[content] watch™

INTERNET PROTECTION

ContentProtect Professional Suite

Administrator’s Guide

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.

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.

Third-Party Materials

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

ContentProtect Professional 3.0 Suite Administrator's Guide
June 18, 2009

Table of Contents

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

- Microsoft* Windows* XP/Vista
- 121.1 MB hard drive space
- Minimum screen resolution of 1024x768
- Internet connection

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 exception 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.

Registering ContentProtect Professional

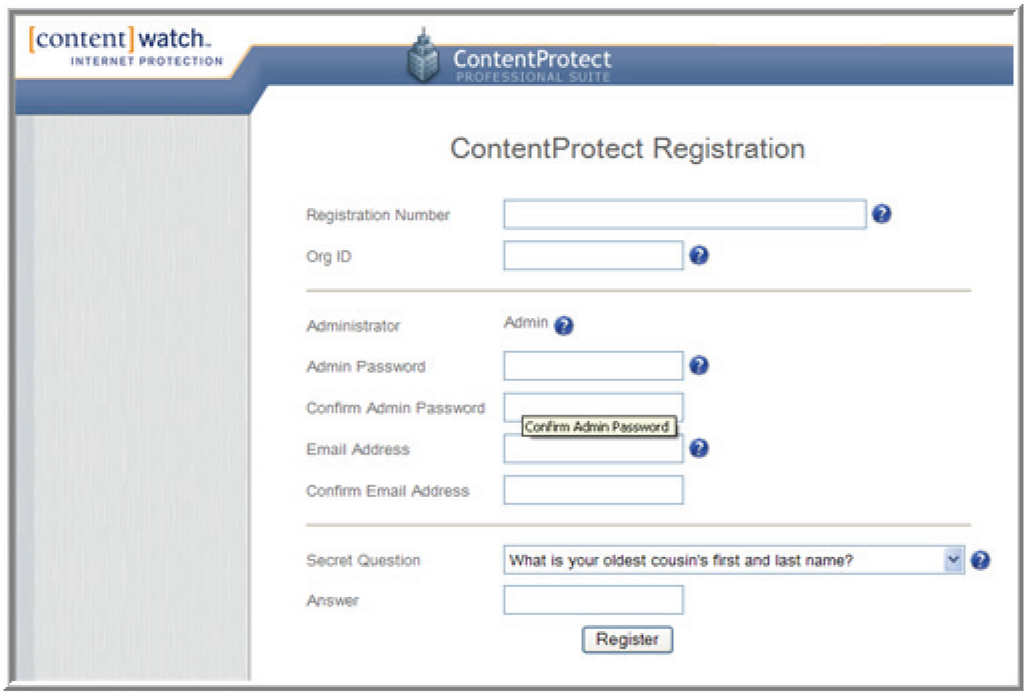
After you have purchased ContentProtect™ Professional™, you must register your product before you can download the ContentProtect Professional client or access the Online Management application. If you purchased ContentProtect Professional online or requested a trialware number, the registration number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

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.



Administrator: Admin

Admin Password

Confirm Admin Password

Secret Question: What is your oldest cousin's first and last name?

2. Enter the registration number provided in your pre-registration.
3. In the Org ID 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.
4. Under Administrator, in the Admin Password and Confirm Password fields, specify a password for the Online Management administrator user account

   The Admin password is also the password you use to install or uninstall ContentWatch Professional. 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.

5. Specify the Administrator's email address and confirm it.

   This email address is where your registration confirmation email is sent.

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.

6. 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, then click **Next**.

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

7. Verify that all information you have entered is accurate, then click **Register**.

   If you need to change any information, make the necessary modifications.

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

8. 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.

Installing and Uninstalling the ContentProtect Professional Client

Installing the Client

After you have registered ContentProtect Professional, you are provided with a link to download the ContentProtect Professional client. There are two different methods for installing the client software:

- Manual installation method

  This method involves taking the client executable to each user's machine and manually starting the installation. Alternately, you can email the executable to users and have them run the installation.

- Unattended installation method

  This method allows you to perform an automated installation of the client software on users' machines.

These methods are discussed in the following sections.

Manual Installation

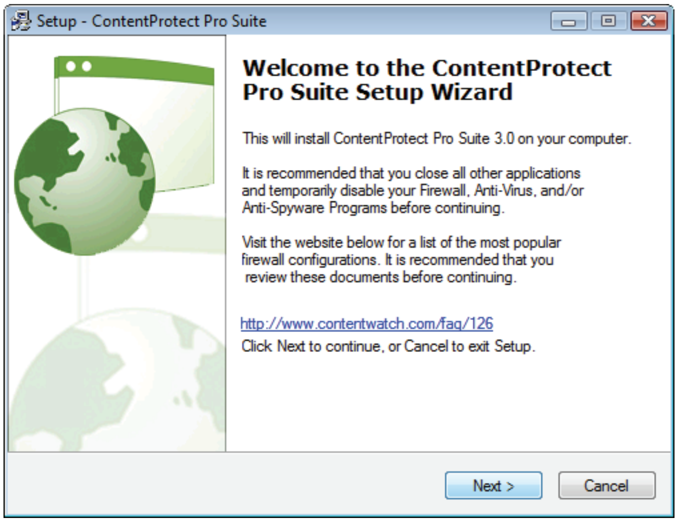
In this section, we discuss how to manually install the ContentProtect Professional client on users' machines. For instructions on automating the distribution of the client, see Unattended Installation on page 14.

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, then click **OK**.
3. Ensure that you are connected to the Internet, then click **OK** to continue.

   The ContentProtect Setup Wizard launches. We recommend that you close all other applications before continuing with the installation.

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



Welcome to the ContentProtect Pro Suite Setup Wizard

This will install ContentProtect Pro Suite 3.0 on your computer.

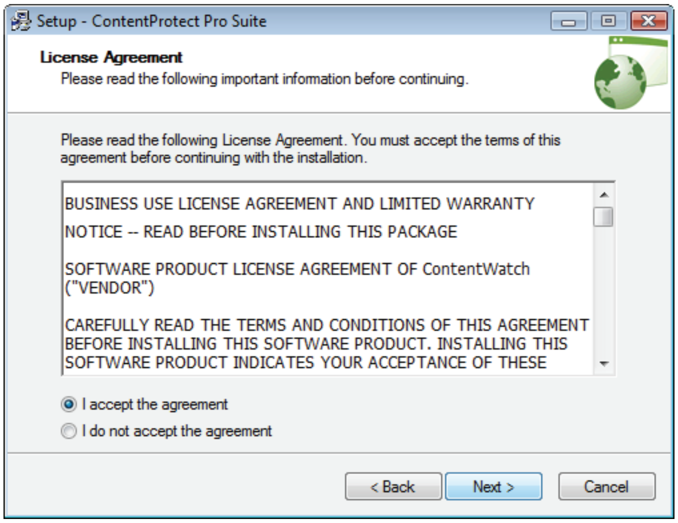
It is recommended that you close all other applications and temporarily disable your Firewall, Anti-Virus, and/or Anti-Spyware Programs before continuing.

Visit the website below for a list of the most popular firewall configurations. It is recommended that you review these documents before continuing.

http://www.contentwatch.com/faq/126

Click Next to continue, or Cancel to exit Setup.

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



License Agreement

Please read the following important information before continuing.

Please read the following License Agreement. You must accept the terms of this agreement before continuing with the installation.

BUSINESS USE LICENSE AGREEMENT AND LIMITED WARRANTY

NOTICE -- READ BEFORE INSTALLING THIS PACKAGE

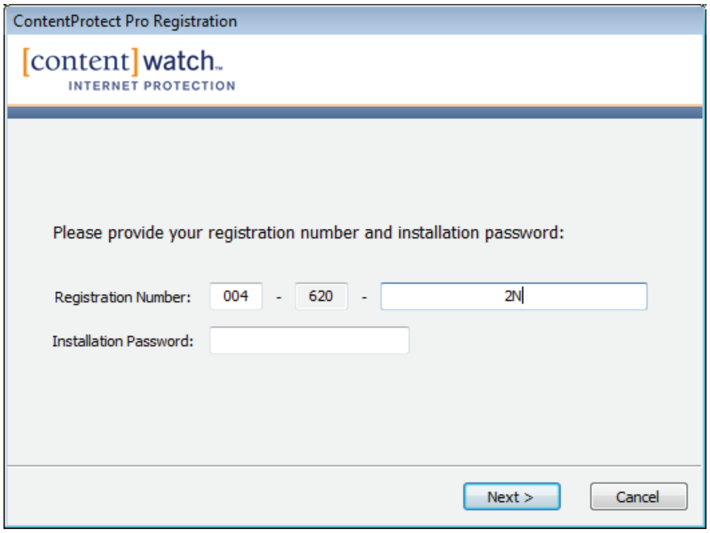
SOFTWARE PRODUCT LICENSE AGREEMENT OF ContentWatch ("VENDOR")

CAREFULLY READ THE TERMS AND CONDITIONS OF THIS AGREEMENT BEFORE INSTALLING THIS SOFTWARE PRODUCT. INSTALLING THIS SOFTWARE PRODUCT INDICATES YOUR ACCEPTANCE OF THESE

● I accept the agreement

○ I do not accept the agreement

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



ContentProtect Pro Registration

Please provide your registration number and installation password:

Registration Number: 004 - 620 - 2N

Installation Password:

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

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

   If ContentProtect Professional is unable to contact the ContentWatch registration server, a message is displayed reminding you to verify that your firewall is disabled, and asking if you want to configure proxy server settings.

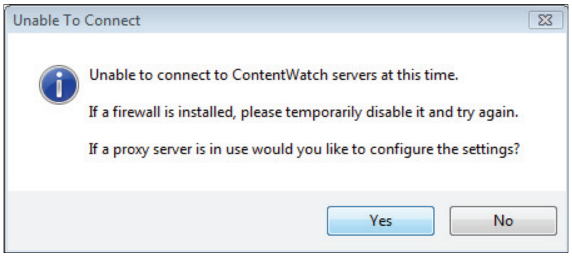
   You can attempt to connect to ContentWatch via a proxy server provided that the following criteria are met:

   - You have verified that your firewall is disabled.
   - You have verified that your Internet connection is working.
   - Your company offers a proxy server as an alternate means of connecting to the Internet.

   To configure proxy settings:

   a) Obtain the necessary proxy server information, such as host name and port number, from your ISP.

   b) At the prompt asking you if you want to configure proxy server settings, click **Yes**.



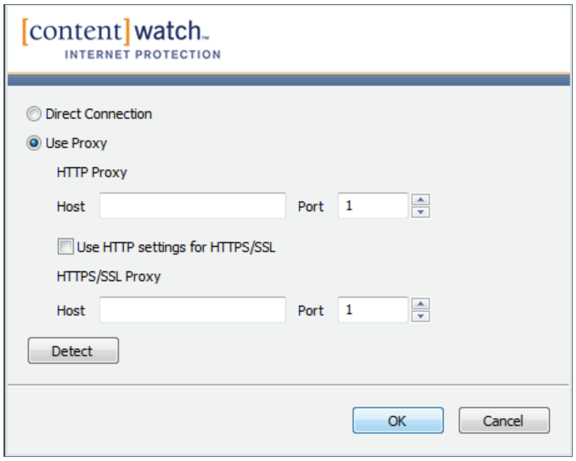
Unable To Connect

Unable to connect to ContentWatch servers at this time.

If a firewall is installed, please temporarily disable it and try again.

If a proxy server is in use would you like to configure the settings?

c) In the Proxy Configuration screen, enter the information for your company's proxy server, then click **OK**.



○ Direct Connection

● Use Proxy

HTTP Proxy

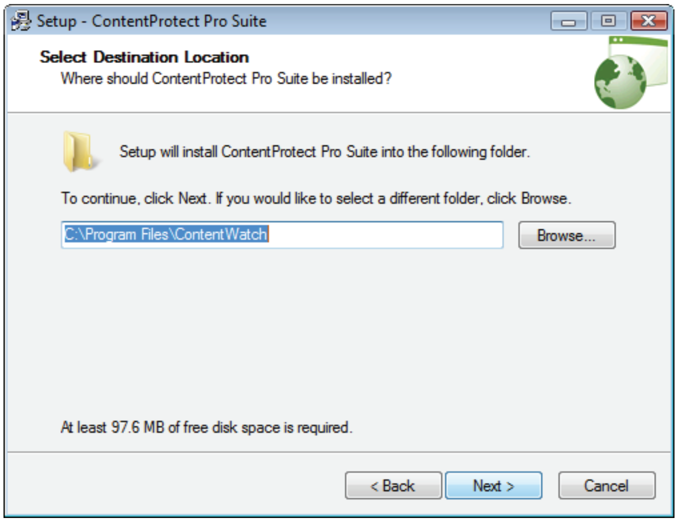
Host Port 1

□ Use HTTP settings for HTTPS/SSL

HTTPS/SSL Proxy

Host Port 1

8. Click **Next** to begin the installation, or browse to a more desirable installation location, then click **Next**.



Setup - ContentProtect Pro Suite

Select Destination Location

Where should ContentProtect Pro Suite be installed?

Setup will install ContentProtect Pro Suite into the following folder.

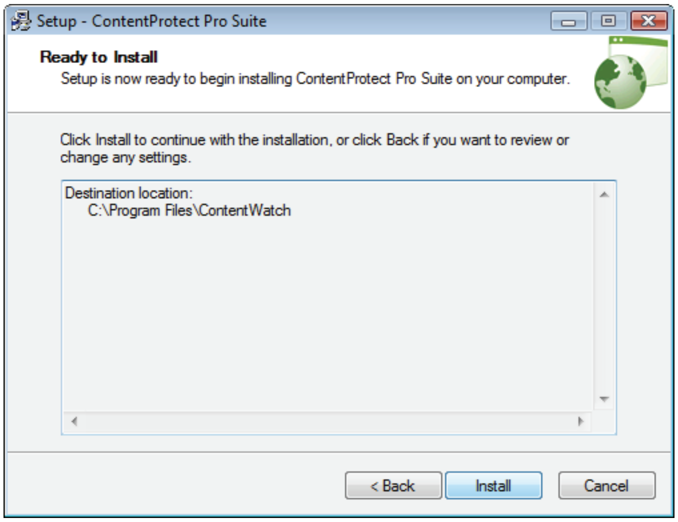
To continue, click Next. If you would like to select a different folder, click Browse.

C:\Program Files\ContentWatch

At least 97.6 MB of free disk space is required.

9. If the specified directory does not exist, click **Yes** to confirm that you want to install to the specified directory.

10. At the Ready to Install screen, click **Install**.



Ready to Install

Setup is now ready to begin installing ContentProtect Pro Suite on your computer.

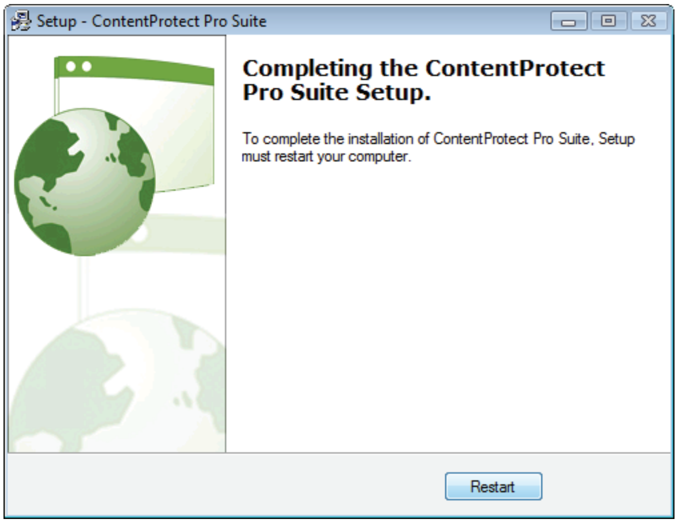
Click Install to continue with the installation, or click Back if you want to review or change any settings.

Destination location:
C:\Program Files\ContentWatch

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

11. Click **Restart** to complete the ContentProtect installation and setup.

    Your computer automatically shuts down and restarts.



Completing the ContentProtect Pro Suite Setup.

To complete the installation of ContentProtect Pro Suite, Setup must restart your computer.

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 Installation

In this section, we discuss how to perform an unattended installation of the ContentProtect Professional client on users' machines. For instructions on manually installing the client, see Manual Installation on page 9.

Prerequisites: You must have a means for pushing out the ContentProtect Professional client executable 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 installation of the ContentProtect Professional client:

1. Download the ContentProtect Professional client from ContentWatch.
2. Use a software distribution tool or a login script to push out the ContentProtect Professional client executable to users' computers and to run the following command line:

   `cwip_prosuite.exe` [`/VERYSILENT`] [`/REGNUM=`< *reg_num* >] [`/INSTPWD=`< *install_pwd* >] [`/NORESTART`] [`/RESTART=manual`]

   For example:

   ```
   cwip_prosuite.exe /VERYSILENT /REGNUM=1-234-5U2DMVZHJQECWRNIFHUF3T3D
   /INSTPWD=secret /NORESTART
   ```

   The purpose of the command line switches is as follows:

Parameter	Description
`/VERYSILENT`	Do not display any installation dialogs.
`/REGNUM=`<*reg_num*>	Specify the registration number.
`/INSTPWD=`<*install pwd*>	Specify the installation password.
`/NORESTART`	Suppress the automatic reboot after installation. Use this parameter if you want your distribution tool or login script to handle the job of informing users that their computer needs to be restarted and to control when the computer is restarted. Generally, you should use this parameter instead of the `/RESTART=MANUAL` switch if you want the installation process to be fully automated.
`/RESTART=MANUAL`	Suppress the automatic reboot after installation and prompt users to manually restart their computers. This parameter is not recommended for unattended installations since it leaves the computer restart to the discretion of the user. ContentProtect Professional requires a reboot after installation in order to function correctly.

Uninstalling the Client

Manual Uninstallation

To uninstall the client manually:

1. Open the Windows Control Panel.
2. For Windows XP:
   a. Double-click **Add or Remove Programs**.
   b. Select **ContentProtect**, then click **Remove**.

   For Windows Vista:
   a. Under **Programs**, click **Uninstall a Program**.
   b. From the list of installed programs, select **ContentProtect**.
   c. Click **Uninstall**.
3. When prompted, enter the password.

   Note: This is the admin password you specified during the registration process, or the uninstall password you specified on the Password screen. If you set an uninstall password, that password is required when uninstalling the software.
4. Complete the uninstall process and restart the computer when prompted.

Unattended Uninstallation

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\Pro
2. At the command prompt, type the following command line:

```
unins000.exe /UninstallPassword=<uninstall_pwd> [/VERYSILENT] [/NORESTART] [/RESTART=manual]
```

   For example:

```
unins000.exe /UninstallPassword=secret /VERYSILENT /NORESTART /RESTART=manual
```

   The purpose of the command line switches is as follows:

Parameter	Description
`/UNINSTALLPASSWORD=`*<uninstall_pwd>*	Specify the uninstall password you chose during the ContentProtect Professional product registration process.
`/VERYSILENT`	Do not display any uninstallation dialogs. The computer is rebooted without warning when the uninstallation process is complete.
`/NORESTART`	Suppress the automatic reboot after uninstallation.
`/RESTART=MANUAL`	Suppress the automatic reboot after uninstallation, and alert the user that they need to manually reboot the computer.

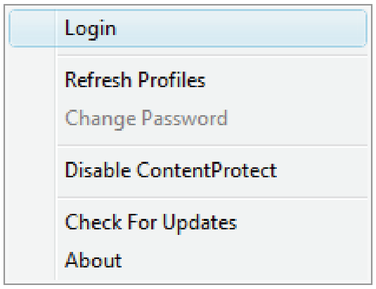
Getting Started with the ContentProtect Professional Client

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:

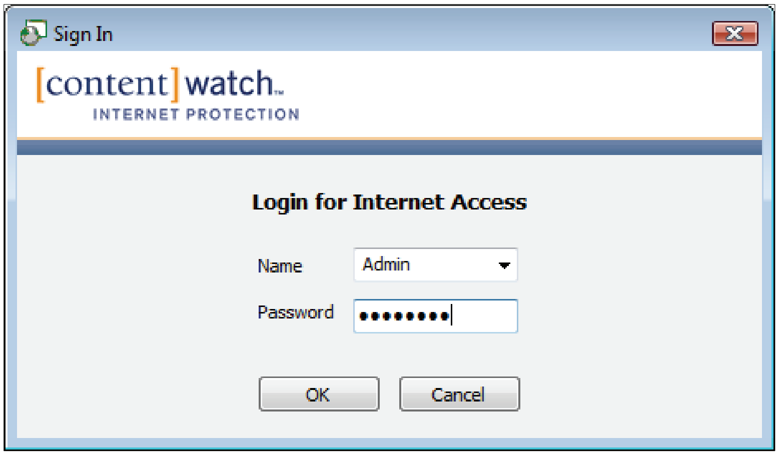
1. Right-click the ContentProtect Professional icon in the system tray located on the taskbar at the bottom of your Windows desktop, then select **Login** from the quick menu.



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

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

   Note: Bullets appear as you type your password to protect it from being viewed.



Login for Internet Access

Name: Admin

Password: ••••••••

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.

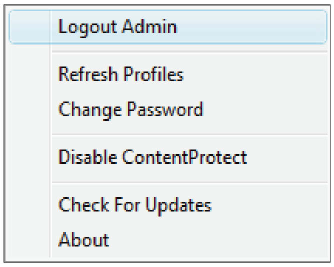
Signing Out

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.



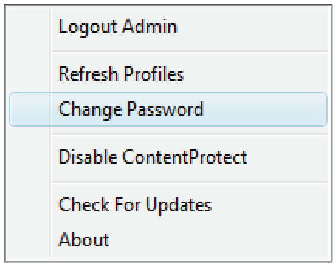
Note: If you shut down your computer without signing out, your session automatically ends. You must sign in again when the computer restarts.

Changing User Passwords

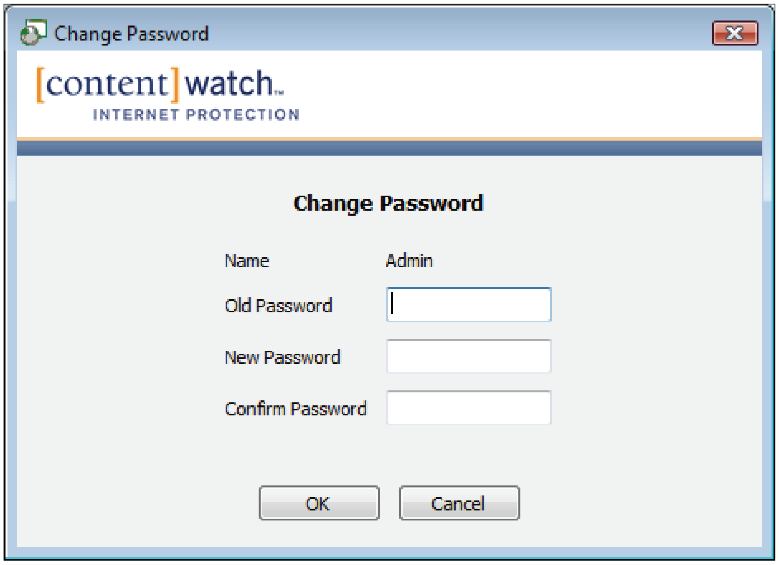
Users can quickly change their own ContentProtect Professional client login passwords.

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, then click **OK**.



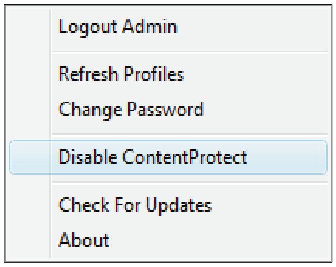
The password is immediately changed in the local client database, and the updated information is sent to the Online Management application.

Disabling the Client

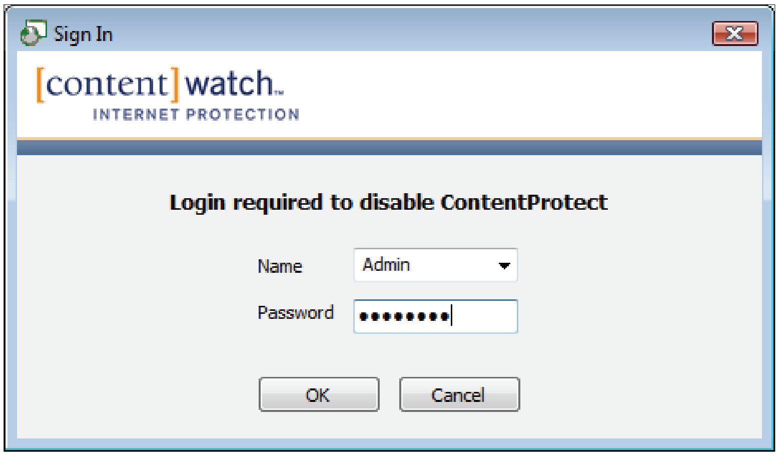
There may be times when you want to temporarily disable the ContentProtect Professional client. For example, you may want to temporarily allow access to the Internet without blocking any content, or you may want to allow a non-safe search in one of the supported search engines. Rather than temporarily 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 Admin as the user name, enter the administrative user’s password, then click **OK**.



Sign In

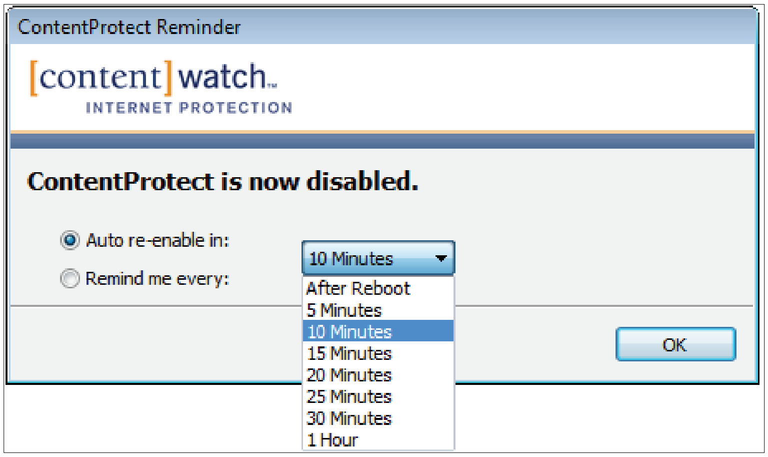
Login required to disable ContentProtect

Name: Admin

Password: ••••••••

4. Choose whether you want the client to automatically re-enable itself or remind you that it is disabled after a certain amount of time has passed.

   From the drop-down list, select the amount of time until the client re-enables itself (After Reboot, 5 Minutes, 10 Minutes, 15 Minutes, 20 Minutes, 25 Minutes, 30 Minutes, or 1 Hour) or gives you a reminder (Never, 5 Minutes, 10 Minutes, 15 Minutes, 20 Minutes, 25 Minutes, 30 Minutes, or 1 Hour), then click **OK**.



ContentProtect Reminder

ContentProtect is now disabled.

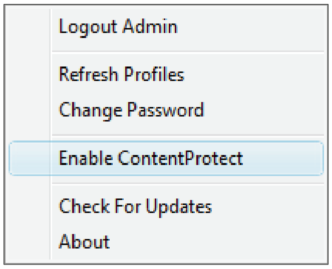
● Auto re-enable in: 10 Minutes

○ Remind me every:

The client is now disabled, and the ContentProtect Professional icon in the system tray changes appearance:

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**.



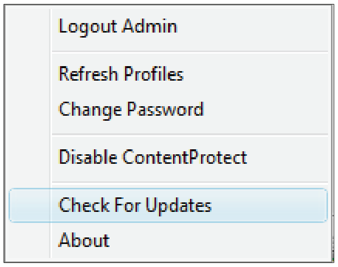
The client is now enabled, and the ContentProtect Professional icon in the system tray returns to its original appearance:

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. Follow the prompts to complete the update wizard.

Note: You may be asked to restart your computer for the changes to take effect.

Managing 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 exceptions.

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

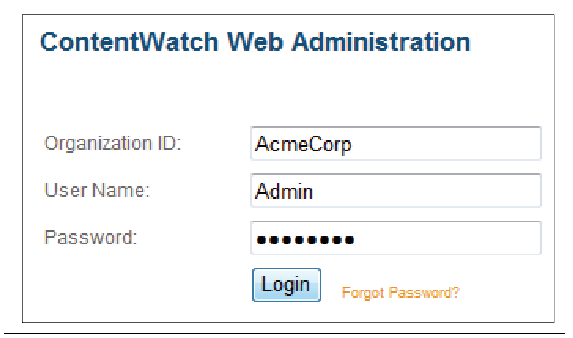
To log in to the Online Management application:

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, then click **Login**.

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



ContentWatch Web Administration

Organization ID: AcmeCorp

User Name: Admin

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**.

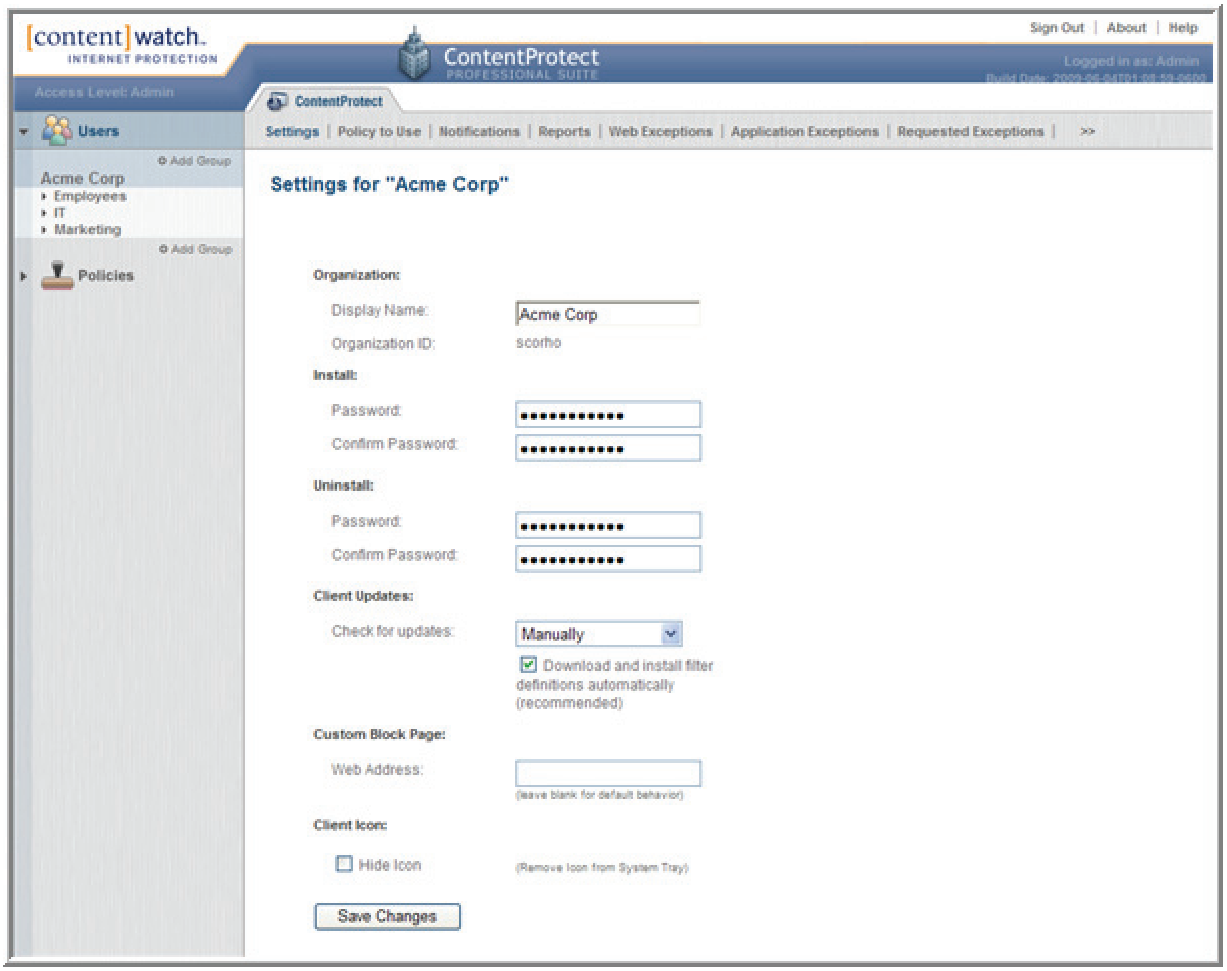
  b. When prompted, provide the Admin user's email address and then click **Send**.

     Note: If you no longer have access to the Admin user's email address, 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:



Settings for "Acme Corp"

Organization:

Display Name: Acme Corp

Organization ID: scorho

Install:

Password: ••••••••••••

Confirm Password: ••••••••••••

Uninstall:

Password: ••••••••••••

Confirm Password: ••••••••••••

Client Updates:

Check for updates: Manually

☑ Download and install filter definitions automatically (recommended)

Custom Block Page:

Web Address:

(leave blank for default behavior)

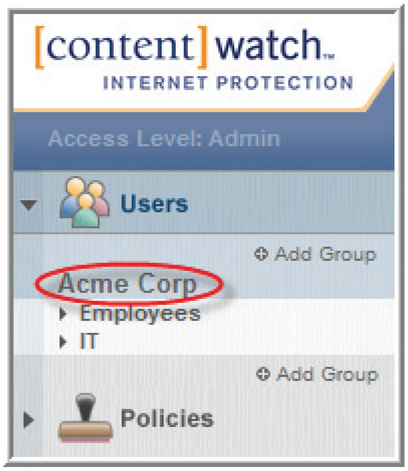
Client Icon:

☐ Hide Icon (Remove Icon from System Tray)

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:



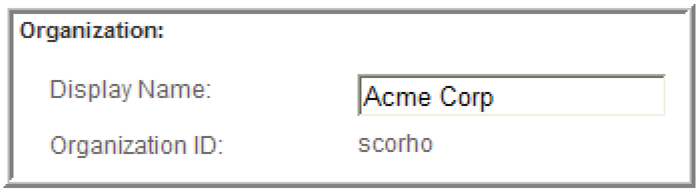
On the Organization Settings page, you can perform the following tasks:

- 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. Click the organization name above the User list.
2. In the Display Name field, type the desired name.



Organization:

Display Name: Acme Corp

Organization ID: scorho

3. Click **Save Changes**.

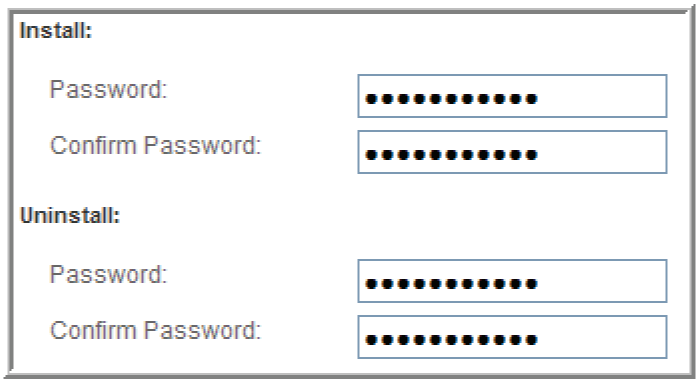
Changing the Client Install and Uninstall Passwords

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. Click the organization name above the User list.

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



Install:

Password: ●●●●●●●●●●●●

Confirm Password: ●●●●●●●●●●●●

Uninstall:

Password: ●●●●●●●●●●●●

Confirm Password: ●●●●●●●●●●●●

3. Click **Save Changes**.

Changing the Client Update Method

To change how client updates are performed:

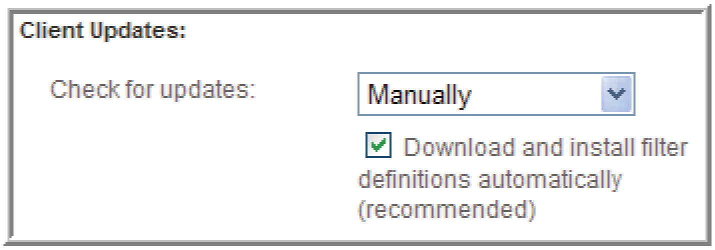
1. Click the organization name above the User list.
2. From the Apply drop-down list, select one of the following client update methods.

   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 notify you when an update becomes available.

   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.

3. Enable the option to download and install filter definitions automatically.



Client Updates:

Check for updates: Manually

☑ Download and install filter definitions automatically (recommended)

   This option is recommended because having up-to-date filter definitions helps to ensure that harmful materials will be filtered.

4. Click **Save Changes**.

Displaying a Custom Message for Blocked Web Sites

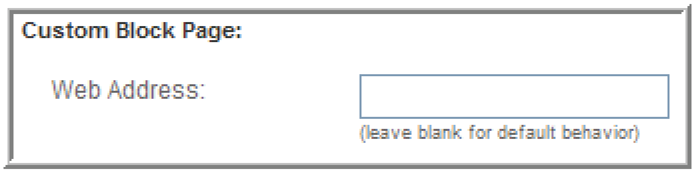
The Custom Block Page option allows you to display a custom Web page (which can include your company logo, corporate Internet usage policy, or any other information you deem necessary) when users attempt to access blocked Web sites. You can use any Web authoring tool to create the page. Once you have 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. Click the organization name above the User list.

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



Custom Block Page:

Web Address:

(leave blank for default behavior)

3. Click **Save Changes**.

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

When ContentProtect Professional displays the URL for a blocked page, it includes a category number that indicates why the page was blocked. For example, if the site www.badsite.com is blocked because it contains pornography, the displayed URL for the block page would be:

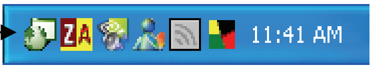
http://www.mysite.com/block.html?url=www.badsite.com&cat18=true

The categories are:

0=Other
1=Adult/Mature
2=Illegal Drugs
3=Chat Site
4=Email
5=Employment/Career
6=Schools/Colleges
7=Financial/Stocks
8=Gambling
9=Games
10=Hate/Violence
11=Health/Medicine
12=Illegal Activities
13=Instructional
14=Intimate Apparel
15=Music/Entertainment
16=News
17=Personals
18=Pornography
19=Search Engines/Portals
20=Shopping
21=Sports
22=Kids
23=Work Related
24=Religious
25=Travel
26=Family Resources
27=Government
28=Ads
29=Proxy
30=Image/Video Search
31=Alcohol/Tobacco
32=Web Scripts
33=Web Images
34=Custom Allow
35=Custom Block

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.

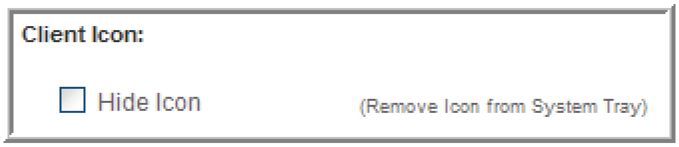


ContentProtect Professional client systray icon

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. Click the organization name above the User list.
2. Select the **Hide Icon** check box.



Client Icon:

□ Hide Icon (Remove Icon from System Tray)

3. 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. Users are organized into groups to make management of large numbers of users easier. Each group can have its own administrator.

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

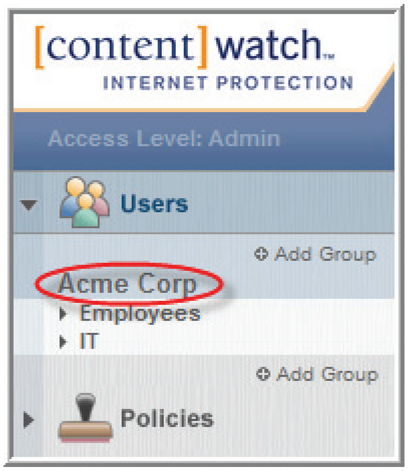
User accounts can exist only within groups, so before you can add users, you must first create groups to contain them. Plan how to group users so it will be easier for you to assign Internet access policies to them. You may group users according to what department they are in or how they use the Internet 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.

Each group can have its own administrators. Group administers are assigned within the user details of the people you want to administer groups.

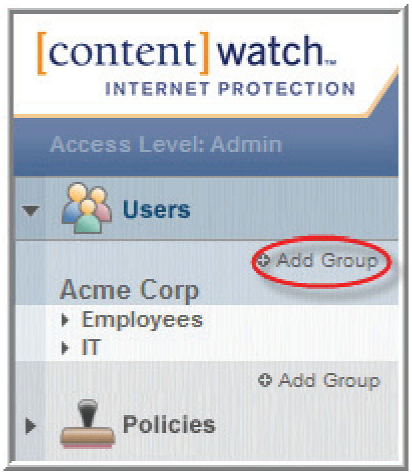
Note: At any time, you can apply any policy you have created to individual users within a group. The policy assigned to an individual user overrides the policy assigned to the group that the user is a member of. For more information on creating and assigning policies, see Managing Policies on page 33.

To create a new group in the Online Management application:

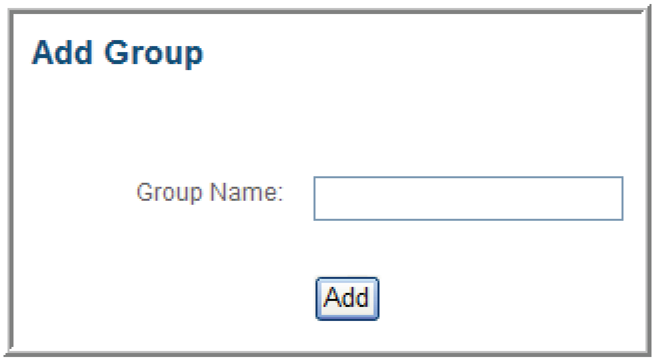
1. Click your organization name in the upper-left area of the screen:



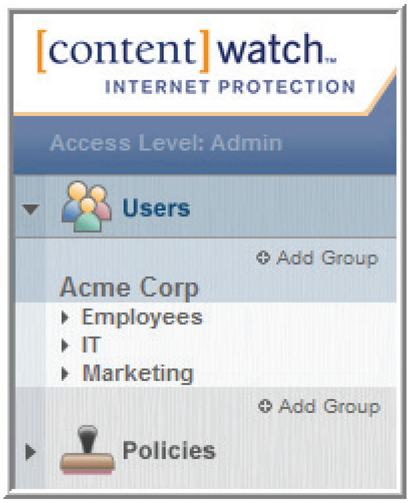
2. Click **Add Group**.



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



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



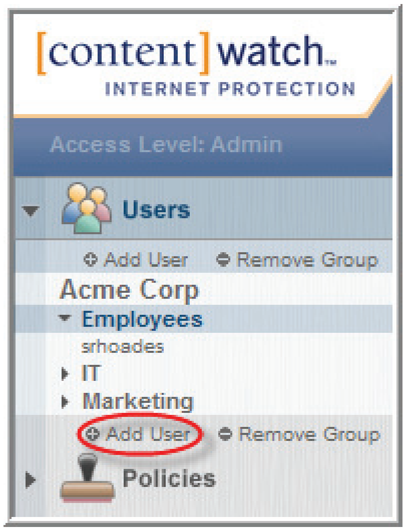
Adding Users

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

To add a user:

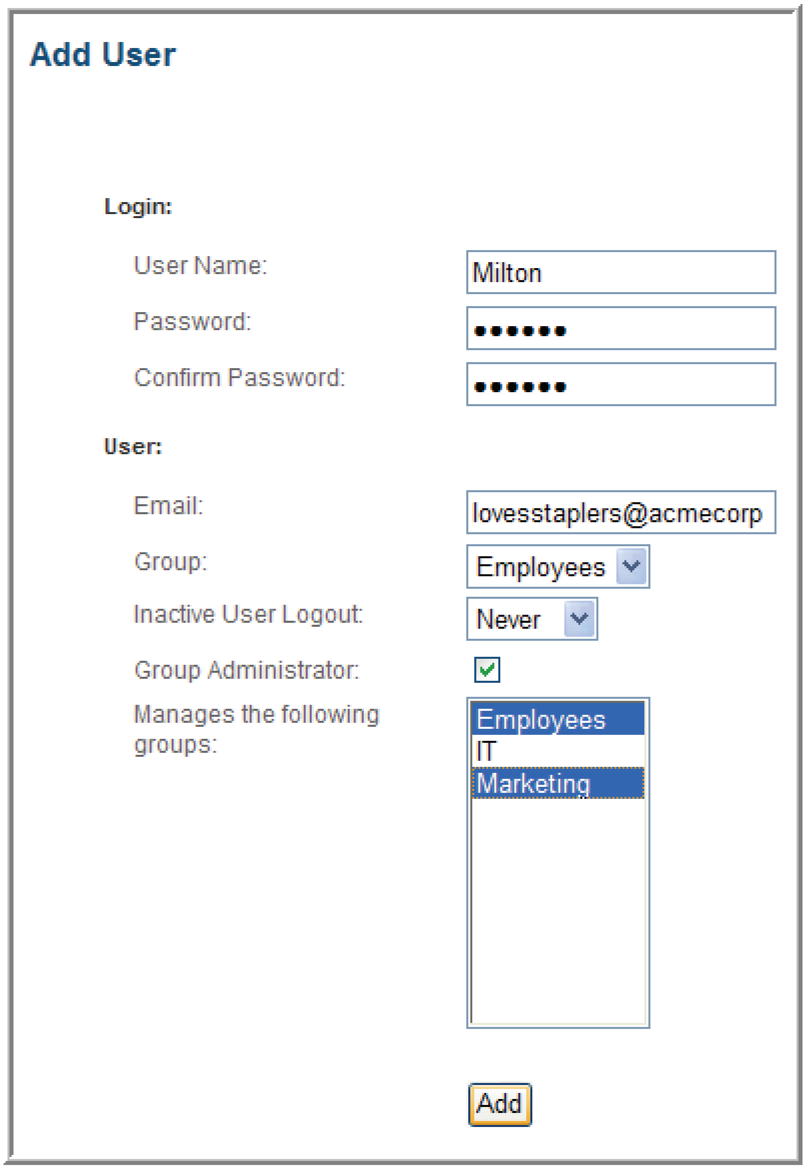
1. Click the group you want to add a user to.

2. Click **Add User**.



3. In the Add User window, fill out the user's login and user information, select whether the user is a group administrator and select the groups that user administers, 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.



Add User

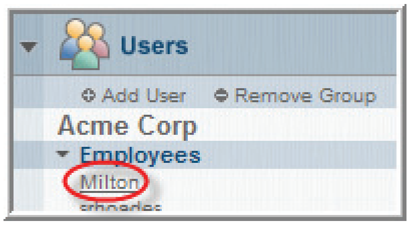
Login:

User Name:	Milton
Password:	••••••
Confirm Password:	••••••

User:

Email:	lovesstaplers@acmecorp
Group:	Employees
Inactive User Logout:	Never
Group Administrator:	☑
Manages the following groups:	Employees IT Marketing

The new user appears in the group.



Modifying User Settings

To modify a user's settings:

1. Click the group where the user is located.
2. Click the user whose settings you want to modify.
3. Modify settings as desired.
4. 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.
Password	Password the user enters to sign in to ContentProtect. Passwords can be between 3 and 13 characters in length. Passwords are case-sensitive. Numbers and alpha characters can be combined. Passwords can also be blank if no password is required. **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.
Email	User's email address.
Group	Group the user is assigned to. A user can belong to only one group. To reassign the user to a different group, select the desired group from the drop-down list.
Inactive User Logout	Designates an inactivity threshold after which the user is automatically logged out. If you select **Never**, ContentProtect does not automatically log out the user.
Group Administrator	Select if the user is a group administrator.
Manages the following groups	If **Group Administrator** is selected, select one or more groups that the user administers. Control-click to select more than one group. An administrator does not have to belong to a group to administer it. In fact, you could place all administrators in a single group with its own profile.

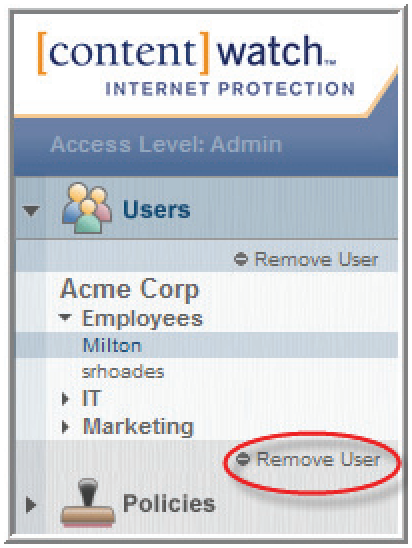
Note: Profile changes are usually updated within one minute. You can also manually refresh profiles by right-clicking the ContentProtect Professional system tray icon on their machines and selecting **Refresh Profiles** to immediately apply changes made in the Online Management application.

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, and peer-to-peer access. 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 (pornography and proxy). 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.

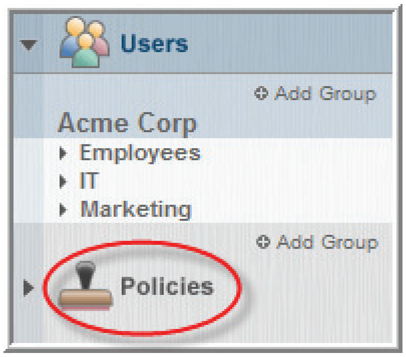
Example 3: No policy is applied to either User3 or his group. Therefore, whatever policy is applied to the organization will govern the group that User3 belongs to, as well as all the users within that group who don't have a policy applied directly to them.

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.

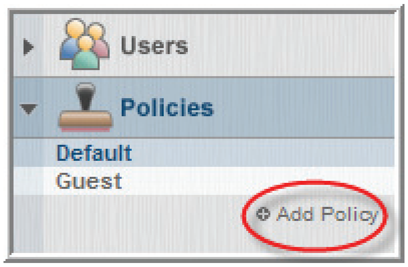
Adding Policies

To add a new policy:

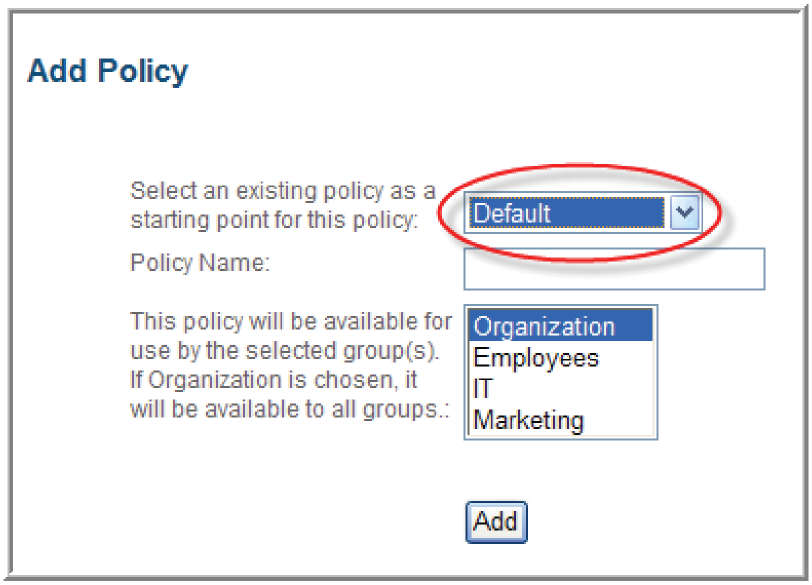
1. In the sidebar of the Online Management application, click **Policies**.



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.



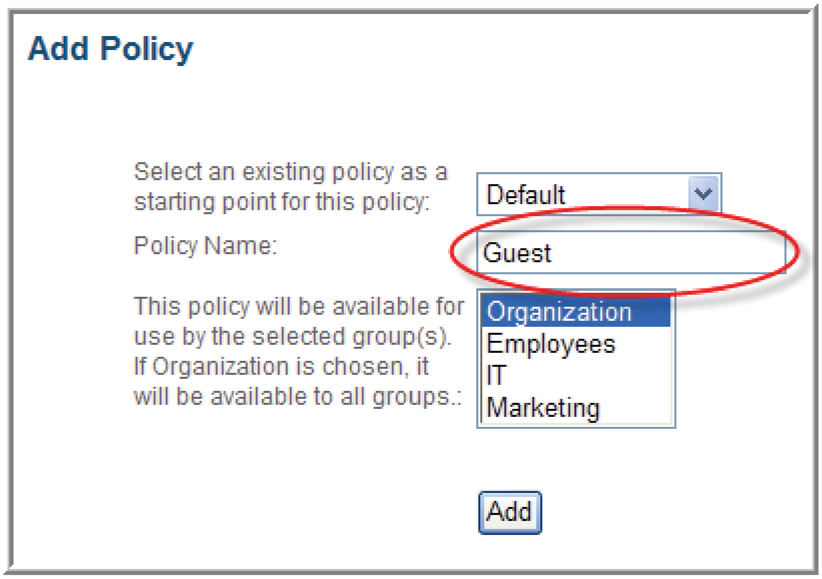
Add Policy

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

Policy Name:

This policy will be available for use by the selected group(s). If Organization is chosen, it will be available to all groups.: Organization, Employees, IT, Marketing

4. In the Policy Name field, specify a name for your new policy.



Add Policy

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

Policy Name: Guest

This policy will be available for use by the selected group(s). If Organization is chosen, it will be available to all groups.: Organization, Employees, IT, Marketing

5. Select one or more groups that will use the new policy, then click **Add**.

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. Configure the settings as desired, then click **Save Changes**.

The following sections describe the policy settings you can modify.

Name Settings

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

Available to Groups

Select one or more groups that can use this policy.

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 2: Privileges to Allow

Option	Description
Administrator	Gives administrative privileges to users assigned to this policy. Users with administrative privileges can change passwords, profile settings, and filters; configure email notifications; and access reporting and remote management.
Override Blocked Messages	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.) **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. If you do not select this option, ContentProtect Professional displays a block message when the user tries to access blocked Internet content.
Request Web Exception	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 exception requests, see Processing Web Exception Requests on page 58.)
Auto Client Login	Prevents a login dialog from displaying each time the user accesses the Internet. 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, then restarted.

Option	Description
Auto Windows Login	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. 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. **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.
Allow user to change password	Enables the user to change the password used for logging in to ContentProtect Professional.

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 Browsing	URLs, normal "surfing" or "browsing"
Instant Messaging	Yahoo!, Windows Live Messenger, AIM*, QQ, Google Talk
Internet Chat	Chat clients or Web-based chat rooms that use the IRC (Internet Relay Chat) protocol
Newsgroups	NNTP (standard news groups)
Peer-to-Peer	Peer-to-peer file sharing applications (for example, Gnutella, BitTorrent*, Kazaa*, eMule*, and eDonkey*)

Record Activity Data From

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 4: Services to Report On

Option	Description
Web Browsing	URLs, normal "surfing" or "browsing"
Instant Messaging	Yahoo!, MSN, AOL *, QQ, Google Talk

For more information on using reporting in ContentProtect Professional, see Working with Reports on page 49.

Secure Internet Content (HTTPS)

Select either **Filter Secure Content** or **Allow secure content**.

If you select **Filter Secure Content**, you can also choose to **Block secure content from unsupported applications**.

Unsupported applications include applications whose SSL implementation ContentProtect Pro does not support. Currently, the only SSL applications that ContentProtect Pro supports are browsers. If a user selects the Block secure content from unsupported sources setting, ContentProtect Pro blocks any SSL application that is not supported, including non-browser applications such as QuickBooks and others.

Enabling this setting might cause unintended side effects with some of your applications.

64-bit Applications

You can choose to block 64-bit applications. This prevents users from bypassing Internet blocks by using a 64-bit browser.

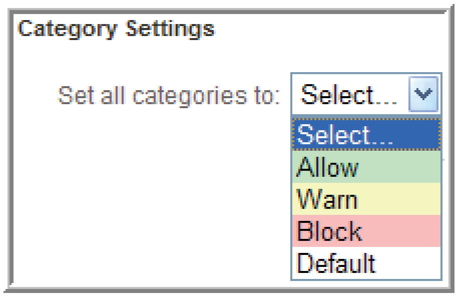
Filter Mode

You can choose whether to filter Web content or restrict browsing to certain sites.

If you select **Restrict browsing to specific sites** the user is only allowed to browse to the sites listed. This is sometimes referred to as whitelist mode. You must have at least one site in the list of allowed sites. If no sites are listed, the user will not be able to access any Web sites. For more information, see Specifying Allowed Web Sites on page 46.

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.

Default: Returns the category settings to the default settings. The following categories are blocked by default, while all other categories are set to Allow:

- Pornography
- Proxy

Note: For message examples and descriptions, see Block and Warning Messages on page 46.

The following table outlines the ContentProtect Pro predefined content categories:

Category	Description
Adult/Mature	Contains subject matter intended for mature audiences, such as obscene or vulgar language and adult instant message rooms. These sites could be considered R-rated.
Alcohol/Tobacco	Contains subject matter that deals with manufacturing, distributing, or obtaining alcohol or tobacco. Sites that depict alcohol or tobacco paraphernalia.
Chat Site	Contains information on instant message protocols or applications and links to instant message organizations, rings, and rooms.
Email	Provides access to email services and applications.
Employment/Career	Allows the posting of jobs or resumes. Provides information on compensation in specific fields or regions. Posts information about jobs and job openings.
Family Resources	Provides family counseling, family safety tips, parenting information and tips, and family planning.
Financial/Stocks	Provides information about finances, financial planning, insurance, stock tickers, and stock reports. Allows the sale and purchase of stock. Includes banks and credit unions and credit rating and reporting sites.
Gambling	Allows a person to wager money on online games with the expectation of winning money or prizes. Contains links to other gambling sites or provides information on gambling strategies or tactics.
Games	Provides access to online or downloadable games, discussions about games, or information about game cheats.
Government	Provides information 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	Promotes or depicts violence against persons, animals, property, or nations. Singles out groups for violence based on race, religion, or creed.
Health/Medicine	Provides information on mental or physical health issues. Allows the online purchase of prescription medications.
Illegal Activities	Provides information about the manufacture, alteration, or sales of weapons, explosives, and explosive devices. Promotes or depicts disorderly conduct .
Illegal Drugs	Contains subject matter that deals with manufacturing, distributing, or obtaining illegal drugs or other controlled substances. Depicts drug paraphernalia and/or includes methods for obtaining or manufacturing them. Does not include sites that provide information on prescription medications except those sites that describe how to obtain them.
Image/Video Search	Allow the user to search for images or videos, including Google Images and YouTube.
Instructional	Contains instructional material, tutorials, or how-to pages.
Intimate Apparel	Displays models wearing underwear, lingerie, or other suggestive or see-through attire, including swimsuits.

Kids
Contains subject matter intended for children, including entertainment, education, crisis counseling, and kid-friendly communities.

Music/Entertainment
Provides access to free downloadable or for-pay online music and video files such as MP3, WAV, MPG, and AVI. Sells music or videos or is dedicated to the music or entertainment industry. Provides information on TV programs and programming, including movie review sites.

News
Provides live, recorded, or written reports or editorials about current events.

Other
Sites that do not fit into any of the existing Net Nanny categories.

Personals
Contains personal ads, personal info pages, and personal portals.

Pornography
Contains subject matter that is 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.

Proxy
Allows users to anonymously surf the Internet, either for the purpose of maintaining online privacy or bypassing content filtering software.

Religious
Provides information on specific religions or religious beliefs. Includes regional religious organizational sites and sites built to promote religious groups, activities, and membership.

Schools/Colleges
Contains information dealing with colleges, schools, seminars, or courses. Sites that end in .edu.

Search Engines/Portals
Provides mechanisms for searching the Internet by specific words or phrases and displays the results as either links or images. Allows a user to customize the look or content and is geared to providing a "starting" place on the Internet.

Shopping
Provides access to online malls, catalogs, or auctions, including classified ads. Includes department store sites, retail store sites, or sites that have coupons for free or discounted items.

Sports
Promotes, advertises, reports on, or is associated with sports teams, individuals, or organizations. Includes sites that are involved with fantasy sports and organizations whose main focus is to report on amateur, college, or professional sports.

Travel
Provides information on travel, such as destination descriptions, ticketing, and reservations. Includes airline, bus, or train company sites and car rental sites.

Work Related
Allows an organization to add URLs for sites that are used by the organization in the course of doing business. It may initially be blank.

Note: When ContentProtect Professional is enabled, it forces a “safe search” for as many search engines as it can. Currently, ContentWatch 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 temporarily disable Net ContentProtect Professional via its system tray icon’s right-click menu.

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. You can configure time controls for a policy, then configure a user or group to use that policy.

To set time controls, select the policy whose time controls you want to set or change, then click **Time Controls**.

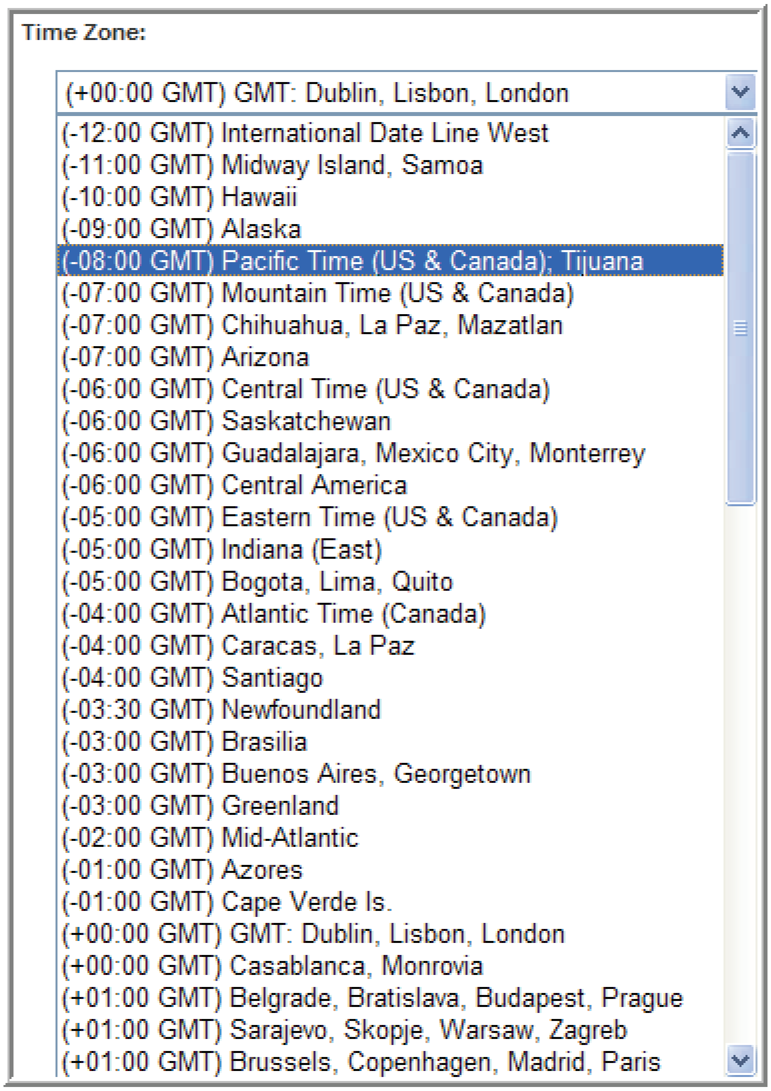
The following sections describe the time controls you can set.

Setting the Time Zone

You can set a time zone for each profile.

To set the time zone:

1. Select the policy whose time zone you want to set or change, then click **Time Controls**.
2. Select the desired time zone from the Time Zone dropdown list.



Time Zone: (+00:00 GMT) GMT: Dublin, Lisbon, London

(-12:00 GMT) International Date Line West
(-11:00 GMT) Midway Island, Samoa
(-10:00 GMT) Hawaii
(-09:00 GMT) Alaska
(-08:00 GMT) Pacific Time (US & Canada); Tijuana
(-07:00 GMT) Mountain Time (US & Canada)
(-07:00 GMT) Chihuahua, La Paz, Mazatlan
(-07:00 GMT) Arizona
(-06:00 GMT) Central Time (US & Canada)
(-06:00 GMT) Saskatchewan
(-06:00 GMT) Guadalajara, Mexico City, Monterrey
(-06:00 GMT) Central America
(-05:00 GMT) Eastern Time (US & Canada)
(-05:00 GMT) Indiana (East)
(-05:00 GMT) Bogota, Lima, Quito
(-04:00 GMT) Atlantic Time (Canada)
(-04:00 GMT) Caracas, La Paz
(-04:00 GMT) Santiago
(-03:30 GMT) Newfoundland
(-03:00 GMT) Brasilia
(-03:00 GMT) Buenos Aires, Georgetown
(-03:00 GMT) Greenland
(-02:00 GMT) Mid-Atlantic
(-01:00 GMT) Azores
(-01:00 GMT) Cape Verde Is.
(+00:00 GMT) GMT: Dublin, Lisbon, London
(+00:00 GMT) Casablanca, Monrovia
(+01:00 GMT) Belgrade, Bratislava, Budapest, Prague
(+01:00 GMT) Sarajevo, Skopje, Warsaw, Zagreb
(+01:00 GMT) Brussels, Copenhagen, Madrid, Paris

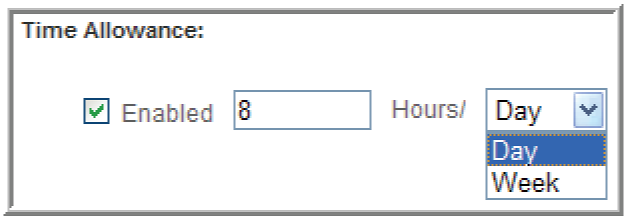
3. Click **Save Changes**.

Setting the Time Allowance

You can limit the total number of hours a user can spend on the Internet over a given period, regardless of the controls that have been specified in the time grid.

To set the time allowance:

1. Select the policy whose time zone you want to set or change, then click **Time Controls**.
2. Select **Enabled**, then specify the number of hours the user is allowed to access the Internet.
3. From the **Hours Per** drop-down menu, select the period (**Day** or **Week**) that the specified amount of hours applies to.



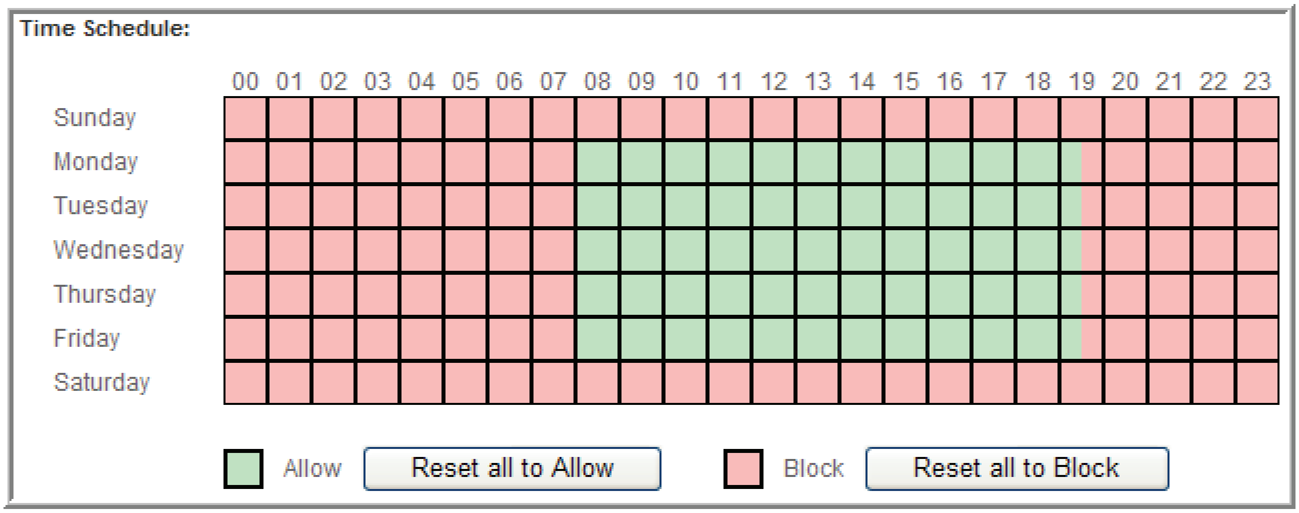
Time Allowance:

☑ Enabled 8 Hours/ Day

4. Click **Save Changes**.

Setting the Time Schedule

The Time Schedule allows you to manage the time of day and the amount of time that each user spends on the Internet. Each day of the week is divided into 30-minute time intervals that can be set to allow (green) or block (red) Internet access.



Time Schedule:

	00	01	02	03	04	05	06	07	08	09	10	11	12	13	14	15	16	17	18	19	20	21	22	23
Sunday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
Monday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩🟥	🟥	🟥	🟥	🟥
Tuesday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩🟥	🟥	🟥	🟥	🟥
Wednesday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩🟥	🟥	🟥	🟥	🟥
Thursday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩🟥	🟥	🟥	🟥	🟥
Friday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩🟥	🟥	🟥	🟥	🟥
Saturday	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥

🟩 Allow 🟥 Block

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

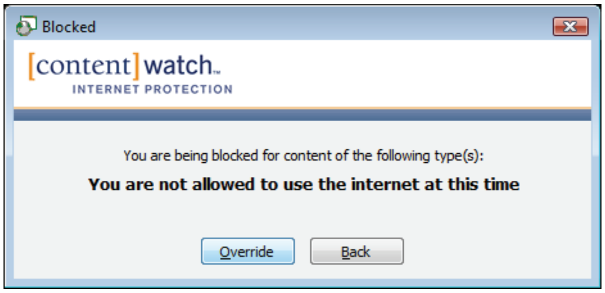
Note: To ensure that Time Schedules are enforced at the times you expect, verify that you have configured ContentProtect Pro™ with the correct time zone for your location. For instructions on setting the time, see Setting the Time Zone on page 40.

To set the Time Schedule:

1. Select the policy whose time zone you want to set or change, then click **Time Controls**.
2. Under **Time** Schedule, select the times you want to block by clicking and dragging over the desired times.
3. Click **Save Changes**.

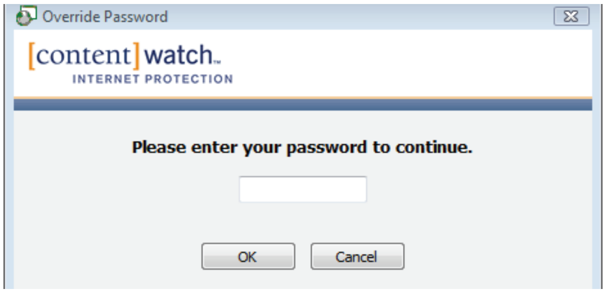
Enforcing Internet Access Schedules

When a time control is in effect, a message displays 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.



You are being blocked for content of the following type(s):

You are not allowed to use the internet at this time



Please enter your password to continue.

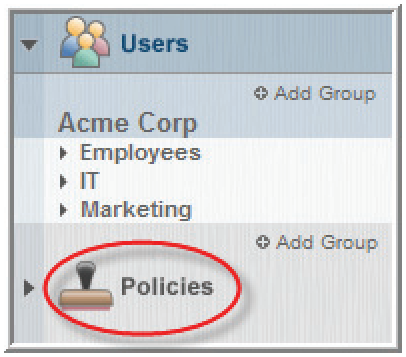
Note: To give a user override privileges, you must select the **Override Blocked Messages** option in the policy assigned to the user. If you do not select that option, the Override button does not appear in the Blocked dialog. For more information, see Allow Privileges on page 35.

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.

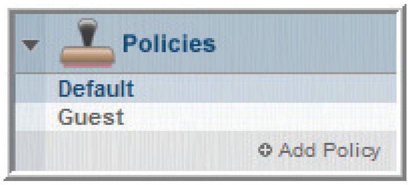
Denying or Allowing Access to Applications

To manage users' access to applications:

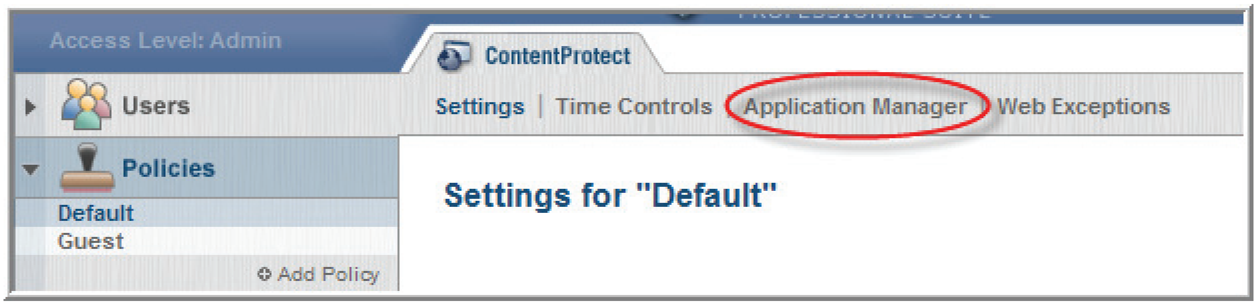
1. In the sidebar of the Online Management application, click **Policies**.



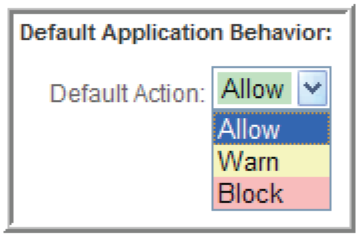
2. Click the policy you want to modify.



3. Click **Applications Manager**.

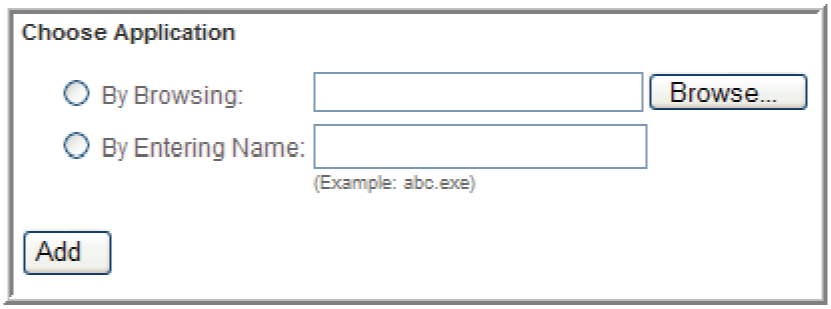


4. Under Default Application Behavior, in the Default Action drop-down list, specify how you want ContentProtect Professional to handle applications that are not included in the Application Management table (Allow, Warn, or Block).


Default Application Behavior:

Default Action: Allow

5. To create a list of applications, under Specific Application Behavior, click **Add or remove applications to be managed.**


Choose Application

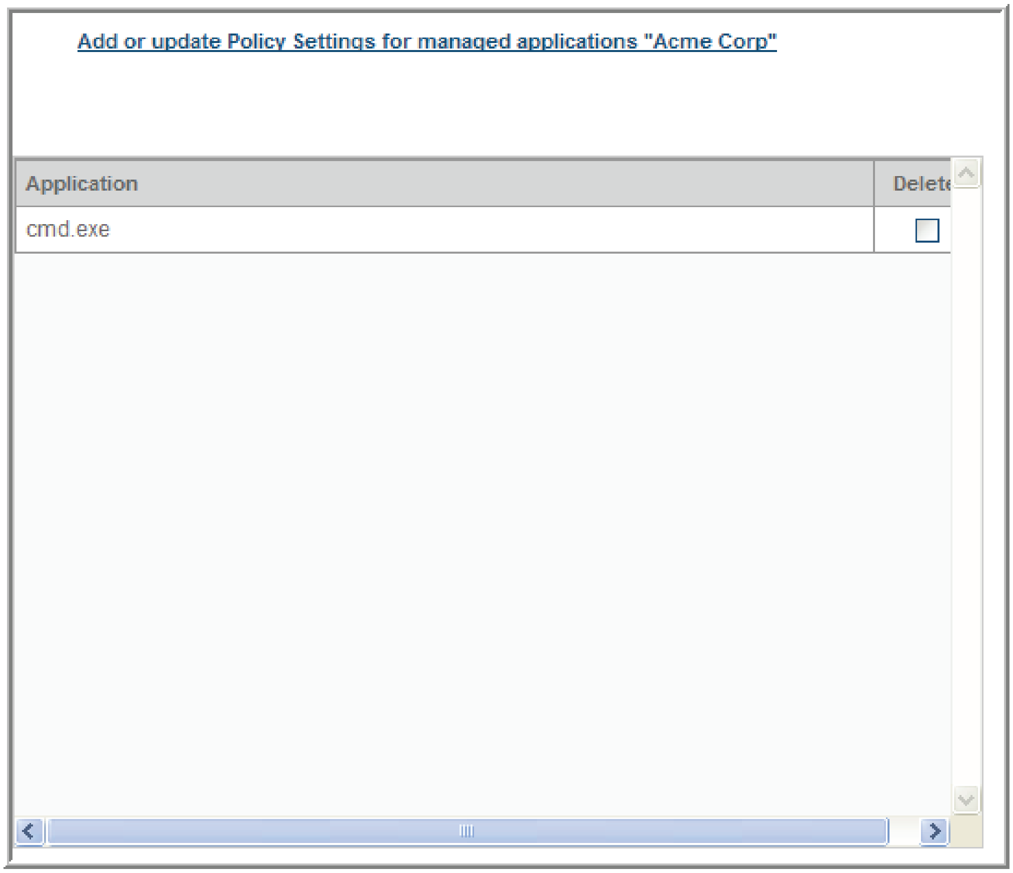
○ By Browsing:

○ By Entering Name:

(Example: abc.exe)

6. Browse to the application or enter its name, then click **Add**.

   The application is added to the list of applications.



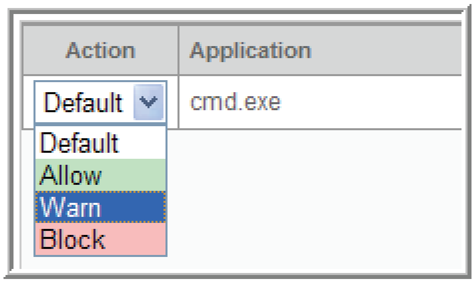
Add or update Policy Settings for managed applications "Acme Corp"

Application	Delete
cmd.exe	□

7. Click **Add or update applications to be managed**.

   The main page of the Application Manager opens, with a configurable list of applications.

8. Configure each application in the list.



Action	Application
Default	cmd.exe

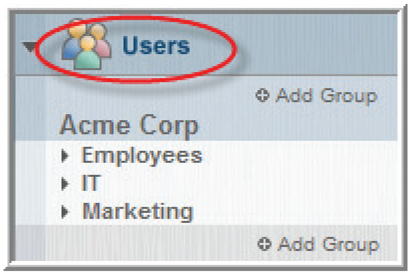
9. When you are finished, click **Save Changes**.

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:

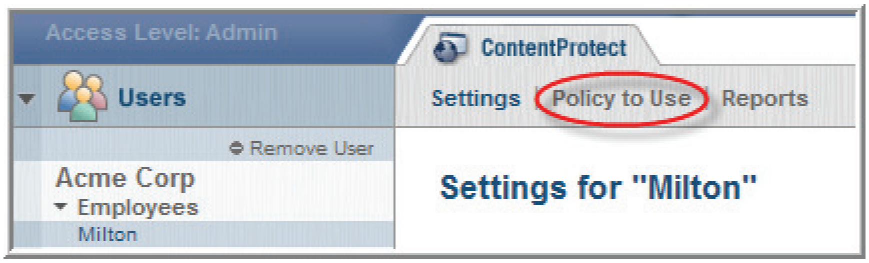
1. Click **Users**.



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

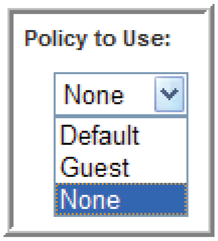
   Note: See the introduction to Managing Policies on page 33 for details on how policy assignments affect groups and users.

3. Click **Policy to Use**.

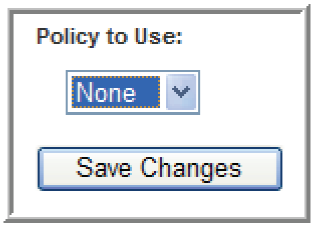


Settings for "Milton"

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



5. Click **Save Changes**.

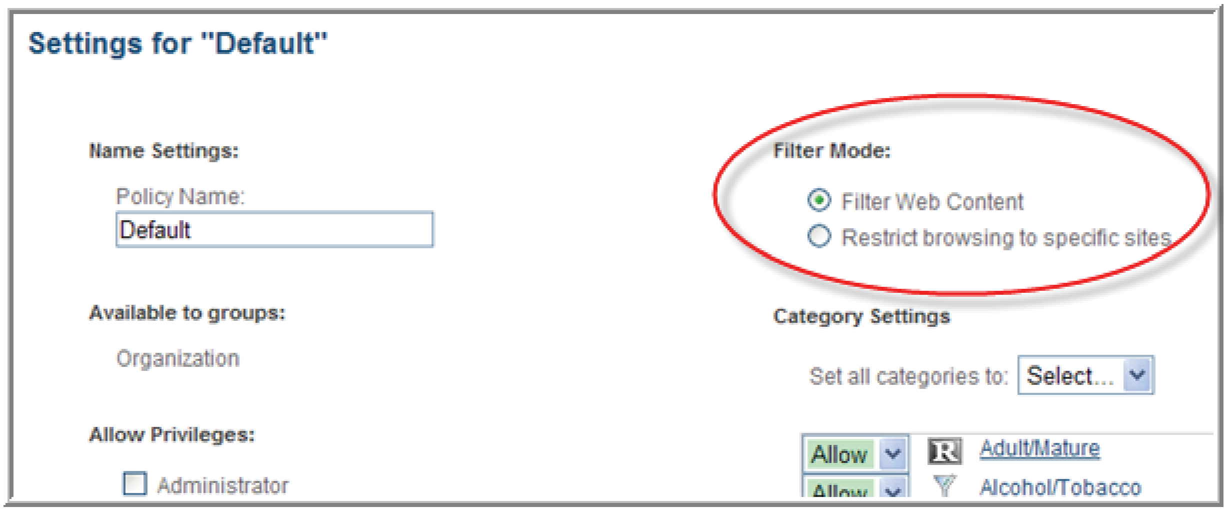


Specifying Allowed Web Sites

If you select Restrict browsing to specific sites the user is only allowed to browse to the sites listed. This is sometimes referred to as whitelist mode. You must have at least one site in the list of allowed sites. If no sites are listed, the user will not be able to access any Web sites.

To add a Web site to the list of allowed sites:

1. Locate the Filter Mode section of the Settings tab for the policy that includes the allowed sites.



Settings for "Default"

Name Settings:

Policy Name: Default

Available to groups:

Organization

Allow Privileges:

☐ Administrator

Filter Mode:

● Filter Web Content

○ Restrict browsing to specific sites

Category Settings

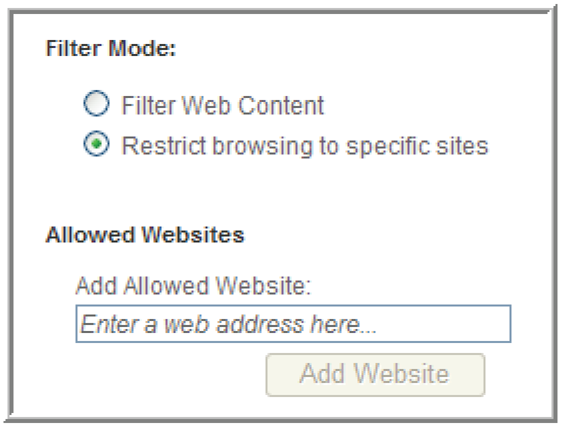
Set all categories to: Select...

Allow Adult/Mature

Allow Alcohol/Tobacco

2. Select Restrict browsing to specific sites.

   The Allowed Sites section containing the Website list appears.



Filter Mode:

○ Filter Web Content

● Restrict browsing to specific sites

Allowed Websites

Add Allowed Website: *Enter a web address here...*

3. Type the URL for the site you want to allow, then click **Add Website**.
4. Repeat steps 2 and 3 for each site you want to add.
5. Click **Save Changes** to save your changes.

After you have added sites to the list, you can select a site and click it to change the URL. You can also select a site and click **Delete** to remove it from the Allowed Sites list.

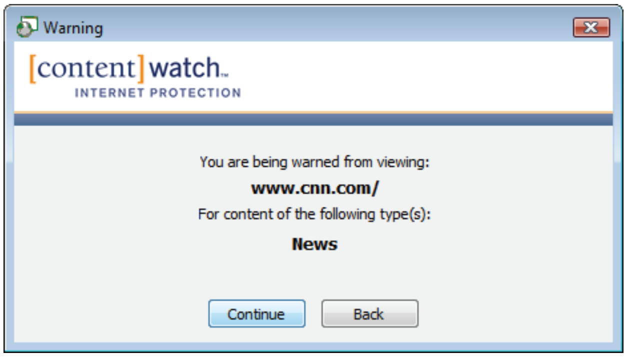
Block and Warning Messages

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:



You are being warned from viewing:

www.cnn.com/

For content of the following type(s):

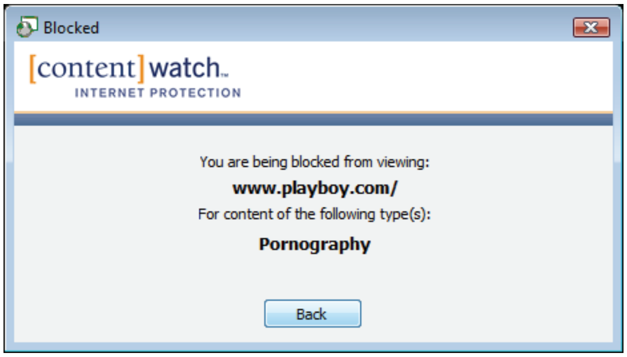
News

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 Record Activity Data From on page 36.

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:



You are being blocked from viewing:

www.playboy.com/

For content of the following type(s):

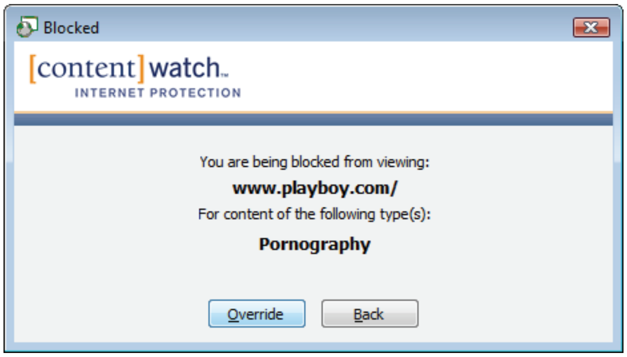
Pornography

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 Record Activity Data From on page 36.

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:



You are being blocked from viewing:

www.playboy.com/

For content of the following type(s):

Pornography

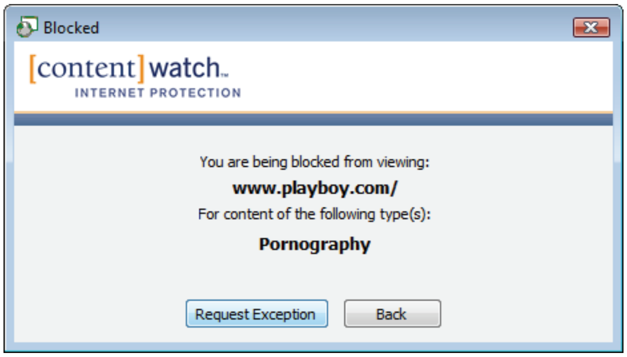
The user can click **Override** to enter the override password and view the requested Web site, or the user can click **Back** to return to the previous Web site. For some Web sites, the user might need to enter the override password more than once to view the content.

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 35.

The action is reported if activity reporting is enabled. For more information, see Record Activity Data From on page 36.

Block or Warning Messages with Request Web Exception Option

If a user has Request Web Exception 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:

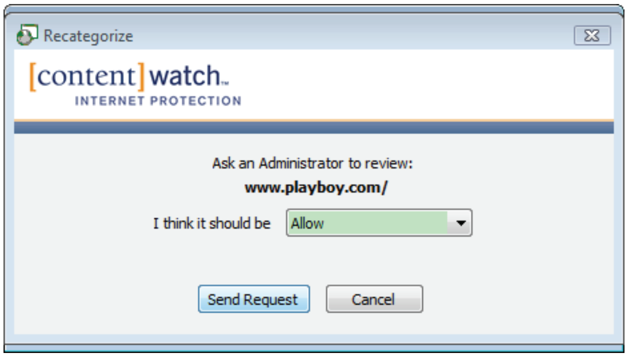

Blocked

You are being blocked from viewing:

www.playboy.com/

For content of the following type(s):

Pornography


Recategorize

Ask an Administrator to review:

www.playboy.com/

I think it should be Allow

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

1. Click **Request Exception** to display the Override Request dialog.
2. From the **I think it should be** drop-down list, select a suggested action (for example, allow the content or assign it to a new category).
3. 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 Exception Requests, see Processing Web Exception Requests on page 58.

   Note: If the user who is preparing the Web Exception Request has administrative privileges, he or she can click **Apply Now** (instead of **Send Request**) to immediately unblock or recategorize the Web page or Web site. The user is asked for the administrative user name and password, 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 Exception privileges, you must select the **Request Web Exception** option in the policy assigned to the user. For more information, see Allow Privileges on page 35.

The action is reported if activity reporting is enabled. For more information, see Record Activity Data From on page 36.

Working with Reports

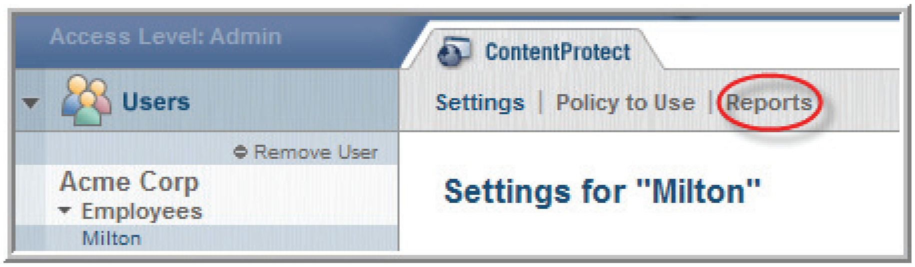
The Online Management application can generate reports for Web and instant messaging activity. These reports allow the administrator to view Internet usage information for the overall organization, a single group, or an individual user.

Important: ContentWatch servers store activity data for up to 30 days.

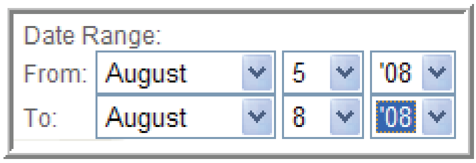
To view Internet usage reports:

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**.



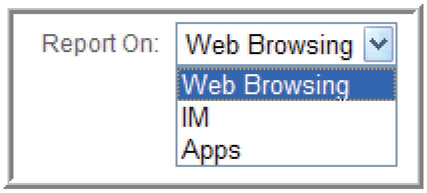
4. From the From and To drop-down lists, select the date range for the report.



Date Range:
From: August 5 '08
To: August 8 '08

.

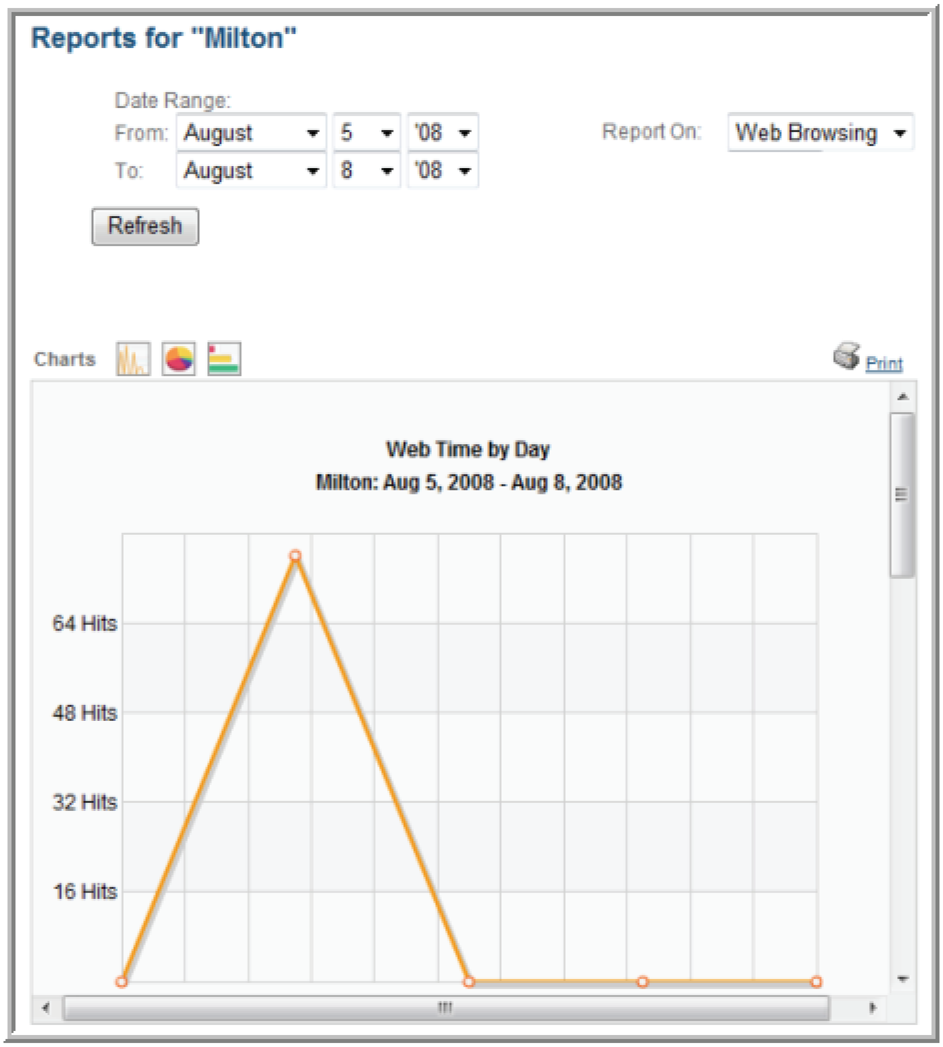
5. From the Report On drop-down list, select whether to report on **Web**, **IM** (instant messaging), or **Apps** Application Management) data.



Report On: Web Browsing

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

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



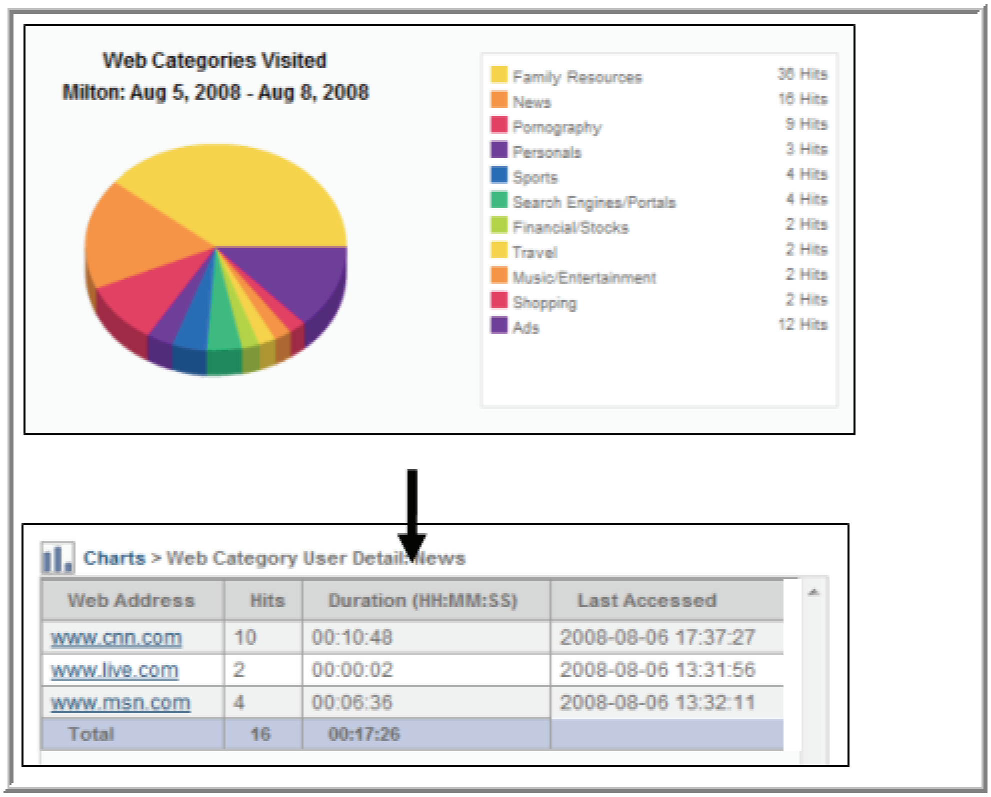
Reports for "Milton"

Date Range:
From: August 5 '08
To: August 8 '08

Report On: Web Browsing

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:

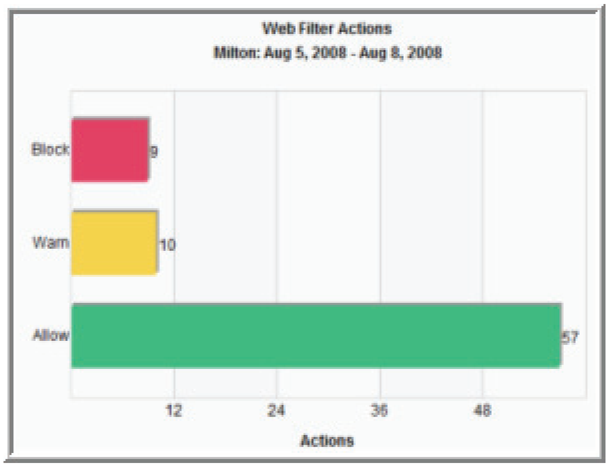

Web Categories Visited
Milton: Aug 5, 2008 - Aug 8, 2008
🟨 Family Resources 36 Hits
🟧 News 16 Hits
🟥 Pornography 9 Hits
🟪 Personals 3 Hits
🟦 Sports 4 Hits
🟩 Search Engines/Portals 4 Hits
🟩 Financial/Stocks 2 Hits
🟨 Travel 2 Hits
🟧 Music/Entertainment 2 Hits
🟥 Shopping 2 Hits
🟪 Ads 12 Hits

Charts > Web Category User Details: News

Web Address	Hits	Duration (HH:MM:SS)	Last Accessed
www.cnn.com	10	00:10:48	2008-08-06 17:37:27
www.live.com	2	00:00:02	2008-08-06 13:31:56
www.msn.com	4	00:06:36	2008-08-06 13:32:11
Total	16	00:17:26	

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.

You can view the ContentProtect filter actions. Click 📊 for a bar graph showing how many times ContentProtect allowed, warned, or blocked access to Web sites.



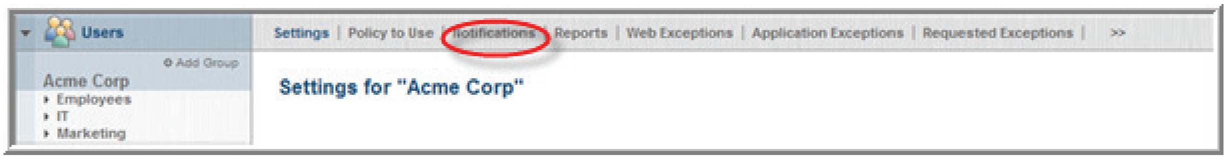
Note on Application Management reports: ContentProtect Professional gathers report data only for applications that have a “Block” or “Warn” action assigned to them. ContentProtect Professional does not gather report data for allowed applications or for applications classified as “Not Used” in a policy. 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. Notifications can be triggered by a variety of conditions, such as when any member of a group views a Web site after being warned, or when a specific user attempts to read a blocked newsgroup.

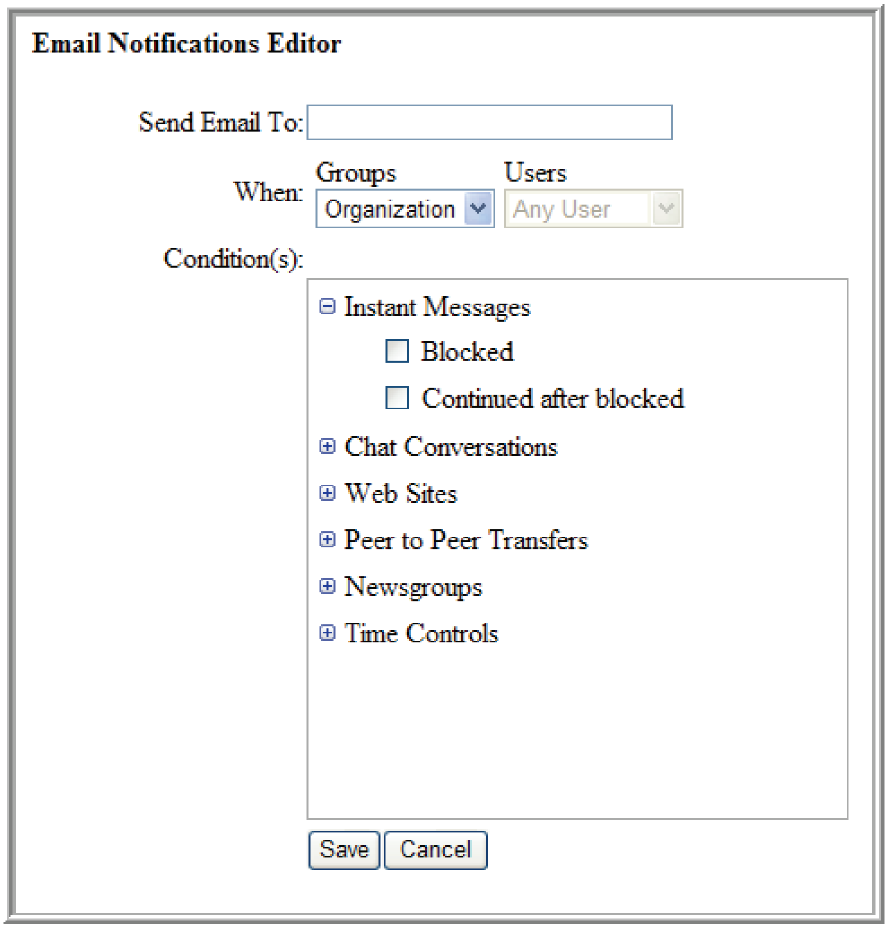
To configure email notifications:

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



4. (Conditional) If no notifications have been set, or if you are adding a new notification, click **Add**.

   To change an existing notification, click **Edit**.



Email Notifications Editor

Send Email To:

When: Groups: Organization; Users: Any User

Condition(s):

⊟ Instant Messages
- □ Blocked
- □ Continued after blocked

⊞ Chat Conversations

⊞ Web Sites

⊞ Peer to Peer Transfers

⊞ Newsgroups

⊞ Time Controls

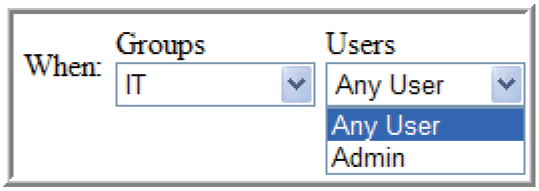
5. Type the email address where you want notifications to be sent.

6. Specify when a notification should be sent by selecting the group and user who perform the action that triggers the notification.

   Select **Organization** from the dropdown list to apply the notification to all groups.

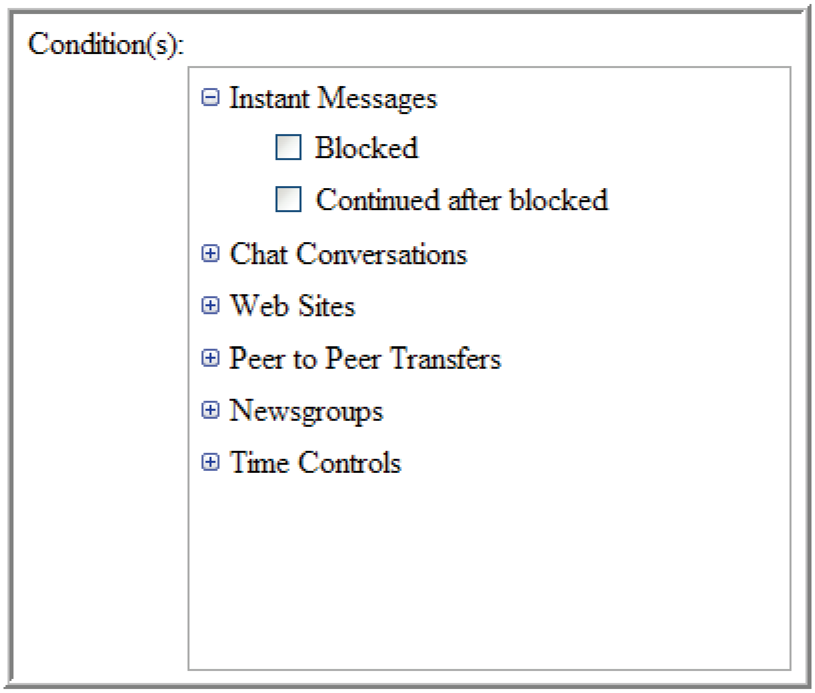
   Select **Any User** from the Users dropdown list to apply the notification to all users in the selected group.

   For example, if the notification applies to all users, select **Organization**, then select **Any User**. If the notification applies to all users in the IT group, select **IT**, then select **Any User**.



When: Groups: IT
Users: Any User

7. Select the conditions you want to be notified.



Condition(s):

⊟ Instant Messages

- □ Blocked
- □ Continued after blocked

⊞ Chat Conversations

⊞ Web Sites

⊞ Peer to Peer Transfers

⊞ Newsgroups

⊞ Time Controls

8. Click **Save**.

9. Repeat these steps 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.

Defining Web Exceptions

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 Category Settings on page 37 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 Exceptions 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.

You can use an asterisk (*) as a wildcard when creating exceptions. The asterisk represents one or more characters. For example, if you create *.google.* as an exception, it would match all of the following Web sites:

- http://www.google.com
- http://images.google.com
- http://www.google.net
- http://video.google.com/foo/bar

Likewise, *playboy* matches any URL that contains the word 'playboy' anywhere in the URL, including:

- http://www.playboy.com
- http://www.playboy.com/stories/page1.html
- http://www.somesite.com/pics/playboy/pic1.jpg
- http://www.somesite.com/pictures/show.cgi?image_source=playboy&img_number=123

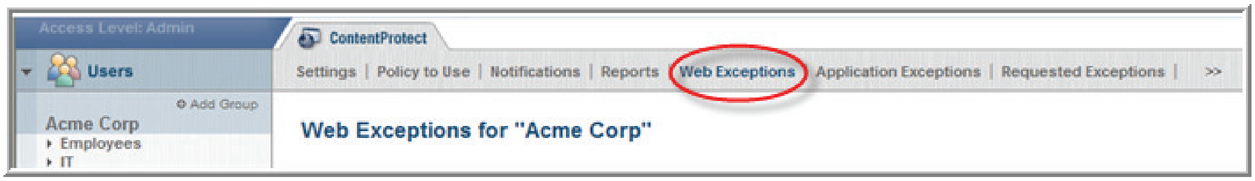
Warning: If the administrator manually assigns a site's content category, the system bypasses all automated site analysis. This means that as the site's content changes, ContentProtect Professional cannot determine the new category for the site. Use the Web Override feature with care.

To define a Web Override:

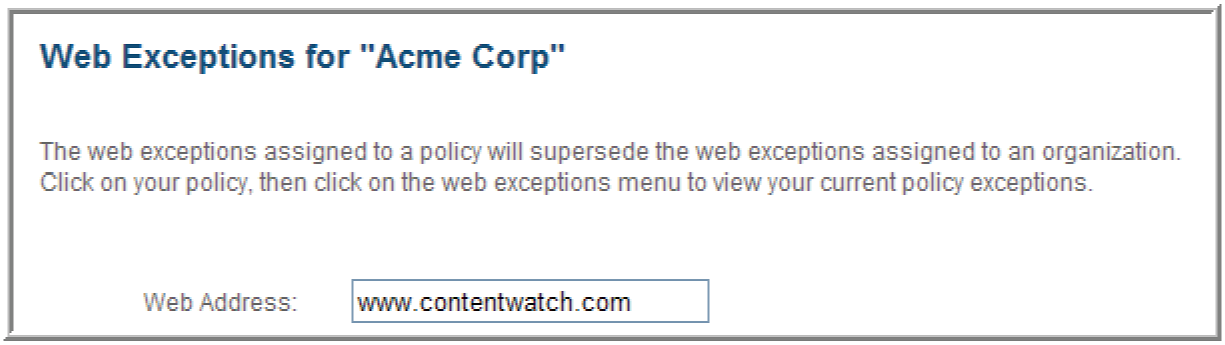
1. Log in to the Online Management application.

2. Make sure your organization's name is selected.

3. Click **Web Exceptions**.



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



Web Exceptions for "Acme Corp"

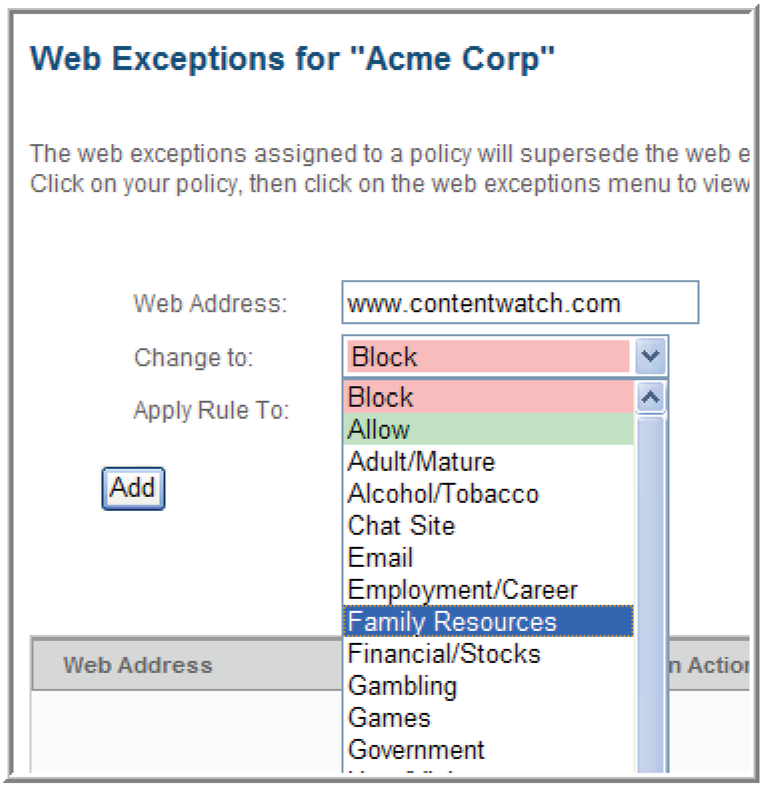
The web exceptions assigned to a policy will supersede the web exceptions assigned to an organization. Click on your policy, then click on the web exceptions menu to view your current policy exceptions.

Web Address: www.contentwatch.com

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

5. 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.



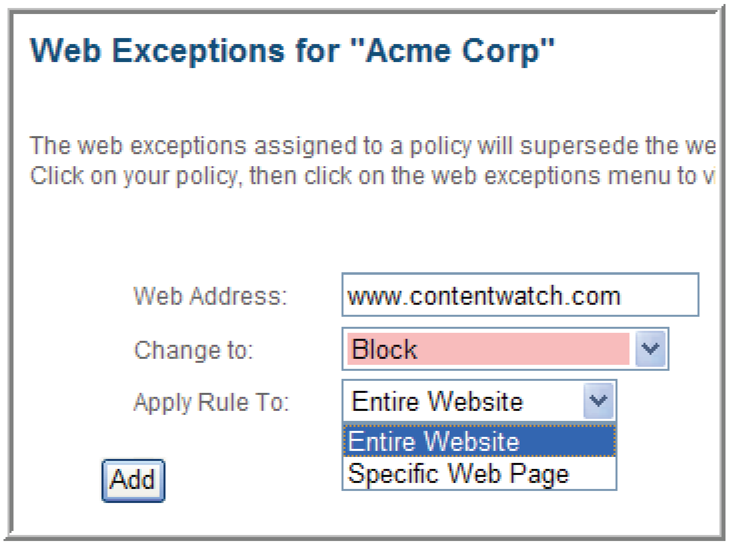
Web Exceptions for "Acme Corp"

The web exceptions assigned to a policy will supersede the web e
Click on your policy, then click on the web exceptions menu to view

Web Address: www.contentwatch.com

Change to: Block

6. 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 Exceptions for "Acme Corp"

The web exceptions assigned to a policy will supersede the we
Click on your policy, then click on the web exceptions menu to v

Web Address: www.contentwatch.com

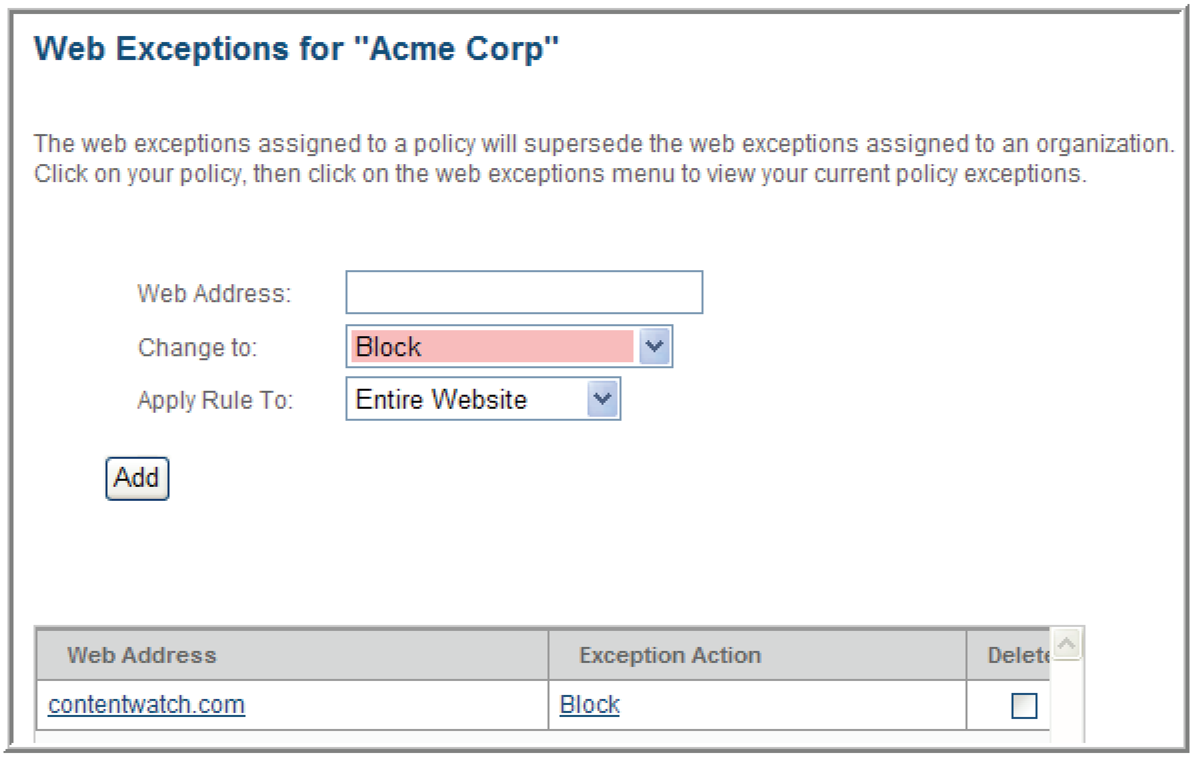
Change to: Block

Apply Rule To: Entire Website

7. Click **Add**.

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

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



Web Exceptions for "Acme Corp"

The web exceptions assigned to a policy will supersede the web exceptions assigned to an organization.
Click on your policy, then click on the web exceptions menu to view your current policy exceptions.

Web Address:

Change to: Block

Apply Rule To: Entire Website

Web Address	Exception Action	Delete
contentwatch.com	Block	□

Adding Applications to the Application Exceptions

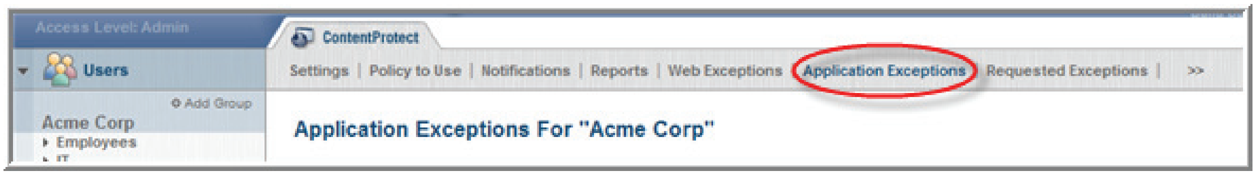
The ContentProtect Professional bypass list helps you work around conflicts that may arise between ContentProtect Professional and other Internet-enabled software on users' systems. For example, ContentProtect Professional may block some applications that require Internet access, such as financial software. 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 **Application Exceptions**.

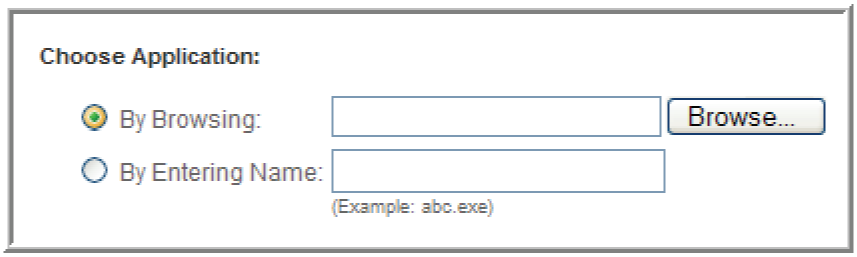

Access Level: Admin
Users
Add Group
Acme Corp
Employees
IT
ContentProtect
Settings | Policy to Use | Notifications | Reports | Web Exceptions | Application Exceptions | Requested Exceptions | >>
Application Exceptions For "Acme Corp"

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.

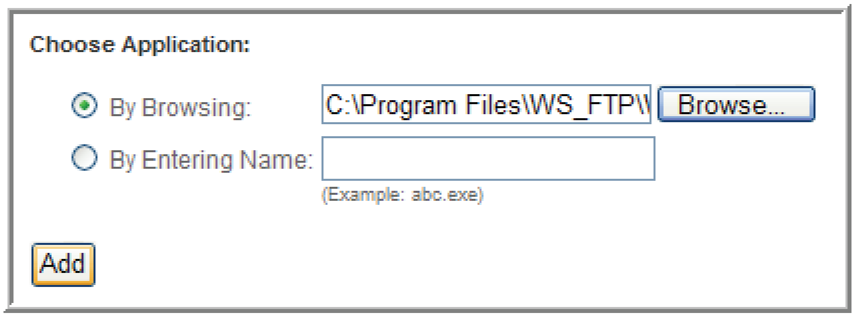
     b. Click **Browse**.



     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:

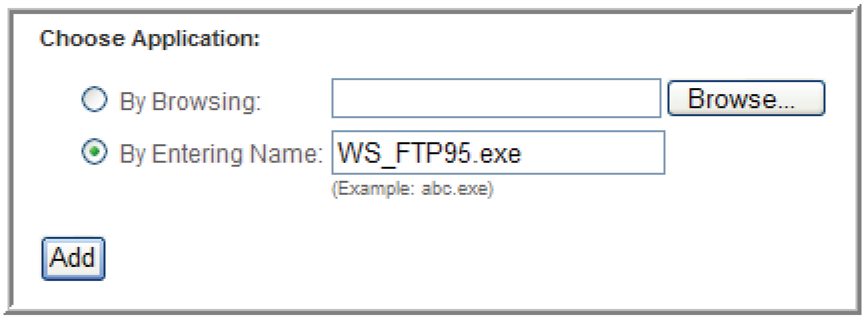
● By Browsing: C:\Program Files\WS_FTP\

- *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: WS_FTP95.exe

(Example: abc.exe)

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**.

Processing Web Exception Requests

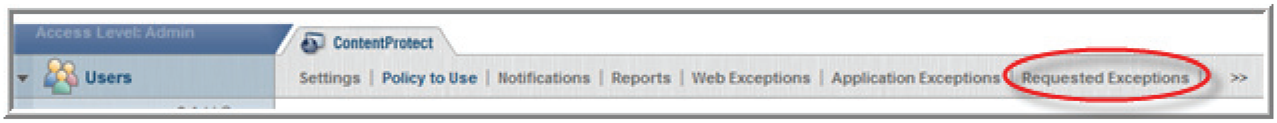
Users who have been granted Request Web Exception privileges can submit requests to the ContentProtect Professional administrator to unblock or recategorize specific Web pages or entire Web sites that fall under a blocked or warning category. The administrator can review these requests in the Online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

To process Web Exception Requests:

1. Log in to the Online Management application.

2. Make sure your organization's name is selected.

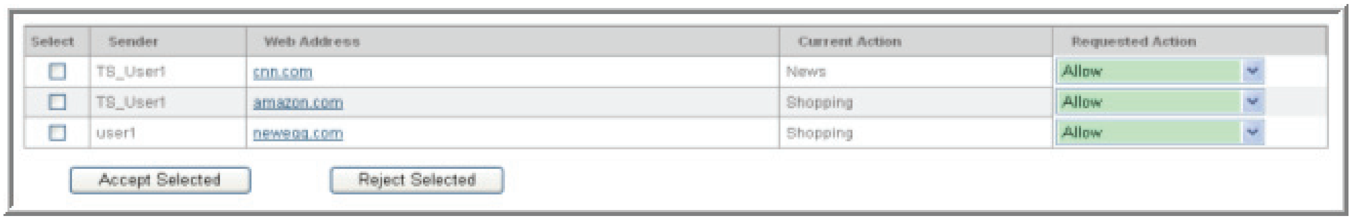
3. Click **Requested Exceptions**.



Access Level: Admin
ContentProtect
Users
Settings | Policy to Use | Notifications | Reports | Web Exceptions | Application Exceptions | Requested Exceptions
>>

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.

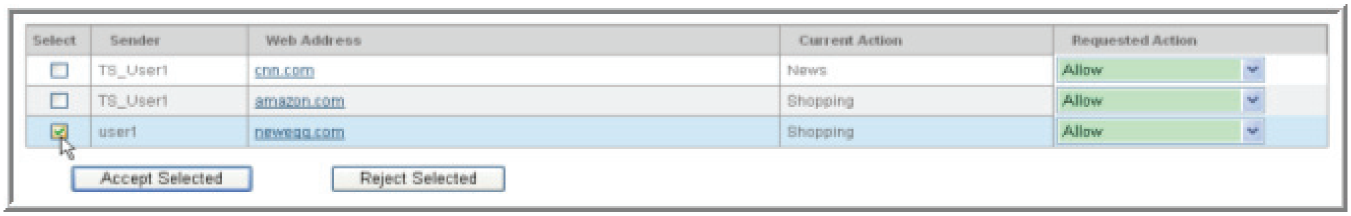
   You can click the hyperlinks in the Web Address column to open requested Web sites in a browser and review their content. Also, before accepting a request, you can change the action or category the user has requested by selecting a different option in the appropriate Requested Action drop-down list.



Select	Sender	Web Address	Current Action	Requested Action
□	TS_User1	cnn.com	News	Allow
□	TS_User1	amazon.com	Shopping	Allow
□	user1	newegg.com	Shopping	Allow

5. To process a request:

   a. Select the request's **Select** check box.



Select	Sender	Web Address	Current Action	Requested Action
□	TS_User1	cnn.com	News	Allow
□	TS_User1	amazon.com	Shopping	Allow
☑	user1	newegg.com	Shopping	Allow

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

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

Controlling User's Access to Applications

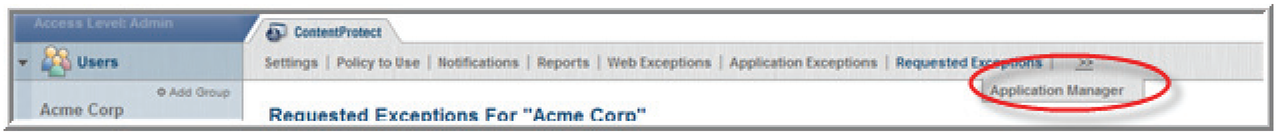
The ContentProtect Professional Suite Application Manager feature lets you control which applications users can run on their desktop computers. Since employees nowadays can easily install applications that may present security threats, Application Manager enhances your corporate security and compliance 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. Mouse over the **>>** icon, then click **Application Manager**.



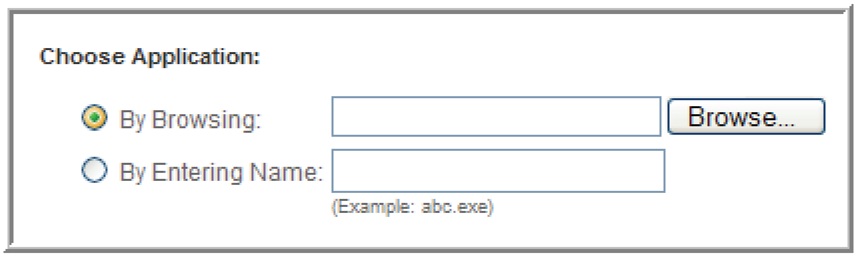
Access Level: Admin
Users
Add Group
Acme Corp
ContentProtect
Settings | Policy to Use | Notifications | Reports | Web Exceptions | Application Exceptions | Requested Exceptions | >>
Application Manager
Requested Exceptions For "Acme Corp"

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: [ ] Browse...

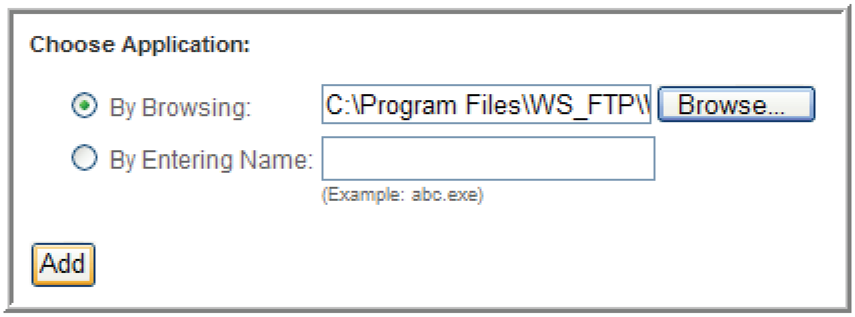
○ By Entering Name: [ ]

(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.



Choose Application:

● By Browsing: C:\Program Files\WS_FTP\\

○ By Entering Name:

(Example: abc.exe)

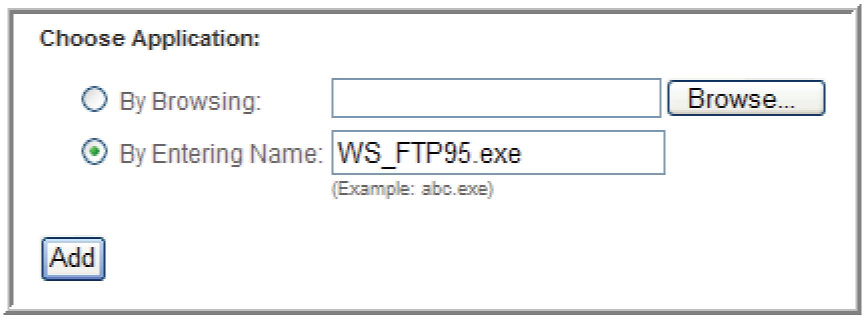
- *Method 2:* Enter the filename of the application's executable file.

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, then select **Internal Name** from the Item Name list.

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



Choose Application:

○ By Browsing:

● By Entering Name: WS_FTP95.exe

(Example: abc.exe)

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.

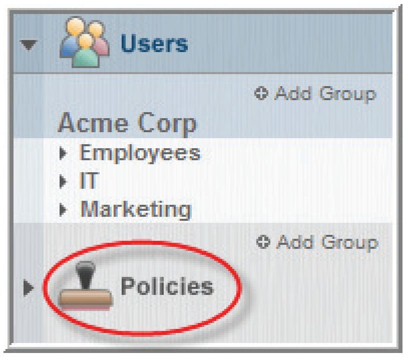
b. Click **Delete Selected**.

Editing Policies for Application Management

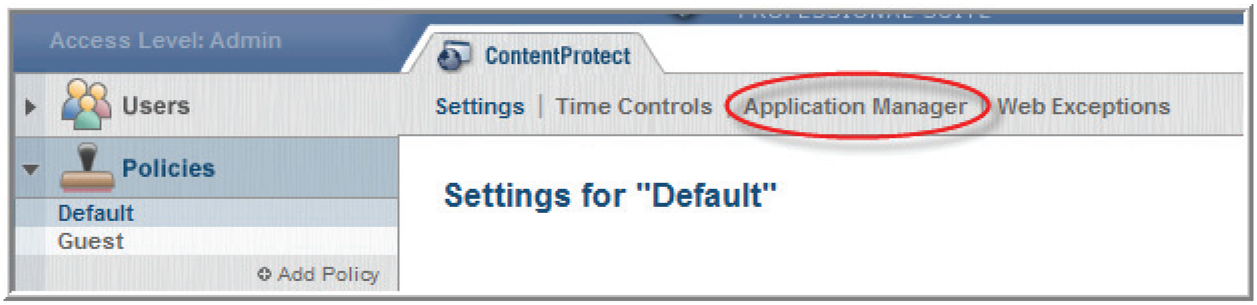
Once you have added programs to the Application Management table, you can control users' access to these programs by modifying Application Manager settings in your policies.

To modify Application Manager settings for a policy:

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

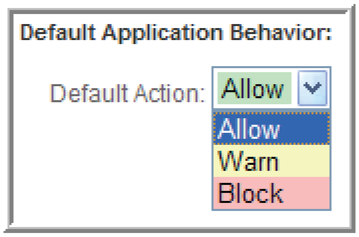


2. Click the policy you want to modify. Click **Application Manager**.



3. Under Default Application Behavior, from the Default 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**).

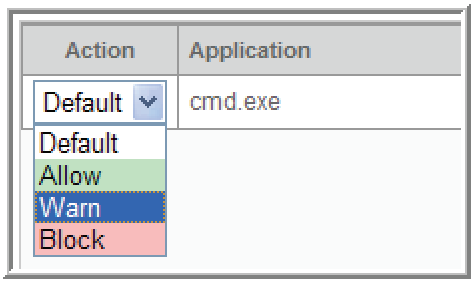
   If you select **Allow**, you create, in effect, a white list of all allowed applications. If you select **Block**, you essentially create a black list of all the applications you want to block.



Default Application Behavior:

Default Action: Allow

4. 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 (**Default**, **Allow**, **Warn**, or **Block**).



Action	Application
Default	cmd.exe

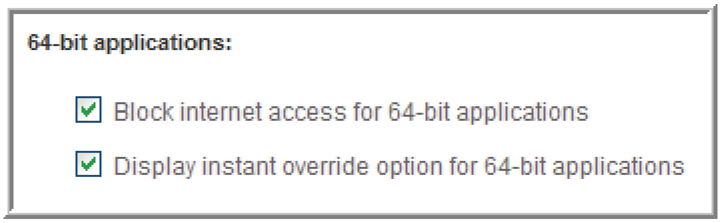
5. When you are finished setting the actions for each application in the table, click **Save Changes**.

Blocking 64-Bit Applications

You can choose to block 64-bit applications. This prevents users from bypassing Internet blocks by using a 64-bit browser.

To block 64-bit applications:

1. Click your organization name.
2. Click **Policy to Use**.
3. Select the policy you want to edit to block 64-bit applications, then click **Edit Policy**.
4. In the settings for the chosen policy, scroll down until you see the 64-bit applications section.



64-bit applications:

☑ Block internet access for 64-bit applications

☑ Display instant override option for 64-bit applications

5. Select **Block internet access for 64-bit applications**.
6. If you want to provide the option to override the block, select **Display instant override option for 64-bit applications**.
7. Click **Save Changes**.

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, 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 on the eDonkey/eMule, Bittorrent, KaZaA, and GNUtella networks.

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