



Websense® Client Policy Manager™ (CPM) delivers desktop security protection against known and unknown security threats and prevents the execution of unauthorized applications. CPM enforces employee application use policies for corporate desktops, laptops, and servers with its unique and comprehensive database of categorized applications, which is updated daily. CPM provides a proactive critical component that closes the window of exposure to today's fast-moving and blended security threats.

## WebSense Client Policy Manager Solution

Websense Client Policy Manager is an innovative end-point security software solution that extends the power of the Websense Master Database to corporate desktops, laptops, and servers. CPM identifies and blocks known and unknown threats transparently without user intervention, and stops the execution of unauthorized applications, such as spyware, keylogging, peer-to-peer (P2P) file sharing, and hacking tools. CPM offers flexible, centralized policy management of application categories and individual applications. Through Websense directory integration, these policies can be implemented at a group level or tailored to individual needs ensuring that desktops are protected and adhere to corporate standards.

Working alongside firewalls and antivirus tools, with advanced lockdown features 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 where security systems are mis-configured. CPM delivers effective, proactive threat mitigation and flexible application use security policy enforcement.

## Key Features and Benefits

**Delivers proactive protection against known and unknown security threats.**

- **Websense Web-based Threat Mitigation™** - Provides unparalleled protection from web-based threats including keyloggers, spyware, Trojan horses, BOTS, scripts, and ActiveX controls. With the most comprehensive and effective database of malicious web-based applications, Websense offers the highest available level of protection by detecting and blocking more web-based threats than any other solution.
- **Websense Network Lockdown™** - Delivers proactive protection against known and unknown security threats by blocking application network access to specific ports and protocols by application category.
- **Websense Application Lockdown™** - Provides maximum control over desktop environments by allowing only approved applications to run on corporate PCs and servers, thereby preventing potentially malicious applications from launching. Detect and analyze end-point desktop security threats and application activity.
- **Websense Removable Media Lockdown™** - Allows system administrators to prevent devices such as flash drives, CD/DVD burners, floppy drives, and external hard drives from being used on client workstations. Organizations can also block writable media, depending upon your organization's policy.

## WebSense® Client Policy Manager™

### WebSense Client Policy Manager Benefits:

- Delivers proactive protection against known and unknown security threats.
- Detects, analyzes, and mitigates desktop security threats and application activity.
- Enforces flexible, auto-updating user and group application use security policies.
- Protects desktops both inside and outside of the corporate network, providing a valuable layer of security for a mobile workforce.
- Provides desktop security policy management from a central management console.
- Manages removable media to mitigate security and legal liability risks.
- Automatically updates security policies with no administrative intervention required.
- Provides unparalleled protection against web-borne threats.

### WebSense Client Policy Manager Scenarios:

**Your employee takes a laptop home or on the road and unknowingly downloads malware.**

**Question:** How do you keep the infection from spreading to your organization's network when the employee returns to the office or connects via your WAN?

**Answer:** Websense Client Policy Manager.

**A new piece of malicious mobile code enters your organization's network before your security solutions have time to develop an antidote and send out an update.**

**Question:** How do you keep your employees from running the destructive program?

**Answer:** Websense Client Policy Manager.

**Your employees have been transferring files via USB ports, opening a critical window of exposure to security risk and legal liability.**

**Question:** How do you keep your employees from using removable media drives without corporate oversight?

**Answer:** Websense Client Policy Manager.

**Your employee unknowingly receives a keylogger in an email and your antivirus solution does not recognize it.**

**Question:** How do you ensure that you keep the keylogger from harming your network?

**Answer:** Websense Client Manager.

- **WebSense Express Lockdown™** - Allows system administrators to swiftly prevent the execution of new applications thereby blocking attacks such as keyloggers, Trojan horses, worms and other malicious code threats. Unlike Application Lockdown, Express Lockdown does not require a machine inventory.

**Detects and analyzes end-point desktop security threats and application activity with WebSense Reporting Tools.**

WebSense Reporting Tools help identify potential problems with real-time and historical views of risks associated with web and application use by employees. Using this information, IT administrators can refine internet access and application policies to effectively reduce the risks associated with employee computing in their organizations. In addition, WebSense reporting tools provide powerful alerts and audit trails to help support compliance efforts.

**WebSense Reporting Tools**

- Determine your organization's risk profile.
- Detect the presence and location of malicious mobile code, spyware, hacking tools, or other security risks in your network.
- Perform critical software assessments that provide categorized and normalized views of programs and applications, enabling early threat detection and identification of potential application vulnerabilities.
- Refine your application use policies with insight from powerful reporting and forensic tools.

**Enforces flexible and auto-updating application use security policies.**

CPM enables users to enforce up-to-date application security policies with minimal administration.

- **Centralized Policy Management** - Minimizes administrative overhead in setting and enforcing security policies with the central, easy-to-use WebSense Manager.
- **Application Database** - Categorizes applications within the WebSense Master Database, allowing flexible security policies to be set by user, group, and most importantly, by category using comprehensive methodologies for categorizing thousands of applications into over 50 categories.

- **WebSense AppCatcher™** - Automatically and anonymously forwards to WebSense Master Database any unknown applications and associated network behavior at customer sites so that policies stay current.
- **WebSense Real-Time Security Updates** - WebSense Real-Time Security Updates allow organizations to obtain timely protection from new security threats. With Real-Time Security Updates, CPM is updated within minutes after new security threats are recognized, providing real-time management of web-based or application-based threats. These updates can occur several times per day, depending on need, and they supplement the regular daily updates to the WebSense Master Database. The Real-Time Security Updates are available as an add-on module to CPM.

**Ease of Deployment**

CPM makes it easy to begin managing corporate PCs and enforcing appropriate application security policies for end users.

- **Automated desktop agent deployment** - Deploys CPM desktop agents onto corporate desktops individually or globally with the click of a button in WebSense Manager.

**System Requirements**

**CPM Server**

**Hardware:** Pentium III processor or greater with at least 512 MB RAM. Hardware requirements will vary by configuration. Please see deployment guide for additional information.

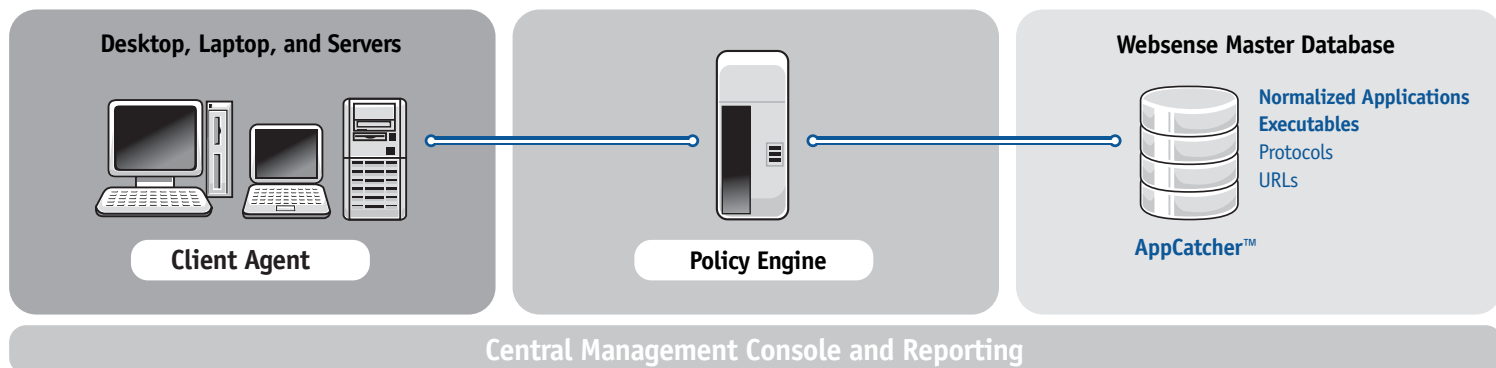
**Supported Operating Systems:** Microsoft® Windows® 2003 Server, Windows® 2000 Server (SP3 or greater).

**Supported Directory Services:** All Microsoft-supported directories

**CPM Client**

**Hardware:** CPM client supports most desktop hardware configurations. Please see deployment guide for additional information.

**Supported Operating Systems:** Microsoft® Windows® XP (SP1 or greater), Windows® 2003 Server, Windows® 2000 Pro/Server/Advanced Server (SP3 or greater), or Windows® NT 4 Client Server (SP6a or greater).



**Download a free, fully-functional 30-day evaluation at [www.websense.com/downloads](http://www.websense.com/downloads) today!**

**WebSense Inc.**  
San Diego, CA USA  
tel 800.723.1166  
tel 858.320.8000  
[www.websense.com](http://www.websense.com)

**WebSense UK**  
Chertsey, England  
tel +44 (0)1932. 796001  
[www.websense.co.uk](http://www.websense.co.uk)

**WebSense France**  
Paris, France  
tel +33 (0)15660. 5814  
[www.websense.fr](http://www.websense.fr)

**WebSense Germany**  
Munich, Germany  
tel +49 (0)89 24445. 4005  
[www.websense.de](http://www.websense.de)

**WebSense Japan**  
Tokyo, Japan  
tel +813.5322.1335  
[www.websense.co.jp](http://www.websense.co.jp)

**WebSense Australia**  
Sydney, Australia  
tel +61 2 9006. 1621  
[www.websense.com.au](http://www.websense.com.au)

**WebSense Greater China**  
Hong Kong  
tel +852.2855.8811  
[www.chinese.websense.com](http://www.chinese.websense.com)  
[www.prc.websense.com](http://www.prc.websense.com)

**WebSense Latin America**  
Sao Paulo, Brazil  
tel +55.11.4612.0798  
[www.espanol.websense.com](http://www.espanol.websense.com)  
[www.portugues.websense.com](http://www.portugues.websense.com)