



ContentProtect Professional Suite Administrator's Guide

© 2006 ContentWatch, Inc. All rights reserved.
2369 West Orton Circle, Salt Lake City, UT 84119



Legal Notices

ContentWatch, Inc. makes no representations or warranties with respect to the contents or use of this documentation, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, ContentWatch, Inc. reserves the right to revise this publication and to make changes to its content, at any time, without obligation to notify any person or entity of such revisions or changes.

Further, ContentWatch, Inc. makes no representations or warranties with respect to any software, and specifically disclaims any express or implied warranties of merchantability or fitness for any particular purpose. Further, ContentWatch, Inc. reserves the right to make changes to any and all parts of ContentWatch software, at any time, without any obligation to notify any person or entity of such changes.

You may not use, export, or re-export this product in violation of any applicable laws or regulations including, without limitation, U.S. export regulations or the laws of the country in which you reside.

Copyright © 2002-2006 ContentWatch, Inc. All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the express written consent of the publisher.

ContentWatch, Inc.
2369 West Orton Circle
Salt Lake City, Utah 84119 U.S.A.

www.contentwatch.com

ContentWatch Trademarks

ContentWatch is a trademark of ContentWatch, Inc. in the United States and other countries.

ContentProtect is a trademark of ContentWatch, Inc. in the United States and other countries.

ContentProtect Professional is a trademark of ContentWatch, Inc. in the United States and other countries.

CallingID Trademarks

CallingID for the Internet is a trademark of CallingID in the United States and other countries.

Third-Party Materials

All third-party trademarks are the property of their respective owners.

ContentProtect Professional 2.5 Suite Administrator's Guide
December 2006





Table of Contents

Welcome to ContentProtect Professional	6
System Requirements and Key Features	6
Registering ContentProtect Professional.....	7
Installing and Uninstalling the ContentProtect Professional Client.....	13
Installing the Client	13
Manual Method.....	13
Unattended Method.....	16
Uninstalling the Client.....	18
Manual Method.....	18
Unattended Method.....	18
Getting Started with the ContentProtect Professional Client	19
Signing In.....	19
Signing Out.....	20
Updating the Client	20
Disabling the Client.....	21
Changing User Passwords	22
Administering ContentProtect Professional	24
Logging In to the Online Management Application.....	24
Modifying Organization Settings.....	26
Changing the Display Name.....	26
Changing the Client Install and Uninstall Passwords.....	27
Changing the Client Update Method	27
Displaying a Custom Message for Blocked Web Sites	27
Hiding the ContentProtect Professional Client Systray Icon	28
Managing Users.....	29
Creating Groups	29
Adding Users	30
Modifying User Settings	31
Removing Users	32
Managing Policies.....	33
Adding Policies	34
Modifying Policy Settings	35
Configuring Time Controls.....	40
Denying or Allowing Access to Internet Applications and Games	44
Assigning Policies	45
Block and Warning Messages.....	46



Working with Reports.....	48
Setting Up Notifications	52
Defining Web Overrides	54
Adding Applications to the Bypass List.....	56
Processing Web Override Requests	58
Controlling Users' Access to Applications	59
Adding Applications to the Application Management List	59
Editing Policies for Application Management.....	61
Protecting Users' Privacy	63
The ContentProtect Professional Appliance (CPS-1000).....	64
Setting Up the Appliance	64
Maintaining the Appliance	67
Glossary	70
Open Code License Text.....	73





Welcome to ContentProtect Professional

Welcome to the ContentProtect™ Professional™ Suite, the most comprehensive and easily adaptable Internet filtering software available today. The ContentProtect Professional Suite comes preset to protect you from objectionable and inappropriate content. However, because not all users are alike, the ContentProtect Professional Suite also provides the ability to modify the filter settings so you can customize ContentProtect Professional to suit your individual usage needs.

The following resources are available to help you use the ContentProtect Professional Suite:

- *ContentProtect Professional Suite Administrator's Guide* (PDF format). It provides
 - Step-by-step instruction
 - ContentProtect category list with descriptions
 - Glossary
 - FAQ (Frequently Asked Questions)
- Customer Support is provided at 1-800-485-4008 for questions and technical assistance. Customer Support is available Monday through Friday, 8 a.m. to 5 p.m. Mountain Standard Time.
- Web-based Customer Support is available anytime at info@contentwatch.com.

Documentation Conventions

A trademark symbol (®, ™, etc.) denotes a ContentWatch™ trademark. An asterisk (*) denotes a third-party trademark.



System Requirements and Key Features

Client System Requirements

- PC or compatible 133 MHz or faster processor
- Microsoft* Windows* 2000/XP
- 128 MB RAM minimum, 256 MB RAM recommended
- 25 MB hard drive space
- CD-ROM drive
- Color monitor with a minimum 1024x768 resolution
- Internet connection
- Internet Explorer* 4.0 or later, Netscape* 6.0 or later, or other current Web browser

Key Features

- ContentProtect Professional is easy to set up and use.
- Profiles permit you to meet the unique needs of individual users and groups.
- Online reports and graphs of Internet activity help you manage risk and increase productivity.
- Online management allows you to manage organization and user account settings from anywhere an Internet connection is available.
- Instant email notifications of inappropriate Internet usage warn you when your Internet usage policy is being violated, enabling you to address issues promptly.
- Blocked Web page override options can be defined by the administrator.
- Peer-to-peer connections, newsgroup access, chat (instant messaging or IM), and Web applications can be controlled, enabling you to manage bandwidth and increase productivity.
- ContentProtect Professional is compatible with anti-virus and firewall software and can integrate into your existing security infrastructure.
- Simple and automatic updates ensure accurate filtering.
- Application Management lets you control which applications users can run on their computers.
- Privacy Protection helps protect users against phishing Web sites and any type of Web site that might put sensitive personal information at risk.





Registering ContentProtect Professional

After you have purchased ContentProtect™ Professional™, you must register your product before you can download the ContentProtect Professional client or access the Online Management application. If you purchased ContentProtect Professional online or requested a trialware number, the registration number was sent to you via email. If you purchased ContentProtect Professional in a store, the registration number came with your CD.

If you purchased the ContentProtect Professional Appliance (CPS-1000), you must complete the registration process before attempting to set up the appliance.

Important: You must have an Internet connection to register and install ContentProtect Professional. If you have a dial-up connection, you should connect to the Internet before beginning the registration process.

To register ContentProtect Professional:

1. In the pre-registration email you received from ContentWatch™, click the **Registration** link.

Your Web browser opens, and you are taken to the registration wizard on the ContentWatch Web site.

2. Enter the registration number provided in your pre-registration email and then click **Next**.

Product Registration: Step 1 of 8

Registration Number

To begin ContentProtect Professional setup, please enter your Registration Number provided at time of purchase.

Registration #:

Next

3. Enter display information.

- a. In the Organization Name field, type your company's name.

The organization name you type here appears in Internet usage reports and the Online Management application. The organization name can contain spaces but no special characters, such as commas or apostrophes.

- b. From the Language drop-down list, select the desired language and then click **Next**.

Product Registration: Step 2 of 8

Display Information

Your Organization Name will be used for display purposes in reporting and the Online Management application.

Organization Name:

Language:

Note: The language you select during product registration affects only how text is displayed in the ContentProtect Professional client interface. It does not affect the language of text displayed in the Online Management application. To change the language displayed, you must configure your browser's preferences accordingly. Refer to your browser documentation for instructions on how to do this.

4. Specify the initial user login information for the ContentProtect Professional client and the administration login information for the Online Management application.
- Under Initial User Login, in the Initial User Name field, specify the name that must be entered to log in to the ContentProtect Professional client for the first time on a computer. This account allows the client to access the Internet so it can download profile and client software updates.
 - Under Initial User Login, in the Password and Confirm Password fields, specify the password for the initial user account.
 - Under Administration Login, in the Organization ID field, type your company's name.
The organization ID must be unique because it is required, along with an administrator user name, to log in to the Online Management application. If you specify an organization ID that already exists in the ContentWatch database, you are informed that the ID is already in use and that you must specify a different organization ID.

Note that the Admin User Name field already contains the name "Admin." This is the mandatory user name for the initial ContentWatch Professional administrator account.

- d. Under Administration Login, in the Admin Password and Confirm Password fields, specify a password for the Online Management administrator user account and then click **Next**.

Product Registration: Step 3 of 8

Initial User Login

In order to login for Internet access an initial user must be created.

Initial User Name:

Password:

Confirm Password:

Administration Login

The Organization ID is a unique identifier used during administration login. The Admin User Name cannot be changed; however, a password must be provided for this account.

NOTE: The "Admin" may not login for Internet access. This account is provided for administration only.

Organization ID:
(/BM)

Admin User Name:

Admin Password:

Confirm Password:

5. Specify and confirm passwords for installing and uninstalling the ContentProtect Professional client on users' machines and then click **Next**.

For security purposes, we recommend that you have different install and uninstall passwords.

Product Registration: Step 4 of 8

Install/Uninstall Passwords

Your Install/Uninstall Passwords will be used to install ContentProtect Professional on individual user machines. (NOTE: For Security reasons we recommend your Install and Uninstall Passwords be unique.)

Install Password:

Confirm Password:

Uninstall Password:

Confirm Password:

- Specify the secret question and answer you want to use for recovering your Online Management application password in the event you forget your login information and then click **Next**.

This information is also used to verify your identity if you contact Customer Support.

Product Registration: Step 5 of 8

Password Reminder

Secret Question: (Example: What is your first pet's name?)

Answer: (This is used if you forget your password.)

- Specify the email address where you want your registration confirmation email to be sent and then click **Next**.

This is also the email address you use in the event that you forget the password for the initial administrator account and need to reset it.

Product Registration: Step 6 of 8

Email Address

Your Email Address will be used for account confirmation.

Email Address:

8. Verify that all information you have entered is accurate and then click **Submit**.

If you need to change any information, click **Edit** next to the information you want to change and make the necessary modifications.

Product Registration: Step 7 of 8

Account Confirmation

Step 1 of 8: Registration Number
Registration Number: 004-210-SX2CDAHYIW75KE2ITPPQYE22 **Edit**

Step 2 of 8: Display Information
Organization Name: My Corporation **Edit**
Language: English

Step 3 of 8: Initial User and Admin Logins
Initial User Name: user1 **Edit**
Password: *****
Organization ID: MyCorp
Admin User Name: Admin
Password: *****

Step 4 of 8: Install/Uninstall Passwords
Install Password: ***** **Edit**
Uninstall Password: *****

Step 5 of 8: Password Reminder
Secret Question: Who is your favorite band? **Edit**
Answer: Jefferson Starship

Step 6 of 8: Email Address
Email Address: kenb@mycorp.com **Edit**

The registration process is now complete. You should receive a confirmation email at the address you provided during registration.

9. Using the links displayed in the last step of the registration wizard or in the registration confirmation email, you can do the following:
- Download the Content Professional client in preparation for installing it on users' machines.
 - Log in to the Online Management application on the ContentWatch Web site to perform administration and configuration tasks, such as creating groups, adding user accounts, and setting up and assigning policies.

Product Registration: Step 8 of 8

Registration Complete

Your Registration has been successfully completed.

A confirmation email has been sent to: kenb@mycorp.com

1. To manage your account from anywhere, go to:
<https://pro.contentwatch.com/ProAdminServlet>
and log in with the Organization ID, User Name and Password.

2. In order to access the Internet you will need to provide the initial User Name and Password

3. To install ContentProtect, go to:
<https://pro.contentwatch.com/RegistrationServlet/Install.htm>



Installing and Uninstalling the ContentProtect Professional Client

Note: You can skip this section if you are using the CPS-1000 appliance as the only method for filtering content and regulating Internet access in your organization and you do not intend to use the ContentProtect™ Professional™ client for remote employees or laptop users. For instructions on setting up and maintaining the CPS-1000 appliance, see [The ContentProtect Professional Appliance \(CPS-1000\)](#) on page 64.

Installing the Client

Manual Method

After you have registered ContentProtect™ Professional™, you are provided with a link to download the ContentProtect Professional client. You can download two versions of the client software:

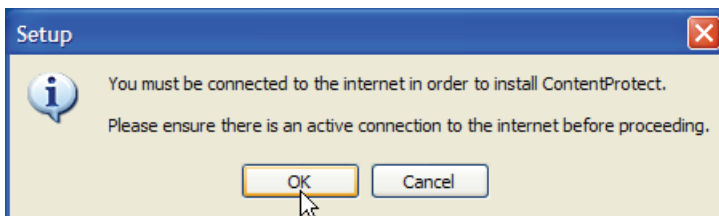
- **Manual Install client**
Lets you take the client executable to each user's machine yourself and manually start the installation or if you want to email the executable to users and have them run the installation.
- **Distribution-Enabled client**
Lets you perform an unattended install of the client on your users' machines.

WARNING: If you download both the manual install and distribution-enabled files for the ContentProtect Professional client, be sure to place the files for the two installation types in different directories. If you try to run the manual install executable from the same directory where the *unattend.txt* file is located, the manual install executable uses the *unattend.txt* file to perform an automated installation. This can be a problem if you have not configured the *unattend.txt* file with a valid registration number and password. If this is the case, the manual install process fails and the client uninstalls itself.

In this section, we discuss how to manually install the ContentProtect Professional client on users' machines. For instructions on automating the distribution of the client, see [Unattended Method](#) on page 16.

To manually install the ContentProtect Professional client:

1. On the user's machine, double-click the Manual Install version of the ContentProtect Professional client (*cwip_prosuite.exe*).
2. Select the language for your installation and then click **OK**.
3. If you are not connected to the Internet when the installation launches, a setup dialog warns that you must have an Internet connection to proceed with the installation.

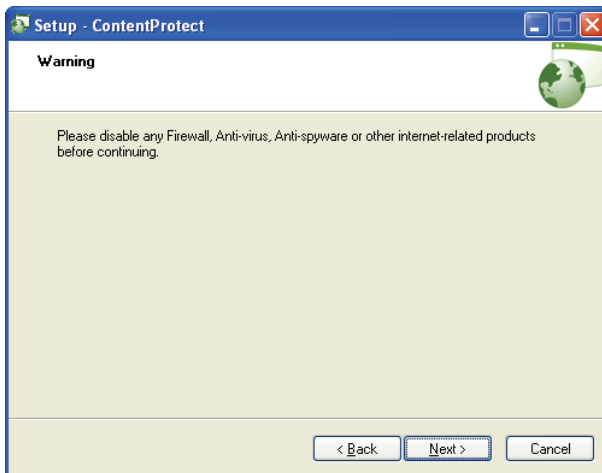


4. Ensure that you are connected to the Internet and then click **OK** to continue.
The ContentProtect Setup Wizard launches. We recommend that you close all other applications before continuing with the installation.

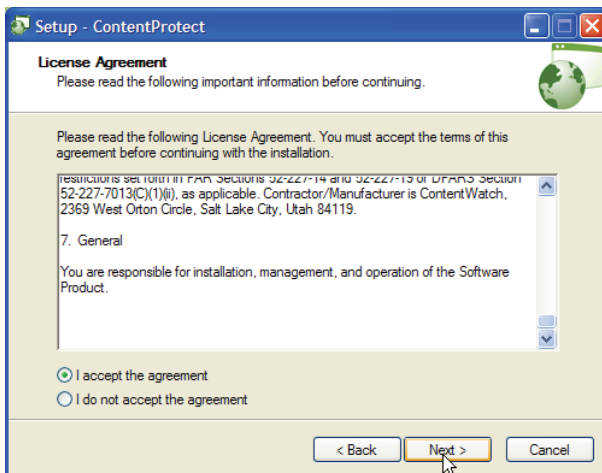
- At the Welcome window, click **Next**.



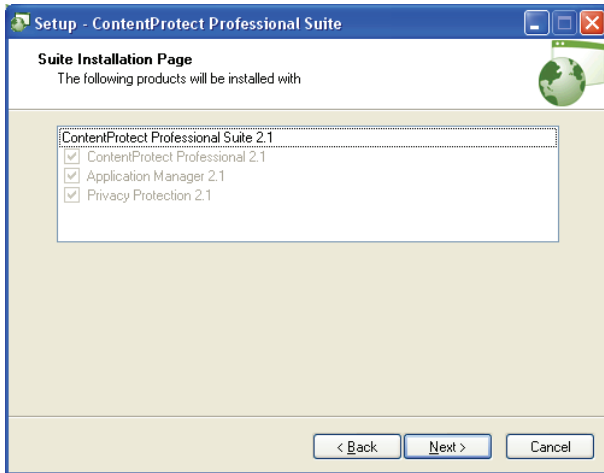
- When the Warning screen appears, make sure you disable any firewall, anti-virus, anti-spyware, or other Internet-related products that may be running on your computer, and then click **Next** to continue.



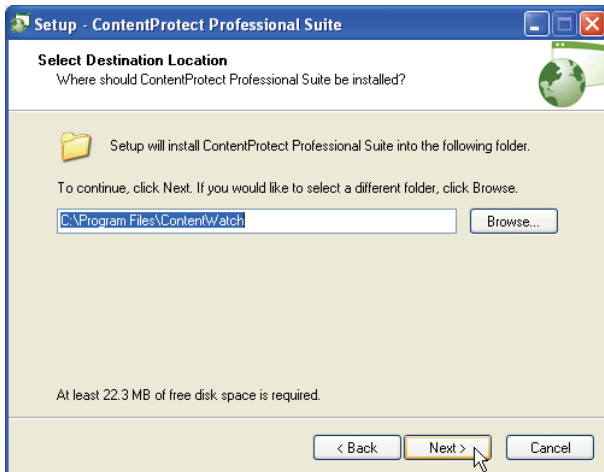
- At the License Agreement window, carefully review the License Agreement, select **I accept the agreement**, and then click **Next** to continue.



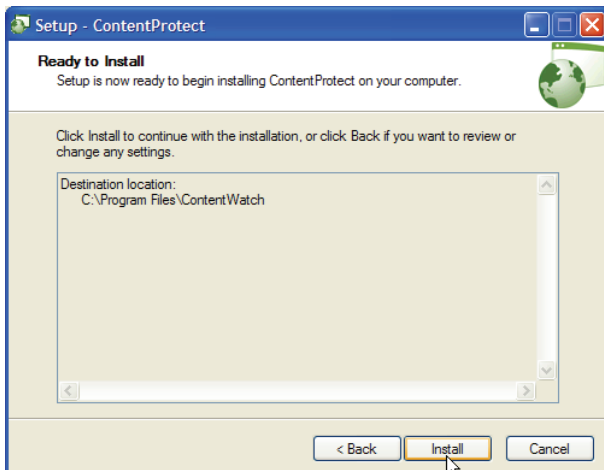
8. At the screen listing the suite components that will be installed, click **Next**.



9. Select the location where you want to install ContentProtect Professional and then click **Next**.
The default location is C:\Program Files\ContentWatch. To choose a different location, click **Browse** and select the new location.

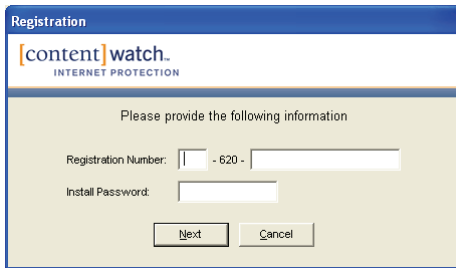


10. At the Ready to Install window, click **Install** to begin the installation.



ContentProtect Professional installs the program files to the destination location and registers the program modules.

11. When prompted, type your registration number and install password and then click **Next** to continue.




12. Wait as ContentProtect Professional verifies and activates your registration number.

Note: You must have an Internet connection to complete this step.

13. Click **Restart** to complete the ContentProtect installation and setup.
Your computer automatically shuts down and restarts.



After installation, ContentProtect Professional is automatically enabled and placed in your startup menu. A ContentProtect icon  also appears in the system tray located on the taskbar at the bottom of the Windows desktop.

Unattended Method

After you have registered ContentProtect Professional, you are provided with a link to download the ContentProtect Professional client. You can download two versions of the client software:

- Manual Install client
Lets you take the client executable to each user's machine yourself and manually start the installation or if you want to email the executable to users and have them run the installation.
- Distribution-Enabled client
Lets you perform an unattended install of the client on your users' machines.

WARNING: If you download both the manual install and distribution-enabled files for the ContentProtect Professional client, be sure to place the files for the two installation types in different directories. If you try to run the manual install executable from the same directory where the *unattend.txt* file is located, the manual install executable uses the *unattend.txt* file to perform an automated installation. This can be a problem if you have not configured the *unattend.txt* file with a valid registration number and password. If this is the case, the manual install process fails and the client uninstalls itself.

In this section, we discuss how to perform an unattended install of the ContentProtect Professional client on users' machines. For instructions on manually installing the client, see [Manual Method](#) on page 13.

Prerequisites: You must have a means for pushing out the Distribution-Enabled client executable and its accompanying text file to your users' machines. You can use a software distribution tool (such as Microsoft Systems Management Server, LANDesk* Management Suite, or Altiris* Client Management Suite*) or a login script to accomplish this. For instructions on pushing out files to computers on your network, see your software distribution tool's documentation.

To perform an unattended install of the ContentProtect Professional client:

1. Download and unzip the Distribution-Enabled version of the ContentProtect Professional client.
2. Edit the *unattend.txt* file:
 - a. Open the *unattend.txt* file in Notepad.
 - b. Delete the placeholder text for the RegistrationNumber and Password values.
 - c. Type your ContentProtect Professional registration number and installation password and specify how the system should restart ("Manual" or "Automatic") after the installation is complete. For example:

```
RegistrationNumber=1-234-5U2DMVZHJQECWRNIFHUF3T3D  
Password=myinstallpwd  
Restart=Automatic
```

If you specify "Automatic" as the Restart parameter, the installation proceeds without requiring any user input. After the installation process is complete, the user's computer reboots automatically and ContentProtect Professional starts running.

If you specify "Manual" as the Restart parameter, the installation proceeds automatically, but a dialog appears at the end of the installation process informing the user that the computer needs to be restarted in order to complete the installation. Users can save any files they have open and shut down running programs before clicking the **Restart** button in the dialog.

- d. Save your changes to the *unattend.txt* file and close Notepad.
3. Use a software distribution tool (or a login script) to push out the *cwip_prosuite_unattend.exe* file and the *unattend.txt* file to users' computers, and to then run the *cwip_prosuite_unattend.exe* file.

IMPORTANT! The *cwip_prosuite_unattend.exe* file and the *unattend.txt* file must be placed in the same directory on users' machines.

Uninstalling the Client

Manual Method

To uninstall the client manually:

1. Open the Windows Control Panel.
For example, in Windows XP, click **Start > Control Panel**.
2. Double-click **Add or Remove Programs**.
3. Select **ContentProtect** and then click **Remove**.
4. When prompted, enter the uninstall password.
Note: This is the uninstall password you specified during the registration process. It is not the same as your ContentProtect Professional login password.
5. Complete the uninstall process and restart the computer when prompted.

Unattended Method

To perform an unattended uninstall of the ContentProtect Professional client:

1. Open a command prompt window and navigate to the folder where the ContentProtect Professional client uninstaller is located.

By default, the uninstaller is located in the following directory:

C:\Program Files\ContentWatch\InternetProtection\ContentProtect

2. At the command prompt, type the following command:

```
unins000.exe /UninstallPassword=<uninstall password>
```

Replace <uninstall password> with the uninstall password you specified during the ContentProtect Professional product registration process.



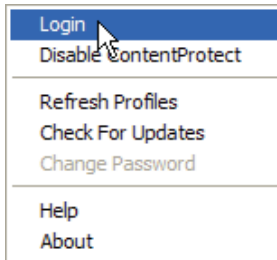
Getting Started with the ContentProtect Professional Client

Signing In

You must sign in to the ContentProtect™ Professional™ client before you can access the Internet or instant messaging. If you do not sign in manually, you are prompted to sign in when you attempt to use the Internet.

To sign in manually:

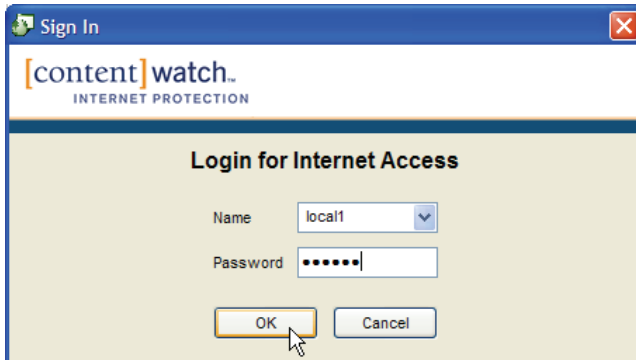
1. Right-click the ContentProtect Professional icon  in the system tray located on the taskbar at the bottom of your Windows desktop and then select **Login** from the quick menu.



2. Select your user name from the drop-down menu, type your password, and then click **OK**.

If you don't know your password, ask the administrator.

Note: Asterisks (*) appear as you type your password to protect it from being viewed.




You are now signed in as a user. Launch your Internet browser and proceed with regular Internet activity. For information about the possible warning and block messages you might receive, see [Block and Warning Messages](#) on page 46.

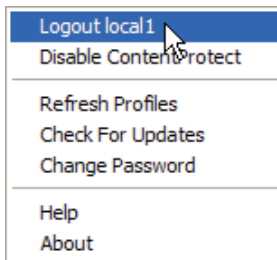
Signing Out

When you finish your Internet or instant messaging session, we recommend you sign out of the ContentProtect Professional client.

WARNING: If you leave your computer without signing out of the ContentProtect Professional client, other users have access to the Internet (under your sign-in name) and your Web and instant messaging privileges. This also means that their Web and instant messaging activity is logged under your name. However, if Inactive User Logout is enabled, you are logged off according to the time limits set by the administrator.

To sign out of the ContentProtect Professional client:

1. Right-click the ContentProtect Professional icon  located in the system tray on the taskbar at the bottom of your Windows desktop.
2. Select **Logout** from the quick menu.




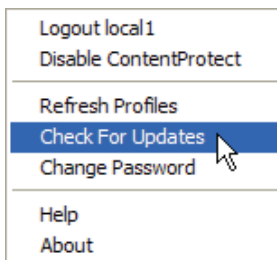
Note: If you shut down your computer without signing out, your session automatically ends. You must sign in again when the computer restarts.

Updating the Client

Online Updates allow you to update the ContentProtect Professional client with the latest software. In the Online Management application, the administrator can configure clients to perform manual or automatic updates.

If clients are set to perform updates manually, complete the following to check for updates:

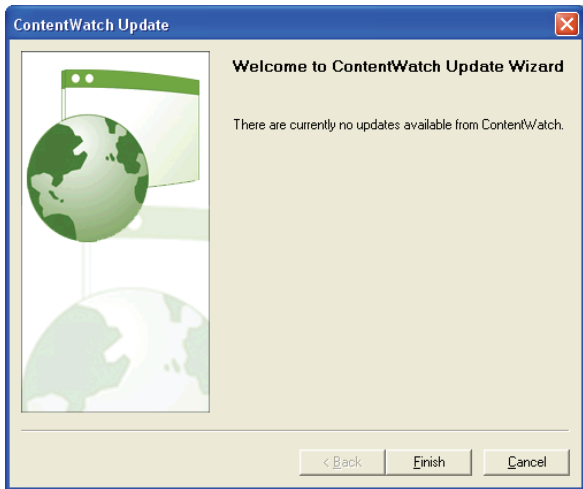
1. Right-click the ContentProtect Professional icon  in the system tray.
2. Select **Check For Updates** from the quick menu.



An update wizard appears.

3. If ContentProtect Professional Suite updates are available, follow the prompts to complete the update wizard.

If ContentProtect Professional Suite updates are not available, the following screen is displayed:




Click **Finish** to close the screen.

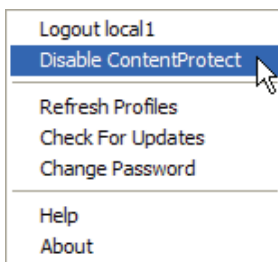
4. If you choose to download and install the updates, you may be asked to restart your computer for the changes to take effect.

Disabling the Client

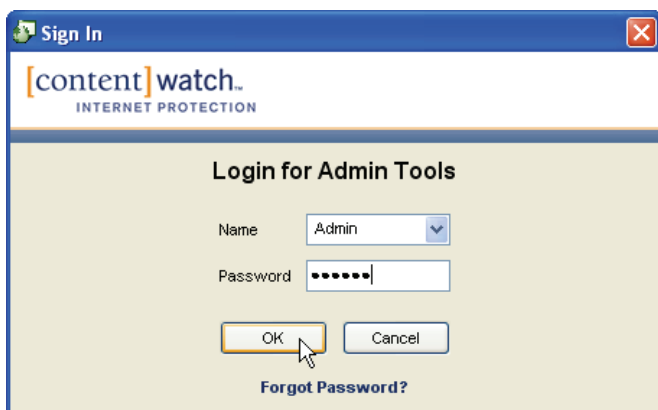
There may be times when you want to temporarily disable the ContentProtect Professional client. For example, you may want to temporarily allow access to the Internet without blocking any content, or you may want to allow a non-safe search in one of the supported search engines. Rather than temporarily changing the current user's policies, a user with administrative rights can temporarily disable the ContentProtect Professional client.


To temporarily disable the ContentProtect Professional client:


1. Right-click the ContentProtect Professional icon  in the system tray located on the taskbar at the bottom of your Windows desktop.
2. Select **Disable ContentProtect** from the quick menu.

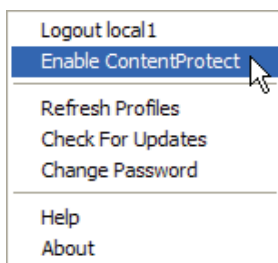


3. Type the administrative user's password and then click **OK**.



The client is now disabled, and the ContentProtect Professional icon in the system tray appears grayed out . To re-enable the ContentProtect Professional client:

1. Right-click the ContentProtect Professional icon  in the system tray located on the taskbar at the bottom of your Windows desktop.
2. Select **Enable ContentProtect**.




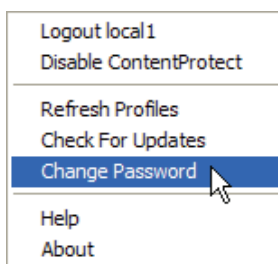
The client is now enabled, and the ContentProtect Professional icon in the system tray appears in color .

Changing User Passwords

Users can quickly change their own ContentProtect Professional client login passwords.

To change a password, the user must complete the following:

1. Make sure that he or she is logged in to the ContentProtect Professional client with his or her own user name.
2. Right-click the ContentProtect Professional icon  in the system tray located on the taskbar at the bottom of the Windows desktop.
3. Select **Change Password** from the quick menu.



4. Type the old password and the new password in the appropriate fields, retype the new password to confirm it, and then click **OK**.



The password is immediately changed in the local client database, and the updated information is sent to the Online Management application.



Administering ContentProtect Professional

Logging In to the Online Management Application

The Online Management application lets you create and customize user and group profiles, define and configure policy settings, generate and view user activity reports, and set up email notifications and Web site overrides.

Important: You must have an Internet connection and be a user with administrator rights to access the Online Management application.

To log in to the Online Management application:

1. Open your Web browser and go to <http://pro.contentwatch.com/ProAdminServlet>.

Note: You may want to bookmark this Web page for fast access in the future.

2. Enter your organization ID, user name, and password, and then click **Login**.

Note: Asterisks (*) appear as you type your password to protect it from being viewed.

ContentWatch Web Administration

Organization ID:

User Name:

Password:

[Forgot Password?](#)

If you forget the Admin password, you must do one of the following:

- If you have more than one administrator account, another administrator can change your password for you by logging in to the Online Management application, selecting your user account, and changing the password in the Settings area.
- At the login screen of the Online Management application, do the following:

- a. Click **Forgot Password**.
- b. When prompted, provide the email address you used to register the product and then click **Send**.

Note: If you no longer have access to the email address you used to register the product, send an email to support@contentwatch.com or call 1-800-485-4008.

- c. At the address specified, check your email for a message from ContentWatch with the subject "Requested Login Information."

IMPORTANT: After ContentWatch™ sends this email to you, you have 10 minutes to reset the Admin password. If you do not reset the password within this timeframe, you must repeat the preceding steps.

After you have successfully logged in, the Online Management application interface is displayed:

The screenshot displays the ContentProtect Professional Suite Online Management application interface. The top navigation bar includes the ContentWatch logo, the product name 'ContentProtect PROFESSIONAL SUITE', and links for 'Sign Out', 'About', and 'Help'. The user is logged in as 'Admin'. The main interface is divided into a left sidebar and a main content area. The sidebar shows a tree view under 'Users' with 'My Corporation' expanded, showing sub-items for 'Employees', 'IT', and 'Tech Support'. Below this is an 'Add Group' button and a 'Policies' section. The main content area is titled 'Settings for "My Corporation"' and contains several sections: 'Organization' with fields for 'Display Name' (My Corporation) and 'Organization ID' (MyCorp1); 'Install' with 'Password' and 'Confirm Password' fields; 'Uninstall' with 'Password' and 'Confirm Password' fields; 'Client Updates' with an 'Apply' dropdown menu set to 'Manually'; 'Custom Block Page' with a 'Web Address' field (with a note to leave blank for default behavior); and 'Client Icon' with a 'Hide Icon' checkbox (with a note to remove icon from system tray). A 'Save Changes' button is located at the bottom of the settings area.

Important: We recommend that you do not leave the Online Management application open if you walk away from your computer because this gives others access to the application and administrator settings. To log out of the Online Management application, click **Sign Out** in the upper-right corner of the Online Management application interface.

Modifying Organization Settings

The Organization Settings page is displayed by default when you log in to the Online Management application. If you are on a different page, you can access the Organization Settings page by clicking your organization name in the upper-left area of the screen:



On the Organization Settings page, you can perform the following tasks:

- Change the organization name that is displayed in the Online Management application and on all Internet usage reports
- Change the password required for installing the ContentProtect Professional client
- Change the password required for uninstalling the ContentProtect Professional client
- Change the method for updating the ContentProtect Professional client
- Specify a custom Web page to display when ContentProtect Professional blocks a user from viewing a site
- Hide or unhide the ContentProtect Professional client icon in users' system trays

Changing the Display Name

To change the organization display name:

1. In the Display Name field, type the desired name.

Organization:	
Display Name:	<input type="text" value="New Corporation"/>
Organization ID:	MyCorp

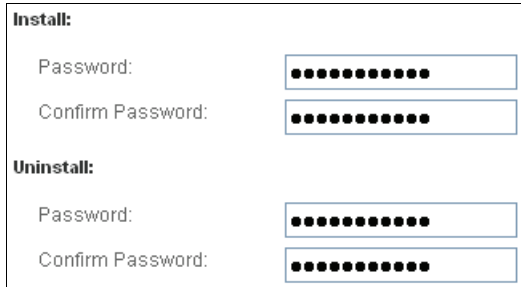
2. Click **Save Changes**.

Changing the Client Install and Uninstall Passwords

Note: For security purposes, we recommend that you set different install and uninstall passwords. The install password may be distributed to users, but you do not usually distribute the uninstall password to users.

To change the client install or uninstall password:

1. In the appropriate Password and Confirm Password fields, type the desired password.



The screenshot shows a form with two main sections: "Install:" and "Uninstall:". Each section contains two text input fields: "Password:" and "Confirm Password:". All four fields are filled with black dots, indicating that passwords have been entered. The "Install:" section is positioned above the "Uninstall:" section.

2. Click **Save Changes**.

Changing the Client Update Method

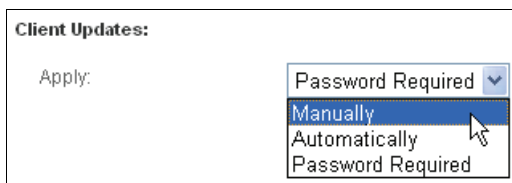
To change how client updates are performed:

1. From the Apply drop-down list, select the desired client update method.

Manually: Requires you to manually choose the **Check for Updates** option from the client's right-click menu. This option is useful for testing the update process on a few sample machines in your company to make sure everything works correctly before you attempt to perform updates on an organization-wide scale.

Automatically: Causes all clients to automatically download and install updates as they become available. You might select this option after you have performed manual testing on a few machines in your company, you have determined that the update process works correctly, and you are ready to allow all machines in your organization to update themselves without user interaction.

Password Required: Prompts for a ContentProtect Professional administrator password to manually access product updates. You might select this option after you are sure all the machines in your organization have been successfully updated at least once and you don't want users to perform further updates without an administrator's knowledge.



The screenshot shows a form titled "Client Updates:". Below the title is a label "Apply:" followed by a drop-down menu. The menu is open, showing four options: "Password Required" (selected), "Manually", "Automatically", and "Password Required". A mouse cursor is pointing at the "Manually" option.

2. Click **Save Changes**.

Displaying a Custom Message for Blocked Web Sites

The Custom Block Page option allows you to display a custom Web page (which can include your company logo, corporate Internet usage policy, or any other information you deem necessary) when users attempt to access blocked Web sites. You can use any Web authoring tool to create the page. Once you have created the page, place it in a location on the Internet or your corporate intranet that is accessible to your users. If your users access the Internet with their company machines outside the corporate network, be sure to place the Web page in

a location that is accessible both inside and outside your network. If you do not, the ContentProtect Professional client will be unable to properly display the block message.

Tip: If you are familiar with a dynamic Web page generation language, such as Java or PHP scripting, you can create a dynamic Web page that parses the parameters it receives from ContentProtect Professional and displays custom block messages that explain specifically why a Web site was blocked.

To point ContentProtect Professional to your custom Web page:

1. In the Web Address field, type the full URL to your custom page.



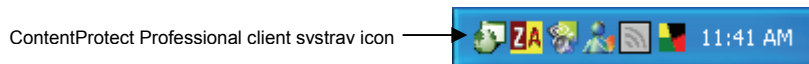
2. Click **Save Changes**.

To revert to ContentProtect Professional's default block messages, remove the URL from the Web Address field and save your changes.

Note: We recommend that you add the Custom Block Page URL to the Web Overrides list. This is important because if the content on the page causes it to fall under a blocked category, ContentProtect will prevent the page from being displayed. Adding the Custom Block Page URL to the Web Overrides list ensures that the page will never be blocked. For instructions on adding URLs to the Web Overrides list, see [Defining Web Overrides](#) on page 54.

Hiding the ContentProtect Professional Client Systray Icon

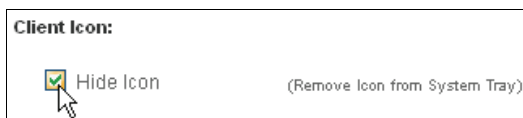
The ContentProtect Professional client icon that resides in the Windows system tray gives users quick right-click access to such features as logging in to the ContentProtect Professional client, checking for updates, refreshing profiles, and disabling ContentProtect Professional.



If you would like to prevent users from accessing ContentProtect Professional features from the systray icon, you can choose to hide the icon.

To hide the icon:

1. Select the **Hide Icon** check box.



2. Click **Save Changes**.

To make the icon reappear in the systray on users' computers, deselect the **Hide Icon** check box and save your changes. The icon will reappear the next time the ContentProtect Professional Web server updates clients' local settings.

Managing Users

A user account must be created for each system user. User accounts let you apply custom policies to individuals and track the Internet usage of users.

Important: Each user must have his or her own account before he or she can access the Internet for browsing or instant messaging.

Creating Groups

User accounts can exist only within groups, so before you can add users, you must first create groups to contain them. Plan how to group users so it will be easier for you to assign Internet access policies to them. You may group users according to what department they are in or how they use the Internet to do their jobs. You can then easily assign a single policy to the group, which is automatically applied to all users within that group. For example, you might group users whose jobs require them to do extensive online research in a group called “Researchers,” and other users who mostly use the Internet for personal pleasure might be added to the “Employees” group. You could then apply a reasonably relaxed policy to the “Researchers” group and a more stringent policy to the “Employees” group.

Note: At any time you can apply any policy you have created to individual users within a group. The policy assigned to an individual user overrides the policy assigned to the group that the user is a member of. For more information on creating and assigning policies, see [Managing Policies](#) on page 33.

To create a new group in the Online Management application:

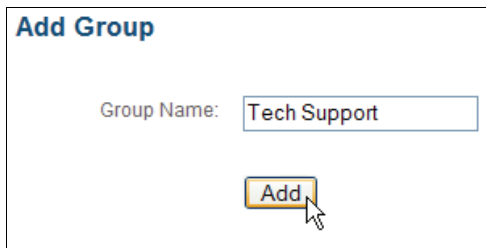
1. Click your organization name in the upper-left area of the screen:



2. Click **Add Group**.



3. In the Group Name field, type the desired group name and then click **Add**.



The new group appears in the group list under the organization name.



Adding Users

After you have created a group, you can add users to the group.

To add a user:

1. Click the group you want to add a user to.
2. Click **Add User**.



The Add User window appears.

- In the Add User window, fill out the user's login and user information and then click **Add**.

Note: For more information on each item you must fill out, see [Table 1: User Settings](#) on page 31. The only item that is not required is the user's email address.

The new user appears in the group.



Modifying User Settings

To modify a user's settings:

- Click the group where the user is located.
- Click the user whose settings you want to modify.
- Modify settings as desired.
- When finished, click **Save Changes**.

The following table outlines the user settings you can edit.

Table 1: User Settings

Field	Description
User Name	Name the user enters (or selects) to sign in to ContentProtect. User names must be between 2 and 20 characters in length.

Field	Description
Password	<p>Password the user enters to sign in to ContentProtect.</p> <p>Passwords must be between 3 and 13 characters in length. Passwords are case-sensitive. Numbers and alpha characters can be combined.</p> <p>Note: We recommend you keep a list of passwords and the corresponding user names in a safe place for reference. However, the administrator can change a password for any user at any time, which eliminates the fear of losing or forgetting passwords.</p>
Email	User's email address.
Group	<p>Group the user is assigned to.</p> <p>To reassign the user to a different group, select the desired group from the drop-down list.</p>
Inactive User Logout	<p>Designates an inactivity threshold after which the user is automatically logged out.</p> <p>If you select Never, ContentProtect does not automatically log out the user.</p>

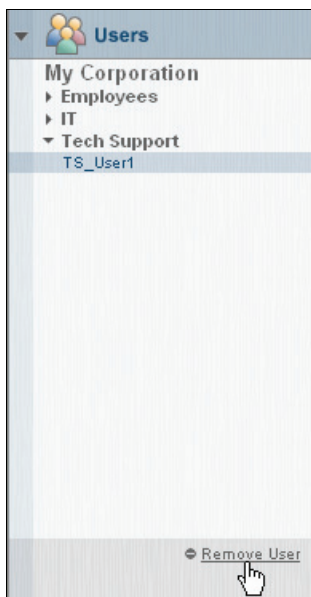
Note: Users must right-click the ContentProtect Professional system tray icon on their machines and select **Refresh Profiles** to immediately apply changes made in the Online Management application. Otherwise, the clients' local settings are updated within 24 hours.

Removing Users

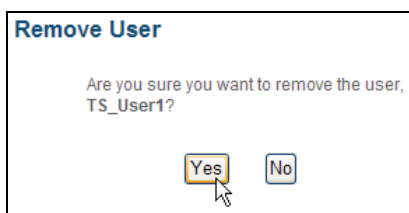
WARNING: This action cannot be undone. If a user account is accidentally deleted, it cannot be restored. If you want to restore the account, you must create it again.

To delete an existing user account:

1. Click the group where the user you want to remove is located.
2. Click the user you want to remove.
3. Click **Remove User**.



4. In the pop-up window that appears, click **Yes** to confirm the deletion or **No** to cancel the deletion.



Managing Policies

Policies are used to control Internet activity (browsing), instant messaging (Yahoo!*, AOL*, MSN*, QQ*, GoogleTalk*), newsgroups, peer-to-peer access, and network gaming. Policies let you select which Internet content types you want to allow or block.

Policies can be assigned to the organization, groups, and individual users. Only the organization *must* have a policy assigned to it. Groups and users you add under the organization are not required to have specific policies assigned to them; they automatically inherit either the organization's policy or the group's policy, and their "Policy in Use" setting defaults to **None**.

When you register ContentProtect Professional, a policy called Default is automatically applied to your organization. This is a general-use policy that blocks the content types most businesses find it expedient to block (adult/mature content, gambling, hate/violence, etc.). All groups and users you add in the Online Management application are governed by the Default policy's restrictions until you assign other policies to your groups or users on an individual basis.

To illustrate how policy assignments affect individual users, consider the following three examples:

Example 1: Policy A is applied directly to User1. Therefore, neither the policy applied to the group that User1 belongs to nor the policy applied to the organization has any effect on User1. As far as this user is concerned, Policy A is the only policy that exists.

Example 2: No policy is applied directly to User2. However, Policy B is applied to the group that User2 belongs to. Therefore, Policy B governs User2. If a different policy is applied to the group in the future, that new policy will govern User2.

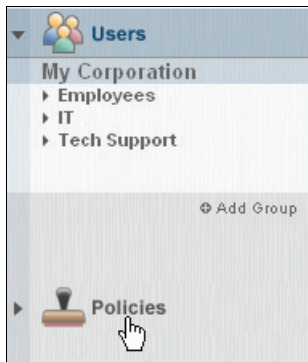
Example 3: No policy is applied to either User3 or his group. Therefore, whatever policy is applied to the organization will govern the group that User3 belongs to, as well as all the users within that group who don't have a policy applied directly to them.

Warning: Because all groups and users you add are governed by the organization's Default policy until you assign a different policy to them, make sure that the Administrator option is *not* selected in the settings for the Default policy. Otherwise, all users you add will have administrative privileges and can log in to the Online Management application and make changes.

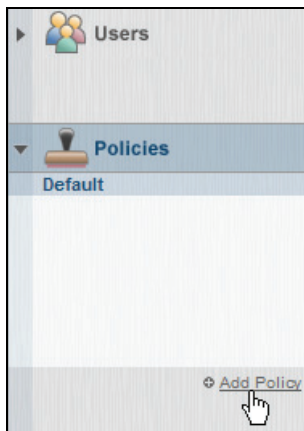
Adding Policies

To add a new policy:

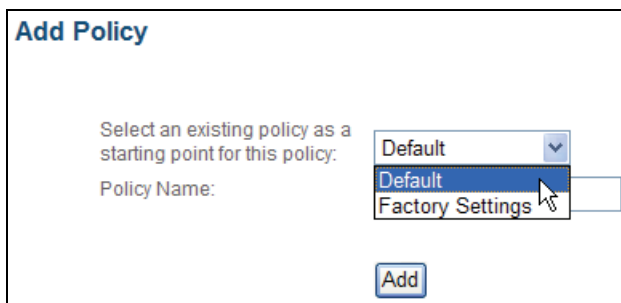
1. In the sidebar of the Online Management application, click **Policies**.



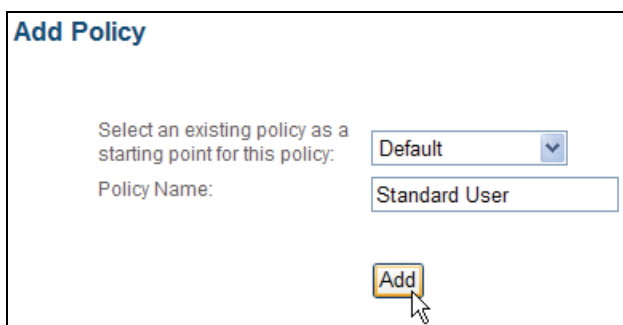
2. Click **Add Policy**.



3. From the drop-down list, select an existing policy whose settings you want to use as a template for your new policy.

A screenshot of the 'Add Policy' dialog box. The title is 'Add Policy'. Below the title, there is a text prompt: 'Select an existing policy as a starting point for this policy:'. To the right of this prompt is a dropdown menu with 'Default' selected. Below the dropdown menu is a text input field labeled 'Policy Name:'. At the bottom of the dialog box, there is an 'Add' button. A mouse cursor is pointing at the dropdown menu.

4. In the Policy Name field, specify a name for your new policy and then click **Add**.



Add Policy

Select an existing policy as a starting point for this policy:

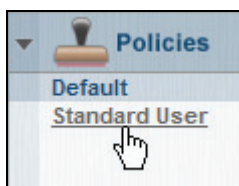
Policy Name:

The new policy appears in the policy list.

Modifying Policy Settings

To modify a policy's settings:

1. Click the policy you want to modify.



2. Block or allow content categories as desired, and then click **Save Changes**.

The following sections describe the policy settings you can modify.

Category Settings

Category settings determine the level of access users have to predefined Internet content categories. Select **Allow**, **Warn**, or **Block** from the drop-down list for each content category.

Allow: Provides access without restriction. No message is displayed, and the user is allowed access to the requested page. The action is logged if activity reporting is enabled.

Warn: Provides access but warns the user of the types of content about to be viewed, and lists the category types that caused the warning. A warning message is displayed, and the user can choose whether to view the requested page. The action is logged if activity reporting is enabled.

Block: Prompts the user that the attempted Web site is being blocked and lists the category types that have blocked it. The requested page does not open unless the user has the privilege to override the block and does so. The action is logged if activity reporting is enabled.


















Note: For message examples and descriptions, see [Block and Warning Messages](#) on page 46.












The following categories are blocked by default, while all other categories are set to Allow:

- Adult/Mature
- Pornography
- Drugs/Alcohol
- Gambling
- Hate/Violence
- Illegal Activities
- Intimate Apparel

The following table outlines the predefined content categories of ContentProtect Professional.

Table 2: Content Categories

Category	Description
 Ads	Advertisements. Note: Because advertisements are commonly embedded in other types of content on the Internet, setting this category to Block or Warn could cause undesirable effects.
 Adult/Mature	Sites or resources that contain subject matter intended for mature audiences, such as obscene or vulgar language and adult instant message rooms. These sites could be considered R-rated.
 Chat Site	Sites or resources that contain information on instant messaging protocols or applications and links to instant messaging organizations, rings, and rooms.
 Drugs/Alcohol	Sites or resources that contain subject matter that deals with manufacturing, distributing, or obtaining illegal drugs, alcohol, or other controlled substances. Sites that depict drug or alcohol paraphernalia and/or include methods for obtaining or manufacturing them. Does not include sites that provide information on prescription medications, except those sites that describe how to illegally obtain them.
 Email	Sites or resources that provide access to email services and applications.
 Employment/Career	Sites or resources that allow the posting of jobs or resumes. Sites that provide information on compensation in specific fields or regions. Sites that post information about jobs and job openings.
 Family Resources	Sites or resources that provide family counseling, family safety tips, parenting information and tips, and family planning.
 Financial/Stocks	Sites or resources that provide information about finances, financial planning, insurance, stock tickers, stock reports, or sites that allow the selling and purchasing of stock. Includes banks and credit unions and credit rating and reporting sites.
 Gambling	Sites or resources that allow a person to wager money on online games with the expectation of winning money or prizes. Sites that contain links to other gambling sites or provide information on gambling strategies or tactics.
 Games	Sites or resources that provide access to online or downloadable games or discussions about games. Sites that provide information about game cheats.
 Government	Sites or resources that are specific to local, state, or federal government organizations or agencies, including political party sites and specific, official political sites. Sites ending in “.gov”.
 Hate/Violence	Sites or resources that promote or depict violence against persons, animals, property, or nations. Sites that single out groups for violence based on race, religion, or creed.
 Health/Medicine	Sites or resources that deal with or provide information on mental or physical health issues. Sites that allow the online purchase of prescription medications.
 Illegal Activities	Sites or resources that provide information about the manufacture, alteration, or sales of weapons. Sites that promote or depict disorderly conduct or that provide information on the manufacture of explosives and explosive devices.
 Instructional	Sites or resources that contain instructional material, tutorials, or how-to pages.
 Intimate Apparel	Sites or resources that display models wearing underwear, lingerie, or other suggestive or see-through attire, including swimsuits.
 Kids	Sites or resources intended for children, including entertainment, education, crisis counseling, and kid-friendly communities.

Category	Description
 Music/Entertainment	Sites or resources that provide access to free downloadable or for-pay online music and video files such as MP3, WAV, MPG, and AVI. Sites that sell music or videos or that are dedicated to the music or entertainment industry. Sites that provide information on TV programs and programming, including movie review sites.
 News	Sites or resources that provide live, recorded, or written reports or editorials about current events.
 Other	Sites that do not fit into any of the existing ContentProtect Professional categories.
 Personals	Sites or resources that contain personal ads, personal info pages, and personal portals.
XXX Pornography	Sites or resources that are meant to sexually arouse the viewer. May show models or real people that are engaged in erotic behavior intended to cause sexual excitement. May describe sexually explicit activities or contain sexually explicit material including images, movies, or text. Sites could be considered X-rated.
 Religious	Sites that provide information on specific religions or religious beliefs. Regional religious organizational sites and sites built to promote religious groups, activities, and membership.
 Schools/Colleges	Sites or resources that contain information dealing with colleges, schools, seminars, or courses. Sites that end in ".edu".
 Search Engines/Portals	Sites or resources that provide mechanisms for searching the Internet by specific words or phrases and that display the results as either links or images. Sites that allow a user to customize the appearance or content of Web pages and that are geared to providing a "starting" place on the Internet.
 Shopping	Sites or resources that provide access to online malls, catalogs, or auctions, including classified ads. Department store sites, retail store sites, or sites that have coupons for free or discounted items.
 Sports	Sites that promote, advertise, report on, or are associated with sports teams, individuals, or organizations. Sites that are involved with fantasy sports. Sites for organizations whose main focus is to report on amateur, college, or professional sports.
 Travel	Online resources that provide information on travel, such as destination descriptions; ticketing and reservation sites; airline, bus, or train company sites; and car rental sites.
 Work Related	Sites that pertain to business-related activities.

Note: If you set Pornography to Block or Warn, ContentWatch Professional forces a "safe search" for as many search engines as it can. Currently, ContentWatch Professional can force a "safe search" for the following search engines: Yahoo!, Google*, AltaVista*, DogPile*, Lycos*, AllTheWeb*, and MSN. To bypass the safe search, you must either allow access to Pornography in the policy's settings or temporarily disable ContentProtect Professional via its system tray icon's right-click menu.

Name Settings

To change the name of the policy, type the desired name in the Policy Name field.

Allow Access To

These settings allow you to specify the services you want this policy to monitor. The following table describes the services you can select.

Table 3: Services to Allow

Option	Description
Web	URLs, normal “surfing” or “browsing”
Peer-to-Peer (P2P)	Peer-to-peer file sharing applications (for example, Gnutella, BitTorrent*, Kazaa*, eMule*, and eDonkey*)
News Groups	NNTP (standard news groups)
Instant Messaging	Google Talk, Yahoo!, AOL Instant Messenger* (AIM*), MSN, QQ

Allow Privileges

These settings allow you to specify privileges for users assigned to this policy. The following table describes the privileges you can select.

Table 4: Privileges to Allow

Option	Description
Administrator	<p>Gives administrative privileges to users assigned to this policy.</p> <p>Users with administrative privileges can change passwords, profile settings, and filters; configure email notifications; and access reporting and remote management.</p>
Override Blocked Messages	<p>Lets users override blocked content. If selected, ContentProtect Professional prompts the user for the override password when it blocks Internet content. (For an example of this message, see Block and Warning Messages on page 46.)</p> <p>Important: The user must enter the override password before ContentProtect Professional displays the blocked content. The override password is the same as the user’s login password for the ContentProtect Professional client.</p> <p>If you do not select this option, ContentProtect Professional displays a block message when the user tries to access blocked Internet content.</p>
Request Web Override	<p>Lets users submit requests to the ContentProtect Professional administrator to unblock or recategorize specific Web pages or entire Web sites that fall under a blocked category or a warning category in the Online Management application. (For examples of the messages displayed to users, see Block and Warning Messages on page 46. For information on how the administrator can respond to Web override requests, see Processing Web Override Requests on page 58.)</p>
Auto Client Login	<p>Prevents a login dialog from displaying each time the user accesses the Internet.</p> <p>When this option is selected, the user is asked to sign in to ContentProtect Professional only once. Until the user manually logs out, he or she remains logged into ContentProtect Professional, even if the computer is turned off and then restarted.</p>

Option	Description
Auto Windows Login	<p>Directs the ContentProtect Professional client to automatically log itself in if a user's Windows login name matches a name in the ContentProtect Professional user list.</p> <p>For example, if the Auto Windows Login option is selected and the user name "JohnD" exists in the ContentProtect user list, a user who logs in to Windows as "JohnD" is automatically signed in to ContentProtect without having to specify a ContentProtect user name and password.</p> <p>Note: When you select the Auto Windows Login option, Windows 2000 users are asked to sign in to ContentProtect Professional only once, in the same manner as they do with the Auto Client Login option. This is necessary to synchronize the users' Windows login information with their data in the ContentProtect Professional database.</p>

Allow Activity Reporting

These settings allow you to select the services you want ContentProtect Professional to keep activity logs on. ContentProtect Professional uses the logs to generate reports that show the online activities of every user that this policy is assigned to. The following table describes the services you can select.

Table 5: Services to Report On

Option	Description
Web	URLs, normal "surfing" or "browsing"
Instant Messaging	Google Talk, Yahoo!, AOL Instant Messenger (AIM), MSN, QQ

For more information on using reporting in ContentProtect Professional, see [Working with Reports](#) on page 48.

Configuring Time Controls

Time Controls allow you to manage the time of day and the amount of time that users can spend on the Internet. Time Controls can be set either by limiting the total number of hours a user can spend on the Internet over a given period, or by setting specific times (in 30-minute intervals) when Internet access is allowed or blocked.

Time Controls for "Standard User"

Time Allowance:

Enable: Hours / Day

Time Schedule:

Day: All Day

Start Time: :

End Time: :

Internet Access :

	Mon	Tue	Wed	Thu	Fri	Sat	Sun
00:00	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked
00:30	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked
01:00	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked
01:30	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked
02:00	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked
02:30	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked
03:00	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked
03:30	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked
04:00	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked
04:30	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
05:00	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
05:30	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
06:00	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
06:30	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
07:00	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
07:30	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
08:00	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
08:30	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
09:00	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
09:30	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
10:00	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
10:30	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
11:00	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
11:30	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
12:00	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
12:30	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
13:00	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
13:30	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
14:00	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
14:30	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
15:00	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
15:30	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
16:00	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
16:30	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
17:00	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
17:30	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
18:00	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
18:30	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
19:00	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
19:30	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
20:00	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
20:30	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
21:00	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
21:30	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
22:00	Allowed	Allowed	Allowed	Allowed	Blocked	Blocked	Blocked
22:30	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked
23:00	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked
23:30	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked	Blocked

Time Zone:

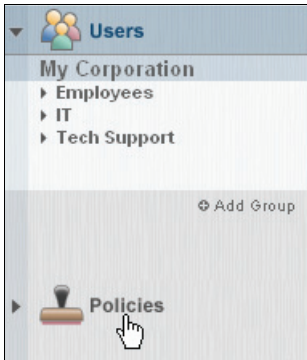
Apply:

By default, Internet access is allowed at all times. If you define a Time Control for a given policy, the restriction applies to all Internet activity such as Internet surfing, instant messaging, newsgroups, peer-to-peer, and network gaming.

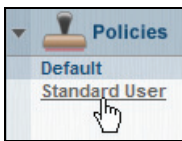
Setting up an Internet Access Schedule

To set up an Internet access schedule for a policy:

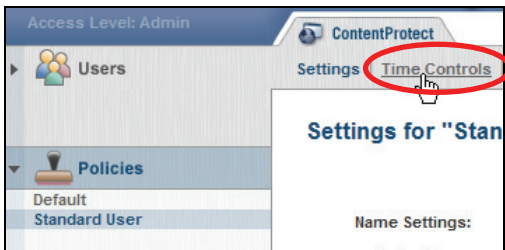
1. In the sidebar of the Online Management application, click **Policies**.



2. Click the policy that you want to set up a schedule for.



3. Click **Time Controls**.



4. If you want to limit the total number of hours a user can spend on the Internet over a day's or week's time:
 - a. Under Time Allowance, select **Enable**.
 - b. In the field to the right of the **Enable** checkbox, specify the amount of hours the user is allowed to access the Internet.
 - c. From the **Hours** drop-down menu, select the period (Day or Week) that the specified amount of hours applies to.
 - d. Click **Save Changes**.



5. If you want to set specific times when Internet access is allowed or blocked:
 - a. In the Day drop-down list, specify how often the schedule should be applied (**Daily**, **Weekdays**, **Weekends**, or individual days of the week).

Time Schedule:

Day: Daily All Day

Start Time: Daily

End Time: Weekdays

Internet Access: Monday

Save Changes

R
R

Note: To quickly apply a Block or Allow setting to all hours of the selected day or group of days, select the option **All Day**.

- b. From the Start Time drop-down lists, select the hour and half hour when the time control should begin; from the End Time drop-down lists, select the hour and half hour when the time control should end.

Time Schedule:

Day: Weekdays All Day

Start Time: 0 : 00

End Time: 0 : 00

Internet Access: 0

Save Changes

R
R

Mon Tue Wed Thu				Sun	Mon Tue	
00:00					12:00	
00:30					12:30	
01:00					13:00	
01:30					13:30	
02:00					14:00	
02:30					14:30	
03:00					15:00	
03:30					15:30	
04:00					16:00	

- c. From the Internet Access drop-down list, select whether to block or allow Internet access during the specified time block.

Time Schedule:

Day: Weekdays All Day

Start Time: 0 : 00

End Time: 4 : 30

Internet Access: Allowed

Save Changes

R

- d. Click **Save Changes** to save the time block settings.

Time Schedule:

Day: Weekdays All Day

Start Time: 0 : 00

End Time: 4 : 30

Internet Access: Blocked

Save Changes

e. Repeat Steps 5a-5d to set up additional time blocks as needed.

Note: To undo all changes you have made or to apply blanket settings to all hours:

- Click **Reset All to Allowed** to remove all time controls and allow Internet access at all times.
- Click **Reset All to Blocked** to completely block Internet access.

6. Under Time Zone, from the Apply drop-down list, select the time zone that applies to the users that this policy will be applied to, and then click **Save Changes**.

If your users are spread out over multiple time zones, you should group users according to their time zones and apply a different policy to each group. This helps ensure that ContentProtect Professional's time-dependent features (such as Time Controls) work correctly.

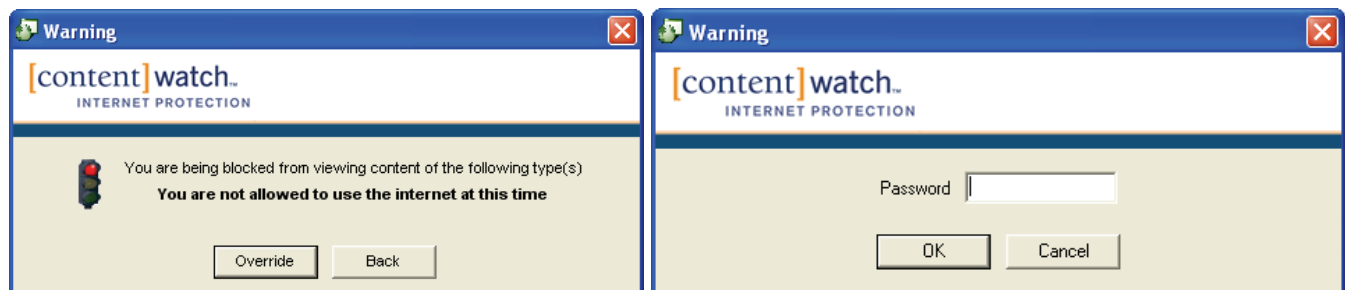
Time Zone:

Apply: (-07:00 GMT) Mountain Time (US & Canada)

Save Changes

Enforcing Internet Access Schedules

When a time control is in effect, ContentWatch displays a message when the user attempts to access the Internet. If a user has override privileges, the user can click **Override** and enter the override password to bypass the blocked connection. The password used to override time restrictions is the same as the user's client login password.



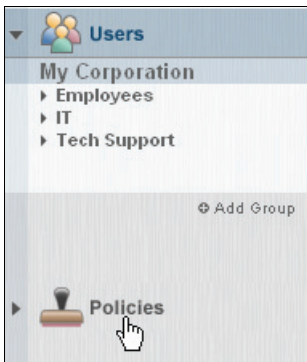
Note: To give a user override privileges, you must select the **Override Blocked Messages** option in the policy assigned to the user. For more information, see [Allow Privileges](#) on page 38.

If the user overrides the time control, Internet access is allowed for the next 30-minute block, after which the user must again override the blocked connection to maintain Internet access.

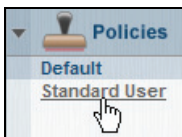
Denying or Allowing Access to Internet Applications and Games

To manage users' access to network applications and games:

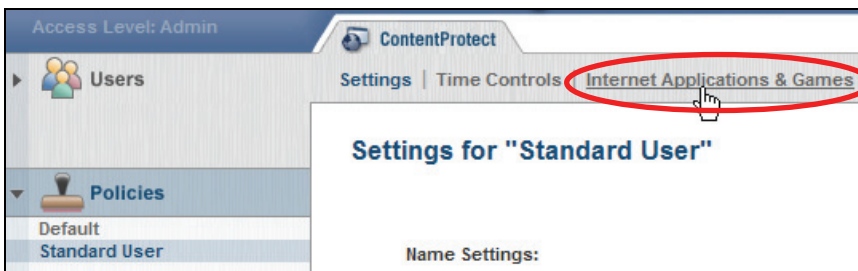
1. In the sidebar of the Online Management application, click **Policies**.



2. Click the policy you want to modify.



3. Click **Internet Applications & Games**.



4. Select the Internet applications you want to allow users to access, and deselect those you want to deny access to.



5. When you are finished, click **Save Changes**.

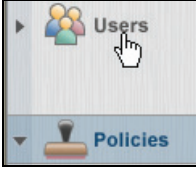
Note: The user must be allowed to access the Internet in order to have access to Internet games. For information on giving the user access to the Internet, see [Allow Access To](#) on page 38.

Assigning Policies

After you have configured a policy to meet your requirements, you are ready to assign it to the organization, groups, and users.

To assign a policy:

1. Click **Users**.

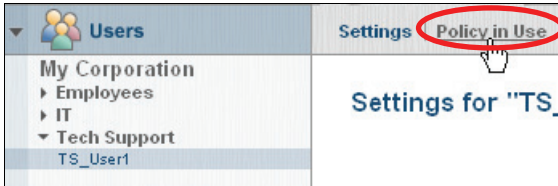


2. Click the object (organization, group, or user) you want to assign a policy to.

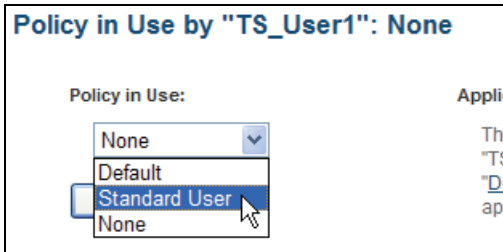


Note: See the introduction to [Managing Policies](#) on page 33 for details on how policy assignments affect groups and users.

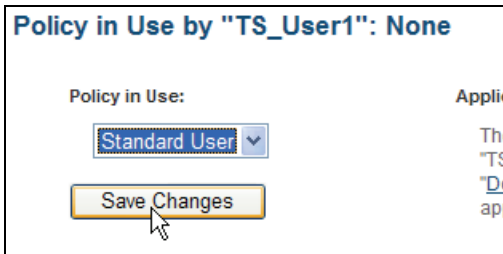
3. Click **Policy in Use**.



4. From the Policy in Use drop-down list, select the policy you want to apply.



5. Click **Save Changes**.



Block and Warning Messages

When you define policy settings, you determine what level of access users have to predefined Internet content categories. User access to these sites can be set to Allow, Warn, or Block.

The following are examples of the Block and Warning messages ContentProtect Professional displays when users access sites with a warning or blocked status.

Warning Messages

When a user attempts to connect to a site with a warning status, ContentProtect Professional notifies the user that the URL has a warning status, and it lists the site's associated content category:

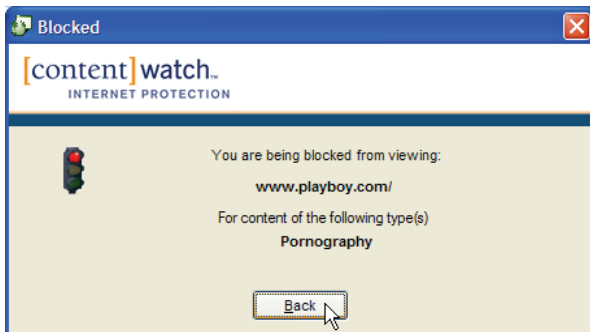


The user can click **Continue** to view the requested page or **Back** to return to the previous Web site.

The action is reported if activity reporting is enabled. For more information, see [Allow Activity Reporting](#) on page 39.

Block Messages

When a user attempts to connect to a site with a blocked status, ContentProtect Professional notifies the user that the URL is blocked, and it lists the site's associated content category:



The requested Web site does not open. The user can click **Back** to return to the previous Web site.

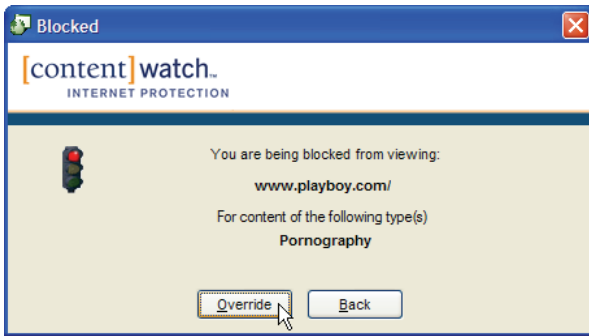
The action is reported if activity reporting is enabled. For more information, see [Allow Activity Reporting](#) on page 39.

Note: If you are routing your Internet traffic through the ContentProtect Professional Appliance, block messages are displayed in a Web page, as in the following illustration:



Block Messages with an Override Option

If a user has override privileges, ContentProtect Professional allows the user to override blocked content. ContentProtect Professional notifies the user that the URL is blocked, and it lists the site's associated content category:



The user can click **Override** to enter the override password and view the requested Web site, or the user can click **Back** to return to the previous Web site. For some Web sites, the user might need to enter the override password more than once to view the content.

Note: To give a user override privileges, you must select the **Override Blocked Messages** option in the policy assigned to the user. For more information, see [Allow Privileges](#) on page 38.

The action is reported if activity reporting is enabled. For more information, see [Allow Activity Reporting](#) on page 39.

Block or Warning Messages with Request Web Override Option

If a user has Request Web Override privileges, ContentProtect Professional lets the user submit requests to the ContentProtect Professional administrator to unblock or recategorize specific Web pages or entire Web sites that fall under a blocked or warning category:



To submit a Web Override Request, the user must perform the following in the Blocked or Warn dialog:

1. Click **Request Override** to display the Override Request dialog.
2. From the As drop-down list, select a suggested action (for example, allow the content or assign it to a new category).
3. From the For drop-down list, select whether the action is applied to the Web page alone or to the entire Web site.
4. Click **Send Request** to submit the request to a queue in the Online Management application, where the ContentProtect Professional administrator can choose to accept or reject the request.

For information on how the ContentProtect Professional administrator can process Web Override Requests, see [Processing Web Override Requests](#) on page 58.

Note: If the user who is preparing the Web Override Request has administrative privileges, he or she can click **Apply Now** (instead of **Send Request**) to immediately unblock or reclassify the Web page or Web site. The user is asked for the administrative user name and password, and then the settings are immediately updated in the policy applied to the user in the Online Management application. The next time the user visits the Web page or Web site, the new settings are in effect.

Note: To give a user Request Web Override privileges, you must select the **Request Web Override** option in the policy assigned to the user. For more information, see [Allow Privileges](#) on page 38.

The action is reported if activity reporting is enabled. For more information, see [Allow Activity Reporting](#) on page 39.

Working with Reports

The Online Management application can generate reports for Web and instant messaging activity. These reports allow the administrator to view Internet usage information for the overall organization, a single group, or an individual user.

Important: ContentWatch servers store activity data for up to 14 days.

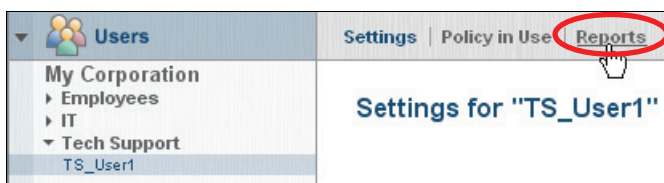
To view Internet usage reports:

1. Log in to the Online Management application.
2. Click the organizational level you want to view reports for.

For example, if you want to view a report for your overall organization, click the organization name. If you want to view a report for a specific user, drill down into the group where the user's account resides and click the user's account name.



3. Click **Reports**.



4. From the From and To drop-down lists, select the date range for the report.

Reports for "TS_User1"

Date Range:

From: November 1 '05

To: December 31 '05

Refresh

Charts: No Chart Available for Date Range

January
February
March
April
May
June
July
August
September
October
November
December

5. From the Report On drop-down list, select whether to report on **Web**, **IM** (instant messaging), or **Apps** (Application Management) data.

Reports for "TS_User1"

Date Range:

From: November 1 '05

To: November 30 '05

Refresh

Report On: Web

Hourly Wage: None

Charts: No Chart Available for Date Range

Print

6. You can select an approximate wage value (in increments of \$10) from the Hourly Wage drop-down list to display the dollar cost of users' Internet usage in the Detail sections of the report.

Reports for "TS_User1"

Date Range:

From: November 1 '05

To: November 31 '05

Refresh

Report On: Web

Hourly Wage: None

Charts: No Chart Available for Date Range

Print

None
\$10
\$20
\$30
\$40
\$50
\$60
\$70
\$80

7. Click **Refresh** to view the report.

Reports for "TS_User1"

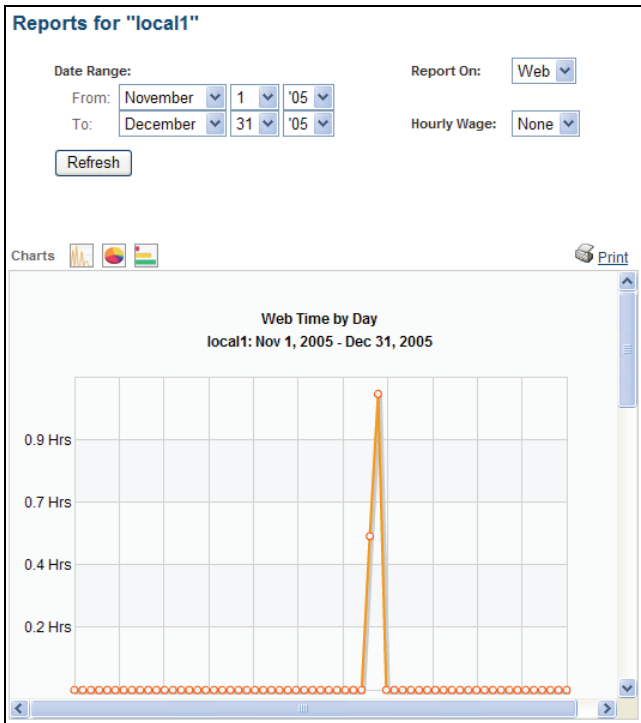
Date Range:




From: November

To: November

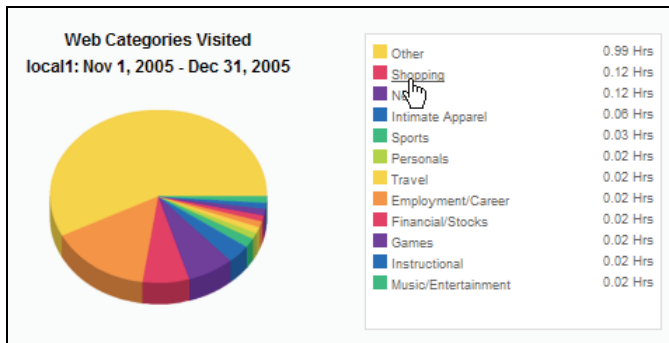
Refresh

If data is available for the date range you have selected, the report is displayed in a scrollable window on the Reports page.



Note: To view all the sections of the report, you must scroll down within the Report window. You can also click the icons    above the Charts window to quickly jump to the corresponding chart.

All of the charts within the report have drill-down capability for further detail. Selecting a clickable category or value generates additional charts that report transaction details:



Reports for "local1"

Date Range: From: To:

Report On: Hourly Wage:

Charts > Web Category User Detail: Shopping

Web Address	Count	Duration (min)
foq.imageq.net/images/cart_icon.gif	2	0.03
shopping.yahoo.com/	5	5.4
www.amazon.com/	1	0.08
www.fox.bg.com/checkout/index.jsp?o=1769167594&c=259478463	1	0.6
www.zdnet.com/	1	1.12
Total	10	7.23

Note that you also have the option of exporting report details. Information is exported as a comma-separated value (CSV) file that can be viewed in programs such as Microsoft Excel*. You can also print reports.



Note on Application Management reports: ContentProtect Professional gathers report data only for applications that have a "Block" or "Warn" action assigned to them. ContentProtect Professional does not gather report data for allowed applications or for applications classified as "Not Used" in a policy. For more information on managing applications, see [Controlling Users' Access to Applications](#) on page 59.

Setting Up Notifications

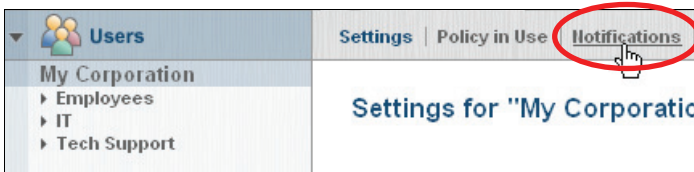
Email notifications can be sent to the administrator or others to provide alerts about users who are blocked, warned, or who override blocks.

To configure email notifications:

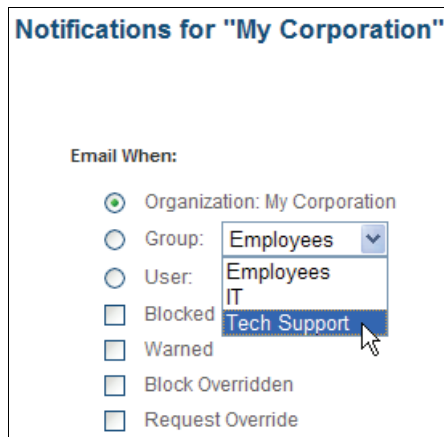
1. Log in to the Online Management application.
2. Make sure your organization's name is selected.



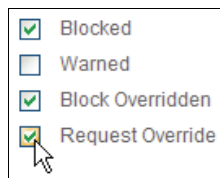
3. Click **Notifications**.



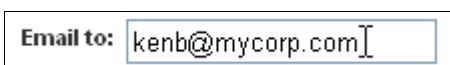
4. Set the conditions for sending notifications.
 - a. Select the organizational level you want to be notified about (**Organization, Group, or User**). If you select **Group** or **User**, select the desired group or user in the accompanying drop-down list.



- b. Select the events you want to be notified about (**Blocked, Warned, Block Overridden, or Request Override**).



5. In the Email To field, type the Email address where you want notification messages to be sent.



- Click **Add**.

Notifications for "My Corporation"

Email When:

Organization: My Corporation

Group: **Tech Support** ▼

User: **Admin** ▼

Blocked

Warned

Block Overridden

Request Override

Email to:

Add

The notification profile is added to the Current Notifications list.

Current Notifications:

Email When	Blocked	Warned	Block Overridden	Request Override	Email to	Delete
Tech Support (Group)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	kenb@mycorp.com	<input type="checkbox"/>
TS_User1 (User)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	kenb@mycorp.com	<input type="checkbox"/>

- Repeat Steps 4-6 for each notification profile you want to add to the Current Notifications list.
- To remove a notification, select **Delete** for the notification in the Current Notifications list.

Current Notifications:

Email When	Blocked	Warned	Block Overridden	Request Override	Email to	Delete
Tech Support (Group)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	kenb@mycorp.com	<input type="checkbox"/>
TS_User1 (User)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	kenb@mycorp.com	<input checked="" type="checkbox"/>

- When you are finished setting up notification profiles, click **Save Changes**.

Current Notifications:

Email When	Blocked	Warned	Block Overridden	Request Override	Email to	Delete
Tech Support (Group)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	kenb@mycorp.com	<input type="checkbox"/>
TS_User1 (User)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	kenb@mycorp.com	<input checked="" type="checkbox"/>

Save Changes

Defining Web Overrides

When a user enters a URL address in a browser, ContentProtect Professional processes the requested page to determine which content category it belongs to. However, administrators can bypass this default process by manually allowing or blocking a specific site, or the administrator can assign a URL to a predefined content category so the policy settings (Allow, Warn, or Block) for that category are then applied to the Web site.

Note: See [Content Categories](#) on page 36 for a list of the predefined content categories.

To illustrate this point, let's consider the following example:

There is a community resource section accessible through the ContentWatch Web site. Because this section contains many educational articles that deal with the problems caused by pornography (and which, therefore, contain some adult content), a normal filter (including ContentProtect Professional) blocks this site as pornography. After going to the site and examining the content, it is clear that the site is not pornographic, and the administrator may wish to allow this site.

Let's assume you want to allow the URL www.contentwatch.com. You need to enter the URL www.contentwatch.com on the Web Overrides page in the Online Management application and select the Family Resources content category. The site is now categorized as a Family Resources site, and access is allowed.

Note: To be sure that this site is allowed under Family Resources, the administrator must verify that the Family Resources category is set to Allow in the policy assigned to the organization.

Warning: If the administrator manually assigns a site's content category, the system bypasses all automated site analysis. This means that as the site's content changes, ContentProtect Professional cannot determine the new category for the site. Use the Web Override feature with care.

To define a Web Override:

1. Log in to the Online Management application.
2. Make sure your organization's name is selected.



3. Click **Web Overrides**.



4. In the Web Address field, type the URL of the site you want to create an override for.



Note: You can copy the URL from your browser and paste it in the Web Address field for accuracy.

- From the Change To drop-down list, do one of the following:
 - Select **Allow** to always allow the site.
 - Select **Block** to always block the site.
 - Select a content category to apply to the site.

Web Overrides for "My Corporation"

Web Address:

Change to:

Apply Rule To:

Web Address	Override Action	Delete
	Allow	<input type="checkbox"/>
	Block	<input type="checkbox"/>
	Ads	<input type="checkbox"/>
	Adult/Mature	<input type="checkbox"/>
	Chat Site	<input type="checkbox"/>
	Drugs/Alcohol	<input type="checkbox"/>
	Email	<input type="checkbox"/>
	Employment/Career	<input type="checkbox"/>
	Family Resources	<input type="checkbox"/>
	Financial/Stocks	<input type="checkbox"/>
	Gambling	<input type="checkbox"/>
	Games	<input type="checkbox"/>

- From the Apply Rule To drop-down list, select whether the override applies to the entire Web site or just the default page at the address you specified.

Web Overrides for "My Corporation"

Web Address:

Change to:

Apply Rule To:

Web Address	Override Action	Delete
	Entire Website	<input type="checkbox"/>
	Entire Website	<input type="checkbox"/>
	Specific Web Page	<input type="checkbox"/>

- Click **Add**.

The URL is added to the override list, along with a description of its associated override action.

Web Overrides for "My Corporation"

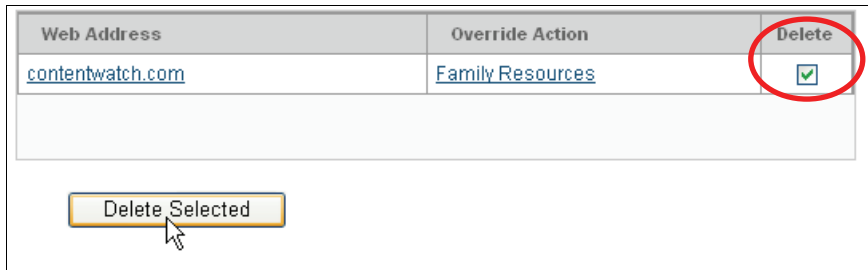
Web Address:

Change to:

Apply Rule To:

Web Address	Override Action	Delete
contentwatch.com	Family Resources	<input type="checkbox"/>

8. To delete a Web Override, select **Delete** for the specific override and then click **Delete Selected**.



Adding Applications to the Bypass List

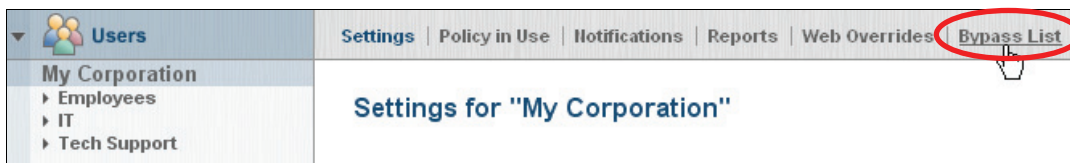
The ContentProtect Professional bypass list helps you work around conflicts that may arise between ContentProtect Professional and other Internet-enabled software on users' systems. For example, ContentProtect Professional may block some applications that require Internet access, such as financial software. You can add such applications to the bypass list so that ContentProtect Professional does not interfere with them when they try to access the Internet.

To add an application to the bypass list:

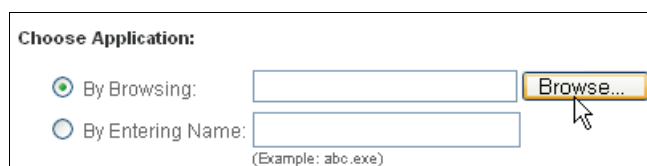
1. Log in to the Online Management application.
2. Make sure your organization's name is selected.



3. Click **Bypass List**.



4. Select a method for locating the application executable you want to add to the bypass list:
 - *Method 1:* Browse to the application executable.
 - a. Select the **By Browsing** option.
 - b. Click **Browse**.



- c. Browse to the location of the application's executable file (<file name>.exe) on your computer's hard drive.
- d. Select the file and click **Open**.

- e. When the executable's full filename (including the local path to the file) appears in the **By Browsing** field, click **Add** to add the application to the bypass list.

Choose Application:

By Browsing: C:\Program Files\QuickBoo Browse...

By Entering Name:
(Example: abc.exe)

Add

- **Method 2:** Enter the filename of the application's executable file.
 - a. Select the **By Entering Name** option.
 - b. In the accompanying field, type the exact filename of the application's executable file.
 - c. Click **Add** to add the application to the bypass list.

Choose Application:

By Browsing: Browse...

By Entering Name: qbx32.exe
(Example: abc.exe)

Add

5. If you want to remove an application from the bypass list:
- a. In the bypass list, Select the executable's **Delete** check box.
 - b. Click **Delete Selected**.

Application	Delete
qbx32.exe	<input checked="" type="checkbox"/>

Delete Selected

Processing Web Override Requests

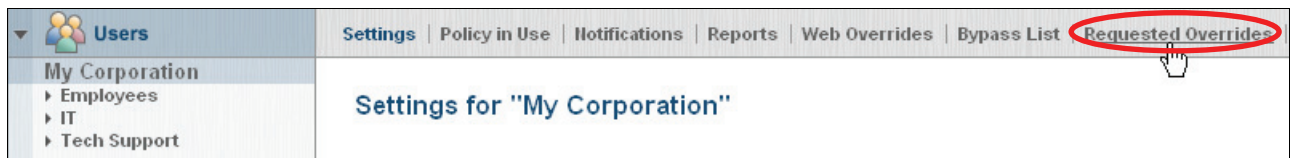
Users who have been granted Web Override Request privileges can submit requests to the ContentProtect Professional administrator to unblock or recategorize specific Web pages or entire Web sites that fall under a blocked or warning category. The administrator can review these requests in the Online Management application and decide on a case-by-case basis which requests to accept or reject.

To process Web Override Requests:

1. Log in to the Online Management application.
2. Make sure your organization's name is selected.



3. Click **Requested Overrides**.



4. Review the list of requests, such as who sent the requests, which Web addresses they are making the requests about, and what actions they are proposing.

You can click the hyperlinks in the Web Address column to open requested Web sites in a browser and review their content. Also, before accepting a request, you can change the action or category the user has requested by selecting a different option in the appropriate Requested Action drop-down list.

Select	Sender	Web Address	Current Action	Requested Action
<input type="checkbox"/>	TS_User1	cnn.com	News	Allow <input type="button" value="v"/>
<input type="checkbox"/>	TS_User1	amazon.com	Shopping	Allow <input type="button" value="v"/>
<input type="checkbox"/>	user1	newegg.com	Shopping	Allow <input type="button" value="v"/>

Accept Selected Reject Selected

5. To process a request:
 - a. Select the request's **Select** check box.

Select	Sender	Web Address	Current Action	Requested Action
<input type="checkbox"/>	TS_User1	cnn.com	News	Allow <input type="button" value="v"/>
<input type="checkbox"/>	TS_User1	amazon.com	Shopping	Allow <input type="button" value="v"/>
<input checked="" type="checkbox"/>	user1	newegg.com	Shopping	Allow <input type="button" value="v"/>

Accept Selected Reject Selected

- b. Click **Accept Selected** or **Reject Selected**.

The new settings take effect immediately. All accepted requests are added to the Web Overrides list.

Select	Sender	Web Address	Current Action	Requested Action
<input type="checkbox"/>	TS_User1	cnn.com	News	Allow ▼
<input type="checkbox"/>	TS_User1	amazon.com	Shopping	Allow ▼
<input checked="" type="checkbox"/>	user1	newegg.com	Shopping	Allow ▼

Controlling Users' Access to Applications

The ContentProtect Professional Suite Application Manager feature lets you control which applications users can run on their desktop computers. Since employees nowadays can easily install applications that may present security threats, Application Manager enhances your corporate security and compliance by controlling users' ability to run such applications.

Adding Applications to the Application Management List

To add applications to the Application Management table:

1. In the Online Management Application, make sure your organization's name is selected.



2. Click **Application Manager**.



3. Select a method for locating the executable for the application you want to manage:

- **Method 1:** Browse to the application executable.
 - a. Select the **By Browsing** option.
 - b. Click **Browse**.

Choose Application:

By Browsing:

By Entering Name:

(Example: abc.exe)

- c. Browse to the location of the application's executable file (<file name>.exe) on your computer's hard drive.

- d. Select the file and click **Open**.
- e. When the executable's full filename (including the local path to the file) appears in the **By Browsing** field, click **Add** to add the application to the Application Management table.

- **Method 2:** Enter the filename of the application's executable file.
 - a. Select the **By Entering Name** option.
 - b. In the accompanying field, type the application's internal name (not simply the filename of the application's executable).

For example, "freecell.exe" is the filename of the executable for the FreeCell game in Windows XP. The game's internal name, however, is "freecell", and this is the name that must be entered in the By Entering Name field to block this application. The easiest way to find an application's internal name is to right-click the application's executable file, select **Properties**, click the Version tab, and then select **Internal Name** from the Item Name list.

- c. Click **Add** to add the application to the Application Management table.

4. If you want to remove an application from the Application Management table:
 - a. In the Application Management table, select the application's **Delete** check box.
 - b. Click **Delete Selected**.

Application	Delete
freecell	<input checked="" type="checkbox"/>

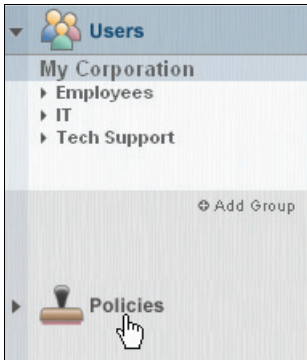
Delete Selected

Editing Policies for Application Management

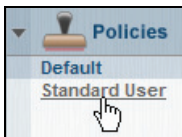
Once you have added programs to the Application Management table, you can control users' access to these programs by modifying Application Manager settings in your policies.

To modify Application Manager settings for a policy:

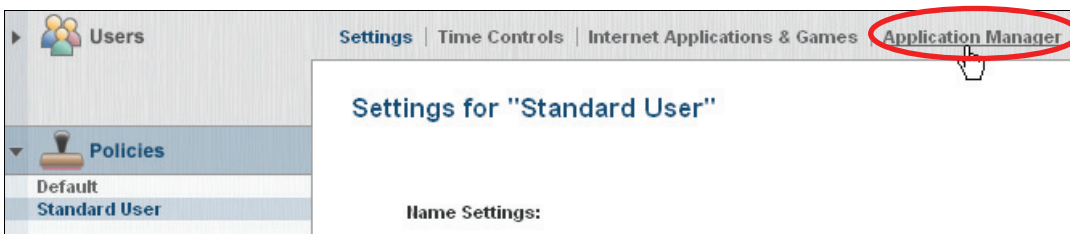
1. In the sidebar of the Online Management application, click **Policies**.



2. Click the policy you want to modify.

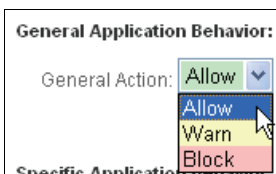


3. Click **Application Manager**.



4. Under General Application Behavior, from the General Action drop-down list, select how you want ContentProtect Professional to handle applications that are *not* included in the Application Management table (**Allow**, **Warn**, or **Block**).

If you select **Allow**, you create, in effect, a white list of all allowed applications. If you select **Block**, you essentially create a black list of all the applications you want to block.



5. In the Specific Application Behavior table, from the Action drop-down lists next to each displayed application, select how you want ContentProtect Professional to respond when a user attempts to run that application (**Not Used**, **Allow**, **Warn**, or **Block**).

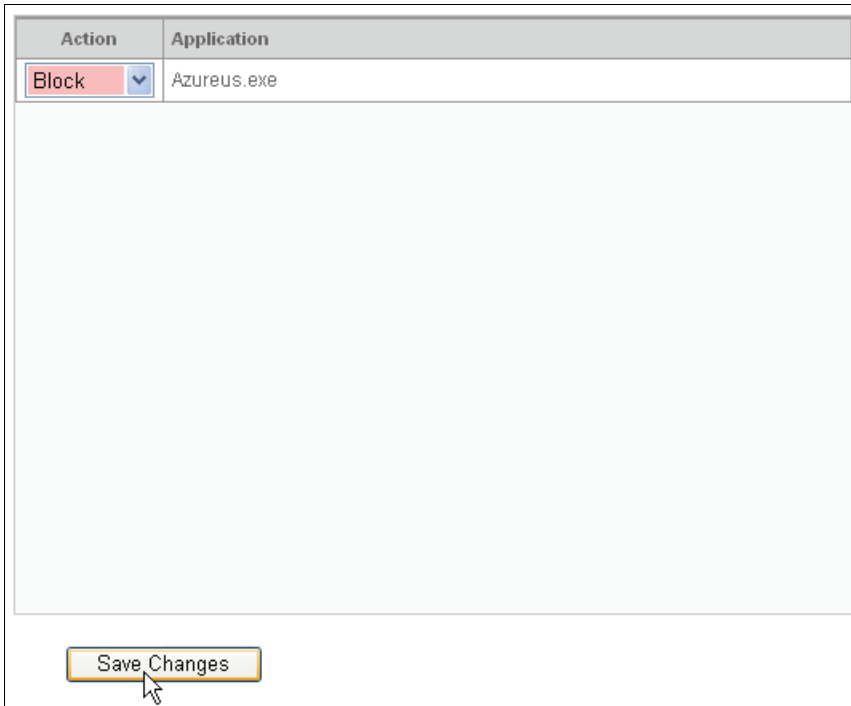
Note: The **Not Used** option indicates that the application is not considered in this policy; therefore, the general action will be applied to this application.

Action	Application
Allow	Azureus.exe



6. When you are finished setting the actions for each application in the table, click **Save Changes**.

Action	Application
Block	Azureus.exe



Protecting Users' Privacy

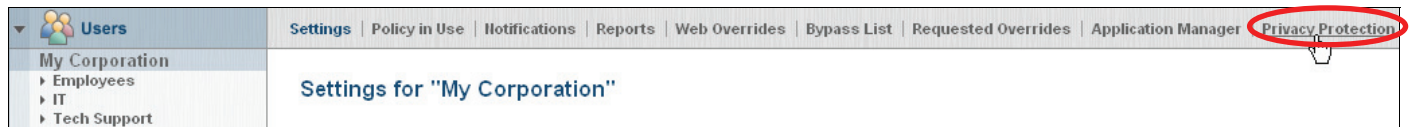
The ContentProtect Professional Suite Privacy Protection feature, which is built on CallingID's anti-phishing and privacy protection technology, helps protect users against phishing Web sites as well as any type of Web site that may put users' sensitive personal information at risk. When a user attempts to access a Web site, Privacy Protection determines whether the site is blacklisted as a known phishing site or is hosted in a suspect country, whether the site's owner is hiding his or her identity, etc.

To configure Privacy Protection for your organization:

1. In the Online Management Application, make sure your organization's name is selected.



2. Click **Privacy Protection**.



3. Under Warning Message, specify how ContentProtect Professional should respond when it detects suspicious Web sites.
 - a. From the High Risk drop-down list, select the type of message that ContentProtect Professional should display when it detects a Web site that poses a high risk for compromising users' personal information.

None: Do not display a message.

Large: Display a message box similar to the standard "block" dialogs ContentProtect Professional shows when a user attempts to access a blocked Web site. Users must click **OK** in the message box to make it disappear.

Small: Display a small pop-up message box in the system tray that disappears by itself after several seconds.
 - b. From the Low Risk drop-down list, select the type of message (**None**, **Large**, or **Small**) that ContentProtect Professional should display when it detects a Web site that poses a lower risk for compromising users' personal information.
4. Click **Save Changes**.





The ContentProtect Professional Appliance (CPS-1000)

The ContentProtect Professional Appliance is a dedicated inline Internet filtering appliance that manages end user access to Internet-based content. It is a plug-and-play, low maintenance, rack-mountable appliance.

The appliance allows you to easily customize ContentProtect settings to fit the needs of each employee in your organization, of separate groups and departments, or of all systems company-wide. Powerful reporting tools enable administrators to review where employees are spending their time online. You can customize ContentProtect filter settings to block specific Web sites, domains, or chat rooms, helping you increase employee productivity, reduce risk, and preserve the network resources within your organization.

For organizations with a mobile workforce or remote offices, the ContentProtect Professional Appliance works hand-in-hand with the client version of ContentProtect Professional, offering users “end-to-end protection.” Intelligent filtering detection means no double filtering if client software is loaded when the client is attached to the corporate network. If the client detects that the appliance is filtering the network, it automatically turns itself off.

Note: The ContentProtect Professional Appliance is limited to enforcing time controls and blocking access to sites that fall under the “Block” or “Warn” classifications in ContentProtect Professional’s category settings. The appliance does not currently support other access control features of ContentProtect Professional such as Internet applications and games, safe search, peer-to-peer, newsgroups, and instant messaging.

Setting Up the Appliance

1. Register your organization.

IMPORTANT: Before you configure and activate the ContentProtect Professional Appliance (CPS-1000), you must first register your organization using your registration number. When you first purchase the CPS-1000, ContentWatch sends an email containing your registration number and instructions for registering your organization. For more information on the registration process, see [Registering ContentProtect Professional](#) on page 7. If you have any further questions, please contact your ContentWatch sales representative.

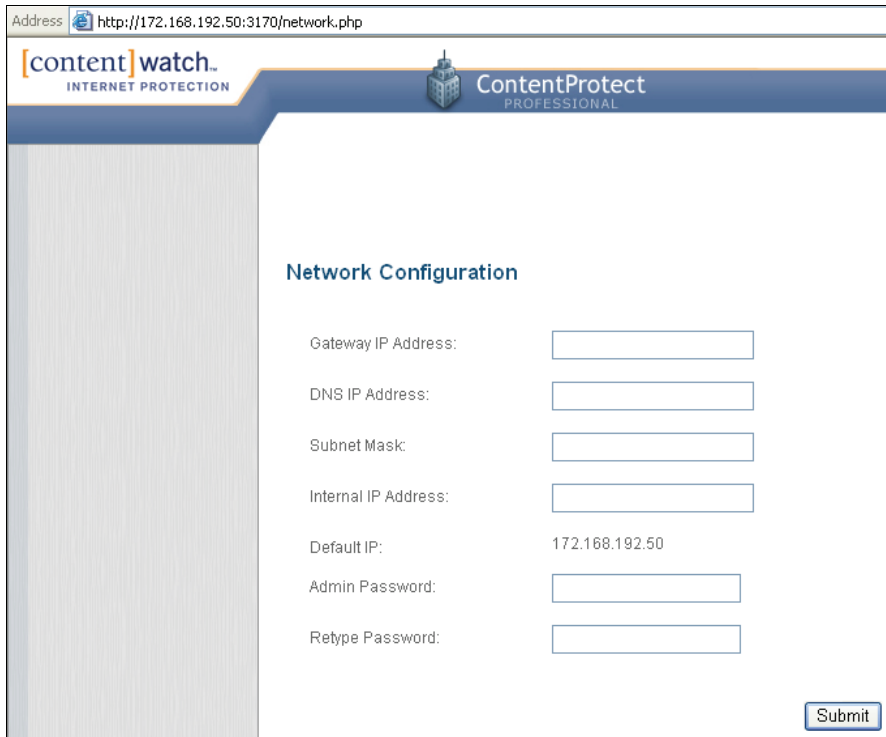
2. Carefully unpack the CPS-1000 from the box.
3. Attach the power cord to the CPS-1000 and plug it in.
4. Press the power button to turn on the CPS-1000.
5. Connect an Ethernet cable from the LAN port of the CPS-1000 to a computer that you can use to configure the appliance.

Note: The computer must have a standard Internet browser installed.

6. Configure the computer connected to the CPS-1000 with an IP address of 172.168.192.49 and a subnet mask of 255.255.255.252.

Note: Refer to your operating system’s documentation for instructions on how to change the computer’s IP address and subnet mask.

7. Using a Web browser open <http://172.168.192.50:3170>.



Address <http://172.168.192.50:3170/network.php>

[content] watch.
INTERNET PROTECTION

ContentProtect
PROFESSIONAL

Network Configuration

Gateway IP Address:

DNS IP Address:

Subnet Mask:

Internal IP Address:

Default IP: 172.168.192.50

Admin Password:

Retype Password:

If the page does not load immediately, wait a few seconds and refresh the browser.

8. Enter the following information as it pertains to your network:

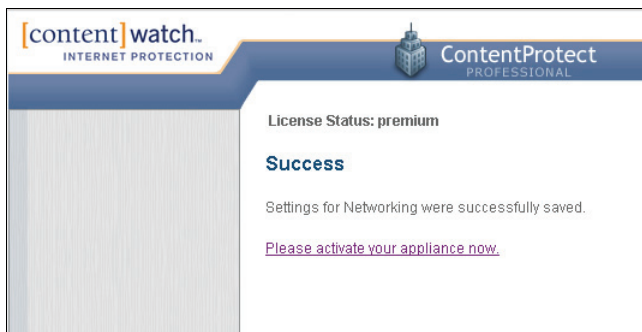
- Gateway IP address
- DNS IP address
- Subnet mask
- Internal IP address

If you do not know these values, consult your network administrator.

9. Type and confirm your Admin Password.

10. Click **Submit**.

The CPS-1000 saves the settings and returns a confirmation.



[content] watch.
INTERNET PROTECTION

ContentProtect
PROFESSIONAL

License Status: premium

Success

Settings for Networking were successfully saved.

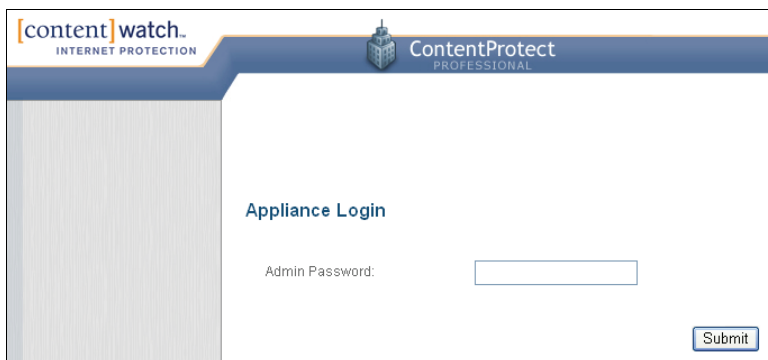
[Please activate your appliance now.](#)

IMPORTANT: Do not click the link to activate your appliance at this time. You will activate the appliance at the end of this procedure. The purpose of the activation link is to enable you to update the appliance's network configuration after you have completed the initial activation. When you activate the appliance for the first time, a snapshot of the appliance configuration is sent to a ContentWatch database. After initial activation, whenever you make changes to the appliance configuration, you must click the activation link to update the appliance's configuration snapshot in the ContentWatch database.

11. Disconnect the computer from the CPS-1000.
12. Connect an Ethernet cable from the WAN port of the CPS-1000 to your Internet gateway or router.
13. Connect an Ethernet cable from the LAN port of the CPS-1000 to your local area network switch or hub.
14. From a computer that is on your LAN, open a browser and connect to `http://<internal_IP_address_of_the_CPS-1000>:3170`.

Important: If you connect to the LAN using the same computer that you used to configure the CPS-1000, you must reconfigure the computer's IP address and subnet mask to your LAN settings.

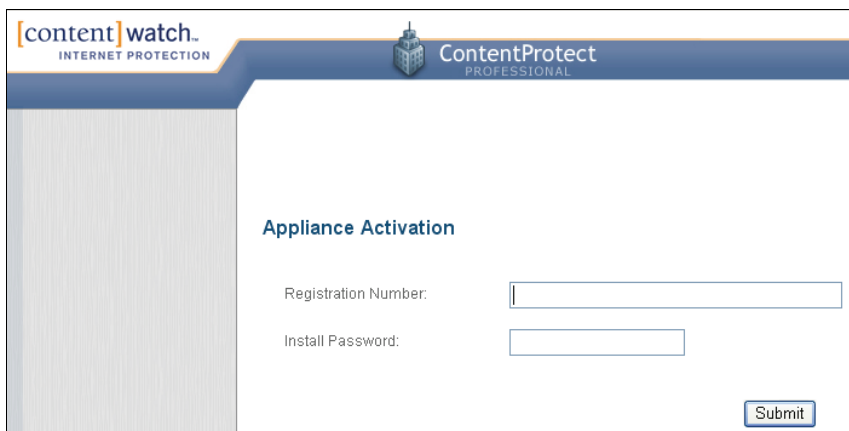
15. Type the Admin Password and then click **Submit**.



The screenshot shows the 'Appliance Login' page of the ContentProtect Professional web interface. The page has a blue header with the 'content watch.' logo on the left and 'ContentProtect PROFESSIONAL' on the right. The main content area is white and contains the text 'Appliance Login' in blue. Below this, there is a label 'Admin Password:' followed by a single-line text input field. At the bottom right of the form area, there is a blue 'Submit' button.

16. Type the appliance Registration Number and the install password you created when you registered your organization.

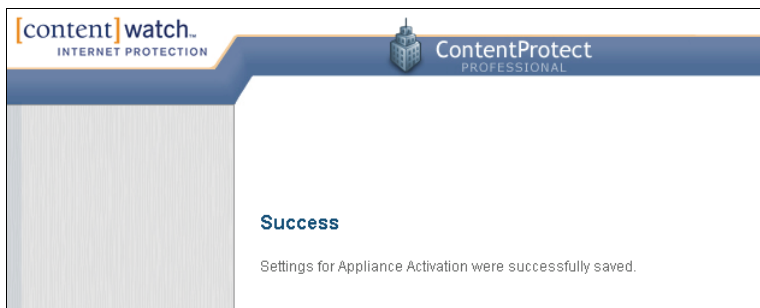
IMPORTANT: You must register your organization before you activate the CPS-1000. When you first purchase the ContentProtect Professional Appliance (CPS-1000), ContentWatch sends an email containing your registration number and instructions for registering your organization. If you have any questions, contact your ContentWatch sales representative.



The screenshot shows the 'Appliance Activation' page of the ContentProtect Professional web interface. The page has a blue header with the 'content watch.' logo on the left and 'ContentProtect PROFESSIONAL' on the right. The main content area is white and contains the text 'Appliance Activation' in blue. Below this, there are two labels: 'Registration Number:' followed by a single-line text input field, and 'Install Password:' followed by a single-line text input field. At the bottom right of the form area, there is a blue 'Submit' button.

17. Click **Submit**.

The CPS-1000 device is activated.



18. (Optional) Configure your organization's Internet usage policy at the appliance management page (<https://pro.contentwatch.com>).

For information on configuring usage policies, see [Managing Policies](#) on page 33.

19. To ensure the CPS-1000 is working correctly, go to any machine that accesses the Internet through this device and ensure that you can browse to a page on the Internet.

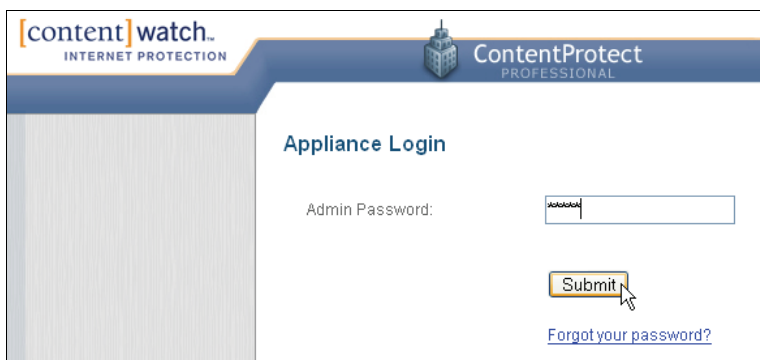
If you encounter any problems, contact ContentWatch Support at support@contentwatch.com or 1-800-485-4008.

Maintaining the Appliance

You can perform maintenance tasks on the CPS-1000 Appliance from the Management Console.

To access the Management Console:

1. From a computer that is on your LAN, open a browser and connect to http://<internal_IP_address_of_the_CPS-1000>:3170.
2. On the Appliance Login page, type the Admin password and click **Submit**.

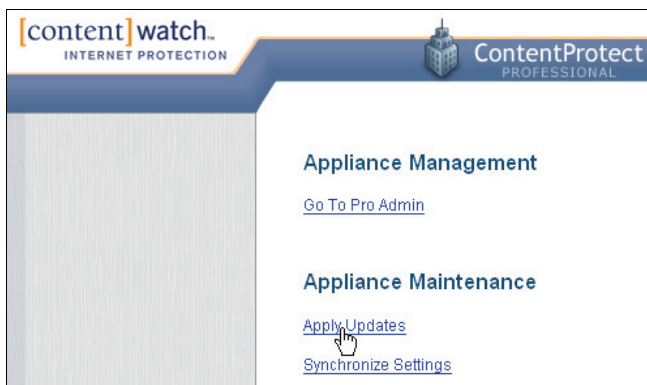


The Management Console page displays.

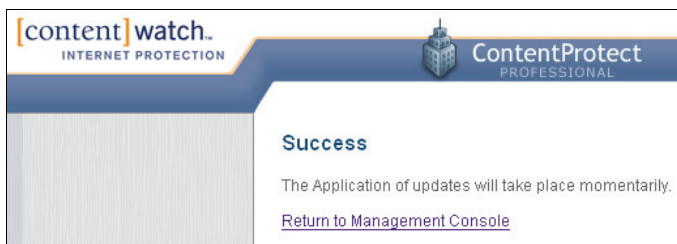


From the Management Console, you can access the ContentProtect Professional Online Management Application or perform a variety of appliance maintenance tasks.

3. To perform a maintenance task, click the desired task's hyperlink.



You are informed whether or not the task was successfully launched.



4. To return to the main Management Console page, click **Return to Management Console**.

The following table describes the maintenance tasks you can perform:

Table 6: Appliance Maintenance Tasks

Task	Description
Apply Updates	Checks for and applies updates to the CPS-1000 Appliance software.
Synchronize Settings	Synchronizes the data stored on the appliance with the data stored on the ContentWatch relay server. This task accomplishes the same thing as selecting Refresh Profiles from the ContentProtect Professional client quick menu.
Change Admin Password	Lets you change the login password for the Appliance Management Console.
Reset Filter	Deletes filter settings stored in the appliance's database and then synchronizes the appliance's database with the filter settings stored on the ContentWatch relay server. During this process, the appliance blocks Web traffic and displays a page indicating that the appliance is performing maintenance.
Change Network Settings	Lets you change the Gateway IP Address, DNS IP Address, Subnet Mask, Internal IP Address, and Admin Password settings for the appliance.
Reset Appliance to Factory Defaults	Resets all appliance settings to their default status; all custom changes to settings are lost. When you reset the appliance to factory defaults, you must run through the appliance setup process again and reactivate the device (see Setting Up the Appliance on page 64 for instructions).
Turn on/off Remote Assistance	Remote Assistance allows ContentWatch support technicians to access the CPS-1000 Appliance when resolving issues. To avoid creating a security hole on your network, you should turn on Remote Assistance only when you are on the phone with a support technician working through an issue. Remember to turn off Remote Assistance once the support representative no longer needs access to the appliance. Note: Remote Assistance uses SSH and may require that the network admin provide SSH access to the appliance through the corporate firewall.



Glossary

Administrative Privileges: Access rights that give a user the same level of access as an administrator.

Administrator: Person who is responsible for setting up and maintaining a group of users. Duties of the administrator include installing ContentProtect, setting up and managing user profiles, and assigning passwords and privileges.

Application: Software, program, or tool used on a computer, such as a word processor, game, or email program.

Browser: The application that lets you navigate around and view pages on the Web. Netscape and Internet Explorer are the two most common.

Category: General term for a whole topic or information type.

Client-Based Filtering: Filtering that is performed from an individual computer. Filtering software and a list of categorized sites are stored on an individual computer, which makes filtering more flexible for the user making decisions about acceptable content. Aside from restricting Internet access to certain Web sites, many client-based filters also offer controls for other Internet services.

Default Settings: A setting that a program is preset to select (usually the recommended settings) if you do not specify other options.

Drill Down: To move from a summary of information to more detailed data. To drill down through a series of reports addressing more detail at each level.

Filtering: Controlling access to a Web page request by analyzing the incoming and outgoing requests and letting them pass or stopping them based on settings selected within ContentProtect.

Guest Profile: A single, generic, limited profile set up for visitors and friends to use.

Hacker: Slang term for an individual who tries to gain unauthorized access to computer systems for the purpose of stealing or corrupting data.

Help: Online documentation. Many programs come with the instructional manual, or a portion of the manual, integrated into the program. If you encounter a problem or forget a command while running the program, you can access help documentation by selecting Help from the Menu bar and then clicking a topic.

Icon: A small picture that represents an object or program.

Instant Messaging: Real-time communication. Typed conversation that is received almost instantly as soon as it is sent. Talking live with one or more people via the Internet. It's like a telephone party line, except you type instead of talk.

Internet: Countless networks of computers that are connected together across the world allowing millions of people to share information. Components of the Internet include the World Wide Web, newsgroups, instant message rooms, and email.

Log: Program or system that enters a record into a log file or report file.

Peer-to-Peer: Type of network that exists on the Internet which allows users to have access to other users' files residing on their hard disks. ContentProtect currently blocks peer-to-peer activity only on the Gnutella network.

Portable User Profiles: Allows a user to install the filter on more than one computer and have settings transferred automatically. This is very useful for multiple-computer households or in a situation where a computer breaks down or is outdated and needs to be replaced.

Remote Management: Capability of accessing files, devices, and other resources not connected directly to your workstation. In the case of ContentProtect, reviewing report results and managing user profiles can be performed from any computer having Internet access.

Screen Name: Identifier that consists of a sequence of one or more alpha or numeric characters that uniquely identifies a person.

Server-Based Categorization and Validation: Method of content filtering in which a list of categorized URLs is maintained on a server and the server is updated regularly to ensure that all users are getting the most up-to-date, accurate information. The server does not actually deliver the requested Web page (URL) to the customer but compares the requested URL to the list. ContentProtect uses this content filtering method.

Shortcut Menu: Pop-up menu that appears by right-clicking an object. When left-clicking once or right-clicking the ContentProtect icon from the System Tray located in the Taskbar, the same pop-up menu is displayed.

System Tray: Located on the Windows Taskbar (usually at the bottom next to the clock). Contains miniature icons for easy access to system functions such as fax, printer, modem, volume, etc.

Taskbar: System bar located at the bottom of the computer screen. Home base for the Start button, system clock, system tray, etc.

Transaction Detail: Activity information based on report results.

Tutorial: Interactive multimedia presentation that explains program features.

URL: (Universal Resource Locator) Internet address that shows the specific path to a site or a document online. The URL for a Web page looks like this: <http://www.domain name/folder name/filename>

User: Individual who uses a computer.

User ID: Identifier that distinguishes a specific user in a program.

User Profile: Program settings that are specific to an individual user.

World Wide Web: (WWW) The visual component of the Internet. Created with HTML language, Web pages can include text, pictures, sound clips, video, links for downloading software, and much more. The Web is only one component of the Internet, although the terms are often (and mistakenly) interchanged.

Web-Based Reporting: Reports that compile Web and instant message activity for a ContentProtect family and are accessible from any computer with Internet access (when enabled by the administrator).



Frequently Asked Questions (FAQ)

Does ContentProtect work with firewalls?

ContentProtect™ is compatible with most popular, commercially available firewall software. Call Customer Support if you are having problems.

I have problems starting Yahoo Messenger after installing ContentProtect Professional. What do I do?

In Yahoo Messenger, open the Preferences section and select the Connection category. Make sure that connection is set to **Firewall with no proxies**. You should then be able to connect.

What if I forget my administrator password?

If you forget the Admin password, you must do one of the following:

- If you have more than one administrator account, another administrator can change your password for you by logging in to the Online Management application, selecting your user account, and changing the password in the Settings area.
- At the login screen of the Online Management application:
 - a. Click **Forgot Password**.
 - b. When prompted, provide the email address you used to register the product and click **Send**.
 - c. At the address specified, check your email for a message from ContentWatch with the subject "Requested Login Information."
IMPORTANT: After ContentWatch™ sends this email to you, you have 10 minutes to reset the Admin password. If you do not reset the password within this timeframe, you must repeat the preceding steps.
- If you no longer have access to the email address you used to register the product, call ContentWatch Support at 1-800-485-4008 or send an email to support@contentwatch.com and provide the following information:
 - Administrator Name
 - Registration Key
 - Account Name
 - Email Address (where to send the password)
 - Secret Question (for example: What's my dog's name?)
 - Answer to the Secret Question



Open Code License Text

PCRE License Text

Regular expression support is provided by the PCRE library package, which is open source software written by Phillip Hazel. Copyright is by the University of Cambridge, England.

<ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/>

SOAP License Text

This product includes software developed by the Apache Software Foundation.

<http://www.apache.org/>

OpenSSL License Text

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit.

<http://www.openssl.org>