



**Client Policy Manager™
Administrator's Guide**

Websense Enterprise[®] v5.5.2 Client Policy Manager[™] Administrator's Guide

©1996–2005, Websense, Inc.

All rights reserved.

10240 Sorrento Valley Rd., San Diego, CA 92121, USA

Published May 2, 2005

Printed in the United States of America

NP33-0003CPMADMIN

This document may not, in whole or in part, be copied, photocopied, reproduced, translated, or reduced to any electronic medium or machine-readable form without prior consent in writing from Websense Inc.

Every effort has been made to ensure the accuracy of this manual. However, Websense Inc., makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Websense Inc. shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Trademarks

Websense and Websense Enterprise are registered trademarks of Websense, Inc. in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

Microsoft, Windows NT, Windows 2000, Windows 2003, Windows XP, Internet Explorer, and Active Directory are trademarks or registered trademarks of Microsoft Corporation.

Solaris is a registered trademark of Sun Microsystems, Inc., in the United States and other countries. Sun, Sun ONE and all Sun ONE based trademarks and logos are trademarks of Sun Microsystems, Inc.

Netscape is a registered trademark of Netscape Communications Corporation in the U.S. and other countries. Netscape Navigator and Netscape Communicator are also trademarks of Netscape Communications Corporation and may be registered outside the U.S.

The following is a registered trademark of Novell, Inc., in the United States and other countries: Novell Directory Services. Adobe, Acrobat, and Acrobat Reader are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States and/or other countries.

Pentium is a registered trademark of Intel Corporation.

Red Hat is a registered trademark of Red Hat, Inc., in the United States and other countries.

Linux is a trademark of Linus Torvalds, in the United States and other countries.

This product includes software distributed by the Apache Software Foundation (<http://www.apache.org>).

Copyright (c) 2000. The Apache Software Foundation. All rights reserved.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Contents

Chapter 1	Introduction	15
	CPM Security Against Viruses	18
	Launch Control and Network Access	19
	The Outbreak Rule and Viruses	20
	Lockdowns and Viruses	20
	Port Blocking and Viruses	21
	Zero Day Response Functionality	22
	Reporting	22
	Naming Conventions	23
	Identifying Corporate Goals	24
	Security	24
	Productivity	24
	Security and Productivity	25
	Educating Employees	25
	Identifying Organizational Roles	26
	Installing and Configuring Client Policy Manager	28
Chapter 2	Understanding CPM Basics	31
	Shared Subscriptions	32
	Understanding the CPM Operating Environment	32
	Shared Websense Enterprise Components	33
	Policy Server	34
	User Service	34
	Websense Enterprise Manager	35
	CPM Components	37
	CPM Server	38
	Client Deployment Service	38
	Client Agent	39

Client Agent Startup Functions	40
Client Agent Offline Functions for CPM	40
Client Policy Manager Databases	41
Database Engine Requirements	42
Websense Enterprise Master Database	42
CPM Inventory Database	45
CPM Log Database	46
Reporting Tools	47
CPM Reporter	47
Explorer for CPM	48
Client/Server Authenticated Communications	50
CPM Policy Differential Downloads	51
Rules and the CPM Policy	51
Part 1: Status Options	52
Part 2: Launch Control	52
Part 3: Port Access Control	53
Part 4: Event Logging	54
Implementing the CPM Policy	56
Chapter 3 Configuring Client Policy Manager	59
Working with Policy Server	60
Adding a Policy Server	60
Connecting to a Policy Server	61
Disconnecting from a Policy Server	62
Deleting a Policy Server	62
Accessing the Settings Pane	63
Subscribing to CPM	63
Working in the Proxy/Authentication Pane	65
Identifying the Proxy Server	66
Forcing Authentication	66
Setting Email Notification for Administrators	67
Configuring User Services	69
Configuring Windows NT Directory	69
Configuring Active Directory Services	71
Adding a Domain Forest	72
Entering Advanced Settings	74

Understanding Database Downloads	77
Defining the Database Download Schedule	78
Monitoring Database Downloads	80
Manually Requesting a Database Download	80
Changing the Password	82
Introducing AppCatcher	83
Configuring AppCatcher	85
AppCatcher Transfer Details	86
User Messages	87
Customizing Text	88
Block Messages for Executables	90
Continue Messages for Executables	90
Network Lockdown Messages for Ports	91
Removable Media Lockdown Message	92
Controlling User Overrides	93
Using Websense HTML Tags	94
Employee Interaction with Messages	95
Interacting with the Executables Block Message	96
Interacting with the Continue Message	97
Interacting with the Network Lockdown Message	98
Interacting with the Removable Media Lockdown Message	99
Reviewing the More Information Message	100
Configuring the Database Connection	101
Setting Client Control	102
Understanding Heartbeats	102
Inventories and Heartbeats	103
Understanding CPM Client-to-Client Distribution	103
Understanding the Application Logging Interval	104
Defining Client Control	104
Globally Enabling and Disabling the CPM Policy	106
Disabling CPM Policy	107
Restoring CPM Policy	107

Chapter 4	Getting Started With Client Policy Manager.....	109
	Working in Websense Enterprise Manager	109
	Menu Options	110
	My Websense.....	110
	Navigation Pane Selections	111
	Content Pane Presentation.....	112
	Symbols	113
	Refreshing Data	114
	Making Multiple Selections.....	114
	Selecting the Web Browser	115
Chapter 5	Viewing Summary Data	117
	Emergency Outbreak Rule Processing	118
	Adding an Emergency Outbreak Rule Entry.....	121
	Removing an Emergency Outbreak Rule Entry	123
	Disabling Client Outbreak Distribution.....	123
	Desktop Lockdown Suite	125
Chapter 6	Deploying Client Agent.....	127
	Client Agent Requirements.....	129
	Deploying Client Agent for Windows XP.....	130
	Upgrading Client Agent v5.2 to v5.5.2	130
	VPN Support	130
	Deploying Clients: The Process	131
	Accessing the Deployment Status Pane	132
	Managing Client Options	134
	Deploying or Uninstalling Client Agent	135
	Refreshing Deployment Data	138
	Removing Clients From the Selected Clients List	138
	Canceling Client Agent Deployment.....	139
Chapter 7	Working with Client Status	141
	Accessing the Client Status Pane	141
	Managing Asset Tags	143
	Adding an Asset Tag	144

	Editing an Asset Tag	145
	Clearing an Asset Tag	146
	Viewing Client Detail	147
	Deleting Clients From the Client Status Pane	148
	Resetting Overrides	149
Chapter 8	Working with Inventories	151
	Understanding Inventories	151
	Inventory Retries	152
	Inventories and Websense Enterprise Manager	153
	Inventories and CPM Reporter	153
	Inventories and Heartbeats	154
	Accessing the Inventory Status Pane	154
	Checking Machine Details in the Inventory Status Pane	155
	Understanding Inventory Status Messages	156
	Running an Inventory	157
	Removing Machines From the Selected Clients List	161
	Canceling an Inventory	161
	Clearing Completed Inventory	161
	Managing Inventories	162
	Generating Software Sets from Inventories	164
	Generating a Software Set for a Specific Machine	164
	Generating a Software Set for Shared File Machines	165
	Inventories, Generated Software Sets, and Rules	167
	Viewing Inventories	167
	Software Views	169
	Filtering the Current Software View	169
	Removing Filters	171
	Software Executables View	171
	Software Applications View	172
	Hardware Views	172
	Deleting an Inventory	174
Chapter 9	Applying Lockdowns	177
	Inventory Lockdown	177
	Lockdowns and User Policy	178

	Applying an Inventory Lockdown	178
	Removing a Lockdown	179
	Express Lockdown	180
	System Requirement	180
	Configuring Express Lockdown	180
	Viewing Lockdown Status.	183
	View Options	184
	Machine Data	185
	Removable Media Lockdown.	185
	Supported External Bus Types	186
	Configuring Removable Media Lockdown.	186
	Viewing Lockdown Status.	188
	View Options	188
	Machine Data	189
	Block Message for Removable Media Lockdown.	189
	Logging in a Lockdown Environment.	189
Chapter 10	Working with Client Sets	191
	Planning for Client Sets	192
	Accessing the Current Client Sets Pane	193
	Managing Client Sets	194
	Adding a Client Set	196
	Editing a Client Set	197
	Removing a Client from a Client Set.	198
	Copying a Client Set	198
	Deleting a Client Set	199
Chapter 11	Working with Categories	201
	Websense Categories	202
	Custom Categories	205
	Risk Classes	205
	Accessing the Categories Pane	207
	Understanding Category Data	209
	Viewing Executable Details	209
	Finding an Executable From the Categories Pane.	210
	Moving an Executable from One Category to Another.	212

Reverting an Executable to the Websense Category	214
Managing Custom Categories	215
Adding a Custom Category	216
Renaming a Custom Category	217
Deleting a Custom Category	218
Using the Classification Wizard	219
Chapter 12 Working with Software Sets	225
Predefined Software Sets	226
Planning for Custom Software Sets	227
Software Sets for Machines	228
Software Sets for Users	228
Software Sets for Machines and Users	229
Accessing the Current Software Sets Pane	229
Managing Software Sets	231
Adding a Software Set	232
Editing a Software Set	235
Copying a Software Set	236
Deleting a Software Set	237
Working in Software Sets	237
Viewing Software Set Contents	238
Searching For and Adding an Executable	239
Manually Adding a File Name to a Software Set	240
Removing an Item from a Software Set	242
Chapter 13 Working with Port Sets	243
Prepopulated Port Sets	244
Accessing the Current Port Sets Pane	244
Managing Port Sets	245
Adding a Port Set	246
Adding a Port to the Port List Manually	247
Adding a Range of Ports to a Port Set	249
Deleting a Port from the TCP or UDP Port List	249
Editing a Port Set	251
Copying a Port Set	252
Deleting a Port Set	253

Chapter 14	Working with Rules	255
	Understanding Rules	255
	Status Settings	256
	Software Launch Control	257
	Network Access Control	259
	Logging	260
	Logging User Data	261
	Logging Machine Data	262
	Websense Rules	262
	Emergency Outbreak Rule	263
	System Files Rule	263
	Harmful Software Rule	264
	Mass Mailing Rule	264
	Lockdown Rule	265
	Global Rule	266
	Connected and Disconnected Rules	266
	Recommended Rules	267
	Understanding the CPM Policy	268
	Policy Updates	270
	Developing the CPM Policy	270
	Goal: Zero Day Response	270
	Goal: Security	271
	Goal: Productivity	271
	Goal: Security and Productivity	272
	Goal: Flexible CPM Policy	273
	Identifying Access Levels	273
	Rule Precedence	275
	Example 1: Only Websense Rules	275
	Example 2: Basic Rule Set	276
	Example 3: Lockdown Rule	277
	Example 4: Manually Entered File Names	278
	Example 5: User and Group Rules	280
	Example 6: Connected/Disconnected Rules	282
	Streamlining Rules	283

The Rules Pane	285
Rule Components	286
Accessing the Rules Pane	287
Reverting Changes	287
Adding a Rule	288
Copying a Rule	291
Editing a Rule	292
Moving a Rule	293
Deleting a Rule	294
Disabling a Rule	294
Excluding Users From Logging	294
Policy Changes and Exiting Websense Enterprise Manager	295
Chapter 15 Troubleshooting	297
Troubleshooting Database Issues	297
Why am I having trouble accessing Websense download sites and my.websense.com?	297
Why can't I download the Websense Enterprise Master Database or send AppCatcher data to Websense?	298
Proxy Information is Required	298
Proxy Information is Not Required	299
Authentication is Required	299
Firewall Restrictions	299
Restriction Applications	300
Where can I find error messages when a Websense Enterprise Master Database download fails?	300
Why am I receiving an "Unable to connect to database" error message?	300
What do I do if a database becomes too large?	301
Troubleshooting Websense Enterprise Manager Functions	302
Why can't I access CPM Reporter from Websense Enterprise Manager?	302
Why can't I connect to the User Service?	302
Restarting the CPM Server	302
Changing the Account	303
What happens if I reconfigure the IP address for CPM Server?	303

Why isn't the CPM policy being enforced?	304
Why isn't updated information appearing in Websense Enterprise Manager?	304
How can I see uncategorized executables?	304
Troubleshooting Inventory Problems	305
Why do I get an error message when I run an inventory?	305
Why do I receive an error message for hardware inventories?	305
Why do I see two entries in the Hardware Inventory list for the same machine?	306
Why can't I view physical memory data in the Hardware View?	307
Why do I see several rows containing the same data in Software Executable Inventory views?	307
Why aren't ZIP drives appearing in inventories?	307
Why do hardware inventories show a fixed hard disk entry with a size of 0.0 GB?	308
Why can I see inventory results in the CPM Inventory Database but not in the Inventory pane in Websense Enterprise Manager?	308
Troubleshooting Client Agent Problems	308
Why are services on a Windows NT machines having problems starting?	308
Why can't I see machines running Client Agent any longer?	309
Why can't I see a machine in the Client Status dialog box?	309
Why do I receive an error message stating "Unable to read workstation data" when I access Client Policy Manager functions in Websense Enterprise Manager?	309
Why don't employees see block or continue messages associated with screen savers on machines running Windows NT or Windows 2000?	310
Why do employees sometimes receive series of block or continue messages?	311
Why am I seeing between 80% and 95% CPU usage on Windows NT machines?	312
Why are employees at machines that are locked down having problems launching software that is included in the inventory?	312
Why are employees having problems with machines where I upgraded Client Agent 5.2 to Client Agent 5.5.2?	313

Appendix A	Technical Support	315
	Websense Technical Services Support Center	315
	Fee-based Support	315
	Support Options	315
	Web Portal	315
	Email Questions	316
	Telephone Assistance	316
	Improving Documentation	317
Appendix B	CPM Category Definitions	319
	Access/Privacy/Security Category	319
	Audio/Video Category	320
	Communication Category	321
	Critical Functions - Never Block Category	322
	Entertainment Category	323
	Malware Category	323
	Miscellaneous Category	324
	Productivity Category	324
	System Category	327
Appendix C	Websense Port List	329
	Glossary	333
	Index	341

Introduction

Websense Enterprise® Client Policy Manager™ (CPM) is an innovative end-point security solution that extends the power of Websense Enterprise to corporate desktops, laptops, and servers. CPM delivers Zero Day protection against unknown security threats, including today's sophisticated blended virus, worm, and Trojan horse attacks.

The CPM policy can also stop the execution of unauthorized applications such as spyware, peer-to-peer file sharing (P2P), and hacking tools, while enabling flexible policy management of applications such as instant messaging (IM) or remote control tools, which only selected users or groups are allowed to use.

Complementing traditional firewall and anti-virus tools, CPM closes the window of exposure to unknown security threats that often bring down networks before virus signatures or appropriate patches can be deployed, or in cases, where security systems are mis-configured. CPM prevents today's fast-moving blended security threats from launching at the desktop and propagating across the network. This Zero Day protection enables organizations to reach higher levels of network security and up time for their mission-critical systems and applications.

Based on a unique application database with over 50 categories, IT administrators can create a CPM policy using categories that stop the execution of unauthorized applications on connected desktops, mobile laptops, and servers. The application database, along with the CPM best-in-class browser-based forensics reporting capabilities, empowers IT to detect and analyze security threats and application activity in the corporate computing environment. Only CPM delivers effective, comprehensive threat detection and flexible application use policy enforcement, enabling organizations to significantly boost their enterprise security and employee productivity.

By preventing unauthorized, malicious applications from launching on corporate PCs, CPM helps mitigate costly security threats, and does so even for disconnected laptops. Going beyond--and yet complementing traditional

firewall and anti-virus solutions--CPM shields the corporation from security threats and boosts employee protection and productivity.

CPM offers a practical way to protect corporate end-points from well-known security threats, as well as those that have yet to be identified. And CPM is unique - featuring the only database of applications classified into categories, enabling quick and easy implementation of the CPM policy on, for example, the "Hacking" category: "No employee will be allowed to launch a hacking application."

IT no longer has to worry about keeping abreast of the growing list of malicious applications--the Websense Master Database, updated nightly, does this. And IT can be confident in the solution, as Websense is recognized as the worldwide leader in integrated filtering solutions that protect and optimize the interaction between employees and their computing resources.

The high-level business benefits CPM affords organizations are the following (in order of importance):

- ◆ **Stronger desktop / laptop security:** CPM helps stop unknown viruses or worms from spreading in the enterprise leading to higher application and network uptime, and also protects sensitive corporate data by limiting access to unregulated communication via P2P and spyware.
- ◆ **Higher employee productivity:** CPM enables IT and Business managers to set appropriate application use rules for corporate PCs. By blocking access to inappropriate and/or unauthorized applications such as games and instant messaging, employee productivity is maximized.
- ◆ **Lower desktop management costs:** CPM reduces help desk and desktop administration costs by eliminating software incompatibilities and their subsequent help desk calls and providing better visibility into the desktop environment through application launch and inventory reports. Software conflicts, often expensive and time consuming to address, created by spyware applications alone are creating an ever-increasing burden on IT Help Desks.

These benefits are available as soon as you purchase and install Websense Enterprise Client Policy Manager. Configuration is easy, and provides monitoring and control functions almost immediately.

Websense Enterprise Client Policy Manager offers organizations the following functionality:

- ◆ Zero Day protection against unknown security threats
 - **Network Access Lockdown** closes the window of exposure to unknown security threats by preventing these attacks from communicating or propagating over the network.
 - **Application Lockdown** allows an approved set of applications to run on corporate PCs and servers and thereby prevents unknown malicious applications from launching.
 - **Outbreak Mode** prevents the launching of specific viruses and worms by enabling IT to stop malware in real-time, specifically when the actual outbreak is occurring.
- ◆ Flexible auto-updating CPM policy
 - The downloaded application database is fully integrated with the Websense Enterprise Master Database. This unique database of categorized applications enables IT administrators to enforce a flexible and auto-updating CPM policy that manages appropriate use of programs like instant messaging and stop the execution of unauthorized applications such as spyware, P2P, and hacking tools.
 - AppCatcher™/ ProtocolCatcher™ automatically and anonymously categorizes unknown applications and captures network behavior for specific applications so the CPM policy stays current with the most relevant applications and protocols in each organization's environment.
 - Connected/disconnected rules enables IT to enforce the CPM policy for all users including mobile employees with laptops.
- ◆ Almost instant reports for analyzing desktop security threats and application activity
 - Explorer for CPM is an interactive, browser-based forensics and reporting tool that detects application launch and network access attempts by employee, department, date, and most importantly, by application category.
 - CPM Reporter is a browser-based reporting tool that provides “out-of-the-box” application launch and inventory reports that can be automatically scheduled and distributed.

- Inventory views in Websense Enterprise Manager show critical hardware and software information. The details show categorized and normalized views of applications and executables and the hardware available at any machine where inventory has taken place.
- ◆ Seamless integration into the existing enterprise network infrastructure
 - Directory integration with Windows Active Directory and NT 4.0 enables IT administrators to detect security threats and enforce rules that impact application launches by user and groups, in addition to systems and machines.
 - Websense Enterprise Manager, the administration console for CPM, serves as a central management console for managing employee computing across the gateway (Web filtering), network (protocol management), and the desktop (application launch and network access).

CPM Security Against Viruses

Client Policy Manager and anti-virus solutions are different but complimentary. Anti-virus applications stop malicious programs and scripts by generating an application signature and checking it against a list of existing signatures. CPM compliments this layer of security by letting organizations block or question launches when the executable is not identified. The ability to block unknown executables is a critical security factor, since some malicious code can change names rapidly.

Five CPM functions are critical for application launch and network access security:

1. **Launch and Port Control**—determines how Client Agent handles application launch requests. For details, refer to [Launch Control and Network Access](#), page 19.
2. **Emergency Outbreak Rule**—helps stop viruses and other malicious software. For details, refer to [The Outbreak Rule and Viruses](#), page 20.
3. **Lockdowns**—restrict software launches to a specific set of executables for each machine and user. For details, refer to [Lockdowns and Viruses](#), page 20. The Removable Media Lockdown feature restricts the use of writable devices such as flash drives, CD/DVD burners, floppy drives, and external hard drives on workstations. For details, refer to [Removable Media Lockdown](#), page 185.

4. **Port blocking**—defines which ports an application can—or cannot use when it is allowed to launch. For details, refer to *Port Blocking and Viruses*, page 21.
5. **Zero Day response**—permits applications to launch but does not allow them to access ports. The default Global rule can be set to provide this functionality, by stopping malicious attacks before they enter your network. For details, refer to *Global Rule*, page 266.

Launch Control and Network Access

At installation, Client Agent receives a complete list of rules, all information available in the Websense Enterprise Master Database, and any custom information based on inventory of the workstations. Each rule defines which software launches are allowed, which ports can be accessed, and what information is logged.

Client Agent checks the list of rules to determine what control and monitoring parameters to implement when a user tries to launch an application, where a user may be the system, an administrator, or an employee. When Client Agent checks rules, it looks at the following parameters to define what action to take:

- ◆ The status assigned to the rule. Options include **Always Apply**, **Never Apply**, **Connected**, and **Disconnected**. The last two options provide the ability to control application launches and port access based on their connection status to the CPM Server. For details, refer to *Status Settings*, page 256.
- ◆ The machine where launch requests occur and the user requesting a launch. These parameters are identified by the Client Set included in the rule, described in *Chapter 10: Working with Client Sets*, page 191.
- ◆ The software categories and/or files that are to be included in the rule, described in *Chapter 12: Working with Software Sets*, page 225.
- ◆ The action that is to occur when Client Agent receives a launch request. This is identified within the rule itself. Read *Understanding Rules*, page 255.
- ◆ What will happen if Client Agent receives a request to access a port. Ports are identified by the port set included in the rule. Read *Chapter 13: Working with Port Sets*, page 243 and *Network Access Control*, page 259.
- ◆ Activity that is to be submitted for logging. Read *Logging*, page 260.

The Outbreak Rule and Viruses

Often, information about a new virus is available in the media before anti-virus applications are able to recognize it. For example, in a recent outbreak, the `msblaster.exe` virus affected thousands of machines. The media dispersed information about the virus, but it was several days before common anti-virus programs were able to identify it and download the data to their customers.

During this outbreak, CPM administrators were able to enter the file name, `msblaster.exe`, into the **Outbreak** dialog box. Within seconds, Websense customers were protected, while other organizations needed to wait for their anti-virus provider to include the data in their downloads.

The Outbreak process passes data to machines running Client Agent almost instantly, which then use peer-to-peer communications to distribute the information within a matter of seconds. As a result, machines are protected, long before anti-virus software is able to detect and stop the virus.



NOTE

Peer-to-peer Outbreak communication between client machines can be disabled. Refer to [Disabling Client Outbreak Distribution](#), page 123 for instructions.

Once peer-to-peer distribution is complete, the details in the **Outbreak** rule become part of the CPM policy. When machines that were offline become available on the network, the CPM policy is downloaded, with Outbreak information, to those machines. For more information, read [Emergency Outbreak Rule Processing](#), page 118.

Lockdowns and Viruses

In addition to the protection inherent in the **Outbreak** rule, CPM provides an additional layer of security by allowing organizations to “lock down” machines. CPM uses two types of lockdowns for client machine executables:

- ◆ **Inventory lockdown**—uses standard inventories to determine what executables to permit. Refer to [Inventory Lockdown](#), page 177 for details.
- ◆ **Express Lockdown**—inventory independent. Permits the launch of executables that are on the machine at the time the lockdown was applied. Refer to [Express Lockdown](#), page 180 for details.

Client Policy Manager includes options for taking inventory of installed software and hardware. When you request an inventory, Client Agent collects data about the installed software and hardware. The Client Agent can search hard drives, CD-ROMs, and/or mapped drives.

The inventory process must occur before you can apply an Inventory lockdown to a machine that runs Client Agent or generate reports based on inventories. For software, you can use the resulting inventory to lockdown client machines to a known set of software, and thus maximize security. For details, refer to *Chapter 8: Working with Inventories*, page 151, and *Chapter 9: Applying Lockdowns*.

When set, a lockdown is included in the CPM policy as one of the last checks before allowing employees to launch software. If an executable is not included in the lockdown for a machine, the file cannot be launched.

Because lockdowns only permit an approved set of executables to run, it is virtually impossible for a virus or other malicious program to impact a machine that is locked down. Because the virus or malicious code cannot run, it cannot infect the machine nor can it spread to other machines.

Port Blocking and Viruses

If you allow a machine and/or a user to continue or permit an application launch, you can specify which ports, if any, the application can access. This serves as an additional layer of security against viruses, and may help stop them from spreading across your network.

Viruses and other malware may ride “piggy-back” with a recognized application, and when a machine is infected, they may try to launch themselves. Sometimes, these processes are set to attack a specific port that may be associated with an application. Other times, these processes scan ports that the application does not normally use.

For example, you are using Internet Explorer, which is typically set to use port 443. You want to use 4443 instead to provide added security. You change the Internet Explorer port settings in that software, and then set CPM to permit only port 4443.

During Internet use, a virus manages to piggy-back on top on Internet Explorer, and then tries to launch itself into your network using port 443. Because you permit Internet Explorer only at port 4443, the virus is unable to spread through your network.

Zero Day Response Functionality

Websense includes the Global rule automatically in any list of rules you create. When Client Agent checks launch requests, the Global rule impacts launch and network access for an application only if preceding rules do not specifically affect the application.

The default setting for the Global rule is to permit all application launches and any network access attempt. By changing the network access setting, you can create an instant Zero Day response that will block malicious code from accessing the network.

When you define your policy, change the network access setting in the Global rule to block network access. This setting permits applications to launch normally, but blocks them from accessing any port. This process ensures your network remains free from attack. For more details, read [Global Rule, page 266](#).

Reporting

Websense Enterprise CPM includes several reporting options that provide you with nearly instantaneous access to information. These options include:

- ◆ Websense Enterprise Manager provides on-demand access to all inventory details. Read [Viewing Inventories, page 167](#).
- ◆ CPM Reporter provides access to inventory and launch details in on-demand or scheduled reports. Read [CPM Reporter, page 47](#).
- ◆ Explorer for CPM provides access to launch data using interactive drilldown options. Read [Explorer for CPM, page 48](#).

Naming Conventions

To make your job easier, Websense Enterprise Client Policy Manager uses standardized publisher names whenever possible. Sometimes, one company may use a variety of different naming conventions for the products they make. For example, Microsoft may appear as:

- Microsoft
- Microsoft Inc.
- Microsoft Incorporated
- Microsoft Inc
- Microsoft, Inc.
- Microsoft Corporation

Whenever Client Policy Manager encounters a Microsoft product, the company name is standardized as **Microsoft Corporation** to reduce confusion. Because Websense maps many names to one common name, your ability to quickly access and understand information increases dramatically.

Standardized data appears in Websense Enterprise Manager when you access the **Software Inventory View** and **Hardware Inventory View** dialog boxes, and in the search dialog boxes for **Categories** and **Software Sets**. In CPM Reporter and Explorer for CPM, standardized data appears in any report that includes publisher names if that data is available.

You may find entries for applications, executables, and even hardware that does not include publisher or manufacturer identification. It is not uncommon for companies to create products that do not include coded information. If the software or hardware does not support coded data, Websense, Inc. cannot provide that data or standardize it.

For example, if you buy an Intel board, the board contains information that has been specifically coded by Intel. However, if you buy a board manufactured by *Bob's Home-Based Computer Parts Supply Warehouse*, there is a chance that Bob did not include coding. As a result, even though the boards may be similar in design, Websense, Inc. includes data for the Intel board, but not for the board that Bob built.

Identifying Corporate Goals

The key to maximizing your Websense Enterprise Client Policy Manager subscription is clearly identifying what benefit you expect to gain when you subscribe. Often, subscribers are looking for security, productivity, or both.

Websense CPM rules provide flexibility, allowing subscribers to define software control and network access that meets their requirements. It is useful to develop your strategy by involving members of your Information Technology and Human Resources staff.

Security

For some organizations, security is of utmost importance. For example, a new coffee house is opening, and a number of machines are being installed so customers can access the Internet. The owners of the coffee house want to make sure that customers cannot download or install any applications that could consume excessive amounts of bandwidth, result in legal action, or otherwise harm the business.

To meet this goal, the system administrator deploys Client Agent to machines. The administrator runs inventories of installed software, and then uses Client Policy Manager to lock down the machines so only those applications can launch.

As a result of this lockdown, customers will be able to launch software the owners of the coffee house have installed, but they cannot install any other software. This protects the owners from licensing issues, eliminates system cleanup, and protects the machines from malicious attacks.

For even tighter security, the system administrator can limit the ports that software can access. This further restricts the parameters in which software can operate.

Productivity

For some organizations, employee productivity is of utmost importance. For example, a telemarketing organization wants to limit access to programs that may cause employees to lose focus.

To maximize productivity, the system administrator deploys Client Agent to machines, and controls launches by using categories to identify the software. She blocks the Games, Instant Messaging, and P2P categories. As a result,

employees will not be able to launch any software that is associated with these categories.

As Websense, Inc. identifies software, that information is saved to the Websense Enterprise Master Database, and entered in the appropriate category. Because the company chooses to download the database on a daily basis, all changes to the database appear immediately in any rule that includes those categories. This allows Client Agent to immediately respond to launch requests for any of the newly included applications as soon as the database download occurs.

Security and Productivity

Many organizations want a secure computing environment, and are also looking for ways to improve employee productivity. For example, a software publishing firm wants to improve productivity, but also knows that Technical Support employees need Instant Messaging software. The company also wants to improve security by using the lockdown functions.

The company uses categories to create rules that block software in the Entertainment category, while permitting Technical Support staff access to the Instant Messaging category. Once machines are installed with the appropriate software, the company runs inventories and uses the inventories to lock down the machines.

Educating Employees

Before a company implements Client Policy Manager solutions at desktops, management should educate employees as part of the process. This is especially important if your company is installing CPM. If the company does not communicate with employees, both the company and management may be at risk legally.

It is important that employees understand why you are implementing desktop monitoring and control, and what is expected of them. For the most effective results:

1. **Maintain published guidelines.** It is critical that you tell employees why your company is implementing CPM, and what the guidelines are. For example, if you are trying to increase productivity and security, and reduce bandwidth consumption, employees are more likely to respond positively than if they see CPM as an arbitrarily imposed control.

It is important that employees understand that software and hardware installations and uninstalls become traceable. For example, if your company prohibits employee modifications to machines, inventory information could lead to confrontations with an employee who violates this policy. If she is informed of the company's ability to monitor these installations, she later has no legal basis to challenge any reasonable corporate response.

2. **Demonstrate Client Policy Manager features to employees.** Your company may want to schedule employee meetings that discuss company guidelines, demonstrate CPM functionality, and present examples of CPM reports. By doing so, employees probably will feel more comfortable with the CPM solution than if they are left to speculate about product capabilities. This is especially critical, as the collected data could create situations where legal issues may be of concern.
3. **Incorporate appropriate employee feedback into policy and deployment decisions.** In addition to making sure employees know exactly what the company expects of them, it is a good idea to listen to their feedback. For example, your company wants to block Instant Messaging (IM). However, some parents keep IM software running so their children can communicate with them at need. Management may decide that people in that situation can continue to use Instant Messaging software while others cannot. By encouraging employees to speak up now, the company can avoid conflicts later.

Identifying Organizational Roles

When your organization decides to implement Client Policy Manager, it is important that there is a clearly defined organizational path for approving any exceptions. This is critical, as there are almost always exceptions to security controls, and it helps to know who can make the necessary changes.

For example, your company is installing CPM to improve productivity. To meet this goal, your CPM policy blocks all imaging devices and instant messaging applications. Once CPM is installed and operating, the help desk receives a call from a technical writer who needs to use imaging devices for documentation purposes. Rather than simply granting access to the writer, there should be a clearly defined process for changing the CPM policy.

When creating an organizational plan, it is important to identify those who will be most effective in responding appropriately. For example, if your

company implements Websense solutions to reduce legal liability and improve productivity, the Human Resources manager may have the final word. However, if the company is seeking to add security to machines on your network, the person capable of making the best decision might be the Information Technology manager.

In some organizations, there may be several people who need to approve an exception. For example, your company is implementing Websense solutions to improve productivity and add security. In this situation, both the Human Resources and the Information Technology managers may be included in the decision making process.

To best meet your goals, begin with the following questions:

1. Why are we implementing Websense solutions? Are we looking for additional security? Are we trying to improve productivity? What is the end goal?
2. Who knows the most about why we are implementing Websense solutions?
3. Who knows the most about the potential harm if an exception to the corporate policy is granted?
4. What groups are most affected by changes to the CPM policy?

Using these questions, you can generate others that apply to your situation, and then determine a plan of action that provides the operational control you need.

For example, a company determines they want to improve employee productivity and reduce security hazards. In order to implement the CPM policy effectively, they determine that:

1. Help Desk staff will initially take any requests for changes to the policy.
2. The employee's department manager must approve the request.
3. The Information Technology manager must approve the request.
4. The Human Resources manager must approve the request.
5. The Client Policy Manager administrator will make the necessary changes once the request is fully signed off.
6. If, at any point, the request is denied, changes are not implemented.

This organizational structure makes sure that both productivity and security needs are met, while considering the needs of the individual employee.

Installing and Configuring Client Policy Manager

When you are installing and configuring Client Policy Manager, be aware of the critical steps that must be completed, and the order in which they occur:

1. **Determine what goals you want to achieve.** CPM provides a number of ways to better manage valuable resources.
2. **Install Client Policy Manager components.** You can install CPM on one machine, distribute it among a number of machines, and/or integrate it with Websense Internet Filtering components. For details, refer to the *Websense Enterprise Client Policy Manager Installation Guide*.
3. **Register and configure Client Policy Manager software.** You must register Client Policy Manager before you can download the Websense Enterprise Application Database. For details, refer to [Chapter 4: Getting Started With Client Policy Manager, page 109](#).
4. **Install Client Agent.** There are a number of ways you can deploy Client Agents. The method you choose depends on your environment. For more information, read the *Websense Enterprise Client Policy Manager Installation Guide*.
5. **Run inventories.** Inventories identify and categorize software installed on machines running Client Agent. For details, refer to [Chapter 8: Working with Inventories, page 151](#).

You can use inventories to create lockdowns that permit employees to launch only software included in the selected inventory. For details, refer to [Chapter 9: Applying Lockdowns, page 177](#).

6. **Create client sets.** Client sets identify your networks, machines, users, and user groups. Read [Chapter 10: Working with Client Sets, page 191](#).
7. **Customize categories to define how CPM identifies executables.** While you can accept the default Websense categorization, you may add custom categories and move executables to different categories to reflect your business environment. Read [Custom Categories, page 205](#).
8. **Create software sets.** Software sets let CPM handle groups of executables as a single entity. Software sets may contain individual executables, categories, software sets generated from inventory, and other software sets, in any combination. For complete details, read [Chapter 12: Working with Software Sets, page 225](#).

9. **Create port sets.** Port sets let CPM handle groups of ports as a single entity in rules, where each port set may contain one or more ports. For details, refer to *Chapter 13: Working with Port Sets*, page 243.
10. **Define rules.** Rules associate client sets and software sets with launch dispositions, identify network access settings; define logging; and enter comments. All rules are downloaded to Client Agent. For an overview, read *Rules and the CPM Policy*, page 51. For configuration details, read *Chapter 14: Working with Rules*, page 255.
11. **Test rules.** Change network access in the Global rule to block. Use CPM Reporter or Explorer for CPM to view the results of the policy and how it impacts machines and users. The information you find can point to changes that are of benefit to your organization.
12. **Generate reports.** CPM Reporter provides the means of viewing information from inventories, application launch requests, and network access attempts. Reports can be run almost instantly, and can be customized to meet specific business needs. Read *Websense Enterprise CPM Reporter Administrator's Guide*, for complete information.

You can also use Websense Enterprise Explorer for CPM to generate reports. This tool is ideal for Human Resource staff, managers, and others who may require access to software launch information. The reports support interactive filtering options. For complete details, read *Websense Enterprise Explorer for CPM Administrator's Guide*.

Understanding CPM Basics

Before installing and using Websense Enterprise Client Policy Manager, it is helpful to understand your subscription, the functions of the various CPM components, and how the CPM policy works. By understanding these areas, you will be able to easily set up and configure CPM:

- ◆ *Subscriptions* are purchased for a period of time, and may affect the Websense Enterprise Web filtering module and/or CPM. Your subscription gives you access to the Websense Enterprise Master Database, which allows you to manage and control Internet and/or application access.
- ◆ *Components* are the Websense executables and files installed at machines in your networks prior to Client Policy Manager configuration.
- ◆ The *CPM policy* is a collection of rules that Client Agent checks when machines or users try to launch software and access network ports. Part of CPM configuration is designing rule components, where each rule identifies:
 - The machines and/or users the rule impacts, that you group into *client sets*.
 - What happens when a machine or user tries to launch software. You group software into *software sets*, and then define control options.
 - What happens when software included in the software set tries to access ports. You group ports into *port sets*, and then define control options.
 - What information is logged.

This chapter introduces the CPM basics to help you get started.

Shared Subscriptions

Websense Enterprise includes two subscription modules, Web filtering and Client Policy Manager. Your subscription provides you with continuous updates from the Websense Enterprise Master Database, which categories Internet sites and software, and provides risk class assignments for these. If you purchase both modules:

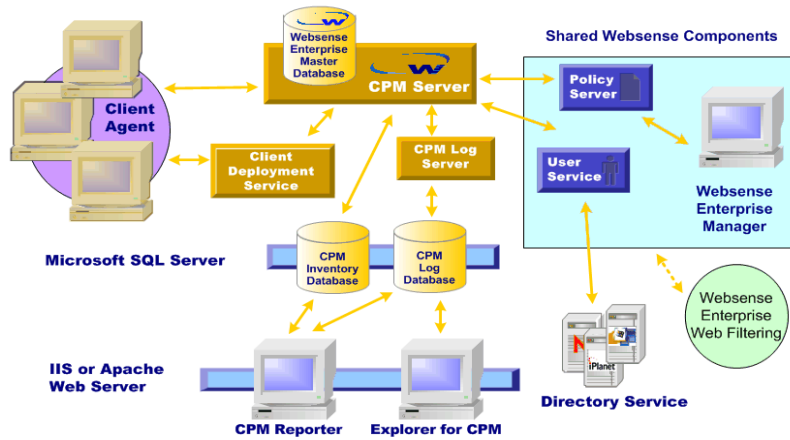
- ◆ One subscription key enables any Websense subscription you have.
- ◆ You may have a different number of seats for each module.
- ◆ Your start dates may be different, but the end date for all subscriptions is the same.
- ◆ If you already subscribe to one Websense module, and then subscribe to the other, you do not need to reregister. Your subscription key immediately updates itself to allow the use of the new module.

Understanding the CPM Operating Environment

CPM is designed to work in tandem with Websense Web Filtering module or in a stand-alone mode. All components, with the exception of reporting tools, must be installed and active if CPM is to work properly.

CPM uses:

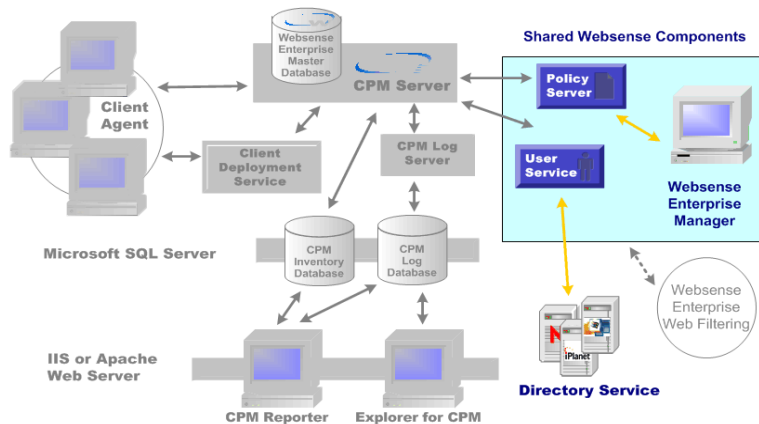
- ◆ **Shared components:** These may be already installed with the Web Filtering module, or may be installed as part of the CPM installation. For details refer to *Shared Websense Enterprise Components*, page 33.
- ◆ **CPM Components:** These are components specific to CPM. For details, refer to *CPM Components*, page 37.



CPM Operating Environment

Shared Websense Enterprise Components

Shared Websense components are necessary for Websense CPM operations, and may be installed with Websense Internet Filtering or Websense CPM. The modules may share components or may use them in standalone mode. Shared components can reduce the overhead required for system and machine operations, and can be distributed across your network.



Shared Websense Enterprise Components

Shared components are:

- ◆ [Policy Server](#), page 34
- ◆ [User Service](#), page 34
- ◆ [Websense Enterprise Manager](#), page 35

Policy Server

The Policy Server stores Websense configuration information. Policy Server communicates this data to the Websense CPM Server, which then passes the information to the Client Agent. If your network is in the enterprise category (10,000+ users), you may want to install and run multiple Policy Servers.



IMPORTANT

Client Policy Manager requires one CPM Server for each Policy Server in your network.

Policy Server configuration first occurs during installation, while connectivity configuration occurs in Websense Enterprise Manager, as described in [Adding a Policy Server](#), page 60. After installation, Policy Server automatically identifies other Websense components, continually tracking the location and status of the Websense services. Policy Server also maintains ongoing policy updates for CPM.

User Service

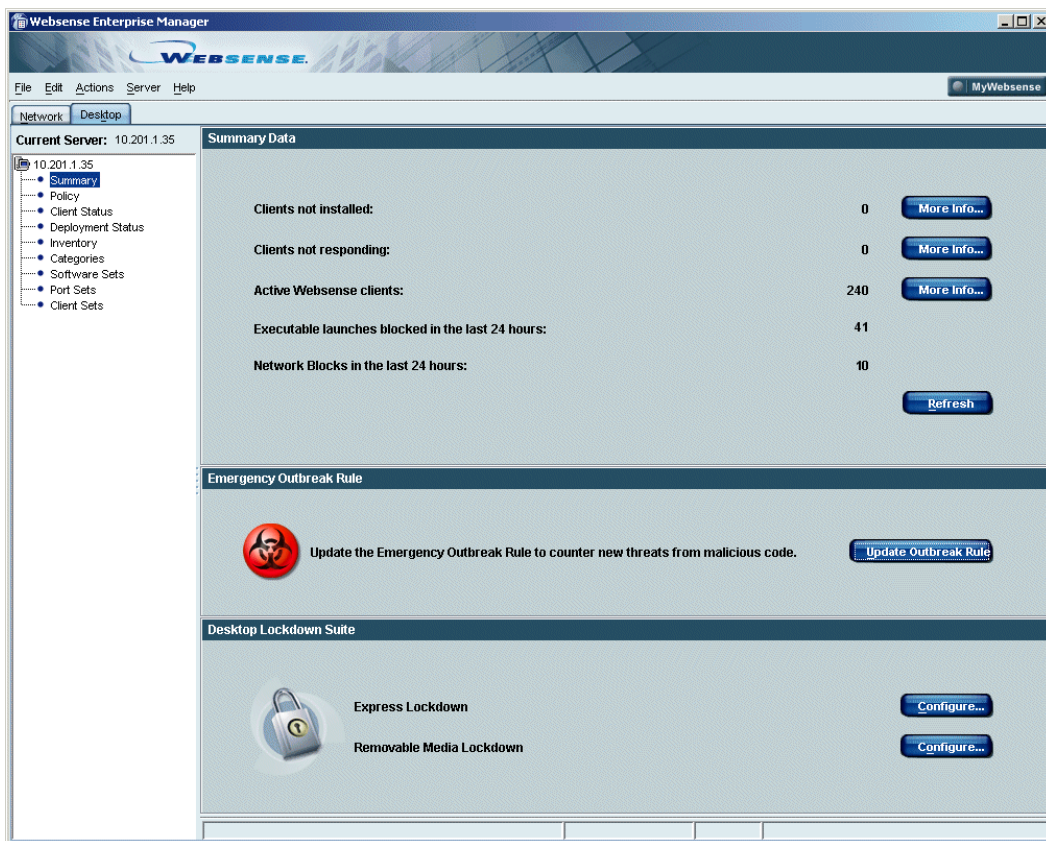
The User Service communicates with your organization's directory service to convey user-related information to Policy Server and CPM Server, for use in identifying machines and applying the CPM policy. This information includes user-to-group and user-to-domain relationships. User Service provides the list of objects residing in your directory service to Websense Enterprise Manager.

User Service configuration first occurs during installation, while other options are available in Websense Enterprise Manager, as described in [Configuring User Services](#), page 69. There must be one instance of User Service for each Policy Server in your network.

Websense Enterprise Manager

Websense Enterprise Manager is the user interface for configuring Websense modules. The Websense Enterprise Manager window contains a menu bar, navigation tree, and content pane:

- ◆ The menu bar appears at the top of the Websense Enterprise Manager window, and contains several menus that provide access to server configuration, communication path identification, CPM Reporter, and more. For details, refer to *Menu Options*, page 110.
- ◆ The navigation tree appears at the left side of the window. Once you open Websense Enterprise Manager and identify one or more CPM Servers, the navigation tree shows those entries. For details, refer to *Navigation Pane Selections*, page 111.
- ◆ The content pane appears at the right side of the window, and displays the information for the topic you select from the navigation tree. For details, refer to *Content Pane Presentation*, page 112.
 - The **Desktop** tab provides access to Client Policy Manager configuration options for networked machines.
 - The **Network** tab provides access to Websense Enterprise configuration options for the Internet. For details, refer to the *Websense Enterprise Administrator's Guide*.



Websense Enterprise Manager, Desktop Tab

If the Policy Server is installed on a remote machine, the navigation tree is empty the first time you start the Websense Enterprise Manager. If the Manager and the Policy Server are installed on the same machine, the IP address of the Policy Server will be added to the Manager.

Once you add servers, The IP addresses of the machines appear when you open Websense Enterprise Manager and click the **Desktop** tab. When you connect to a server, the navigation tree changes to show selections for that server.

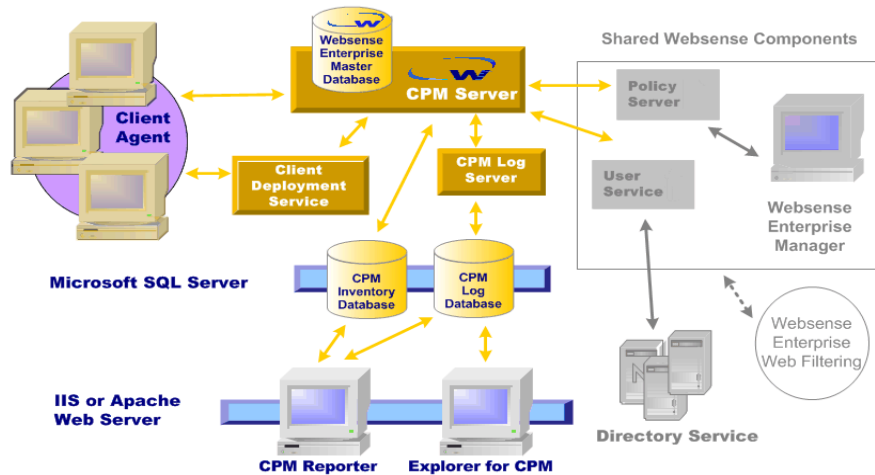
Like most applications that run in the Windows, Websense Enterprise Manager includes standard keyboard shortcuts. Keyboard shortcuts, if they are supported by your operating system, appear on dropdown menus in Websense Enterprise Manager.

To access Websense Enterprise Manager:

- ◆ Select **Start > Programs > Websense Enterprise > Websense Enterprise Manager**.

CPM Components

Client Policy Manager components interact with Websense shared components for desktop monitoring and control. The CPM components provide the interfaces and communications necessary to inventory client machines and populate the CPM databases. For Websense Enterprise Manager, CPM Reporter, and Explorer for CPM.



CPM components

CPM components are:

- ◆ *CPM Server*, page 38
- ◆ *Client Deployment Service*, page 38
- ◆ *Client Agent*, page 39
- ◆ *CPM Reporter*, page 47
- ◆ *Explorer for CPM*, page 48
- ◆ *Client Policy Manager Databases*, page 41

CPM Server

CPM Server processes are responsible for handling communications with machines running Client Agent for such tasks as sending CPM inventory requests, transferring CPM rules, and sending database information.

CPM Server calls the User Service, one of the shared Websense Enterprise components, for most directory service information. The User Service identifies directory objects in the network, which are individual users, user groups, domains, and machines identified by machine names.

For CPM Server and Client Agent communications, authentication is set using a unique, encrypted key. During installation, you enter a passphrase of your choice. This phrase and unpublished keys in CPM, are combined and then encrypted. The result is a highly secure recognition code that authenticates the communications and protects data. Authentication is used by both CPM Server and Client Agent.

CPM Server has a one-to-one relationship with the Websense Policy Server. If you install an additional Policy Server in your network, you must install a corresponding CPM Server.

Client Deployment Service

The Client Deployment Service makes it easy to deploy Client Agent using one of several methods:

- ◆ **Websense Enterprise Manager:** Use the Client Deployment pane to deploy Client Agent to one, many, or all machines. You can also uninstall Client Agent in the same manner.
- ◆ **Scripts:** Scripts can also be used to uninstall Client Agent.

If you choose to deploy Client Agent using Websense Enterprise Manager, CPM Server passes deployment information to Client Deployment Service,

which then deploys Client Agent. Communications at this point occur between:

- ◆ Client Deployment Service and the machine where the deployment is taking place.
- ◆ Client Deployment Service and CPM Server, where deployment status is sent from the service to CPM Server.

Once Client Agent is installed, the communication between Client Deployment Service and Client Agent stops.

Client Agent

Client Agent resides on desktops, laptops, and/or servers in the CPM network, and communicates with the CPM Server as long as connections are available. Machines are considered connected when Client Agent can communicate with CPM Server, regardless of the method. Methods may include local LAN, VPN, and so forth.

When you first install Client Agent on a machine, it registers with CPM Server, and begins downloading the CPM policy. When the download is complete, Client Agent checks the policy, which it uses to control launch and port access requests, and to determine data logging requirements.

The policy contains:

- ◆ The entire list of rules that control launch and port access for machines and users.
- ◆ An encrypted file contain information about custom categories you create, and any applications that you or other system administrators have included in a generated software set, which is a customized list of applications identified during an inventory, and then specifically identified for inclusion in a software set

After this initial download, Client Agent registers with CPM Server whenever the machine starts up. During the registration process, CPM Server checks version data from Client Agent, and compares it to version data at the server. If there is a difference between the two versions, CPM Server downloads only information that has changed since the last download.

Whenever a machine or user tries to launch an application or access a port, Client Agent checks the CPM policy to determine the appropriate response for that machine and/or that user. Because the policy is available locally, Client Agent does not consume any bandwidth for monitoring and control

operations. Also, the local availability of the policy means that Client Agent can respond to any user logging on to a machine, without the need to contact CPM Server.

Client Agent is also responsible for handling requests from CPM Server. Functions include scanning drives, detecting and reporting inventory details for installed software and hardware. Client Agent also forwards the results of any launch requests and network access attempts.

Client Agent Startup Functions

When employees start their desktops, laptops, or servers, the Client Agent installed at that machine registers with CPM Server—if both machines are online. It sends a message that contains the machine ID, IP address, version information, the machine name, and the current status.

If CPM Server determines there is a difference between the policy at the machine and the policy at the server, it downloads only the changed information to Client Agent. The ongoing heartbeat data sent by Client Agent ensures that CPM Server continuously updates the CPM policy at local machines.

When Client Agent is running, it sends regularly scheduled information to CPM Server. This “heartbeat” provides the CPM Server with the following information:

- ◆ Client machine is running.
- ◆ Client Agent is installed and working.
- ◆ Information contained in the last download from CPM Server

If the versions are different, CPM Server downloads only the policy information that has changed.



NOTE

Heartbeat configuration is described in *Defining Client Control*, page 104.

Client Agent Offline Functions for CPM

Client Agent continues to work even if client machines cannot communicate with CPM Server. Offline functions begin as soon as Client Agent determines that it cannot contact the server. Whenever this occurs, Client Agent uses the

last available CPM policy to monitor and/or control application launches and network access.

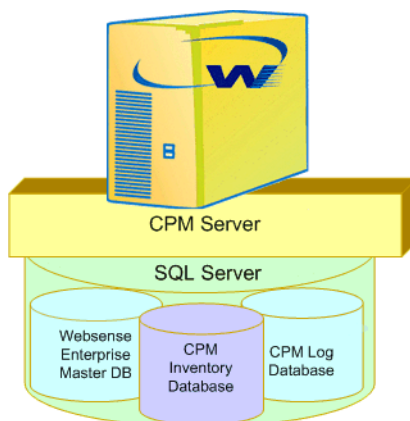
During offline periods, Client Agent creates a log cache that can store approximately to a month's worth of data. If the cache is full when Client Agent receives a new record, Client Agent drops the oldest record to make room for the new. This process continues until Client Agent is able to submit the cached information to CPM Server.

Client Agent continues to try and reestablish connections to CPM Server at every heartbeat. When CPM Server again becomes available, Client Agent waits for the first launch event before it can process offline data. Once a new event occurs, the Client Agent submits all logged data to CPM Server, which then sends the information to the CPM Log Database. When the process is complete, the Client Agent empties the cache.

Client Policy Manager Databases

Client Policy Manager uses Microsoft SQL databases to store information. The SQL Server may be on the same machine as CPM Server or on a machine that is able to communicate with the machine where you install CPM Server. While database population occurs in the background, it is useful to understand the functions associated with each database, and the source of the information each database includes.

The CPM databases are:



Websense CPM Databases

Client Policy Manager uses three databases that are saved to SQL Server:

- ◆ **Websense Enterprise Master Database**—a proprietary and encrypted database which Websense, Inc. creates and maintains. The database identifies executables, applications, and port information and stores category and risk class details. Read *Websense Enterprise Master Database*, page 42.
- ◆ **CPM Inventory Database**—contains information collected during machine inventories. The database contains information about software and hardware that physically resides at machines that run Client Agent. Read *CPM Inventory Database*, page 45.
- ◆ **CPM Log Database**—contains CPM information collected when employees request launches. The database records date, time, user, machine name or IP address, and tracks category and risk class data as well. Read *CPM Log Database*, page 46.

Database Engine Requirements

The Websense CPM installation requires a licensed version of SQL Server. SQL Server can be purchased from Microsoft or a Microsoft reseller.

SQL Server must be installed and able to communicate with any other machines that will have CPM components installed *before* you begin CPM installation. If you do not have SQL Server, CPM cannot be configured or used.

Websense Enterprise Master Database

The Websense Enterprise Master Database contains signatures for executables and applications, and information about the ports that applications are assigned to use if they require network access. In the database, Websense, Inc. identifies executables based on the task they are designed to perform, and associates them with a specific Websense category. Ports are identified based on their functional use.

The Websense Enterprise Master Database downloads automatically as part of the subscription process. During configuration, you can schedule downloads, as described in *Understanding Database Downloads*, page 77, or you can accept the daily default download. You can also manually download the database at any time, without impacting any scheduled download, as described in *Manually Requesting a Database Download*, page 80.

CPM Server downloads the entire Websense Enterprise Master Database the first time, after which, only changes to the database are sent to Client Agent. When a launch or port access request is identified, Client Agent calculates the signature for the installed application, and then looks for a match to known signatures in the locally saved database information to determine how to handle that launch request.



Application Signature Collection

If employees try to bypass CPM security by renaming files, CPM is able to recognize the executable for what it is. For example, your company uses `greatwords.exe`, a word processing executable. An employee decides to bypass CPM security and changes the name of the Microsoft Solitaire game, `sol.exe`, to `greatwords.exe`.

CPM checks the signature against those in the Websense Enterprise Master Database. Using the results, CPM determines that the executable is not the "real" `greatwords.exe`, and identifies it accurately as Solitaire.

The signature data in the Websense Enterprise Master Database comes from one of three sources:

- ◆ **Websense:** Websense, Inc. collects, researches, and categorizes executables and applications to provide a prepopulated database. This process is ongoing, and the database is updated daily with new signatures.

The collection process includes a daily search of the entire Internet—roughly nine million sites—for executables and applications. Websense, Inc. also mines software and download software sites searching for new software that appears in these Web sites.

Websense, Inc. includes identification of ports that applications are designed to use. This process allows CPM administrators to identify expected behaviors—and those that are not. This information can help you better manage ports and reduce unauthorized access to network resources.

- ◆ **Inventories:** You run inventories on local machines. If the inventory process locates executables and/or applications that do not appear in the Websense Enterprise Master Database, the executables and/or applications, and any signature data, are inserted into the database as Uncategorized. If AppCatcher is enabled, this information is sent to Websense, Inc. for research.

If the inventory locates executables and/or applications that are identified in the master database, CPM recognizes the categories that identify what the executables and/or applications are designed to do.
- ◆ **AppCatcher:** Client Agent flags ports that are not identified in the port list, and—if AppCatcher is enabled—sends the information to Websense, Inc. After some research, Websense, Inc. includes the port and its default uses in the Websense Enterprise Master Database.

Websense Enterprise AppCatcher

Websense CPM includes AppCatcher, a software tool that allows system administrators to automatically submit application signature and port data to Websense, Inc. The process uploads information about executables, applications, and ports that are not identified in the currently available version of the Websense Enterprise Master Database.

Once Websense, Inc. receives information about such executables, applications, and or ports, a team reviews the information, performs any necessary research, and then inserts the information into the Websense Enterprise Master Database. The process takes between 7 and 14 business days.

When you next download the updated database, the new information is available to CPM processes immediately. The download automatically places each executable into the correct category, and removes it from the Uncategorized list. It also inserts any new port identities. Complete details are available in *Introducing AppCatcher*, page 83.

Executables

The Websense Enterprise Master Database may include any of the following executable types:

- ◆ Portable executable (PE), native binary files that are not Dynamic Link Libraries (DLLs)
- ◆ OS/2 formatted native binary files

- ◆ DOS-MS binary files
- ◆ DOS-COM binary files
- ◆ Files with one of the following extensions:
 - **.EXE**-Executable files
 - **.BAT**-DOS batch files
 - **.VBS**-Visual Basic Script files, interpreted by wscript.exe or other .exe scripts
 - **.JS**-JavaScript files
 - **.CLASS**-Java Class files
- ◆ All files that are executables, regardless of their extension

Scripts

Because CPM focuses on executables, not embedded scripts such as JavaScript, CPM cannot block JavaScript code that is directly embedded inside another executable. However, if a JavaScript executable is referenced by another executable, CPM recognizes it, and handles it based on rules you develop. An example of referenced JavaScript is JavaScript run from inside a Web page.

CPM identifies scripts as executables, and calculates a unique signature for each. If you lock down the machine, scripts that were not in the original inventory cannot execute as they are stopped by the script host, for example, Visual Basic Script host, Windows scripting host, and so forth.

If employees hack plain-text scripts maliciously, the changes in the script file force the unique ID to change. In lockdown mode, Client Agent blocks the changed script, even if it still has the same name, because the ID does not match any signature in the inventory.

CPM Inventory Database

CPM Server builds the CPM Inventory Database from scans of local hard drives for machines running Client Agent. Companies can use the data to:

- ◆ Monitor and control software.
- ◆ Monitor hardware installations.

You can run inventories immediately, schedule them to occur at a specific date and time, and/or run them on a repeating basis. Client Agent scans the

machine where it is installed, and sends the collected data back to CPM Server. The data is then stored in the CPM Inventory Database.

To fully populate the CPM Inventory Database, you must:

1. Have SQL Server installed and able to communicate with machines where you are installing CPM components.
2. Install CPM components. For details, refer to the *Websense Enterprise Client Policy Manager Installation Guide*.
3. Enter subscription data and allow the Websense Enterprise Master Database to download. Read [Chapter 4: Getting Started With Client Policy Manager, page 109](#).
4. Load Client Agent software on machines you want to inventory. Read [Deploying Client Agent, page 127](#).
5. Run an inventory. Websense, Inc. recommends running inventories early in the setup process, as it simplifies later steps. You should schedule inventories during off work hour periods, as the inventory process may have a slight impact on machine performance while it is running. Read [Running an Inventory, page 157](#).
6. Rerun inventories whenever necessary to maintain accurate records and improve executable control. You can schedule inventories on a weekly or monthly basis.

CPM Log Database

CPM Log Database stores information about CPM launch requests that are defined to use logging. Each time an employee attempts to launch an application, the local Client Agent saves a record of the transaction that contains:

- ◆ Executable file name
- ◆ Version, if known
- ◆ Date and time of file installation, if known
- ◆ Publisher, if known
- ◆ Category
- ◆ User name
- ◆ Client Agent IP address

- ◆ Action (Permit, Block, Continue)
- ◆ Date and time of response

Websense CPM Reporter and Explorer for CPM use this information to generate detailed reports.

Reporting Tools

CPM includes two reporting tools. Both tools are Web-based and present information from the CPM databases. The similarities and differences between these tools appear in the next table.

Function	Explorer for CPM	CPM Reporter
Web-based reporting	X	X
Near real-time data access	X	X
Software launch data	X	X
Interactive access to data	X	
Hide sensitive data	X	
Schedule reports		X
Report delivery via email or FTP posting		X
View Inventory data		X

The CPM installation uses a batch process and places both reporting tools on the same machine. Anyone who is authorized can access either tool via the correct IP address and password entries. Complete details for use appear in the *Websense Enterprise CPM Reporter Administrator's Guide* and the *Websense Enterprise Explorer for CPM Administrator's Guide*.

CPM Reporter

CPM Reporter provides reports about desktop inventory, the results of launch requests and network access attempts. The application uses information collected by Client Agent and stored in the CPM Log database.

CPM Reporter provides on-demand and scheduled reports. Reports are available in a browser, can be sent via email, or can be posted to an FTP server.

Some reports in CPM Reporter require inventories from machines where Client Agent is installed. If you do not run inventories, these reports will be empty.

Existing customers find that CPM Reporter is invaluable for day-to-day business needs, as well as providing the data necessary for identifying existing resources and making informed decisions about equipment and/or software purchases. You can generate reports using default settings, or can customize reports to provide information that is specific to a given need. For complete details, read *Websense CPM Reporter Administrator's Guide*.

Accessing CPM Reporter from Websense Enterprise Manager

You can open CPM Reporter from Websense Enterprise Manager if you have the appropriate access:

1. In Websense Enterprise Manager, select **Actions > Launch CPM Reporter** on the menu. A browser opens and presents the login window.
2. Enter your user name and password.
3. Click **Login**.

Accessing CPM Reporter from the Start Menu

You can open CPM Reporter from the **Start Menu** if you have a user name and password. This option allows you to go directly to CPM Reporter rather than opening Websense Enterprise Manager and accessing it from there.

1. On Windows 2000, select **Start > Programs > Websense Enterprise > CPM Reporter Login**.
2. When the login dialog box opens, enter your user name and password.
3. Click **Log On**.

Explorer for CPM

Websense Enterprise Explorer for CPM allows employees to access report data instantly in a browser. The reports provide interactive options for filtering data, and sensitive information can be hidden. Explorer for CPM is an ideal way for managers and Human Resources staff to access data. It supports rapid access of information, and critical details can be masked.

Because Explorer for CPM is designed for general use, Websense includes two configurations:

- ◆ One access method allows users to see all data. This includes employee and machine names.
- ◆ One access method allows users to see software data but hides the employee names and machine names. This option allows employees to perform statistical and analytic review of data without having access to information that could violate privacy laws.

Explorer for CPM shows only software launch and network access details: for inventory data, use CPM Reporter. For complete details, read *Websense Enterprise Explorer for CPM Administrator's Guide*.

Accessing Explorer for CPM from Websense Enterprise Manager

You can open Explorer for CPM from Websense Enterprise Manager if you have the appropriate access:

1. In Websense Enterprise Manager, select **Actions > Launch Explorer for CPM** on the menu.
2. When the Administration page opens, select:
 - **Unlimited Access** if you want to see all available information including user and machine names.
 - **Restricted Access** if you want to see available information without seeing user and machine names.
3. If you are asked for a user name and password, enter them, and then click **OK**.

Explorer for CPM opens for use.



NOTE

Your user name and password are case sensitive.

For complete details about Explorer for CPM, read the *Websense Enterprise Explorer for CPM Administrator's Guide*.

Accessing Explorer for CPM from the Start Menu

You can open Explorer for CPM from the **Start** menu if you have appropriate access. This option allows you to go directly to Explorer for CPM rather than opening Websense Enterprise Manager and accessing it from there.

1. Select **Start > Programs > Websense Enterprise > Explorer for CPM**.

2. When the **Administration** page opens, select:
 - **Unlimited Access** if you want to see all available information including user and machine names.
 - **Restricted Access** if you want to see available information without seeing user and machine names.
3. If you are asked for a user name and password, enter them, and then click **OK**. Explorer for CPM opens for use.

Client/Server Authenticated Communications

CPM uses authenticated communications between CPM Server and Client Agent. This adds extra security to communications, and stops any potential unauthorized access to CPM Server and changes to rules that are sent to Client Agent.

CPM verifies authenticated communications using a unique, unpublished encrypted key. The key is created from a passphrase you provide during installation and unpublished keys in CPM. The combination of these elements identify the encrypted key.



NOTE

If, for some reason, you do not want to use authentication for your CPM installation, contact Websense Technical Support for assistance. Phone numbers and email addresses are listed in *Appendix A: Technical Support*, page 315.

Once you have installed CPM on your server or servers, the Client Agent receives the encrypted key through one of the following methods:

- ◆ If you deploy the Client Agent with the Websense Enterprise Manager, the encryption key is installed with the Client Agent.
- ◆ If you deploy the Client Agent using scripts and the Client Deployment Service, the encryption key is installed with the Client Agent.
- ◆ If you install Client Agent locally, you must provide either your passphrase or the encrypted key. You can locate the encrypted key in the `CAMServer.ini` file. By default, the file is at `C:\Program Files\Websense\bin`.

CPM Policy Differential Downloads

The CPM policy download from CPM Server to Client Agent is designed to minimize bandwidth use and maintain rapid changes to the policy. Once the initial information is available to Client Agent, CPM Server sends only changes to the data:

- ◆ When you first install CPM, the Websense Enterprise Master Database downloads to CPM Server. In Websense Enterprise Manager, basic Websense rules immediately take affect.
- ◆ When you install Client Agent, CPM Server transfers the current rules, and a subset of the master database that is appropriate for Client Agent control.
- ◆ If you run an inventory, and then create a software set from the inventory, CPM Server sends a subset of the inventory data to Client Agent.
- ◆ Once the initial data is transferred, CPM Server sends only changed information:
 - If the Websense Enterprise Master Database changes, CPM Server sends only the changed information.
 - If the rules change, CPM Server sends only the changes.
 - If the inventory and/or software sets from inventory change, CPM Server sends only the changes.

Rules and the CPM Policy

Websense Enterprise Client Policy Manager uses a rules-based policy to monitor and control software launch requests and network access attempts. This approach combines flexibility, maximizes usability, while balancing power and ease of use.

Each CPM rule is, essentially, an equation that identifies how Client Agent is to process software launch requests and/or network access attempts by a given user, at a particular machine.

Each CPM rule identifies:

- ◆ The circumstances when the rule is applied. For details, refer to [Part 1: Status Options](#), page 52.
- ◆ What Client Agent does when a machine or employee tries to launch software. For details, refer to [Part 2: Launch Control](#), page 52.

- ◆ What Client Agent does when software tries to access a network port. For details, refer to *Part 3: Port Access Control*, page 53.
- ◆ What information—if any—Client Agent passes to CPM Server for logging. For details, refer to *Part 4: Event Logging*, page 54.

System administrators create and define rules in the **Rules** pane, described in *Chapter 14: Working with Rules*, page 255.

Part 1: Status Options

The first part of a rule defines the circumstances when the rule is in effect. Each rule is set to one of the following:

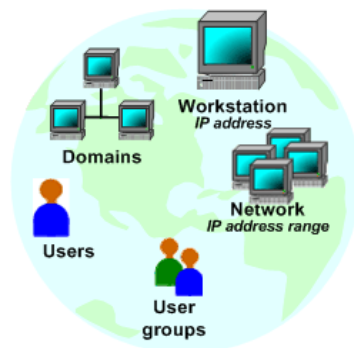
- ◆ **Always active:** The rule is always in the policy, and impacts machines and users regardless of network connection details.
- ◆ **Never active:** The rule is never in the policy, and never impacts machines and users. This selection is often used during initial setup and testing to inactivate rules.
- ◆ **Connected:** The rule is in the policy only when the machine is able to communicate with CPM Server.
- ◆ **Disconnected:** The rule is in the policy only when the machine is not able to communicate with CPM Server.

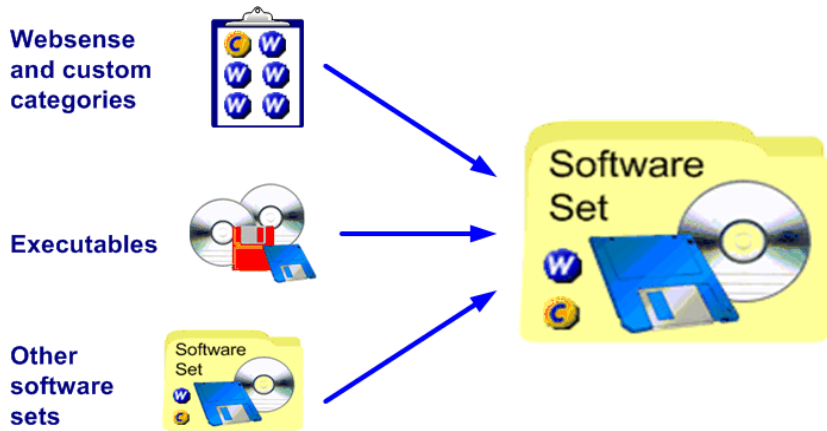
For complete details, read *Status Settings*, page 256.

Part 2: Launch Control

The second part of a rule defines what happens when a specific machine or employee tries to launch a specific software file. This part identifies:

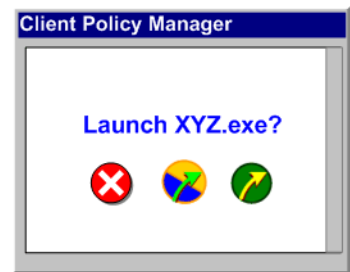
- ◆ Whom the rule affects, as identified by the client set. Client sets may include machines, users, user groups, and domains, in any combination. For complete details, refer to *Chapter 10: Working with Client Sets*, page 191.
- ◆ What software files are controlled by the rule, as identified by the software set. Software sets may include entries for Websense and/or custom categories, individual executables, and existing software sets. For details, refer to *Chapter 12 Working with Software Sets*.





Potential Software Set Contents

- ◆ How Client Agent responds when a launch request occurs. Each rule is set to Block, Continue, or Permit an application launch. For each rule, this setting affects all machines and users included in the client set, and all files included in the software set.





CPM Server processes the second part of the rule to decide how to handle launch requests. If launch control is set to Permit or Continue, then CPM Server checks network access settings.

Part 3: Port Access Control

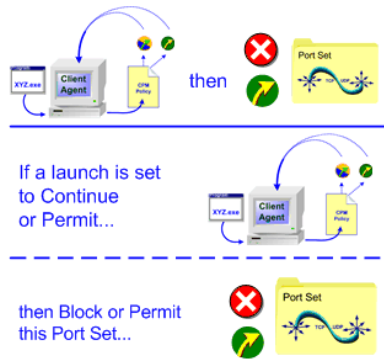
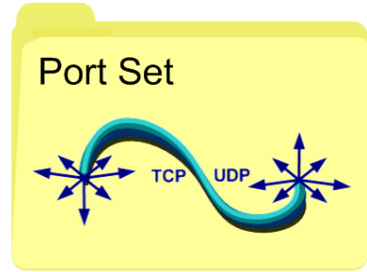
The third part of a rule identifies what happens if the application tries to access a port. If the rule is set to Block, port access is not supported for any application in the rule. However, if CPM Server determines that an application may launch, it then checks to see what happens if the application tries to access the network.

Port access settings define:

- ◆ If Client Agent is to permit or block ports.  

- ◆ What port set Client Agent is to permit or block. For more details, read *Chapter 13: Working with Port Sets*, page 243.

The results of the port access checks determine whether or not an application identified in the software set, and set to Continue or Permit, can access the network via the port the software is trying to use.

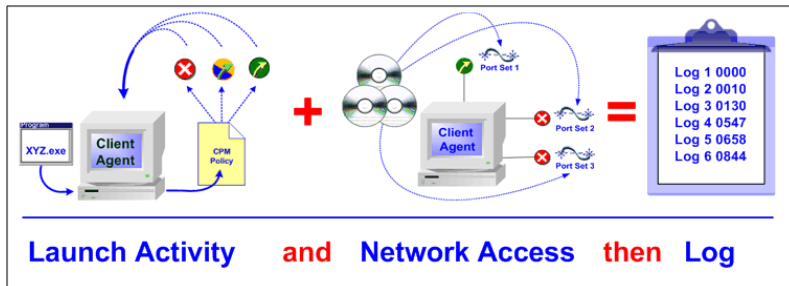


Network Access Control

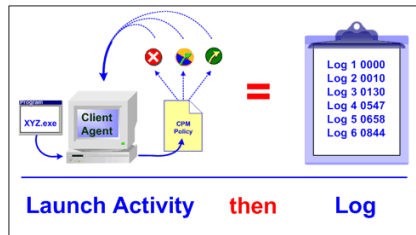
Part 4: Event Logging

The final portion of the rule identifies logging parameters. Logging can be set to log the following:

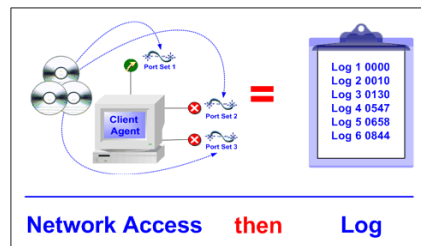
- ◆ Launches and network activity



◆ Launch activity



◆ Network activity



◆ Nothing at all



Do Not Log

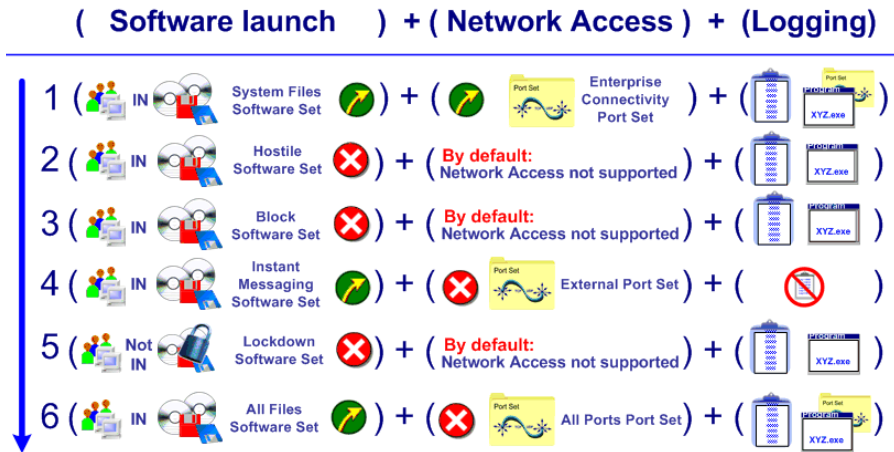
The settings you choose for logging impact any activity that occurs for the rule. Information that may be logged includes:

- ◆ User or machine information
- ◆ Date and time
- ◆ File information, including name, publisher and suite, depending on the available information.
- ◆ Results of launch activity (block, continue, permit)
- ◆ Results of network access (block, permit)

Implementing the CPM Policy

When Client Agent recognizes a launch or port access attempt, it checks the CPM rules, stored locally, to determine what the correct response will be. It also checks the locally saved database information to correctly identify the application that is trying to launch, and implement any custom parameters.

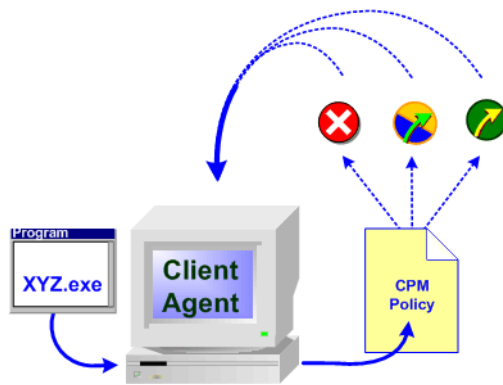
Client Agent starts with the first rule in the policy and moves to the last. When Client Agent finds the first true statement, it processes the launch request or network access attempt accordingly.



Rules Processing Order

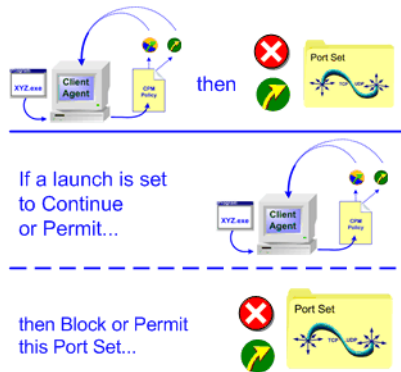
For each rule, Client Agent determines:

- ◆ Whether the rule affects the machine, the user, or both
- ◆ If the software appears in the included software set
- ◆ The action that Client Agent is to take when that executable tries to launch



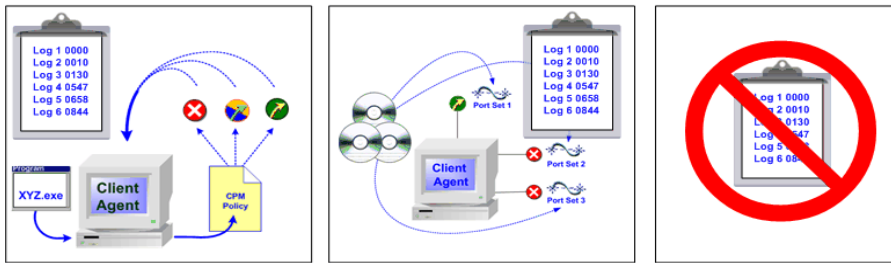
Client Agent Launch Request Checks

- ◆ Whether or not that executable is allowed to access ports if the launch is set to Continue or Permit
- ◆ Which ports are affected by the network block or permit setting



Client Agent Network Access Check

- ◆ What logging—if any—is to occur for software launch requests and/or port access attempts.



Log Launch Activity (and/or) Log Network Access (or) Do Not Log

Logging Selections

If logging occurs, Client Agent sends the details to CPM Server, which then forwards the data information to the CPM Log Database. Launch and port information can be viewed in CPM Reporter and Explorer for CPM.

Configuring Client Policy Manager

Before you fully implement Client Policy Manager, you may want to configure options that impact the module. Some options are set the first time when you install Client Policy Manager. For other functions, you can accept default values or change them when necessary.

Use Websense Enterprise Manager to configure:

- ◆ CPM connections and support settings
 - *Working with Policy Server*, page 60
 - *Subscribing to CPM*, page 63
 - *Configuring User Services*, page 69
 - *Understanding Database Downloads*, page 77
 - *Changing the Password*, page 82
 - *Configuring AppCatcher*, page 85
 - *Configuring the Database Connection*, page 101
- ◆ Client Agent and/or user interaction settings
 - *Setting Email Notification for Administrators*, page 67
 - *User Messages*, page 87
 - *Setting Client Control*, page 102

Working with Policy Server

The Websense Enterprise Manager **Server** menu allows you to work with Policy Servers in your network. These options are also available by clicking the right mouse button in the navigation tree.

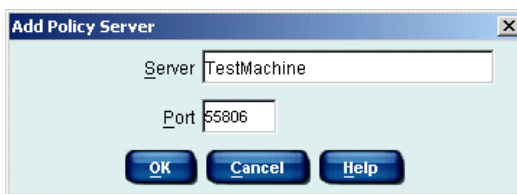
Adding a Policy Server

You cannot configure Client Policy Manager until you add a Policy Server via Websense Enterprise Manager. You must perform this operation for each Policy Server if you have not done so previously.

To add Policy Server, you must know the IP address or host name of the Policy Server machine. This machine may or may not be the same machine on which Websense Enterprise Manager is installed. You must add at least one Policy Server when you first set up the Client Policy Manager system. When you add a server, you must create a password for secure access.

To add a Policy Server:

1. Select **Start > Websense > Websense Enterprise Manager** to open Websense Enterprise Manager.
2. In Websense Enterprise Manager, click the **Desktop** tab.
3. Right-click in the Websense Enterprise Manager navigation tree, and then select **Add Server**. You can also select **Server > Add Policy Server** from the menu. The **Add Server** dialog box appears.



Add Server Dialog Box

4. Enter the IP address or host name of the Policy Server machine in the **Server** field.
5. Enter the port number for sending configuration information to Policy Server. The default is 55806. The actual entry should be the configuration port you identified during installation.

6. Click **OK**. An icon and the IP address or host name appears in the navigation tree.
7. Double-click the entry for the Policy Server in the navigation tree to configure or enter the password.
 - If this is the first time you are accessing a Policy Server, the Set Websense Password dialog box opens for password configuration.



Set Websense Password Dialog Box

- a. Enter the password in the **Password** field, and then press the **Tab** key on the keyboard.
 - b. Reenter the password in the **Confirm Password** field.
 - c. Click **OK** to save the password and access the Policy Server.
- If the Policy Server already has an assigned password, the **Password** dialog box opens for password entry. Enter the password, and then click **OK**.

The **Summary Data** pane opens, which is described in [Chapter 5: Viewing Summary Data, page 117](#). If this is a new installation, you must enter the subscription data now. For information, read [Subscribing to CPM, page 63](#).

Connecting to a Policy Server

To work with Client Policy Manager, you need to connect to a Policy Server. Specific behaviors of which you should be aware are:

- ◆ During future sessions, the password you enter the first time is required to connect to the Policy Server.
- ◆ If you have already connected to the Policy Server during the current session in Websense Enterprise Manager, a **Connecting** message appears while the Manager connects to the Policy Server. The password is not necessary.
- ◆ If you are in a session and already connected to a Policy Server, you can connect to any other server as needed.

The Policy Server stores CPM policy details and user access information. To connect to the Policy Server:

1. Choose the Policy Server you need from the **Current Server** list, and then select **Server > Connect to Server** from the menu. You can also right-click the Policy Server, and then select **Connect to Server** from the shortcut menu.
2. Enter the password, and then click **OK**.

Disconnecting from a Policy Server

You can disconnect from a Policy Server at any time. Once you disconnect, you cannot configure that server until you reconnect to it again. If you exit from Websense Enterprise Manager, the process automatically disconnects all identified Policy Servers. If you log back onto the system, you need to connect to the Policy Server or servers again.

- ◆ Choose the Policy Server you need from the **Current Server** list, and then select **Server > Disconnect from Server**. You can also right-click the Policy Server in the **Current Server** list and then select **Disconnect from Server**.

Websense Enterprise Manager severs the current connection.

Deleting a Policy Server

You can delete a Policy Server when necessary. For example, the CPM Server is being moved to a new machine. You delete the entry for the machine that is no longer used.

1. If necessary, disconnect from the Policy Server. Read *Disconnecting from a Policy Server*, page 62.
2. Select the Policy Server you want to remove, and then click **Delete**. You can also right-click the Policy Server and then select **Delete**. Websense Enterprise Manager displays a warning message.
3. Click **OK** to delete the Policy Server from the **Current Server** list.

Accessing the Settings Pane

The **Settings** pane supports configuration options for Websense servers and operating procedures. The initial settings are defined during installation or by Websense, Inc., and can be changed at any time. When the **Settings** pane is open, links on the left provide navigation.

To access the **Settings** pane:

- ◆ Click **Server > Settings** on the Websense Enterprise Manager menu to open the **Settings** pane. You can also right-click anywhere in the navigation tree, and then select **Settings** from the shortcut menu.

Subscribing to CPM

You initially enter subscription data when you first install Websense Enterprise CPM. Later, however, you may need to update the subscription information to add licenses or when you extend your subscription.

Additionally, the **Subscription** pane provides a link to your saved subscription data, the current number of licenses you have, and your current expiration date.

You must have an active internet link to connect to Websense and complete the subscription process:

1. Click **Server > Settings** on the Websense Enterprise Manager menu to open the **Settings** pane. You can also right-click anywhere in the navigation tree, and then select **Settings** from the shortcut menu.
2. Select **Subscription** from the **Settings Selection** list to access **Subscription** settings.



Subscription Pane

3. If your subscription key does not already appear in the **Subscription Key** field, type in your 16- or 18-character key. Your entry must match exactly the subscription key that Websense, Inc. provides
4. Click **Subscription Info** to open a browser and link to the Websense **Registration** page. Follow on-screen instructions to complete the registration process.
5. Click **Update Registration Info** to save your entries and close the registration form.
6. Close the browser.
7. Click **OK** to save the changes you made since you opened the **Settings** pane.

If you originally subscribe to one Websense module, and then later add a second module, you do not need to resubscribe to the new module. When you contact Websense and purchase another subscription, automatic processes update the subscription key when you receive a download of the Websense

Enterprise Master Database. The changes in the subscription then take effect, and register the new subscription details with CPM Server.

Working in the Proxy/Authentication Pane

If your network connection to the Internet uses a proxy server, provide authentication information so the Websense Enterprise Master Database downloads without manual intervention. The **Proxy/Authentication** pane provides the tools for identifying the proxy server and required authentication if necessary.

The screenshot shows a 'Settings' dialog box with a 'Proxy' pane selected. The 'Proxy' pane contains the following configuration options:

- Use proxy server
- Server:
- Port:

The 'Authentication' pane contains the following configuration options:

- Use authentication
- Authentication name:
- Password:

At the bottom of the dialog box are three buttons: **OK**, **Cancel**, and **Help**.

Proxy/Authentication Pane

Identifying the Proxy Server

If Websense must go through a proxy server or firewall to access the Internet and download the Websense database, you must identify that proxy for database download operations:

1. Select **Server>Settings** on the Websense Enterprise Manager menu to open the **Settings** pane. You can also right-click anywhere in the navigation tree, and then select **Settings** from the shortcut menu.
2. Select **Proxy/Authentication** from the **Settings Selection** list to access **Proxy/Authentication** settings.
3. Click the **Use proxy server** checkbox, and then enter the following:
 - Enter the IP address or server name for the proxy server in the **Server** text box. There is no default address.
 - Enter the port for the proxy server in the **Port** text box.
4. Define authentication if appropriate.
5. Click **OK** to save the changes you made since you opened the **Settings** pane.

If you have other tasks to complete, you can continue defining settings without clicking **OK** until you are done.

Forcing Authentication

You can force authentication for the Websense Enterprise Master Database downloads. This lets downloads pass through proxy servers and/or firewalls without manual intervention. When Websense, Inc. receives the download request, the authentication information you provide is passed on with the database download.

To force authentication:

1. Select **Server>Settings** on the Websense Enterprise Manager menu to open the **Settings** pane. You can also right-click anywhere in the navigation tree, and then select **Settings** from the shortcut menu.
2. Select **Proxy/Authentication** from the **Settings Selection** list to access **Proxy/Authentication** settings.
3. Click in the **Use authentication** check box to activate the function. The default value is not checked.
4. Define the **Use Authentication** setting:

- Type a user name in the **Authentication name** text box. The entry may be from 1 to 64 alphanumeric characters in length.
 - Enter a user password in the **Password** text box. Passwords are case-sensitive and appear as asterisks (* * *) when you enter them.
5. Click **OK** to save the changes you made since you opened the **Settings** pane.

If you have other tasks to complete, you can continue defining settings without clicking **OK** until you are done. Once authentication is set, the Websense Enterprise Master Database downloads occurs on schedule, without manual intervention.

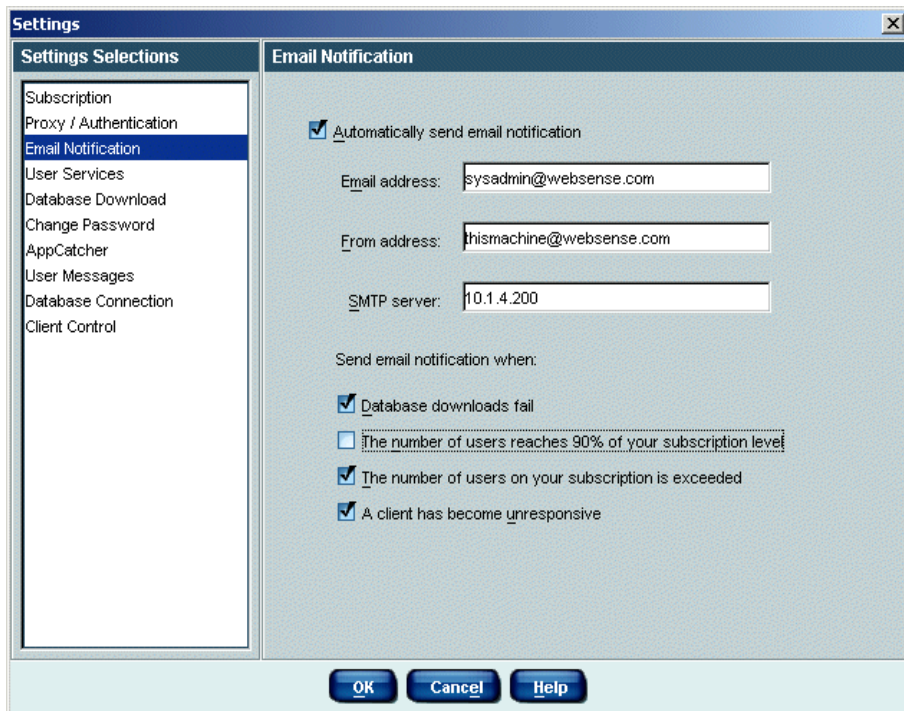
Setting Email Notification for Administrators

You can set email notification to notify yourself or another system administrator when:

- ◆ Database downloads fail
- ◆ The number of users reaches 90% of the subscription level
- ◆ The number of users exceeds the number of subscribed users
- ◆ Client Agent is not in communication with CPM Server but the machine where Client Agent is installed is online

These selections provide you with up-to-the-minute monitoring advantages because you receive emails whenever notification is appropriate. For example, you receive emails showing that the number of users is exceeding the number of subscriptions. This allows you to determine how many more licenses you need to assure network security.

1. Click **Server > Settings** on the Websense Enterprise Manager menu to open the **Settings** pane. You can also right-click anywhere in the navigation tree, and then select **Settings** from the shortcut menu.
2. Select **Email Notification** from the **Settings Selection** list to open the **Email Notification** pane.



Email Notification Pane

3. Click the **Automatically send email notification** check box to activate email notification.
4. Enter the email address for email delivery in the **Email address** field. This can be any appropriate email address.
5. Enter the email address that is identified as the originator in the **From address** field. This can be any appropriate address.
6. Enter the IP address for the SMTP server in the **SMTP server** field.
7. Select the events for which you want an email sent:
 - **Database downloads fail** sends an email when the Websense Enterprise Master Database download fails for any reason.
 - **The number of users reaches 90% of your subscription level** sends an email when the number of users is nearing the upper limit of the available subscription level.

- **The number of users on your subscription is exceeded** sends an email when send an email when the number of users exceed your subscription level.
 - **Unresponsive Clients** sends an email if a Client Agent is not communicating with CPM Server, but the machine where Client Agent is installed is identified as being online.
8. Click **OK** to save the changes you made since you opened the **Settings** pane.

If you have other tasks to complete, you can continue defining settings without clicking **OK** until you are done.

Configuring User Services

The Client Policy Manager components use Directory Services functions to provide access to users, groups, and/or domains. To do so, however, Websense Enterprise Manager must be configured to access your directory service for information. Once this is set, you can request inventories for specific machines and domains, and add objects to client sets. For information, read *Chapter 10: Working with Client Sets*, page 191.

There are two user services that you can choose from. The decision depends entirely on your network configuration.

- ◆ Windows NT Directory
- ◆ Windows Active Directory



NOTE

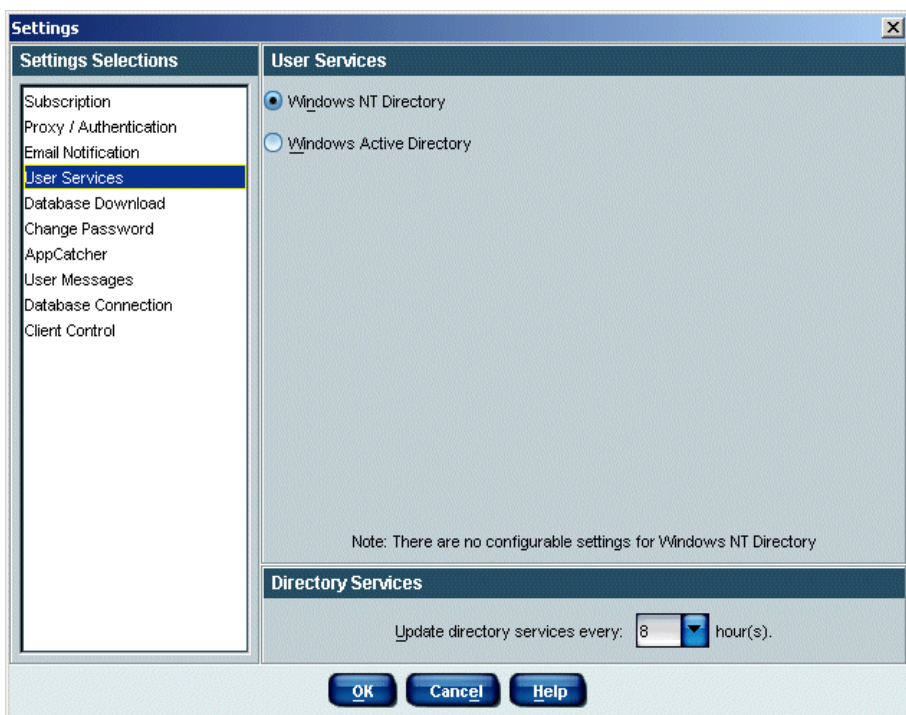
If you change the directory service once you have initially configured it, you need to modify the services to run as a particular user. Likewise, you may have to add domain forests if you are using Windows Active Directory.

Configuring Windows NT Directory

To configure Windows NT Directory:

1. Select **Server > Settings** on the Websense Enterprise Manager menu to open the **Settings** pane. You can also right-click anywhere in the navigation tree, and then select **Settings** from the shortcut menu.

2. Select **User Services** from the **Settings Selection** list to access **User Services** settings.



User Services Pane

3. Select **Windows NT Directory**.
4. Enter a time frame for updating the list of users that Websense Enterprise Manager recognizes in the **Update directory servers every n hours**, where **n** is a numeric value you specify. The default is once every 8 hours. You can select any value between 1 and 24 hours.
5. Click **OK** to save the changes you made since you opened the **Settings** pane.

If you have other tasks to complete, you can continue defining settings without clicking **OK** until you are done.

Configuring Active Directory Services

If you use Active Directory, configure Websense to communicate with the Global Catalog Server. This section describes the basic process. Refer to the *Websense Enterprise Administrator's Guide* for additional details. This guide can be found at: <http://ww2.websense.com/global/en/SupportAndKB/ProductDocumentation/>.

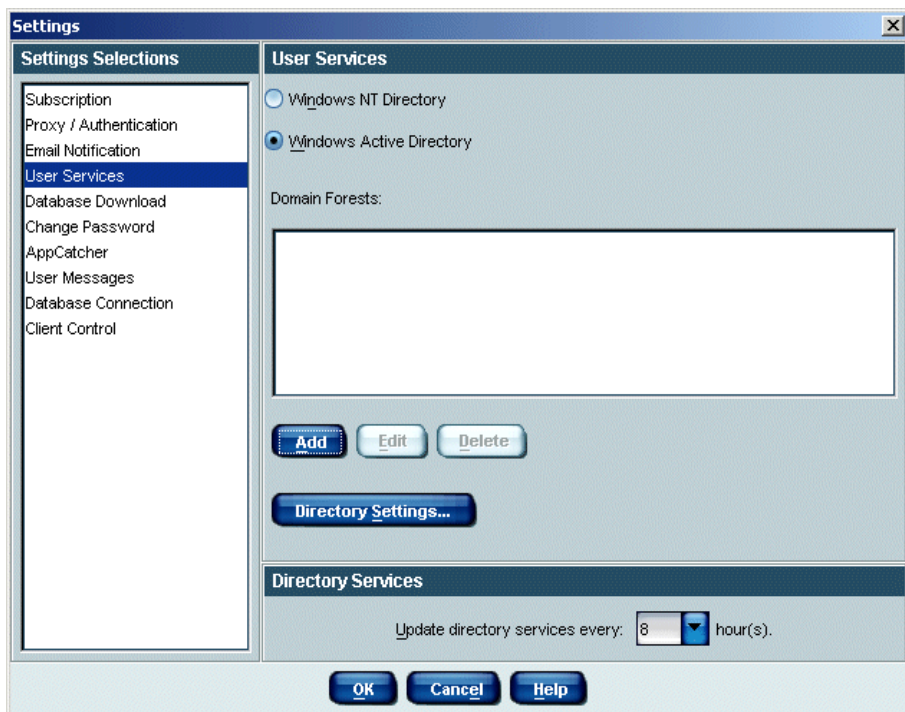


NOTE

If you have more than 2,000 users in a single Active Directory container, you must increase the user limit in Global Catalog Server in order for the users in your directory service to be included for Client Policy Manager. Check Websense Knowledge Base item 741 for instructions at <http://www.websense.com/support/knowledgebase/>.

To identify the User Service:

1. Make sure the User Service can connect to domain controllers in your network. Otherwise, local groups will display when you add directory objects to Websense Enterprise Manager.
2. Connections to domain controllers are enabled automatically during Active Directory setup, but it's a good idea to verify this from the User Service machine, using ping or a similar utility.
3. In Websense Enterprise Manager, choose **Server > Settings**. The **Settings** dialog box appears.
4. Select **User Service** in the navigation pane to access directory service options.
5. Select **Active Directory**.



Active Service Directory Settings

6. Add any domain forests that are necessary. Read [Adding a Domain Forest](#), page 72.
7. Define any advanced settings that are necessary. Read [Entering Advanced Settings](#), page 74.
8. Click **OK** to close the **Settings** dialog box and update Policy Server with your changes.

Adding a Domain Forest

To add a domain forest for Windows Active Directory:

1. In Websense Enterprise Manager, choose **Server > Settings**. The **Settings** dialog box appears.
2. Select **User Service** in the navigation pane to access directory service options.
3. Add a Global Catalog Server as a domain forest:
 - a. Click **Add** to open the **Domain Forest** dialog box.

Domain Forest

Global Catalog Server: test5 Port: 3268

Root Context: (optional)

Administrative Account

To access the domain forest, Websense requires the distinguished name for a user account with administrative privileges. Enter the individual components or the full distinguished name below.

Distinguished Name by Components:

User Name: Administrator

Password: ****

Account Folder: Users

Domain Name: t1test

Full Distinguished Name:

User DN: cn=Administrator, cn=Users, dc=t1test

Password: ****

OK Cancel Help

Domain Forest Dialog Box

- b. Enter the machine name or IP address of the **Global Catalog Server**. Websense, Inc. recommends using the machine name to reduce any problems that may be caused to your data if IP addresses change.
- c. Enter the **Port** over which Global Catalog Server communicates with Policy Server. The default is 3268.
- d. Enter the top-level **Root Context** for the organization, for example, *dn=com*.
 - If you leave this field blank, Websense begins searching at the top level of the directory service.
 - You can use an entry further down in the directory if appropriate.



NOTE

If transparent user identification is enabled, do not assign the same user name to multiple domains. If you have multiple domains and need to use duplicate user names, configure Websense to search one domain at a time. If Global Catalog Server is associated with more than one domain, and Policy Server finds duplicate account names that are used by employees to log on, Websense cannot transparently identify that user.

- e. Under **Administrative Account**, select **Distinguished Name by Components** to enter the distinguished name (DN) for the administrative account Websense will use to access the domain forest. Use the common name (cn) form of the administrative user name, and *not* the user ID (uid) form.

- f. Enter the DN components separately in the **User Name**, **Password**, **Account Folder** and **Domain Name** fields.

The Account Folder field does not support values with the *organizational unit (ou) tag, for example, ou=Finance*. If your administrative account name contains an *ou* tag, you must enter the **Full Distinguished Name** for the administrative account, as described below. For example, *cn=Admin, cn=Users, ou=InfoSystems, dc=company, dc=net*.

- 4. Repeat Step a through Step f for each Global Catalog Server machine.
- 5. Click **OK** when finished.

Entering Advanced Settings

Advanced settings allow you to provide granular information for processes that access user services. You can specify custom filters and security.

When Client Policy Manager components call user services, it searches the directory service for user, group, and domain information--which are also called *class types*. The search looks for entries with the attribute names of *organization* and *organizationalunit* by default.

If you have customized object class types within the directory, you must configure Websense Enterprise Manager to recognize the new object class types. To do this, edit search filters in Websense Enterprise Manager.

For example, instead of only searching for objects of type *organizationalunit* in the directory, Websense would also search for object of type *dept*. Alternatively, you could replace the argument (*objectclass=organizationalunit*) with (*objectclass=dept*), to have Websense search for objects of type *dept* instead of *organizationalunit*.



NOTE

The **Use SSL** option is specific to iPlanet Directory, which may be used by the Websense Enterprise Web filtering component. This setting does not impact Client Policy Manager components.

To enter advanced settings for Windows Active Domain:

1. In Websense Enterprise Manager, choose **Server > Settings**. The **Settings** dialog box appears.
2. Select **User Service** in the navigation pane to access directory service options.
3. Click **Directory Settings** to open the **Advanced Directory Settings** dialog box. Check default settings and use them if appropriate. If you need to make changes, continue with this procedure.

The image shows the 'Advanced Directory Settings' dialog box. It is divided into three main sections: Filters, SSL, and Character Set.

Filters Section:

- Use Custom Filters
- User ID Attribute: sAMAccountName
- First Name Attribute: givenname
- Last Name Attribute: sn
- User Search Filter: (&(objectclass=person)((objectclass=computer)((cn=*\$)))
- Group Attribute: cn
- Group Search Filter: (objectclass=group)
- Domain Search Filter: organizationalunit(objectclass=domain)(&(objectclass=container)(cn=users)))
- User's Groups Search Filter: (&(member=%dn)(uniquemember=%dn))

SSL Section:

- Use SSL
- Check if the server's certificate is issued by a trusted CA
- Certificate Database: [Empty text box]
- Use certificate based client authentication
- Key Name: [Empty text box]
- Key Database: [Empty text box]
- Password: [Empty text box]

Note: Database files must reside on the Websense User Service machine.

Character Set Section:

- UTF-8
- MBCS

Buttons: OK, Cancel, Help

Advanced Directory Settings Dialog Box

4. If you want to define custom filtering, insert a check in the **Use Custom Filters** checkbox. Attributes are strings used in searching the directory service contents.
 - a. Enter the **User ID attribute** to define which attribute is used to identify or authenticate users.
 - b. Enter the **First Name attribute** to define which attribute appears as the first name in Client Policy Manager Reporter.
 - c. Enter the **Last Name attribute** to define which attribute appears as the last name in Client Policy Manager Reporter.
 - d. Enter the **User Search Filter** to define which objects appear as users in Websense Enterprise Manager.
 - e. Enter the **Group Attribute** to define which attribute appears as the group name in Websense Enterprise Manager.

- f. Enter the **Group Search Filter** to define which objects appear as groups in Websense Enterprise Manager.
- g. Enter the **Domain Search Filter** to define which objects appear as folders in Websense Enterprise Manager.
- h. Enter the **User's Groups Search Filter** to define search parameters used for determining group membership.

The **Use SSL** selections do not impact Client Policy Manager modules. These are specific to directories other than Active Directory, and only impact Websense Enterprise Web filtering installations.

5. Click **OK** to close the **Settings** dialog box and update Policy Server with your changes.

Understanding Database Downloads

The Websense Enterprise Master Database is created and maintained by Websense, Inc., and contains application and port data in addition to Websense categorization and risk class association. The database must be present for Client Agent installation and for policy implementation.



IMPORTANT

If you edit host files and/or routing tables that restrict the URLs a Websense server can access, make sure you permit the following:

- ◆ download.websense.com
- ◆ ddsdom.websense.com
- ◆ ddsint.websense.com
- ◆ portal.websense.com
- ◆ www.my.websense.com

You must permit these URLs to access Websense Enterprise Master Database downloads and your Websense subscription data.

Downloads of the Websense Enterprise Master Database occur:

- ◆ Immediately after you have finished entering subscription data
- ◆ On a regular schedule and changes in the database have occurred
- ◆ When manually requested and changes in the database have occurred



IMPORTANT

Once the initial database download is successful, failure to download the database in the future has no impact on internal processes: your Client Policy Manager subscription continues to work until it expires. However, if you do not continuously update your local copy of the database, your policy will not contain the latest application and port information.

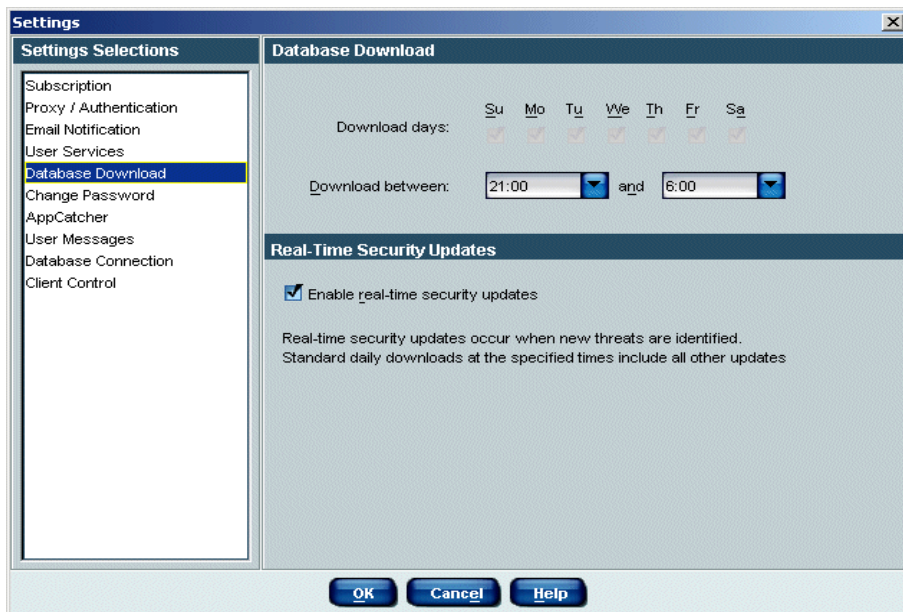
Defining the Database Download Schedule

When you install CPM, the Websense Enterprise Master Database is scheduled to download every day, between the hours of 9:00 pm and 6:00 am. You can change the schedule at any time, to meet your business requirements.

For example, your company runs two overlapping shifts: one from 8:00 am to 5:00 pm, and one from 4:00 pm to 11:00 pm. You decide that you do not want the database download to potentially interfere with computer usage during the second shift, and change the range of download time to 12:00 am to 7: am. The database download will now occur within the time frame you identified.

To change the database download schedule.

1. Click **Server>Settings** on the Websense Enterprise Manager menu to open the **Settings** pane. You can also right-click anywhere in the navigation tree, and then select **Settings** from the shortcut menu.
2. Select **Database Download** from the **Settings Selection** list to access **Database Download** settings.



Database Download Schedule Pane

3. Click in the **Download days** check boxes to identify any day, or combination of days, you want the download to occur. By default, all days are checked. For example, if check marks appear for Mo (Monday), We (Wednesday), and Fr (Friday), downloads occur every Monday, Wednesday, and Friday.
4. Define a time range for the download by selecting a start and end time in the **Download between nn and nn** fields, where **nn** is the time you select. Websense Enterprise Manager attempts to download the Websense database sometime within this time frame. By default, the time range is between 21:00 and 06:00 hours (9:00 pm and 6:00 am).
5. Select **Enable real-time security updates** to receive updates when new threats are identified rather than at your regularly scheduled download time.
6. Click **OK** to save the changes you made since you opened the **Settings** pane.

If you have other tasks to complete, you can continue defining settings without clicking **OK** until you are done.

Monitoring Database Downloads

You can monitor downloads as they are active if you wish. Monitoring a database download during initial configuration is not uncommon, as you cannot deploy Client Agent until the download is complete.



NOTE

Because regularly scheduled downloads usually occur after business hours, monitoring downloads after the initial configuration is usually not necessary.

To monitor the initial download, scheduled downloads, or manually requested downloads during the download process:

1. Connect to the appropriate Policy Server. Read [Adding a Policy Server](#), page 60.
2. Select **Server > Database Download**. The **Database Download** dialog box opens, which shows the status as **Loading**.

When the download is complete, the following details are updated:

- Result of the last database download, which may be **Success**, **Fail**, or **Error Connecting**
 - Current database version
 - Date and time of the last download attempt
3. When the current download status changes to **Idle**, click **Close** to close the dialog box.

Manually Requesting a Database Download

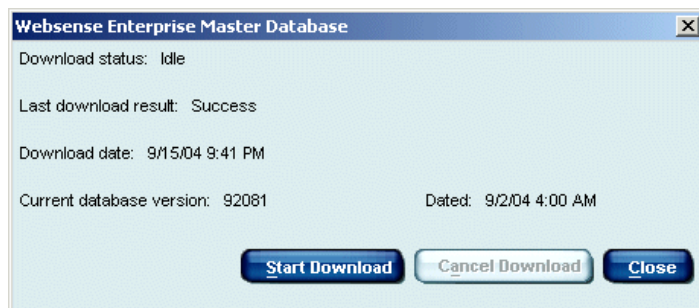
You can manually request a Websense Enterprise Master Database download at any time, without impacting your regularly scheduled download. For example, your company closes for two weeks at the end of the year, and all outside communications are cut off during this period. When you return you manually request the database to collect the most recent information.

**WARNING**

If you request a manual download, be sure that you are not impacting any critical system operations. The download may take some time to complete, and CPU usage may peak at 100% usage. Generally, Websense, Inc. recommends that downloads occur during non-business hours.

To manually request a download:

1. Connect to the appropriate Policy Server. Read *Adding a Policy Server*, page 60.
2. Select **Server > Database Download**. The **Database Download** dialog box opens, which shows:
 - Current download status, which may be **Idle**, **Connecting**, **Downloading**, or **Loading**
 - Result of the last database download, which may be **Success**, **Fail**, or **Error Connecting**
 - Current database version
 - Date and time of the last download attempt



Manual Database Download Dialog Box

3. Click **Start Download** to begin the download. You can stop the download at any time if necessary by clicking **Cancel Download**.
4. When the current download status is **Idle** again, click **Close** to close the dialog box.

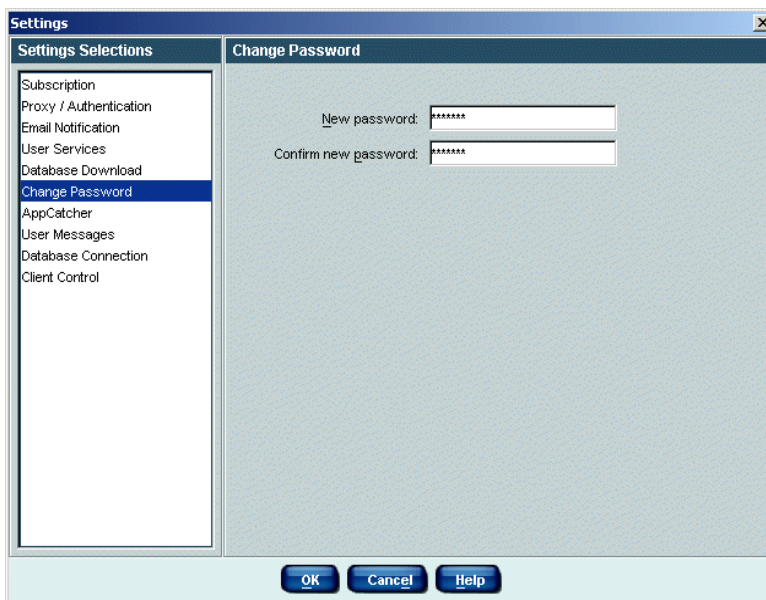
Changing the Password

You originally define your Websense Enterprise Manager password when you first log on and subscribe to Client Policy Manager. You can change the password when appropriate. Though Websense Enterprise Manager does not force you to make password changes, it is a good idea to change the password every 30 to 45 days, or whenever there is any situation that may cause security concerns.

Passwords are case-sensitive, and appear as asterisks (* * *) when you enter them. If others need to use the password, make sure you provide them with the new password, including any case-sensitive characters.

To change the password:

1. Select **Server>Settings** on the Websense Enterprise Manager menu to open the **Settings** pane. You can also right-click anywhere in the navigation tree, and then select **Settings** from the shortcut menu.
2. Select **Change Password** from the **Settings Selection** list to access **Change Password** settings.



Change Password Dialog Box

3. Enter the new password in the **New password** text box. Your entry must be 4 to 25 characters in length, and may include any combination of alphanumeric characters.
4. Enter the new password a second time in the **Confirm new password** text box.
5. Click **OK** to save the changes you made since you opened the **Settings** pane.

If you have other tasks to complete, you can continue defining settings without clicking **OK** until you are done.

You need to enter the new password the next time you connect to Policy Server, and every time thereafter, until you change it again.

Introducing AppCatcher

Websense AppCatcher™ helps improve the accuracy of the Websense Enterprise Master Database, and thus improve CPM monitoring and control options. When AppCatcher is enabled, details about unrecognized applications and ports are sent to Websense, Inc. While it is not mandatory to use this function, it plays a critical role in your ability to maintain your Websense Enterprise Master Database and access updated information.

Client Agent collects inventory, launch, and port data. This information is sent to CPM Server, and server processes start that try to match the Client Agent data to information in the Websense Enterprise Master Database. If the executable or application is not in the database, CPM Server inserts it and marks it as *Uncategorized*.

When AppCatcher is enabled, you decide if you want to submit information on all executables or applications found during inventories or identified during launch requests, or only those executables and applications that are not in the Websense Enterprise Master Database. Unrecognized port access is automatically sent if you enable AppCatcher

When it is time to submit information to Websense, Inc., AppCatcher queries CPM Server for information, using the configuration options to determine if you want to upload all available data or only information about uncategorized files. Once information is available, AppCatcher forwards the details to Websense, Inc. for review.

For each executable and/or application, the uploaded data contains the following information:

- ◆ File name
- ◆ Version
- ◆ Header information
- ◆ File size, measured in bytes
- ◆ Registry data settings from HKEY_LOCAL_MACHINE
- ◆ **Start** menu shortcut settings
- ◆ Any port activity that is unrecognized for the application

When Websense, Inc. receives AppCatcher lists of executables, applications, and/or ports, a response team analyzes the information, and then classifies the executable or application. Once analysis is complete, the response team adds the new information into the master Websense Enterprise Master Database.

The Appcatcher also passes details about network ports that software has attempted to use. This allows Websense, Inc. to identify software behavior and help customers respond to threats in a more useful manner.

When any Websense customer downloads the newest version of the Websense Enterprise Master Database, CPM Server overwrites the local database with the new information to complete the cycle. It generally takes between 7 and 14 working days to complete a full review cycle—that is, from the time Websense, Inc. receives information about an uncategorized executable until the results appear in the Websense Enterprise Master Database download at your site.

You can select the time of day when you want AppCatcher to send information to Websense, Inc. This lets you transmit details when network activity is low and least likely to impact business activity.



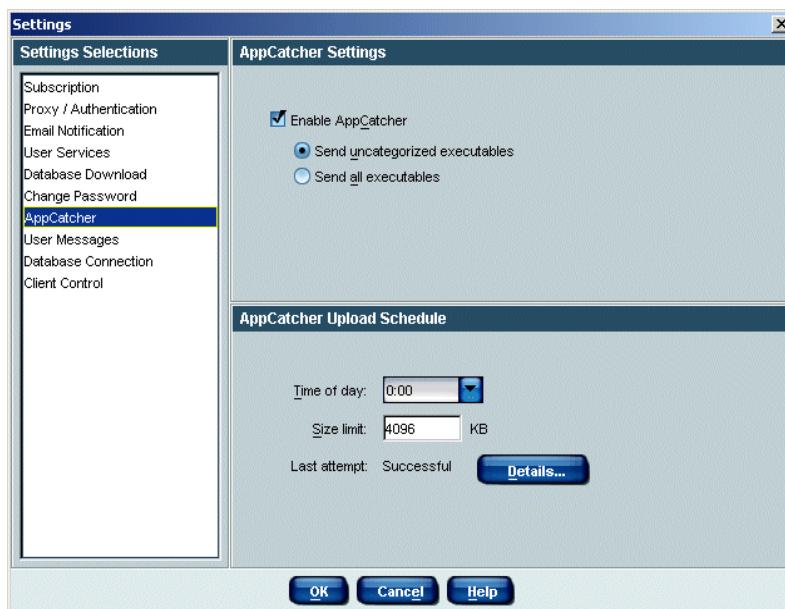
NOTE

For AppCatcher functionality, you must install IIS 4.0 or above on the CPM Server machine, and have an Internet connection to post HTTP successfully

Configuring AppCatcher

To configure AppCatcher:

1. Select **Server > Settings** on the Websense Enterprise Manager menu to open the **Settings** pane. You can also right-click anywhere in the navigation tree, and then select **Settings** from the shortcut menu.
2. Select **AppCatcher** from the **Settings Selection** list to access **AppCatcher Settings** options.



AppCatcher Dialog Box

3. Check the **Enable AppCatcher** check box to send software information to Websense, Inc. for review. This is selected by default.
4. Identify what information is sent to Websense, Inc. in the **AppCatcher Settings** area:
 - **Send uncategorized applications** sends reports to Websense, Inc. only for executables and/or applications that do not appear in the Websense Enterprise Master Database. By default, this is enabled.

- **Send all applications** sends reports to Websense, Inc. that contain all executables and/or applications found during inventory.



NOTE

If you manually categorize an executable by moving it from one Websense category to a different Websense category, or to a custom category, the executable is sent to Websense, Inc. as *Uncategorized*. Response teams may reanalyze how these executables appear in the Websense Enterprise Master Database to better reflect actual business use.

5. Define the daily submission schedule in the **AppCatcher Upload Schedule** area:
 - Select the time you want the daily update to occur in the **Time of day** field. The default time is midnight, local time.
 - Enter a number that defines the maximum size for any submittal in the **Size limit** field. This value is measured in kilobytes (Kb), with a default of 4096 Kb. By controlling the size of the update, you can better control bandwidth consumption.
6. Click **OK** to save the changes you made since you opened the **Settings** pane.

If you have other tasks to complete, you can continue defining settings without clicking **OK** until you are done.

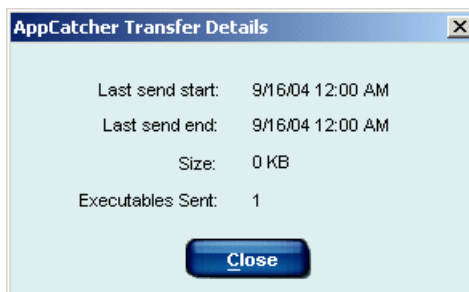
The information associated with the **Last attempt** entry is read-only and shows the results for the last submission attempt. The text is either **Successful** or **Failed**.

AppCatcher Transfer Details

When the **AppCatcher** pane is open, you can view details about the last transfer of AppCatcher data.

1. Click **Details**. The **AppCatcher Transfer Details** dialog box opens and shows the following information:
 - **Last send start**. Shows the date and time when the last submission started.

- **Last send end.** Shows the date and time when the last submission ended.
- **Size.** Shows the total size of the AppCatcher report file.
- **Executables sent.** Shows the total number of executable and/or application signatures included in the file.



AppCatcher Transfer Details

2. Click **Close** to return to the **Settings** pane.
3. Click **OK** to save the changes you made since you opened the **Settings** pane.

If you have other tasks to complete, you can continue defining settings without clicking **OK** until you are done.

User Messages

Default user messages are available immediately when Client Policy Manager is installed. As you customize your installation, you can modify these messages.

You can redefine the user messages that appear when Client Agent blocks a launch or port request, or when it presents a continue message. The messages are fully configurable, and can be edited at any time to reflect your organization's launch permissions and restrictions. Client Agent presents these messages when it blocks an executable or a port, or when the executable is set to "Continue."

The messages are HTML-based. If you change the default wording, be sure to include any existing HTML tags if you want to continue showing specific executable and category information. You can insert other HTML tags in the text to further customize the message if you want. Read [Using Websense HTML Tags](#), page 94, for a complete list of HTML tags, and their use.

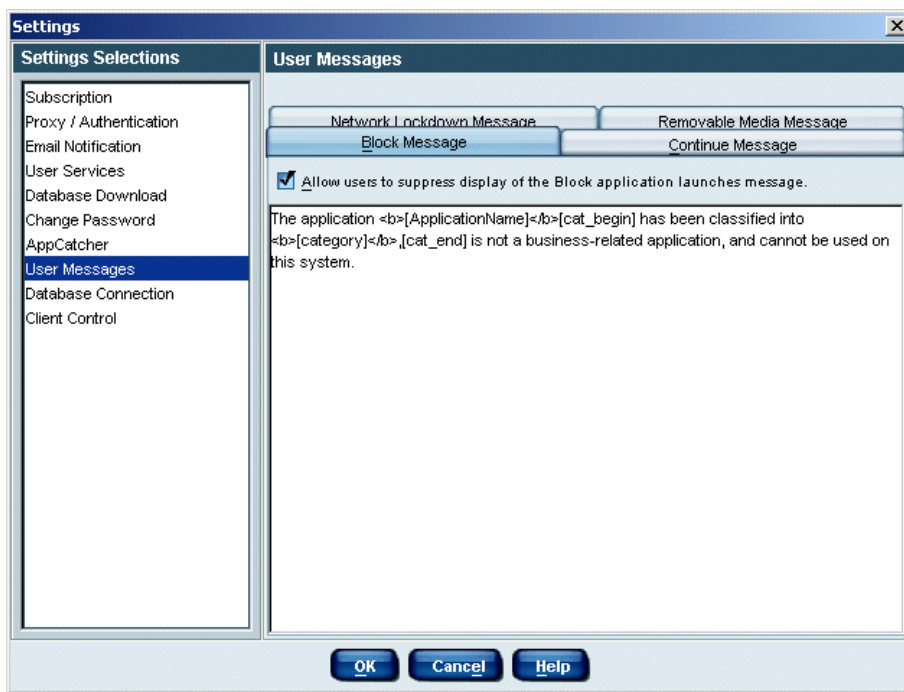
Websense, Inc. recommends using a message that briefly and clearly explains why an executable or port is blocked or an executable is set to continue. If you provide solid information, company employees have a better understanding of why your organization is blocking port or launch requests or setting executable launches to “Continue.”

Customizing Text

While Websense, Inc. provides standard text for user messages, some companies prefer to create their own. For example, a company may decide to mention that applications are blocked to increase security and improve productivity, rather than simply informing employees that they are being blocked from an application.

To change a user message:

1. Click **Server>Settings** on the Websense Enterprise Manager menu to open the **Settings** pane. You can also right-click anywhere in the navigation tree, and then select **Settings** from the shortcut menu.
2. Select **User Messages** from the **Settings Selection** list to open the **User Messages** pane.



User Message Selections

3. Click the appropriate tab to modify a message. Your choices are:
 - **Block Message.** For specifics, refer to *Block Messages for Executables*, page 90.
 - **Continue Message.** For specifics, refer to *Continue Messages for Executables*, page 90.
 - **Network Lockdown Message.** For specifics, refer to *Network Lockdown Messages for Ports*, page 91.
 - **Removable Media Message.** For specifics, refer to *Removable Media Lockdown Message*, page 92.
4. Specify any changes to the default settings and/or text messages. Each message may be between 4 and 1,000 characters in length, may include any keyboard characters, and may include HTML tags in the body.

The default message includes codes that Client Agent uses to identify an executable by name and category. You should not remove these codes if you want messages to include specific details. Read *Using Websense HTML Tags*, page 94.

5. Select how you want the message to be displayed.
 - **Do not display the <blocking feature> message to users**—disables the block message for all users.
 - **Allow users to suppress display of the <blocking feature> message**—a checkbox appears on the block message allowing individual users to suppress the message at their discretion.
6. Click **OK** to save the changes made since you opened the **Settings** pane.

If you have other tasks to complete, you can continue defining settings without clicking **OK** until you are done.

Block Messages for Executables

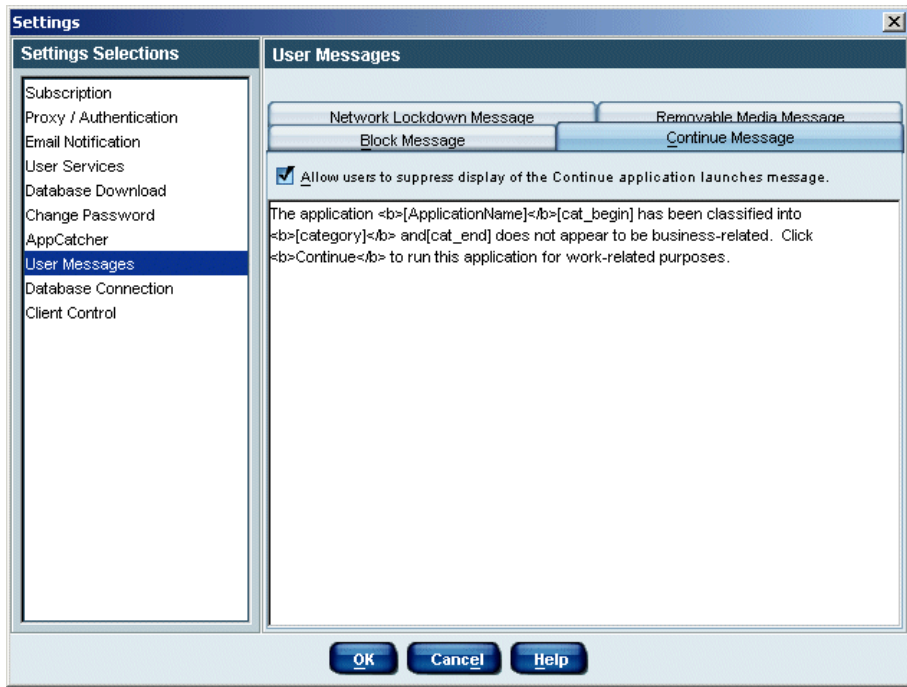
The text that appears when you select **Server > Settings > User Messages > Block Message** forms the message that Client Agent presents to employees when they try to launch software that is blocked. You can customize the default Websense text to meet company requirements.

The default text is:

```
The application <b>[ApplicationName]</b>
[cat_begin] has been classified into
<b>[category]</b>, [cat_end] is not a business-
related application and cannot be used on this
system.
```

Continue Messages for Executables

The text that appears when you select **Server > Settings > User Messages > Continue Message** forms the message that Client Agent presents to employees when they try to launch software that is set to continue. You can customize the default Websense text to meet company requirements.



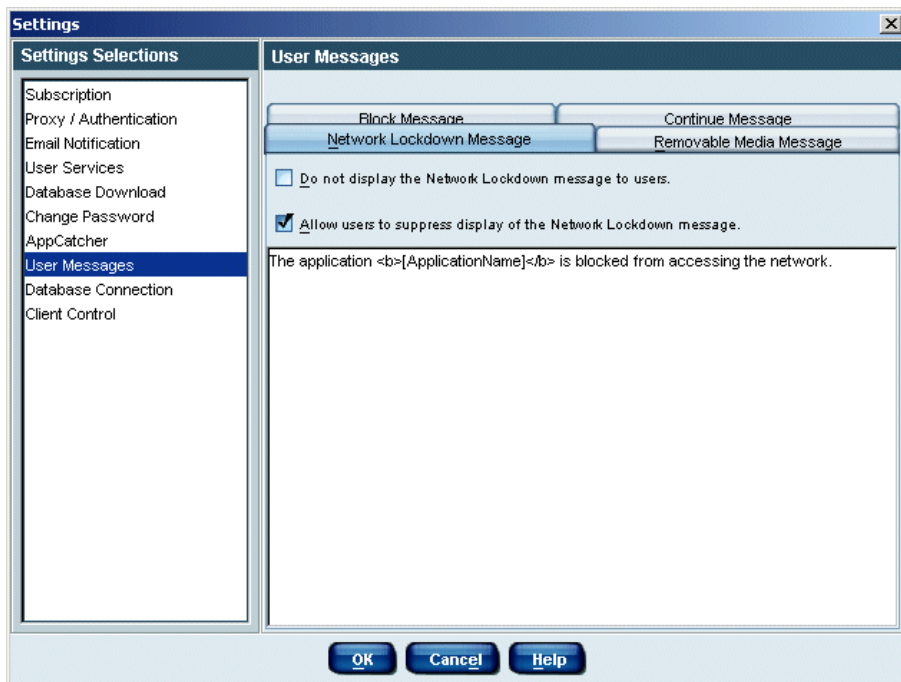
Continue Message Setup

The default text is:

```
The application <b>[ApplicationName]</b>
[cat_begin] has been classified into
<b>[category]</b> and [cat_end] does not appear
to be business-related. Click <b>Continue</b> to
run this application for work-related purposes.
```

Network Lockdown Messages for Ports

The text that appears when you select **Server > Settings > User Messages > Network Lockdown Message** forms the message that Client Agent presents to employees when they try to launch software and access a port that has been blocked. You can customize the default Websense text to meet company requirements.



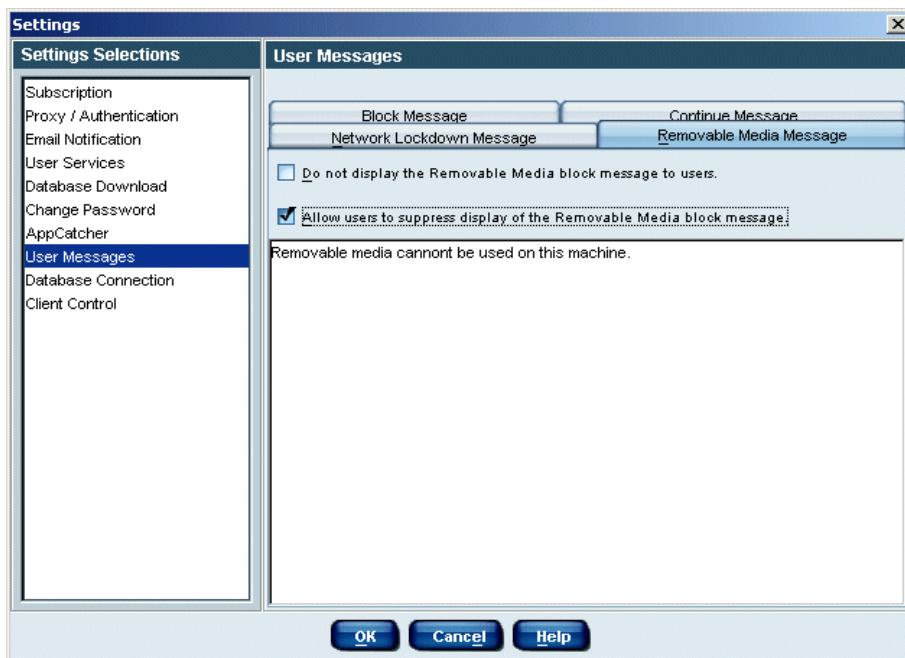
Network Lockdown Message Setup

The default text is:

```
The application <b>[ApplicationName]</b>
[cat_begin] is blocked from accessing the
network.
```

Removable Media Lockdown Message

The text that appears when you select **Server > Settings > User Messages > Removable Media Message** forms the message that Client Agent presents to employees when Removable Media Lockdown is enabled. Users in lockdown cannot mount devices such as flash drives, CD/DVD burners, floppy drives, and external hard drives



Removable Media Lockdown Message Setup

The default text is:

Removable media cannot be used on this machine.

Controlling User Overrides

When employees see block, continue, and network lockdown messages, the messages may include a check box labeled **Remember my selection**, which, if you accept default settings, appears in the lower left corner of all user messages. This allows employees to determine whether they want to ignore messages or continue viewing them.



NOTE

Your setting on the user override function impacts all employees who receive the message.

When the **Remember my selection** option is active, and the employee enables this feature, Client Agent retains the employee selection for that executable forever. The only way to change settings at client machines is to

change the selection in the appropriate message dialog box or an administrator resets overrides.

For example, an employee receives a continue message for Microsoft Photo Editor, selects **Remember my selection**, and then clicks **Block**. From now on, Client Agent blocks Microsoft Photo Editor, and the continue message does not reappear.

You can reset the user override option in Websense Enterprise Manager. For details, refer to [Resetting Overrides](#), page 149.

Using Websense HTML Tags

The text that Websense, Inc. provides as a default for user messages include HTML code that, if changed, impact the way messages look, the information that is included, and/or may impact variable text. The next table shows HTML tags that are in the original Websense message, and that you can also use in custom messages.

Code	Description
 and 	These start and end codes appear around text that is bold in the message. For example, the entry Continue, bolds the word Continue .
[Application]	Brackets around the word “application” causes the message to show the application that is being blocked or that has been set to continue. This value changes, depending on the application the employee is trying to open. Note: If you alter this tag, the application name will not appear in the message, and/or your new message may include unwanted text.
[Category]	Brackets around the word “category” causes the message to show the category to which the application that is being blocked or that has been set to continue is assigned. This value changes, depending on the application the employee is trying to open. Note: If you alter this tag, the category will not appear in the message, and/or your new message may include unwanted text.

Code	Description
[cat_begin] and [cat_end]	<p>The HTML tags [cat_begin] and [cat_end] bracket variable text. In the Websense message, the brackets and text string read: [cat_begin] has been classified into [category] [cat_end].</p> <p>If an employee tries to open an application that is blocked or set to continue, but is not assigned to a category, the text between the [cat_begin] and [cat_end] tags does not appear. Otherwise, the message includes the bracketed text and identifies the category to which the application is assigned.</p> <p>Note: If you alter these tags, the category will not appear in the message, the variable text will not work, and/or your new message may include unwanted text.</p>
[Port]	<p>Brackets around the word “port” causes the message to show the port that has been accessed by software, but is being blocked. This value changes, depending on the port that is impacted by the application launch.</p> <p>Note: If you alter this tag, the network name will not appear in the message, and/or your new message may include unwanted text.</p>
[Transport]	<p>Brackets around the word “transport” causes the message to show the network that has been accessed by software, but is affected by a blocked port. This value changes, depending on the network that is impacted by the application launch.</p> <p>Note: If you alter this tag, the network name will not appear in the message, and/or your new message may include unwanted text.</p>

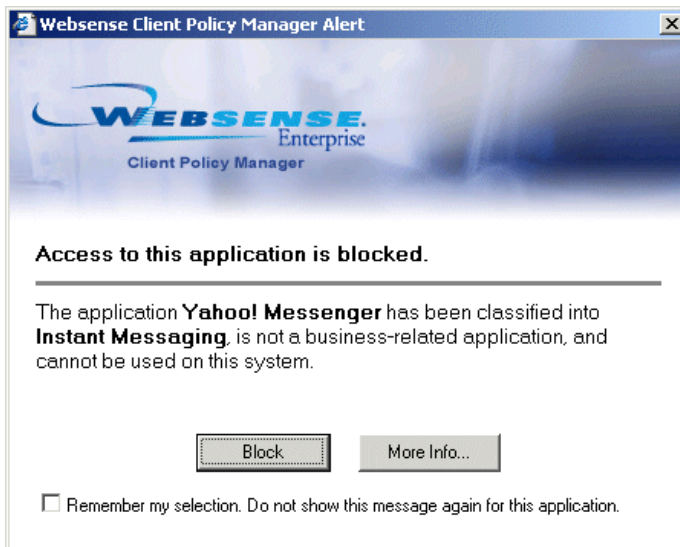
Employee Interaction with Messages

When employees receive user messages, they must respond before Client Agent allows access to any application. Messages stay on top of any currently open applications.

These messages provide information about the application or port, and why the employees are receiving the message. The message can help educate employees and reduce or eliminate their attempts to access software that is blocked or that calls blocked ports.

Interacting with the Executables Block Message

When an employee accesses an application that is blocked, a block message appears.



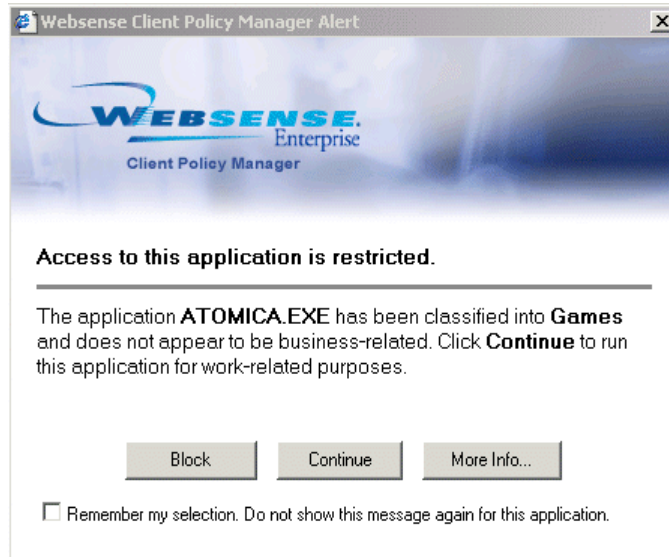
Block Message Example

The employee can:

- ◆ Click **Block** to close the message.
- ◆ Click **More Info** to view details. Read [Reviewing the More Information Message, page 100](#).
- ◆ Check the **Remember my selection** check box if Websense administrators enabled the **User Override** function, described in [Controlling User Overrides, page 93](#).

Interacting with the Continue Message

When an employee accesses an application that is set to continue, a continue message appears.



Continue Message Example

The employee can:

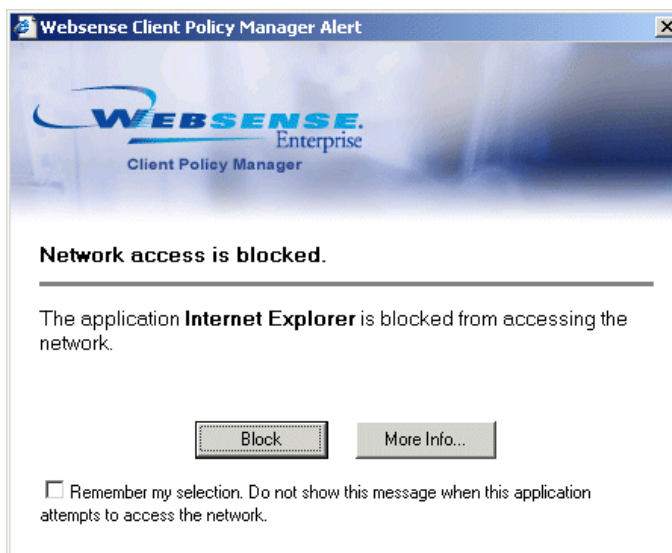
- ◆ Click **Block** to close the message and stop the launch.
- ◆ Click **Continue** to close the message and continue the launch.
- ◆ Click **More Info**. Read [Reviewing the More Information Message](#).
- ◆ Check the **Remember my selection** check box if Websense administrators enabled the **User Override** function, described in [Controlling User Overrides](#), page 93.

Interacting with the Network Lockdown Message

Network Lockdown messages appear anytime an application launch tries to access a blocked port. This impacts any launch attempt that access a blocked port, regardless of whether the original request was generated by users, other applications, system startup, or any other way a launch can be started.

When an employee accesses an application that is blocked at the network level, a block message appears. The employee can:

- ◆ Click **Block** to close the message.
- ◆ Click **More Info** to view details. Read [Reviewing the More Information Message, page 100](#).
- ◆ Select the **Remember my selection** checkbox if you do not want to see the block message in the future when the indicated application tries to launch.



Network Alert Message Example

Interacting with the Removable Media Lockdown Message

The Removable Media Lockdown message is displayed to users who attempt to mount removable media. Removable Media Lockdown can be configured to block writable media only or all types of removable media. The message should reflect the blocking option selected.



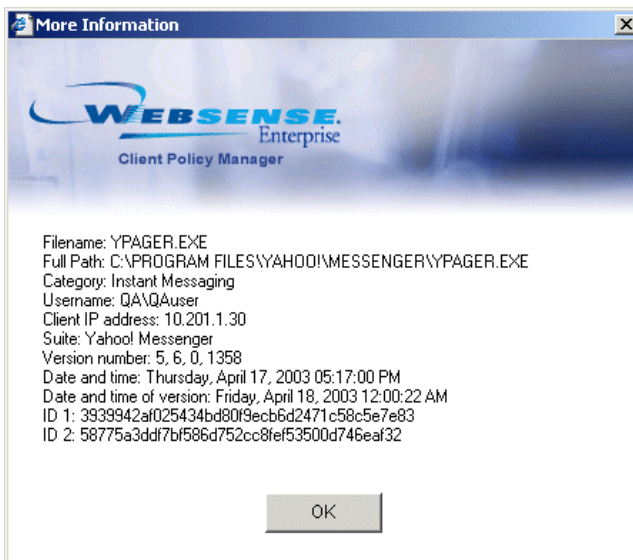
Removable Media Lockdown Message

To resolve the message:

1. If present on the message screen, you can select the **Remember my selection** checkbox to conceal the message in the future.
If this option is not selected, or if the system administrator has not granted users this right, the message will appear each time users attempt to mount removable media on a locked down machine.
2. Click **OK** to clear the message.

Reviewing the More Information Message

If employees receive block or continue messages, they can view executable details by clicking the **More Info** button.



More Information Dialog Box Example

The **More Information** dialog box users access includes the following details for the application they are trying to launch:

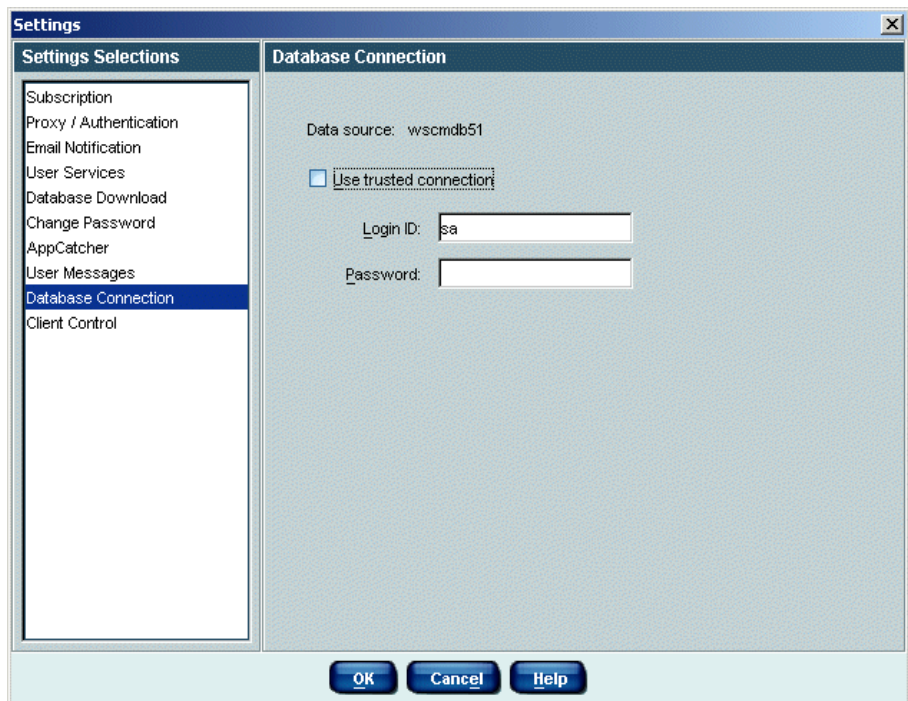
- ◆ File name
- ◆ Full path where the executable resides
- ◆ Category to which Websense, Inc. has assigned the executable
- ◆ User name, which includes the domain and user login name
- ◆ IP address for the client machine
- ◆ Version number of the executable
- ◆ Date and time the launch request occurred
- ◆ Date and time the publisher assigned to the executable
- ◆ Encrypted Websense IDs
- ◆ If the **More Information** dialog box is associated with blocked ports, TCP port ID number appears

After employees view the **More Information** dialog box, they must click **OK** to close it, and then must respond to the original block or continue message before they can continue working at that client machine.

Configuring the Database Connection

Microsoft SQL database configuration occurs the first time during installation. You can modify these settings, however, if you change connections you **must** restart Client Policy Manager Server service. Your entries link CPM Server and the SQL Server database: without this setting, CPM Server is not able to access any CPM database.

1. Click **Server > Settings** on the Websense Enterprise Manager menu to open the **Settings** pane. You can also right-click anywhere in the navigation tree, and then select **Settings** from the shortcut menu.
2. Select **Database Connection** from the **Settings Selection** list to access **Database Connection** settings.



Database Connection Pane

3. Click in the **Use trusted connection** check box if you want to use the account that CPM Server is configured to run as to access the database. The default is not enabled.
4. Enter a user ID in the **Login ID** field. The default value is **sa**.
5. Enter a password in the **Password** field. The default is blank.
6. Click **OK** to save the changes you made since you opened the **Settings** pane.

If you have other tasks to complete, you can continue defining settings without clicking **OK** until you are done.

Setting Client Control

Client Control lets you define heartbeat settings that enable Client Policy Manager Server to monitor system health, control the peer-to-peer port for Outbreak distribution, and define logging intervals to reduce network impact. The settings you make here affect Client Agent at machines in your network.

Functions you can set are:

- ◆ Heartbeats. Refer to [Understanding Heartbeats, page 102](#).
- ◆ Client-to-Client Distribution port. Refer to [Understanding CPM Client-to-Client Distribution, page 103](#).
- ◆ Application Logging intervals. Refer to [Understanding the Application Logging Interval, page 104](#).
- ◆ Disabling your policy for all machines. Refer to [Globally Enabling and Disabling the CPM Policy, page 106](#).

Understanding Heartbeats

CPM Server uses the heartbeat entry to monitor the health of client machines. The heartbeat helps you identify situations when an employee may have attempted to disable Client Agent or when a machine is not communicating with CPM Server.

When Client Agent sends heartbeat data to CPM Server, the message lets the server know that the Client Agent installation at the machine is functional. Client Agent sends the following data with the heartbeat:

- ◆ Overall status
- ◆ Client ID

- ◆ Client version
- ◆ Current user of the machine
- ◆ The domain\user path
- ◆ Machine name
- ◆ The domain\machine path
- ◆ Version information for the CPM policy residing at the client machine

The heartbeat does not impact network traffic in a significant manner, as each heartbeat packet is less than 1K in size. If you are concerned about traffic, you can increase the time between heartbeats to reduce network impact.

If a client does not send heartbeat data as expected, CPM Server waits for 5 minutes plus 2 heartbeats, and then changes the status to **Not Responding**. For example, if your heartbeat is set to 15 minutes, CPM Server would declare a client machine as non-responsive after 35 minutes [5 +2(15)]. You can view current client status in the **Client Status** pane, described in [Chapter 7: Working with Client Status, page 141](#).

CPM Server uses the heartbeat to update data. When Client Agent sends a heartbeat and pings the server, CPM Server checks to see if there are any changes in the policy and/or the databases. If so, CPM Server sends the new information back to the agent.

Inventories and Heartbeats

An inventory may begin on a client machine slightly later than scheduled, depending on the heartbeat interval you set. For example, an inventory is scheduled to run at 12:40, but agent/server communications are scheduled to occur at 12:30 and 12:45. When the CPM Server communicates with Client Agent at 12:45, the inventory scheduled for 12:40 is triggered. For complete details about inventories, read [Working with Inventories, page 151](#).

Understanding CPM Client-to-Client Distribution

The client-to-client distribution port identifies the port for CPM Outbreak distribution, described in [Emergency Outbreak Rule Processing, page 118](#). When you identify this port, machines that run Client Agent use that port to distribute critical information about malicious files between other machines in the network.

Depending on your internal communications, network and machine processing speeds, and other similar details, the Outbreak list may be

available to machines connected to your network within seconds. Once the data is available to Client Agent, any file in the list is immediately blocked whenever an employee tries to run that file.

This process allows you to protect your system from malware, which is any malicious file or process, including worms, viruses, Trojan horses, and harmful scripts.

By default, the port is set to zero, which lets CPM Server randomly choose any port that is available. Generally, this is the best selection as it allows machines to use any available path to distribute the Outbreak list. This distribution port can be disabled if your network policy prohibits peer-to-peer communication. Outbreak notification, in this case, will occur during regularly scheduled Policy Server downloads.

Understanding the Application Logging Interval

The value you enter in the **Application logging interval** field defines a buffer for application launches. Client Policy Manager logs launch requests for a given application once within the space of this interval.

This reduces repetitive entries, and consumes less database space than if Client Policy Manager were to log repetitive launches. For example, you define a 15 minute logging interval. An employee opens **Notepad** at 10:50 am, and then again at 11:00 am.

The CPM Log Database shows only the first launch request at 10:50 am, because the launch request at 11:00 am is within the buffered interval of 15 minutes. If the employee again launches **Notepad** at 11:20 am, Client Policy Manager inserts a second record in the CPM Log Database, because the third launch was more than 15 minutes after the second.

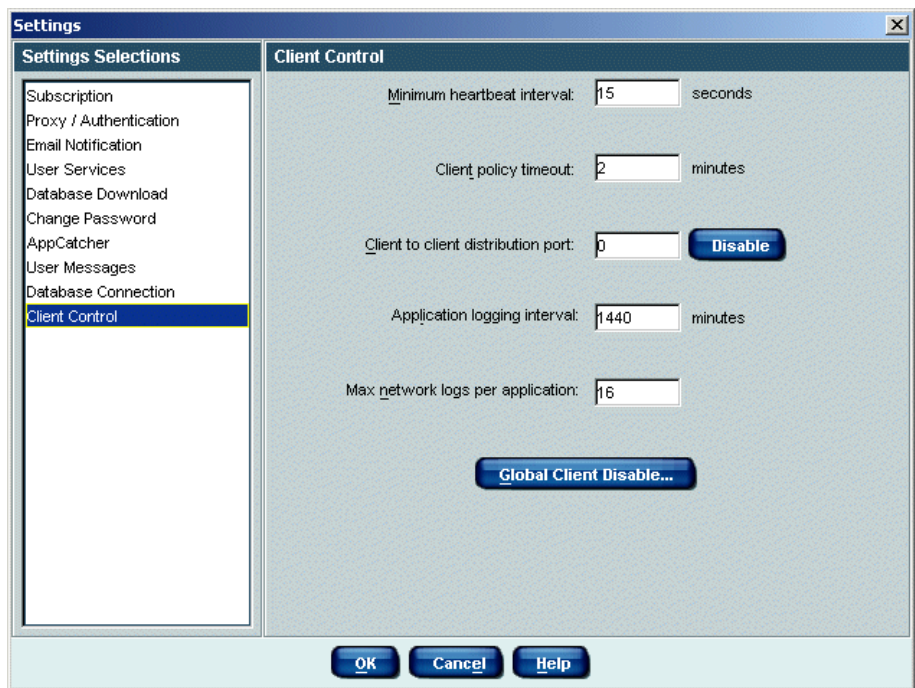
Defining Client Control

When you define Client Control, you may modify any function that appears in the pane, or any combination of functions. For example, you may only want to change the heartbeat interval, or you may want to change both the heartbeat and the application logging interval. If you do not make changes to existing data, the existing settings are enforced.

To define client control:

1. Select **Server > Settings** on the Websense Enterprise Manager menu to open the **Settings** pane. You can also right-click anywhere in the navigation tree, and then select **Settings** from the shortcut menu.

2. Select **Client Control** from the **Settings Selection** list to access **Client Control** settings.



Client Control Pane

3. Enter a number in the **Minimum heartbeat interval** field. The default setting is 15 seconds. This value defines how frequently Client Agent will try to communicate with CPM Server. The minimum value is 1 second and the maximum value is 86,400 seconds (1 day).
4. Enter a number in the **Client Policy Timeout** field. The default setting is two minutes. This value defines the length of time the connection between CPM Server and Client Agent is left open for policy transfer from the server to the client. In organizations with slow connections, the policy timeout period can be increased to allow the transfer to complete. The minimum value is 1 minute and the maximum value is 1,440 minutes (1 day).

5. Enter the port number for Outbreak distribution in the **Client to client distribution port** field. The entry may be any value between 0 and 65535.



NOTE

Your entry identifies the port for client-to-client distribution of Outbreak information. The default value of zero allows the Outbreak process to randomly chose any port that is available during processing.

You may click **Disable** to disable the port and prevent peer-to-peer client communication. Outbreak notification will then occur during policy updates.

6. Enter a number that identifies how frequently applications are logged. For details, refer to *Understanding the Application Logging Interval*, page 104.
7. Define how many network attempts should be logged for each period identified in the **Application logging interval** field. The default value is 1440.
8. Click **OK** to save the changes you made since you opened the **Settings** pane.

If you have other tasks to complete, you can continue defining settings without clicking **OK** until you are done.

Globally Enabling and Disabling the CPM Policy

The **Client Control** pane lets you completely disable the CPM policy at all machines that are connected to the network and running Client Agent. This can be useful if you are troubleshooting or reinstalling Client Agent.

When you select this option, CPM Server cancels the CPM policy completely. For all machines running Client Agent, all executables and applications are permitted to launch, and are permitted to access all ports. The policy is retained in memory, and is immediately reset when you enable it again.

Disabling CPM Policy

To disable the CPM policy:

1. Select **Server>Settings** on the Websense Enterprise Manager menu to open the **Settings** pane. You can also right-click anywhere in the navigation tree, and then select **Settings** from the shortcut menu.
2. Select **Client Control** from the **Settings Selection** list to access **Client Control** settings.
3. Click **Global Client Disable**.

The following confirmation message appears: *Are you sure you want to disable all clients? A default policy allowing all applications will be sent to all active clients.*

4. Click **Yes**. CPM Server sends the global policy to all machines connected to the network and running Client Agent. The policy permits all clients to launch all applications, and applications have complete access to network ports.
5. When the process is complete, the message box closes, and the button label changes to **Global Client Enable**. Click **OK** to close the **Settings** pane.

Restoring CPM Policy

When you are ready to restore the CPM policy for machines that are connected to the network and running Client Agent:

1. Click **Global Client Enable**. A confirmation message opens.
2. Click **Yes**. CPM Server restores the last saved policy on machines that are connected to the network and running Client Agent, closes the message dialog box, and changes the button text to **Global Client Disable**.
3. Click **OK** to close the **Settings** pane.

Getting Started With Client Policy Manager

The Websense Enterprise Manager is the central console for Websense modules. The Manager provides the following:

- ◆ Tools for deploying and monitoring Client Agent
- ◆ Tools for creating your desktop policies
- ◆ Links to reporting tools
- ◆ Client Agent status.

This section describes the basics for interacting with Websense Enterprise Manager.

Working in Websense Enterprise Manager

Websense Enterprise Manager provides the tools necessary to configure the application, set parameters for control, deploy clients, run inventories and more. These options use standard windows functions including:

Menu Options

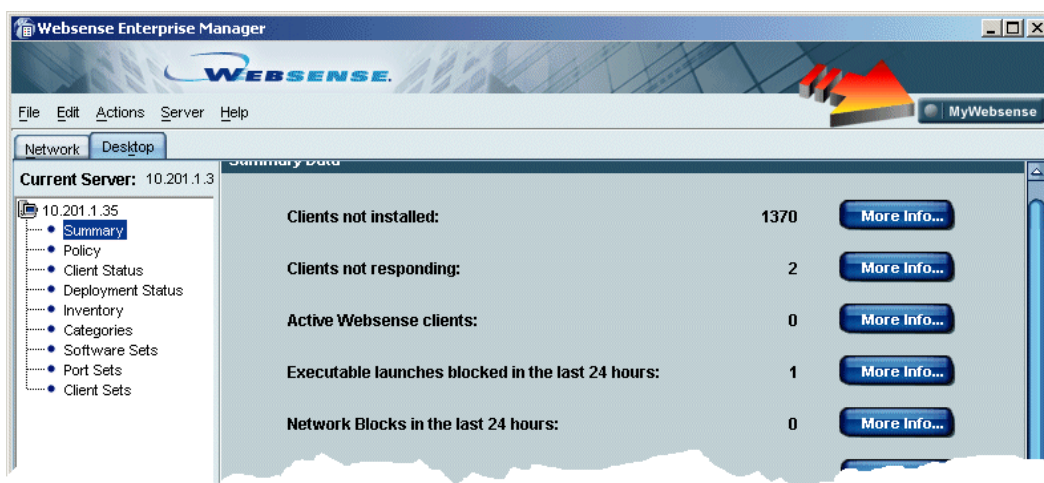
The Websense Enterprise Manager menu appears at the top of all panes, and provides jump points for server access options, setting up the Client Policy Manager system, and manually requesting a database download. If an item on the menu is grayed out, that item is not available for the module you are working with.

The available menus are:

- ◆ **File.** Exit Websense Enterprise Manager.
- ◆ **Edit.** Access cut, copy, and paste functions. These selections work in Websense Enterprise Manager text fields that appear in panes, but they do not work in dialog boxes. You can also use standard Windows keyboard shortcuts in text boxes.
- ◆ **Actions.** Access:
 - CPM Reporter, described in *CPM Reporter*, page 47 and *Websense Enterprise CPM Reporter Administrator's Guide*.
 - Explorer for CPM, described in *Explorer for CPM*, page 48 and *Websense Enterprise Explorer for CPM Administrator's Guide*.
- ◆ **Server.** Configure servers and system settings. Read *Working with Policy Server*, page 60, and *Chapter 3: Configuring Client Policy Manager*, page 59. You can also manually request database downloads, described in *Manually Requesting a Database Download*, page 80.
- ◆ **Help.** Access help topics and version information. You can also identify the browser for CPM Reporter. Read *Selecting the Web Browser*, page 115.

My Websense

The upper right corner of the Websense Enterprise Manager contains the **My Websense** button. When you click this button, the **MyWebsense** portal opens. You can also access the **MyWebsense** portal by selecting **Server > Settings > Subscription**, and clicking the **Subscription Info** button; however, the **MyWebsense** button provides fast access.



My Websense Button

The **MyWebsense** portal is customized for you. You can:

- ◆ Modify your contact information.
- ◆ See if there are any hot fixes or patches for your installed modules.
- ◆ Access Power Point training slides.
- ◆ Upgrade your subscription.
- ◆ Evaluate modules for which you do not yet have subscriptions.
- ◆ Links to the Knowledge Base and documentation

Navigation Pane Selections

When you first access Websense Manager, the navigation pane allows you to select, and connect to, CPM Servers. Once you select a server, you can then access configuration options for that server.

- ◆ To add a server, read [Adding a Policy Server](#), page 60.
- ◆ To connect to a server, read [Connecting to a Policy Server](#), page 61.

After you identify a server, and log on to it, options appear for monitoring CPM data, and setting up the CPM policy for that server. The selections you can make are:

- ◆ **Summary:** For details, refer to [Chapter 5: Viewing Summary Data](#), page 117.

- ◆ **Policy:** For details, refer to [Chapter 14: Working with Rules, page 255](#).
- ◆ **Client Status:** For details, refer to [Chapter 7: Working with Client Status, page 141](#).
- ◆ **Deployment Status:** For details, refer to [Chapter 6: Deploying Client Agent, page 127](#).
- ◆ **Inventory:** For details, refer to [Chapter 8: Working with Inventories, page 151](#).
- ◆ **Categories:** For details, refer to [Chapter 11: Working with Categories, page 201](#).
- ◆ **Software Sets:** For details, refer to [Chapter 12: Working with Software Sets, page 225](#).
- ◆ **Port Sets:** For details, refer to [Chapter 13: Working with Port Sets, page 243](#).
- ◆ **Client Sets:** For details, refer to [Chapter 10: Working with Client Sets, page 191](#).

To access any configuration option for a server, after you connect to it, double-click on your selection. Read [Chapter 3: Configuring Client Policy Manager, page 59](#).



NOTE

This guide discusses CPM features using a process flow, from start to finish. The process flow does not always follow the layout of selections in Websense Enterprise Manager.














Content Pane Presentation

The content pane, on the right side of the Websense Enterprise Manager window, changes depending on the selection you make in the navigation tree. Each selection forces the contents pane to a unique configuration for the option you choose.

For example, if you select **Policy** in the navigation pane, the content pane shows a list of existing rules that define the CPM policy. If you select **Software Sets** instead, the content pane shows the available software sets.

Symbols

When you are working with Client Policy Manager, various symbols let you interpret specific information at a glance. The following table contains the symbols, and a brief description of each.

Symbol	Description
	Permit the launch. This appears in the Rules pane. For details, refer to Chapter 14: Working with Rules, page 255 .
	Block the launch. This appears in the Rules pane.
	Warn and then continue the launch if the employee so chooses. This appears in the Rules pane.
	Websense defined this category. This appears in the Category pane and the Manage Custom Categories dialog box. For details, refer to Chapter 11: Working with Categories, page 201 .
	You or one of your peers defined this category. This appears in the Category pane and the Manage Custom Categories dialog box.
	Single machine, which may be a server or machine.
	Single user with a personal account.
	A domain is a group of computers and devices on a network that are administered as a unit with common rules and procedures.
	User group or domain users.
	There is a lockdown on this machine. This appears in the Manage Inventory dialog box. For details, refer to Managing Inventories, page 162 .
	There is a newer inventory than the one used to create the lockdown. This appears in the Manage Inventory dialog box.
	There is not a lockdown for this machine. This appears in the Manage Inventory dialog box.
	View a software set. This appears in the Add/Edit Software Sets dialog box. For details, refer to Adding a Software Set, page 232 .

Refreshing Data

Websense Enterprise Manager calls information from the appropriate database or Client Agent when you first open a dialog box, and then severs the connection and freezes the information. While you are working, you can update information you see onscreen. Websense Enterprise Manager calls the information and then freezes it again.

To update data, click **Refresh** in the:

- ◆ **Deployment Status** pane: For details, refer to *Chapter 6: Deploying Client Agent*, page 127.
- ◆ **Summary Data** pane: For details, refer to *Chapter 5: Viewing Summary Data*, page 117.
- ◆ **Client Status** pane: For details, refer to *Chapter 7: Working with Client Status*, page 141.
- ◆ **Categories** pane: For details, refer to *Chapter 11: Working with Categories*, page 201.

You can also use keyboard shortcuts to refresh these screens. The available shortcuts are:

- ◆ Press **F5**.
- ◆ Press **Alt** and **R** at the same time.

Making Multiple Selections

Websense Enterprise Manager allows you to make multiple selections when you work in the following panes and dialog boxes:

- ◆ **Deployment Status** pane: For details, refer to *Chapter 6: Deploying Client Agent*, page 127
- ◆ **Outbreak** dialog box: For details, refer to *Chapter 5: Viewing Summary Data*, page 117
- ◆ **Client Status** pane: For details, refer to *Chapter 7: Working with Client Status*, page 141
- ◆ **Run Inventory** dialog box: For details, refer to *Running an Inventory*, page 157
- ◆ **Manage Inventory** dialog box: For details, refer to *Managing Inventories*, page 162
- ◆ **Add/Edit Software Sets** dialog box: For details, refer to *Managing Software Sets*, page 231

- ◆ **Add/Edit Client Sets** dialog box: For details, refer to [Managing Client Sets, page 194](#)
- ◆ **Add/Edit Port Sets** dialog box: For details, refer to [Managing Port Sets, page 245](#)

These panes and dialog boxes support the following multiple selection methods:

- ◆ **Shift** key selections to choose a contiguous range
 - Click on an item at the top or the bottom of a series of items you want to select.
 - Press and hold the **Shift** key on your keyboard.
 - Click on an item at the other end of the series of items you want to select.

Websense Enterprise Manager highlights the items you selected and any items between them.

- ◆ **Ctrl** key selections to choose non-contiguous items
 - Click on any item.
 - Press and hold the **Ctrl** key on your keyboard.
 - Continue clicking items to select them, while continuing to hold down the **Ctrl** key.

Only the items you select are highlighted. You can remove individual items if you decide not to include them:

- ◆ Press and hold the **Ctrl** key while clicking a second time on a previously selected item. The item is no longer highlighted and is not included in the list.

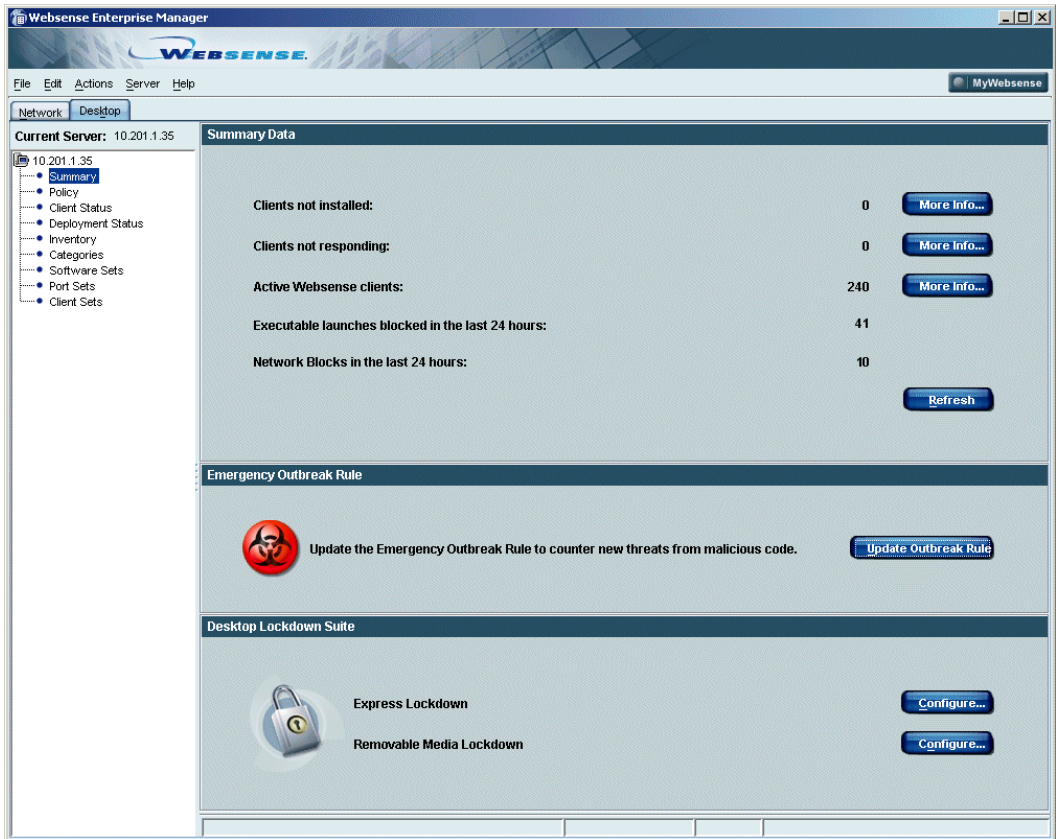
Selecting the Web Browser

You need to select the Web browser you want to use to view online help, CPM Reporter, and Explorer for CPM if the browser was not previously set.

1. In Websense Enterprise Manager, select **Help > Select Web Browser**. A navigation tool opens that helps locate the Web browser you want to use.
2. When you are done identifying the Web browser, you can open help, CPM Reporter, or Explorer for CPM.

Viewing Summary Data

The **Desktop** tab of the **Summary Data** pane provides summary information for Client Policy Manager, and is the first pane you see when you log on to Websense Enterprise Manager and access Client Policy Manager functions. Click **More Info** to access details for the associated selection.



Summary Data Pane

The **Summary Data** pane shows the following information:

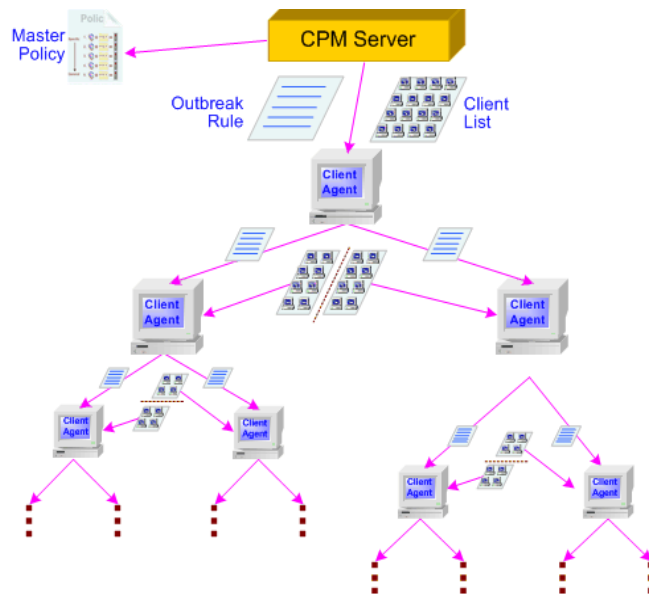
- ◆ **Clients not installed:** The total number of machines on the network that do not include a Client Agent installation. If you click **More Info**, the **Client Status** pane opens and shows a list of these machines. For additional information, refer to [Chapter 7: Working with Client Status](#), page 141.
- ◆ **Not Responding:** Client Agent is installed, and the machine is currently on the network, but CPM Server is not receiving data from that Client Agent. If you click **More Info**, the **Client Status** pane opens and shows a list of these machines. For additional information, refer to [Chapter 7: Working with Client Status](#), page 141.
- ◆ **Active Websense clients:** The number of machines that include a functioning Client Agent installation and are logged on to the network. If you click **More Info**, the **Client Status** pane opens and shows a list of these machines. For additional information, refer to [Chapter 7: Working with Client Status](#), page 141.
- ◆ **Executable launches blocked in the last 24 hours:** A running count of the executables Client Policy Manager blocked during the most recent 24-hour period.
- ◆ **Network Lockdown Blocks in the last 24 hours:** A count of how many times a network block occurred during the last 24 hours.
- ◆ **Express Lockdown:** The Express Lockdown feature allows system administrators to prevent the execution of any code that is not currently installed on a machine *without* requiring an inventory of that machine first. For additional information, refer to [Express Lockdown](#), page 180.
- ◆ **Removable Media Lockdown:** The Removable Media Lockdown feature allows system administrators to prevent all media, or just writable media, from mounting on client workstations. For additional information, refer to [Removable Media Lockdown](#), page 185.

Emergency Outbreak Rule Processing

The CPM Emergency Outbreak Rule lets you stop viruses and other malicious executables within seconds of entering file names into the rule. This ability allows you to protect your network machines more quickly than anti-virus organizations can add the data to their block lists and download the information to their customers.

Although the Policy Server includes the **Outbreak** list in CPM policy, it does not appear in the **Rules** pane. When you enter an executable name into the **Outbreak** list, it immediately triggers system-wide notification in a matter of seconds, and inserts a new entry into the CPM policy.

The process uses peer-to-peer communications between machines running Client Agent. This method of communication provides nearly instantaneous protection against viruses and other malicious code. If your network policy does not permit peer-to-peer communication between client machines, you may disable the distribution port that clients use for Outbreak communication. Refer to *Disabling Client Outbreak Distribution*, page 123 for instructions.



Emergency Outbreak Rule and Peer-to-Peer Communication

When you add an entry to the **Outbreak** list, Websense processes the data in the most expedient way possible. The chain of events is:

1. The system administrator enters the file name of the virus or malicious executable in the **Outbreak** dialog box to add it to the Emergency Outbreak Rule. The **Outbreak** dialog box may contain any number of file names. CPM Server inserts the entry into the policy.
2. CPM Server waits for the first Client Agent on a subnet to send heartbeat data to CPM Server. A subnet is a portion of a network that shares a common address component. For example, all devices with IP addresses that start with **10.10.2.** are part of the same subnet.

Once the first Client Agent sends the heartbeat data, CPM Server gives that machine the Emergency Outbreak Rule, and the IP address and port number for the other client machines on that subnet.

3. Client Agent applies the Emergency Outbreak Rule at the local machine, contacts the first two machines in the list of client machines, and sends them the Emergency Outbreak Rule, and half the list of other client machines on the subnet.
4. Each Client Agent repeats the process until machines connected to the subnet and running Client Agent have received the **Outbreak** list.
5. If a client machine is not available at the time the **Outbreak** list is distributed, one of two things may occur:
 - The client machine that is trying to distribute the Outbreak list places the unavailable client machine at the bottom of the client list and passes the new version of the rule to the next available client machine. This process continues until all machines connected to the network and running Client Agent have received the Emergency Outbreak Rule.
 - The next time the previously unavailable client machine sends heartbeat data to CPM Server, CPM Server sends the new version of the policy, which includes the new Emergency Outbreak Rule, to that machine.
6. If the file name is not in the Websense Enterprise Master Database, and AppCatcher is enabled, the file name appears in any executable lists submitted to Websense, Inc. When Websense, Inc. receives the data, staff research the executable, and identify a category that best matches the intended use. The new information appears in the Websense Enterprise Master Database and is available to all CPM subscribers. For information about enabling AppCatcher, read *Introducing AppCatcher*, page 83.

This method of dividing information and sending it to Client Agent speeds distribution of the Outbreak rule, and reduces the potential of viral attacks. Depending on the heartbeat setting for Client Agent, the **Outbreak** list can be distributed across your entire network within seconds of the data being available to CPM Server.

**NOTE**

You may experience temporary slowdowns on your network during distribution of the **Outbreak** list. Given the destructive nature of viruses, however, slowdowns may be preferable to the problems a virus can cause.

Websense, Inc. includes a list of executables that you cannot add to the Emergency Outbreak Rule. The executables included in the list are those associated with critical functions that could cause system failure if blocked. For example, an administrator cannot enter **krnl386.exe**, an operating system executable, because that entry would cause company-wide downtime.

Adding an Emergency Outbreak Rule Entry

You can add file names to the Emergency Outbreak Rule at any time. The distribution function, described in [Emergency Outbreak Rule Processing, page 118](#), makes sure that machines connected to the network and running Client Agent are protected against a known virus within a matter of seconds.

For example, you are driving to work and listening to the radio. The announcer mentions that a new virus, `badvirus.exe`, is rapidly infecting systems around the world.

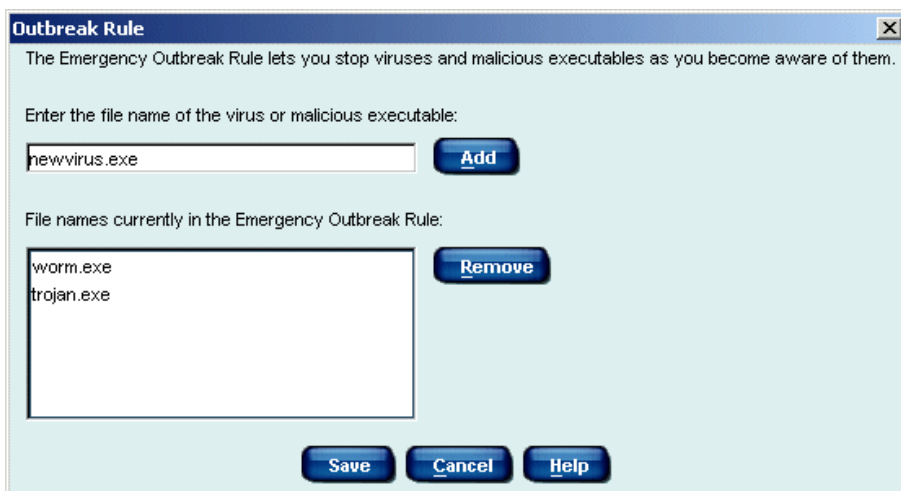
When you get to work, you open the **Summary Data** pane. You click **Outbreak**, enter the file name `badvirus.exe`, and then save the data. CPM Server begins processing the list as soon as the **Outbreak** dialog box closes. Within seconds, all machines that are connected to the network and running Client Agent receive the Outbreak list and are protected from `badvirus.exe`.

Later that same morning, Susie in Purchasing receives an email and attempts to open the attached file. Client Agent recognizes `badvirus.exe` and presents a block message instead of allowing the executable to run.

To add an outbreak entry:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Summary Data** in the navigation pane to access the **Summary Data** pane.
3. Click **Update Outbreak Rule** to open the **Outbreak** dialog box.

The list shows any existing file names in the Outbreak rule.



Outbreak Dialog Box

4. Enter the file name in the text field, and then click **Add**.



IMPORTANT

If you enter a file name that Websense, Inc. identifies as an application with a critical function, an error message appears, and your entry will not appear in the Outbreak list.

5. Click **Save** to save your entry and close the dialog box.

Removing an Emergency Outbreak Rule Entry

You can remove entries from the Emergency Outbreak Rule at any time. This lets you keep your list up-to-date and retain only necessary entries.

For example, you normally run anti-virus software. Because you know it takes a period of time for companies in the anti-virus marketplace to update and release new virus databases, you entered `badvirus.exe` in the **Outbreak** dialog box when you first heard about it. Several weeks have passed, and you notice that `badvirus.exe` is now included in the virus database provided by your anti-virus software publisher. You remove the file name from the **Outbreak** dialog box because it is no longer needed.

To remove an Emergency Outbreak Rule entry:

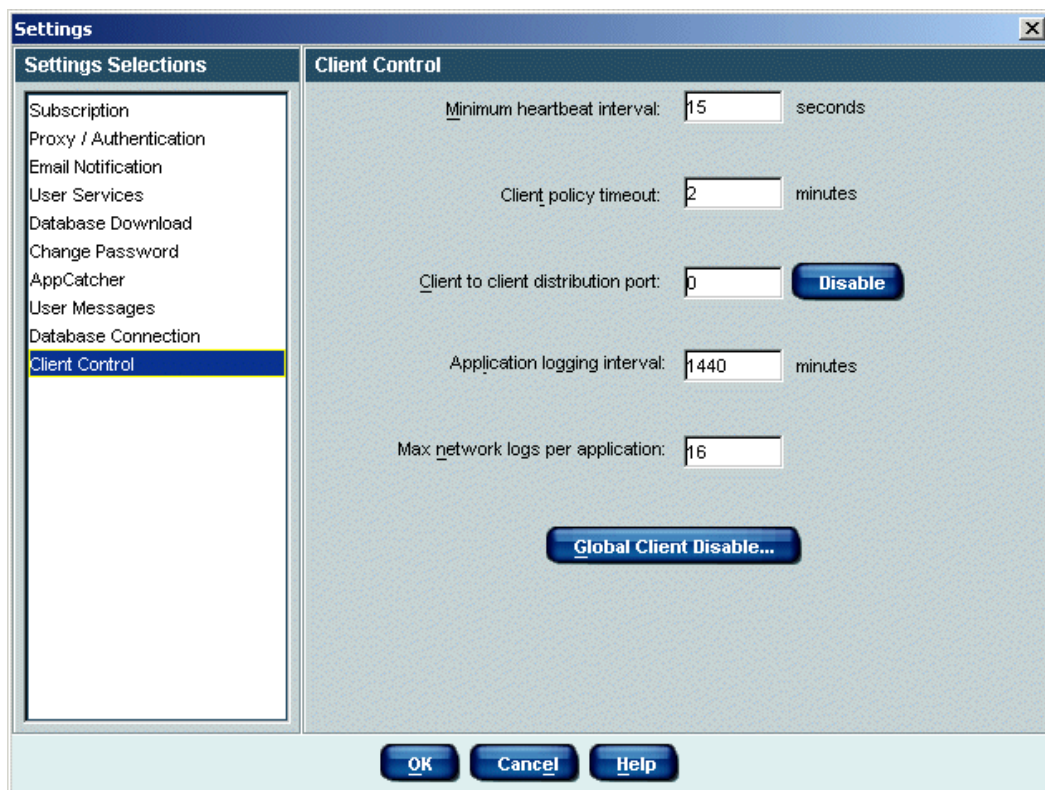
1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Summary Data** in the navigation pane to access the **Summary Data** pane.
3. Click **Update Outbreak Rule** to open the **Outbreak Rule** dialog box. The list shows the file names currently in the Outbreak Rule.
4. Select the file name you want to remove, and then click **Remove**.
5. Click **Save** to close the dialog box and return to the **Summary Data** pane.

Disabling Client Outbreak Distribution

The CPM administrator has the ability to disable client-to-client communication by closing the distribution port used by the clients to communicate with one another. This setting disables the peer-to-peer Outbreak communication between clients, but does not prevent the Policy Server from passing Outbreak information to the client through a policy update.

To disable the client-to-client distribution port used for Outbreak communication:

1. Open the Websense Enterprise Manager and connect to the Policy Server.
2. Select **Server > Settings**.
3. In the Settings dialog box, select **Client Control** from the navigation pane.



Client Control Dialog Box

4. Click **Disable** next to the **Client to client distribution port** field.
A pop-up dialog box asks you if you want to disable Outbreak.

5. Click **Yes**.

Outbreak is disabled, and the distribution port field turns gray.

To enable the distribution port again, open the Client Control dialog box and click **Enable**.

Desktop Lockdown Suite

The Desktop Lockdown Suite consists of two enhanced security features.

- ◆ **Express Lockdown**—allows system administrators to block executables *without* requiring an inventory of that machine first. For details, refer to [Express Lockdown](#), page 180.
- ◆ **Removable Media Lockdown**—allows system administrators to prevent removable devices such as flash drives, CD/DVD burners, floppy drives, and external hard drives from being mounted on client workstations. For details, refer to [Removable Media Lockdown](#), page 185.

Click **Configure** to configure the feature in the Policy screen.

Deploying Client Agent

There are four ways to deploy, install, or uninstall Client Agent. Each method has advantages and disadvantages, often dependant on the knowledge level of the administrator. The four installation options are:

- ◆ In Websense Enterprise Manager, select the **Deployment Status** pane. This allows administrators to deploy Client Agent to networked machines. For details, refer to [Managing Client Options](#), page 134. This is the easiest way to deploy Client Agent and to track deployment progress.
- ◆ Use scripts to deploy Client Agent. For information, read *Chapter 6: Deploying Client Agent via Scripts* in the *Websense Enterprise Client Policy Manager Installation Guide*. This is the most robust way to deploy Client Agent, but requires some understanding of script development.
- ◆ Manually install a single copy of Client Agent at a local machine using Websense setup files. This installation method is relatively easy, but is generally of use in a small organization or test environment. For details, refer to Chapter 6 in the *Websense Enterprise Client Policy Manager Installation Guide*.
- ◆ Use third-party applications to deploy Client Agent. Read the third-party documentation for information. This is useful for organizations that often deploy software using third-party tools. Generally, this option is useful only if you have experience using such tools.

Potentially, an organization may use a combination of methods to manage Client Agent deployment. For example, John is an experienced system administrator. He uses the **Deployment Status** pane in Websense Enterprise Manager to manage the initial agent deployment, but wants to automate potential upgrades or new installations using scripts. By leveraging these two options, John can rapidly set up his Websense system from Websense Enterprise Manager, and then later take the time to create scripts that automate the update process.

The next table provides a quick reference of the advantages and disadvantages of the available deployment options.

Considerations for use >						
Deployment Method v	Mass Deployments	Single Deployment	Deployment Service	Scripting Required	Automated updates	Deployment Status
Client Deployment Service with Websense Enterprise Manager	X	X	X			X
Manual deployment using Websense files		X				
Client Deployment Service with custom or third-party login scripts		X	X	X	X	X
Custom or third-party login scripts						
Third-party deployment software	X	X	X	X		

If you use scripts or third-party deployment software, requirements are dependant on the method you select.

In the above table:

- ◆ *Mass deployment* indicates that numerous machines may be included in the deployment process.
- ◆ *Single deployment indicates* that one machine at a time may be impacted by the deployment process.
- ◆ *Deployment Service* indicates that Client Deployment Service is required. For third-party options, this requirement is script- or application-dependant.
- ◆ *Scripting Required* indicates that advanced scripting knowledge is recommended. If you do not have scripting experience, Websense, Inc. recommends calling someone who does or using some other deployment option. For third-party options, this requirement is application-dependant.
- ◆ *Automated updates* indicates that processes can be set to check version data and update the agent.

- ◆ *Deployment Status* indicates that tracking of the deployment process is available in the Websense Enterprise Manager **Deployment Status** pane. The status shows active processes and/or anticipated schedules. For details, refer to [Accessing the Deployment Status Pane](#), page 132.

Client Agent Requirements

You must install Client Agent on machines you want to inventory and/or control. The agent is responsible for processing inventory at the machine where it is installed, for applying CPM policies, and for all communications with CPM Server.

The Client Agent is backwardly compatible, in that a v5.5 client will still get policies from a v5.5.2 CPM Server; however, new features will not be available to the earlier version Client Agent.



WARNING

Do not install Client Agent on:

- ◆ Machines running Windows 2000, Service Pack 2 or lower.
 - ◆ Machine or machines where you installed CPM Server or CPM Reporter/Explorer for CPM.
-

Client Agent is supported on the following operating systems:

- ◆ Microsoft Windows 2000 Professional with Service Pack 3 or Service Pack 4
- ◆ Microsoft Windows 2000 Server with Service Pack 3 or Service Pack 4
- ◆ Microsoft Windows 2000 Advanced Server with Service Pack 3 or Service Pack 4
- ◆ Microsoft Windows NT 4.0 Workstation with Service Pack 6a
- ◆ Microsoft Windows NT 4.0 Server with Service Pack 6a
- ◆ Microsoft Windows XP Professional with Service Pack 1 or Service Pack 2
- ◆ Microsoft Windows Server 2003

Other minimum Client Agent requirements are:

- ◆ **Processor:** Pentium III 500 MHz
- ◆ **Disk Space:** 25 MB for installation; 15 MB to run the application
- ◆ **Memory:** 64 MB RAM, 128 MB pagefile
- ◆ File and Printer sharing must be enabled at the client machine to use the CPM Deployment Service.

Deploying Client Agent for Windows XP

Installing Windows XP with Service Pack 2 may disable File and Printer Sharing services. This blocks CPM from deploying clients via Client Deployment Service (CDS).

Have your system administrator enable File and Printer Sharing services:

1. Go to the **Advanced** tab of the properties of a connection and click **Settings** to launch the new Windows Firewall control panel.
2. Go to the **Exceptions** tab.
3. Check the **File and Printer Sharing** box to enable file and printer sharing services, and then click **OK**.

The XP firewall settings will no longer impact CPM, and Client Agent can be deployed via Client Deployment Service.

Repeat this procedure to turn on File and Printer Sharing services for each client machine.

Upgrading Client Agent v5.2 to v5.5.2

If you are upgrading Client Agent from v5.2 to v5.5.2, users at the machines where Client Agent v5.5.2 has been installed need to reboot those machines for optimal functionality of the Client Agent. If users fail to reboot their machines, they may encounter situations where applications that use socket connections may fail. By default, the restart message appears to users.

VPN Support

The deployment of Client Agent is *not* supported over a VPN connection; however, you can update policies, perform inventories, and apply lockdowns with the Client Agent through the following VPN clients:

- ◆ Microsoft L2TP/IPSec VPN Client

- ◆ Check Point VPN-1 SecureClient
- ◆ Cisco VPN Client v4.6

**NOTE**

After Installing Client Agent on a machine running Check Point VPN-1, you must restart the machine before Client Agent can function.

Deploying Clients: The Process

When you are ready to deploy clients, you can configure and monitor the process from Websense Enterprise Manager, using the following process:

1. Access the **Deployment Status** pane. For details, refer to [Accessing the Deployment Status Pane, page 132](#).
2. Identify a machine or a group of machines to which you want to deploy Client Agent. For details, refer to [Deploying or Uninstalling Client Agent, page 135](#).
3. Set the **Deployment Status** pane to the domain you want to monitor and set the **Current view** field to *Deployment status*. For details, refer to [Deploying or Uninstalling Client Agent, page 135](#).

You can refresh data as often as you wish. CPM Server updates the list once every 60 seconds. For details, refer to [Refreshing Deployment Data, page 138](#).

Accessing the Deployment Status Pane

When you first open the **Deployment Status** pane, the list shows all deployment related details for machines. You can view information for all domains or by a specific domain, and by deployment status. For example, you can view all machines in the Finance domain where a deployment action is pending, or machines in the Purchasing domain where Client Agent is not yet installed.



IMPORTANT

If you need to uninstall and then reinstall Client Agent, make sure Windows Service Control Manager (SCM) is closed at the machine where activity is to occur. If SCM is open during the uninstall process, you will not be able to start Client Agent. For more information, refer to *Microsoft Knowledge Base Article #287516*.

To access the **Deployment Status** pane:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Deployment Status** in the navigation pane to access the **Deployment Status** pane.

The screenshot shows the Websense Enterprise Manager interface. The main content area is divided into several sections:

- Deployment Summary:**

Scheduled:	0
Retrying:	0
Failed:	0
Succeeded:	3
- Uninstall Summary:**

Scheduled:	0
Retrying:	0
Failed:	0
Succeeded:	0
- Deployment Status:**

Domain: All | Current View: All | Refresh

Domain	Machine ...	Asset Tag	Status	Client Version	Install Date
SDSD	WS-MACHINE01				
TEST	WS-MACHINE01				
WORKGROUP	WS-MACHINE01				
DEV1	WS-MACHINE01				
QA	WS-KMTEST				
SDSD	WS-KMTEST				
TEMP	WS-KMTEST				
TEST	WS-KMTEST				
WORKGROUP	WS-KMTEST				
DEV1	WS-KMTEST				
QA	WS-KENSQL				
SDSD	WS-KENSQL				
WORKGROUP	WS-KENSQL				
TEMP	WS-KENSQL				
TEST	WS-KENSQL				
DEV1	WS-KENSQL				
QA	WS-JWANG3				
ARBEITSGRUPPE	WS-JWANG3				
TEMP	WS-JWANG3				
QUALITY.COM	WS-JWANG3				

Check the Event Viewer on the CPM Deployment Service machine for deployment error details.
- Deployment Actions:**

Deployment Options... | Cancel Deployment / Uninstall

At the bottom of the window, it shows "1644 workstation(s)" and "All clients updated."

Deployment Status Pane

3. Select a domain from **Domain** drop-down list. The default setting is **All**.
4. Select the appropriate machine status from the **Current View** drop-down list. Your choices are:
 - **All**—all machines that Websense Enterprise Manager recognizes.
 - **Installed**—machines where Client Agent is installed.
 - **Not Installed**—machines where Client Agent is not installed.
 - **Deployment status**—status of the deployment process at machines affected by a deployment option.

- **Uninstall status**—status of any uninstall processes at machines that are affected by such processes.

The **Deployment Status** pane shows the machines whose status matches your entry in the filter fields. Information is available only for machines where deployment or uninstall processes have been scheduled using the **Deployment Status** pane or scripts.

Each row in the pane identifies one machine, and provides the following information:

- ◆ **Domain Name**—network domain on the client machine
- ◆ **Machine Name**—client machine name. This may be a server, a laptop, a desktop system, or any other machine
- ◆ **Asset Tag**—user-defined asset tag name for the machine, if any
- ◆ **Status**—current status of the machine
- ◆ **Client Version**—current version of Client Agent installed at the associated machine
- ◆ **Install Date**—date when the current version of Client Agent was installed at the associated machine

The information in the **Deployment Status** pane reflects actual situations at machines that are in the list. For example, if you set the **Current View** field to **Deployment Status**, only machines where Client Agent is being deployed appear in the **Deployment Status** list. If you set the field to **Not installed**, only machines that do not have Client Agent installed appear.

Managing Client Options

If you include the Websense Client Deployment Service component during installation, Websense Enterprise Manager allows you to install, repair, upgrade, or remove Client Agent from a single location, without using scripts or third-party tools. These functions allow you to maintain your Client Policy Manager system with a minimum of effort.

Details for the Client Deployment Service are available in the following locations:

- ◆ Check Release Notes at <http://ww2.websense.com/global/en/SupportAndKB/> for the latest information.
- ◆ For installation details, check *Chapter 3: Installing Policy Manager* in the *Websense Enterprise Client Policy Manager Installation Guide*.

- ◆ For deploying Client Agent using scripts, read *Chapter 6: Deploying Client Agent via Scripts* in the *Websense Enterprise Client Policy Manager Installation Guide*.

When you deploy Client Agent using Websense Enterprise Manager, client installation selections respond as follows:

- ◆ **Deploy**

- If you select **Deploy**, and there is not a current version of Client Agent at a machine, the process installs Client Agent.
- If you select **Deploy**, and there is a current version of Client Agent at a machine, the process repairs the existing Client Agent.

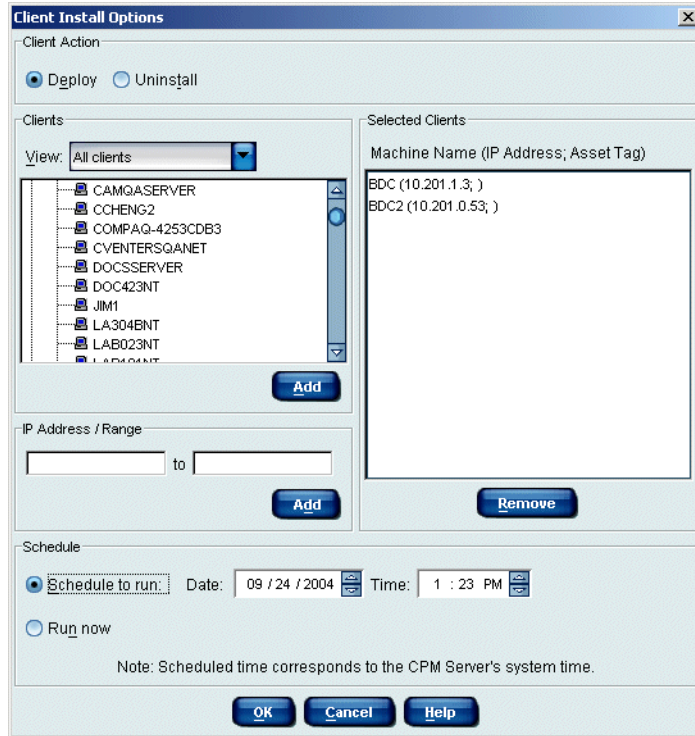
- ◆ **Uninstall**

If you select **Uninstall**, and there is a current version of Client Agent at a machine, the process removes the Client Agent.

Deploying or Uninstalling Client Agent

To deploy or uninstall Client Agent using Websense Enterprise Manager:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Deployment Status** in the navigation pane to access the **Deployment Status** pane.
3. Click **Deployment Options** to open the **Client Install Options** dialog box.



Client Install Options Dialog Box

4. Select either **Deploy** or **Uninstall**. Only one option may be set at a time. If you change this setting later, any selections you may have made in the meantime are dropped.



NOTE

Generally, Websense, Inc. does not recommend uninstalling and then reinstalling Client Agent. It is better to deploy the agent and let the deployment process upgrade or repair the agent. For more information, read *Chapter 9: Troubleshooting in the Websense Enterprise Client Policy Manager Installation Guide*.

5. Click in the **View** field, and then select one of the following:

- Select **All Clients** to see all machines that are connected to the network.
- Select **Clients not installed** to see only those machines where Client Agent has not been installed.
- Select **Clients installed** to see only those machines where Client Agent is installed.
- Select **Clients active** to see only those machines where Client Agent is currently running and communicating with CPM Server.
- Select **Clients not responding** to see only those machines where clients are installed but are not communicating with CPM Server.
- Select **Clients disconnected** to see only those machines where Client Agent has been installed, but the machines are not currently on the network.

6. Add client machines using one of the following methods:

- Scroll through the **Clients** list, select the domain you want to include, and then click **Add**. If you add a folder, all domains in the folder are automatically included. If you add a single domain, only that domain is included. In either case, only machines that meet the criteria in the **Client Action** area are affected.
- Enter a single IP address in the first **IP Address/Range** field, and then click **Add** to add a single machine to the list.
- Enter the starting and ending IP addresses of a range of IP address in the **IP Address/Range** fields, and then click **Add**. The starting IP address must be a smaller number than the ending IP address. For example, **10.10.2.1** to **10.10.2.20** is a valid entry, while **10.10.2.20** to **10.10.2.1** is not.



WARNING

Do **not** install Client Agent on the machine or machines where you have installed CPM Server or CPM Reporter. If you do, you may encounter serious operational problems with CPM functions.

7. Decide how you want Websense to manage the action you select:

- **By Schedule:** The selected action occurs once, based on these settings.
 - a. Click **Schedule to run** to activate the scheduling option.

- b. Select the start date in the **Date** field.
- c. Select the start time in the **Time** field.

CPM Server provides the timestamp, not the client machines.

- **Run now:** The action you selected begins processing as soon as you click **Run now**, and close the **Client Install Options** dialog box.
8. Click **OK** to submit the action for processing.



NOTE

When Client Agent is deployed to a machine, the employee receives a pop-up window. The message tells the employee that the network administrator has deployed new software, and the machine must be restarted. The employee can choose to restart the machine immediately or restart at a later time.

Refreshing Deployment Data

The **Deployment Status** pane updates automatically every 60 seconds when it is open. This process checks the current status of any deployment operations, and then inserts the details into the **Deployment Status** pane. If you want to monitor deployment progress more closely, use the **Refresh** button near the top of the pane:

- ◆ Click **Refresh**. New status data appears in the **Deployment Status** pane.

Removing Clients From the Selected Clients List

You can remove clients from the **Selected Clients** list if you accidentally include them, and have not yet sent your deployment request. When you remove clients from the list, Websense Enterprise Manager will not include that machine in any deployment action that is being set:

1. Scroll through the **Selected Clients** list and select the client or clients you want to remove.
2. Click **Remove** to delete the client or clients from the list.

Canceling Client Agent Deployment

You can cancel a scheduled deployment action whenever necessary, and the list may include both install and uninstall processes. If a process has already been started at a machine, this option will not work.

For example, four machines in the Deployment Status list are scheduled for upgrades, and one is currently uninstalling Client Agent. If you select these five machines and click **Cancel Deployment/Uninstall**, Websense Enterprise Manager cancels the four upgrades, but cannot cancel the uninstall process that has already started.

To cancel a deployment action:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Deployment Status** in the navigation pane to access the **Deployment Status** pane.
3. Make selections in the **Domain** and **Current View** fields to list machines that meet your criteria.
4. Select the machines to be included in the cancellation, and then click **Cancel Deployment/ Uninstall**. A confirmation message appears.
5. Click **Yes** to cancel the installation action.

Working with Client Status

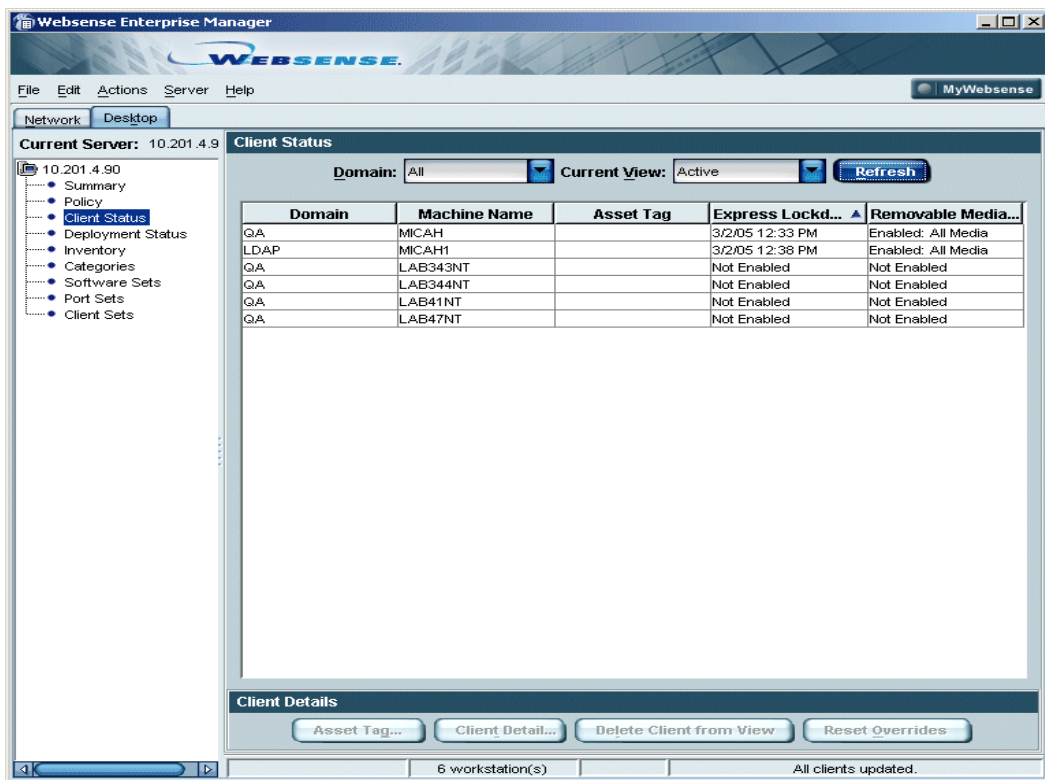
The **Client Status** pane provides information about the operating status of machines on your network. You can check the status and basic installation details for Client Agent.

The pane also allows you to add asset tag information for any machine. Asset tags provide a way to customize machine identification, and are often used to provide critical details in an easy-to-access format.

Accessing the Client Status Pane

When you first open the **Client Status** pane, the list shows all machines in all domains that are connected to the network and running Client Agent. You can sort information for specific domains, by specific client status. For example, you can view all machines where Client Agent is installed but is not responding, or all machines in the Finance domain that are disconnected from the network. To access the **Client Status** pane:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Client Status** in the navigation pane to access the **Client Status** pane.



Client Status Pane

3. Select a domain from the **Domain** drop-down list. The default setting is **All**.
4. Select the appropriate machine status from the **Current View** drop-down list:
 - **Active**. Client Agent is installed and operational, and is communicating with CPM Server normally.
 - **Not Responding**. Client Agent is installed, and the machine is currently on the network, but CPM Server is not receiving data from that client.
 - **Disconnected**. Client Agent is installed, but is not communicating with CPM Server, and the machine is not currently on the network. Disconnected machines can include remote machines, laptops, machines undergoing maintenance, and machines that are turned off.

Each row in the pane identifies one machine, and provides the following information:

- **Domain Name.** Shows the network domain for the client machine.
- **Machine Name.** Shows the client machine name.
- **Asset Tag.** Shows the user-defined asset tag name for the machine

Once you make selections in the fields, the **Client Status** pane shows machines that match the parameters you chose.

Managing Asset Tags

Asset tags provide an optional way to identify machines in addition to the IP address and the machine name. The **Asset Tag** dialog box includes fields that are assigned default values, such as an asset tag name, and primary user, and other fields you can customize.

The asset tag provides a central depository for important information that is readily available and easy to access. This can be extremely valuable for groups including Information Technology, Asset Management, and Help Desks. The information is viewable only in the **Edit Asset Tag** dialog box.

Custom information that may be of value includes:

- ◆ The machine's serial number
- ◆ A corporate asset number
- ◆ The machine type—for example, laptop, server, or workstation
- ◆ The manufacturer's name and model type
- ◆ Department identification
- ◆ Physical location
- ◆ Any information that is meaningful for your company

Asset Tag:	4-909-0098
Machine Name:	DOC423NT
Primary User:	Engineering
Department:	Technical Communications
Location:	Fourth Floor
User-Defined Fields	
Vendor	: HP
Maintenance	: ext 2000
Last upgrade	: 03/16/2004
Next upgrade	: add memory
	:
Comments:	256 mb, used only for document reviews by engineers

Asset Tag Dialog Box

Adding an Asset Tag

You can add an asset tag when you are in the **Client Status** pane or **Client Details** dialog box. All entries are optional.

To add an asset tag:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Client Status** in the navigation pane to access the **Client Status** pane.
3. Define what you want to see:
 - Select a domain from the **Domain** drop-down list. The default setting is **All**. The **Client Status** pane shows customer-specific machine information and status.
 - Select the appropriate machine status from the **Current View** drop-down list. Your choices are **Active**, **Not Responding**, and **Disconnected**.

4. Locate the machine name you want to add an asset tag for, and then click **Asset Tag**, or right-click and select **Asset Tag** from the shortcut menu. The **Asset Tag** dialog box opens. If you prefer, you can access the **Asset Tag** dialog box from the **Client Detail** dialog box. Read *Viewing Client Detail*, page 147, for details.
5. Enter data for the asset tag. All entries are optional:
 - Enter a name in the **Asset tag name** field to identify the asset tag. The entry may be between 4 and 64 alphanumeric characters in length.
 - Websense Enterprise Manager populates the **Machine Name** field using information it collects when Client Agent submits information during startup. You cannot change this value.
 - Enter the name of the primary user in the **Primary user** field.
 - Enter the department with which the machine is associated.
 - Enter a location that identifies where the machine is physically located.
 - Enter up to five custom definitions. The field on the left becomes the label for the field on the right. For example, enter the text **Serial Number** in the left field, and then enter the actual serial number in the field at the right. Other possibilities include maintenance dates, vendor information, corporate asset numbers, and so forth.
 - Enter any comments in the **Comments** field. For example, your comment includes purchase and maintenance contract data.
6. Click **OK** to save your entry and return to your starting point.

Editing an Asset Tag

You can edit an asset tag to reflect changes when necessary. Entries can be overwritten at any time.

To edit an asset tag:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Client Status** in the navigation pane to access the **Client Status** pane.
3. Define what you want to see:
 - Select a domain from the **Domain** drop-down list. The default setting is **All**. The **Client Status** pane shows customer-specific machine information and status.

- Select the appropriate machine status from the **Current View** drop-down list. Your choices are **Active**, **Not Responding**, and **Disconnected**.
4. Locate the machine name associated with the asset tag you want to modify, and then click **Asset Tag**. You can right-click and select **Asset Tag** from the shortcut menu if you prefer. The **Asset Tag** dialog box opens.
 5. Make any necessary edits in the appropriate fields.
 6. Click **OK** to save your entry and return to your starting point.

Clearing an Asset Tag

To clear data in an asset tag:

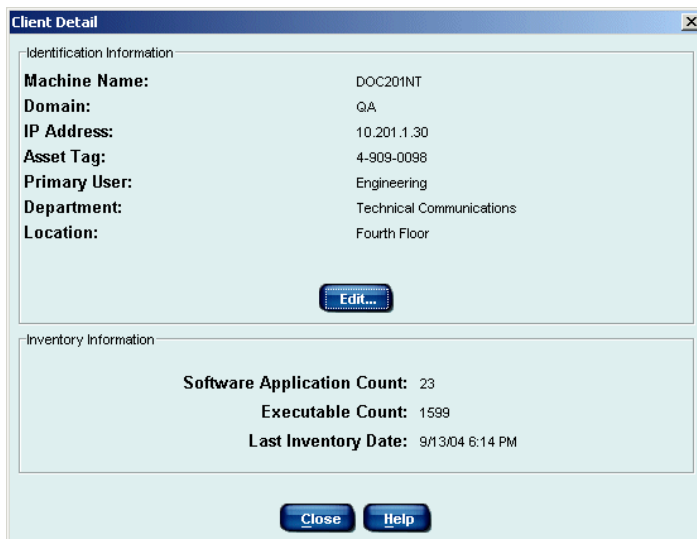
1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Client Status** in the navigation pane to access the **Client Status** pane.
3. Define what you want to see:
 - Select a domain from the **Domain** drop-down list. The default setting is **All**. The **Client Status** pane shows customer-specific machine information and status.
 - Select the appropriate machine status from the **Current View** drop-down list. Your choices are **Active**, **Not Responding**, and **Disconnected**.
4. Locate the machine name associated with the asset tag you want to modify, and then click **Asset Tag**. You can right-click and select **Asset Tag** from the shortcut menu if you prefer. The **Asset Tag** dialog box opens.
5. Highlight all text in a field, and then click the **Delete** key on your keyboard.
6. Continue deleting text in the remaining fields.
7. Click **OK** to save the changes. From now on, the **Asset Tag** column in the **Client Status** pane will be blank for the selected machine.

Viewing Client Detail

You can view machine details in the **Client Detail** dialog box. This shows critical information for one machine.

To view the status of your client:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Client Status** in the navigation pane to access the **Client Status** pane.
3. Define what you want to see:
 - Select a domain from the **Domain** drop-down list. The default setting is **All**. The **Client Status** pane shows customer-specific machine information and status.
 - Select the appropriate machine status from the **Current View** drop-down list. Your choices are **Active**, **Not Responding**, and **Disconnected**.
4. Locate the machine name you want details about, and then click **Client Detail**, or right-click and then select **Client Detail** from the shortcut menu. The **Client Detail** dialog box opens.



Client Detail Dialog Box

Machine information includes the following details:

- Machine name
- Domain
- IP address
- Custom details

If an asset tag has been created for the machine, the following information may appear:

- Asset tag name: You can add or edit the asset tag by clicking the associated button. If you have not defined an asset tag for the machine, there is no entry. For specifics, read *Managing Asset Tags*, page 143.
 - Primary user: If you have not identified a primary user for the machine, there is no entry.
 - Department: If you have not identified a department that “owns” the machine, there is no entry.
 - Location: If you have not identified a location for the machine, there is no entry.
- Number of software applications found during the most recent inventory. If an inventory for the machine is not available, text indicates this.
 - Number of executables found during the most recent inventory. If an inventory for the machine is not available, text indicates this.
 - Date when the most recent inventory occurred. If inventory has not been taken, a message indicates this.
5. When you are done viewing details, click **Close** to close the **Client Detail** dialog box.

Deleting Clients From the Client Status Pane

If machines are disconnected or not responding, you can remove these machines from the **Client Status** pane. By removing machines that are not currently active, you can more easily review active machines that are of interest to you, and reduce the amount of scrolling necessary during operations.

To delete disconnected or non-responsive clients from the pane:

1. In Websense Enterprise Manager, click the **Desktop** tab.

2. Select **Client Status** in the navigation pane to access the **Client Status** pane.
3. Click **Delete Client from View** to remove all disconnected and/or non-responsive clients from the **Client Status** pane. A confirmation message opens.
4. Click **OK** to remove the clients from the **Client Status** pane.

Resetting Overrides

When you configure block and continue messages, Websense Enterprise Manager allows you to define user overrides, as described in [Controlling User Overrides](#), page 93. When user overrides are set, it creates a **Remember my selection** option for user messages. If the option is enabled, employees can decide whether they want to be notified each time they try to launch a specific controlled executable, or if Client Agent remembers what the employee chose to do the last time they attempted the launch.

For example, you include the **Remember my selection** option for both block and continue messages. Sabrina tries to launch Microsoft Photo Editor, which the company has set to Continue, as they are concerned that employees may be wasting time when using the application. When Sabrina first receives the continue message, she activates the **Remember my selection** option, and then clicks **Block** to stop the launch. From this time on, whenever Sabrina tries to launch Microsoft Photo Editor, Client Agent automatically blocks it, but does not display the block message.

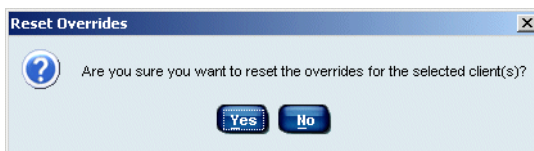
Some time later, Sabrina has a business need for Microsoft Photo Editor. Since she activated the **Remember my selection** option and blocked the software, she cannot change her setting.

Only system administrators with access to Websense Enterprise Manager can easily reset this option. When a system administrator resets overrides, the impacted Client Agent restores the original message parameters. When the system administrator makes this change, the override impacts all applications at that machine.

Using the same example as above, Sabrina calls the system administrator and explains that she needs to use Microsoft Photo Editor for business but can no longer access it. The system administrator resets the override, which causes Client Agent to again present block and continue messages, regardless of Sabrina's earlier settings for the **Remember my selection** option.

To override employee settings at a specific machine:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Client Status** in the navigation pane to access the **Client Status** pane.
3. Select the client machine that you want to reset overrides for. Click **Reset Overrides** at the bottom of the pane, or right-click and select **Reset Overrides** from the shortcut menu.
4. A confirmation message appears. Click **Yes** to reset the override data for that machine.



Reset Override dialog box

For more information about the **Remember my selection** feature, read:

- ◆ [Controlling User Overrides, page 93](#)
- ◆ [Employee Interaction with Messages, page 95](#)

Working with Inventories

The **Inventory Status** pane provides options for collecting information for Client Policy Manager. You define how you want inventories to collect data: immediately, once at a predefined time, or on an ongoing basis.

During an inventory, Client Agent collects information about the following:

- ◆ Installed executables. The inventory may be used to create lockdowns, described in *Chapter 9: Applying Lockdowns*. The inventory can also be used to generate a software set for the machine where the inventory originated, as described in *Generating Software Sets from Inventories*, page 164.
- ◆ Installed applications and hardware.

For CPM Reporter, inventories populate some of the pages that allow you to configure reports. CPM Reporter is fully populated with data only when machines that are running Client Agent have been inventoried.

Understanding Inventories

When you run an inventory, Client Agent searches the specified machines for installed executables, applications, and hardware. The inventory process can run immediately, or can be scheduled for a future time and/or date.

The process takes lower precedence than machine and/or user operations, which reduces any potential impact at the machine where the inventory is running. During an inventory, it is not uncommon to see CPU usage at 20% to 100%, with higher usage occurring only if other processes are not active.

The time it takes to run an inventory depends on the following machine attributes:

- ◆ Processing speed of the machine
- ◆ Size of the client machine's drives
- ◆ Number of drives included in the inventory
- ◆ Number of files on the inventoried drives

As a result, processing times may vary widely.

Generally, Websense, Inc. recommends running inventories after business hours to ensure that the process does not impact day-to-day operations. If employees normally shut machines off at the end of the work day, you may need to send notification that their machines must remain on for this process to occur.



WARNING

If machines in your system are in Standby mode, the operating system at the client machine will determine whether or not the inventory will run. If the Standby mode at a machine allows systems operations to occur, the inventory will be able to run. However, if Standby mode at the client machine does not support system operations, the inventory will generate an error message.

When inventory is complete, Client Agent sends the details to CPM Server, which then saves executable and application data to the Websense Enterprise Master Database and saves all inventory information to the CPM Inventory Database.

If AppCatcher is enabled, information about unrecognized executables and applications is uploaded to Websense, Inc. for review. When the software is identified, details are inserted into the default Websense Enterprise Master Database, and are included in any download to your system. For information about the AppCatcher process, read [Introducing AppCatcher, page 83](#). For details about scheduling database downloads, read [Understanding Database Downloads, page 77](#).

CPM Reporter includes report templates that show inventory. These are *Inventory by Machine*, *Inventory Status by Risk Class*, and *Inventory by Risk Class and Category*. Read the *Websense Enterprise CPM Reporter Administrator's Guide* for complete details.

Inventory Retries

Inventories may not be able to run if:

- ◆ An employee shuts down a machine before a scheduled inventory.
- ◆ An employee shuts down a machine currently running an inventory.
- ◆ Communications are lost between CPM Server and the machine on which the inventory is scheduled to run.

If an inventory cannot run, CPM Server tries to run the inventory five more times, at half-hour intervals. This is a default setting. If the inventory still cannot run, an error message appears in the Windows Event Viewer. If the five retry attempts fail, you will need to schedule a new inventory.

Inventories and Websense Enterprise Manager

CPM Server uses inventory data to populate the following:

- ◆ Inventory details in the **Inventory Status** pane, described in *Accessing the Inventory Status Pane*, page 154.
- ◆ Executables that appear in the **Categories** pane, described in *Accessing the Categories Pane*, page 207.
- ◆ Lists of executables that can be added to CPM software sets, described in *Working with Software Sets*, page 225.

Inventories and CPM Reporter

For CPM Reporter, inventories populate criteria sets for all inventory-related reports. The criteria set defines the specifics that will appear in any report that is associated with that criteria set. For more details, read *Client Policy Manager Reporter Administrator's Guide, Chapter 6: Criteria Sets*.

In CPM Reporter:

- ◆ The **Applications** page shows application and publisher names found during inventory
- ◆ The **Operating Systems** page shows the operating system names and publishers for operating systems found during inventory.
- ◆ The **Processors** page shows microprocessor or CPU names, manufacturer names, and processor speed for those processors found during inventory.
- ◆ The **Physical Memory** page shows physical memory size and manufacturer names found during inventory.
- ◆ The **Hard Disks** page shows hard disk size and manufacturer names found during inventory.

The above pages shows **only** items found during the inventory. For example, if your company runs only *Windows 2000* and *Windows XP* operating systems, these two operating systems will be the only selections available in the **Operating Systems** page. You will not see Windows 95 as an operating system entry, since there are no machines using it.



NOTE

You can view inventory reports in CPM Reporter. Explorer for CPM does not support inventory-based reports.

Inventories and Heartbeats

Client Agent and CPM Server communicate using network messages that occur at a regular, timed interval. These messages are called *heartbeats*, and can be set as described in [Defining Client Control](#), page 104.

Client Policy Manager uses time at the CPM Server to determine when the inventory begins. An inventory may begin on a client machine slightly later than scheduled, depending on the heartbeat interval you set. CPM Server reschedules inventories in half-hour increments.

For example, an inventory is scheduled to run at 12:40 am, but Client Agent/CPM Server communications are scheduled to occur at 12:30 am and 12:45 am. When CPM Server communicates with Client Agent at 12:45 am, the inventory scheduled for 12:40 am begins running at 1:15 am.

Accessing the Inventory Status Pane

The **Inventory Status** pane lets you view machine status, check inventories, and run inventories on client machines that are currently connected to the network. For full details, read [CPM Inventory Database](#), page 45, and [Understanding Inventories](#), page 151.

To access the **Inventory Status** pane:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Inventory** in the navigation pane to access the **Inventory Status** pane.

When you access the **Inventory Status** pane, information in the **Summary** section shows totals for inventory processes. This allows you to rapidly identify what activity has occurred for both hardware and software inventories.

Checking Machine Details in the Inventory Status Pane

When you open the **Inventory** pane, the **Summary** area shows information about machine status, and the total number of machines currently showing that status. You can check the following details:

- ◆ **Scheduled**—total number of client machines that are scheduled for inventory
- ◆ **Running**—number of client machines currently running inventories
- ◆ **Complete**—number of client machines with completed inventories
- ◆ **Total Clients**—total number of clients in the inventory view, regardless of their state

The screenshot shows the Websense Enterprise Manager interface. The main content area is divided into several sections:

- Hardware Inventory Summary:**

Scheduled:	1
Running:	0
Complete:	0
Total Clients:	3
- Software Inventory Summary:**

Scheduled:	1
Running:	0
Complete:	0
Total Clients:	3
- Inventory Status Table:**

Domain	Machine Name	Hardware Status	Software Status	Next Scheduled	Last Completed
QA	DOC423NT	Pending	Pending	10/16/04 1:58 AM	
QA	DOCSSERVER	Pending	Pending	10/16/04 1:58 AM	
QA	LAB332NT	Scheduled	Scheduled	10/16/04 1:58 AM	
- Inventory Functions:**

Check the Event Viewer on the CPM Server machine for inventory error details.

Buttons: Run Inventory..., Manage Inventory..., Cancel Inventory, Clear Completed

Status: All clients updated.

Inventory Status Pane

Each row of information in the **Inventory Status** pane contains the following information:

- ◆ **Domain**—domain for the associated machine

- ◆ **Machine name**—machine name
- ◆ **Hardware Status**—current hardware inventory status. For descriptions of the various status messages, refer to *Understanding Inventory Status Messages*, page 156.
- ◆ **Software Status**—current software inventory status. For descriptions of the various status messages, refer to *Understanding Inventory Status Messages*, page 156.
- ◆ **Next Scheduled**—next date on which the inventory is scheduled to run. If no further inventories are scheduled, the field is blank.
- ◆ **Last Completed**—date, if any, of the last completed inventory.

Understanding Inventory Status Messages

The **Inventory** pane includes the **Software Status** and **Hardware Status** columns. As inventories are scheduled and run, the messages in these columns change to reflect the current state of the inventory. Possible messages are:

- ◆ **Pending**: A request for inventory has been received and CPM Server is processing the request
- ◆ **Scheduled**: The inventory request has been fully processed and is scheduled.
- ◆ **Running**: The inventory is physically running on the identified machine.
- ◆ **Uploading**: The data from the inventory is being uploaded to CPM Server for processing and database insertion.
- ◆ **Complete**: The entire inventory process was successful.
- ◆ **Rescheduled**: The inventory process was not able to run, and has been rescheduled 30 minutes in the future.
- ◆ **Error**: The inventory did not complete because of some processing problem. Check the Windows **Event Viewer** on the CPM Server machine for specific information.



IMPORTANT

For both the **Hardware Status** and **Software Status** columns, the **Error** status indicates that a problem occurred during operations. Check the Windows **Event Viewer** on the CPM Server machine for details about the error.

Running an Inventory

You can run inventory on any machine where Client Agent is installed. The inventories may contain information that can determine how to best maintain your system. For example, using CPM Reporter to present data, you can determine how many versions of a specific application you need to order when upgrading, identify where software is installed, and more.



You can also use inventories to create a lockdown that restricts executables at the machine where the inventory was taken, or to create a software set based on the inventory, and then use it in a rule.



IMPORTANT

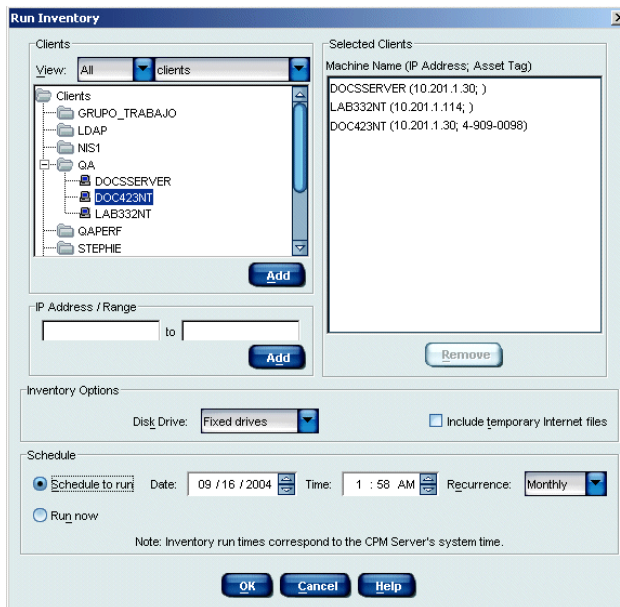
Make sure machines are not in a power-save mode or shut off when inventories are scheduled. If the inventory process encounters these situations, the inventory cannot run. If, however, the machine is able to perform system operations while in **Standby** mode, the inventory will run as scheduled. For specific details, read [Understanding Inventories](#), page 151.

When you are in the **Run Inventories** dialog box, the following symbols identify the various clients.

Symbol	Descriptions
	Single machine, which may be a server or machine
	Domain

To run an inventory:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Inventory** in the navigation pane to access the **Inventory Status** pane.
3. Click **Run Inventory** to open the **Run Inventory** dialog box.



Run Inventory Dialog Box

4. Click in the first **View** field and select which machines you want to run inventory for. Your choices are:
 - **All** to see all machines.
 - **Active** to see only those machines where Client Agent is installed and communicating with CPM Server.
 - **Offline** to see only those machines that are offline.
5. Click in the second **View** field and select the status of the machines you want to run inventory for. Your choices are:
 - **Clients** to see all client machines, regardless of the inventory status at the machines.
 - **Clients inventoried** to see only those machines that have been inventoried at least once.
 - **Clients not inventoried** to see only those machines that have never been inventoried. This is the default setting.
6. Add client machines to the inventory using any or all of the following methods:

- Scroll through the **Clients** list, select the domain or machine you want to include in the inventory, and then click **Add**. You can make multiple selections at one time. For details, refer to [Making Multiple Selections](#), page 114.
- Enter a single IP address in the first **IP Address/Range** field, and then click **Add** to add a single machine to the inventory.
- Enter the starting and ending IP addresses of a range of IP address in the **IP Address/Range** fields, and then click **Add**. The starting IP address must be a smaller number than the ending IP address. For example, **10.1.1.1** to **10.1.1.99** is a valid entry, while **10.1.1.99** to **10.1.1.1** is not.

Your selections appear in the **Selected Clients** list as follows:

- If you add machine names, the machine names and IP addresses appear in the list.
- If you added entire domains, the domain name and the range of IP addresses appear in the list.
- If you added an IP address, both the machine names and IP addresses appear in the list.
- If you added a range of IP addresses, the range of IP addresses appear in the list.

7. Click in the **Disk drive** field and identify the drives you want to inventory. Your options are **All local drives**, **Fixed drives**, and a list of drive letters.
 - **All local drives** identify any fixed drives at the client machine.
 - **Fixed drives** may be hard drives, including any partitions. This is the default.
 - **Drive letters** identify only those mapped drives that reside at the client machine.

**IMPORTANT**

Inventories cannot detect external ZIP drives that are attached by parallel cable. At this time, there is no way to work around this issue.

8. Click in the **Include temporary Internet files** check box to include temporary Internet files in the inventory.



NOTE

For most inventories, including temporary Internet files is not suggested. Temporary files remain on a machine for a limited time, and may cause reports to show information that has little to no value. For shared machines however, for example, those in a corporate library, there may be cases where the additional detail is useful.

9. Indicate how you want to run the inventory: **By Schedule** or **Run Now**.
 - If you select **Run Now**, Client Agent performs an inventory immediately.
 - If you select **By Schedule**, you specify the date and time Client Agent runs a full inventory.
10. To schedule an inventory, click **Schedule to run** to activate the scheduling option, and then
 - a. Select the start date in the **Date** field.
 - b. Select the start time in the **Time** field.
 - c. Identify how often you want to run the inventory in the **Recurrence** field:
 - **None**: A full inventory runs once on the date and at the time you indicate.
 - **Daily**: The inventory runs once every 24 hours, at the time you specify in the **Time** field.
 - **Weekly**: The inventory runs every seven days, at the time you specify in the **Time** field.
 - **Monthly**: The inventory runs every month, at the time you specify in the **Time** field.

If you select a date and/or time that has already passed, an error message warns you of this, and instructs you to reset the schedule.

11. Click **OK** to save the inventory schedule, or to run it immediately if you selected the **Run now** option.

Removing Machines From the Selected Clients List

You can remove a machine from the **Selected Clients** list when you are defining an inventory. This function is available only at this time: you cannot modify machines, drive selections, or scheduling options once you submit an inventory. If you want to stop a pending or running inventory, read [Canceling an Inventory](#), page 161.

1. Scroll through the **Selected Clients** list and select the client or clients you want to remove from the inventory you are scheduling. You can select multiple clients at once. For details, refer to [Making Multiple Selections](#), page 114.
2. Click **Remove**. The machine name disappears from the list.

Canceling an Inventory

You can cancel a scheduled inventory or stop a running inventory whenever necessary:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Inventory** in the navigation pane to access the **Inventory Status** pane.
3. In the **Inventory Status** pane, select the row or rows identifying the machine or machines whose inventory you want to stop, and then click **Cancel Inventory**. A confirmation message appears.
4. Click **Yes** to cancel the inventory.
 - If you select a machine with a pending inventory, the inventory never starts.
 - If you select a machine with a running inventory, the inventory stops, and any data that may have already been collected is dropped.

Clearing Completed Inventory

You can temporarily clear completed inventories from the **Inventory Status** pane. This makes it easier to review machines that have not yet been inventoried, and to track the progress of inventories that are pending or currently running. You can select the **Clear Completed** option at any time to remove inventories.

When you select this option, it impacts only the list at the machine where you are working, and only as long as the **Inventory Status** pane is open. If you close the pane and then return to it, the entries for the completed inventories are gone.






To clear inventories:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Inventory** in the navigation pane to access the **Inventory Status** pane.
3. Click **Clear Completed** to clear all completed inventories. You can also right-click anywhere in the **Inventory Status** pane, and then select **Clear Completed** from the shortcut menu. A confirmation message appears.
4. Click **Yes**. Now, only pending and running inventories appear in the **Inventory Status** pane.

Managing Inventories

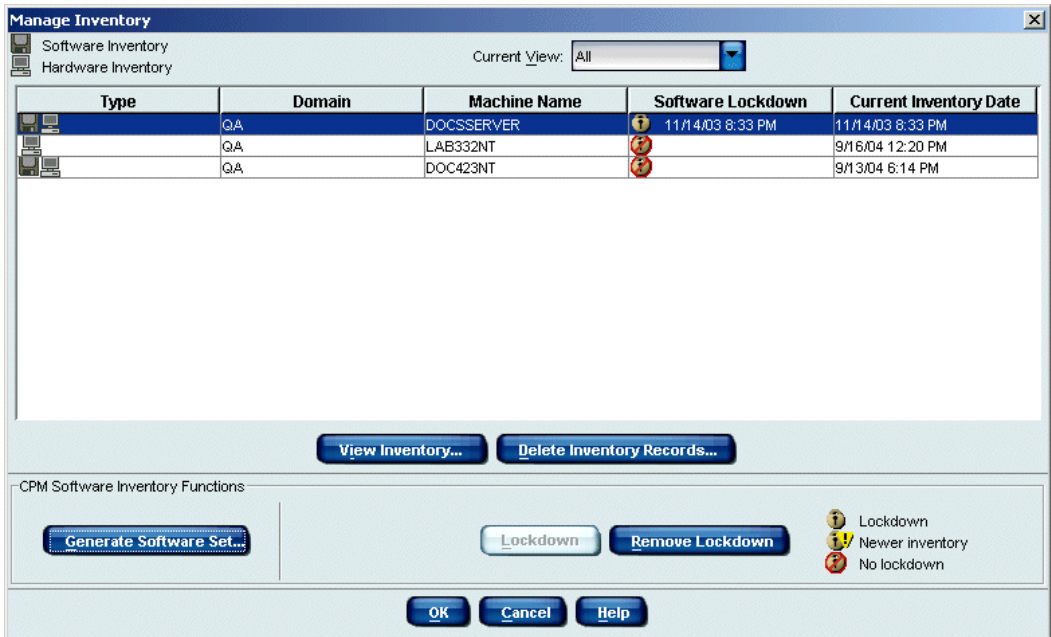
The **Manage Inventory** dialog box allows you to apply and remove lockdowns, as described in [Chapter 9: Applying Lockdowns](#), and view software and hardware inventories for machines running Client Agent. These functions let you access available information quickly, and define critical details for control.

The **Manage Inventory** dialog box uses icons to show the lockdown status and the types of inventory that are available. Icons are identified in the following table.

Symbol	Description
	There is a software inventory available for the machine.
	There is a hardware inventory available for the machine.
	There is a lockdown on this machine.
	There is a newer inventory than the one used to create the lockdown.
	There is not a lockdown for this machine.

To access the **Manage Inventory** dialog box:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Inventory** in the navigation pane to access the **Inventory Status** pane.
3. Click **Manage Inventory** to open the **Manage Inventory** dialog box.



Manage Inventory Dialog Box

4. Click in the **Current View** field and select one of the following:
 - **All Machines**—includes all machines.
 - **List of domains**—includes any domains recognized by Client Policy Manager. When you select a domain, the resulting list shows all machines in the domain you chose.

The **Manage Inventory** pane shows the following information for each machine in the list:

- ◆ **Type**—uses icons to show what type of inventory is available for a given machine. Check the tables earlier in this topic for examples.
- ◆ **Domain**—domain name for the client machine
- ◆ **Machine Name**—name of the machine

- ◆ **Software Lockdown**—symbol to indicate lockdown status. Check the table earlier in this topic for examples.
 - **Locked Down—Lockdown** symbol
 - **Newer Inventory—Newer Inventory** symbol
 - **No Lockdown—No Lockdown** symbol
- ◆ **Current Inventory Date**—time and date of the most recent successful inventory for the machine.

Generating Software Sets from Inventories

You can use inventories to create software sets that can then be inserted into rules. The software set impacts only the machine where the inventory occurred. This can be of benefit for controlling executables at a single machine or allowing executables at shared file servers to run on any machine that accesses the shared file server for logon processes, startup programs, or application access.

The two generation methods are:

- ◆ [Generating a Software Set for a Specific Machine, page 164](#)
- ◆ [Generating a Software Set for Shared File Machines, page 165](#)

Generating a Software Set for a Specific Machine

You can generate a software set for a single machine, and then use the software set in a rule to control access to executables at that machine. If other machines have *exactly* the same configuration, the software set can also be used at those machines.

To generate a software set for a specific machine:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Inventory** in the navigation pane to access the **Inventory Status** pane.
3. Run an inventory if necessary: read [Running an Inventory, page 157](#).
4. Click **Manage Inventory** to open the **Manage Inventory** dialog box.
5. Click in the **Current View** field and select the domain associated with the machine whose inventory you want to use to generate the software set.

6. Select the row which contains information about the machine, and then click **Generate Software Set**. You can also right-click the row, and then select **Generate a Software Set** from the shortcut menu. A dialog box opens and prompts for a name.
7. Enter a name for the software set. Your entry may be between 4 and 60 alphanumeric characters in length.
8. Click **OK**. The **Manage Inventory** dialog box becomes active.

The **Manage Inventory** pane does not show any information about software sets that are generated from inventory: the new software set appears in the **Software Sets** pane, described in *Working with Software Sets*, page 225.

Generating a Software Set for Shared File Machines

Generating a software set from an inventory is critical for organizations that want to use lockdowns, but employees often need to access logon processes, startup programs, or applications installed on shared file servers. For example, Steve is the manager of the Finance department, and wants all desktops in his group locked down. However, there is a shared file server that employees access from their desktop machines to run the accounting package. Because of the lockdowns, employees would not be able to access the shared file server.

To address the problem, perform the following tasks:

- ◆ Schedule an inventory for the shared file server.
- ◆ Generate a software set from the inventory, and call it **FinanceShare**.
- ◆ Run inventories on machines in Finance that are running Client Agent, and create lockdowns for each.
- ◆ Create a rule that lets Finance employees access the executables in the **FinanceShare** software set, and place it above the Lockdown rule. See *Rule Precedence*, page 275.

The Finance employees can now launch the executables in the **FinanceShare** software set in addition to those identified in the lockdown for their machines.

To generate and use software sets for shared file servers:

1. Go to a machine running Client Agent.
2. Logon to the machine as a user with read access privileges to the network shares you want to inventory.
3. Map the network shares you want to include in the inventory, using standard procedures.

4. Stop the Client Agent service using the Windows **Service Control Manager**.
5. Select **Start > Run** to open a command prompt window, type in **cmd.exe**, and then press **Enter**.
6. Go to the directory where Client Agent is installed. The default location is `C:\Program Files\WebSense\WDC`.
7. Type **wdc.exe -c** and press **Enter**. Client Agent is now running in console mode.
8. Go to a machine running Websense Enterprise Manager, select the **Desktop** tab, and then connect to the appropriate Policy Server.
9. Select **Inventory** in the navigation tree, and then click **Run Inventory**.
10. Find the client machine running in console mode and add it to the **Selected Clients** list.
11. In the **Inventory Options** field, select the letter of the mapped network drive. You can select all network drives by clicking **All Drives**, which inventories fixed drives and all mapped drives.
12. Click the **Run Now** radio button to start an immediate inventory.
13. Click **OK** to exit the **Run Inventory** dialog box.
14. Wait until the client machine's inventory status changes to **Completed**.
15. Leave Websense Enterprise Manager open, as you need to come back to it in a few moments.
16. Go back to the client machine, and press any key while in the command prompt window to stop Client Agent.
17. Restart Client Agent using the Windows **Service Control Manager**.
18. Return to Websense Enterprise Manager, select **Inventory** in the navigation tree, and then click **Manage Inventory**.
19. When the **Manage Inventory** dialog box opens, select the client machine that you just inventoried, and then click **Generate Software Set**.
20. Enter a name for the software set and click **OK**.
21. Click **OK** to exit the **Manage Inventory** dialog box.
22. Select **Policy** in the navigation pane and select the **Rules** tab.
23. Click **Add** to add a new rule to the policy, and then:
 - a. Select **All clients** in the **Client Set** field.
 - b. Select **In** in the **In/Not In** field.

- c. Select the software set you generated from the inventory in the **Software Set** field.
 - d. Select **Permit** in the **Action** field.
 - e. Specify if you want to log activity.
 - f. Enter an appropriate description for the rule in the **Comment** field.
24. Make sure the new rule appears above the **Lockdown** rule in the **Rules** pane, using the **Move Up** and **Move Down** buttons as necessary.
 25. Click **Save Changes**.

Inventories, Generated Software Sets, and Rules

Once you use an inventory to generate a software set, and then use that software set in a rule, Client Policy Manager processes stop any deletion unless you start at the top of the sequential chain. For example:

- ◆ You generate a software set. If you try to delete the inventory, a message warns you that there is a software set associated with the inventory. You will not be able to delete the inventory until you first delete the software set.
- ◆ You generate a software set, and then use it in a rule. If you try to delete the inventory, a message warns you there is a software set associated with the inventory. If you try to delete the software set, a message warns you the software set is used in a rule. You will not be able to delete the inventory until you first remove any references to the software set from the rules, and then delete the software set.

Viewing Inventories

You can view details about any executables found during inventory. This can be helpful if you are creating software sets using inventories as the starting point, determining what the machine configuration looks like, or determining what software needs to be removed from a given machine.

Inventories show installed executables, applications and hardware. To view inventory:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Inventory** in the navigation pane to access the **Inventory Status** pane.

3. Run an inventory if necessary. For details, refer to [Running an Inventory](#), page 157.
4. Click **Manage Inventory** to open the **Manage Inventory** dialog box.
5. Select the row associated with the machine whose inventory you want to see in detail, and then click **View Inventory**. You can also right-click on the inventory or lockdown, and then choose **View Inventory** from the shortcut menu. The **View Inventory** dialog box opens.



View Inventory Dialog Box

6. In the **Type** field, select one of the following inventory views:
 - **Software:** The results vary, depending on your selection:
 - The **Inventory View** list shows the executables in the selected inventory. For information, read [Software Executables View](#), page 171.
 - The **Inventory View** list shows the applications in the selected inventory. For information, read [Software Applications View](#), page 172.
 - **Hardware:** The **Inventory View** list shows the hardware in the chosen inventory. For information, read [Hardware Views](#), page 172.
7. Click **OK** to close the dialog box and populate the **Inventory View** dialog box.

The information that appears in the **Inventory View** list depends on your selection in Step 6 of the above procedure.

For details about the information you can access, read:

- ◆ [Software Executables View](#), page 171
- ◆ [Software Applications View](#), page 172
- ◆ [Hardware Views](#), page 172

Software Views

The **Inventory View** dialog box shows software information for both executables and applications. The information you see depends on your selection. You can view the following information discovered during inventory:

- ◆ **Executables installed:** Executables are single files that run programs or applications in programs. For example, winword.exe is an executable. For a complete list of executable file types, refer to [Executables](#), page 44.
- ◆ **Applications installed:** These are groups of files that may include executables, and which are logically associated with each other. For example, **Microsoft Word** is an application.

The information can be useful to determine needed licensing, upgrading, and/or system cleanup. To access software views:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Inventory** in the navigation pane to access the **Inventory Status** pane.
3. Run an inventory if necessary: read [Running an Inventory](#), page 157.
4. Click **Manage Inventory** to open the **Manage Inventory** dialog box.
5. Select the inventory you want to see in detail, and then click **View Inventory**. You can also right-click on the inventory or lockdown, and then choose **View Inventory** from the shortcut menu. The **View Inventory** dialog box opens.
6. View either executables or software applications:
 - Select **Executables**, in the **View** field, to view details about installed executable files.
 - Select **Software Applications**, in the **View** field, to view details about installed applications.

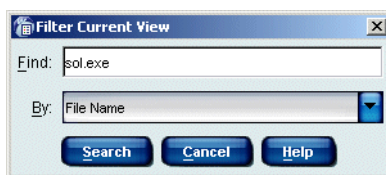
Filtering the Current Software View

When you are viewing software inventories, you can sort the current view by data of interest to you. This function lets you locate information easily.

To set filters:

1. In Websense Manager, click the **Desktop** tab.
2. Select **Inventory** in the navigation pane to access the **Inventory Status** pane.

3. Run an inventory if necessary: read *Running an Inventory*, page 157.
4. Click **Manage Inventory** to open the **Manage Inventory** dialog box.
5. Select the inventory you want to see in detail, and then click **View Inventory**. You can also right-click on the inventory, and then choose **View Inventory** from the shortcut menu. The **View Inventory** dialog box opens.
6. Select **Software** in the **Type** field, and then click **OK**. The Software Inventory View dialog box opens.
7. Change the entry in the **View** field if you want to toggle between viewing executables and software applications.
8. Click **Filter current view** to access the filtering dialog box.



Filter Current View Dialog Box

9. In the **Find** field, type an entry that defines the text that Websense will search for. This entry may be a partial or complete string.
10. In the **By** field, select one of the following search parameters:
 - **Application Name**—available in both **Software Executables** and **Software Application** views
 - **Publisher**—available for both **Software Executables** and **Software Application** views
 - **File name**—available only in the Client Policy Manager **Software Executables** views
 - **File extension**—available only in the Client Policy Manager **Software Executables** view
11. Click **Search**.

The **Software Inventory View** lists any software that matches your entry in the **By** field. If you enter text that the search cannot locate, an error message appears that reads: “Sorry, search produced no results.” You will need to reenter text in the **By** field.

Removing Filters

If you want to return to the complete view for either executables or applications, you can quickly remove any filter you have applied:

- ◆ Click the **Clear Filter** button to return the current view to the default presentation. The button is grayed out if a filter has not been set.

Software Executables View

The **Software Executables** view shows the following information for each installed executable:

- ◆ **Category:** Shows the category to which the executable is assigned.
- ◆ **Publisher:** Shows the company responsible for developing the executable.
- ◆ **Application:** Shows the application name.
- ◆ **File Name:** Shows the executable file name and extension.
- ◆ **Version:** Shows the version number of the executable.

Category	Publisher	Application	File Name	Version
File Management	Microsoft Corporation	Cluster Administrator	cludadmin.exe	5.0.2195.2104
Infrastructure	Microsoft Corporation	System Information	msinfo32.exe	5.0.2134.1
Scripts		dispnode.vbs	dispnode.vbs	
Instant Messaging	Microsoft Corporation	Windows NT Intersite Messa...	ismserv.exe	5.0.2195.6684
Web Browsers	Microsoft Corporation	Internet Explorer	IEXPLORE.EXE	5.0.2920.0
Games	Not Available	Not Available	WinBejZone_setup[1].exe	Not Available
Anti-virus Software	Network Associates, Inc.	McAfee Installation Cleanup	cleanup.exe	3.0.0.0
Installers	Microsoft Corporation	Self-Extracting Cabinet	WindowsNT4Workstation-KB...	5.1.2600.27
Operating Systems - Never ...	Microsoft Corporation	Smart Card Resource Manag...	scardsvr.exe	5.0.2195.6609
Operating Systems - Never ...	Microsoft Corporation	WinRep Windows Report Tool	winrep.exe	5.0.2195.2104
Java Files		setup.jar	setup.jar	
Infrastructure	Microsoft Corporation	Microsoft Connection Manag...	cmdl32.exe	7.1.2186.1
Anti-virus Software	Network Associates, Inc.	Task Manager : scheduling a...	VsTskMgr.exe	7.0.0.0
Miscellaneous Utilities	Microsoft Corporation	Query User Utility	quser.exe	5.0.2134.1
File Management	Microsoft Corporation	Extended Copy Utility	xcopy.exe	5.0.2147.1
WebSense	Not Available	Not Available	keytool.exe	Not Available
WebSense	Not Available	Not Available	rmid.exe	Not Available
Scripts		ucoff8.cmd	ucoff8.cmd	

Software Inventory View Dialog Box: Executables

Software Applications View

The **Software Applications** view shows the following information for each installed application:

- ◆ **Publisher:** Shows the company responsible for developing the executable.
- ◆ **Application:** Shows the application name.

The screenshot shows a window titled "Software Inventory View: DDCSSERVER". At the top, there is a "View:" dropdown menu set to "Software Applications", a "Filter Current View..." button, and a "Clear Filter" button. Below this is a table with two columns: "Publisher" and "Application". The table lists various installed applications and their publishers.

Publisher	Application
BigFix	Enterprise Client 3.0
Eastman Software	Image Viewer 5.0
Executive Software International	Diskeeper 5.0
Hilgraeve	HyperTerminal 5.0
Jasc Software	Animation Shop 3
Jasc Software	Paint Shop Pro 7
Jasc Software	Picture Tube Converter 1.0
Microsoft	Client Connection Manager 5.0
Microsoft	Disk Label 5.0
Microsoft	FrontPage 2000
Microsoft	Internet Connection Wizard 5.0
Microsoft	Internet Explorer 5.0
Microsoft	License Manager 5.0
Microsoft	NetMeeting 4.4
Microsoft	Notepad 5.0
Microsoft	Open Database Connectivity 3.52
Microsoft	Performance Monitor 5.0
Microsoft	Phone Dialer 5.0

At the bottom of the window is a "Close" button.

Software Inventory View

Hardware Views

The **View Inventory** selection supports hardware inventory. To access the **Inventory View** dialog box, read [Viewing Inventories, page 167](#). Hardware inventories show:

- ◆ General machine data such as machine name, manufacturer/model, system type, and serial number.
- ◆ Operating data such as physical memory, measured in MB, BIOS details, operating system, and current user.
- ◆ Physical hardware data such as fixed, floppy, and removable disk drives; display adapters, input devices, monitors, network adapters, printers, processors, sound, and miscellaneous.

If a machine has a Pentium II processor installed, with a cache of 512 K of L2 cache, CPU identification in reports is not always accurate. This is caused by an overlap in the Intel product line, which Websense cannot programmatically resolve.

- ◆ If the Pentium II processor is from family 6, model 5, the processor is identified within the Intel code as being either a Pentium II or Pentium II Xeon.
- ◆ If the Pentium II processor is of family 6, model 7, the processor is identified within the Intel code as being either a Pentium III or a Pentium III Xeon.

To address this issue, entries in the **Hardware Inventory View** will identify these processors as either Pentium II Xeons or Pentium III Xeons.



Inventory View: Hardware

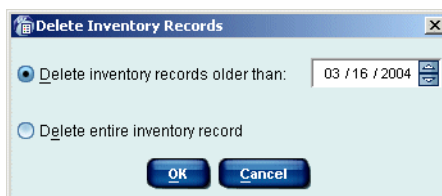
Deleting an Inventory

There may be occasions when you want to completely delete an inventory. When you choose this option, you are deleting the inventory from CPM Inventory Database—not just the **Inventory Status** and **Manage Inventory** dialog boxes. Your decision impacts all CPM users.

You cannot delete an inventory that has been used to create a lockdown or that has been used to generate a software set that is included in a rule. This is a safeguard to ensure continued operations. If you decide after review that you do, in fact, want to delete the inventory, remove the lockdown or the generated software set from the rule, and then delete the inventory.

To delete an inventory:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Inventory** in the navigation pane to access the **Inventory Status** pane.
3. Click **Manage Inventory** to open the **Manage Inventory** dialog box.
4. Select the inventory you want to remove from the CPM system, and then click **Delete Inventory**. You can also right-click the inventory row and select **Delete Inventory** from the shortcut menu. The **Delete Inventory** dialog box opens.



Delete Inventory Dialog Box

5. Decide what you want to do:
 - Click the radio button for **Delete inventories older than <date>** field, and then select the appropriate date. This is the default selection, and the date in the field automatically defaults to the current date. This selection deletes all inventories for the machine that are older than the date you choose.
 - Click the radio button for **Delete entire inventory record** to delete all records for the machine.

6. Click **OK** to delete the inventory. The **Delete Inventory** dialog box closes, and the **Manage Inventory** dialog box becomes active.



NOTE

If the inventory you are trying to delete is set on a recurring scheduled inventory, you must cancel the inventory in the main **Inventory** pane. For details, refer to [Canceling an Inventory](#), page 161.

7. Perform any other necessary tasks in the **Manage Inventory** dialog box.
8. Click **OK** to close the **Manage Inventory** dialog box. The **Inventory Status** pane becomes active.

Applying Lockdowns

Lockdowns are specific to Client Policy Manager and allow a system administrator to control and maintain software access, reduce bandwidth use, increase security, and limit legal liability.

Client Policy Manager offers three types of lockdowns:

- ◆ Inventory Lockdown (inventory dependent)
- ◆ Express Lockdown (inventory independent)
- ◆ Removable Media Lockdown

Inventory Lockdown

A inventory lockdown is based on the inventory for a given machine. When you set a lockdown, Client Agent allows users to access only those applications on the machine at the time the inventory was taken. This provides a last line of defense against viral attacks, as the lockdown effectively restricts access to a limited software set. If an employee or machine attempts to launch executables that are not in a lockdown set, Client Agent automatically blocks access.

Lockdowns are effective for:

- ◆ Limiting access to executables for machines in common areas.
- ◆ Increasing system security by permitting launches of a known software set.
- ◆ Improving departmental or company wide uniformity.
- ◆ Increasing productivity by restricting launches outside a given software set.

Lockdowns may vary in size, depending on the number of executables found during the inventory. As a result, if a machine has a large number of executables in the original inventory, enforcing the lockdown may consume more memory at the local machine than lockdowns containing fewer executables.

Lockdowns provide effective security measures against malicious viruses that are self-modifying. Even though the viruses may change their names as they

attempt to populate a machine, the lockdown prevents the employee from being able to execute the file.



IMPORTANT

To set a standard application lockdown, you must first run an inventory for the machine. Lockdowns impact only the machine where the inventory took place. You cannot apply one lockdown to more than one machine.

Lockdowns and User Policy

Lockdowns affect users differently, depending on the user's access rights as defined in CPM, and the software that is included in the lockdown. If an executable is included in the inventory, any user whose personal policy permits the use of that executable will be permitted to launch it on a locked down machine. If an executable is not included in the inventory when the machine is locked down, no user can install that executable on that machine, regardless of his or her personal policy rights.

Applying an Inventory Lockdown

You can apply an inventory lockdown on any client machine in the Client Policy Manager network once you run an inventory for that machine.

To apply an inventory lockdown:

1. In Websense Enterprise Manager, select the **Desktop** tab.
2. Select **Inventory** in the navigation pane to access the **Inventory Status** pane.
3. Run a new inventory if necessary. For details, refer to [Running an Inventory, page 157](#).
4. Click **Manage Inventory** to open the **Manage Inventory** dialog box.
5. Select the domain in the **Current View** field. Client Policy Manager populates the machine list with current information. This shows each machine name where an inventory has been taken, a symbol showing the lockdown status, and the date and time of the most recent inventory.
6. Select the appropriate machine from the list, and then click **Lockdown**. You can also right-click the machine name and then select **Lockdown** from the shortcut menu.

Client Policy Manager inserts the **Lockdown** symbol in the **Lockdown** column. The lockdown remains in effect for that machine until you remove it.

7. Click **OK** to close the **Manage Inventory** dialog box.

Removing a Lockdown

You can remove lockdowns if necessary. This may be appropriate if you are moving a machine from one department to another, if the assigned machine user is a new employee or changing roles, or if management decides a lockdown is not appropriate any longer. When you remove a lockdown, the inventory remains intact, and can be used again as a lockdown if appropriate.



WARNING

If you are upgrading Client Agent, you must remove lockdowns for any machine that is scheduled to be upgraded. If you do not, you will not be able to complete the upgrade process.

To remove a lockdown:

1. In Websense Enterprise Manager, select the **Desktop** tab.
2. Select **Inventory** in the navigation pane to access the **Inventory Status** pane.
3. Click **Manage Inventory** to open the **Manage Inventory** dialog box.
4. Select the domain in the **Current View** field. Client Policy Manager populates the list with the name of each machine that has had an inventory run, the **Lockdown** symbol appears, and the date and time the last inventory was taken.
5. Select a row, and then click **Remove Lockdown**. You can also right-click on the row, and then select **Remove Lockdown** from the shortcut menu. Client Policy Manager removes the lockdown. The users can now load and launch executables at will, as long as the executables do not exist in any excluded lists.
6. Click **OK** to close the **Manage Inventory** dialog box.

Express Lockdown

The Express Lockdown feature allows system administrators to prevent the execution of any code that is not currently installed on a machine without requiring an inventory of that machine first. Bypassing the inventory requirement eliminates any delay that might allow the spread of malicious code.

System Requirement

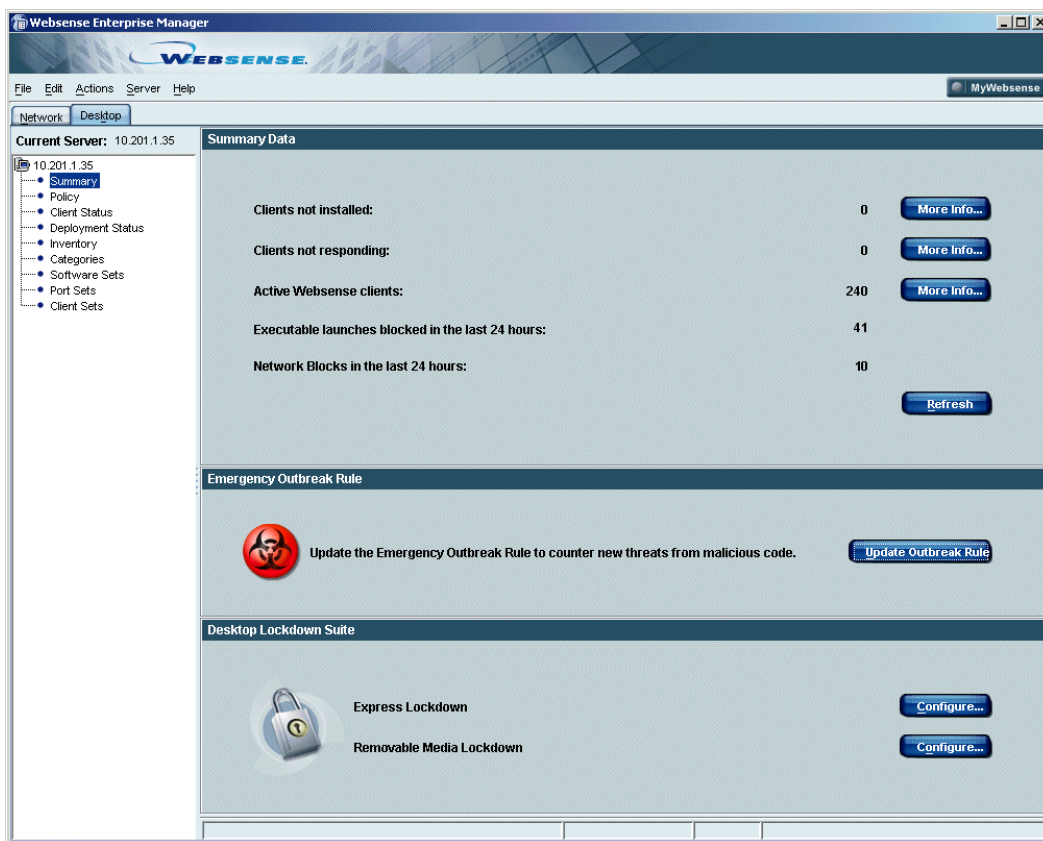
Only NTFS files systems are supported. Express Lockdown is not supported on FAT, FAT32, or other file systems.

Configuring Express Lockdown

To enable Express Lockdown on a client machine:

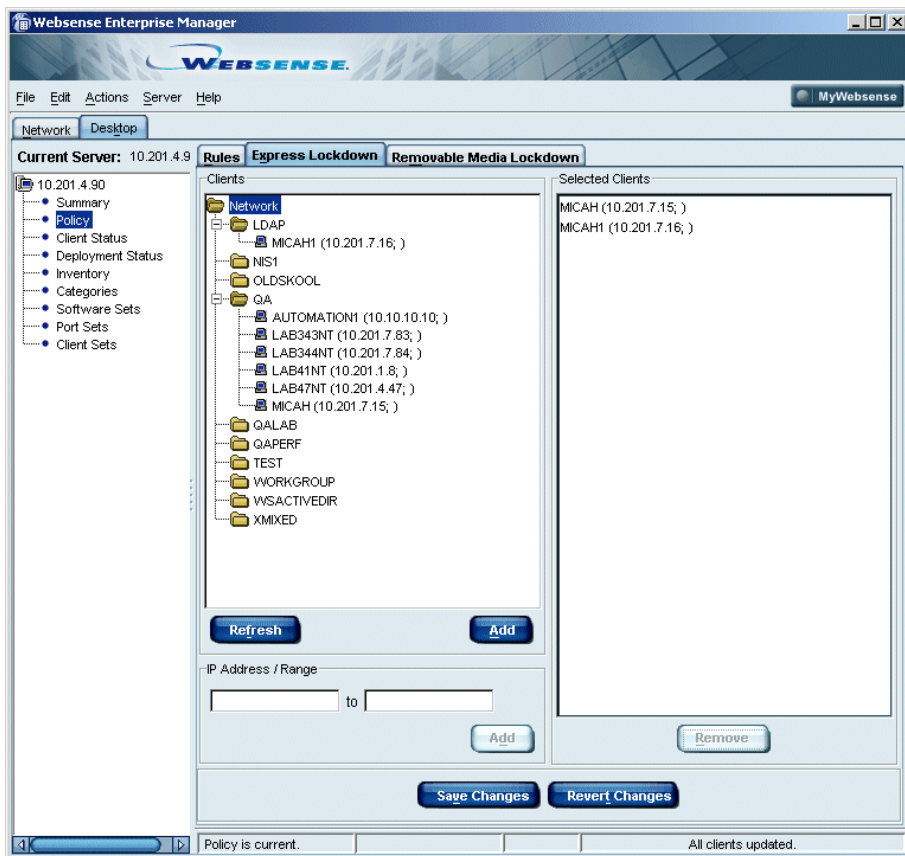
1. Open the Websense Enterprise Manager.
2. Select the **Desktop** tab.

The **Summary Data** pane is displayed with the controls for the new lockdown features at the bottom of the panel.



Summary Data Pane in the Websense Enterprise Manager

3. Click **Configure** for Express Lockdown.
The Express Lockdown tab in the Policy screen is displayed.



Express Lockdown Configuration Pane

4. Expand the tree structure in the **Clients** field to display the machines in your network on which the Express Lockdown feature has *not* been enabled.
5. To apply application lockdown controls to an individual machine, select the machine name from the network tree, and then click **Add**.

The machine is moved to the **Selected** list, indicating that an application lockdown will be applied.



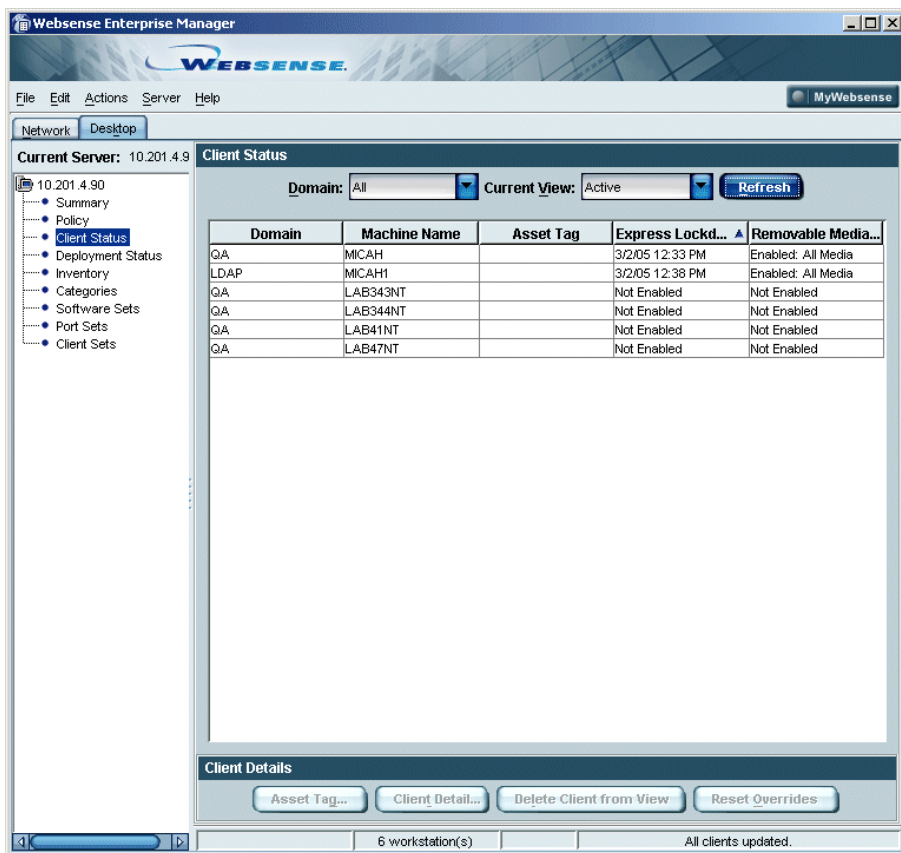
NOTE

New clients (from a new deployment or an upgrade) do not have lockdown status automatically. You must add them to the **Selected** list as they come on-line.

6. To add a subnet or a group of machines to the selected list, enter an IP address range in the **IP Address/Range** field, and then click **Add**.
7. To remove a workstation from the **Selected** list, select the machine, and then click **Remove**.
8. Click **Save Changes** to apply or remove the lockdown to the selected machines.
9. Click **Revert Changes** to undo all the selections you have made and revert to the previous settings.

Viewing Lockdown Status

To view the lockdown status of your workstations, select **Client Status** from the navigation pane in the Websense Enterprise Manager. The Client Status screen provides a CPM view of your client workstations, including the new lockdown features. For further information about Client Status, refer to *Chapter 7: Working with Client Status*.



Client Status Screen

View Options

- ◆ **Domain:** Select a domain to view from the drop-down list. The default setting is **All**.
- ◆ **Current View:** Select one of the following view options from the drop-down list:
 - **Active.** Client Agent is installed and operational, and is communicating with CPM Server normally.
 - **Not Responding.** Client Agent is installed, and the machine is currently on the network, but CPM Server is not receiving data from that client.

- **Disconnected.** Client Agent is installed, but is not communicating with CPM Server, and the machine is not currently on the network. Disconnected machines can include remote machines, laptops, machines undergoing maintenance, and machines that are turned off.

Machine Data

Each row in the pane identifies one machine, and provides the following information:

- ◆ **Domain**—network domain for the client machine.
- ◆ **Machine Name**—client machine name.
- ◆ **Asset Tag**—user-defined asset tag name for the machine. Refer to the *CPM Administrator's Guide* for instructions on creating and editing asset tags.
- ◆ **Express Lockdown**—indicates one of the following statuses for each machine:
 - **Date/Time:** The date and time (from the CPM Server) that Express Lockdown was enabled.
 - **Pending:** This status indicated that Express Lockdown has been enabled, but that the server has not yet received the updated status.
 - **Not enabled:** Express Lockdown is not enabled on this client machine.
 - **Unsupported:** These pre-v5.5.2 client workstations do not support Express Lockdown.
- ◆ **Removable Media Lockdown**— indicates the lockdown status of the removable media on the client workstation. See [Removable Media Lockdown](#), page 185 for details.

Removable Media Lockdown

Removable media present a potential security problem for networks of any size. Writable USB drives and FireWire devices make the theft of intellectual property a real threat. The Removable Media Lockdown feature allows system administrators to prevent devices such as flash drives, CD/DVD burners, floppy drives, and external hard drives from being mounted on client workstations. CPM can be configured to prevent all removable media from being mounted or only writable media, depending upon your organization's policy.



NOTE

Music CDs may not be locked down by this feature. Audio CDs can be played directly by the CD drive without being mounted. Media players that use software to render the audio data from a CD cannot be used. Lockdown will prevent these CDs from being mounted.

Supported External Bus Types

- ◆ USB
- ◆ FireWire/IEEE 1394

Configuring Removable Media Lockdown

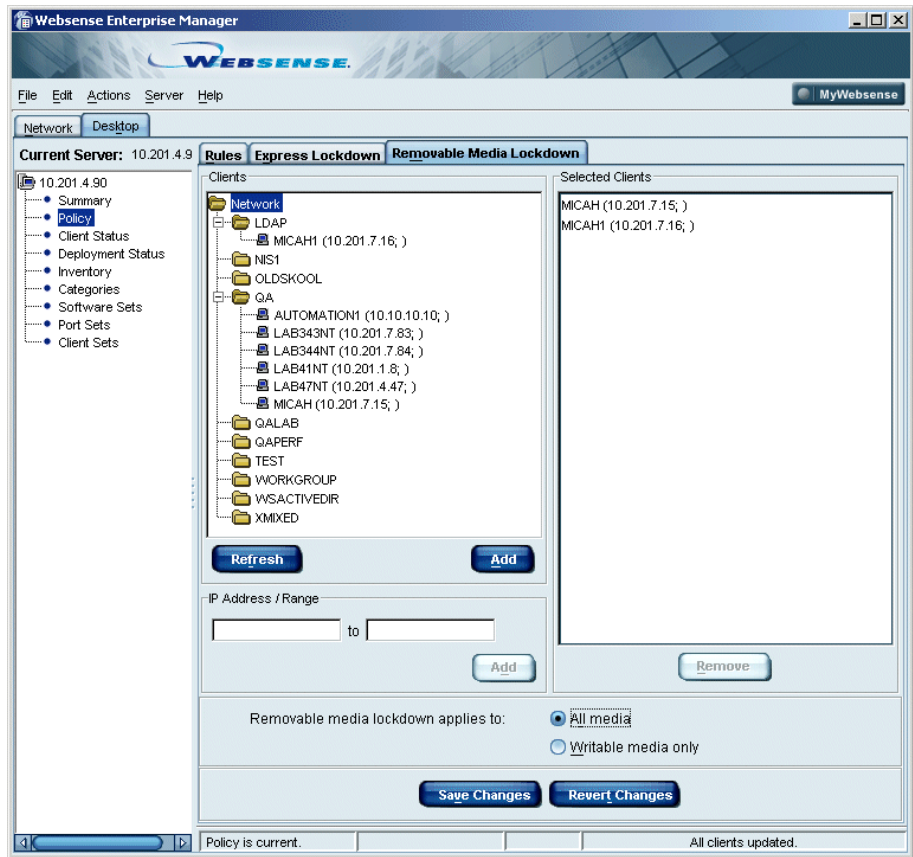
To apply Removable Media Lockdown to workstations in your network:

1. Open the Websense Enterprise Manager.
2. Select the **Desktop** tab.

The **Summary** pane is displayed with the controls for the new lockdown features at the bottom of the panel (*Summary Data Pane in the Websense Enterprise Manager*, page 181. For full details on this screen, refer to the *CPM Administrator's Guide*).

3. Click **Configure** for Removable Media Lockdown.

The Removable Media Lockdown tab in the Policy screen displays.



Removable Media Lockdown Configuration Pane

4. Expand the tree structure in the **Clients** field to display the machines in your network on which the Removable Media Lockdown feature has *not* been enabled.
5. To apply media lockdown controls to an individual machine, select the machine name from the network tree, and then click **Add**.
The machine is moved to the **Selected** list, indicating that media lockdown controls will be applied.



NOTE

New clients (from a new deployment or an upgrade) do not have lockdown status automatically. You must add them to the **Selected** list as they come on-line.

6. To add a subnet or a group of machines to the selected list, enter an IP address range in the **IP Address/Range** field, and then click **Add**.
7. To remove a workstation from the **Selected** list, select the machine, and then click **Remove**.
8. Apply one of the following lockdown options:
 - **All media**
 - **Writable media only**



NOTE

The lockdown option you choose will be applied universally to all the machines being locked down. You cannot mix options among client workstations.

9. Click **Save Changes** to apply or remove the lockdown to the selected machines.
10. Click **Revert Changes** to undo all the selections you have made and revert to the previous settings.

Viewing Lockdown Status

To view the lockdown status of your workstations, select **Client Status** from the navigation pane in the Websense Enterprise Manager (*Client Status Screen*, page 184).

View Options

- ◆ **Domain:** Select a domain to view from the drop-down list. The default setting is **All**.
- ◆ **Current View:** Select one of the following view options from the drop-down list:
 - **Active:** Client Agent is installed and operational, and is communicating with CPM Server normally.
 - **Not Responding:** Client Agent is installed, and the machine is currently on the network, but CPM Server is not receiving data from that client.

- **Disconnected:** Client Agent is installed, but is not communicating with CPM Server, and the machine is not currently on the network. Disconnected machines can include remote machines, laptops, machines undergoing maintenance, and machines that are turned off.

Machine Data

Each row in the pane identifies one machine, and provides the following information:

- ◆ **Domain Name**—network domain for the client machine
- ◆ **Machine Name**—client machine name
- ◆ **Asset Tag**—user-defined asset tag name for the machine. Refer to the *CPM Administrator's Guide* for instructions on creating and editing asset tags.
- ◆ **Express Lockdown**—indicates lockdown particulars for each machine. For additional information, refer to *Express Lockdown*, page 180.
- ◆ **Removable Media Lockdown**— indicates the lockdown status of the removable media on the client workstation. The status entries are:
 - **Enabled: All media**
 - **Enabled: Writable media**
 - **Not enabled**
 - **Pending:** List of clients whose lockdown status is in the process of being changed, before the confirmation response has been received by the server.
 - **Unsupported:** This status indicates pre-v5.5.2 client workstations, which do not support Removable Media Lockdown.

Block Message for Removable Media Lockdown

The block message sent to users when lockdown is enabled is configurable, as is the display of the message. For a discussion of user messages and instructions for changing them, refer to *User Messages*, page 87.

Logging in a Lockdown Environment

The following information is logged when users attempt to mount removable media.

- ◆ Date and time of the attempt
- ◆ Action (block or permit)

- ◆ Workstation ID
- ◆ User ID
- ◆ Drive name (if available)
- ◆ Drive letter (if available)

CHAPTER 10 | Working with Client Sets

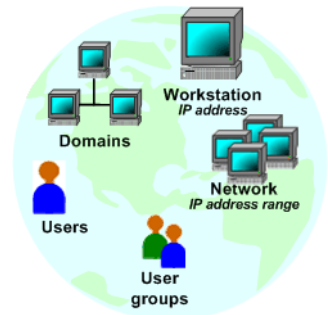
When you configure Client Policy Manager operations, you must identify either Windows NT or Windows Active Directory as the Directory Service. The Directory Service retrieves lists of users and groups—called clients. You can add these users and groups to *client sets*.

A client set identifies a group of clients for inclusion in a CPM rule. When processing the rule, Client Agent enforces the rule for the specific machine or user, based on the entry in that client set. Any launch request or network access attempt by any machine or user included in the client set is handled in the same way.

For example, you block games for the Finance client set, which includes all machines and users in the Finance department. When Client Agent checks the policy, it will block any game that is trying to launch at any machine included in the client set. If an employee logs on to a machine that is not in the Finance client set, and if other rules do not take precedence, that employee will still be unable to launch games, even though she is not at her assigned machine.

Specific clients are:

- ◆ **User**—individual users who have their own user account, identified by the Directory Service.
- ◆ **User Group**—groups of users, often sorted by departmental or functional roles, identified by the Directory Service.
- ◆ **Machine**—individual machine names, identified by the Directory Service by the machine name.
- ◆ **Domain**—single collection of users, user groups, and machines. Domains are often associated with a department or company site, or by functionality, and identified by the Directory Service.





NOTE

Do not create client sets that contain all machines running Client Agent. This type of client set can cause policy creation to be extremely slow. If you want a rule to impact all machines, use the default *All Clients* selection provided as an option in the **Client Set** field of the rule.

Planning for Client Sets

Because client set use is flexible, it is a good idea to have a logical approach to client set development. It is useful to know how you intend to control application launches *before* you begin creating client sets.

Generally, organizations group clients by determining what the specific security goals are, and then identifying what applications each group of machines and/or users will be able to launch. The organizational structure of your existing network and domains may be of value in identifying the contents of client sets, as these often are grouped logically as part of a normal networking strategy.

For example, you have 100 machines on your network, divided into domains. The domains group the machines based on the department they are used by. This structure can be used to easily identify client sets that impact machines.

Each domain includes information about the employees with access to that domain. You can quickly locate the employees that need to be included in rules that define exceptions. These may include managers that require access to applications that are restricted for other employees, marketing staff that use instant messaging software to communicate with existing and potential clients, and so forth.

To help determine the contents of a client set, it is valuable to consider a layered approach, where potential access is defined as extremely restricted, moderately restricted, or minimally restricted, and then ask yourself these questions:

What type of access does this machine, domain, or user group need?

- ◆ If you answered extremely restricted or minimally restricted, consider including the machine in a client set designed to impact machines.

- ◆ If you answered moderately restricted, or if a user's requirements are relatively unique, consider including the user in a client set designed to impact users with similar requirements.

Do I need to block or permit this application or Websense category for a limited number of employees?

- ◆ If you answer *Yes*, consider including these employees in a client set designed to impact users with similar requirements.
- ◆ If you answer *No*, allow default Websense rules to control application launches.

Do I need to block or permit this application or Websense category for a large group of employees?

- ◆ If you answer *Yes*, consider including the application or category in software sets that will be used in rules to impact machines.
- ◆ If you answer *No*, allow default Websense rules to control application launches.

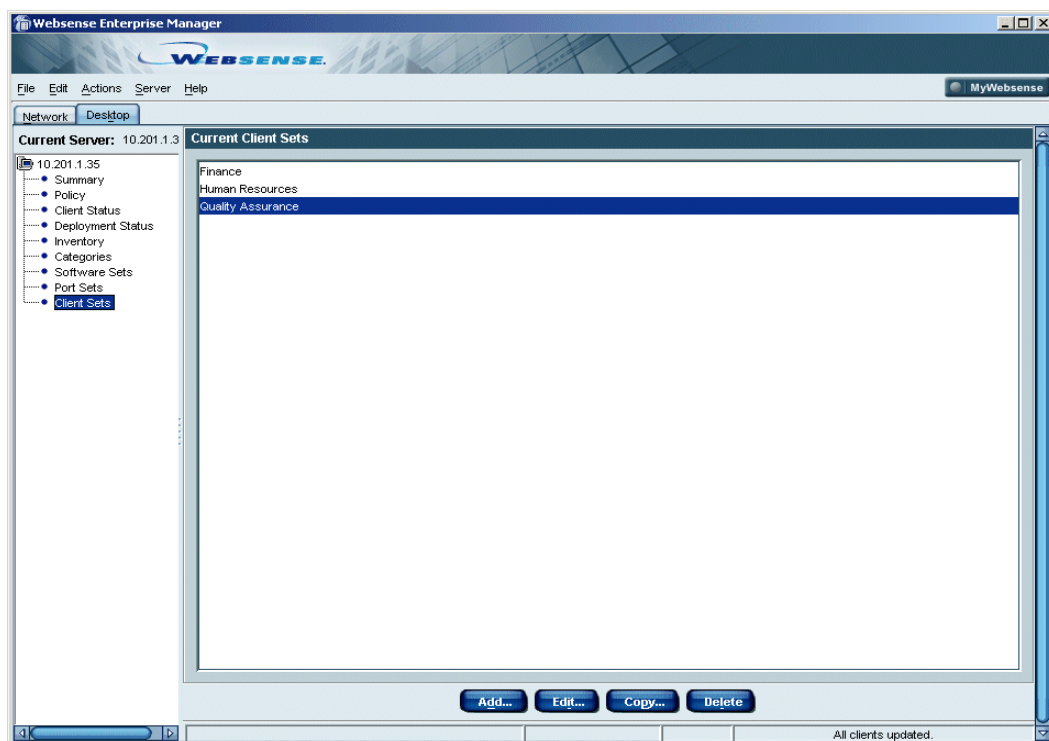
Accessing the Current Client Sets Pane

The **Current Client Sets** pane lets you create logical groups that may contain individual users, user groups, machines, and domains. You can then apply restrictions and permissions to a group of clients while keeping maintenance time to a minimum. This reduces the amount of time spent maintaining Client Policy Manager.

For example, you create a client set that identifies the machines and employees in the Sales department. You can then use the client set in a rule to permit all standard office executables, in addition to those specific to the Sales department. The **Current Client Sets** pane shows all client sets your organization has created. You can add, edit, copy, or delete client sets as appropriate.

To access the **Current Client Sets** pane:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Client Sets** in the navigation pane to access the **Current Client Sets** pane.



Current Client Sets Pane

Managing Client Sets

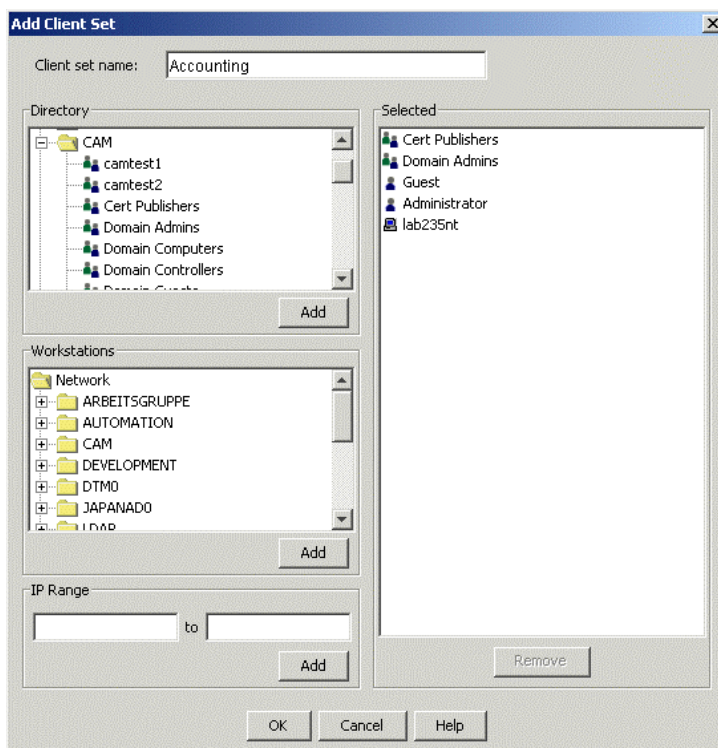
The **Add/Edit Client Sets** dialog box appears when you create or edit a client set. The dialog box lets you identify the clients in a client set. You can add or remove users, user groups, machines, and domains to maintain logical groups.

When you are working in the **Add/Edit Client Sets** dialog box, Client Policy Manager uses symbols to identify the items in the **Selected** list. To view a table of the symbols used in CPM, refer to *Symbols*, page 113.

To work with client sets:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Client Sets** in the navigation pane to access the **Current Client Sets** pane.

3. Click **Add** or select an existing set, and then click **Edit**. The **Client Sets** dialog box opens, and contains the following:
 - **Client set name**. Shows the client set name. If this is a new set, you must enter an appropriate name.
 - **Directory** list. Shows users and user groups you may select and add to the client set using the **Add** button.
 - **Machines** list. Shows machines and domains you may select and add to the client set using the **Add** button.
 - **IP Range** area. Lets you enter a single IP address or a range of IP addresses that you add to the client set using the **Add** button.
 - **Selected** list. Shows users, user groups, machines, and domains you have already selected. You can remove any client using the **Remove** button.



Add/Edit Client Set Dialog Box

Adding a Client Set

You can add a client set at any time. The client set allows you to combine users, user groups, machines, and domains into logical groups, and then apply rules that impact them all. By creating client sets, you can easily manage your system: a single change in one location can be distributed widely without a lot of time and effort on your part.

For example, your company is adding a new department for handling customer service calls. Steve, the manager, wants to control software access for the entire group. Because there is software that is specific to the department, the standard client sets are not appropriate. He calls you and describes the situation.

You open Client Policy Manager and select **Client Sets**. You create a group you call **CustServe**, and then add the names of the department employees and the machines assigned to the department. Later, you create a rule that links the client set with a software set that is also specific to the department.



IMPORTANT

This is one of the first steps you **must** perform to set up your system. When Client Policy Manager is fully configured, adding client sets usually occurs only if it is necessary to support organizational changes.

To add a client set:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Client Sets** in the navigation pane to access the **Current Client Sets** pane.
3. Click **Add**. You can also click anywhere in the pane using the right mouse button, and select **Add** from the menu. The **Add/Edit Client Set** dialog box opens.
4. Enter an appropriate name for the client set in the **Client set name** field. Your entry must be a minimum of 4 and a maximum of 64 characters in length.
5. There are several ways you can add objects to the client set. As you select and add objects, the system populates the **Selected** list.

- Scroll through the **Directory** list and select the users and/or user groups you want to add to the client set, and then click **Add**.
- Scroll through the **Machines** list and select the machines and/or domains you want to add to the client set, and then click **Add**.
If you add a domain, you are adding all users, user groups, and machines that are associated with that domain.
- Enter a single IP address in the first field of the **IP Range** area, and then click **Add**. This adds one machine to the **Selected** list.
- Enter a range of IP addresses in the **IP Range** fields, and then click **Add**. The value you enter in the first field must be less than the value you enter in the second. For example, **10.1.1.1** to **10.1.1.99** is a valid entry, while **10.1.1.99** to **10.1.1.1** is not.

6. Click **OK** to save the new client set.

Editing a Client Set

You can edit client sets when appropriate. This lets you maintain logical groups of clients. You can add and remove clients from the client sets as necessary.

To edit a client set:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Client Sets** in the navigation pane to access the **Current Client Sets** pane.
3. Select the client set you want to change, and then click **Edit**. You can also select the client set, and then click the right mouse button and select **Edit** from the shortcut menu. The **Edit Client Set** dialog box opens.
4. Add clients to the client set if appropriate. When you add a client it appears in the **Selected** list.
5. Remove clients from the client set if necessary. When you remove a client, it no longer appears in the **Selected** list.
6. Continue adding or removing clients as necessary.
7. Click **OK** to save your changes.

Removing a Client from a Client Set

You can remove clients from existing client sets when appropriate. This lets you keep client sets up-to-date.

For example, the Technical Communications department originally reported to Customer Service. However, since the business focus changed, they now report to the Engineering department. To maintain an accurate client set, you remove them from the **Customer Service** client set and add them to the **Engineering** client set.

To remove a client from a client set:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Client Sets** in the navigation pane to access the **Client Sets** pane.
3. Select the client set you want to change, and then click **Edit**. The **Edit Client Set** dialog box opens.
4. In the **Selected** list, choose the client you want to delete, and then click **Remove**. You can delete multiple clients by selecting them, and then clicking **Remove**. Client Policy Manager removes the client or clients from the **Selected** list.
5. Continue removing clients as appropriate.
6. Click **OK** to save your changes.

Copying a Client Set

You can copy an existing client set to create a new one. This is useful if there is a client set similar to one you need. You then edit the copy to customize it.

To copy a client set:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Client Sets** in the navigation pane to access the **Current Client Sets** pane.
3. Select the client set you want to duplicate, and then click **Copy**. You can also select the client set, click the right mouse button, and then select **Copy** from the menu.

The **Copy Client Set** dialog box opens. Client Policy Manager inserts a default name that is the name of the original client set with the word **Copy** added. For example, if the original rule has the word **Engineering** in the **Comments** field, the default entry is **Copy of Engineering**.

4. Accept the default entry or enter a custom name, and then click **OK**.
5. Make any necessary edits.
6. Click **OK** to save your changes.

Deleting a Client Set

You can delete client sets when appropriate. When you delete a client set, you are simply removing the group identity. The process does not remove the clients: they are still available for addition to other client sets.

For example, upper management has determined that the company focus should be Research and Development. As a result, the Manufacturing division has been sold to another company, although a number of engineers are staying with the organization. You delete the **Manufacturing** client set, but still are able to add the engineers to another client set.



NOTE

You cannot delete a client set if you are using it in a rule. You must first remove the client set from the rule before you can delete the actual client set. For more information, read [Deleting a Rule, page 294](#).

To delete a client set:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Client Sets** in the navigation pane to access the **Current Client Sets** pane.
3. Select the client set you want to remove, and then click **Delete**. You can also click on the client set using the right mouse button and select **Delete** from the menu. A confirmation message appears.
4. Click **Yes** to delete the client set.

Working with Categories

Websense categories identify software by what it is designed to do. For example, *Windows 2000* executables appear in the System:Operating System category. The Websense Enterprise Master Database contains all Websense categories, and identifies all known software with a specific category.

The Websense Enterprise Master Database is continuously updated by Websense, Inc. As software is identified, it is categorized and then inserted into the database, to provide you with an ever more powerful tool for desktop control.

Categories serve two purposes in the Client Policy Manager system:

- ◆ Client Policy Manager uses categories when they are in software sets to determine if the executables in the categories should be permitted, blocked, or if the employee should receive a Continue message.
- ◆ CPM Reporter and Explorer for CPM use categories as filters for running reports.

You can use Websense categories in software sets, or you can create custom categories that identify software in a manner that supports business goals. This is a useful tool for companies that use or develop custom software, and/or to identify software that may be included in a Websense category, but that a company wants to track in a different manner.

Categories form a parent/child hierarchy, with the following relationships:

- ◆ A parent category may contain any number of child categories
- ◆ A child category may contain any number of executables
- ◆ You cannot move executables directly into parent categories
- ◆ You cannot create child categories in other child categories



NOTE

For the sake of brevity, this document refers to both parent and child categories as categories, unless there is a specific reason to identify the parent/child relationship.

You can also use the Classification Wizard to run an inventory on a specific folder without using Client Agent. This process allows you to inventory files on the machine where Websense Enterprise Manager is installed, and associate a software set and category with the files. The tool is valuable for companies who run proprietary software, need to update applications, or install new applications.

Websense Categories

Websense categories are included in the Websense Enterprise Master database and identify known software by its use. You cannot delete built-in Websense categories, although you can move executables from one Websense category to another, or move executables from a Websense category to a custom category.

By using Websense categories in software sets, you are able to easily control software launches--you do not need to manually populate software sets with file information. Anytime new information is available from the Websense Enterprise Master Database, each Websense category automatically updates to include any new, relevant information.

For example, you create a rule that blocks the Games category. A new game, `toomuchfun.exe`, appears in the Websense Enterprise Master Database. Later, an employee tries to launch `toomuchfun.exe`. Client Agent blocks it because the software is included in the Games category. As the system administrator, you do not need to do anything special--Websense, Inc. does the work for you.

The Websense categories that identify software use are:

- ◆ The **Access/Privacy/Security** category represents executables that restrict system access or threaten it. Subcategories include:
 - Anti-virus software
 - Authentication and Authorization

- Encryption and PKI
- Firewalls
- Hacking
- Proxy Avoidance
- Keyloggers
- Remote Access
- Spyware
- System Audit.

**NOTE**

Websense, Inc. includes the Hacking and Spyware category in the Harmful Software software set. For more information, read [Predefined Software Sets](#), page 226.

- ◆ The **Audio/Video** category contains executables that support audio and video. Subcategories are *Media Players* and *Image Viewers*.
- ◆ The **Communications** category represents communication executables. Subcategories include *Collaboration*; *Dedicated Browsers*; *Email*; *Instant Messaging*; *Peer-to-peer file sharing*; *Telephony*, *Conferencing*, and *Fax*; and *Web Browser* executables.
- ◆ The **Critical Functions - Never Block** category represents executables that must be present for normal system operations. Subcategories include *File Management - Never Block*, *Infrastructure - Never Block*, and *Operating Systems - Never Block*. This category automatically populates the System Files software set, described in [Predefined Software Sets](#), page 226. These categories are hidden in Client Policy Manager, but are available in reports from Client Policy Manager Reporter.
- ◆ The **Entertainment** category represents executables that have little to no business value. Subcategories include *Games*, *Gambling*, *Adult*, and *Screen Savers*.
- ◆ The **Malware** category represents software identified as malicious code, including executables, applets, and scripts. The only subcategory is *Malicious Software*.

NOTE

Websense, Inc. includes this category in the Harmful Software software set. For more information, read *Predefined Software Sets*, page 226.

- ◆ The **Miscellaneous** category represents common business executables. Subcategories include *Java Files*, *Other*, *Scripts*, and *Temporary Internet Files*.
- ◆ The **Productivity** category represents common business executables. Subcategories include *Contact Managers*; *CRM*; *Data Warehousing*, *Analytics*, and *Reporting*; *Database*, *Document Viewers*, *ERP* and *SCM*; *Graphics*; *Presentation*; *Project Managers*; *Proprietary*; *Reference* and *Information tools*; *Search*, *Retrieval*, and *Knowledge Management*; *Software Development*; *Spreadsheets*; *Suites* and *Integrations*; *Web* and *Desktop Publishing*; and *Word Processing* executables.
- ◆ The **System** category and subcategories represent executables necessary for machine operations. Subcategories include *File Management*, *Infrastructure*, *Installers*, *Miscellaneous Utilities*, *Operating Systems*, and *Scripting Hosts*.
- ◆ The **Uncategorized** category contains one subcategory of the same name. These are executables that are not currently categorized, or that cannot be categorized.

For a complete list of category definitions, read *Appendix B: CPM Category Definitions*, page 319. The most recent category definitions are available at <http://ww2.websense.com/global/en/ProductsServices/MasterDatabase/ApplicationCategories.php>.

When you are working with Websense categories, the following apply:

- ◆ You cannot delete Websense categories
- ◆ You can move executables from any Websense child category to another
- ◆ You can move executables from a Websense category to a custom category
- ◆ You cannot move executables into the Websense **Uncategorized** category

Custom Categories

Custom categories let you develop classifications specific to your organization. This can be useful if your company uses or creates custom software.

For example, your company uses in-house software in Finance. You create a custom category, Finance, that allows you to include all the related files in a rule that allows access to the software by machines and/or users that are associated with the Finance department.

You can also create custom categories that can be useful to fine-tune reports. This can provide more specific granularity than would be available if you were to use Websense categories.

For example, you have software that is used specifically by your Marketing department. While your graphics software is included in a Websense category, you do not want anyone outside of Marketing to use it. You also want other departments to be able to access most graphics programs. You create a custom category, and populate it with the software specific to Marketing. You can now permit the custom category for Marketing only, and permit the other graphic applications using the Websense category.

When you are working with custom categories:

- ◆ You can insert custom categories into parent categories defined by Websense, Inc.
- ◆ You can insert custom child categories into custom parent categories
- ◆ You can move software associated with a Websense category into a custom category

Risk Classes

Risk classes identify potential risk or loss that may be associated with software, and are available as filters in CPM Reporter and Explorer for CPM. Each category maps into one or more risk classes, based on problems that may be associated with executables in that category.

For example, the **Communications** category and **P2P File Sharing** subcategory appear in the **Legal Liability** risk class because of legal issues that may be associated with executables assigned to that category. The same

category also appears in the **Network Bandwidth Loss** risk class because of P2P file sharing bandwidth requirements.

The Websense risk classes are:

- ◆ **Legal Liability:** The executables in this class may result in legal liability. For example, if an employee is playing strip poker on a company machine, other employees may file sexual harassment charges against the organization and the employee. Legal complications can also arise if an executable is pirated or contains offensive materials.
- ◆ **Network Bandwidth Loss:** This risk class contains executables that consume large amounts of network bandwidth. As a result, they may impact overall network operations and could hamper business needs. For example, several employees open media players and are running executables from Web sites at quarter-end. The network bandwidth loss could have a negative impact on the Finance department.
- ◆ **Non-business Usage:** Executables in this class are ones that have little value to most businesses and may negatively impact employee productivity. The strip poker application described in the **Legal Liability** risk class and the media players described in the **Network Bandwidth Loss** risk class would also fall into this risk class.
- ◆ **Security Risk:** This risk class identifies executables that are security risks and include viruses, worms, and other malignant executables, hacking software, and spyware. For example, an executable is able to sniff IP addresses and may be sent to your organization via email. If not caught, outsiders could gain valuable corporate information.
- ◆ **Business usage:** Executables in this class are those generally used by businesses and have no anticipated risk or loss associated with them.

Even though one parent category may contain a number of child categories, the child categories do not necessarily map to the same risk classes. For example, the parent category **Entertainment** includes the **Adult** and **Games** child categories:

- ◆ The **Adult** category maps to the **Legal Liability** risk class
- ◆ The **Games** category maps to the **Non-business Usage** risk class

Although you will not use or see risk classes in Websense Enterprise Manager, it is useful to know they exist, as they are available in CPM Reporter and Explorer for CPM.

CPM Reporter includes a *Risk and Loss* report for each risk class. These show the added value Client Policy Manager provides by tracking launch requests that could lead to potential risk or loss. The only risk class that does not have an associated *Risk and Loss* report is the **Business usage** class, because the included executables do not cause risk or loss. The risk class does appear in other reports, however, and can be manually included in many.

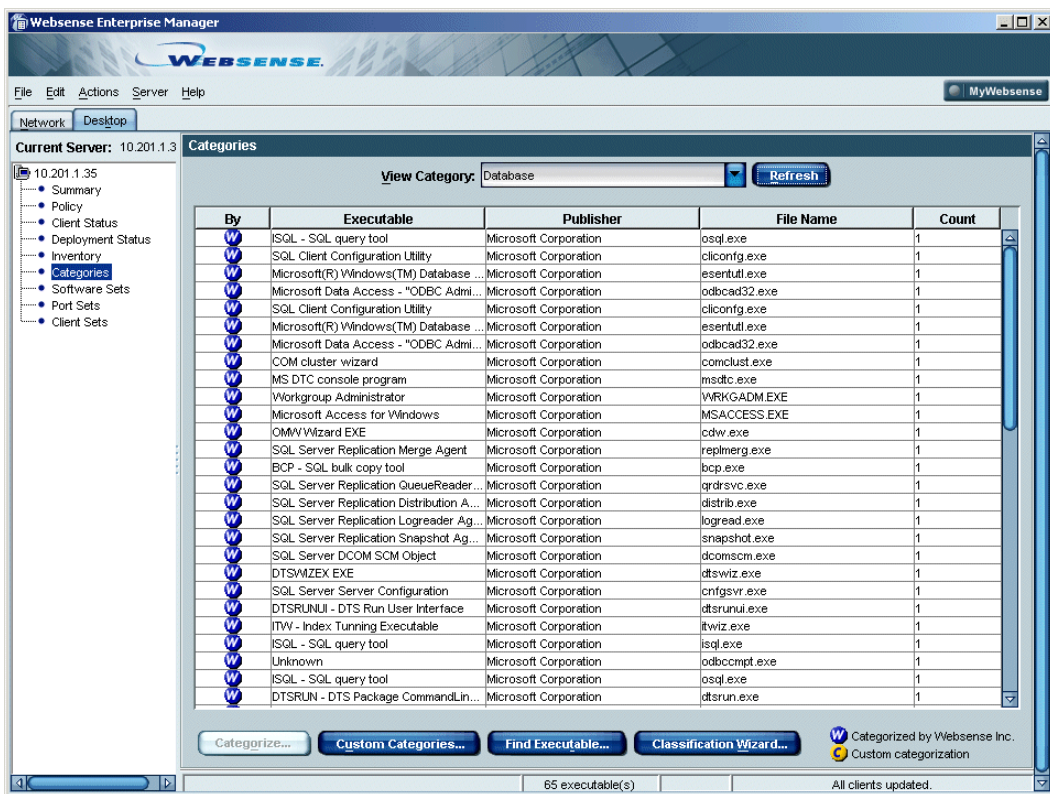
Accessing the Categories Pane

The **Categories** pane allows you to view Websense categories, and add, delete, and remove custom categories. This flexibility lets you define how your Client Policy Manager system sees and handles software. The **Categories** pane also allows you to move any executable found during inventory from a Websense category to any other Websense or custom category.

Using CPM Reporter and Explorer for CPM, you can request reports, filtered by categories, that accurately reflect software installations and/or use in your environment. This information can help you secure and monitor valuable resources.

To access the **Categories** pane:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Categories** in the navigation pane to access the **Categories** pane.



Categories Pane

3. Select the category in the **View Category** field that identifies the types of executables you want to see. Your choices include any category in Client Policy Manager, including custom categories.
4. Scroll through the resulting list to see the executables in the category you chose.

**NOTE**

You may select categories that do not populate the **Categories** list. When this occurs, it means that executables associated with that category were not found during inventory. For example, you select **Malicious Software** in the **View By** field, but the list remains empty. This means that machines that are running Client Agent do not have any known malicious applets or scripts installed.

Understanding Category Data

The **Categories** list contains the following information:

- ◆ **By:** Presents a symbol that indicates how the executable was categorized. If Websense, Inc. categorized it, the Websense symbol displays. If someone in your organization categorized it, the Custom symbol displays.
- ◆ **Executable name:** Shows the executable name.
- ◆ **Publisher:** Shows the publisher of the executable.
- ◆ **File name:** Shows the file name and extension for the executable.
- ◆ **Count:** Shows how many copies of a given executable Client Agent found during scheduled inventories of all client machines on your network.

When you are working with categories, symbols identify both Websense and Custom categories, as described in the following table. To view a table of the symbols used in CPM, refer to [Symbols, page 113](#).

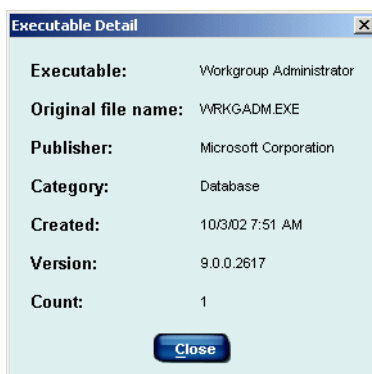
Viewing Executable Details

You can view executable details while you are in the **Categories** pane. This can help identify executables that are either not categorized and should be, or executables that your organization wants to move from the Websense category to a custom category.

To view these details:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Categories** in the navigation pane to access the **Categories** pane.

3. Right-click the appropriate row, and then select **Executable Detail** from the shortcut menu. The **Executable Detail** dialog box opens, and shows the following information for the executable you selected:
 - Executable name.
 - File name and extension.
 - Name of the publisher.
 - Category to which the executable is assigned. This may be a Websense or custom category.
 - Date and time the file was created.
 - Version number.
 - Total number of copies of the same executable, found during inventories, at all machines on the network that run Client Agent.

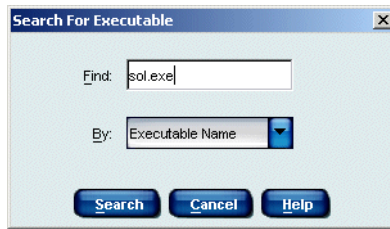


Executable Detail Dialog Box

4. Click **Close** to return to the **Categories** pane.

Finding an Executable From the Categories Pane

You can find executables that were discovered by Client Agent when client machines were inventoried, and then change the category assignment for the executable. This makes the process of managing executables easier, as you can view executable details before making your final decisions about which category is most appropriate for the executable in question.



Search for Executable Dialog Box

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Categories** in the navigation pane to access the **Categories** pane.
3. Click **Find Executable** to open the **Search for Executable** dialog box.
4. Decide what you want to search by: you can use the executable name, the file name, or the publisher's name in the **Find** field. You can also use partial strings.
5. Click in the **By** field and select one of the following:
 - **Executable Name.** Any executable name that matches your entry populates the resulting list of executables. For example, if your entry is **word**, the resulting list could contain `wordpad.exe`, `mswordd97.cmd`, `uword.cmd`, or any other executable that includes the text **word** in the executable name.
 - **Publisher.** Client Policy Manager uses the publisher's name for the search. Any application produced by any publisher that matches your entry populates the resulting list of executables. For example, if your entry is **Micro**, the resulting list could contain any number of *Microsoft* applications, applications from *Orange Micro*, and applications from any other publisher whose name includes the text **Micro** in the publisher's name.
 - **File Name.** The search uses the file name for the search. Any file name that matches your entry populates the resulting list of files. For example, if your entry is **sol.exe**, the resulting list could contain `sol.exe`, `microsol.exe`, and any other executable that includes the string **sol.exe** in the file name.



NOTE

Make sure your entry in the **Find** field and your selection in the **By** field are appropriate. For example, Client Policy Manager cannot find a file if you enter a file name in the **Find** field and select **Executable Name** in the **By** field.

6. Click **Search** to run the search. The **Search for Executable** dialog box closes, and the search results appear in the **Categories** pane.

Moving an Executable from One Category to Another

You can find executables located during inventories in the **Categories** pane, and change category assignments. This makes the process of managing executables easier, as you can view details before making your final decisions about which category is most appropriate for the executable in question.

When you:

- ◆ Move an executable from one Websense category to another, Client Policy Manager associates the executable with the risk class for the new category.
- ◆ Create custom categories and move executables into them, Client Policy Manager does not associate the executable with any risk class, because that category is not associated with a risk class.
- ◆ Use the **Revert** option, described in [Reverting an Executable to the Websense Category, page 214](#), Client Policy Manager restores the original category and risk class assignment.

**NOTE**

When you first set up Client Policy Manager, Websense, Inc. recommends you move any custom executables your organization uses to the **Productivity** category. This ensures that critical programs are not identified as **Miscellaneous:Other** or **Uncategorized**. Otherwise, use default executable assignments and categories until you analyze business needs.

The reports available from CPM Reporter and Explorer for CPM can aid you in this process. Once you are comfortable with Client Policy Manager and how it works, you can then assign executables to a category other than the original one, while still managing to fine-tune risk and loss parameters.

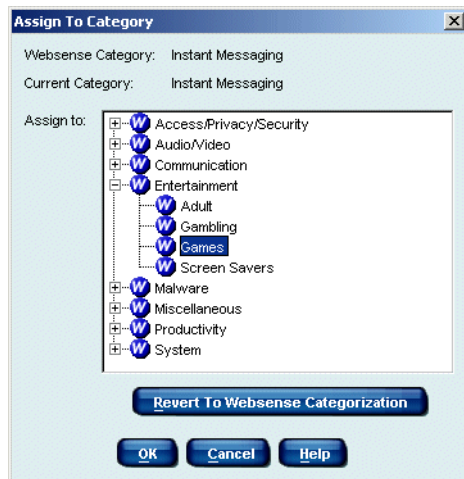
For example, your company designs games. When you are setting up your Client Policy Manager system, you want your products identified as business software, not as games or uncategorized. You add the games you develop to the **Productivity:Proprietary** category.

You can now block the default **Games** category using a rule that includes that category as a parameter. This lets your employees continue to access the games you design, while blocking all others.

To move an executable:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Categories** in the navigation pane to access the **Categories** pane.
3. Click in the **View By** field and select the category you want to see in greater details. The **Categories** list shows all executables currently assigned to that category, and found during machine inventories at machines running Client Agent.

4. Select the executable whose category assignment you want to change, right-click the row, and then select **Categorize** from the shortcut menu. The **Assign To Category** dialog box opens.
5. Scroll through the list of categories to find the category to which you want to assign the executable, and then click **OK**.



The **Assign To Category** dialog box closes. From now until you revert the executable back to the default category, or change the assignment again, the executable appears in the new category, and is marked with the **Custom** symbol.

Reverting an Executable to the Websense Category

You can easily revert the assignment of an executable that you have moved to a category other than the default Websense category. When you do, Client Policy Manager discards any custom assignment and reverts the executable back to the original category association in Websense Enterprise Master Database. This action also re-establishes the risk class assignment. Thus, if you remove custom categories, you do not need to try and remember where Websense originally placed the executable.

To revert an executable:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Categories** in the navigation pane to access the **Categories** pane.
3. Select the executable you want to revert, and then click **Categorize**. You can also click the application row using the right mouse button and select **Categorize** from the menu. The **Assign to Category** dialog box opens.
4. Click **Revert to Websense Categorization**.

The **Assign to Category** dialog box closes. Client Policy Manager reverts the executable back to the default category and risk class to which it was assigned in the default Websense Enterprise Master Database. The next time you see the executable, the **Custom** symbol has reverted back to the **Websense** symbol, and the executable appears in the originally assigned Websense category.

Managing Custom Categories

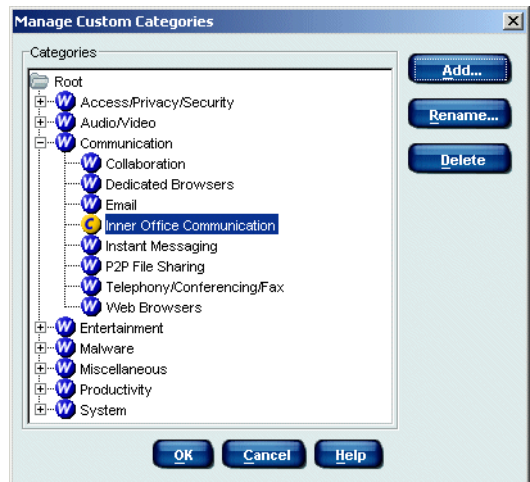
You can add, rename, and delete custom categories to enhance and fine-tune Client Policy Manager functionality. Once you add custom categories in Client Policy Manager, the next time users access CPM Reporter, they can view any custom categories and include them in reports. This lets you categorize executables specifically for your organization and include them in reports for ongoing monitoring.

To access the **Manage Custom Categories** dialog box:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Categories** in the navigation pane to access the **Categories** pane.

3. Click **Custom Category**.
The **Manage Custom Categories** dialog box opens.

The dialog box lists all Websense and custom categories in a tree structure. You can add custom categories at the parent or child level, rename them if necessary, and delete them when they are no longer appropriate.



Client Policy Manager supports two levels of categorization. An example of this structure is:

- ◆ ROOT
 - PARENT category
 - CHILD category
 - PARENT category
 - CHILD category
 - CHILD category
 - CHILD category

Client Policy Manager uses the **Websense** symbol for categories identified and maintained by Websense, Inc. The **Custom** symbol identifies custom categories you create. This helps you identify the category source at a glance.

Adding a Custom Category

You can add custom categories to the list of Websense categories at any time. This function lets you set up categories that meet your specific needs, change the way Client Policy Manager views the executables for reporting, and provide instant control when you add the custom category to software sets that are used in rules.

For example, your company develops games and has a number of custom test executables. Initially, the inventory process inserts these executables in the **Uncategorized** category because they have not been identified by Websense, Inc. You create two custom categories in the **Productivity** category called **InhouseGames** and **Test**, and move your custom executables into them.

To add a custom category:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Categories** in the navigation pane to access the **Categories** pane.
3. Click **Custom Category**. The **Manage Custom Categories** dialog box opens.
4. Identify where you want to insert the custom category.

To add a category:

- Select the **Root** folder at the highest level.
 - Select that category row within an existing category.
5. Click **Add**. You can also right-click the category, and then select **Add** from the shortcut menu. The **Add Custom Category** dialog opens.
 6. Type a name in the field, and then click **OK**.



Client Policy Manager inserts the new category into the tree where you created it. From now on, the **Custom** symbol identifies the category.

You can add executables to any custom child category using the **Categorize** option in the **Categories** pane. When you make this association, your settings override the Websense settings.

Renaming a Custom Category

You can rename custom categories at any time. This allows you to manipulate your custom categories to meet ongoing changes in your business environment. If you change the name of a custom category, your changes will appear in any software sets that use it.

Any category name change also impacts reports that include executables associated with that category:

- ◆ For reports that show launches, the report uses the category name associated with the executable at the time of the launch.
- ◆ For reports that show inventory, the report uses the most recent category name, regardless of the category name at the time of inventory.

For example, your company develops games and has a number of custom test executables. You created a custom category called **Test** and moved the test executables into it. Later, reviewers decide that **Test** is not as accurate a title as **QA** is, and ask you to change the name.

After you remove the category, and you run launch reports that include executables from the **Test** or renamed **QA** category, the report shows the category name assigned at the time the launch request occurred. If you run inventory reports that include executables in the **Test** or renamed **QA** category, the reports show the category name **QA**--the most recent name.

To rename a custom category:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Categories** in the navigation pane to access the **Categories** pane.
3. Click **Custom Category** to open the **Manage Custom Categories** dialog box.
4. Select the custom category you want to rename, and then click **Rename**. You can also right-click the custom category, and then select **Rename** from the shortcut menu. The **Rename Custom Category** dialog box opens.
5. Type the new name in the **Category name** field, and then click **OK**.

Client Policy Manager replaces the former category name with your entry.

Deleting a Custom Category

You can delete custom categories from the list of categories at any time. This function lets keep your categories up-to-date, and respond to business changes. You cannot delete categories defined by Websense, Inc.

You do not need to move executables from categories you are going to delete: the executable automatically reverts back to the original category assigned by Websense, Inc. when you delete the custom category. This makes category management almost foolproof, as accurate reversion does not require any work on your part.

For example, you defined a number of custom categories, identified by department, when you first began using Client Policy Manager. Now, because of business issues, the Manufacturing group is being sold.

One of these custom categories, **Manufacturing**, included software that tracked product through the system. Since Manufacturing is no longer a part of the organization, you no longer need the category and so delete it.



NOTE

You cannot delete a custom category if you are currently using it in a software set that is in a rule. You must first remove the custom category from the software set before you can delete the custom category. For more information, read [Removing an Item from a Software Set, page 242](#).

To delete a custom category:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Categories** in the navigation pane to access the **Categories** pane.
3. Click **Custom Category** at the bottom of the **Categories** pane to open the **Manage Custom Categories** dialog box.
4. Select the custom category you want to remove, and then click **Delete**. You can also right-click the category, and then select **Delete** from the shortcut menu. A confirmation message opens.

**NOTE**

If you delete a custom parent category that contains custom child categories, you will delete the parent and all the child categories it contains. The executables in the categories revert back to the original Websense category assignment.

5. Click **Yes** to remove the category from the list.
6. Click **OK** to return to the **Category** pane.

Using the Classification Wizard

The Classification Wizard provides a way to collect information via “mini” inventories at the machine where you have installed Websense Enterprise Manager. The wizard allows you to:

- ◆ Run inventories on a specific directory, without using Client Agent. The files discovered during the process appear in the CPM Inventory Database, described in [CPM Inventory Database, page 45](#).
- ◆ Add the files found by the Classification Wizard to an existing or new software set. If you create a new software set, it appears in the **Software Set** pane, described in [Chapter 12: Working with Software Sets, page 225](#).
- ◆ Associate the files found by the Classification Wizard to an existing or new category. If you add a custom category, it appears in the **Categories** pane, described in [Accessing the Categories Pane, page 207](#).

The Classification Wizard is ideal for companies that develop and/or use proprietary software, need to add product updates to existing software packages, or that are installing new software on machines. Usually, the process is complete within minutes.

For example, a company produces software used in the insurance industry and releases new add-on modules each quarter. Their CPM policy is relatively restrictive, but they want to quickly identify their proprietary software as they build it, and allow it to launch.

The system administrator places all the files necessary for the latest version in a directory at the machine where Websense Enterprise Manager is installed. She accesses the Classification Wizard and identifies the:

- ◆ Directory where she placed the files.
- ◆ Category with which the files are to be associated. This may be an existing or new category.
- ◆ Name for the software set in which the files will be included. This may be an existing or new software set.

Once the administrator completes these steps, CPM then:

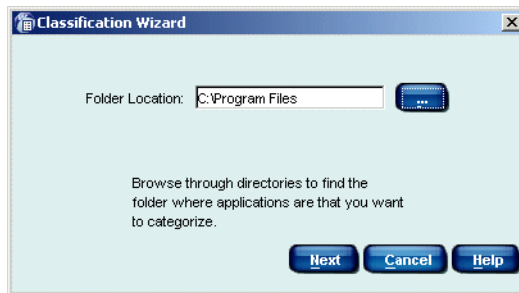
- ◆ Inserts the new inventory in the CPM Inventory Database.
- ◆ Adds the files to the indicated existing or new category, which then appears in the **Categories** pane, described in [Accessing the Categories Pane, page 207](#).
- ◆ Adds the files to the indicated existing or new software set, which then appears in the **Software Sets** pane, described in [Chapter 12: Working with Software Sets, page 225](#).

The files that are added in this manner are available in CPM Reporter and in the **Inventory Views**, described in [Viewing Inventories, page 167](#).

To use the Classification Wizard:

1. Place the files you want to inventory on the machine where you have installed Websense Enterprise Manager. You may have any number of files and folders.
2. In Websense Enterprise Manager, click the **Desktop** tab.
3. Select **Categories** in the navigation pane to access the **Categories** pane.
4. Click **Classification Wizard**.

The **Classification Wizard Folder Location** dialog box opens.



Classification Wizard Folder Location dialog box

5. Type path data into the **Folder Location** field for the directory you want to inventory.

Alternately, you can click **Browse** to browse to the directory if you want. The **Open** dialog box appears.

- a. Locate the folder you want to inventory, using onscreen buttons and fields for navigation. You must inventory all files in the folder you select.
- b. Click **Select Folder**.

The **Classification Wizard File Location** dialog box reopens. The **File Location** field contains the path of the folder you want to inventory and classify.

6. Click **Next**.

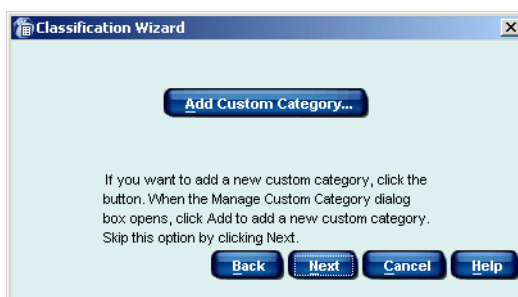
The **Classification Wizard Software Set** dialog box opens.



Classification Wizard Software Set dialog box

7. Click in the **Software Set** field. You can:
 - Select an existing software set, if appropriate. The field displays all currently existing software sets.
 - Manually enter a software set name if appropriate:
8. Type the name for the new software set in the **Software Set name** field. The software set name appears in the **Software Set** field of the Classification Wizard.
9. Click **Next**.

The **Classification Wizard Custom Category** dialog box opens.



Classification Wizard Add Custom Category Dialog Box

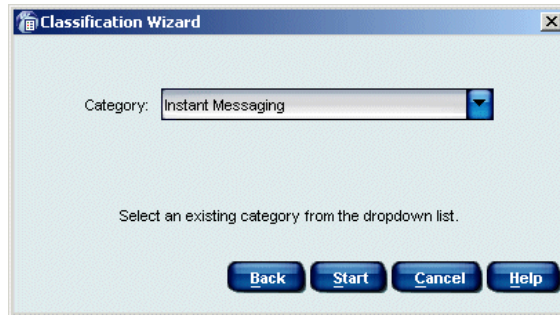
10. If you want to add a custom category, click the **Add Custom Category** checkbox. The **Manage Custom Category** dialog box opens.
11. Select the parent category to which you want to add a new custom category, and then click **Add**.



NOTE

You can enter “parent” categories at this time, but you then need to create a “child” category within the parent. CPM does not allow you to select “parent” categories when classifying files.

12. Click **OK** to close the **Manage Custom Category** dialog box.
13. When the **Add Custom Category** dialog box reopens, click **Next**. The **Category** dialog box opens.



Classification Wizard Category Dialog Box

14. Click the arrow for the **Category** field, and then select the category to which you are assigning executables and applications.
15. Click **Start** to run the Classification Wizard.
A progress window appears during the inventory.



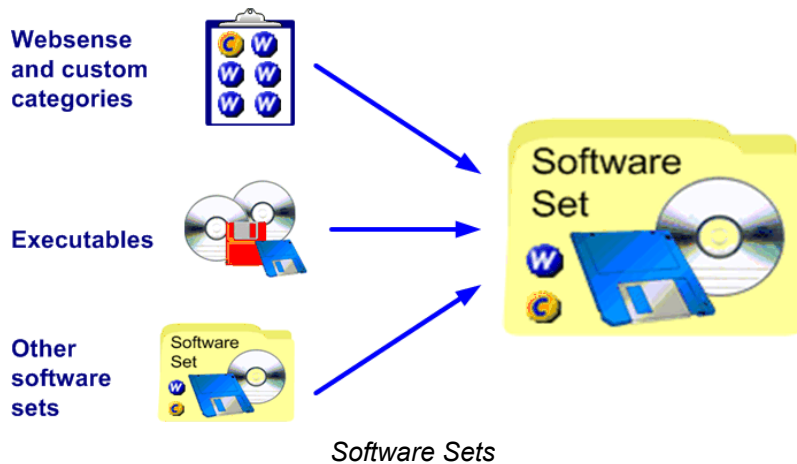
Classification Wizard Progress Dialog Box

16. When the inventory is complete, the progress window indicates the completed status. Click **Close** to return to the **Categories** pane.
17. If necessary, add the software set you used for inventory to a rule, and then set control options. For details, refer to [Adding a Rule, page 288](#).

CHAPTER 12 | Working with Software Sets

Client Policy Manager uses software sets as filters for controlling launches. A software set is a group of executables that Client Policy Manager handles as a single entity. One software set may include any number of:

- ◆ Individual executables. For a list of recognized executables files, read [Executables](#), page 44.
- ◆ Category selections. Read [Chapter 11 Working with Categories](#) .
- ◆ Other software sets.



It is useful to know how you plan to use a software set for before you develop it. For example, you may create four software sets:

- ◆ Categories you will block
- ◆ Common software you will permit
- ◆ Software you will permit for Accounts Payable and Receivable
- ◆ Software you will permit only for the Technical Communications department

Once you identify a basic group of software sets, you can use them in other software sets. For example, you create a software set called *Finance* that includes:

- ◆ Software set that identifies common software used by all departments. This same software set is used in other department specific software sets.
- ◆ Software set that contains software specific to Accounts Payable and Receivable

The resulting *Finance* software set identifies all executables used by Finance employees.

After you create software sets, you then use them in rules to control launches. Read [Chapter 14: Working with Rules, page 255](#).

Predefined Software Sets

Websense, Inc. includes four predefined software sets. These appear in predefined Websense rules:

- ◆ **All Categories**, which includes all custom and Websense categories.
- ◆ Enterprise Productivity, which includes the Websense Web Browsers, Database, Email, CRM, Anti-virus Software, and Document Viewer categories.
- ◆ **System Files**, which automatically populates the preset **System Files** rule, described in [System Files Rule, page 263](#). The software set contains the Websense Critical Functions - Never Block category. You cannot edit or remove the System Files software set.
- ◆ **Harmful Software**, which automatically populates the predefined Harmful Software rule, described in [Harmful Software Rule, page 264](#). The software set contains the Websense Hacking, Malware, and Spyware categories.

Planning for Custom Software Sets

When you create a software set, it is useful to know, in advance, what type of rule you intend to use the software set in. This allows you to plan a logical approach as you begin applying launch control.

Websense recommends that you create software sets to meet specific goals within your organization. For example, you may create software sets to accomplish the following:

- ◆ Block applications that may cause risk or loss
- ◆ Permit applications that are used by only a few employees, for example, Management
- ◆ Control machine requested launches
- ◆ Control employee requested launches

You can create any type or number of software sets. However, it is valuable to minimize duplication wherever possible, so that you can easily manage the software sets.

You can use software sets in the following manner:

- ◆ Create software sets to reflect departments in your company to increase monitoring and control options.
- ◆ Use one software set in any number of rules.
- ◆ Use one software set in any other software set.

For example, you can create a software set that contains the Instant Messaging category, and then use it in rules to accomplish the following:

- ◆ Permit launches for Sales.
- ◆ Block launches for Shipping and Receiving, Manufacturing, and Purchasing.
- ◆ Allow employees to continue the launch for Management.

By planning ahead, you can save yourself considerable duplication and work. To help determine the contents of a software set, ask yourself these questions:

Do I want to block or permit this application or Websense category for most employees?

If you answer *Yes*, consider including the application or category in software sets that will be used in rules specific to machines.

Do I need to block or permit this application or Websense category for a select group of employees?

If you answer *Yes*, consider including the application or category in software sets that will be used in rules to impact employees.

Can I use this software set in more than one rule?

If you answer *Yes*, determine how to best implement the rules that will use the software set.

Can I use this software set in another software set, thus reducing the number of rules I need to create?

If you answer “Yes,” plan the “parent” software sets carefully. While you can quickly remove a software set from a rule, you will still need to test your results with every change.

Software Sets for Machines

You can create software sets that will appear in rules designed specifically to impact machines. This can be a valuable method to help control unwanted application launches.

For example, startup applications are identified with the machine as the user, not the employee. If there is an instant messaging application in the **Start Up** folder, it could be launched by employees unless you specifically block the application at the machine level.

Software Sets for Machines and Users

Software Sets for Users

Software sets designed specifically to impact employees often have more variation than do software sets designed specifically to impact machines. For example, your Marketing group uses imaging tools for ad layout. However, you do not want other groups using imaging tools at all.

You create a software set that includes the Websense Imaging category, and then use the set to:

- ◆ Permit imaging software launches only for the Marketing group.
- ◆ Block imaging software launches for all other groups.

Software Sets for Machines and Users

You may create software sets that will impact both machines and users. In many organizations, this type of software set is created to impact the machines and the users in specific departments.

For example, you create a software set that contains a number of categories you want to block. When you create the rule, you select a client set that includes all machines and users in the Human Resources department. The rule will block the indicated software associated with the categories, regardless of whether it is the machine or the user that is requesting a launch.

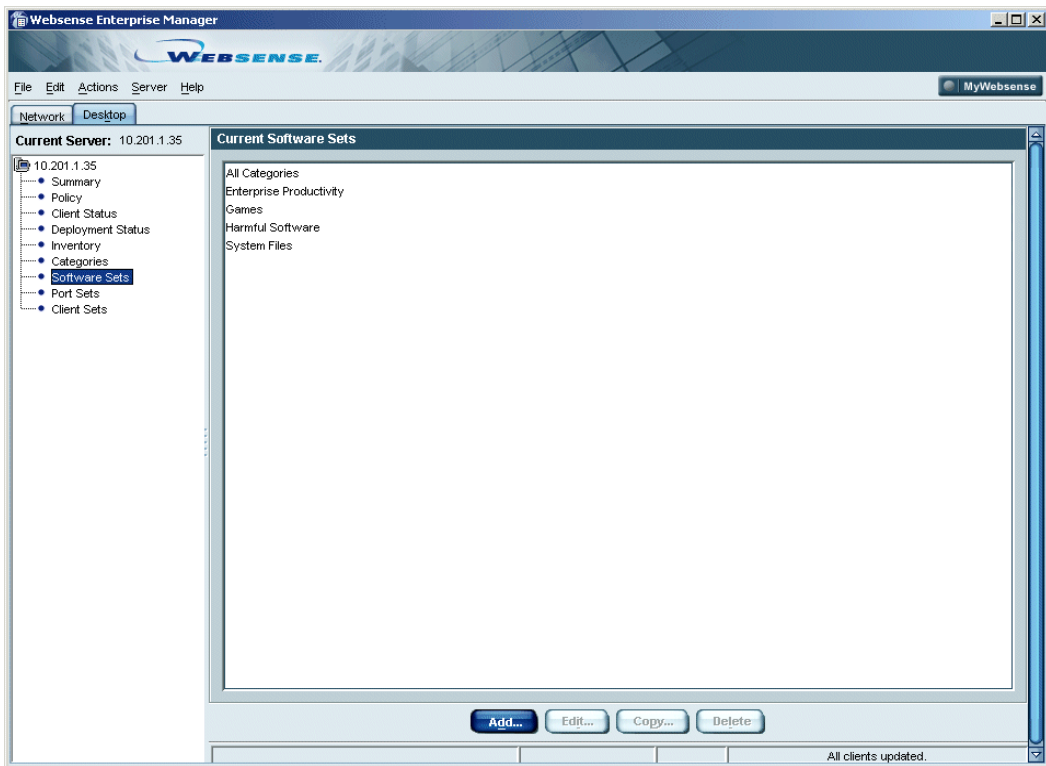
Accessing the Current Software Sets Pane

Software sets allow you to group executables, categories, and other software sets into logical combinations. You can then define rules that permit or block launches, or let employees decide how to respond to launch requests by setting the rule to continue.

To access the **Current Software Sets** pane:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Software Sets** in the navigation pane to access the **Current Software Sets** pane.

The **Current Software Sets** pane lists all existing software sets in alphabetic order.



Current Software Sets Pane

When you first install CPM, the Current Software Sets pane includes the default Websense software sets described in [Predefined Software Sets, page 226](#).

When you are working in the **Add/Edit Software Set** dialog boxes, symbols identify both Websense and Custom categories. To view a table of the symbols used in CPM, refer to [Symbols, page 113](#).

Managing Software Sets

The **Add/Edit Software Set** dialog box lets you combine categories, existing software sets, and individual executables into a logical group. You can also view the contents of existing software sets, and drill down as far as necessary.

To access the **Add/Edit Software Set** dialog box:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Software Sets** in the navigation pane to access the **Current Software Sets** pane.
3. Determine what to do:
 - If you are creating a new software set, click **Add**.
 - If you are adding an executable, category, or another software set to an existing software set, select the software set you want to modify, and then click **Edit**.

The **Add/Edit Software Set** dialog boxes contain the following options:

- ◆ **Software Set Name**—shows the name of the software set. If you are creating a new software set, enter an appropriate name.
- ◆ **Categories**—shows the categories you may select and add to the software set using the associated **Add** button. You can add both Websense and custom categories.
- ◆ **Software Sets**—shows the existing software sets that you may select and add to the software set using the associated **Add** button. You can also click in any row containing the **View** symbol and check software set contents.
- ◆ **Selected**—shows any existing contents of the software set. Each item is identified as a software set, category, or file. You can click in any row that contains the **View** symbol and check software set contents. You can remove any item in the **Selected** list by selecting the item, and then clicking **Remove**.

Adding a Software Set

You can create software sets that group individual executables, categories, and other software sets into a logical set. You can then define rules that control launch requests using the software set to identify the executables affected by that rule.

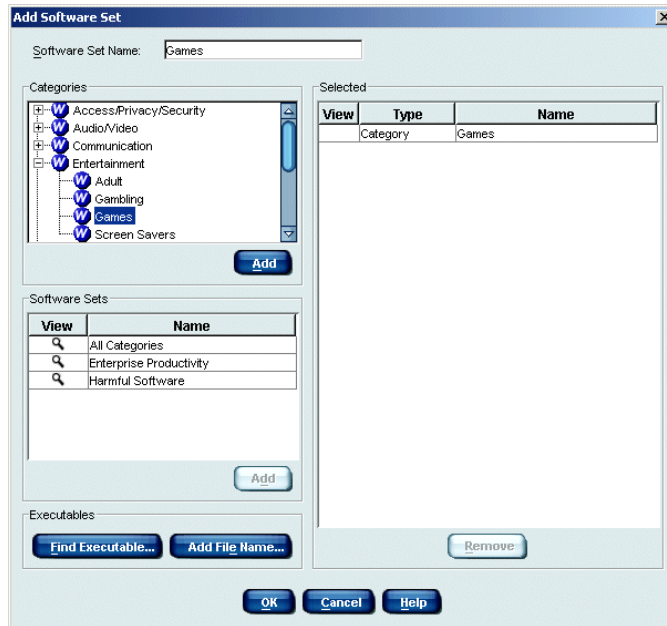
For example, you want to block executables that result in productivity loss. You create a software set that contains:

- ◆ The **Instant Messaging** category.
- ◆ The **Image Viewer** category.
- ◆ The game `toomuchfun.exe`, which you discovered on a machine in the corporate library, but is not yet in the Websense Enterprise Master Database.
- ◆ The existing **Block Software Set**, which you created when you began configuring Client Policy Manager. The software set includes the **Games**, **Adult**, and **Malicious Applets and Scripts** categories.

Once you create the software set, you then include it in a rule. This associates the software set with a client set that identifies users, user groups, machines, and domains. You set the action to **Block**. In the future, these employees and/or machines are unable to launch the executables identified in the software set. For details, refer to [Chapter 14: Working with Rules, page 255](#).

To add a software set:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Software Sets** in the navigation pane to access the **Current Software Sets** pane.
3. Click **Add**. You can also right-click anywhere in the **Current Software Sets** list, and then select **Add** from the shortcut menu. The **Add Software Set** dialog box opens.



Add Software Set Dialog Box

4. Add items to the software set as appropriate, using any of the following methods:
 - To add a category:
 - a. Scroll through the **Categories** list.
 - b. Expand any parent category to find the child category you want to include in the software set.
 - c. Select the category, and then click **Add**.
The category name appears in the **Selected** list.

You can add parent or child categories, and may select multiple items and add them as a group if you want.



WARNING

Websense, Inc. recommends that you do not include the **Uncategorized** category in software sets, as there may be files necessary for critical startup and logon processes. If you add the **Uncategorized** category to a software set, a warning message appears that provides alternate suggestions.

Also, do not include the **Java Files** category in any software set that may impact the machine where you install Websense Enterprise Manager. If you do, and create a rule that blocks Java Files, you will not be able to access Websense Enterprise Manager.

- To add another software set:
 - a. Scroll through the **Software Sets** list
 - b. Select any software set you want to include.
 - c. Click **Add**.

You may select multiple software sets and add them as a group if you want.
 - Click **Find Executable** to search for a file and then add it. The file must have been discovered during an inventory on at least one machine running Client Agent. Read *Searching For and Adding an Executable*, page 239.
 - Click **Add File Name** to manually add files by name. Read *Manually Adding a File Name to a Software Set*, page 240.
5. Continue adding any necessary items.
 6. Click **OK**. The **Current Software Sets** pane becomes active.

Editing a Software Set

You can edit software sets by adding or removing individual executables, categories, and other software sets. This allows you to maintain software sets appropriate to your business environment.

For example, your company has decided to purchase a new software application that tracks your product through development. Management contacts you. You open the **Manufacturing** software set, and add the new software executable to enable parallel testing. When parallel testing is complete, you reopen the same software set, and remove the old product tracking executable.

To edit a software set:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Software Sets** in the navigation pane to access the **Current Software Sets** pane.
3. Select the software set you want to change, and then click **Edit**. You can also right-click the software set, and then select **Edit** from the shortcut menu. The **Edit Software Set** dialog box opens.
 - If appropriate, add an item to the software set.
 - a. In the **Categories** list, select any category you want to include in the software set, and then click **Add**. You may select multiple categories and add them as a group if you want.
 - b. In the **Software Sets** list, select any executable you want to include, and then click **Add**. You may select multiple items and add them as a group if you want.
 - c. Click **Find Executable** to search for a file and then add it. Read [Searching For and Adding an Executable](#), page 239.
 - d. Click **Add File name** to manually add files by name. Read [Manually Adding a File Name to a Software Set](#), page 240.
 - If appropriate, remove an item from the software set: select the item in the **Selected** list, and then click **Remove**.
4. Click **OK**. The **Current Software Sets** pane becomes active.

Copying a Software Set

You can copy existing software sets to create new ones. This is useful if you already have a software set similar to what you need. Once you make the copy, you can edit the new software set by adding or removing executables, categories, or software sets to customize it.

For example, your company has just split the Technical Support department, creating a new Customer Service department. Management contacts you and explains the situation. Although the Customer Service group could use the same software set as Technical Support, there are a few differences in the executables they require—but not many.

Instead of completely defining a new software set, you copy the existing **Technical Support** software set, and then add and/or remove individual executables, categories, or other software sets to create a new rule for the new department. You also remove the tracking software specific to Technical Support. When you are done, you create a rule that blocks all executables not in the software set, and associate it with the new **Customer Service** client set.

To copy a software set:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Software Sets** in the navigation pane to access the **Current Software Sets** pane.
3. Select the software set you want to duplicate, and then click **Copy**. You can also right-click the software set, and then select **Copy** from the shortcut menu. The **Copy Software Set** dialog box opens, and contains a default name using the original name and the word **Copy**. For example, if the original rule has the word **Engineering** in the **Software Set name** field, the default entry is **Copy of Engineering**.
4. Accept the default name or enter a new one.
5. Edit the copy to meet your requirements. You can add or remove executables, software sets and categories as necessary.
6. Click **OK** to close the dialog box and return to the **Current Software Sets** pane.

The new software set appears in the software set list.

Deleting a Software Set

You can delete software sets when appropriate. This may occur as a result of departmental name changes or during efforts to simplify your policy. When you delete a software set, it does not affect the executables, categories, or software sets it contains: they are still available for inclusion in other software sets. The only exceptions are those executables that you identified manually.



NOTE

If you delete a software set, there is no way to recover it: if you find later that you deleted it in error, you must create it again from scratch.

Further, you cannot delete a software set that is currently used in a rule. Either delete the rule, or remove the software set from the rule, before deleting the software set.

To delete a software set:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Software Sets** in the navigation pane to access the **Current Software Sets** pane.
3. Select the software set you want to remove from the list, and then click **Delete**. You can also right-click the software set, and then select **Delete** from the shortcut menu. A confirmation message appears.
4. Click **Yes** to delete the software set.

Working in Software Sets

The information in this section describes processes that impact software sets when you add, edit, or copy them. Topics include:

- ◆ [Viewing Software Set Contents](#), page 238
- ◆ [Searching For and Adding an Executable](#), page 239
- ◆ [Manually Adding a File Name to a Software Set](#), page 240
- ◆ [Removing an Item from a Software Set](#), page 242

Viewing Software Set Contents

The **View Software Set** dialog box shows the contents of a software set. This can be useful if you are trying to determine which software sets can be added to other software sets to create a logical group.

For example, you decide to create a software set that contains executables you want to block. You can check a software set to make sure that it contains executables, categories, and other executables that you do, in fact, want to block.

One software set may contain any number of individual executables, categories, and other software sets. The **View Software Set** dialog box lets you drill down as far as necessary to fully review what a software set contains.

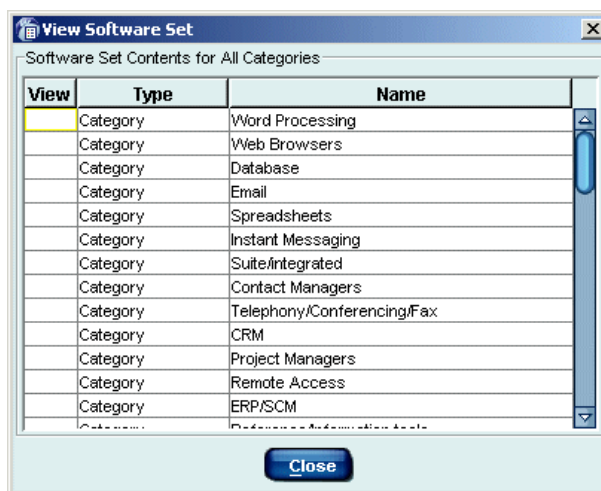
To view the contents of a software set:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Software Sets** in the navigation pane to access the **Current Software Sets** pane.
3. Click **Add** to add a new software set, or select a software set you want to modify and click **Edit**. The **Add/Edit Software Set** dialog box opens.

The **Add/Edit Software Set** dialog box shows all existing software sets in the **Software Sets** list on the left. The **Selected** list on the right shows any current entries. The **View** symbol appears for each software set in the dialog box, regardless of the list in which the software set appears.

4. Select the software set you want to see in greater detail, and then double-click the magnifying icon in the **View** column. The **View Software Set** dialog box opens, and shows the contents of the software set you chose.

If the software set includes other software sets, these also have a **View** symbol associated with them. You can click the symbol to drill down through the software sets as necessary. Each time you drill down, a new **View Software Set** dialog box appears.



View Software Set Dialog Box

5. When you are done viewing the contents, click **Close** to close the dialog box.

Searching For and Adding an Executable

You can search for executables found during inventories and add them to a software set. This lets you include executables that exist in Client Policy Manager Inventory Database to a software set.



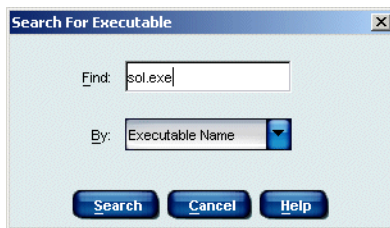
NOTE

An executable must exist in at least one inventory for you to add it to a software set using this method.

To search for and add an executable to a software set:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Software Sets** in the navigation pane to access the **Current Software Sets** pane.
3. Determine what to do to add an executable to the software set:
 - If you are creating a new software set, click **Add**.
 - If you are adding an executable to an existing software set, select the software set, and then click **Edit**.

4. When the **Software Sets** pane opens, click **Find Executable** to open the **Search for Executable** dialog box.
5. Enter the executable name, file name, or publisher's name in the **Find** field. You can enter partial strings: the search locates all entries with that string.
6. Click in the **By** field and select the appropriate entry. Your choices are:
 - **Executable Name**. The search checks only executable names.
 - **Publisher**. The search checks only publisher names.
 - **File name**. The search checks only file names.Be sure you select the correct parameters for the search. For example, if you type **word** because you want to add *Microsoft Word* to a software set, but select **Publisher** in the **By** field, your search returns empty.
7. Click **Search** to run the search. Executables that meet search parameters appear in the **Results** list and show the publisher, the application name, and the file name.
8. Select the executable or executables you want to add to the software set, and then click **Add Selected**.
9. Click **OK** to close the dialog box. The **Add/Edit Software Set** dialog box reopens.
10. Continue adding items to the software set or removing them as appropriate.
11. Click **OK** to close the **Add/Edit Software Set** dialog box. The **Software Sets** pane reopens.



Manually Adding a File Name to a Software Set

You can manually add file names to software sets. This lets you enter a file name and extension that identifies the file.



WARNING

Read the following before manually entering file names to any software set: there are security issues that may concern you.

Although Client Policy Manager lets you add executables by file name, it is better to use the **Find Executable** option, described in [Searching For and Adding an Executable](#), page 239. When you search for and find an application, Client Policy Manager identifies the file by the application signature, which stops employees from bypassing security by changing file names. If you enter the file name manually, users can change the name of the executable and launch it because Client Policy Manager does not check signature information.

If you **do** manually add file names to a software set, and then use the software set in a policy, be sure the associated rule is the last user-developed rule in the policy. This ensures that any possible rule that can take precedence over the manually identified file does so. Read [Rule Precedence](#), page 275.

**NOTE**

If you manually enter a file name that Websense, Inc. identifies as a critical function, Client Policy Manager protects client machines using the **System Files** rule, described in [System Files Rule](#), page 263. This functionality ensures that system executables continue running.

To manually add a file name:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Software Sets** in the navigation pane to access the **Current Software Sets** pane.
3. Determine what to do to add an item to the software set:
 - If you are creating a new software set, click **Add**.
 - If you are adding an executable to an existing software set, select the software set, and then click **Edit**.
4. When the **Add/Edit Software Set** dialog box opens, click **Add File Name** to open the **Add File Name** dialog box.
5. Enter the executable file name in the **File name** field. You must enter the file name *exactly* as it would appear in a directory, including extensions.
6. Click **Add** to add the file name to the software set.
7. Continue working in the dialog box as appropriate.

8. Click **OK** to close the **Add/Edit Software Set** dialog box. The **Software Sets** pane reopens.

Removing an Item from a Software Set

You can remove individual executables, categories, and other software sets from software sets in the **Add/Edit Software Set** dialog box. To do so:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Software Sets** in the navigation pane to access the **Current Software Sets** pane.
3. Select the software set you want to change, and then click **Edit**. The **Edit Software Set** dialog box opens.
4. Choose the item in the **Selected** list that you want to delete, and then click **Remove**. Client Policy Manager removes the individual executable, category, or software set from the list.
5. Continue removing items from the software set as appropriate.
6. Click **OK** to save your changes.

CHAPTER 13 | Working with Port Sets

Websense Enterprise Client Policy Manager provides subscribers with the ability to block ports that may be used during software launches. Software that may require network communications include Web browsers, instant messaging software, and Internet games, amongst others.

This function allows more flexibility than ever before, by helping to stop problems before they start. For example, Web browsers are typically set to communicate via port 80. A new virus, which is transmitted during Web browser use, resets the Web browser to communicate via port 8080. Because you have blocked access to port 8080 for Internet Explorer, allowing it to communicate only via port 80, the virus is stopped in its efforts to circumvent the security measures you have in place.

The Websense Port Sets functions provide you with the ability to group ports into a single set. This port set can then be included in a rule to control application launches that use network communications.

One port set may contain any combination of ports. The port set may contain:

- ◆ TCP ports
- ◆ UDP ports
- ◆ UDP Broadcast ports
- ◆ Other existing port sets

Prepopulated Port Sets

Websense prepopulates the **Current Port Sets** list with the port sets identified in the next table. Actual entries may vary slightly if Websense finds additional ports of concern for the port set.

Port Set	Description and Default Contents
All Ports	Identifies the entire range of potential ports (0 to 65536).
Email	Identifies ports that are most often accessed by email software.
Enterprise Connectivity	Identifies ports that are most often accessed by software used for internal communications.
Productivity Ports	Identifies ports that are most often used by applications that are commonly used in business.
TCP High	Identifies ports that are “unreserved” and do not require administrator or root privileges to use. The default ports are from 1025 to 65535.
Worldwide Web	Identifies ports that are most often used by products that can be used to browse the Internet.

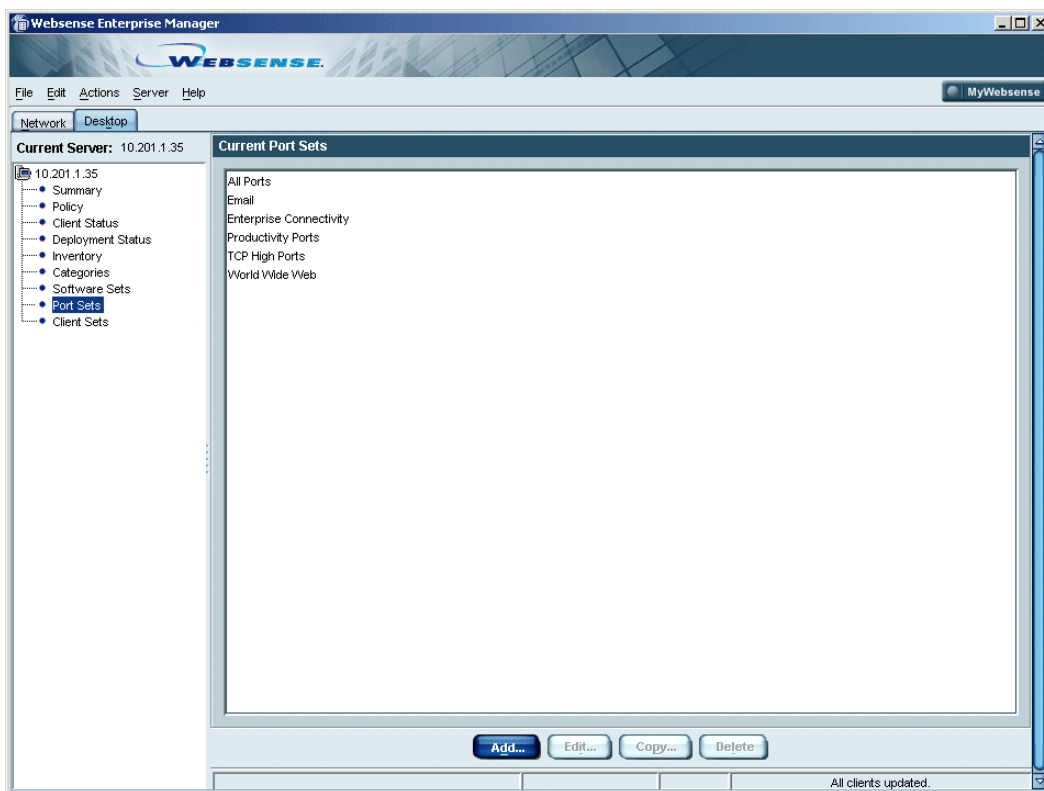
Accessing the Current Port Sets Pane

Port sets allow you to group ports for controlling network access by software applications. You use port sets in CPM rules to control which ports software can or cannot access.

To access the **Current Port Sets** pane:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Port Sets** in the navigation pane to access the **Current Port Sets** pane.

The **Current Port Sets** pane lists all existing port sets in alphabetic order.



Current Port Sets Pane

Managing Port Sets

You can add or edit port sets at any time to better manage application launches that require network access. You can also copy and delete port sets if necessary. When CPM Server handles rules, all ports are processed by the associated settings in the rule.

There are two primary ways to populate port sets:

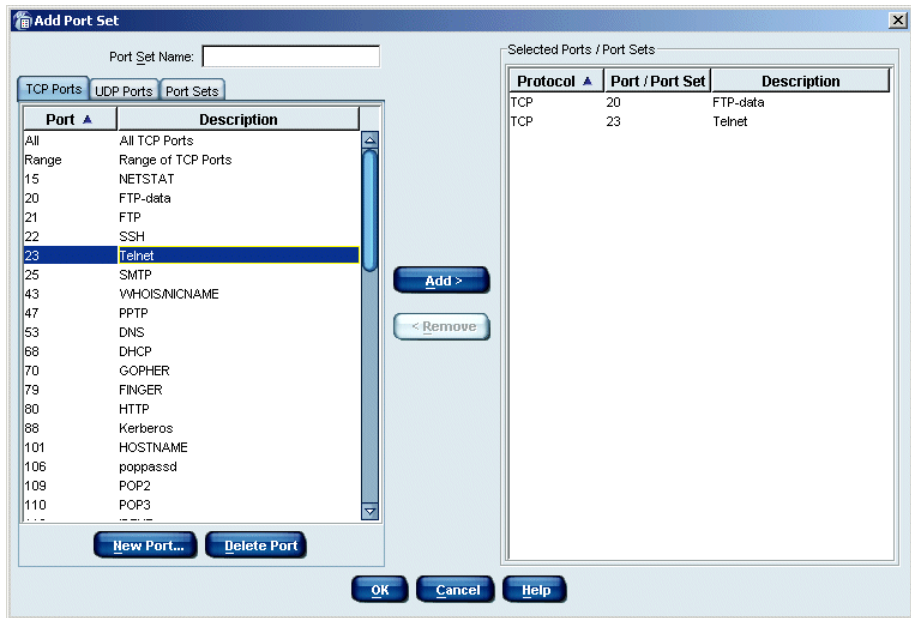
- ◆ You can add all TCP and/or all UDP ports as single groups.
- ◆ You can add TCP and/or UDP ports individually.
- ◆ You can add existing port sets individually.

Once a port is included in a port set, you cannot add it again to that same port set. For example, if you include the **All TCP** selection in a port set, then try to insert a single TCP port into the same port set, Websense Enterprise Manager displays an error message. You need to remove the **All TCP** entry before you can insert an individual TCP port to the port set.

Adding a Port Set

To add a port set:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Port Sets** in the navigation pane to access the **Current Port Sets** pane.
3. Click **Add**. You can also right-click anywhere in the **Current Port Sets** list, and then select **Add** from the shortcut menu. The **Add Port Set** dialog box opens.



Add Port Set Dialog Box

4. Enter an appropriate name in the **Port Set Name** field at the top of the dialog box.

5. Click a tab to view ports that are available for selection:
 - Click the **TCP Ports** tab to view TCP port selections.
 - Click the **UDP Ports** tab to view UDP port selections.
 - Click the **Port Sets** tab to view port sets that are already defined.
6. Select the port or port set you want to add to the **Selected Ports** list, and then click the button with arrows that point to the right. The port or port set moves to the **Selected Ports** field. For a list of individual ports that Websense identifies for you, read [Appendix C: Websense Port List](#), page 329.
7. If you do not see a port that you need, you can add it manually to the list you are currently working in. Read [Adding a Port to the Port List Manually](#), page 247.
8. You can add a range of ports if appropriate. For details, refer to [Adding a Range of Ports to a Port Set](#), page 249.
9. Continue adding any necessary ports to the **Selected Ports** list.
10. Click **OK**. The **Current Port Sets** pane becomes active and lists the new port set.

The port set you have defined can now be added to a rule. For details, refer to [Adding a Rule](#), page 288.

Adding a Port to the Port List Manually

While Websense provides a list of commonly used ports for inclusion in port sets, there are ports not identified in the default list of ports. You can manually add any port in the range between 1 and 65535.

By limiting access to ports that are not the default selection for an application you can reduce opportunities for malicious code to infect your system. For example, your organization may decide that Internet browsers must use port 1500. By default, Internet browsers often use TCP 80 or TCP 443. By changing the default, and limiting the application to a single port, malicious code finds it difficult to propagate.

**IMPORTANT**

If you force an application to use ports other than the default ports, you may need to modify information at the application level, in addition to defining it in CPM. If you have questions, check help for the application or contact the application publisher for assistance.

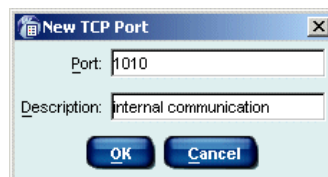
To provide control for Internet browser access to port 1500, you would need to manually add it to the **TCP Ports** list.

To manually add a port to either the **TCP Port** or **UDP Port** list:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Port Sets** in the navigation pane to access the **Current Port Sets** pane.
3. Either create a new port set by clicking **Add**, or locate and select the port set you want to change, and then click either **Edit** or **Copy** as appropriate.

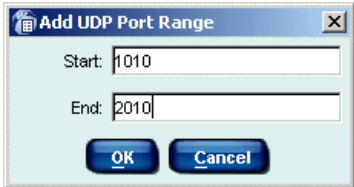
You can also right-click anywhere in the **Current Port Sets** list, and then make your selection from the shortcut menu. The **Port Set** dialog box opens.

4. Click a tab to view ports types:
 - Click the **TCP Ports** tab to view TCP port selections.
 - Click the **UDP Ports** tab to view UDP port selections.
5. Click the **New Port** button associated with the **TCP Port** or **UDP Port** tabs. The **Add TCP Port** or **Add UDP Port** dialog box opens.
 - a. Enter the port identification in the **Port** field.
 - b. Enter a description for the port in the **Description** field.
 - c. Click **OK**. The port name appears in the associated port list.
6. To add the new port to the **Selected Ports** list, locate the new entry and click **Add**.
7. Continue working with the port set as appropriate.
8. When you are done working with the port set, click **OK**. The **Current Port Sets** pane becomes active.



Adding a Range of Ports to a Port Set

You can add a range of ports to a port set if you want. This makes it easy to add a large number of ports at one time. You can add a range of TCP ports or a range of UDP ports.

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Port Sets** in the navigation pane to access the **Current Port Sets** pane.
3. Either create a new port set by clicking **Add**, or locate and select the port set you want to change, and then click either **Edit** or **Copy** as appropriate. You can also right-click anywhere in the **Current Port Sets** list, and then make your selection from the shortcut menu. The **Port Set** dialog box opens.
4. Click a tab to view ports types:
 - Click the **TCP Ports** tab to view TCP port selections.
 - Click the **UDP Ports** tab to view UDP port selections.
5. Double-click the **Range/Range of TCP Ports** or **Range/Range of UDP Ports** entry. The **Add TCP Port Range** or **Add UDP Port Range** dialog box opens.
 
6. Identify the appropriate range:
 - a. Enter the first number of the range in the **Start** field. This value must be smaller than the value you enter in the **End** field.
 - b. Enter the last number of the range in the **End** field. This value must be greater than the value you enter in the **Start** field.
 - c. Click **OK** to close the dialog box.
7. Continue adding or removing other ports, port sets, or ranges as necessary.
8. When your changes in the **Add/Edit/Copy Port Sets** dialog box are complete, click **OK**.

Deleting a Port from the TCP or UDP Port List

To help maintain a functional list of TCP or UDP ports you may find it advantageous to delete a port from the **TCP Port** or **UDP Port** list. For example, port 443 is often used by HTTPS traffic for Web browsers.

However, your company already uses port 443 for some other application. You can delete the entry for port 443, and then add it again to show what it is.



IMPORTANT

You cannot delete a port that has been included in the **Selected Port** list, or any port set that has already been defined. You must first remove the port from the **Selected Port** list or the existing port set, and then delete it.

You also cannot delete groups of ports. This includes the Websense default groups: **All TCP Ports**, **All UDP Ports**, and **All UDP Broadcasts**; it also includes any groups of ports that your organization has grouped using a range of port numbers.

To remove a port from the **TCP Ports** or the **UDP Ports** lists in the **Add/Edit/Copy Port Set** dialog box:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Port Sets** in the navigation pane to access the **Current Port Sets** pane.
3. Either create a new port set by clicking **Add**, or locate and select the port set you want to change, and then click either **Edit** or **Copy** as appropriate. You can also right-click anywhere in the **Current Port Sets** list, and then make your selection from the shortcut menu. The **Port Set** dialog box opens.
4. Click a tab to view ports types:
 - Click the **TCP Ports** tab to view TCP port selections.
 - Click the **UDP Ports** tab to view UDP port selections.
5. Select the port you want to remove in either the **TCP Ports** or the **UDP Ports** list.
6. Click **Delete Port**. This removes the port from any **Port Set** dialog box you may access in the future.
 - You can delete an individual port only if it is not used in a port set. If it is used in a port set, you will receive an error message informing you that it is used.

- You cannot delete groups of ports. This includes Websense default groups of ports, and ports that your organization adds using a range of port numbers. An error message appears if you try.
7. Continue working with the port set as appropriate.
 8. When you are done working with the port set, click **OK**. The **Current Port Sets** pane becomes active.

**NOTE**

To delete a port set from the list of existing port selections, you must delete it from the **Current Port Sets** list. For details, refer to [Deleting a Port Set](#), page 253.

Editing a Port Set

You can edit a port set at any time. This allows you to quickly change how Client Policy Manager handles application launches when they attempt to use a specific port during launches.

For example, you have previously allowed Internet Explorer to launch via port 80 and set this with a rule that permitted a port set you called Browser. Now, however, the company wants to restrict Internet Explorer to port 12405.

You edit the Browser port set by removing port 80, and adding port 12405. As soon as you save the change to the port set, CPM Server sends the CPM policy to machines. As a result, Internet Explorer would now be permitted only on port 12405.

To edit a port set:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Port Sets** in the navigation pane to access the **Current Port Sets** pane.
3. Locate and select the port set you want to change, and then click **Edit**. You can also right-click anywhere in the **Current Port Sets** list, and then select **Edit** from the shortcut menu. The **Edit Port Set** dialog box opens.
4. If appropriate, change the port set name in the **Port Set Name** field at the top of the dialog box.

5. Add items to the port set as appropriate, using any of the following methods:
 - To add a port that has been identified by CPM, scroll through the **TCP Ports** or the **UDP Ports** list, locate the port you want to include in the port list, and then click **Add**.
 - To add a port manually, read *Adding a Port to the Port List Manually*, page 247.

As you add TCP or UDP ports to the **Selected Ports** list, the entry moves to the **Selected Ports** field.
6. Remove items from the port set if appropriate by highlighting the port information in the **Selected Ports** field, and then clicking **Remove**. For complete details, read *Deleting a Port Set*, page 253.
7. When you are done editing the port set, click **OK**. The **Current Port Sets** pane becomes active.

Copying a Port Set

You can copy a port set and then modify it, if an existing port set is close to your requirements when you need a new one.

For example, your company has identified that several software products are set to use the same port, and some employees have experienced conflict when trying to launch these products. You already have a port set that includes the ports where this conflict occurs, and have used it in a rule that permits launches at these ports.

Now, to better manage the network access, you determine that you need to permit these ports for one product, while blocking them for the other. You copy the original port set, change the name, then use the newly copied port set in a rule that blocks network access for the other product.

To copy a port set:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Port Sets** in the navigation pane to access the **Current Port Sets** pane.
3. Locate and select the port set you want to duplicate, and then click **Copy**. You can also right-click anywhere in the **Current Port Sets** list, and then select **Copy** from the shortcut menu. The **Copy Port Set** dialog box opens.
4. Change the default port set name in the **Port Set Name** field at the top of the dialog box. The default is **Copy <Port Set Name>**.

5. Add items to the copied port set as appropriate, using any of the following methods:
 - To add a port that has been identified by CPM:
 - a. Scroll through the **TCP Ports** list or the **UDP Ports** list.
 - b. Locate the selection you want to add to the port list.
 - c. Click **Add**.
 - To manually add a TCP or UDP port
 - a. Click the **Add Port** button associated with the port type.
The **Add TCP Port** or **Add UDP Port** dialog box opens.
 - b. Enter the port identification in the **Port** field.
 - c. Enter a description for the port in the **Description** field.
 - d. Click **OK**.
The port name appears in the **Selected** list.

As you add TCP or UDP ports to the **Selected Ports** list, the entry moves to the **Selected Ports** field. A list of default entries in the TCP and UDP Ports list can be found in [Appendix C: Websense Port List](#), page 329.
6. Remove items from the copied port set if appropriate by highlighting the port information in the **Selected Ports** field, and then clicking **Remove**.
7. When you are done modifying the copied port set, click **OK**. The **Current Port Sets** pane becomes active and lists the new port set.

Deleting a Port Set

You can delete a port set whenever necessary. This allows you to maintain a list of active port sets and removing those no longer useful. To delete a port set:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Port Sets** in the navigation pane to access the **Current Port Sets** pane.
3. Select the port set you want to remove, and then click **Delete**. You can also right-click anywhere in the **Current Port Sets** list, and then select **Delete** from the shortcut menu. A confirmation message appears.

If the port set appears in a rule or in another port set, you cannot delete it; you need to modify or delete the rule or other port set first. Once that is done, you can delete the port set without further complications.

4. Click **Yes** to delete the port set from the **Current Port Sets** list.

CHAPTER 14 | Working with Rules

Rules are the core of Client Policy Manager processing as they define what executables are available to specific users and machines. During initial configuration, you start with a basic set of rules, and refine them as necessary.

Each rule identifies a series of checks that Client Agent processes whenever a machine or an employee tries to launch applications and/or access ports. Depending on the rule, Client Agent may block or permit launches, block or permit network access, and log information--or not.

Understanding Rules

Websense, Inc. provides a set of basic rules that permit most application launches while blocking software that may lead to security concerns. Even if you do not define custom rules immediately, Client Policy Manager adds security and value with this basic rule set. The Websense rules are fully described in *Websense Rules*, page 262.

When you add a custom rule, CPM sets all values in new rules to default values, which allows all users to access all applications, access any port, and log everything.



New Rule with Default Settings

As you configure the rule, you tighten control parameters. You can add rules that range from extremely permissive to extremely restrictive.

Settings in the rule define:

- ◆ When the rule is in effect. Choices are always Active, Never Active, or active based on communications between CPM Server and Client Agent. For details, refer to *Status Settings*, page 256.
- ◆ How Client Agent responds to application launch requests. For details, refer to *Software Launch Control*, page 257.

- ◆ How Client Agent responds to network access attempts. For details, refer to *Network Access Control*, page 259.
- ◆ What information is logged. For details, refer to *Logging*, page 260.

You may add any number of rules to the policy. Be careful, however: the more rules Client Policy Manager must process, the more complex maintenance becomes. Generally, organizations add between 3 and 20 custom rules.

Status Settings

The first part of a rule defines when that rule is active. Options include:

- ◆ **Always active.** The rule always impacts machines and users in the client set. This selection is often found for rules that limit legal liability and improve desktop security.
- ◆ **Never active.** The rule never impacts machines and users in the client set. This selection is often found when companies are testing CPM policy implementation. Administrators create the rules, setting the status as Never active, then activating the rules one at a time to test functionality.
- ◆ **Connected.** The rule impacts machines and users in the client set only when the machine is able to communicate with CPM Server. When the machine cannot communicate with CPM Server, the rule does not impact the machine or user.
- ◆ **Disconnected.** The rule impacts machines and users in the client set only when the machine is not able to communicate with CPM Server. When communications are possible, the rule does not apply.

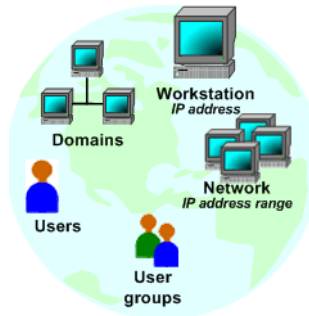
The **Connected** and **Disconnected** selections allow you to define rules that affect the same machines and users differently, depending on the communication status with CPM Server. For example:

- ◆ The Sales department staff often visit trade shows and customers. You want them to be able to access games for entertainment while waiting at airports, and instant messaging for communications with their families and friends.
You define a rule that permits these activities when the machines are not able to communicate with CPM Server.
- ◆ Field technicians are away from the office frequently. You have had problems in the past with unauthorized applications being installed. You define a rule that blocks `setup.exe` files when the machines cannot communicate with CPM Server.

Software Launch Control

The second part of a rule identifies what happens when a software launch is requested. The request may originate with the machine or with the user. This part of the rule identifies:

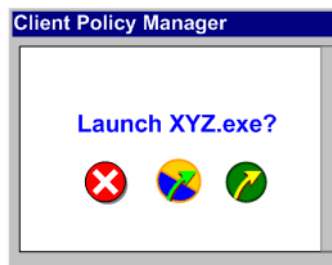
- ◆ Which machines and/or users are impacted, identified by the client set. Client sets may include any combination of workstations, IP addresses, domains, user, and/or user groups.



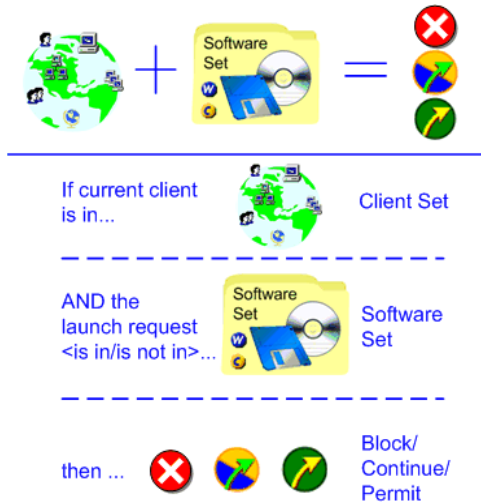
- ◆ Which software is impacted, identified by the software set. Software sets may include any combination of executables, Websense or custom categories, file names, and/or other software sets.



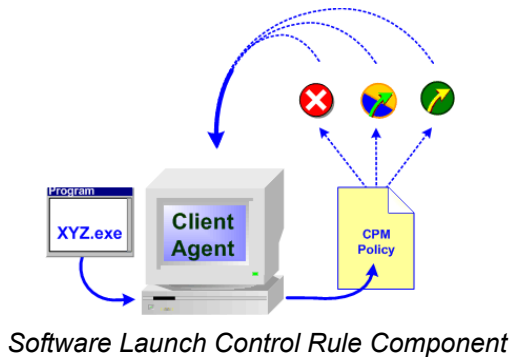
- ◆ What happens when a launch request occurs, identified by the action. Possible actions include block, continue, or permit.



When Client Agent receives a software launch request, it locates the first true rule, and then checks parameters that impact the launch request.



When Client Agent checks the CPM policy, it is able to quickly determine how it should handle each software launch. It scans the available data to find the first true statement that impacts the machine, the user, and the software.

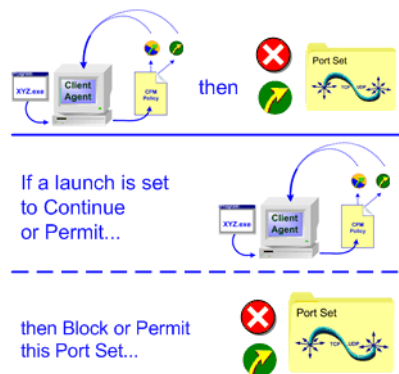


Network Access Control

The third part of a rule identifies network access rights. Rules with network access settings add an additional functionality to the launch control equation by permitting or blocking specific ports.

This portion of the rule is directly impacted by the launch control setting:

- ◆ If the application launch is blocked, you cannot define network access.
- ◆ If the application launch is permitted or set to continue, you can permit or block network access.



Network Access Parameters

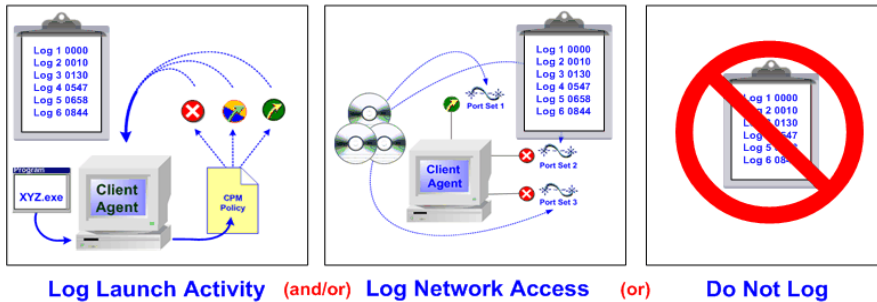
For example, you permit launches for the Websense Web Browsers category. When you set the network access options, you decide to block network access if the application uses any port besides one that you specifically permit.

Because viruses or other malware may attempt to use ports other than the default port 443 that the browser uses to communicate, you decide that port 443 is the only port that browsers may access. Thus, you permit network access for all employees, but only if the launch uses port 443. If the launch tried to access any other port, Client Agent blocks access.

However, if you have a group that should not have Internet access and set a rule to block the Web Browser access, you would not be able to set any network control. This occurs because CPM Server never resolves blocked launches far enough to request port access.

Logging

The fourth part of an active rule defines logging. You can set logging for software launch activity, network access activity for rules that are set to permit or continue launches, or both. You can also completely disable logging. This lets you determine whether or not CPM Server should save the information to CPM Log Database.



If you do not log data, reports will not include those details. The ability to enable and disable logging lets you minimize the impact on valuable system resources.

For example, you create a software set that includes all the software necessary for day-to-day business operations including word processors, spreadsheets, database software, email software, and so forth.

When you add a rule using that software set, you decide not to log the information, since these executables do not lead to security or legal liability risks, nor do they lead to any productivity loss. Because you are not logging the information, your decision reduces the size of CPM Log Database.

Alternately, you add a rule that uses a software set containing software that consumes large amounts of bandwidth. You decide to log information, giving CPM Reporter users the ability to monitor these launches and create tighter controls.



NOTE

Carefully analyze your requirements before disabling logging. It is usually better to log information than lose data that may be useful.

When you select any logging option, it impacts only those actions that meet every parameter in the associated rule. If a rule does not identify logging activity for a particular application or port, Client Agent searches until it finds a rule that does.

For example, you create a rule that permits employees to launch Web browsers, lets the software access port 443, and does not log launch or network access information. This is the only custom rule you add. You also change the network setting in the Global rule to block all ports.

As long as Internet Explorer launches and accesses port 443, logging does not occur. However, if an employee launches Internet Explorer, and Explorer tries to access port 1010 (which is not permitted), Client Agent searches the policy and finds that the Global rule is the only other rule that applies. Using this rule, Client Agent permits Internet Explorer to launch, but blocks port 1010, and then logs both the application launch and the network attempt.

Logging User Data

CPM automatically identifies the actual *user* who requests a software launch or port access, and identifies logged on users, system users, and process users. This recognition occurs automatically for any launch request and port access attempt: it does not require specific configuration on your part. By identifying process users, system users, and logged on users, this functionality helps you analyze launch and port access attempts:

- ◆ If an employee is logged on and requests a software launch, CPM identifies the logged on employee as the user.
- ◆ If one software program tries to launch another program, for example, using “Run As,” the requesting process/software is identified as the user.
- ◆ If the process is part of the operating system, CPM identifies the system as the user.

In CPM Reporter and Explorer for CPM, the user identified in reports will be the actual user, not the logged on user. For example, depending on how a launch or access request is generated, you could see a number of users identified for one machine:

- ◆ Machine 1/Logged on User
- ◆ Machine 1/System User
- ◆ Machine 1/<Anti-virus “process user”>

These details can help identify normal and/or abnormal software behavior and calls, and may help determine additional control.

Logging Machine Data

CPM Reporter and Explorer for CPM reports identify machines by machine name. This occurs even if you deploy Client Agent using IP addresses. Internal processes in CPM check for, and then use, the machine name to add clarity to reports.

Websense Rules

Websense includes five default rules with Client Policy Manager, in the following order:

- Rule 1** -The **Outbreak** rule is invisible, and takes effect only if you add a file name to the **Outbreak** dialog box. CPM Server processes the **Outbreak** rule before any other rules. For complete details, refer to [Emergency Outbreak Rule Processing, page 118](#).
- Rule 2** -The **System Files** rule is always active, is always the first rule in the list, and cannot be disabled, edited, moved, or deleted. For more information, refer to [System Files Rule, page 263](#).
- Rule 3** -The **Mass Mailing** rule allows you to reduce or eliminate the impact of malware that uses infected machines to send emails. The Mass Mailing rule does not impact the CPM policy until you activate it. The rule can be disabled, moved, edited, or deleted. For more details, refer to [Mass Mailing Rule, page 264](#).
- Rule 4** -The **Harmful Software** rule blocks the Hacking, Malware, and Spyware categories by default. For more information, refer to [Harmful Software Rule, page 264](#).
- Rule 5** -The **Lockdown** rule does not take effect until such time as one or more lockdowns are applied at client machines. The rule can be disabled and moved. It cannot be directly edited or deleted. For more details, refer to [Lockdown Rule, page 265](#).
- Rule 6** -The **Global** rule permits all applications to launch, and allows access to all ports. You can quickly change the network access setting to Block (Zero Day Response), and create a last line of defense, stopping network access for any application that is not specifically identified by previous rules in the list. For details, refer to [Global Rule, page 266](#).

These rules provides subscribers with the ability to monitor application launch requests and track port access, even if they do not develop a custom set of rules immediately. For example, you can install Client Policy Manager, study employee software launches, and then identify custom rules that make the most sense for your organization.

Emergency Outbreak Rule

Although there is not a visible Emergency Outbreak Rule in the Policy pane, Client Agent processes any entries you have made in the **Outbreak** dialog box when it checks the policy. As soon as an entry is made in the Emergency Outbreak Rule, that information is passed between all machines that are online and running Client Agent. The same details are added to the CPM Policy and distributed to machines when they contact CPM Server the next time.

For example, you enter data in the Outbreak dialog box, and all machines that are online receive the information via peer-to-peer communications. At the same time, several salesmen are on trips, and their machines cannot receive the latest outbreak data. When the salesmen return to the office, they plug the laptops into the network, and Client Agent contacts CPM Server. CPM Server sends the most recent version of the CPM policy, which includes the changes to the Emergency Outbreak Rule.

System Files Rule

Websense, Inc. includes the System Files rule as one of the permanent rules that impact your CPM policy. This rule contains the Websense categories that must be permitted for critical system operations. The only setting you can change is logging.

Websense, Inc. automatically populates the System Files rule using the System Files software set, which contains the Critical Functions - Never Block category. As a result, the System Files rule contains the following categories:

- ◆ File Management – Never Block category
- ◆ Infrastructure – Never Block category
- ◆ Operating Systems – Never Block category

For more information, read [Working with Categories](#), page 201, and [Predefined Software Sets](#), page 226.

The System Files rule is set to permit all ports for network access and uses the All Ports port set.



Harmful Software Rule

When you install Client Policy Manager, the CPM policy contains the Harmful Software rule. This provides an immediate layer of security for machines running Client Agent.

The Harmful Software rule automatically blocks any software launches associated with these Websense categories:

- ◆ Hacking
- ◆ Malware
- ◆ Spyware
- ◆ Keyloggers

The rule may be disabled, edited, moved, or deleted.



Mass Mailing Rule

When you install Client Policy Manager, the **Rules** pane includes the Mass Mailing rule. The rule allows you to protect machines from worms and other malware that infect machines and/or networks, and then use them to send emails. You must manually activate the rule to include it in your CPM policy.

Once you activate the Mass Mailing rule, by default it:

- ◆ Is always active, whether or not the machine running Client Agent is in communication with CPM Server
- ◆ Impacts all machines running Client Agent
- ◆ Permits all Uncategorized software file launches
- ◆ Blocks access to port 25

You can edit, copy, move, or delete the Mass Mailing rule.



Lockdown Rule

When you install Client Policy Manager, the policy includes a Lockdown rule that cannot be deleted. The rule is not populated until you specify a lockdown for a given machine.

Once populated, the Lockdown rule automatically blocks any executables excluded by inventory with an Inventory Lockdown or that were not present when an Express Lockdown was established. For details, refer to [Chapter 9: Applying Lockdowns](#).



When you use lockdowns:

- ◆ The Lockdown rule does not impact a machine until you apply a lockdown for that machine.
- ◆ The Lockdown rule does not allow any network access or port sets as it is set to block launches. These settings cannot be changed.
- ◆ Once you lockdown a machine, Client Policy Manager automatically places the lockdown into the Lockdown rule. As a result, the lockdown client set and the software set are automatically generated by Client Policy Manager.
- ◆ The Lockdown rule contains both Inventory Lockdown and Express Lockdown. In the order of rule processing, Inventory Lockdown has precedence over Express Lockdown.
- ◆ The Lockdown rule initially appears beneath the Harmful Software rule and above the Global rule, but you can move the rule if appropriate. You can also enable and disable it, and define logging. You cannot delete the rule.

Global Rule

Websense, Inc. includes the Global rule with your Client Policy Manager installation. As you develop rules, they take precedence over the Global rule. You cannot delete or disable the Global rule.

The Global rule always appears at the bottom of the sequence of rules, and is always the last rule CPM Server processes when generating a policy. The rule is set to permit all applications and permit all network access. You can define network access parameters and logging.

By changing the network access settings to Block All Ports, you can enable Zero Day response. This setting permits applications to launch, but does not allow the applications to access any port.

Websense, Inc. recommends the following use of the Global rule when defining your policy:

- ◆ During evaluation and analysis periods, keep the default settings for the Global rule. This allows you to monitor launches and network access, and thus better understand changes that are suitable for your organization.
- ◆ During rule testing, block network access for all ports. This creates a “Zero Day response” functionality, where files not explicitly addressed by previous rules are allowed to launch but cannot access the network. If you find the Global rule blocks critical applications, you will need to create a rule that specifically permits these applications.
- ◆ When you are satisfied with your list of rules, continue blocking ports in the Global rule. By keeping the Zero Day response functionality, you can provide ongoing security for your machines.



Connected and Disconnected Rules

You can define rules that are enabled or disabled, based on the availability of communications with CPM Server. This allows Client Agent to respond differently, based on this connection status. One rule may impact a machine and/or user when communications are intact, while other impacts a machine and/or user when Client Agent cannot communicate with CPM Server.

For example, a high school installs Client Agent on student laptops. The school wants to block instant messaging while students are on campus and able to communicate with CPM Server, but does not have any problems with students using instant messaging when they are off-site.

The system administrator creates a rule that blocks instant messaging when a laptop is able to contact CPM Server. If the laptop is connected to the Internet from home or a coffee house, students can access instant messaging applications without any restrictions.

You could create a rule that:

- ◆ Blocks instant messaging only when the machine is able to communicate with CPM Server.
- ◆ Permits instant messaging only when the machine is not able to communicate with CPM Server.

Both rules have the same impact on how Client Agent responds. Instant messaging will be blocked when the machine is able to communicate with CPM Server, and will be permitted when the machine is unable to communicate with the server.

You can layer connected and disconnected rules to fine-tune control. For example, the school decides that only students receiving high marks for effort and deportment can access instant messaging when their laptops are not communicating with CPM Server. The system administrator creates the following two rules to implement this:

Rule 1 -Blocks instant messaging for all students when laptops can communicate with CPM Server.

Rule 2 -Always blocks instant messaging for students who are not achieving high marks in effort and deportment.

Recommended Rules

As you develop your policy, you create a series of rules to meet business goals. As part of your policy, Websense, Inc. recommends using the following rules in any rule set you create:

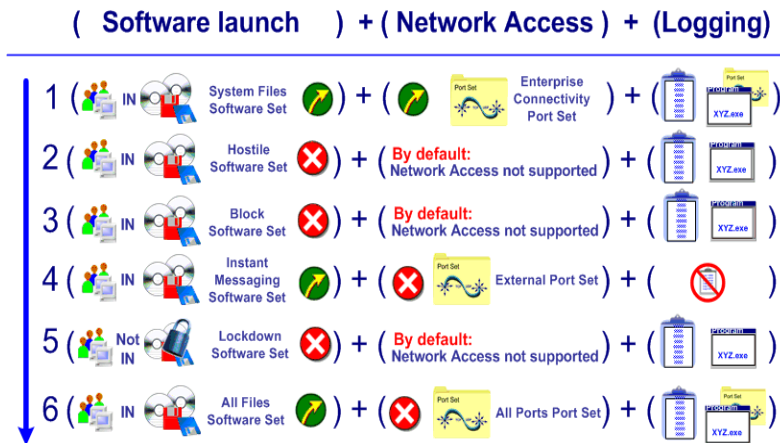
Rule 1 -A custom rule impacting only system administrators that permits all applications and all network ports. This allows system administrators to perform necessary maintenance and upgrades at machines without conflicting with the CPM policy for that machine.

Rule 2 -Enable the Mass Mailing rule.

Rule 3 -Set the Global rule to permit all launches and block all network access. This serves as a Zero Day response, as potentially dangerous applications cannot access the networks.

Understanding the CPM Policy

When Client Agent checks the CPM policy, it begins with the first rule in the policy and moves to the last, following the order shown in the **Rules** list. For each rule, Client Agent checks if the machine or user is impacted by the rule. When it finds a rule that applies to the machine and/or user, the server checks the rule and then enforces the indicated action.



Rules Processing Example

In the above example, the rules—and the results of these rules—are:

Rule 1 -The Websense System Files rule permits all executables in the System Files category. The rule permits access to all ports.

Rule 2 -The Emergency Outbreak Rule is hidden in the Policy pane, but blocks any files using the file names that you and other system administrators insert in the **Outbreak** dialog box.

Rule 3 -The Websense Harmful Software rule blocks launches of any software in the Websense *Hacking*, *Malware*, and *Spyware* categories.

Rule 4 -A custom rule blocks all executables in the **Games** and **Adult** categories.

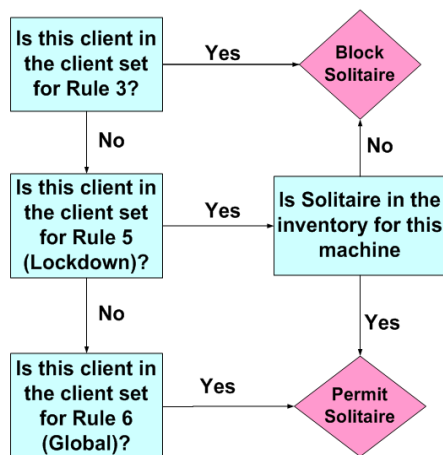
Rule 5 -A custom rule you design permits all media player launches, but blocks all port access.

Rule 6 -The Lockdown rule permits only executables discovered during inventory for machines that are locked down.

Rule 7 -The Websense Global rule permits all executables and blocks all ports, providing a Zero Day response.

Depending on the software sets included in the rules, an application signature may appear any number of times in the CPM policy. Client Agent enforces the first true entry it finds.

For example, John is in the Finance group, and wants to play *Solitaire*. In the above policy, Rule 3, 5, and 6 have the potential of impacting the launch, as shown in the next diagram.



Client Agent Decision Flow

Policy Updates

After the first CPM policy download, which occurs when you first install Client Agent, CPM Server downloads new policy data whenever information changes in the:

- ◆ Outbreak list
- ◆ Websense Enterprise Master Database
- ◆ Custom categories you create
- ◆ Generated software sets, which are based on inventory
- ◆ Rules

CPM Server checks the version information from Client Agent, then checks the policy stored at the server. Only changed information is sent to Client Agent, making policy updates very fast and requiring little bandwidth.

Developing the CPM Policy

The CPM policy is extremely flexible, and allows you to define software control that fits with daily business practices. Before you create your policy, you should determine what you want Client Policy Manager to do for your organization. There are several ways that you can approach this task, depending on your goals.

For the purposes of demonstrating possible goals, this section identifies each goal as a separate entity. In reality, you can combine any of these goals to customize your approach to software and network access control and monitoring.

Goal: Zero Day Response

With the impact of viruses and other malware being greater today than ever before, “Zero Day response” is rapidly moving to the forefront of corporate security requirements. CPM is able to fulfill this need with a simple change to the Global rule, which is always the last rule that Client Agent processes when a launch attempt takes place. To enable Zero Day response, simply change the network access setting in the Global rule to Block when you finalize your list of rules.

If the Zero Day response function is set, and no other rules apply to the network access request, Client Agent permits applications to launch but does not permit network access. This provides immediate and continuous control of applications that may cause harm to machines and/or your network.



IMPORTANT

Websense, Inc. strongly encourages customers to implement the Zero Day response functionality whatever the ultimate goal is. This single change to the default CPM policy provides a valuable layer of extra security, and can save your organization time and money.

Goal: Security

If you want a completely secure policy, you should run inventories on all machines where you have installed Client Agent, and then use the inventories to lock down the machines. Websense, Inc. also recommends activating the Mass Mailing rule.

If your network includes shared machines or logon servers, you **must**:

1. Run inventories at those machines.
2. Generate software sets from the inventories.
3. Use the generated software sets to create a rule that permits executables in the Server/Shared software set, and allow it to access all ports.
4. You **must** place this rule above the Lockdown rule for it to have any impact.

For step-by-step instructions for running an inventory at a shared machine, and then using it to generate a software set, read [Generating a Software Set for Shared File Machines](#), page 165.

Goal: Productivity

If you want a CPM policy that improves employee productivity, you can create software sets and populate them with categories. When you do so, you can permit or block all executables within a category and fine-tune control as necessary.

You can create any number of rules to block or permit launches using this method. For example, you create a software set that includes all executables in the Communications category and use it in a rule that permits launches on a

limited number of ports. You also create a software set that includes the Entertainment category and Adult, Gambling, Games, and Screen Savers subcategories, and then use it in a rule that blocks all launches.



WARNING

A CPM policy developed using categories in the software sets does not provide a last line of defense as does a policy that includes lockdowns and/or the Zero Day response setting in the Global rule. As a result, employees can launch any executable that is uncategorized. Check [Goal: Security and Productivity, page 272](#), for a more secure approach.

Goal: Security and Productivity

If you want a CPM policy that provides security and improves employee productivity, combine lockdowns and rules that block and permit launches based on categories. This gives you the best of both worlds.

For example, you create a policy that contains:

Rule 1 -A rule for all machines running Client Agent that blocks the Entertainment category, which includes the subcategories Adult, Gambling, Games, and Screen Savers.

Rule 2 -A rule that permits the Instant Messaging category for the Technical Support department.

Rule 3 -The Mass Mailing rule, which is enabled and blocks port 25.

Rule 4 -Lockdowns for all machines running Client Agent.

Rule 5 -The Global rule, which is set to block all network access attempts (Zero Day response).

This combination of rules still provides security while adding flexibility.

In this scenario, any rule that blocks launches by category does not have a negative impact on the security provided by the lockdown. However, if you include rules that permit launches by category, the end result could weaken the last line of defense provided by the lockdown: it is theoretically possible that a permitted executable could run even if it has been affected by a virus. In most environments, however, a policy that combines lockdowns and category-based rules is valuable and the security trade-off is very small.

Goal: Flexible CPM Policy

If you want the CPM policy to control applications differently, depending on whether Client Agent is able to communicate to the CPM Server or not, use the Connected and/or Disconnected selections in the **Active Status** drop down list to create a set of rules that identifies differences in the policy. This allows you to define a policy that behaves one way when communications with CPM Server are intact, and another when the machine cannot communicate with CPM Server.

For example, you create a policy that contains:

- ◆ A rule for all machines running Client Agent, set to the **Always Active** status. The rule blocks the Adult and Gambling categories at all times.
- ◆ A rule for all machines running Client Agent, set to the **Connected** status. The rule blocks the Games and Instant Messaging categories when the machine is able to communicate with CPM Server. When the machine cannot communicate with CPM Server, games and instant messaging applications can be launched normally.
- ◆ The Global rule set to block all network access attempts (Zero Day response).

In this scenario, the combination of rules provides flexibility based on network connectivity, while still enhancing employee productivity.

Identifying Access Levels

Because the CPM policy is so flexible, it is a good idea to determine in advance which groups have special access requirements. By preplanning your approach, you can set a policy quickly.

For example, many organizations find it useful to identify four access levels:

- ◆ **Extremely permissive.** Often used for management and system administrators, and others who need software access for testing or whose level within the organization reduces requirements. For this level of access, standard settings include:
 - Rule 1** -Enabled Harmful Software rule
 - Rule 2** -Custom rules that specifically permit applications that may be restricted for other users (examples include instant messaging, games, and audio visual)

Rule 3 -Enabled Mass Mailing rule

Rule 4 -Global rule that blocks all ports (Zero Day response setting)

- ◆ **Relatively permissive.** Often used for Technical Support, Customer Service, Sales, and/or Marketing. For this level of access, standard settings include the following rules:

Rule 1 -Enabled Harmful Software rule

Rule 2 -Custom rules that specifically permit categories. which may be restricted for other users (examples include the Instant Messaging and Audio/Video categories)

Rule 3 -Custom rule that blocks the Entertainment category

Rule 4 -Enabled Mass Mailing rule

Rule 5 -Global rule that blocks all ports (Zero Day response setting)

- ◆ **Flexible.** Often used for staff members that are offsite on a regular basis, including Sales, Field Support, and other similar groups. For this level of access standard settings include the following rules:

Rule 1 -Enabled Harmful Software rule

Rule 2 -Custom rule that blocks the Adult, Gambling, and P2P File Sharing categories at all times.

Rule 3 -Custom rule that blocks the Games and Instant Messaging categories only when a machine is unable to communicate with CPM Server.

Rule 4 -Enabled Mass Mailing rule

Rule 5 -Global rule that blocks all ports (Zero Day response setting)

- ◆ **Restrictive.** Often used for internal departments with little customer access, including Accounting, Shipping and Receiving, and other similar groups. For this level of access standard settings include the following rules:

Rule 1 -Enabled Harmful Software rule

Rule 2 -Custom rule or rules that block the Entertainment, Audio/Visual, and Instant Messaging categories

Rule 3 -Enabled Mass Mailing rule

Rule 4 -Global rule that blocks all ports (Zero Day response setting)

Rule Precedence

When Client Agent receives a launch request from a client machine or a user, it checks the list of rules to determine how to handle the request. When processing a request, Client Agent begins at the top of CPM policy and moves to the bottom.

When Client Agent encounters the first true reference to the software, it stops and performs whatever action the policy specifies: the remaining rules are not processed. Because rule order determines where entries appear in the policy, it is critical that you consider the effects of rule precedence.

To help you in this process, the following examples discuss specific situations. While these may not exactly reflect the exact situation within your organization, they will help you understand how rule precedence can impact launch requests.



NOTE

During policy generation, CPM Server **always** processes the System Files rule first, described in [System Files Rule, page 263](#), thus permitting all critical operations. Once that is complete, the server then checks for any entries in the Outbreak rule, described in [Emergency Outbreak Rule, page 263](#), before processing any other rules. The System Files rule appears in the list of rules, while the Outbreak rule is hidden.

Example 1: Only Websense Rules

Client Policy Manager includes a default set of rules that creates a policy for basic systems operations. This policy allows employees to freely launch applications and does not impose any restrictions. This lets client machines on your network continue operations until you have created your own rules.

The preset rules appear in the following order:

Rule 1 -System Files rule. The rule permits categories that are critical for system operations, and permits all ports. This rule always remains in the first position in the list of rules. For details, refer to [System Files Rule, page 263](#).

Rule 2 -Emergency Outbreak Rule (hidden). The rule blocks any file name you enter in the **Outbreak** dialog box. For details, refer to *Emergency Outbreak Rule*, page 263.

Rule 3 -Harmful Software rule. The rule blocks the Websense Hacking, Malware, and Spyware categories. For details, refer to *Harmful Software Rule*, page 264.

Rule 4 -Global rule. This rule permits all executables that are not specifically controlled by rules that appear above it, and permits all ports. Blocking network access for this rule enables a Zero Day response functionality. The rule always appears in the last position in the list of rules. For details, refer to *Global Rule*, page 266.

You cannot disable, move, or delete the System Files or Global rules. You can change logging for both. For the Global rule, you can change network access from permit to block, or limit the ports that it will permit.



NOTE

The Emergency Outbreak Rule is invisible in the **Policy** pane, and takes precedence over all other rules, except the System Files rule.

Although the Lockdown rule always appears in the list of rules, it is not populated until you run inventories and lock down client machines. For details, refer to *Chapter 9: Applying Lockdowns*.

Example 2: Basic Rule Set

During evaluations and CPM policy configuration, most subscribers choose to immediately:

- ◆ Enable the Mass Mailing rule to stop malware from using infected machines to send emails.
- ◆ Add a custom rule that blocks executables that may lower employee productivity or lead to legal liability.
- ◆ Set the Global rule to block all ports (Zero Day response).

Even if you do nothing else, you can significantly impact overall performance and machine security within a matter of minutes.

An example of a productivity-enhancing rule, which could be labelled **Always Block**, contains all the executables in the following categories:

- ◆ Games
- ◆ Adult
- ◆ Instant Messaging
- ◆ P2P File Sharing

The **Always Block** rule blocks applications in the **Always Block** software set. The resulting list of rules is:

Rule 1 -System Files rule. For details, refer to [System Files Rule, page 263](#).

Rule 2 -Emergency Outbreak Rule (hidden). For details, refer to [Emergency Outbreak Rule, page 263](#).

Rule 3 -Harmful Software rule For details, refer to [Harmful Software Rule, page 264](#).

Rule 4 -Custom **Always Block** rule, which contains the Websense categories, identified above.

Rule 5 -Mass Mailing rule. For details, refer to [Mass Mailing Rule, page 264](#).

Rule 6 -Global rule blocks all ports (Zero Day response). For details, refer to [Global Rule, page 266](#).

Example 3: Lockdown Rule

Although the Lockdown rule always appears in the **Rules** list, it is active only if you create lockdowns at client machines, as described in [Chapter 9: Applying Lockdowns](#), and only if the rule is enabled. The Lockdown rule is important if your goal is to create a policy that provides the highest possible level of security.

Due to the nature of the Lockdown rule—which permits only those executables discovered during inventory (Inventory Lockdown) or present on the machine when Express Lockdown was applied—the position of the rule is critical. If the rule is not placed appropriately, you can create situations that block executables necessary for day-to-day operations.

For example, if you set lockdowns before IT installs a new custom software package that everyone needs to use, none of the CPM client machines will be able to use the software.

You create a new rule called **Custom Software** that permits application launches and network access. You do not, however, run a new inventory. Your list of rules is:

Rule 1 -System Files rule. For details, refer to *System Files Rule, page 263*.

Rule 2 -Emergency Outbreak Rule (hidden). The rule blocks any file name you enter in the Outbreak dialog box. For details, refer to *Emergency Outbreak Rule, page 263*.

Rule 3 -Harmful Software rule. For details, refer to *Harmful Software Rule, page 264*.

Rule 4 -Lockdown rule. For details, refer to *Lockdown Rule, page 265*.

Rule 5 -**Custom Software** rule you create. This rule contains the custom software package described above.

Rule 6 -Mass Mailing rule. For details, refer to *Mass Mailing Rule, page 264*.

Rule 7 -Global rule blocks all ports (Zero Day response). For details, refer to *Global Rule, page 266*.

In the above example, Rule 4 blocks the custom applications because they were not present during inventory. Rule 5 will never apply.

To resolve this problem, move the Lockdown rule to the position immediately above the Global rule, as shown below:

Rule 1 -System Files rule

Rule 2 -Hidden Emergency Outbreak Rule

Rule 3 -Harmful Software rule

Rule 4 -The **Custom Software** rule

Rule 5 -Mass Mailing rule

Rule 6 -Lockdown rule

Rule 7 -Global rule blocks all ports (Zero Day response)

In the fixed example, Rule 4 permits the custom applications. This is true, even though Rule 6 would block the executable if it were not in the original inventory.

Example 4: Manually Entered File Names

If you manually add file names to a software set, described in *Manually Adding a File Name to a Software Set, page 240*, you may encounter some problems because the file name is not associated with an application

signature. If you add executables to rules using categories, described in [Working with Categories, page 201](#), or **Search and Find** operations, described in [Searching For and Adding an Executable, page 239](#), CPM Server uses application signatures in the policy. As a result, Client Agent can recognize executables, even if file name changes occur.

If you do enter a file name manually, the only parameter that CPM recognizes is the text you enter—the system cannot check other information to determine whether or not the executable is what it seems to be.

There are, however, times when manually entered rules are useful. For example, your organization uses a timesheet program that is developed in-house, and which does not appear in the Websense Enterprise Master Database. You can add the file name manually, and include it in a rule. In these situations, rule position is critical if security is of concern.

Review the following list of rules, assuming one rule permits an application by using the file name to identify the software, and another blocks games using Websense data.

Rule 1 -System Files rule. For details, refer to [System Files Rule, page 263](#).

Rule 2 -Emergency Outbreak Rule (hidden) For details, refer to [Emergency Outbreak Rule, page 263](#).

Rule 3 -Harmful Software rule. For details, refer to [Harmful Software Rule, page 264](#).

Rule 4 -The **Custom Software** rule. The software set includes the manually entered file name `timesheet.exe`

Rule 5 -The custom **Block Games** rule, which contains the Websense category, *Games*

Rule 6 -Mass Mailing rule. For details, refer to [Mass Mailing Rule, page 264](#).

Rule 7 -Global rule blocks all ports (Zero Day response). For details, refer to [Global Rule, page 266](#).

In the above example, the rules cause a problem. Because you manually added `timesheet.exe`, the custom program, to Rule 4, an employee could change the name of Solitaire to `timesheet.exe`. Given the above rule order, Agent permits Solitaire to execute. This is because the file name matches the file name you entered in the rule. Although Rule 5 blocks the *Games* category, it has no impact because the rule is lower in precedence than Rule 4.

To resolve this problem, move the rule that includes manually entered file names below the other rules, and immediately above the Lockdown and Global rule.

Rule 1 -System Files rule

Rule 2 -Hidden Emergency Outbreak Rule

Rule 3 -Harmful Software rule

Rule 4 -Mass Mailing rule

Rule 5 -The custom **Block Games** rule

Rule 6 -The **Custom Software** rule

Rule 7 -Global rule, set to block network access attempts (Zero Day response)

The above example is much better than the first one in this section. Rule 5 blocks *Solitaire* using the application signature—even though the *Solitaire* file has been renamed. Even though Rule 6 permits `timesheet.exe`, the only executables the rule impacts are those not addressed by rules that are higher in precedence.



NOTE

If you manually enter a file name that Websense, Inc. identifies as a critical function, the System Files rule always takes precedence. This functionality ensures that system applications continue running.

Example 5: User and Group Rules

There may be situations where you want to create rules that are relatively permissive for individuals or small groups, while other rules are more prohibitive, but may impact some of the same users. In this situation, rule precedence is critical.

For example, Customer Service employees need to be available to online customer, and are allowed to access Instant Messaging software, but other employees are not. You create the following:

- ◆ A client set that includes only the Customer Service employees in the online department. You add employees to the client set as individuals and then call the client set **Service**.

- ◆ A client set using groups to identify all company employees by departments and call it **All Departments**.
- ◆ An **Instant Messaging** software set that includes only the *Instant Messaging* category.

You then create two rules and insert them into the list of rules, as follows:

Rule 1 -System Files rule. For details, refer to [System Files Rule, page 263](#).

Rule 2 -Emergency Outbreak Rule (hidden). For details, refer to [Emergency Outbreak Rule, page 263](#).

Rule 3 -Harmful Software rule. For details, refer to [Harmful Software Rule, page 264](#).

Rule 4 -A custom **Block Instant Messaging** rule, which impacts the **All Departments** client set.

Rule 5 -A custom **Permit Instant Messaging** rule, which impacts the **Service** client set.

Rule 6 -Mass Mailing rule. For details, refer to [Mass Mailing Rule, page 264](#).

Rule 7 -The Global rule blocks all ports (Zero Day response). For details, refer to [Global Rule, page 266](#).

In the above example, Rule 4 blocks all Instant Messaging software for all employees—even online Customer Service representatives—because they are included in the **All Departments** client set. Even though Rule 5 would allow access, it is lower in precedence than Rule 4, and therefore does not impact the policy.

To resolve this situation, reposition the rules as follows:

Rule 1 -System Files rule

Rule 2 -Emergency Outbreak Rule (hidden)

Rule 3 -Harmful Software rule

Rule 4 -Custom **Permit Instant Messaging** rule

Rule 5 -Custom **Block Instant Messaging** rule

Rule 6 -Mass Mailing rule

Rule 7 -Global rule, set to block network access attempts (Zero Day response)

The new order resolves the problem since Rule 4 now permits Instant Messaging for the online Customer Service staff. Rule 5 no longer impacts them, but continues to block Instant Messaging software for all other employees.

Example 6: Connected/Disconnected Rules

There may be situations where you want to create rules that impact machines and users, based on the ability of the machine to connect with CPM Server. This is valuable especially for employees who may have significantly different requirements in the office than they do when they are off-site. For example, Sales staff use laptops when they are visiting customers. Often, they spend a lot of time in airplanes and/or at airports. As a result, management wants them to be able to access instant messaging applications and games when they are off-site. However, management does not want them accessing these applications when they return and are working in the office. Create the following sets:

- ◆ A client set that includes only the Sales staff that are frequently offsite, and the machines they use. You add machines and employees to the client set individually, and then call the client set **SalesForce**.
- ◆ An **Offsite** software set that includes the Instant Messaging and Games categories.

Then create two custom rules and insert them into the list of rules, as follows:

Rule 1 -System Files rule. For details, refer to [System Files Rule, page 263](#).

Rule 2 -Emergency Outbreak Rule (hidden). For details, refer to [Emergency Outbreak Rule, page 263](#).

Rule 3 -Harmful Software rule. For details, refer to [Harmful Software Rule, page 264](#).

Rule 4 -A custom **Block Offsite** rule that impacts all clients.

Rule 5 -A custom **Permit Offsite** rule that impacts all clients in the **SalesForce** client set when machines/users are disconnected from the corporate network.

Rule 6 -Global rule, set to block network access attempts (Zero Day response). For details, refer to [Global Rule, page 266](#).

In the above example, Rule 4 blocks all Instant Messaging and Games software for all employees—even those in Sales when they are off-site—because they are included in the **All Clients** client set. Even though Rule 5 would allow access, it is lower in precedence than Rule 4, and therefore does not impact the policy.

To resolve this situation, reposition the rules as follows:

Rule 1 -System Files rule.

Rule 2 -Emergency Outbreak Rule (hidden).

Rule 3 -Harmful Software rule.

Rule 4 -A custom **Permit Offsite** rule that impacts all clients in the **SalesForce** client set when machines/users are disconnected from the corporate network.

Rule 5 -A custom **Block Offsite** rule that impacts all clients.

Rule 6 -Global rule, set to block network access attempts (Zero Day response).

The new order resolves the problem since Rule 4 now permits applications associated with the **Offsite** software set for the Sales staff when they are away from the office. When a salesperson is in the office, Rule 4 blocks access to applications in the software set because the machine can communicate with CPM Server. Rule 5 continues to block everyone.

Streamlining Rules

Although you can create series of rules that provide duplicate control for different departments, or a number of rules that control launch requests in a similar manner, it is best to streamline your rules whenever possible. One advantage is the creation of a smaller CPM policy, which saves processing time. Perhaps even more important, streamlining rules can make ongoing maintenance of the rules easier, thus allowing you to meet your other, perhaps more critical, obligations.

For example, you create a list of rules as follows:

Rule 1 -System Files rule. For details, refer to [System Files Rule, page 263](#).

Rule 2 -Emergency Outbreak Rule (hidden).

Rule 3 -Harmful Software rule. For details, refer to [Harmful Software Rule, page 264](#).

Rule 4 -A rule that permits executables in the Communications category and allows them to access the Enterprise Productivity port set. For details, refer to [Prepopulated Port Sets, page 244](#).

Rule 5 -A rule that permits the Audio/Video category and blocks all ports.

Rule 6 -A rule that permits executables in the Screen Saver category and blocks all ports.

Rule 7 -A rule that blocks executables in the Games category.

Rule 8 -The Mass Mailing rule is enabled.

Rule 9 -The Global rule blocks all ports (Zero Day response). For details, refer to *Global Rule*, page 266.

Because the Global rule permits launches and blocks ports for all executables not identified by other rules, you can streamline the list as follows:

Rule 1 -System Files rule.

Rule 2 -Emergency Outbreak Rule (hidden).

Rule 3 -Harmful Software rule.

Rule 4 -A rule that permits executables in the **Communications** category and allows them to access a limited set of ports.

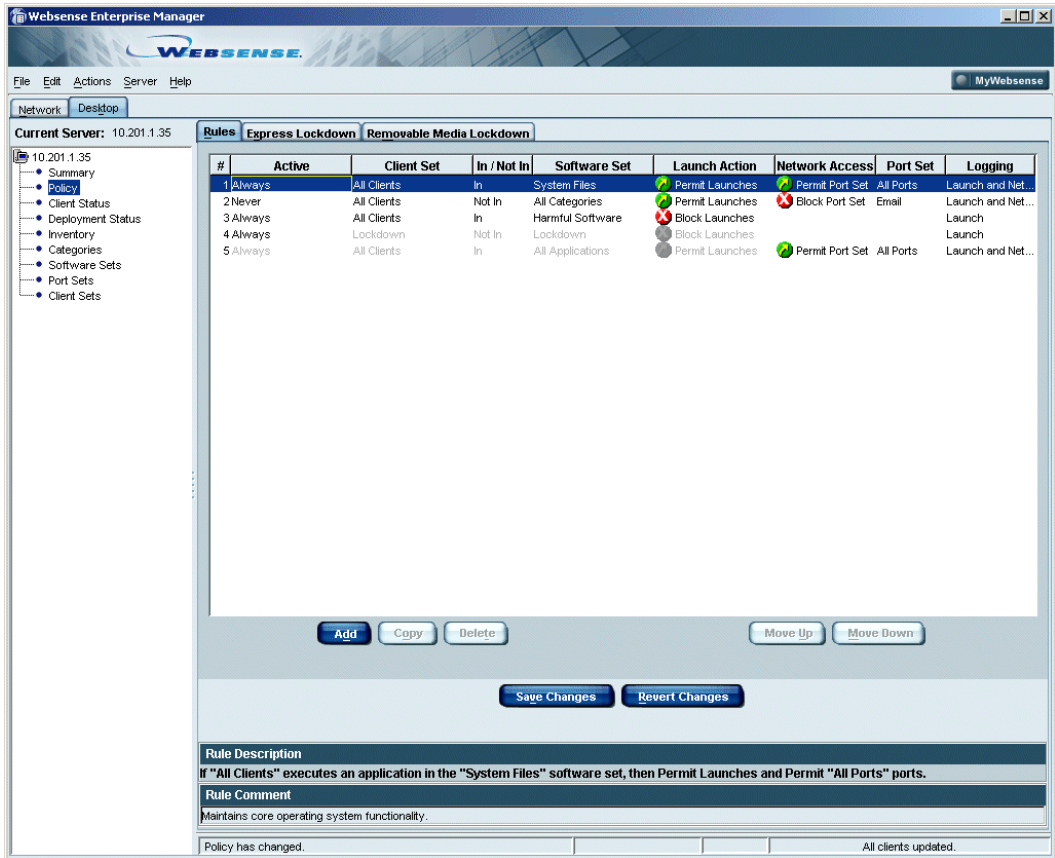
Rule 5 -A rule that blocks executables in the **Games** category.

Rule 6 -The Mass Mailing rule is enabled.

Rule 7 -The Global rule blocks all ports (Zero Day response).

The Rules Pane

The **Rules** pane allows you to add, view, edit, position, and delete rules. The combination of rules defines the CPM Policy.



Rules Pane

When you first use Client Policy Manager, the **Rules** pane contains five visible rules:

- ◆ A System Files rule that always permits the System Files software set. The software set contains the Critical Functions - Never Block category, which identifies software critical for normal systems operations. The rule always appears in the first position of the list. You cannot disable, move, edit, or delete the rule.

- ◆ A Mass Mailing rule that must be manually enabled. When the rule is active it permits all launches of Uncategorized software files, and blocks port 25.
- ◆ A Harmful Software rule that blocks launch applications contained in the Hacking, Malware, and Spyware categories. The rule appears below the System Files rule in the default list. You can disable, move, edit, or delete the file.
- ◆ A Lockdown rule that is empty until you apply at least one lockdown at a machine on the Client Policy Manager network. Client Policy Manager automatically inserts any lockdowns you apply to this rule. You can enable, disable, and move the rule, and define logging. You cannot delete it. A Global rule that allows all clients to launch all executables and access all ports. The Global rule is always at the bottom of the list of rules. You can change network access settings and logging. You cannot disable, move, or delete the rule.

Rule Components

Each rule has eight active components:

- ◆ The **Active Status** selection identifies if and when CPM Server processes a rule. Depending on the selection, a rule may or may not be included in a given policy. For details, refer to [Status Settings, page 256](#).
- ◆ The **Client Set** column shows the users, user groups, domains, and/or machines that are impacted by the rule. For details, refer to [Working with Client Sets, page 191](#).
- ◆ **In/Not In** defines whether the executable being launched must be in the associated software set or not.
- ◆ The **Software Set** column shows the software set the rule impacts. A software set is a group of individual executables, categories, other software sets, or any combination of these. For complete details, read [Working with Software Sets, page 225](#).
- ◆ The **Launch Action** column shows **Permit Launches**, **Continue Launches**, or **Block Launches**. The field uses symbols to indicate the current setting. To view a table of the symbols used in CPM, refer to [Symbols, page 113](#).
- ◆ The **Network Access** column shows if applications in the software set are to be permitted access to the ports in the associated port set, or if they are to be blocked. Possible entries are **Permit Port Sets** and **Block Port Sets**.

- ◆ The **Port Set** column shows the port set that will be blocked or permitted if the application launch is permitted or set to continue.
- ◆ The **Logging** column shows whether logging will occur, and if it does, the information that is to be logged. Possible entries are **Launch and Network**, **Launch**, **Network**, and **No Logging**.

The **Rule Description** field at the bottom of the pane allows you to select a rule, and then see a sentence that describes it more fully. You can change the description if appropriate. If you do not select a rule, the area provides a basic description of a generic rule.

Accessing the Rules Pane

To access the **Rules** tab:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Policy** in the navigation pane and select the **Rules** tab.
3. Select the function you want to perform. You can add, copy, edit, move, or delete a rule. You can also revert changes to the last saved information.

Reverting Changes

When you are working in the **Rules** pane, you can revert any changes you make as long as you have not yet saved your changes. This lets you revert the rules back to the way they were when you first opened the pane, removes any new rules you may have added, and restores any rules you may have deleted. The process does not affect any information you have already saved.

1. In Websense Enterprise Manager, click the **Desktop** tab, and then select **Policy** to open the **Rules** pane.
2. Create or edit rules as necessary. If you decide you do not want to keep the new or edited rules, click **Revert Changes**. Client Policy Manager restores the last saved settings.
3. Continue working with the rules as appropriate.
4. Click **Save Changes** at any time to save rules.

Adding a Rule

You can create rules for Client Policy Manager at any time. This allows you to define how Client Agent responds to launch requests and network access attempts, based on the action you select.

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Policy** in the navigation pane and select the **Rules** tab.
3. Click **Add**. You can also right-click in the **Rules** list, and then select **Add** from the shortcut menu.

Client Policy Manager inserts the new rule above the row you selected. The default settings for new rules are:

- Rule is **Active**
 - **Client Set** field is set to **All Clients**
 - **In/Not In** field is set to **In**
 - **Software Set** field is set to **All Applications**
 - **Action** field is set to **Permit**
 - **Network Action** field is set to **Permit Ports**
 - **Port Set** field is set to **All Ports**
 - **Logging** function is **Active**
 - **Comment** field is set to **New Rule**
4. Click on the settings in each column to display the available options in a drop-down menu.
 5. Indicate the **Active Status** of the rule. Selections that are available are:
 - **Always active**: The rule is always active and impacts all machines and users included in the client set. Use this setting for rules that:
 - Reduce legal liability.
 - Increase security.
 - Should always affect machines and users.
 - **Never active**: CPM Server never includes the rule in a policy. This setting is often used during testing.

For evaluating CPM or testing your CPM policy, create a list of rules and set them to **Never active**. When testing begins, change the status of the first rule to the selection of choice, and leave the remaining

rules set to **Never Active**. Once the first rule passes testing, set the status in the next rule. Continue this process until the entire list of rules is tested and all rules are active.

- **Connected:** CPM includes the rule only if a machine in the client set is able to communicate with CPM Server. This is often set in rules that are designed to increase employee productivity during normal office situations.
- **Disconnected:** CPM includes the rule only if a machine in the client set is not able to communicate with CPM Server. This is often used in rules that permit access to applications that may normally impact employee productivity.

Other potential scenarios for using the disconnected status include situations where connections could cause security concerns. For example, if the machine is not in communication with CPM Server, and an employee accesses the Internet, it is possible that unrecognized viruses could infest the machine. By creating a rule whose status is set to **Disconnect**, and which blocks port access, you can ensure adequate security.

6. Click in the **Client Set** field and select a client set from the list.
7. Click in the **In/Not In** field, and then select either **In** or **Not In**. Your entry defines the relationship between any launch requests and the software set.
 - If you select **In**, and the executable **is in** the associated software set, Client Agent performs the action defined in the **Action** field.
 - If you select **In**, and the executable **is not in** the associated software set, Client Agent does not perform the action defined in the **Action** field.
 - If you select **Not In**, and the executable **is not in** the associated software set, Client Agent performs the action defined in the **Action** field.
 - If you select **Not In**, and the executable **is in** the associated software set, Client Agent does not perform the action defined in the **Action** field.
8. Click in the **software set** field, and then select a software set from the list.
9. Click in the **Action** field, and then select **Permit Launches**, **Block Launches**, or **Continue Launches**.

- If you select **Permit Launches**, Client Agent permits launch requests if they fulfill the requirements indicated by the rule. The process is completely transparent, and the employee responsible for launching the executable is given access. When you select this option, Client Policy Manager inserts the **Permit Launches** symbol in the field.
 - If you select **Block Launches**, Client Agent blocks launch requests if they fulfill the requirements indicated by the rule. When you select this option, Client Policy Manager inserts the **Block Launches** symbol in the field. When an employee tries to launch a blocked executable, a block message appears.
 - If you select **Continue Launches**, Client Agent presents a message before launching an executable. When you select this option, Client Policy Manager inserts the **Continue Launches** symbol in the field. When an employee tries to launch a software set to continue, a message appears which allows the employee to decide whether to cancel the request or continue with the launch.
10. If you are defining network access:
 - a. Click in the **Network Access** field and select either **Permit Ports** or **Block Ports**. Your selection will impact the port set you select next.
 - b. Click in the **Port Sets** field and select the port set you want the rule to impact.
 11. Click in the **Logging** check box and select a logging option.
 - **Launch and Network**: Log application launch and network access information for this rule.
 - **Launch**: Log only application launch information for this rule.
 - **Network**: Log only network access information for this rule.
 - **No Logging**: Do not log any information.

For more information, read [Logging, page 260](#) and [Excluding Users From Logging, page 294](#).
 12. Click in the **Comments** field, at the bottom of the page, to add any information about the rule. You may enter up to 500 keyboard characters. The text may act as a title or describe the intended function of the rule.

13. Use the **Move Up** and **Move Down** buttons to move a rule to an appropriate position if necessary. To better understand the importance of rule positioning, read [Rule Precedence, page 275](#).

**IMPORTANT**

You cannot place rules above the System Files rule or below the Global rule. These restrictions ensure proper functioning of your CPM policy.

14. Click **Save Changes** to save the rules.

Copying a Rule

You can copy existing rules to create new rules. This is useful if you want a new rule similar to one already in your policy. Once you copy the existing rule, you can edit the copy. You cannot copy the System Files, Lockdown, or Global rules.

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Policy** in the navigation pane and select the **Rules** tab.
3. Click the rule you want to duplicate, and then click **Copy**. You can also right-click the rule, and then select **Copy** from the shortcut menu.

The new rule appears directly above the copied rule. The default entry in the **Comments** field shows the text from the original rule, and adds the word **Copy**. For example, if the original rule has the word **Engineering** in the **Comments** field, the default entry is **Copy of Engineering**.

4. Accept the default comment or type your own entry in the **Comments** field.
5. Edit or move the rule as appropriate.
6. Click **Save Changes** to save your changes.

Editing a Rule

When you are developing your CPM policy, you may need to edit rules to fine-tune control. Later in the cycle, it is probable that only changes to organizational structure or company requirements will result in changes to your rules.

The following rules can be edited as indicated:

- ◆ **System Files:** Edit logging only.
- ◆ **Lockdown:** Edit logging or select either the *Always Active* or *Never Active* status.
- ◆ **Global:** Edit logging and network access.

To edit a rule:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Policy** in the navigation pane and select the **Rules** tab.
3. Locate the rule you want to change, and then click in the appropriate fields:
 - Click in the **Active** check box to make changes in how CPM handles the rule.
 - Click in the **Client Set** field, and then select a client set.
 - Click in the **In/Not In** field and select either **In** or **Not In**.
 - Click in the **Software Set** field and select the software set.
 - Click in the **Action** field and select either **Block Launches**, **Permit Launches**, or **Continue Launches**.
 - Click in the **Network Access** field and select either **Permit Ports** or **Block Ports**.
 - Click in the **Port Sets** field and select the port set you want the rule to control.
 - Click in the **Logging** checkbox and select the logging parameters you want to use.
4. Click **Save Changes** to save the rules.

Moving a Rule

The **Rules** pane contains a list of all rules. The numeric order defines how Client Agent processes the rules. You can change the position of the rules, thus changing the order in which Client Agent checks the list.

**NOTE**

You cannot change the positions of the System Files or Global rules.

To move a rule:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Policy** in the navigation pane and select the **Rules** tab.
3. Select the rule you want to move, and then:
 - Click the **Move Up** button to move the rule up one position. You can also right-click the rule, and then select **Move Up** from the shortcut menu.
 - Click the **Move Down** button to move the rule down one position. You can also right-click the rule, and then select **Move Down** from the shortcut menu.
4. Continue moving the rule until it appears in the correct position in the **Rules** pane.
5. Click **Save Changes** to save the rules.

**WARNING**

Be sure to test your CPM policy after moving rules. It is critical to developing a functional CPM policy that works in the way you expect. For detailed information and examples, read [Rule Precedence, page 275](#).

Deleting a Rule

You can delete rules when they are no longer applicable, with three exceptions: you cannot delete the System Files, Lockdown, or Global rules. You can delete any rule you or other system administrators have entered in the policy.

To delete a rule:

1. In Websense Enterprise Manager, click the **Desktop** tab.
2. Select **Policy** in the navigation pane and select the **Rules** tab.
3. Select the rule you want to remove, and then click **Delete**. You can also right-click the rule, and then select **Delete** from the shortcut menu. A confirmation message opens.
4. Click **Yes** to delete the rule.
5. Click **Save Changes** to save the rules.

Disabling a Rule

If you are not sure you want to delete a rule, you can disable it instead. This allows you to retain the rule for future use, but stops Client Policy Manager from processing the rule in the meantime.

1. Identify the rule you want to disable, and then click the rule in the **Active** column. Select **Never** from the drop-down list.
2. Click **Save Changes** to save the rules.

Excluding Users From Logging

There may be times when you want or need to exclude users from the logging function. For example, you do not want to log launch details for the company CEO, senior management, and two independent contributors in the research department.

To exclude individual users from logging:

1. Create a client set including any individual or group whose launches should not be logged.
2. Create a rule using the client set you defined in Step 1.

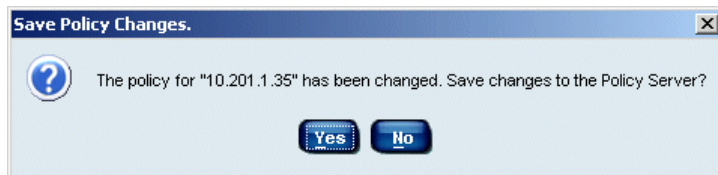
Disable logging for the rule you created in Step 2.

Policy Changes and Exiting Websense Enterprise Manager

If you make changes to the CPM policy and then try to close Websense Enterprise Manager before saving, a dialog box opens to remind you about the changes. This ensures that you have an opportunity to save or drop those changes.

If you receive the **Save Policy Changes** dialog box:

- ◆ Click **Yes** to add your changes to the policy.
- ◆ Click **No** to drop your changes and revert to the last saved policy.



Save Policy Changes Dialog Box

As soon as you respond, Websense Enterprise Manager closes.

CHAPTER 15 | Troubleshooting

If you encounter problems with Client Policy Manager setup or configuration, check the topics in this appendix to troubleshoot the problem.

A critical tool for troubleshooting includes access to logged data. When Client Policy Manager encounters error, logs appear in the following locations for the indicated events:

- ◆ Server errors log to the Windows **Event Viewer**.
- ◆ Connection errors between the directory services and CPM Server log to the Windows **Event Viewer**. Entries include warnings and actual errors.
- ◆ Connection errors between Client Agent and CPM Server appear in the server user interface.
- ◆ Client Policy Manager user interface errors appear in messages at the user interface.

Troubleshooting Database Issues

If you encounter problems with the Websense Enterprise Master Database, this section may be of value. If a particular problem is not addressed here, check the Websense Knowledge Base at <http://www.websense.com/support/knowledgebase/>. The Knowledge Base is updated whenever customers, developers, or other users of Websense products find and then resolve problems.

Why am I having trouble accessing Websense download sites and my.websense.com?

If you edit host files and/or routing tables that restrict the URLs a Websense server can access, make sure you permit the following:

- ◆ **download.websense.com**
- ◆ **ddsdm.websense.com**
- ◆ **ddsint.websense.com**

- ◆ **portal.websense.com**
- ◆ <http://www.my.websense.com>

You must permit these URLs in order to access Websense Enterprise Master Database downloads and your Websense subscription data.

Why can't I download the Websense Enterprise Master Database or send AppCatcher data to Websense?

The machine running CPM Server must have access to HTTP and must be able to receive incoming transmissions to download the Websense Enterprise Master Database or send AppCatcher data to Websense, Inc. for review. You can verify Internet access by performing the following steps:

1. Check to see if CPM Server is accessing the Internet through a proxy server. Select **Proxy / Authentication** in the navigation tree, and check the information in the **Proxy** area.
2. Determine what to do next.
 - If proxy information is required, refer to *Proxy Information is Required*, below.
 - If proxy information is not required, refer to *Proxy Information is Not Required*, page 299.
 - If authentication is required, refer to *Authentication is Required*, page 299.
 - If CPM Server sits behind a firewall, refer to *Firewall Restrictions*, page 299.
 - If your system includes any restriction-type software, refer to *Restriction Applications*, page 300.

Proxy Information is Required

If your configuration includes a proxy server:

1. From CPM Server, open either Internet Explorer or Netscape.
2. Set the browser to access the Internet with the same proxy settings as CPM Server.
3. Enter one of the following addresses:
 - <http://download.websense.com>
 - <http://asia.download.websense.com>
 - <http://europe.download.websense.com>

If you reach one of these sites, the Websense logo appears, along with a message that indicates you are being redirected to the Websense home screen. This verifies that proxy settings are correct and the CPM Server should have the appropriate access for downloading the database.

Proxy Information is Not Required

If your configuration does not include a proxy server:

1. From CPM Server, open the **Command Prompt** dialog box by selecting **Start>Applications>Command Prompt**.
2. Use the **nslookup** command with the address of the download site to make sure CPM Server can resolve the download location to an IP address. Your choices are:
 - nslookup download.websense.com
 - nslookup asia.download.websense.com
 - nslookup europe.download.websense.com
3. If this does not return an IP address, you must set up CPM Server so it can access a DNS server.

Authentication is Required

If CPM Server must access the Internet through an upstream firewall or proxy server that requires authentication, check the following:

- ◆ Check the spelling and capitalization for the user name and password in the **Proxy/Authentication** dialog box.
- ◆ Make sure the firewall or proxy is configured to accept clear text or basic authentication.

Firewall Restrictions

If your firewall restricts access to the Internet at the time CPM Server calls for the download, or if the firewall limits the size of files that can be sent via HTTP, CPM Server cannot receive the download.

- ◆ Make the appropriate changes on the firewall, or change the time for the download by selecting **Settings > Database Download** and changing values in the **Download** time fields.



NOTE

If you are running CPM Server behind a Gauntlet firewall, check FAQs at <http://www.websense.com/support/knowledgebase/> for specific information.

Restriction Applications

Some restriction applications, such as virus scanners or size-limiting applications, can interfere with database downloads. You need to disable the restrictions relating to CPM Server and the download location.

Where can I find error messages when a Websense Enterprise Master Database download fails?

If you have problems downloading the Websense Enterprise Master Database, you can check the Windows application **Event Log** for information about the download or any other error and status messages.

- ◆ If you are using a Windows NT system, select **Start > Programs > Administrative Tools > Event Viewer**. Once the **Event Viewer** opens, select **Log > Application**.
- ◆ If you are using a Windows 2000 system, select **Start > Programs > Administrative Tools > Event Viewer**. Once the **Event Viewer** opens, select **Application Log**.

Use the information available in the log to troubleshoot the download issue.

Why am I receiving an “Unable to connect to database” error message?

If you select Apache 2.x as your Web Server, and use Windows authentication to connect to the SQL database, you may receive database error connections. The Apache service tries to run as the local system user to connect to the SQL database. If the SQL database can be accessed with only certain Windows authentication, then the Apache service should be made to run as the Windows user who has privilege to access the database.

For example, if the SQL database allows **User1** access, but the Apache Service accesses the database as **User2**, an error will occur. In this event, manually configure Apache to access the database as User1.

To configure Apache:

1. Select **Start > Settings > Control Panel > Administrative Tools > Services** to open the **Services** window.
2. Locate Apache 2.x in the list, and then right-click.
3. Select **Properties** from the shortcut menu.
4. In the **Properties** dialog box, click the **Log On** tab.
5. Click **Select this account** and enter the same Windows authentication data that you defined during installation. The user must have privileges to access the database. Enter the following information:
 - Account
 - Password
 - Password again.
6. Click **OK** to close the **Properties** dialog box and save your information.

What do I do if a database becomes too large?

It is possible that running CPM Server continually may result in an extremely large inventory and/or log database. How quickly this occurs is dependant on your environment. When the database becomes too large, manually archive or back up the database, and then recreate it.



WARNING

The following procedure is provided for experienced system administrators. If you do not have the appropriate knowledge, contact someone in your organization who does.

To recreate the database:

1. Locate the **Websense > bin > sql** directory.
2. Locate and run the `DTM-CreateTables.sql` script to create the necessary tables.
3. Locate and run the `DTM-InsertDefaults.sql` script to insert the necessary defaults.
4. Locate and run the `DTM-CreateStoredProcedures.sql` script to create the necessary tables.

5. Locate and run the `DTM-CreateReporterObjects.sql` script to create the necessary tables.

Troubleshooting Websense Enterprise Manager Functions

Situations that may affect Websense Enterprise Manager appear in this section. There are some situations that may impact the Manager and another component. If you determine the answer is not included in this section, check other troubleshooting topics if it is possible that another component may be causing the problem.

Why can't I access CPM Reporter from Websense Enterprise Manager?

If you install CPM Reporter, and then change the port for the Web Server at that machine, links between Websense Enterprise Manager and CPM Reporter will not function. The **Actions>CPM Reporter** menu selection will call your browser, but will not be able to present CPM Reporter for your use.

You can type the correct address in the browser to immediately access CPM Reporter.

Why can't I connect to the User Service?

If you change the User Service, described in [Configuring User Services](#), page 69, you need to stop and restart CPM Report Scheduler and CPM Server services. Otherwise, you will not be able to connect to the necessary information.

Restarting the CPM Server

To restart the CPM Server service:

1. Click the Windows **Start** button, and then select **Settings > Control Panel > Administrative Tools > Services**.
2. Locate CPM Server, right-click on the entry, and then select **Stop** from the shortcut menu.
3. Right-click on the entry again, and then select **Start** from the shortcut menu.
4. Close the **Services** window. This forces any new details to the servers.

If stopping and restarting the server does not solve the problem, you may need to modify the service to run as a specific user, described in [Configuring User Services](#), page 69.

Changing the Account

To change the account under which the service runs:

1. Click the Windows **Start** button, and then select **Settings > Control Panel > Administrative Tools > Services**.
2. Locate CPM Report Scheduler or CPM Server, right-click the entry, and then select **Properties** from the shortcut menu.
3. Click the **Log On** tab, and then click the radio button associated with **This Account**.
 - Enter the account name in the **This Account** field. You can alternately click **Browse** and locate the account.
 - Enter the password for the account in the **Password** field.
 - Enter the password a second time in the **Confirm password** field.
 - Click **OK** to close the window.
4. Close the dialog boxes as appropriate.

What happens if I reconfigure the IP address for CPM Server?

If you change the IP address or machine name for CPM Server, you will lose communications with other servers and Client Agent, as these paths are set when you install Client Policy Manager components. Because you can deploy servers to various machines, IP address changes may impact servers other than the CPM Server. Two of the most common instances occur if:

- ◆ The Policy Server and User Server are on one machine, and CPM Server is on another. If this is the case, uninstall and reinstall only CPM Server.
- ◆ The Policy Server, User Server, and CPM Server are on the same machine. If this is the case, uninstall Client Policy Manager and then Websense Enterprise Manager, and then reinstall Websense Enterprise Manager and Client Policy Manager.

Other deployment scenarios may exist. If you have questions regarding specifics for your installation, contact Websense Technical Support for assistance.

To uninstall and reinstall Client Policy Manager components, locate the following in the installation disk or from: <http://ww2.websense.com/global/en/downloads/>:

- ◆ Online installer: Setup552.exe
- ◆ Offline installer: Websense552Setup.exe (This large file contains the full installer.)

Complete details for uninstalling and installing CPM components are in the *Websense Enterprise Client Policy Manager Installation Guide*.

Why isn't the CPM policy being enforced?

If the “Computer Browser” service is not started in **Service Control Manager**, and users and groups are administered using Active Directory-Mixed mode, then machines do not always broadcast their machine names. As a result, rules using machine names may not work.

There are two ways to address this problem:

- ◆ Create rules using machine IP addresses.
- ◆ Include user-based rules, not machine-based rules.

Why isn't updated information appearing in Websense Enterprise Manager?

If Policy Server goes down as updates are being sent, details will not appear in Websense Enterprise Manager. This may impact any task that involves the Policy Server.

If you make changes that are not recorded in Websense Enterprise Manager due to Policy Server availability, simply redo those tasks. You may encounter this type of situation when you are running and/or scheduling inventories, submitting policy changes, changing category assignments, and so forth.

How can I see uncategorized executables?

You can view uncategorized executables in the **Category** dialog box, when set to view by **Uncategorized** executables. CPM Server updates executable counts as it finds the files. You can also use CPM Reporter or Explorer for CPM to view uncategorized files.

Troubleshooting Inventory Problems

When you are working with inventories, you may encounter problems when running the inventory or viewing information. Other components that may impact the inventory are identified in this document, and are also available in the Websense Knowledge Base at <http://www.websense.com/support/knowledgebase/>.

Why do I get an error message when I run an inventory?

The word *Error* in the **Status** column in the **Inventory** pane usually indicates one of two situations:

- ◆ The client machine was shut down by an employee while an inventory was running.
- ◆ CPM Server was offline or otherwise not available when a client machine tried to send a completed inventory.

You can check the Windows Event Viewer at the machine where you installed CPM Server to access a detailed description of the error.

Why do I receive an error message for hardware inventories?

If you run inventory on a machine where anti-virus software is installed, you may encounter problems running the hardware inventory script. Typically, this problem becomes apparent when the scheduled inventory remains in a *Running* status, in the **Inventory** pane, long after the status should have changed to *Completed*.

If this occurs, the Event Viewer at the CPM Server shows the message:
"Script was aborted by the client. Workstation:
<workstation name>."

To fix the problem:

1. Go to the client machine where the inventory was not able to run.
2. Open the Windows **Services** dialog box.
 - For Windows 2000: Click the Windows **Start** button, and then select **Settings > Control Panel > Administrative Tools > Services**.
 - For Windows NT: Click the Windows **Start** button, and then select **Settings > Control Panel > Services**.
3. Locate **Websense Desktop Client** and stop the service.

4. At the client machine, open the directory where you loaded Client Policy Manager components, and locate the hardware script. The default path is **C:\Program Files\WebSense\WDC\Scripts\WsInventory.vbs**.



NOTE

If you do not see the **Scripts** folder, it is probably hidden. Change your Windows Explorer settings.

5. Double-click the `WsInventory.vbs` file.
6. When the certification message opens, set the file so it is always certified, and then click **OK**.
7. Return to the Windows Services dialog box and restart **WebSense Desktop Client**.

`WsInventory.vbs` is now able to run correctly, and future inventories should proceed without the appearance of this error.

Why do I see two entries in the Hardware Inventory list for the same machine?

When you have a single client machine running two different operating systems, the **Hardware Inventory** in Client Policy Manager shows two different client IDs that share the same machine name. This may be of concern, especially if you are working with inventory.

It is possible that you will see the same client ID in the **Inventory** pane, but with different information. For example, you have a machine that runs Windows NT and Windows 2000. You run an inventory for Windows NT, and then later run one for Windows 2000. Your inventory list may contain two apparently conflicting entries.

You can flush the entry for the inactive client at any time:

1. In the navigation tree, select the server you are currently logged onto.
2. Click the server name using the right mouse button, and then select **Disconnect from Server**.
3. In the navigation tree, select the server again.
4. Click the server name once more using the right mouse button, and then select **Connect to Server**.

5. In the navigation tree, select **Inventory**.
6. Check the **Inventory** list. You should now see only one entry for the client machine.

Why can't I view physical memory data in the Hardware View?

If you are working in Websense Enterprise Manager, and the text “Not Available” appears instead of physical memory data in the **Hardware View** dialog box, the problem is associated with the client installation. This may occur at machines running Windows NT or on machines using a ghost image.

Client Policy Manager uses **Windows Management Instrumentation** (WMI) to help collect data. When you deploy agents to machines without WMI as a default, or if the existing WMI is an old version, the Client Deployment Service installs the necessary files.

Even though WMI files install correctly, sometimes they do not initialize. To initialize WMI and solve the physical memory display problem, reboot the machine running Client Agent.

Why do I see several rows containing the same data in Software Executable Inventory views?

When you access Software Executable Inventory Views in Client Policy Manager, it is possible that you may see two or more rows of data that seem to show the same information. While the data may seem the same, there are differences in the underlying information.

When Websense, Inc. identifies executables, it uses information from the file itself for that identification. If there are even slight differences between two files, the data collection process identifies two unique executables.

For example, you install `greatwords.exe`, and then later install an upgrade that includes a bug fix. If the upgrade does not remove the original installation, your machine now has two files, both called `greatwords.exe`. Because the contents of these two files are different, Websense, Inc. sees them as separate executables.

Why aren't ZIP drives appearing in inventories?

If you have attached external ZIP drives that connect to machines with parallel cables, you cannot include them in inventory. There is no workaround for this issue.

Why do hardware inventories show a fixed hard disk entry with a size of 0.0 GB?

If you run an inventory for a machine with a parallel port ZIP drive that does not have a zip disk in the drive, you may see a fixed hard disk entry with a size of 0.0 GB. If you insert a zip disk and run the inventory again, the hard disk entry shows the zip disk size, for example, 100 GB.

Why can I see inventory results in the CPM Inventory Database but not in the Inventory pane in Websense Enterprise Manager?

If you run an inventory, but the Policy Server goes offline before any operating detail can be submitted, you will not be able to see inventory progress or results. This may occur even if Client Agent completed the inventory. To resolve the situation, restart the Policy Server, and, if necessary, reschedule and/or run the inventory again.

Troubleshooting Client Agent Problems

If you encounter problems with Client Agent, the most common situations revolve around client/server communications or deployment issues. If the information you need is not in this troubleshooting section, check the Websense Knowledge Base at <http://www.websense.com/support/knowledgebase/>.

Why are services on a Windows NT machines having problems starting?

If you block a service that runs on a Windows NT machine, you may encounter delays when other services try to start. This happens because the Services Control Manager (SCM) on the Windows NT machine has a preset timeout associated with startup if a service does not register.

When the machine begins processing startup executables, the CPM policy is handled first. When it encounters an executable that is supposed to be blocked, the block goes into effect immediately.

Because the blocked service cannot start, it cannot register with SCM. SCM waits for up to two minutes for the registration to occur, forcing any other pending services to wait.

For example, you create a rule that blocks the **Media Players** category. This blocks all media players, including *Windows Media Services*. When an

employee shuts off, and then restarts his or her machine, the Client Policy Manager block immediately affects Windows Media Service.

Because the service cannot register with SCM, other services set to *Automatic* do not start until the two-minute timeout is done. Once the timeout has expired, the other services start almost immediately. The only solution to this situation at this time is to avoid blocking any NT service.

Why can't I see machines running Client Agent any longer?

If machines running Client Agent disappear from Websense Enterprise Manager, and you have changed the IP address for CPM Server, any installed Client Agent disappears. This is because the IP addresses are set specifically for clients during client installation, and your changes stop communications.

To fix this problem, uninstall and then reinstall the Client Agent. You may use the Client Deployment Service, create log in scripts, or use third-party tools. For details, refer to the *Websense Enterprise Client Policy Manager Installation Guide*.

Why can't I see a machine in the Client Status dialog box?

If a machine is hidden, that machine will not appear in the **Client Status** dialog box. Hidden machines do not appear in the Network Neighborhood or the Client list, and the Directory Information Server is unable to locate it. You can revert hidden machines to a viewable status when appropriate:

1. Stop the Server service.
2. Issue the command `net config server /hidden:no`.

You can check the current status for any machine running Client Agent in the Client Policy Manager **Client Status** dialog box, described in [Chapter 10 Working with Client Sets, page 191](#).

Why do I receive an error message stating “Unable to read workstation data” when I access Client Policy Manager functions in Websense Enterprise Manager?

When you first deploy Client Agent to a machine, the application creates a unique machine ID. If you uninstall Client Agent or ghost the client machine, this ID may no longer be valid.

When you open Websense Enterprise Manager the next time, the manager is using the original machine ID for communications with Client Agent. When it

is unable to locate that ID, it generates the “Unable to read workstation data” error message. This causes any application set created using the inventory to become unusable. To resolve this situation:

1. In Websense Enterprise Manager, click the **Desktop** tab, and then select **Software Sets** to open the **Software Sets** pane.
2. Remove the software set that was created using the inventory as a baseline. For details, refer to *Deleting a Software Set*, page 237.
3. Run an inventory for the client machine. Read *Running an Inventory*, page 157.
4. Generate a new application set using the inventory as a baseline. Read *Generating Software Sets from Inventories*, page 164.
5. If you want, you can include this software set as a subset of other software sets. Read *Managing Software Sets*, page 231.
6. Use the application set in an appropriate rule. Read *Adding a Rule*, page 288.



WARNING

If you change the directory service, you may also need to modify the services to run as a particular user. Likewise, you may need to add domain forests if you are going to use Windows Active Directory.

While Websense Enterprise Manager includes tools for working with domain forests and defining directory settings, this document does not describe the operations or the reasons for them. If you are not knowledgeable about LDAP requirements, contact someone in your organization who is.

Why don't employees see block or continue messages associated with screen savers on machines running Windows NT or Windows 2000?

If you include screen savers in rules that are set to block or continue the executable, employees do not see messages, and will not be able to respond to continue messages. This impacts screen savers identified in the Websense **Entertainment:Screen Saver** category, and those which are identified by file name. This occurs because in Windows NT and Windows 2000, screen savers

are associated with `winlogon.exe`, which activates the `winlogon` desktop, and does not impact the employee desktop.

When a screen saver tries to launch:

- ◆ If the policy blocks the screen saver, blocking occurs without presenting the message, and the screen saver will not run. Websense, Inc. recommends that employees be notified if you decide to block screen savers, which may save valuable time for Help Desk personnel.
- ◆ If the policy is set to continue the screen saver, the screen runs normally. This is because continue messages allow the associated executable to run if the continue message cannot be presented to the user.

Why do employees sometimes receive series of block or continue messages?

If your organization subscribes to both Websense Enterprise Web Filtering and Client Policy Manager, it is possible that employees may see messages from both modules. In certain circumstances, it is possible that the Internet Filtering and CPM policy overlap, which results in a series of messages to which an employee must respond.

For example, your organization imposes the following Websense Enterprise policies, two associated with the Web filtering module, and one associated with CPM:

- ◆ **Quota Time**—Internet filtering option that allows employees to access various categories of Web sites for a given length of time, after which they are blocked.
- ◆ **Protocols**—Internet filtering option that monitors and controls access based on protocols.
- ◆ **CPM policy**—Client Policy Manager option including a rule that blocks instant messaging applications.

Jason, an employee in the Accounting department, decides that he wants to install and use an instant messaging application. The following series of events occurs, based on Jason's choices as messages appear:

- ◆ Jason accesses a Web site that includes downloads for instant messaging. However, the policy that impacts Jason limits the Web site by quota time.
- ◆ Jason receives a quota block message. Jason has to decide whether or not he wants to use any of his remaining quota time to access the site.

- ◆ Jason decides to continue. He accesses the Web site, and tries to download the instant messaging installer. Websense detects that the download process uses a protocol that is set to continue.
- ◆ Jason decides he wants to go ahead in spite of the warning and acknowledges the Continue message.
- ◆ Jason downloads the installation software and saves the program to his machine.
- ◆ Jason tries to launch the instant messaging program, but receives a Client Policy Manager block message. His only choice at this point is to acknowledge the message, which automatically stops the launch of the installation program.

Why am I seeing between 80% and 95% CPU usage on Windows NT machines?

If you are working on a machine running Windows NT and using Trend Micro Virus software, you may encounter a regularly occurring situation where:

- ◆ CPU usage measures between 75% and 99%.
- ◆ You may have problems accessing your **Start** menu and **Control** panel.
- ◆ Client Agent processes do not function correctly, if the client is installed on the machine.

These situations may occur whether or not Client Agent is installed.

If you notice any of the above situations, they are caused by the **cidaemon.exe** file, an indexing service for Windows NT machines. To solve the problem:

1. Select **Start > Settings > Control Panel**, and then double-click **Services**.
2. When the **Services** dialog box opens, locate the **Indexing Services** entry, and then click the **Stop** button.

Why are employees at machines that are locked down having problems launching software that is included in the inventory?

If you impose lockdowns on machines, and system administrators perform upgrades, the upgrades change the information that CPM uses to control application launches. As a result, employees may encounter difficulties launching applications that were included in the upgrade.

To correctly install upgrades:

1. Remove the lockdown at the machine where the upgrade is to occur. For details, refer to [Chapter 9: Applying Lockdowns](#).
2. Install the upgrades.
3. Run an inventory. For details, refer to [Running an Inventory, page 157](#).
4. Use the new inventory to lock down the machine. For details, refer to [Chapter 9: Applying Lockdowns](#).

Why are employees having problems with machines where I upgraded Client Agent 5.2 to Client Agent 5.5.2?

If you have upgraded from Client Agent v5.2 to Client Agent v5.5.2, and employees are having problems at machines where the upgrade occurred, it is possible that the machines need to be restarted. Applications may fail, or the machine may not work properly if the restart does not occur.

This occurs because previous socket bindings become invalid when you upgrade Client Agent. When the employee restarts the machine, the socket bindings are reset.

To address this issue:

1. Inform employees before upgrade that they will need to restart machines.
2. If employees call and complain about failed applications, problems with machines, or difficulty accessing networks, ask them to restart the machine.

APPENDIX A | Technical Support

Websense, Inc. is committed to providing excellent service worldwide. Our goal is to provide professional assistance in the use of our software wherever you are located.

Websense Technical Services Support Center

Technical information about Websense Enterprise is available 24 hours a day on the Internet at: <http://ww2.websense.com/global/en/SupportAndKB/>.

You will find here the latest release information, Frequently Asked Questions (FAQ), a Knowledge Base, product documentation, and other information.

Fee-based Support

The Websense 24x7 support contract is available for purchase. For a list of services, please visit our Web site at: <http://www.websense.com/products/about/24x7/>.

For additional information, please contact our Sales Department at **800.723.1166** or **858.320.8000**, or send an email to **sales@websense.com**.

Support Options

Websense Technical Support can be requested 24 hours a day.

Web Portal

You can submit support tickets through the Web Portal 24 hours a day. The response time during business hours is approximately 4 hours. Response to after-hours requests will occur the next business day. Support tickets can be submitted at: <http://ww2.websense.com/global/en/SupportAndKB/CreateRequest/>.

Email Questions

You may email your questions to us at the addresses listed below. Make sure you include your subscription key. This option is available 24 hours a day, 7 days a week. We will respond during business hours Monday through Friday.

- ◆ **support@websense.com**—San Diego, California, USA
- ◆ **japansupport@websense.com**—Japan (Asia)



NOTE

For technical support in the UK, submit support tickets through the Web Portal address.

Email support can 24 hours or more for a response. If you need a quicker turnaround, submit your issues through the Web Portal.

Telephone Assistance

Before you call a Websense Technical Support representative, please be ready with the following:

- ◆ Websense subscription key.
- ◆ Access to Websense Enterprise Manager.
- ◆ Access to the machine running the Filtering Service, the Websense Reporter server, and the database (MSDE or SQL) server.
- ◆ Permission to access the Websense log database.
- ◆ Familiarity with your network's architecture, or access to a person who has this familiarity.
- ◆ Specifications of the machines running the Filtering Service and Websense Enterprise Manager.
- ◆ A list of other applications running on the Filtering Service machine.

For severe problems, additional information may be needed.

Telephone assistance is available during normal business hours Monday through Friday at the following numbers:

- ◆ San Diego, California, USA: **858.458.2940**
- ◆ London, England: **+44 (0) 1932 796244**

Improving Documentation

Websense, Inc. understands the value of high quality, accurate documentation. If you have any suggestions for improving the documentation, contact us at **DocFeedback@websense.com**. We appreciate your input.

CPM Category Definitions

The following are descriptions of all CPM categories and subcategories included in the Websense Enterprise Master Database download. Descriptions are provided for each parent category and all associated children. For the most recent category definitions, check at <http://ww2.websense.com/global/en/ProductsServices/MasterDatabase/ApplicationCategories.php>.

Access/Privacy/Security Category

Software that enables or prevents access to local machines, or that is used to defeat or evade access controls; that enables or attacks measures to establish privacy of, use of, and content on the local machine; or that permits administrative review and control of access and use.

Category	Description
Anti-virus Software	Software that detects, filters, and eliminates viruses imported into the network. Examples include Norton Antivirus and McAfee VirusScan .
Authentication and Authorization	Software that restricts access to, and use of, the machine and its contents to authorized users and authorized uses. Examples include SafeWord , ActiveCard , and Websense Enterprise .
Encryption	Software that enables data encryption and/or decryption for security purposes. Examples include RSA Keon and Blowfish .
Firewalls	Software that protects the machine from unauthorized remote access. The software typically also logs access attempts. Examples include ZoneAlarm and Tiny .
Hacking	Software used to attack or evade access controls and privacy measures on other machines. Examples include BO2K and AirSnort .

Category	Description
Keyloggers	Surveillance software that has the capability to record every keystroke you make to a log file. This log file can then be sent to a specified receiver. An example of a keylogger is SpectorSoft .
Proxy Avoidance	Software that bypasses proxy server features (such as Web filtering) or gains access to URLs in any way that bypasses the proxy server.
Remote Access	Software that enables authorized access to and use of a desktop machine or private network from a remote location. Examples include Visual IP InSight , PCAnywhere , and Telnet .
Spyware	Software that logs and reports on activity at the local machine without the user's knowledge. Examples include Aureate , BESS , FlashTrack , and KeyLogger .
System Audit	Software that monitors and logs activity on a machine network. Examples include Port Scanner and Shields UP!

Audio/Video Category

Software that enables the use and manipulation of sound or image files.

Category	Description
Imaging	Software that enables the creation, manipulation, and display of photographs or other images, where the quality is lower than executables in the Productivity:Graphics category. Examples include LView , PhotoShop , and ACDSee .
Media Players	Software that lets employees create or play audio or video files. Examples include WinAmp and Media Player .

Communication Category

Software that enables the exchange of data in various forms with other machines inside or outside the network, other than those in the **System:Device Drivers** category.

Category	Description
Collaboration	Software that lets employees share files and applications, sometimes called <i>groupware</i> . Examples include Intraspect , Lotus Sametime , Plumtree , OneSpace , and CUseMe .
Dedicated Browsers	Software that enables connection to a specified Web site or set of Web sites that often refresh frequently or constantly to dialog box new content. Examples include CNN AddsWatch and America Online .
Email	Software that lets employees receive, dialog box, compose, and send emails from their local machines. This includes the client side of network applications, for example, Outlook , and freestanding packages residing at the local machine, for example, Eudora . The definition also includes bulk email software, but does not include email software built into Web browsers, for example, Netscape Communicator .
Instant Messaging	Software that lets employees send and receive synchronous, real-time messages at a local machine. Instant messaging software is also called <i>chat-room software</i> . Examples include AOL Instant Messenger , Yahoo Instant Messenger , and MSN Messenger .
P2P File sharing	Software that enables file searching and sharing across a network, without depending on a central server. Examples include Gnutella , KaZaA , and Morpheus .

Category	Description
Telephony, Conferencing, Fax	Software that enables telephonic transmission of voice and other data, including software for BBS and IP telephony, but not including device drivers for modems. Examples include HearSay, Web2Call, SoftPhone, and FaxPort.
Web Browsers	Software that interprets HTTP content, and presents it on the desktop screen. Examples include Netscape , MS Explorer , and Opera .

Critical Functions - Never Block Category

Software that is critical for system operations and that you cannot block. These categories are completely hidden in Websense Enterprise Manager, but can be viewed in reports from Client Policy Manager Reporter.

Category	Description
File Management - Never Block	Software that lets employees control file format, organization, backup, and transfer.
Infrastructure - Never Block	Software used for system assessment and maintenance, user support, and other administrative tasks.
Operating Systems - Never Block	Operating systems are relatively few in number. The most common are DOS ; the successively numbered Apple O/S applications; Windows ; and versions of Linux , and any executable directly associated with operating system functions.

Entertainment Category

Software intended to amuse or divert employees and that has little to no business value, except in very rare circumstances.

Category	Description
Adult	Software that includes depictions of nudity, sexual activity, or other elements that might be objectionable to non-consenting employees. Examples include VirtuaGirl and Sensual Jack .
Gambling	Software that enables online wagering or pay-for-play activity. Examples include Riverbelle and Gold Club Casino .
Games	Software that lets employees play games by themselves or with other players. Examples include Solitaire , Mah Jongg , and Bejeweled .
Screen savers	Software that creates a dialog box on the desktop screen when no keystrokes or mouse movements have occurred for some specified time. Examples include Fishtank Aquarium , Plus! Da Vinci , and Johnny Castaway .

Malware Category

Software that poses a threat to the security and integrity of networks or individual machines.

Category	Malicious Software: Description
Malicious Software	Software designed to attack or manipulate networks or local machines, and that may cause damage or make unauthorized use of information or resources. Examples include Duke , msblast.exe , and HoseMocha.java .

Miscellaneous Category

Software executables that are classified by something other than functions.

Category	Description
Java Files	Binary files containing code to be executed by a Java interpreter. Examples include files with .class or .jar extensions.
Scripts	Files containing non-malicious code that are executed by a scripting host. Examples include files with .bat , .pl , and .vbs extensions.
Temporary Internet Files	JavaScript files, which load onto the desktop chiefly in association with HTML files.

Productivity Category

Software executables that employees use regularly on the job, for business purposes.

Category	Description
Contact Managers	Programs that store and manage information about business clients, customers, publishers, and other classes of business contacts, and may also be called <i>personal information managers</i> . Examples include Act! , Sage , and Maximizer .
CRM	<i>Customer Relationship Management (CRM)</i> software that manages customer data, usually for Sales, Marketing, and Shipping and Receiving. Examples include SalesLogix , PeopleSoft CRM , and Kana iCare .
Data Warehousing, Analytics, Reporting	Software that gathers and stores large quantities of data, and that may analyze data and provide reports. Data warehousing applications include Red Brick Warehouse , and StorHouse/DM ; analytic applications include BusinessMiner , Scenario , and Clementine ; and reporting applications include Brio ONE , Crystal Reports , and Data Cruiser .

Category	Description
Database	Software that lets employees create and use structured sets of information, and that support analysis, synthesis, and comparison across large quantities of data in a database. Examples include Access and SQL clients .
Document Viewers	Software that lets employees create and view documents and diagrams, where the software is not incorporated into word processors or Web browsers. Examples include Acrobat Viewer , Visio Viewer , and PowerPoint Viewer .
ERP, SCM	<i>Enterprise Resource Planning (ERP)</i> and <i>Supply Chain Management (SCM)</i> software lets employees track and manage some or many core business processes, including Purchasing, Inventory, Human Resources, General Ledger and other accounting tasks, logistics and other planning processes. Examples include eTIMESheet , mySAP , iBaan , and QuickSell .
Graphics	Software that lets employees create sophisticated graphics and manipulate engineering or studio images. Examples include AutoCAD , AutoDesk , Volsh , Geocart , and Visio .
Presentation	Software that lets employees create and edit charts, slides, and multimedia displays. Examples include Pro Presentation , and PowerPoint .
Project Managers	Software that support project planning, estimating, scheduling, and managing, job tracking, and cost accounting. Examples include TimeControl and Timeslips .
Proprietary	Software developed within an organization for its own use, and not as a product or component of a product.
Reference, Information tools	Software that provides a body of reference information, and the means for accessing and displaying it. Examples include calendars, clocks, and calculators, Encarta , and Atomica .

Category	Description
Search, Retrieval, Knowledge Management	Software that lets employees search for data on file servers, intranets, or Web sites, and retrieve relevant results, and may support indexing. Examples include Copernic , Alexa , SmartEncode , Verity , and Autonomy .
Software Development	Software that lets employees create, debug, test, compile, and prepare applications to install the application, or use new software programs. Examples include Visual Basic , Visual Studio , and InstallShield .
Spreadsheets	Software that lets employees create and manage dynamic tables. Examples include Excel and Lotus 1-2-3 .
Suite, Integrated	Software utilities and other executables that are part of an application suite, but are not specifically associated with any one of them. For example, GRAPH9.exe , is a file in Microsoft Office, but is not one of the executables that run Word , Excel , or any other specific application.
Web, Desktop Publishing	Software that lets employees convert formats, manipulate and integrate text and image files for online or on paper publication. Examples include Quark Xpress and Macromedia .
Word Processing	Software that lets employees create, edit, view, and manage documents. Examples include Microsoft Word , AmiPro , and WordPerfect .

System Category

Software executables that define the basic operation of the desktop machine, enable higher-level executables, and perform other work focused on the machine itself, or on software, not on business tasks.

Category	Description
File Management	Software that lets employees control file format, organization, backup, and transfer. Examples include CuteFTP , WinZip , and NovaBACKUP .
Infrastructure	Software used for system assessment and maintenance, user support, and other administrative tasks. Examples include Remedy , nGenius , WebTrends , and CA Unicenter .
Installers	Software that installs applications of any type, for example, InstallShield .
Miscellaneous Utilities	Software that lets employees perform some task that is not otherwise categorized. Examples include Easy CD Creator and Palm Desktop .
Operating Systems	Operating systems are relatively few in number. The most common are DOS ; the successively numbered Apple O/S applications; Windows ; and versions of Linux , and any executable directly associated with operating system functions.
Scripting Hosts	Software that includes scripts for a variety of tasks. Examples of scripting hosts in this category include Windows Scripting Host , SQL Job Agent , and JavaScript Host .

Websense Port List

The following table identifies the ports, standard protocols and applications, the default ports for these protocols and applications that Websense provides for inclusion in port sets, described in [Working with Port Sets, page 243](#).

Because other default ports may be added to the Websense Enterprise Master Database as they are identified, this list may not be fully complete.

Port	Description	TCP	UDP	Other Ports Used
15	NETSTAT	X	X	
20	FTP-data	X		
21	FTP	X		
21	FSP		X	
22	SSH		X	
23	Telnet	X		
25	SMTP	X		
43	WHOIS/NICNAME	X	X	
47	GRE/PPTP	X		TCP 1723
53	DNS	X	X	
68	DHCP	X		
68	BOOTP		X	
70	GOPHER	X	X	
79	FINGER	X	X	
80	HTTP	X		TCP 8080
88	Kerberos	X	X	
101	HOSTNAME	X		
106	poppassd	X		

Port	Description	TCP	UDP	Other Ports Used
109	POP2	X		
110	POP3	X		
113	IDENT	X	X	
115	SFTP	X		
119	NNTP	X		
123	NTP	X	X	
135	Microsoft Exchange	X		
137	NetBIOS-ns		X	
138	NetBIOS-dgm		X	
139	NetBIOS	X		
143	IMAP	X		
161	SNMP	X	X	
220	IMAP3	X	X	
389	LDAP	X		
443	HTTPS	X		
514	RSH	X		
517	TALK	X	X	
518	NTALK	X		
531	IRC	X		
545	QuickTime	X		
553	RTSP	X		
554	RTSP	X		TCP 7070
563	NNTP over SSL	X		
593	MS-RPC	X		
636	SLDAP	X		
993	S-IMAP	X		
995	S-POP	X		
1080	SOCKS	X		

Port	Description	TCP	UDP	Other Ports Used
1352	Lotus Notes	X	X	
1433	Microsoft SQL Server	X	X	
1434	Microsoft SQL Monitor	X	X	
1494	Citrix ICA	X		UDP 1604
1604	Citrix ICA		X	TCP 1494
1723	PPTP	X		TCP 47
1755	Microsoft Windows Media	X	X	
3128	Squid	X		
3389	Microsoft RDP (Terminal Server)	X	X	TCP 1494, UDP 1604
5190	AIM	X		
5800	VNC	X		TCP 5900
5900	VNC	X		TCP 5800
6667	IRC	X		
6970	RTP	X	X	
7070	RTSP	X		TCP 553
8080	HTTP	X		TCP 80

GLOSSARY

APPLICATION DIGEST

A file that contains signature information for all applications found by a Client Agent during the inventory process.

AUTHENTICATION

The process of submitting a valid user name and password as evidence that the requestor has authority to perform the action. There are two general types of authentication: transparent and manual. Transparent authentication occurs when the software provides a user name and password automatically. Manual authentication occurs when the user must enter the user name and password.

Authentication may be required if the machine running Client Policy Manager must download the Websense Enterprise Master Database through a proxy server or firewall upstream from your integration partner. If such authentication is required, you can enter the user name and password required by the proxy server or firewall in the **Server Configuration** dialog box. Authentication may also be required in browsers, firewalls, and so forth.

BLOCK LAUNCH

When you create a rule and define the action as **Block Launch**, the rule prevents software launches.

BLOCK NETWORK ACCESS

When you create a rule and define network access as **Block Ports**, the rule prevents launched software from accessing the network.

BLOCK MESSAGE

A block message appears when the Client Policy Manager blocks an application. Client Policy Manager administrators can accept the default block message or create a custom message.

CATEGORIES

Categories define how an application is normally used, and enable Client Policy Manager to process launch requests appropriately when categories are used in rules. Categories also enable Client Policy Manager Reporter to filter information for reports.

CLIENT

The term “client” has several different definitions. A client may be a machine that accesses shared information from a server, or a machine that is running Client Agent. In Websense Enterprise Manager and Client Policy Manager Reporter, the term client may refer to users, user groups, machines and/or domains in your network. For the reporter, you can specify clients as filters of the information you see in a report.

CLIENT/SERVER AUTHENTICATION

Communications between Client Agent and CPM Server are authenticated for additional security. During installation, a passcode is specified. This code forces a unique encrypted signature that secures communications between the client and the server machines. This process makes it virtually impossible for anyone to attack or access information contained in the communications.

CLIENT AGENT

Client Agent is responsible for receiving instructions from CPM Management Server, and sending information back to it. Client Agent also performs inventories, and uses the local policy to determine how each launch request is handled. Client Agent is active whenever the system starts up or a user logs on.

CLIENT SET

A client set is a group of users, user groups, machines, and domains in any combination. Client Policy Manager processes a client set as a single entity. For example, you have two users, one user group, and one domain in a client set, and decide to block instant messaging for that client set. If anyone in the client set, or any one at any machine in the client set tries to launch instant messaging applications, the instant messaging software will not run.

CPM INVENTORY DATABASE

The CPM Inventory Database is populated by inventories collected at machines running Client Agent. This database is specific to your organization. The CPM Reporter accesses the database when any report requires inventory data.

CPM LOG DATABASE

The CPM Log Database is populated by employee launch requests. This is specific to your organization. The CPM Reporter and Explorer for CPM accesses data when any report requires launch request data.

CPM REPORT SCHEDULER

The CPM Report Scheduler schedules and processes requests for reports.

CPM REPORTER

The CPM Reporter calls data Client Policy Manager collects, and then stores the information in the databases. Reports can be scheduled or printed immediately, and may provide either summary or detail information.

CPM SERVER

The CPM Server handles all communications with Client Agent and other servers. CPM Server also populates the databases with information and retrieves information when necessary.

CUSTOM CATEGORIES

System administrators may create custom categories to identify what applications are designed to do, and to better manage system resources.

DATABASES

Your Client Policy Manager installation includes three databases. One, the Websense Enterprise Master Database is proprietary and encrypted. The other requires an SQL server for operations, and includes the CPM Inventory Database and CPM Log Database tables. Throughout Client Policy Manager documentation, these SQL tables are called databases for simplicity.

DIRECTORY SERVICE

A directory service identifies network resources and makes them available to users and applications. Resources include email addresses, machines, and peripheral devices such as printers. Directory services provide access to resources so networked users do not have to know where the resource is, or how it is physically connected.

DNS

A *Domain Name System* (DNS) is a distributed Internet directory service, used most often to translate domain names to IP addresses, or visa versa; and to control Internet email delivery.

DOMAIN

A domain is a group of users, user groups, machines and, devices on a network. The machines and devices share a common portion of an IP address, and are administered as a unit with common rules and procedures.

DOMAIN FOREST

A domain forest is an organizational group of one or more domain trees. The trees in a domain forest do not need to have continuous DNS names. A forest shares a schema, and Global Catalog Servers. The schema determines what types of objects, classes, and attributes may be created in each of the domain databases in the forest. *See also* DNS and Domain Tree.

DOMAIN TREE

A domain tree is an organizational group of one or more machines with the same root DNS name. For example, **it.win.websense.com** and **su.win.websense.com** share the same root, and are contiguous DNS names; but **superdooper.com** and **win.websense.com** are not. The machines in a domain tree are administered as a unit with common rules and procedures.

FILTERING

In the Client Policy Manager system, there are two definitions for *filtering*:

- ◆ Filtering is the process Client Agent uses to determine if a launch should be permitted or blocked, or if the employee must decide to continue the launch. Client Agent performs filtering based on the rules you define in Client Policy Manager.
- ◆ CPM Reporter uses filtering to determine the type of information a report includes. You define the filtering parameters when you create or use criteria sets.

GLOBAL RULE

The Global rule is the last rule CPM Server checks to define a policy. By default, the rule permits all applications and all ports. When you define your policy, change the network access setting in the Global rule to block ports.

This stops port access for any application not identified by earlier rules, thus providing Zero Day response for system security.

GROUP

A group of users that Client Policy Manager handles as a unit.

HARMFUL SOFTWARE RULE

The default Harmful Software rule is included with your Websense Enterprise Client Policy Manager installation as a means of blocking hacking, malware, and spyware. The rule is active immediately, providing extra security, even before you configure custom rules.

HEARTBEAT

Client Agent sends a regularly scheduled response to CPM Server indicating the client machine is alive and functional. When a machine is online but does not transmit, CPM Server assumes the client application is damaged, and may trigger repair.

IP ADDRESS

An *IP address* is a number that uniquely identifies a machine on a TCP/IP or UDP network. An IP address is a 32-bit numeric address written as four numbers separated by periods, where each number is between 0 and 255. For example, 192.168.0.253 can be an IP address.

LOCKDOWN

Lockdowns occurs when a system administrator runs an inventory on a system, and then uses the inventory to lockdown the machine. A lockdown restricts the applications at an identified machine to those in the original inventory.

LOCKDOWN RULE

The Lockdown rule is automatically installed with Client Policy Manager, but is empty. If you run inventories and use them to lockdown machines, Client Policy Manager automatically associates the lockdown to the Lockdown rule. You cannot change any values. To remove a machine from the Lockdown rule client set, you must remove the lockdown.

LOGGING

Logging occurs whenever an employee requests a launch. The Client Agent forwards log information to CPM Server, which stores the information in CPM Log Database. CPM Reporter then accesses the database to generate reports based on launch activity.

MACHINE

Machines are any computers on a network. The machine may be a desktop system, laptop, or server. Machines are identified by a machine name, an IP address, or by a user-defined asset tag.

MALICIOUS MOBILE CODE (MMC)

Any software program designed to move from machine to machine and/or network to network, in order to intentionally modify machine systems without the consent of the owner/operator.

NETWORK

A network is a range of IP addresses. launch requests are processed by the network or domain policy, and the specifics are defined by the rules.

POLICY

The CPM policy is identified by rules created in Websense Enterprise Manager and processed by Client Agent. The policy defines how application launches and network access attempts are handled.

PORT

A port is a numeric value that identifies a logical connection that two programs use for communications.

PROXY SERVER

A proxy server is software that acts as a relay between one network and another. Proxy servers are frequently implemented on security firewalls as one method of increasing network security, and reducing bandwidth consumption during Internet access.

PRODUCTIVITY CATEGORY

The Productivity category identifies applications common to homes and businesses. Applications in this category are sorted into the following default

subcategories: Contact Managers, Databases, Project Managers, Reference, Spreadsheet, Suite/Integrated, and Word Processing.

RULES

The CPM policy uses rules to define application access. Each active rule, in essence, is a four-part equation that Client Agent processes. The format is:

- ◆ **Part 1: Status**—rule is <Always Active> <Never Active> <Active when communications with CPM Server are possible> <Active when communications with CPM Server are not possible>
- ◆ **Part 2: Software Launch Control**—if <Client Set> tries to launch an application that is <In/Not In> this <Software Set>, then perform this action <Block, Continue, Permit>
- ◆ **Part 3: Network Access Control**—<Block, Permit Ports> in this <Port Set>
- ◆ **Part 4: Logging Control**—log the results of this rule as <Launch and Network, Launch, Network, No Logging>

SOFTWARE SETS

A list of executables that system administrators use to create rules. Client Policy Manager processes all executables in a software set as a single entity. For example, if you put Microsoft Word and Yahoo Instant Messaging executables into a software set, and then use the software set in a rule, Client Policy Manager blocks both executables, even though they are very different.

SERVERS

A server may be a hardware or software server. A hardware server is a machine that manages network resources. Software servers are the programs that manage network resources. For example, CPM Server is software that manages applications. CPM Server may be one of many applications on a given hardware server.

SUBNET

A portion of a network that shares a common address component. For example, all devices with IP addresses that start with **100.10** are part of the same subnet. Dividing a network into subnets is useful for both security and performance reasons.

SYSTEM ADMINISTRATOR

Staff members who configure CPM Server and define Client Policy Manager rules.

SYSTEM CATEGORY

Identifies applications that are common to homes and businesses. Applications in this category are sorted into the following subcategories: File Management, Infrastructure, Installers, Miscellaneous Utilities, Operating Systems, and Scripting Hosts.

SYSTEM FILE RULE

The **System File** rule is automatically installed with Client Policy Manager, and impacts applications that are critical to system operations. The **System File** rule takes precedence over all other rules, and any Outbreak entries.

USER

Users may be entire domains, groups—often defined by department or reporting roles--or individual users.

VIRUS

A piece of programming code that runs by itself and is able to replicate itself again and again. Some viruses are designed to transmit themselves across networks and bypass security systems.

WEBSense ENTERPRISE MASTER DATABASE

The Websense Enterprise Master Database is originally delivered with your Client Policy Manager installation, and identifies applications using a variety of tools. It also sorts known files into categories to help customers more easily manage software. You can define regular downloads to access the latest entries from Websense. Websense, Inc. does not include forced parameters for database downloads.

WORM

A self-replicating virus that does not alter files but resides in active memory and duplicates itself.

Index

A

- Active Directory, configuring, 71
- AppCatcher
 - configuring, 85
 - described, 44
 - introduction, 83
 - transfer details of, 86
- application logging interval, 104
- asset tags
 - adding, 144
 - clearing, 146
 - editing, 145
 - introduction, 143
- authenticated communications between client and server, 50
- authentication for proxy servers and firewalls, 66

B

- block messages
 - executables, 90, 96
 - multiple being displayed, 311
 - network lockdown for ports, 91, 98
 - not appearing on Windows NT or 2000, 310
 - Removable Media Lockdown, 92, 93, 99
 - user overrides, 93

C

- categories
 - accessing interface, 207
 - custom
 - adding, 216
 - deleting, 218
 - introduction to, 205
 - managing, 215
 - renaming of, 217

- restrictions for deleting, 218
- customizing
 - reference links, 28
- defined, 202
- introduction to, 201
- reclassifying executables, 212
- risk classes, 205
- rules for use of, 204
- understanding data, 209
- WebSense default
 - access, audio, visual, 320
 - access, privacy and security, 319
 - communication, 321
 - entertainment, 323
 - malicious software, 323
 - miscellaneous, 324
 - never block, 322
 - productivity, 324
 - system software, 327
- categories pane
 - accessing, 207
 - discovering executables in, 210
 - re-categorizing executables in, 212
 - reverting executables to WebSense categories, 214
 - viewing executable detail, 209
- classification wizard
 - running inventories with, 202
 - using, 219
- Client Agent
 - AppCatcher functions, 83
 - cancelling deployment of, 139
 - checking deployment status in Manager, 141
 - deploying or uninstalling, 135
 - deployment options in Manager, 134

- deployment status of, 132
 - described, 39
 - File and Printer Sharing services on
 - Windows XP, 130
 - introduction to, 127
 - machines not visible in Manager, 309
 - offline functions, 40
 - problems with upgraded machines, 313
 - rules based on connection status, 266, 273, 282
 - rules processing order, 275
 - startup functions, 40
 - system requirements for, 129
 - troubleshooting issue with, 308
 - upgrade considerations, 130
 - using the Manager to monitor
 - deployment, 131
 - VPN support for, 130
- Client Agent hardware requirements, 130
- client control
- enabling or disabling CPM policy, 106
 - heartbeats, 102
 - introduction, 102
 - settings, 104
- Client Deployment Service
- described, 38
 - options in Manager, 134
- client detail for single machines, 147
- Client Policy Manager database, 41
- client sets, 52
- accessing view in Manager, 193
 - adding, 196
 - copying, 198
 - defined, 191
 - deleting, 199
 - editing, 197
 - managing, 194
 - planning and development of, 192
 - reference links, 28
 - removing client from, 198
 - restrictions for creating, 192
 - restrictions for deleting, 199
- client status pane
- accessing, 141
 - deleting clients from, 148
- clients
- removing from selected list in Manager, 138
- client-to-client distribution port, 103
- components
- Client Agent, 39
 - Client Deployment Service, 38
 - Client Policy Manager database, 41
 - CPM Server, 38
 - reference for, 28
 - shared with Web filtering
 - Policy Server, 34
 - User Service, 34
 - Websense Enterprise Manager, 35
 - Websense Enterprise Master Database, 42
- configuration reference links, 28
- content pane of Websense Enterprise Manager, 112
- continue message
- employee interaction with, 97
 - for executables, 90
 - multiple being displayed, 311
 - not appearing on Windows NT or 2000, 310
- CPM policy
- access levels, 273
 - as implemented by rules, 56
 - enabling or disabling, 106
 - not being enforced, 304
 - saving in Manager, 295
 - understanding, 268
 - updates to, 270
 - Zero Day protection implementation in, 270
- CPM Reporter
- access problems in Manager, 302
 - criteria sets and inventories, 153
- CPM Server
- changing IP address of, 303
 - client heartbeat
 - and inventories, 103
 - description, 102
 - described, 38
- CPU usage excessive on Windows NT, 312
- criteria sets
- inventories in, 153

D

- database
 - controlling the size of, 301
 - inventory, 45
 - log, 46
 - troubleshooting issues, 297
- database download
 - authentication for proxies and firewalls, 66, 299
 - email failure notification, 67
 - error messages for, 300
 - firewall restrictions for, 299
 - interference of applications that restrict access, 300
 - introduction to, 77
 - manual, 80
 - monitoring, 80
 - proxy server information required for, 298
 - scheduling of, 78
 - URL access required for, 77
 - URLs to permit for, 297
 - verifying Internet access for, 298
- deployment status pane
 - accessing, 132
 - refreshing data in, 138
- desktop lockdown suite, 125
- desktop tab
 - introduction to, 35
- domain forest, 72

E

- email notification for events, 67
- employee information
 - demonstrations, 26
 - feedback, 26
 - publishing guidelines, 25
- encrypted key, 50
- error message
 - failure to read workstation data, 309
 - inventory, 305
- executables
 - adding to software sets, 239
 - adding to software sets (manually), 240

- file types, 44
- finding in categories pane, 210
- identifying scripts as, 45
- re-categorizing, 212
- removing from software sets, 242
- reverting to default Websense
 - categories, 214
- viewing uncategorized executables, 304

Explorer

- accessing
 - Start menu, 49
 - Websense Enterprise Manager, 49
- described, 48

Express Lockdown

- access controls in Manager, 118
- access to, 125
- configuring, 180
- description of, 180
- system requirements for, 180
- viewing status of, 183

F

- file types for executables, 44
- firewall identification, 66
- firewalls
 - restrictions for database download, 299

G

- global rule, 266
- guidelines for employees, 25

H

- hardware inventory
 - disk size listed as 0.0 GB, 308
 - duplicate entries for machines, 306
 - error messages, 305
 - physical memory data missing from, 307
- hardware requirements for Client Agent, 130
- harmful software rule, 264
- heartbeat
 - and inventories, 103
 - data sent, 40
 - description of, 102

- references, 102
- scheduling inventories around, 154

HTML tags in messages, 94

I

installation

- reference links, 28

inventories

- acquiring signature data, 44
- canceling, 161
- classification wizard for running, 202
- clearing completed inventory, 161
- CPM Reporter and criteria sets, 153
- deleting, 174
- error messages with, 305
- generating software sets
 - shared file machines, 165
 - specific machines, 164
- heartbeat interval and, 154
- lockdowns and, 177
- machine details in, 155
- managing, 162
- possible reasons for failure, 152
- problem launching software included in, 312
- reference links, 28
- removing machines from selected client list, 161
- results missing from Manager, 308
- running, 157
- running with classification wizard, 219
- similar software data in, 307
- status messages in, 156
- symbols used, 162
- troubleshooting issues for, 305
- understanding, 151
- using software sets in rules, 167

views

- accessing software views, 169
- applications, 172
- executables, 171
- filtering, 169
- hardware, 172
- removing filters, 171

- selecting, 167
- working with in Manager, 153
- ZIP drives missing from, 307

inventory database

- described, 42
- populating with data, 45

inventory status pane

- accessing, 154
- checking machine details in, 155
- introduction to, 151

IP address

- changing for CPM Server, 303

K

Keyloggers, 320

L

lockdown

- express
 - configuring, 180
 - viewing status of, 183
- inventory
 - applying, 178
 - introduction, 177
 - removing, 179
 - user access rights and, 178
- managing, 162
- problem launching software in inventory, 312
- removable media
 - block messages, 189
 - configuration of, 186
 - description of, 185
 - logging for, 189
 - supported bus types, 186
 - viewing status of, 188

lockdown rule, 265

log database

- described, 42
- populating with data, 46

logging

- application logging interval, 104
- defined in rules, 54
- defining for rules, 260

excluding users from, 294
machine data, 262
user data, 261

M

manager, *See Websense Enterprise Manager*

mass mailing rule, 264

menu options in Websense Enterprise
Manager, 110

messages

blocking for executables, 90, 96
continue option, 90, 97
customizing, 88
executable details (More Info), 100
HTML tags in, 94
introduction, 87
inventory status, 156
network lockdown for ports, 91, 98
Removable Media Lockdown, 92, 93, 99
See also block messages
suppression of, 90
user override selection, 93
user overrides, 149

Microsoft SQL database
configuring, 101

more information message, 100

MyWebsense, 110

N

naming conventions, 23

navigation pane of Websense Enterprise
Manager, 111

network lockdown message
for ports, 91
user interaction with, 98

O

offline functions of Client Agent, 40

operating environment, 32

organizational roles, 26

outbreak distribution, 103

outbreak rule

adding entries to, 121

description of, 118
disabling peer-to-peer communication, 123
overview, 263
removing entries from, 123
overriding messages, 93

P

password

changing, 82

peer-to-peer communication

description of, 119
disabling, 123
outbreak, 20

policy

defined, 31

Policy Server

adding, 60
connecting to, 61
deleting, 62
disconnecting from, 62
shared with Web filtering, 34

port list

adding ports manually, 247
deleting ports from, 249

port sets

accessing in Manager, 244
adding, 246
adding a range of ports, 249
copying, 252
creating
reference links, 29
deleting, 253
editing, 251
introduction to, 243
managing, 245
predefined, 244

ports

accessing and rules, 53
client-to-client distribution, 103
default ports, 329
network lockdown message for, 91

productivity goals, 24

Proxy avoidance, 320

proxy server

identifying, 66
information for database download, 298

R

Removable Media Lockdown

access controls in Manager, 118
access to, 125
configuration of, 186
description of, 185
logging for, 189
message, 92, 99, 189
supported bus types, 186
viewing status of, 188

Reporter

accessing
 Start menu, 48
 Websense Enterprise Manager, 48
description of, 29, 47

reporting tools, 22, 47

risk classes

defined, 205

rules

action of, 52
adding, 288
adding file names to emergency outbreak rule, 121
based on connection status, 266, 273, 282
basic set, 276
client sets, 52
components of, 286
copying, 291
default, 262
defining access levels with, 273
deleting, 294
disabling, 294
editing, 292
emergency outbreak, 263
evaluation of to implement policy, 56
global, 266
harmful software, 264
introduction and reference, 51
lockdown, 265, 277
logging controls in, 54
logging definitions for, 260

mass mailing, 264
moving, 293
network access control, 259
outbreak rule description, 118
port access, 53
precedence for, 275
recommended by Websense, 267
reference links, 29
removing file names from emergency outbreak rule, 123
reverting changes to, 287
security and productivity, 271
software launch control, 257
software sets, 52
status settings, 52, 256
streamlining, 283
system files, 263
understanding, 255
used in CPM policy, 268
users and groups, 280
using manually entered file names, 278
using software sets in, 167
using to exclude users from logging, 294
Websense default, 275
Zero Day protection response in, 270

rules pane

accessing from Manager, 287
description of, 285

S

scripts and CPM blocking, 45
security goals, 24, 25
services not starting on Windows NT, 308
settings pane, 63
signature checking, 43
software sets, 52
 accessing pane in Manager, 229
 adding, 232
 adding executables to, 239
 adding executables to (manually), 240
 categories in, 202
 copying, 236
 creating
 reference links, 28

- custom
 - for users and machines, 228
 - planning for, 227
 - deleting, 237
 - editing, 235
 - generating
 - shared file machines, 165
 - specific machines, 164
 - introduction to, 225
 - managing, 231
 - predefined, 226
 - removing executables from, 242
 - restrictions for creating, 234, 241
 - restrictions for deleting, 237
 - symbols for, 230
 - viewing contents, 238
- SQL database
- configuring, 101
- SQL Server
- as database engine, 42
- Start menu
- Explorer access from, 49
 - Reporter access from, 48
- startup functions of Client Agent, 40
- subscription
- aspects of, 32
 - defined, 31
 - process for in Manager, 63
- subscription level notification by email, 67
- summary data
- additional information access, 117
- symbols
- software sets, 230
- symbols in Websense Enterprise Manager, 113
- system files rule, 263
- system requirements
- Client Agent, 129
- T**
- TCP ports, 243
- technical support
- documentation feedback, 317
 - email, 316
 - fee-based, 315
 - support Web site, 315
 - telephone assistance, 316
 - Web portal, 315
- U**
- UDP ports, 243
- upgrading
- Client Agent, 130
 - Client Agent problems after, 313
- user rules, 280
- User Service
- configuration
 - Active Directory, 71
 - advanced settings (attributes), 74
 - domain forest, 72
 - supported directory services, 69
 - Windows NT Directory, 69
 - connection problems with, 302
 - CPM Service calls to, 38
 - shared with Web filtering, 34
- V**
- VPN support, 130
- W**
- Websense Enterprise Manager
- access to additional information, 117
 - accessing MyWebsense from, 110
 - accessing rules pane from, 287
 - asset tags
 - adding, 144
 - clearing, 146
 - editing, 145
 - introduction, 143
 - cancelling deployment of Client Agent
 - in, 139
 - categories pane, 207
 - changing password in, 82
 - Client Agent machines not visible in, 309
 - client detail, 147
 - client status pane
 - accessing, 141
 - deleting clients from, 148

- content pane, 112
 - CPM Reporter access problems, 302
 - current software sets pane, 229
 - deploying or uninstalling Client Agent
 - from, 135
 - deployment options in, 134
 - deployment status in, 132
 - desktop tab, 35
 - error message when reading workstation data, 309
 - Explorer access from, 49
 - Express Lockdown access from, 125
 - inventory controls, 154
 - inventory controls in, 153
 - inventory results missing from, 308
 - machine details in inventory pane, 155
 - making multiple selections in, 114
 - menu options, 110
 - navigation pane, 111
 - port sets access from, 244
 - refreshing data in, 114
 - Removable Media Lockdown access
 - from, 125
 - removing clients from deployment list, 138
 - Reporter access from, 48
 - rules pane description, 285
 - saving CPM policy in, 295
 - scheduling inventories and heartbeat intervals, 154
 - shared with Web filtering, 35
 - symbols use in, 113
 - troubleshooting issues, 302
 - updated information not appearing in, 304
 - user overrides, 149
 - User Service connection problems, 302
 - viewing client sets in, 193
 - Web browser selection, 115
 - Websense Enterprise Master Database
 - AppCatcher additions to, 84
 - default categories in
 - access, privacy and security, 319
 - audio, visual, 320
 - communication, 321
 - entertainment, 323
 - malicious software, 323
 - miscellaneous, 324
 - never block, 322
 - productivity, 324
 - system software, 327
 - described, 42
 - differential download, 51
 - downloading
 - introduction to, 77
 - manually, 80
 - monitoring, 80
 - scheduling of, 78
 - introduction to, 16
 - URL access required for, 77
 - Websense Enterprise Master Database, *See also database*
 - Windows 2000
 - block or continue messages not displayed on, 310
 - Windows Active Directory user service configuration, 69
 - Windows NT
 - block or continue messages not displayed on, 310
 - excessive CPU usage on, 312
 - problems starting services on, 308
 - Windows NT Directory
 - configuring, 69
 - Windows XP
 - requirements for Client Agent, 130
- ## Z
- Zero Day protection
 - described, 15
 - setting in rules, 270
 - ZIP drives not in inventory, 307