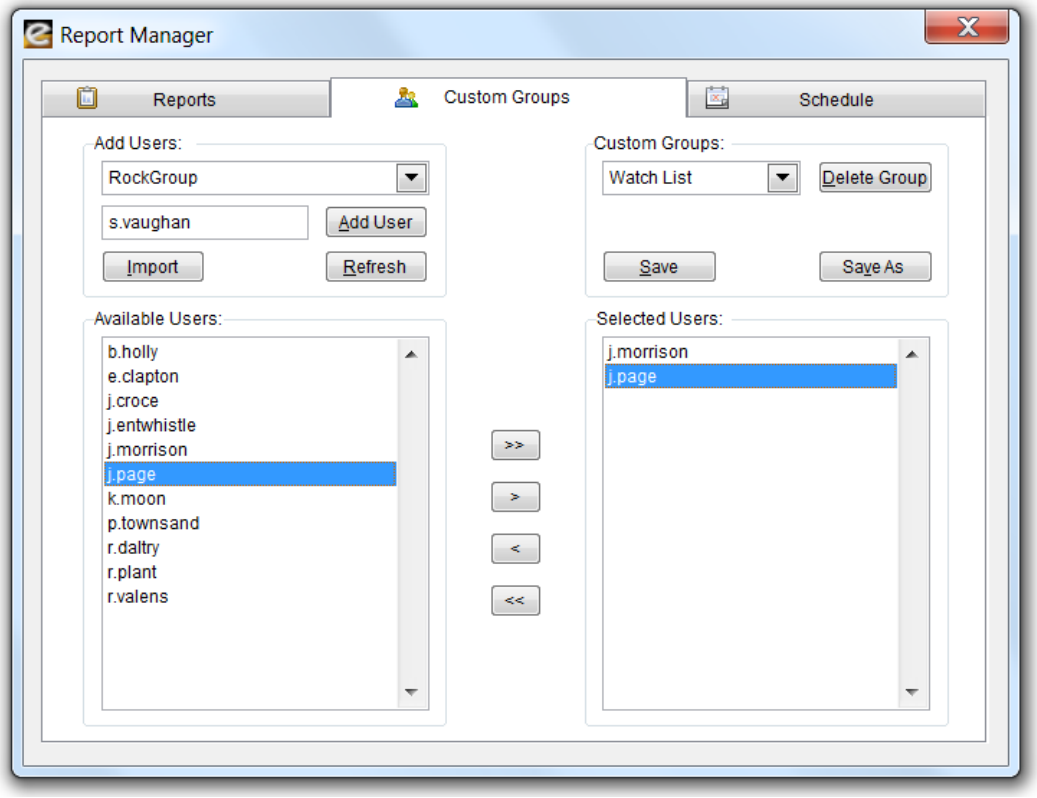
Pearl Echo Custom Report Groups

The group of users included in a report is selected on the Reports tab in the Pearl Echo Report Manager. In addition to your existing Windows Groups, you may define Custom Groups against which your reports may be run. Creating Custom Report Groups and defining users that belong to a Custom Report Group is done in the Groups tab in the Pearl Echo Report Manager. You may create a Custom Report Group from scratch or begin with the users in an existing Windows Group.

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.



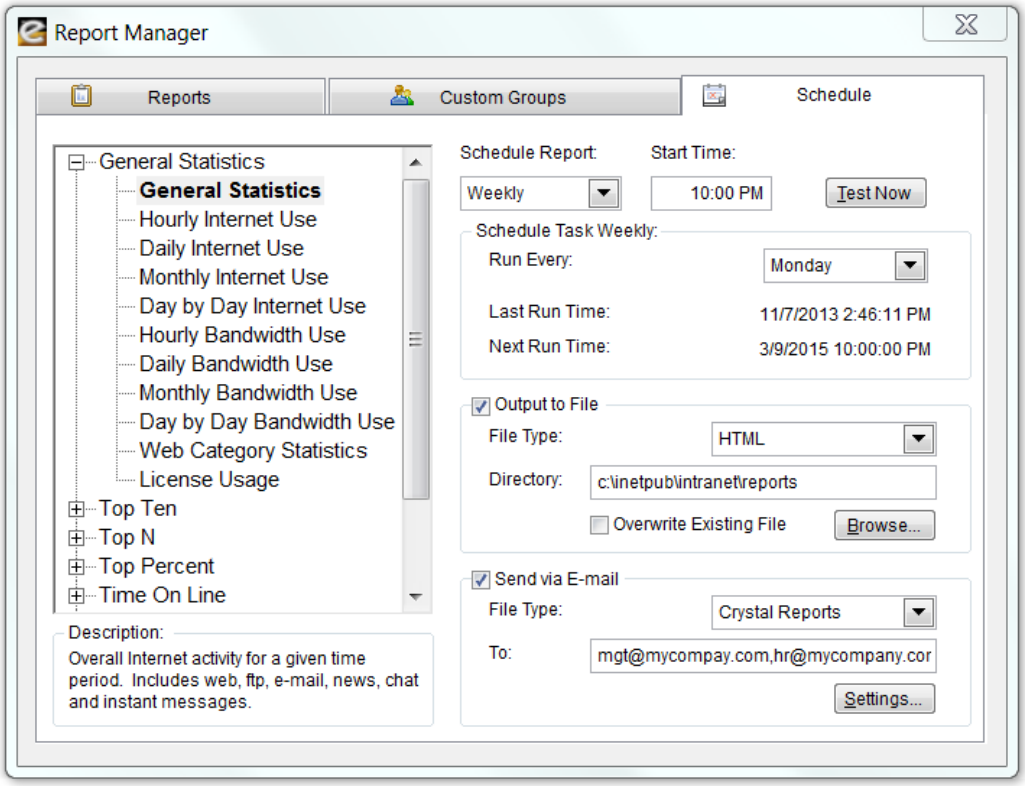
Lastly, you can manually add users to the Available Users list by typing a user name in the name box and selecting the Add User button. To delete a name from the Name list, select the name and then select the delete key.

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 Pearl Echo 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 Pearl Echo Administration Machine or network share. Pearl Echo 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 the most dynamic report experience for users.

By saving scheduled reports to a shared location, users can conveniently access Pearl Echo 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.

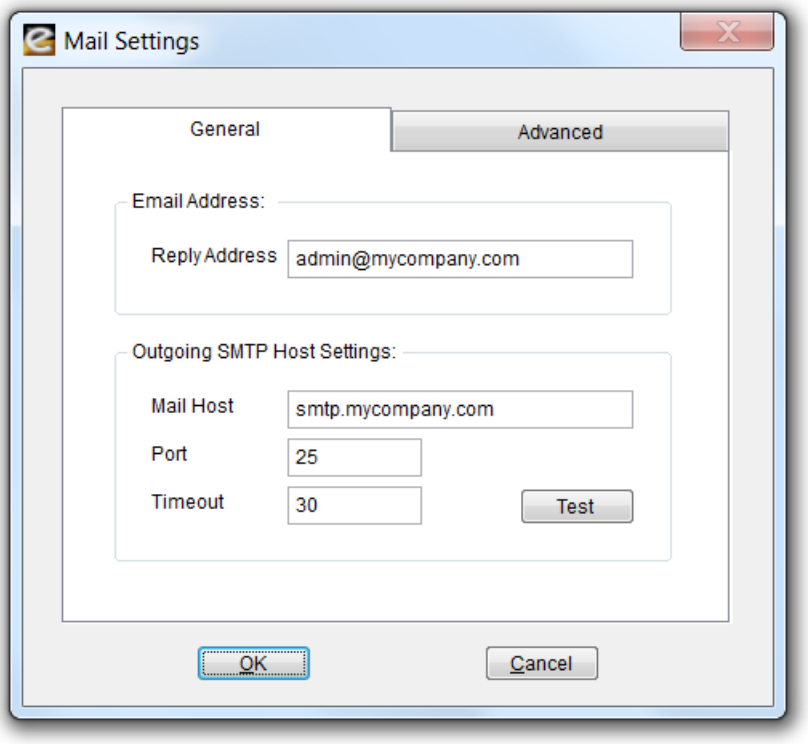
E-mail Output

The Schedule tab allows you to specify if a report is distributed via Pearl Echo'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 E-mail Service

The Pearl Echo Report Manager emails 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 reply email address, SMTP server and port with which the Pearl Echo 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 Pearl Echo Reporting Console

A copy of the Pearl Echo 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 Pearl Echo 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 Pearl Echo workstation agents are not configured to communicate with the manager's 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 Pearl Echo 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 Pearl Echo 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:

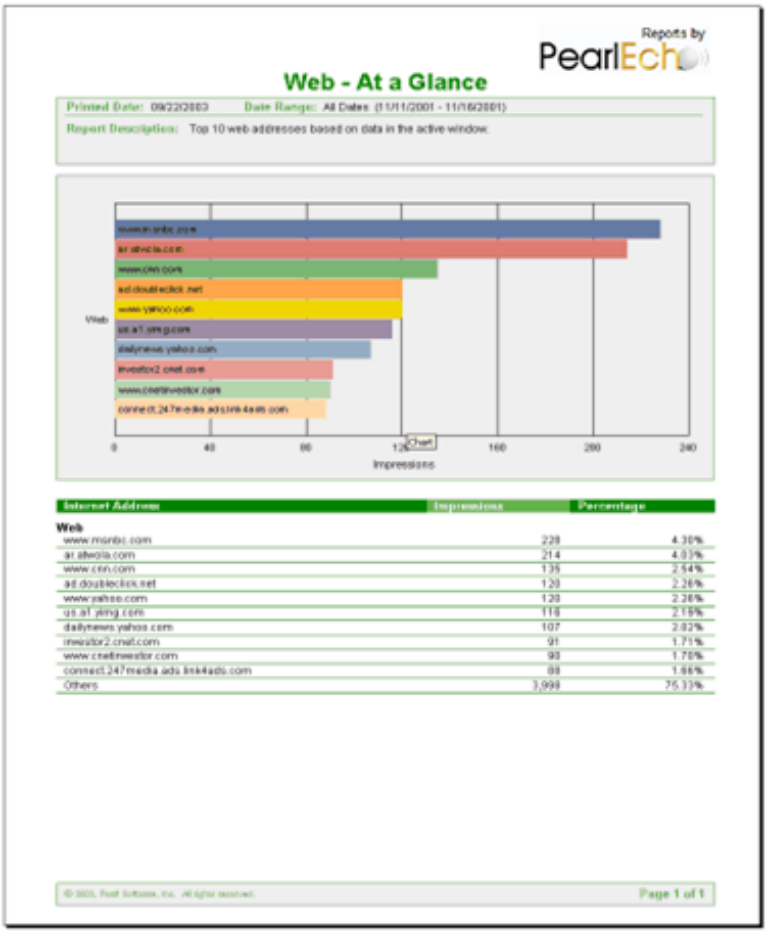
1. Run setup.exe from the installation media or download directory.
2. Select Server Setup.
3. Run the Pearl Echo Administration Console and proceed through the Setup Wizard.
4. When prompted, enter your Restricted OU Reporting Console serial number.

Chapter 8

Data Analysis

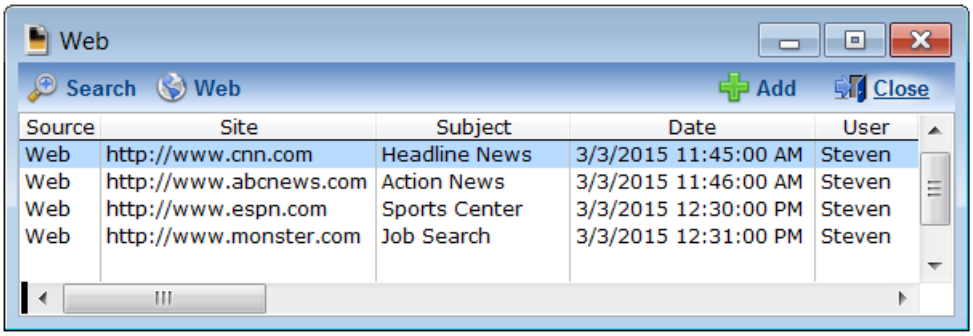
At-a-Glance Reports

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



Time on Web Reports

Pearl Echo can *estimate* the amount of time users spend on the World Wide Web. Pearl Echo calculates the duration of web activity by looking at successive log entries in the Pearl Echo Activity Log. Because Pearl Echo can not determine if users are actively reading a web page or may 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.



Source	Site	Subject	Date	User
Web	http://www.cnn.com	Headline News	3/3/2015 11:45:00 AM	Steven
Web	http://www.abcnews.com	Action News	3/3/2015 11:46:00 AM	Steven
Web	http://www.espn.com	Sports Center	3/3/2015 12:30:00 PM	Steven
Web	http://www.monster.com	Job Search	3/3/2015 12:31:00 PM	Steven

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, Pearl Echo reports against data in the active Pearl Echo window. For more extensive reporting, refer to the Pearl Echo Report Manager section above.

Appendix A

Appendix A: Pearl Echo Program Components

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

The following is a list of Pearl Echo directories and components that must not be altered, scanned, **interrogated while running** or opened by third party applications:

Pearl Echo Administration Machine	
All Files in the Pearl Echo program directory	Typically c:\Program Files (x86)\Pearl Echo
Pearl Echo Workstation	
All files in the Pearl Echo program directory	Typically c:\Program Files (x86)\Common Files\Microsoft Shared\pse7
Network Layer driver component	Typically c:\Windows\System32\wfpent8.sys
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 Layered Provider

Appendix B

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 and Social Networks	Sites that offer social networking or 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, or 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.
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.
In Queue	Sites not yet categorized by Echo.Filters automatically submitted to Echo.Filters categorization queue for human review.
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

Appendix C: Troubleshooting Tips

Issue	Resolution
Pearl Echo Workstation installation fails to connect to Pearl Echo server. Error 10060 occurs during installation.	Configure software firewalls to allow Pearl Echo Server Software (echoComm) and Workstation (rnappp7, updater7) processes. (On Win7 / 2008 add echoComm.exe to firewall exceptions list even though the firewall may be turned off.) Verify that the Pearl Echo Management State is On in the Pearl Echo Administration Console. Verify that a hardware firewall is not blocking communications on any of the Pearl Echo TCP/IP ports. If your Server Software is on Windows 7 or Vista, confirm that you ran the Administration Console with elevated privileges.
Pearl Echo Administration Console hangs at startup every few weeks.	The Pearl Echo Administration Console optionally checks for product updates every two weeks. Verify that a firewall is not blocking ftp communication from EchoAdmin.exe or disable auto-updates from the Options->Preferences menu.
Pearl Echo Administration Console periodically stops updating the Activity Log. After rebooting, logging resumes and missing activity is present.	Pearl Echo requires exclusive access to the Pearl Echo database files. Exempt the Pearl Echo Program Directory from antivirus and antispyware scans.

Issue	Resolution
"The Echo workstation agent has been altered without authorization on this computer..." appears in the Pearl Echo Activity Log.	Pearl Echo's Winsock 2 components have been modified, displaced, or removed by a third party program. Uninstall and reinstall the Pearl Echo Workstation Software. See Appendix C of this User's Guide for details on configuring third party security utilities with Pearl Echo.
Pearl Echo 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 Pearl Echo 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
Installation Error, "1:Failed to Install ISKernel Files."	When installing on Windows 7 or Vista, setup.exe should be run with elevated privileges. This is done by disabling User Account Control or right clicking on the setup.exe icon and selecting "Run as administrator". Do not launch the workstation .msi directly on Windows 7 or Vista. Run the install from setup.exe.
External/roaming users are not monitored or controlled.	See Chapter 2 of this User's Guide for firewall configuration settings.
Other Issues	View other troubleshooting tips and issues at www.pearlsoftware.com/support/kbase.html

Appendix D

Appendix D: Contacting Pearl Software

By Email

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

By the Web

- Corporate Web: www.PearlSoftware.com
- Purchase Web: www.PearlSoftware.com/Store
- Support Web: www.PearlSoftware.com/Support

By Telephone

- (800) 732-7596 (800-PEARL96)
- (610) 400-3690 (Outside USA)

By Mail

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