websense®

Release Notes

Websense Content Gateway
Version 7.5

Contents

For updates published after these Release Notes:

For additional information that became available after these Release Notes were published, see the Knowledge Base article titled Websense Content Gateway v7.5 Release Notes Additions.

To view any Websense Knowledge Base article:

1. Log in to MyWebsense.

2. Click the **Support** tab, then click the **Knowledge Base** drop-down list and select Websense Security Gateway.

3. Enter the article title or number in the **Search** box.

New features in version 7.5

Supported platforms

Websense Content Gateway version 7.5 is supported on:

- Red Hat Enterprise Linux 5, update 3 and update 4, base or Advanced Platform (32-bit only)

  Although not certified, Websense, Inc. provides “best effort” support for newer versions of Red Hat Enterprise Linux. Under “best effort” support, Websense Technical Support makes a best effort to troubleshoot cases in standard fashion unless the issue is deemed a Red Hat Enterprise Linux-specific issue, at which point you must contact Red Hat directly for assistance.

> ✓ **Note**
>
> At the time of version 7.5.0 release, this known issue is documented: *Installation on Red Hat Enterprise Linux 5, update 5 does not install ARM*. The problem is easily worked around by following the procedure described in the Knowledge Base article titled “Installing the ARM on Red Hat Enterprise Linux 5, update 5”.

> ✓ **Note**
>
> Websense recommends that systems hosting Content Gateway be registered with **Red Hat Network** and kept up-to-date with the latest security patches.

Content Gateway is designed to run on a dedicated machine and is not guaranteed to be compatible with other server applications installed on the same machine.

A direct upgrade from a prior version of Content Gateway to version 7.5 is not possible. To migrate to Content Gateway version 7.5, update your operating system to the required version or obtain a machine running the required operating system. Then, install version 7.5 as a new installation.

For a complete description of platform requirements, see *Hardware* and *Software*.

Client authentication

Authentication realms

In networks with multiple authentication realms, rules can be defined to direct sets of IP addresses to distinct authentication servers (also known as domain controllers). Configuration is performed in the Content Gateway Manager. Rules are stored in the **auth.config** file.

Multiple authentication realms are supported for NTLM and LDAP. Separate rules must be created for NTLM and LDAP. Only one authentication method can be active at a time and only rules for that method are applied. Rules are applied first-match, top down in the list.

For more information, see the section titled *Multiple Authentication Realms* in Websense Content Gateway Online Help.

Additional authentication enhancements

- Transparent authentication configuration settings now have a separate tab in the Content Gateway Manager. Go to **Configure > Security > Access Control > Transparent Proxy Authentication**.
- Filtering configuration rules, stored in **filter.config**, can be written to match User-Agent header data. This allows administrators to write rules for applications that can be identified by User-Agent header data. For example, use a filtering rule to:
  - Allow applications that don’t properly handle authentication challenges to bypass authentication
  - Block certain client-based applications from accessing the Internet
- When **NTLM** authentication is configured, the **Fail Open** option can be used to allow requests to proceed when authentication fails due to no response from the domain controller, or because of malformed messages from the client.

  Fail Open provides excellent results when Web filtering is used with the proxy and an XID agent is configured. Then, if NTLM authentication fails, the requester can still be identified by the XID agent and the correct policy applied.

  Fail Open is enabled by default.

  (NTLM Fail Open was introduced into the 7.1 series of releases beginning with 7.1.4.)

Split DNS

Content Gateway can now be configured to use specific DNS servers to meet specific network access and network security requirements. For example, you can configure Content Gateway to use one set of DNS servers to resolve host names on your internal network, while allowing DNS servers outside the firewall to resolve hosts on the Internet. This maintains the security of your intranet, while continuing to provide direct access to sites outside your organization. For more information, see the section titled “Using the Split DNS option” in Websense Content Gateway Online Help.

Proxy chaining

Parent proxy configuration options

In Content Gateway Manager, several configuration options have been added for when Content Gateway is the child in a proxy chain. Options are set on the **Configure > Content Routing > Hierarchies > Parenting** tab.

New options include:

- Bypass the parent when a request is not cacheable
- Bypass the parent for tunneled requests
- Bypass the parent when traffic is HTTPS

HTTPS traffic in a proxy chain

Routing SSL traffic in a proxy chain involves the same parent proxy configuration settings used with other proxy-chained traffic. You identify the ports on which HTTPS requests should be decrypted and policy applied when SSL is enabled in **Configure > Protocols > HTTP > HTTPS Ports**. Parent proxy rules established in **parent.config** for HTTPS traffic (destination port 443) determine the next proxy in the chain for that traffic.

Tunneled traffic

Traffic on specified ports may be allowed to tunnel to an origin server. Content Gateway allows tunneling to the ports listed in **Configure > Protocols > HTTP > Tunnel Ports**, when SSL is not enabled. When SSL is enabled, traffic to any tunneled port that is also listed in the HTTPS Ports field is not tunneled, but is decrypted and filtering policy is applied.

HTTP privacy options

In Content Manager, on the **Configure > Protocols > HTTP > Privacy** tab, you can now set two common privacy options (set in records.config in prior versions):

- Select **Via** to insert a Via header into the outgoing request. Enabled by default.
- Select **X-Forwarded-For** to insert an X-Forwarded-For header into the outgoing request. Disabled by default.

Web Security Gateway: Scanning features

Scanning feature enhancements are described in more detail in the Websense Web Security/ Websense Web Filtering Release Notes. New capabilities include:

- Embedded URL link analysis: During Content Categorization, optional analysis of URL links embedded in the page contribute to categorization of the requested page.
- Content Categorization sensitivity control: A Content Categorization sensitivity control allows the administrator to increase or decrease the sensitivity of the analysis that classifies content.
- Tunneled Protocol Detection: Tunneled Protocol Detection detects protocols tunneling through the proxy using HTTP or HTTPS. This capability augments Network Agent in protocol detection

and policy enforcement. Signatures added to the database for tunneled protocol detection allow for the filtering of the Google Wave and Gmail Chat application protocols. These protocols are labeled "WSG only" in the Web Security Manager Protocols window. (Note that Network Agent can no longer filter the Gmail Chat protocol.) See the Knowledge Base article titled *Google Wave and Gmail Chat protocol signatures* for more information.

- Scanning of rich Internet applications: Security Threat scanning of rich Internet applications, such as Flash, to detect and block malicious content.
- Outbound content scanning: Outbound content scanning detects and blocks bot and spyware phone home traffic, and other malicious content.
- Web 2.0 History charts and Presentation reports

Web Security Gateway: SSL decryption bypass

To support organizations using SSL Manager to manage encrypted traffic, and who do not want to decrypt HTTPS sessions that users establish with sensitive sites, such as personal banking or health provider sites, administrators can now specify categories of sites that will bypass SSL decryption. A list of hostnames or IP addresses for which SSL decryption is **not** performed can also be maintained. These capabilities are configured on the **Scanning > SSL Decryption Bypass** page in TRITON - Web Security (Web Security Manager).

Web Security Gateway Anywhere: Data Security policy engine

When Content Gateway version 7.5 is installed, a copy of the Websense Data Security policy engine is also installed (it is disabled until registered). When the Websense Data Security Manager is installed and configured (on a separate system), and then registered with Content Gateway, the combination provides data loss prevention (DLP) over Web channels such as HTTP, HTTPS, FTP, and FTP over HTTP. For a detailed description of Websense Web Security Gateway Anywhere data loss prevention, see the Data Security Deployment Guide. For step-by-step Data Security registration instructions, see the section titled *Working with Websense Data Security* in the Websense Content Gateway Online Help.

As in prior releases of Content Gateway, Websense Data Security Suite is also supported over ICAP.

Web Security Gateway Anywhere

Websense Web Security Gateway Anywhere™ is a Web security solution designed for distributed enterprises with one or more branch offices and multiple remote users.

Web Security Gateway Anywhere offers an alternative to pure service-based or pure appliance-based solutions. Rather than choosing between an all in-the-cloud or all on-premises Web filtering solution, you can deploy a blended solution that encompasses the best of both worlds, and you can manage it from a single user interface—the TRITON™ Unified Security Center.

Web Security Gateway Anywhere includes Websense Web Security and Websense Content Gateway as well as hybrid Web and DLP features. For complete information, see the Websense Web Security Gateway Anywhere Getting Started Guide.

Within the TRITON Unified Security Center, the names of several components are changed.

TRITON Unified Security Center name	Version 7.1 name
TRITON - Web Security	Websense Manager
TRITON - Data Security	DSS Manager
***Content Gateway Manager - *cannot be accessed within TRITON Unified Security Center in version 7.5**	Websense Content Manager

Corrected in version 7.5

The following problems have been corrected.

- After creating a very large list of access configuration rules (>300), clicking Apply to save the rules resulted in an empty list.
- In a proxy chain in which Websense Content Gateway was the downstream proxy, the “No DNS and Just Forward to Parent” option was enabled, the proxy handled explicit traffic, and the traffic was HTTPS, the proxy would return a Server Hangup error.
- When the proxy handled explicit traffic, ARM was enabled, and NTLM authentication was configured, NTLM authentication was not always performed when Internet Explorer was the browser.
- Sometimes when Websense Content Gateway connected to the Database Download Server, the connection timed out.
- When Websense Content Gateway was connected to an origin server using HTTP 1.0, the connection was not closed until the connection with the server timed out.
- When Websense Content Gateway serviced transparent traffic, HTTP 1.0 clients could not connect to HTTPS sites.
- Microsoft Windows Update failed when sent through the proxy.
- When hosted on an HTTPS site, some CRLs (certificate revocation lists) would not download through the proxy.
- When SSL was enabled with the certificate validation option enabled and the client certificate create incident option enabled, sometimes no incident was created when an HTTPS site requested a client certificate.
- Caching was enabled even though it had been disabled during installation.
- Enabling both SOCKS and NTLM caused the proxy to reset.
- Upgrading failed if /tmp became full.
- Snapshots were not preserved across upgrades.

New features in version 7.1.4

- Updated Root CA store: For users of SSL Manager, the Root CA store has been updated to match the latest versions of Internet Explorer (version 8) and Firefox (version 3).
- Transparent authentication settings now have a separate tab in Websense Content Manager. Go to **Configure** > **Security** > **Access Control** > **Transparent Proxy Authentication** to set **Redirect Hostname**, **Authentication Mode**, and **Session TTL** (time-to-live).
- Filtering configuration rules (stored in **filter.config**) can be written to match **User-Agent** header data. This allows administrators to write rules that match applications that can be identified by User-Agent value.

Corrections in version 7.1.4

The following problems have been corrected:

- When Websense Content Gateway handled FTP requests, user names that included an "@" symbol (e.g.: abc@ftp.server.com) failed to connect, returning "501 Syntax error in parameters or arguments".
- When handling FTP requests, after Websense Content Gateway connected to the FTP server, sometimes the user would receive a "/ Folder not found" error.
- When storing content in the cache, if the document size exceeded the configured maximum document size (unlimited by default), the connection was left in the CLOSE_WAIT state, which does not release the associated file descriptors. When the number of file descriptors reached 5000, the proxy reset.
- When browsing to secure Web sites that other browsers could access, the Macintosh Safari browser failed to access the site, returning an error stating that the identity of the Web site could not be verified.
- In some situations, when Websense Content Gateway experienced a very high number of concurrent connections, the proxy would reset.
- When NTLM was configured for authentication, some error responses from the domain controller were erroneously counted as domain controller failures, which could cause the proxy to treat the domain controller as if it were down, suspending attempts to authenticate users.
- When NTLM was configured for authentication, if the host name exceeded 16 characters, authentication failed.
- With SSL Manager, when the destination server requested a client certificate and the **Create incident** option was enabled, sometimes no incident was created for some sites.
- When Websense Content Gateway was the parent proxy in a chain and a child proxy performed user authentication, expected user-based policy was not applied to HTTPS requests. Note: For this configuration to work, **Read authentication from child proxy** must be enabled on the **Configure** > **MyProxy** > **Basic** page in Websense Content Manager.
- When a 2-digit port was added to the **HTTPS Redirect** port tunnel list, traffic on that port was not tunneled.
- CPU usage spikes related to the processing of Scanning data files have been remedied. Download time has been cut by two thirds (average). File load time (into memory) has been reduced by half.

- When real-time Scanning was enabled, the scanning routines did not always release all of the memory they used. This could eventually cause the proxy to reset.

New features in version 7.1.3

- IP spoofing is supported in networks that use WCCP-configured devices.

  IP spoofing is applied to HTTP traffic only.

> **Warning**
>
> Deploying IP spoofing requires precise control over the routing paths on your network, overriding the normal routing process for traffic running on TCP port 80.
>
> With IP spoofing enabled, traditional debugging tools such as **traceroute** and **ping** have limited utility.

For more information, see *IP spoofing*, in Websense Content Gateway Online Help.

Corrections in version 7.1.3

The following problems have been corrected:

- After Microsoft security patch MS09-13 (April, 2009) was applied to Internet Explorer 7 or 8, NTLM credential caching stopped working for users of those browsers. After upgrading to 7.1.3, sites using NTLM authentication and NTLM credential caching (enabled by default) will benefit from many more authentication requests serviced from cache.

  It is recommended that you review your settings at **Configure** > **Security** > **Access Control** > **NTLM** and that you adjust the credential cache timeout (**Caching TTL**) to a value that meets your performance and security requirements. The existing value of **Caching TTL** is not changed by the upgrade (3600 seconds by default). If 7.1.3 is a new installation (rather than an upgrade), the default value of **Caching TTL** is 900 seconds.

  Also on the **Configure** > **Security** > **Access Control** > **NTLM** screen, in the **Multi-user Hostnames** field (renamed **Multi-user IP Exclusions** in version 7.1.4), you may create a list of Microsoft Terminal servers or Citrix servers that access the Internet through the proxy. Credentials for users on the hosts in that list cannot be cached. For sites using version 7.1.3, the host exception list in the **Multi-user Hostnames** field can contain only IP addresses and IP address ranges, separated by commas. Host names in any other format are ignored. So, a previous exception list containing host names (instead of IP addresses) would need to be re-entered with IP addresses, immediately after upgrade.
- Websense Content Gateway was not compatible with upstream Sun Java System Web Proxy Server.
- In some configurations, when a domain controller used by the proxy reset or went off line, for several minutes (sometimes as many as 20) the proxy would become very slow or appear to stop processing traffic.

- When a very large file download was followed immediately by a second download of the same file, the second download would sometimes fail.
- When a very large file download was initiated with a HEAD request, the download would fail.
- Attempts to update the Scanning data files through the Database Download Server (DDS) sometimes failed with: “Error connecting to Websense DDS”.
- Sometimes when an HTTPS site returned an expired RootCA, the certificate was added to the certificate tree.
- When the proxy was configured to handle transparent traffic and SSL was enabled, attempts to access some HTTPS sites produced the error “Connection refused” or “Unable to connect to the next proxy”.
- In version 7.1.2, when Websense Content Gateway received traffic as a transparent proxy and packets were bypassed, a kernel debug message was displayed on the console for every bypassed packet.
- When NTLM authentication was used with Internet Explorer 8 and Windows 7, requests for HTTPS pages did not display.
- When Websense Content Gateway was deployed in a cluster with transparent proxy service supported by WCCP, and client authentication was transparent NTLM, proxies in the cluster did not identify themselves uniquely to the domain controller causing authentication to fail.

Corrections in version 7.1.2

The following problems have been corrected:

- Windows Update failed to complete when routed through the proxy.
- When a backed up root CA that was originally created in Websense Content Manager was re-imported in Content Manager, the import failed with the error: This is not a valid certificate or a certificate chain.
- When Websense Content Gateway was deployed as a transparent proxy, when visiting sites that used an extended validation certificate, the user would receive an “invalid name” certificate error.
- When Websense Content Gateway was deployed as an explicit proxy, only Basic Authentication to the content server would work for Internet Explorer. (Proxy Authentication was unaffected.)
- A static bypass rule that specified only a destination IP address, whether it was a single IP address or an IP address range, did not work.
- Sometimes after installation, Websense Content Gateway couldn’t connect to the Download Server. The condition resolved only after the Websense Web filtering service was restarted.
- In rare circumstances, when Websense Content Gateway processed high volumes of traffic, the proxy would reset. The proxy log file (default: /opt/WCG/logs/content_gateway.out) would record a FATAL error or 2 Signal 11 messages, 1 accompanied by a stack trace.

Corrections in version 7.1.1

The following problem was corrected:

- In some instances, when transferring multi-gigabyte files over HTTP, or over HTTPS when configured as an explicit proxy, Websense Content Gateway failed to forward all of the requested data to the client.

  As documented in the Installation Guide and Content Manager Online Help, when Websense Content Gateway is an explicit proxy, HTTPS traffic should be routed to port 8070. In Content Manager Online Help, see the topic titled *Working with Encrypted Data > Running in explicit mode*.

Operation tips

Hardware

CPU	Quad-core running at 2.8 GHz or faster
Memory	4 GB
Disk space	2 disks: • 100 GB for the operating system, Websense Content Gateway, and temporary data. • 147 GB for caching If caching will not be used, this disk is not required. The caching disk: – Should have minimum size of 2 GB, maximum 147 GB for optimal performance – Must be a raw disk, not a mounted file system – Must be dedicated – Must *not* be part of a software RAID – For best performance, use a 10K RPM SAS disk on a controller that has at least 64MB of write-through cache.
Network Interfaces	2

To support transparent proxy deployments:

Router

WCCP v1 routers support redirection of HTTP only. If your deployment requires additional protocols, such as HTTPS, your router must support WCCP v2.

A Cisco router must run IOS 12.2 or later.

The clients, the destination Web server, and Websense Content Gateway must reside on different subnets.

—or—

Layer 4 switch

You may use a Layer 4 switch rather than a router.

To support WCCP, a Cisco switch requires the EMI or IP services image of the 12.2SE IOS release (or later).

Websense Content Gateway must be Layer 2 adjacent to the switch.

The switch must be able to rewrite the destination MAC address of frames traversing the switch.

The switch must be able to match traffic based on the layer 4 protocol port (i.e., TCP port 80).

Software

Linux operating system:

- Red Hat Enterprise Linux 5, update 3 and update 4, base or Advanced Platform (32-bit only)

  Although not certified, Websense, Inc. provides “best effort” support for newer versions of Red Hat Enterprise Linux. Under “best effort” support, Websense Technical Support makes a best effort to troubleshoot cases in standard fashion unless the issue is deemed a Red Hat Enterprise Linux-specific issue, at which point you must contact Red Hat directly for assistance.

  - Only kernels shipped with the above Linux versions are supported by Websense Content Gateway. Visit www.redhat.com for kernel information. To display the kernel version installed on your system, enter the command:

    ```
    /bin/uname -r
    ```

    Important

    If SELinux is enabled, disable it before installing Websense Content Gateway.

  - PAE (Physical Address Extension)-enabled kernel required
    - By default, Red Hat Enterprise Linux 5, update 3 and later has PAE enabled. If you are running the non-PAE kernel, reboot with the PAE-enabled kernel before installing Websense Content Gateway.
  - RPM compat-libstdc++-33-3.2.3-47.3.i386.rpm (or higher version of this package)
    - To display a list of RPMs installed on your system with the string “compat-libstdc” in their name, enter the command:

      ```
      rpm -qa |grep compat-libstdc
      ```
  - GNU C library (glibc) version 2.5-42

  - Note that Red Hat Enterprise Linux 5, update 3 ships with glibc version 2.5-34. Be sure to update it to version 2.5-42.
  - Example command to update this library (running as `root`): `yum update glibc`.

Websense Web filtering products:

- Version 7.5

> **Important**
>
> Websense filtering software must be installed prior to Websense Content Gateway. When the filtering software is installed, Content Gateway must be specified as the integration product.

Websense Data Security:

- On-box policy engine: Version 7.5
- ICAP: Any 7.x version

When Content Gateway is used with Websense Data Security only (no Web filtering) the order of installation does not matter.

Supported browsers:

- Content Gateway is configured and maintained with a Web-based user interface called the Content Gateway Manager. Supported browsers include:
  - Internet Explorer 7 and 8
  - Mozilla Firefox 3

Cache size

Cache size should be restricted to 147 GB. This size provides optimal resource utilization while also providing an excellent end-user experience. Because today’s Internet sites are often composed of dynamic, uncacheable content, caching is a less significant factor in the end user’s Web browsing experience.

Software installation cannot be completed without Internet connectivity

It is recommended that the Content Gateway host computer have Internet connectivity before starting the software installation procedure. The software will install without Internet connectivity, but Websense license keys (and licensed features) cannot be validated until Internet connectivity is available.

Proxy ‘admin’ password restrictions

The password you enter for the Content Gateway administrator during installation (default name: admin) must be 15 characters or fewer.

To create a strong password (recommended), use 8 or more characters, with at least 1 each of the following: capital letter, lower-case letter, number, special character.

The password **cannot** contain the following special characters:

- space
- $ (dollar symbol)
- : (colon)
- ‘ (backtick; typically shares a key with tilde, ~)
- \ (backslash)
- “ (double-quote)

Installation file paths

During installation, when you specify installation file folders and file names:

- Use only upper-case and lower-case letters, digits, hyphens, and underscores.
- Do **not** use spaces in file or folder names.
- Do **not** use single quotes or other non-standard characters.

Although you may not be prevented from entering quotation marks or other special characters in the path name, the installation itself may be unable to complete successfully.

Security recommendations

Websense recommendations for the physical and operational security of your proxy server are included in the Websense Content Gateway Installation Guide and in 2 Knowledge Base articles: *Proxy security and hardening recommendations*, and *Configuring IPTables for Websense Content Gateway.*

Port configuration

A full deployment of Content Gateway requires that several ports be open. See the Websense Content Gateway Installation Guide for information about open ports and reassignment ports, if necessary.

Configuring your router

If your site is running Content Gateway in a transparent proxy deployment and you intend to proxy HTTPS or FTP traffic, you must use the SSL Manager and you must configure your router to support WCCP v2. See Websense Content Gateway Online Help.

Configuring multiple ports for the HTTP WCCP v2 service group

When using WCCP v2 routers to support transparent proxy traffic, administrators can configure multiple ports for the HTTP service group in **records.config**.

Configuration Variable Data Type	Default Value	Description
`proxy.config.wccp2.HTTP_svc_port` `STRING`	`80`	Specifies multiple HTTP ports. Ports are given in a comma-separated list, i.e.: 80,81,82,99 To use this variable you must add it to **records.config**.

Virtual IP address must not match any real IP address

When configuring the Virtual IP feature, make sure that the Virtual IP addresses do not conflict with any existing IP addresses assigned to the system.

Email address for receiving proxy alarms

In Content Gateway Manager, on the **Configure** > **General** tab you can provide an email address to receive proxy Alarm email (for example, admin_proxy_one@acme.com).

Email addresses for alarm notifications cannot be longer than 64 ASCII characters. The management interface does not enforce this character limitation, but an invalid email address may prevent the proxy from starting.

To correct an email Alert address, manually edit ***<Install_Dir>*****/config/records.config** (default location: /opt/WCG/config/records.config) and modify the line containing the email address string:

```
CONFIG proxy.config.alarm_email STRING admin_proxy_one@acme.com
```

Restart the proxy after protocol settings change

Any time you change your protocol settings in Content Gateway Manager (for example, with **Configure** > **SSL** > **Decryption/Encryption** > **Inbound** > **Protocol Settings**), you must restart the proxy for the new settings to take effect.

Reverse proxy

Content Gateway **does not** function as a reverse proxy.

Reverse DNS

In prior versions of Content Gateway, by default the proxy performed reverse DNS lookup whenever a URL contained an IP address and there was a rule in **filter.config**, **cache.config**, or **parent.config**. In version 7.5, reverse DNS lookup is disabled by default. If you have rules in **filter.config**, **cache.config**, or **parent.config** that are based on destination hostname or domain name, you need to enable reverse DNS lookup on the **Configuration** > **Protocols** > **HTTP** > **General** tab.

Registering with the Data Security Management Server

When Content Gateway is **not** located on a V-Series appliance (is installed on a separate Linux server):

- Registration with Data Security Management Server requires that the Content Gateway host system have an IPv4 address assigned to the eth0 network interface. After registration, the IP address may move to another network interface on the host; however, that IP address is used for data security configuration deployment and must be available as long as the two modules are registered.
- The Content Gateway host system must have a unique fully qualified domain name (FQDN) specified in the **/etc/hosts** file. (This is done automatically as part of the setup process on V-Series appliances.)

The process of registering Content Gateway with the Data Security Management Server is described in detail in the Websense Content Gateway Online Help.

Browser limitations

Not all Web browsers support all authentication modes.

The browsers that provide the most complete support are: **Internet Explorer 7 and 8**, and **Mozilla Firefox 2 and 3**. Other browsers have limitations, especially when the configured mode is NTLM (Integrated Windows Authentication/Single Sign-on). Transparent NTLM authentication is **not** supported by Google Chrome, Opera or Windows Safari.

Browser	When the client request originates on a **different domain** than the proxy (prompt for credentials)		When the client request originates on the **same domain** as the proxy (transparent authentication; no prompt)	
	HTTP	HTTPS	HTTP	HTTPS
Internet Explorer 7 and 8	Full support			
Mozilla Firefox 2 and 3	Full support			
Google Chrome	NTLM transparent authentication: Not supported. The user is prompted for credentials.			
	Explicit authentication: Supported. The user is prompted for credentials.			
Opera 10	NTLM transparent authentication: Not supported. The user is prompted for credentials.			
	Explicit authentication:			
	Supported. The user is prompted for credentials.	Not supported.	Supported. The user is prompted for credentials.	Not supported.

Browser	When the client request originates on a **different domain** than the proxy (prompt for credentials)		When the client request originates on the **same domain** as the proxy (transparent authentication; no prompt)	
	HTTP	HTTPS	HTTP	HTTPS
Windows Safari 4	NTLM transparent authentication: Not supported. The user is prompted for credentials.			
	Explicit authentication:			
	Supported. The user is prompted for credentials.	Supported. When LDAP authentication is configured, the user is prompted twice for credentials.	Supported. The user is prompted for credentials.	Supported. When LDAP authentication is configured, the user is prompted twice for credentials.

When prompted for credentials, if the user does not enter a domain name, a "session timeout" error can result, or the user may be re-prompted.

Mozilla Firefox users browsing from the same domain as the proxy may sometimes be prompted multiple times for authentication. The user should configure the browser as follows:

1. Open Firefox and enter "about:config" in the location bar.
2. Click the "I will be careful I promise" button.
3. In the **Filter** entry field enter "ntlm".
4. Double click "network.automatic-ntlm-auth.trusted-uris" and enter: http://<*proxy_name*>:8080

   For example: http://XYZProxy1:8080
5. Click OK and close and reopen the browser.

Active Directory 2008 with NTLM

As in past version 7-series releases, support is provided for Windows Active Directory 2008 with NTLMv1.

If you plan to authenticate users with NTLM and Active Directory 2008, you must use port 445 or turn on the Windows Computer Browser service on the Active Directory servers. Also, the Windows **Network Security: LAN Manager Authentication level** must be set to **Send NTLM response only**. See your Windows Server 2008 documentation for details.

To enable the Windows Computer Browser service, perform the following procedure on each machine running Windows Server 2008 and Active Directory:

1. Make sure that Windows Network File Sharing is enabled.
   a. Go to **Start** > **Network** > **Network and Sharing Center**.
   b. In the **Sharing and Discovery** section, set **File Sharing** to **On**.
2. Go to **Control Panel** > **Administrative Tools** > **Services**.
3. Double-click **Computer Browser** to open the Properties dialog box.
4. Set the **Startup type** to **Automatic**.

5. Click **Start**.
6. Click **OK** to save your changes and close the Services dialog box.

NTLM load balancing and failover

When NTLM is configured and multiple domain controllers are specified, even if load balancing is *disabled*, when the load on the primary domain controller reaches the maximum number of connections allowed, new requests are sent to a secondary domain controller as a short-term failover provision, until such time that the primary domain controller can accept new connections.

Accessing Intranet sites in an explicit proxy deployment

If your clients cannot access your Intranet sites, verify that your operating system has been correctly configured to resolve all internal and external host names. Use the **nslookup** command to verify that a domain is listed in your DNS server:

For internal-facing servers:

```
nslookup intranet.mycorp.com
```

For external Web sites:

```
nslookup www.websense.com
```

If your corporation has multiple DNS domains, verify that a host name in each domain resolves correctly. If you are unable to resolve host names, verify the contents of the **/etc/resolv.conf** file, which provides search rules for how domain names are resolved in DNS.

Known issues

Installation on Red Hat Enterprise Linux 5, update 5 does not install ARM

When version 7.5 is installed on Red Hat Enterprise Linux 5, update 5 (base or Advanced Platform; 32-bit only), the installer warns that the kernel version is not supported. Should the user enter ‘y’ to continue the installation, the installation appears to complete normally, but the ARM is not installed.

For instructions on how to install the ARM for Red Hat Enterprise Linux 5, update 5, see the Knowledge Base article titled “Installing the ARM on Red Hat Enterprise Linux 5, update 5”.

Restart of Content Gateway can cause warning message

When you restart the proxy, you may see this message: “Warning: Form data out of date. Press Cancel to reload page and try again.”

Simply press **Cancel** to reload the page and restart again.

Virtual IP address not enabled or disabled on nodes in a cluster

When a Virtual IP address is enabled or disabled on one node in a cluster, this change does not propagate until the other nodes are restarted.

Alarm indicates that connection throttle is too high

After initial installation, Content Gateway Manager may display an alert that the throttle connection limit is too high. The condition is resolved by rebooting the proxy.

Child proxy cannot pass credentials to parent proxy

When Content Gateway is the downstream child in a proxy chain and it authenticates users, it cannot pass authentication credentials to the parent proxy. If the parent proxy cannot authenticate the client, the user request cannot be processed.

This situation occurs whether the upstream parent proxy is a third-party proxy or another Content Gateway proxy.

Workarounds are described in the Knowledge Base article “Websense Content Gateway as child proxy passing credentials to parent proxy”.

Parent proxy not authenticating

In a hierarchical caching environment, users cannot access the Internet if the proxy is running in a transparent proxy deployment, and NTLM or LDAP authentication is through the parent proxy.

For best results, authentication should take place on the proxy closest to the browser. A parent cache may contain child proxies that perform authentication. If authentication is through the child proxy, ensure that users/browsers do not have access to the parent proxy; otherwise they will be able to bypass authentication.

Enabling IP forwarding

By default, IP forwarding is disabled when Content Gateway is installed. Rebooting Content Gateway after installation enables IP forwarding. Note that IP forwarding must be enabled for static and dynamic bypass rules to take effect in a transparent proxy deployment.

You can also enable IP forwarding via the command line.

1. Become root and enter the root password.
2. Add the following line to the **/etc/sysctl.conf** file:

   ```
   net.ipv4.ip_forward = 1
   ```

3. Enable the changes:

   ```
   sysctl -p /etc/sysctl.conf
   ```

Then edit the **bypass.config** file as appropriate. See Websense Content Gateway Online Help for details on **bypass.config**.

Web sites in the Static or Dynamic bypass list fail to connect

When Content Gateway is a transparent proxy, normal requests succeed as expected, but requests to IP addresses listed in static or dynamic bypass rules can fail to connect to the server. The problem occurs when the outbound request is routed using the proxy’s routing table instead of to a router that knows how to route to the client IP address.

To work around the problem, modify the proxy's routing table such that the return frames are directed to a router that can route client traffic. For more information, see the Knowledge Base article titled "Web sites in the Static or Dynamic bypass list fail to connect".

Internet Explorer using a PAC file may choose wrong proxy port

The automatic proxy caching feature in Internet Explorer may ignore the protocol field in the URL and send client requests to the incorrect proxy port. Consider disabling automatic proxy caching in Internet Explorer. For information, see http://support.microsoft.com/?kbid=271361.

NTLM: No 'domain controller down' message with HTTPS

When NTLM is the authentication method and a client makes an HTTPS request and the domain controller is down (or otherwise not responding), no error message is displayed in the browser.

If the user is prompted for credentials with NTLM single sign-on

In a transparent proxy deployment, users may be prompted for credentials when using NTLM single sign-on. Users who need single sign-on through Internet Explorer must set a local Intranet site to the IP address of the proxy. If you do not achieve the desired results using dot notation (xx.xxx.xx.xxx), use the URL that resolves to the IP address of the proxy.

To configure Internet Explorer for single sign-on, you must configure the browser to consider the proxy as a local server.

Follow these steps in Internet Explorer:

1. Select **Tools** > **Internet Options** > **Security** > **Local intranet** > **Sites** > **Advanced**.
2. Enter the URL or IP address of the proxy.
3. Click **Add**.
4. Click **OK** until you have closed all the dialog boxes.

Then:

1. Select **Tools** > **Internet Options** > **Security** > **Internet** > **Custom Level**.
2. Select **Automatic logon with current username and password**. You can find this near the bottom of the settings tree.
3. Click **OK** until you have closed all of the dialog boxes.

Usernames with extended characters may not authenticate

When authentication is done through the proxy, usernames containing extended characters authenticate only when the client browser is Internet Explorer. When other browsers are used, such names fail to authenticate, leaving the user unable to browse.

If this occurs, use a Websense filtering transparent identification (XID) agent, instead of the proxy, for user identification.

Also note that although names with extended characters authenticate with Internet Explorer, the names may not appear in reports.

Content Gateway services may not start if a port conflict exists

Content Gateway services, including Content Gateway Manager, will not start if there is a port conflict. A port conflict results when a Content Gateway service attempts to use the same port as any other service running on Linux, including other Content Gateway services. Users are not informed that there is a port conflict.

For more information, see the Content Gateway Installation Guide.

Limited access filter conflicts with content stripping

In Websense Web Security, a list of individual Web sites (called a limited access filter) can be active in a Web filtering policy. When a limited access filter is active in a policy, users assigned that policy can visit only sites in the list. All other sites are blocked.

When a limited access filter is in effect, Websense software checks to see only if a requested site appears in the list. No other checking is performed.

However, an exception exists in Content Gateway.

If you enable Content Stripping for ActiveX, JavaScript, and VBScript, and then add the hostname of a URL from a limited access list to the Always Scan List for Content Stripping in the Web Security Manager, then ActiveX, JavaScript, and VBScript content is stripped from that URL, even when the limited access list is active in the users' policy.

To work around this exception, so that no content is stripped, remove the URL hostname from the Always Scan List for Content Stripping.

Filtering rules cannot include backslash in regular expressions

The Primary Destination Type of a filtering rule (**Configure** > **Security** > **Access Control** > **Filtering**) can be a URL regular expression. Typically, such expressions can include backslashes to **escape** the meaning of special characters. However, in this release backslash is mishandled and should not be used.

NTLM with SOCKS not supported

In version 7.5, NTLM cannot be used in combination with SOCKS.

FTP in transparent proxy deployments

Native FTP is supported in transparent proxy deployments. However, some native FTP clients don't work in passive (PASV) mode. To work around the problem, reconfigure the FTP client to operate in active mode.

FTP combined with IPTables requires Active FTP clients

If you run the Linux IPTables firewall on your Content Gateway server, and you turn on FTP processing on the proxy (**Configure** > **My Proxy** > **Basic** > **General**), then all FTP clients must be configured to use the PORT command (known as Active mode) against the FTP server.

Please also make sure that your FTP clients are allowed to receive incoming TCP connection requests from the client's host firewall.

- For a Windows system, you may add the clients to Windows Firewall/Exceptions.
- For a Linux system, you may enable the "ip_conntrack_ftp" connection tracking module for iptables.

This is a known restriction that applies only for sites using IPTables.

- Most FTP clients allow you to set them to Passive or Active mode.
- ftp.exe in the Windows CMD line uses only the PORT command (Active mode) against the FTP server.
- Internet Explorer uses Passive mode by default. Uncheck the **Browsing** setting on **Tools > Internet Options > Advanced**. Uncheck the Browsing option "Use Passive FTP."

For additional information about configuring IPTables, see the Knowledge Base article titled: v7: Configuring IPTables for Websense Content Gateway.

FTP over HTTP: Internet Explorer does not display block page

When an FTP over HTTP request is made in Internet Explorer 7 or 8 and the request is blocked by file scanning (anti-virus or advanced detection), the block page does not display properly. This is because Internet Explorer expects an FTP response and does not recognize the HTTP response (Firefox and other browsers recognize the HTTP response). To cause the block page to be displayed, refresh the browser window.

Native FTP upload can hang when blocked by Data Security

A native FTP upload will hang under the following conditions:

- Content Gateway is integrated with Websense Data Security, either with the on-box policy engine or over ICAP.
- The FTP upload is blocked by Data Security policy.
- The FTP server is single threaded (has "async_abor_enable=no").

Because the FTP server is single threaded (synchronous) with respect to handling the FTP client command and data connections, when the data connection is open, the FTP server can't read from the command channel until the upload is complete, which never happens due to the Data Security block. On the client end, the FTP application never gets the block message and the client application hangs.

LDAP and Active Directory: authentication fails for users outside the base domain

When proxy authentication is configured for LDAP with Active Directory, a request from a user located outside the global catalog's base domain fails to authenticate. This is because the default port for LDAP is 389 and requests sent to 389 search for objects only within the global catalog's base domain.

To authenticate users from outside the base domain, change the LDAP port to 3268. LDAP requests sent to port 3268 can search for objects in the entire forest.

1. In the Content Gateway Manager, go to **Configure > Security > Access Control > LDAP**.
2. In the port configuration field, enter 3268.
3. Click **Apply**.
4. Click **Restart** on **Configure > My Proxy > Basic > General**.

Connections to some HTTPS sites fail with a certificate verification error

When SSL is enabled, users cannot successfully connect to some HTTPS sites. While attempting to connect, the browser displays a certificate verification error. The problem results when the origin server mishandles the cipher negotiation. Most servers do not exhibit this problem.

For more information, see the Knowledge Base article titled “Connections to some HTTPS sites fail with a certificate verification error”.

Browsing to a site with self-signed certificate (Websense Manager) may generate an error

Attempting to browse to any Web site that has a self-signed certificate will generate a certificate incident if the SSL certificate verification engine is enabled.

(By default, the SSL certificate verification engine is disabled.)

If the certificate verification engine is enabled, you can add the domain/URL of the site with the self-signed certificate as an exception.

Other options:

- If the browser is configured for explicit proxy, you can remove the explicit browser entries.
- If the browser is configured using WPAD or a PAC file, then that configuration can be disabled.
- If your site is using WCCP, there is no workaround.

Users may receive a certificate error from Internet Explorer when visiting secure sites

When Content Gateway is running in a transparent proxy deployment with SSL Manager, users may receive a certificate error from Internet Explorer before they receive the certificate verification result from SSL Manager, when certain secure sites are visited.

This can occur when a user attempts to access a site whose CA (certificate authority) is not listed on the **Configure > SSL > Certificates > Certificate Authorities** page. CAs are added to this list when a user attempts to access a site requiring a certificate; however CAs are added with **deny** status by default. The administrator must change the status to **allow**.

If a user attempts to visit the site before the status has been changed, the user receives a certificate error. See Websense Content Gateway Online Help for information on incidents and changing the status of a certificate.

This can also occur when the common name of the certificate (for example, company_name.com) does not match the URL (for example, www.business_name.com).

This does not occur when you are running in an explicit proxy deployment.

Internet Explorer does not display block page when HTTPS is disabled

If HTTPS is disabled, and an Internet Explorer browser is configured to send both HTTP and HTTPS traffic to port 8080, when a user browses to a secure site that should result in a block or quota page, Internet Explorer does not send the block or quota page.

This happens the first time a user tries to access a secure site in a browser session. After the user visits a non-secure site in the same category, future visits to secure sites in a quota-blocked category result in the user's viewing the page if quota time remains. However, for sites that should be blocked, the user does not receive a block page.

This occurs only in Internet Explorer; it does not occur in Firefox.

Users may receive garbled content when content stripping is on and a Web page contains non-ASCII content

If you use content stripping, Web content that is not ASCII-encoded (not UTF-8 encoded) is transcoded to UTF-8 before it is scanned for possible content stripping. The content that is not stripped can be returned garbled to the client, unless you have set an option in Content Gateway Manager:

1. In Content Gateway Manager go to **Configure** > **Protocols** > **HTTP** > **Privacy** > **Remove Headers** > **Remove Others**.
2. Add **Accept-Encoding**.
3. Click **Apply**, and then click **Restart**.

Accessing Citrix Online products (GoToAssist, GoToMeeting, GoToMyPC, GoToWebinar)

Citrix Online products use port 8200, or 80 or 443. If your clients cannot access GoToAssist, GoToMeeting, GoToMyPC, or GoToWebinar, you may need to create an ARM static bypass rule, or modify the PAC file to allow access to Citrix Online IP addresses. See the Knowledge Base article titled "Connecting to GoToAssist and other Citrix collaboration products". For a list of Citrix collaboration product IP addresses, go to http://www.citrixonline.com/iprange/.

Real Player fails to stream content

Real Networks Real Player fails to stream content when the combined conditions are true:

1. Websense Content Gateway is the only path to the Internet.
2. Traffic is explicitly routed to Content Gateway.
3. NTLM authentication is enabled.

By default, Real Player uses RTSP or PNA to stream media, bypassing Content Gateway. However, when Content Gateway is the only path to the Internet, Real Player uses HTTP through Content Gateway. Unfortunately, Real Player doesn't handle NTLM authentication properly and the connection fails. (For related information, see Microsoft knowledge base article http://support.microsoft.com/kb/288734/).

To work around the problem add an Allow rule to **filter.config** that identifies the Real Player application and allows Real Player traffic:

1. In Content Gateway Manager (Websense Content Manager), go to **Configure > Security > Access Control > Filtering** and click **Edit File**.
2. Add the following filtering rule:

   Rule Type = Allow

   Primary Destination Type = dest_domain

   Primary Destination Value = .

   User-Agent = realplayer
3. Click **Add**. The new rule appears in the table at the top of the page. It should have the format:

   Rule Type=Allow , dest_domain=. , User-Agent=realplayer
4. Click **Apply** and then **Close**.

Remap rules cannot mix scheme (protocol) types

Remap rules (in **remap.config**) cannot map a URL of one protocol type (scheme) to a URL of another protocol type, i.e., HTTP to HTTPS. The scheme type (HTTP, HTTPS, FTP) of the *target* and *replacement* must match.

HTTPS configuration not synchronized in a cluster

The SSL Manager feature settings are not processed by the management clustering feature. In a Content Gateway deployment with multiple servers, one work around is to devote one server to HTTPS traffic and the other nodes to HTTP traffic. To discuss other solutions, contact your Websense Technical Account Manager.

Updating the list of Certificate Authorities

After an initial deployment of SSL decryption and re-encryption only, you may choose to verify certificates. For peak performance, the Certificate Authorities (CAs) listed on the **Configure > SSL > Certificates > Certificate Authorities** page should match the certificates available in Internet Explorer. Follow these steps in Internet Explorer and then in Content Gateway Manager to import those certificates into SSL Manager.

In Internet Explorer

1. Navigate to the **Tools > Internet Options > Content** page.
2. Select **Certificates**, and then select the **Trusted Root Certificate Authorities** tab.
3. Double-click a CA, such as America Online Root Certification Authority 1, and then click **Details**.
4. Click **Copy to File** to launch the Export Certificate wizard.
5. In the wizard:
   a. Click **Next**.
   b. Select **Base-64 encoded X.509 (.CER)**.
   c. Click **Next**.

d. Click **Browse**.

   In the **Save As** window, browse to the location where certificates are stored and enter a name for the certificate. Ensure that the file type is Base64 Encoded X.509. Then click **Save**.

e. Click **Next**.

f. Click **Back** if you must make changes, or click **Finish**.

6. After you receive a message that the import was successful, close the windows of the dialog box.

In Content Gateway Manager

1. Navigate to the **Configure > SSL > Certificates > Add Root CA** page.
2. Click **Browse** and navigate to the location where certificates are stored. This is the location in Step 5 for Internet Explorer.
3. Select the certificate and click **Open**.
4. Click **Add Certificate Authority**.

You can confirm the successful import by navigating to the **Configure > SSL > Certificates > Certificate Authorities** page, and checking that the Certificate Authority is listed there.

Objects marked “pin-in-cache” are dropped if the cache becomes full

Objects that are marked “pin-in-cache” in the **cache.config** file are dropped from the cache when the cache become full.

Recurring redirect page on first access of some HTTPS sites

When SSL Manager is enabled and Client Certificate handling is set to “Tunnel” (Configure > SSL > Client Certificates > General), the first time some HTTPS sites are visited, the browser may get a redirect page that, after the user clicks OK, is displayed again, sometimes repeating many times in an apparent loop.

To eliminate the problem for the current site, the user should simply Refresh (F5) the browser window.

Some HTTPS requests are filtered and logged by loopback address

The problem results when an HTTPS page includes a WebDAV method in the header that is not recognized by SSL Manager. The unrecognized WebDAV methods include: BCOPY, BDELETE, BMOVE, BPROPFIND, BPROPPATCH, NOTIFY, UNSUBSCRIBE, X-MS-ENUMATTS. The result is that HTTPS pages containing an unrecognized WebDAV method are filtered and logged by loopback address (127.0.0.1) rather than their actual source IP address.

Technical assistance

Technical information about Websense software and services is available 24 hours a day at www.websense.com/support/, including:

- the latest release information
- the searchable Websense Knowledge Base
- Support Forums
- Support Webinars
- show-me tutorials
- product documents
- answers to frequently asked questions
- Top Customer Issues
- in-depth technical papers

For additional questions, click the **Contact Support** tab at the top of the page.

If your issue is urgent, please call one of the offices listed below. You will be routed to the first available technician, who will gladly assist you.

For less urgent cases, use our online **Support Request Portal** at ask.websense.com.

For faster phone response, please use your **Support Account ID**, which you can find in the Profile section at MyWebsense.

Location	Contact information
North America	+1-858-458-2940
France	Contact your Websense Reseller. If you cannot locate your Reseller: +33 (0) 1 5732 3227
Germany	Contact your Websense Reseller. If you cannot locate your Reseller: +49 (0) 69 517 09347
UK	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Rest of Europe	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Middle East	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Africa	Contact your Websense Reseller. If you cannot locate your Reseller: +44 (0) 20 3024 4401
Australia/NZ	Contact your Websense Reseller. If you cannot locate your Reseller: +61 (0) 2 9414 0033
Asia	Contact your Websense Reseller. If you cannot locate your Reseller: +86 (10) 5884 4200
Latin America and Caribbean	+1-858-458-2940

For telephone requests, please have ready:

- Websense subscription key
- Access to the Websense management console.
- Access to the machine running reporting tools and the database server (Microsoft SQL Server or MSDE)

Familiarity with your network's architecture, or access to a specialist

Subscription agreement

WEBSENSE SUBSCRIPTION AGREEMENT

IMPORTANT - THIS SUBSCRIPTION IS PROVIDED ONLY ON THE CONDITION THAT THE SUBSCRIBER (REFERRED TO IN THIS AGREEMENT AS "SUBSCRIBER") AGREES TO THE TERMS AND CONDITIONS SET FORTH IN THE FOLLOWING LEGAL AGREEMENT WITH WEBSENSE, INC. AND/OR ONE OF ITS SUBSIDIARIES ("WEBSENSE"). READ THIS AGREEMENT CAREFULLY BEFORE ACCEPTING IT. BY CLICKING ON THE "I AGREE" BUTTON BELOW OR BY USING THE SOFTWARE, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AGREEMENT AND UNDERSTAND IT, AND THAT (1) YOU, ON BEHALF OF YOURSELF, OR (2) SUBSCRIBER, IF SUBSCRIBER IS A BUSINESS, AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS.

1. Subscription and Grant of Right to Use.

Subject to the terms and conditions of this Agreement, Websense agrees to provide Subscriber the subscription services ("Subscription") as described in the purchase commitment mutually agreed upon between the parties ("Order"). Websense grants to Subscriber as part of the Subscription a non-exclusive, nontransferable right to use certain proprietary software applications ("Software"), proprietary database(s) of URL addresses, applications and other valuable information ("Databases"), changes to the content of the Databases ("Database Updates") and certain modifications or revisions to the Software ("Software Upgrades"), together with applicable documentation and the accompanying media, if any, (collectively, the "Products"). The Products are provided for the number of Seats or servers for use in Subscriber's own internal business operations (not for the benefit of any other person or entity) for the time period set forth herein or in the applicable Order ("Subscription Term"), provided Subscriber has and continues to pay the applicable fees for the Products ("Subscription Fees"). Subject to compliance with the terms of this Agreement, Subscriber may relocate or transfer the Product for use on a different server within its location. All fees paid for the Products are nonrefundable. "Seat" means each computer, electronic appliance or device that is authorized to access or use the Products, directly or indirectly. Subscriber may only exceed the number of ordered Seats if Subscriber increases its Order and pays additional Subscription Fees. Websense may, at any time, audit the use of the Products remotely or, upon reasonable notice, at Subscriber's site. Unless specifically authorized in writing in advance by Websense, Subscriber may not rent, lease or timeshare the Products or provide subscription services for the Products or permit others to do so. Any source code provided to Subscriber by Websense is subject to the terms of this Agreement. Subject to the terms of this Agreement, Subscriber may allow its agents and independent contractors to use the Products solely for the benefit of Subscriber; provided, however, Subscriber remains responsible for any breach of this Agreement. Any other use of the Products by any person, business, corporation, government organization or any other entity is strictly forbidden and is a violation of this Agreement. Evaluation subscriptions to the Products are provided by Websense subject to the terms and conditions of this Agreement. Evaluation subscriptions are available for a period of up to thirty (30) days, and may be used only to evaluate and facilitate Subscriber's decision to purchase a subscription to Products, and at the end of the evaluation period, Subscriber must pay the applicable Subscription Fees or this Agreement will automatically terminate and Subscriber must comply with the terms of Section 7 below.

2. Technical Support.

Standard technical support includes online website and/or portal access, telephone support during business hours, and Software Upgrades for the Products during the Subscription Term upon payment of the Subscription Fees. Standard technical support is provided pursuant to the terms of this Agreement and the then-current technical support policies which are available at support.websense.com. Websense may require Subscriber to install Software Upgrades up to and including the latest release. Enhanced support offerings and services are available for additional cost and are also subject to the terms of this Agreement. Database Updates and Software Upgrades will be provided to Subscriber only if Subscriber has paid the appropriate Subscription Fees for all Seats and/or servers.

3. Intellectual Property Rights.

The Products and all intellectual property rights therein and related thereto are the sole and exclusive property of Websense and any third party from whom Websense has licensed software for incorporation in or distribution with the Products. All right, title and interest in and to the Products and any modifications, translations, or derivatives thereof, even if unauthorized, and all applicable rights in patents, copyrights, trade secrets, trademarks and all intellectual property rights in the same shall remain exclusively with Websense and its licensors. The Products are valuable, proprietary, and unique, and Subscriber agrees to be bound by and observe the proprietary nature thereof. The Products contain material that is protected by patent, copyright and trade secret law, and by international treaty provisions. All rights not granted to Subscriber in this Agreement are reserved to Websense. No ownership of the Products passes to Subscriber. Websense may make changes to the Products at any time without notice. Except as otherwise expressly provided, Websense grants no express or implied right under Websense patents, copyrights, trademarks, or other intellectual property rights. Subscriber may make a sufficient number of copies of the Software for its authorized use and may maintain one (1) copy of the Software for backup purposes only. Subscriber may not remove any proprietary notice of Websense or any third party from any copy of the Products.

4. Protection and Restrictions.

Subscriber agrees to take all reasonable steps to safeguard the Products to ensure that no unauthorized person has access thereto and that no unauthorized copy, publication, disclosure or distribution, in whole or in part, in any form is made. Subscriber acknowledges that the Products contain valuable, confidential information and trade secrets and that unauthorized use and/or copying is harmful to Websense. Subscriber may not directly or indirectly transfer, assign, publish, display, disclose, rent, lease, modify, loan, distribute, or create derivative works based on the Products or any part thereof. Subscriber may not reverse engineer (except as required by law in order to assure interoperability), decompile, translate, adapt, or disassemble the Products, nor shall Subscriber attempt to create the source code from the object code for the Software. Any third party software included in the Products may only be used in conjunction with the Products, and not independently from the Products. Subscriber may not, and shall not allow third parties to, publish, distribute or disclose the results of any benchmark tests performed on the Products without Websense's prior written approval. Subscriber represents and warrants that it will comply with all laws, rules and regulations which apply to its use of the Products. Subscriber further represents and warrants that the Products will not be used to filter, screen, manage or censor Internet content for consumers without (a) permission from the affected consumers and (b) Websense's express prior written approval which may be withheld in Websense's sole and absolute discretion. Additional charges may apply if Subscriber assigns more than twenty (20) administrators to administer certain Websense products.

5. Limited Warranty.

For the Subscription Term, Websense warrants that the Products will operate in substantial conformance with the then-current Websense published documentation under normal use. Notwithstanding the previous sentence, Websense does not warrant that: (i) Products will be free from defects; (ii) Products will satisfy all of Subscriber's requirements; (iii) Products will operate without interruption or error; (iv) Products will always locate or block access to or transmission of all desired addresses, applications and/or files; (v) Products will identify every transmission or file that should potentially be located or blocked; (vi) addresses and files contained in the Products will be appropriately categorized; or (vii) algorithms used in the Products will be complete or accurate. Websense shall use reasonable efforts to remedy any significant Product non-conformance reported to Websense that Websense can reasonably identify and confirm. Websense or its representative will repair or replace any such non-conforming or defective Products, or refund a pro-rata share of the Subscription Fees paid for the then-current term, at Websense's sole discretion. This paragraph sets forth Subscriber's sole and exclusive remedy and Websense's entire liability for any breach of warranty or other duty related to the Products. Any unauthorized Product modification, tampering with the Products, Product use inconsistent with the accompanying documentation, or related breach of this Agreement shall void the aforementioned warranty. EXCEPT AS EXPLICITLY SET FORTH HEREIN AND TO THE EXTENT ALLOWED BY LAW, THERE ARE NO OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, TITLE OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE PRODUCTS.

6. Limitation of Liability.

TO THE FULLEST EXTENT PERMITTED BY LAW, UNDER NO CIRCUMSTANCES WILL WEBSENSE, ITS AFFILIATES, ITS LICENSORS OR RESELLERS BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, SPECIAL, PUNITIVE OR INCIDENTAL DAMAGES, WHETHER FORESEEABLE OR UNFORESEEABLE, ARISING OUT OF OR RELATED TO THIS AGREEMENT INCLUDING, BUT NOT LIMITED TO CLAIMS FOR LOSS OF DATA, GOODWILL, OPPORTUNITY, REVENUE, PROFITS, OR USE OF THE PRODUCTS, INTERRUPTION IN USE OR AVAILABILITY OF DATA, STOPPAGE OF OTHER WORK OR IMPAIRMENT OF OTHER ASSETS, PRIVACY, ACCESS TO OR USE OF ANY ADDRESSES OR FILES THAT SHOULD HAVE BEEN LOCATED OR BLOCKED, NEGLIGENCE, BREACH OF CONTRACT, TORT OR OTHERWISE AND THIRD PARTY CLAIMS, EVEN IF WEBSENSE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL WEBSENSE'S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT EXCEED THE TOTAL AMOUNT ACTUALLY PAID BY SUBSCRIBER TO WEBSENSE FOR THE APPLICABLE PRODUCTS OVER THE ONE YEAR PERIOD PRIOR TO THE EVENT OUT OF WHICH THE CLAIM AROSE FOR THE PRODUCTS THAT DIRECTLY CAUSED THE LIABILITY.

7. Termination.

This Agreement is effective until the end of the Subscription Term for such use as is authorized, or until terminated by either party. Subscriber may terminate this Agreement at any time upon notification to Websense. However, Subscriber shall not be entitled to a refund of any prepaid or other fees. Websense may terminate this Agreement if Websense finds that Subscriber has violated the terms hereof. Upon notification of termination by either party, Subscriber agrees to uninstall the Software, cease using and to destroy or return to Websense all copies of the Products and to certify in writing that all copies thereof, including backup copies, have been destroyed. Section 3-7, 9 and 11 shall survive the termination of this Agreement.

8. Government Restricted Rights.

The Products are provided with "RESTRICTED RIGHTS." Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in FAR 52.227-14 and DFAR 252.227-7013 et seq. or its successor. Use of the Products by the U.S. Government constitutes acknowledgment of Websense's proprietary rights therein. Contractor or Manufacturer is Websense.

9. Third Party Products.

The Products include software products licensed from third parties. Such third parties have no obligations or liability to Subscriber under this Agreement but are third party beneficiaries of this Agreement.

10. Export.

Certain Products provided under the Agreement are subject to export controls administered by the United States and other countries ("Export Controls"). Export or diversion contrary to U.S. law is prohibited. U.S. law prohibits export or re-export of the software or technology to Cuba, Iran, North Korea, Sudan and Syria or to a resident or national of those countries ("Prohibited Country" or "Prohibited Countries"). It also prohibits export or re-export of the software or technology to any person or entity on the U.S. Department of Commerce Denied Persons List, Entities List or Unverified List; the U.S. Department of State Debarred List; or any of the lists administered by the U.S. Department of Treasury, including lists of Specially Designated Nationals, Specially Designated Terrorists or Specially Designated Narcotics Traffickers (collectively, the "Lists"). U.S. law also prohibits use of the software or technology with chemical, biological or nuclear weapons, or with missiles ("Prohibited Uses"). Subscriber warrants that it is not located in, or a resident or national, of any Prohibited Country; that it is not on any Lists; that it will not use the software or technology for any Prohibited Uses; and that it will otherwise comply with Export Controls.

11. General.

Websense may periodically send Subscriber messages of an informational or advertising nature via email. Subscriber may choose to "opt-out" of receiving these messages by sending an email to optoutlegal@websense.com requesting the opt-out. Subscriber acknowledges and agrees that by sending such email and "opting out" it will not receive emails containing messages concerning upgrades and enhancements to Products. However, Websense may still send emails of a technical nature. Subscriber acknowledges that Websense may use Subscriber's company name in a list of Websense customers. Subscriber may not transfer any of Subscriber's rights to use the Products or assign this Agreement to another person or entity, without first obtaining Websense's prior written approval. Notices sent to Websense shall be sent to the attention of the General Counsel at 10240 Sorrento Valley Road, San Diego, CA 92121 USA. Any dispute arising out of or relating to this Agreement or the breach thereof shall be governed by the federal laws of the United States and the laws of the State of California, USA for all claims arising in or related to the United States, Canada, or Mexico; the laws of England and Wales for all claims arising in or related to the United Kingdom; and Dublin, Ireland for all other claims, without regard to or application of choice of laws, rules or principles. Both parties hereby consent to the exclusive jurisdiction of (1) the state and federal courts in San Diego, California, USA, for all claims arising in or related to the United States, Canada or Mexico, (2) the competent courts in England and Wales for all claims arising in or related to the United Kingdom; or (3) the competent courts in Dublin, Ireland for all other claims. Both parties expressly waive any objections or defense based upon lack of personal jurisdiction or venue. Neither party will be liable for any delay or failure in performance to the extent the delay or failure is caused by events beyond the party's reasonable control, including, fire, flood, acts of god, explosion, war or the engagement of hostilities, strike, embargo, labor dispute, government requirement, civil disturbances, civil or military authority, disturbances to the Internet, and inability to secure materials or transportation facilities. This Agreement constitutes the entire Agreement between the parties hereto regarding the subject matter contained herein and the parties acknowledge that they have not relied on any promise, representation, or warranty, express or implied, that is not contained in this Agreement. Any waiver or modification of this Agreement shall only be effective if it is in writing and signed by both parties or posted by Websense at http://www.websense.com/legal. If any part of this Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this Agreement shall be interpreted so as to reasonably effect the intention of the parties. Each party agrees to comply with all applicable laws and regulations. Websense is not obligated under any other agreements unless they are in writing and signed by an authorized representative of Websense.

If your Order includes the purchase of a subscription to the Websense Anywhere Product(s), the following Anywhere Product Subscription Agreement governs your use of those products:

WEBSENSE ANYWHERE PRODUCT SUBSCRIPTION AGREEMENT

THE PRODUCTS ARE PROVIDED ONLY ON THE CONDITION THAT THE SUBSCRIBER AGREES TO THE TERMS AND CONDITIONS IN THIS SUBSCRIPTION AGREEMENT ("AGREEMENT") BETWEEN SUBSCRIBER AND WEBSENSE BY ACCEPTING THIS AGREEMENT OR BY USING THE PRODUCTS, SUBSCRIBER ACKNOWLEDGES THAT IT HAS READ, UNDERSTANDS, AND AGREES TO BE BOUND BY THIS AGREEMENT.

1. Definitions.

"**Databases**" means proprietary database(s) of URL addresses, email addresses, Malware, applications and other valuable information.

"**Database Updates**" means changes to the content of the Databases.

"**Order**" means a purchase commitment mutually agreed upon between (1) Websense and Subscriber, or (2) a Websense authorized reseller and Subscriber.

"**Permitted Capacity**" means the Permitted Number of Seats set forth in the Order.

"**Seat**" means (i) each computer, electronic appliance or device that is authorized to access or use the Products, directly or indirectly; and (ii) a separate email address or account that receives electronic messages or data within Subscriber's email system or network. For (ii), up to 5 aliases for a single user are considered one Seat. (For example: A user with a default email address of john.doe@acme.com who also has an alias of jdoe@acme.com counts as a single Seat).

"**Permitted Number of Seats**" means the number of Seats or Users set forth in the Order.

"**Products**" means Software, Databases, Database Updates, Software Upgrades, the on-line web-based components thereof, and services together with applicable documentation and media.

"**Software**" means Websense's proprietary software applications.

"**Software Upgrades**" means certain modifications or revisions to the Software.

"**Subscriber**" means the individual, company, jointly owned subsidiaries and their parent company, or other legal entity that has placed an Order.

"**Subscription**" means a non-exclusive, nontransferable right to use the Products in accordance with this Agreement and the Order.

"**Subscription Fees**" means the agreed upon fees in an Order.

"**Subscription Term**" means the agreed upon time period in an Order.

"**User**" means Seat.

"**Virus**" or "**Malware**" means computer software or program code that is designed to damage or reduce the performance or security of a computer program or data.

"**Websense**" means Websense, Inc., a Delaware corporation with its principal place of business at 10240 Sorrento Valley Road, San Diego, California 92121, USA or, as the context may require, Websense International Limited, with a principal place of business at Minerva House, Simmonscourt Road, Dublin 4, Ireland; or Websense Hosted R&D Ltd., with its principal place of business at Jordans Limited 20-22 Bedford Row, London WC1R 4JS; or Websense UK, Ltd., with its principal place of business at Riverside, Mountbatten Way, Congleton Cheshire, CW121DY.

Email Definitions

"**Average Emails Per Seat**" means the total number of emails processed in performance of Anywhere Email divided by the number of Seats.

"**Bulk Mail**" means a large number of email messages with similar content sent or received in a single operation or a series of related operations.

"**Anywhere Email**" means the online, Web-based component of the Products provided by Websense when set forth in the Order, including associated offline components.

"**Open Relay**" means an email server configured to receive email from an unauthorized third party and that forwards the email to other recipients who are not part of the server's email network.

"**Spam**" means a large number of unsolicited email messages (typically over 500 per month) with similar content sent or received in a single operation or a series of related operations.

Web Definitions

"**Average Bandwidth Per Seat**" means the total bandwidth used in the performance of Anywhere Web divided by the number of Seats.

"**Web Content**" means any data and requests for data processed by Anywhere Web including but not restricted to that accessed using the Internet protocols HTTP and FTP.

"**Anywhere Web**" means the online, Web-based component of the Products provided by Websense when set forth in the Order, including associated offline components.

2. Subscription and Grant of Right to Use.

Subject to the terms and conditions of this Agreement, Websense will provide Subscriber the Subscription at the Permitted Capacity set forth in the Order for the Subscription Term. Subscriber may use the Products solely for Subscriber's own internal business operations (not for the benefit of any other person or entity) during the Subscription Term, provided Subscriber has paid and continues to pay the Subscription Fees. Subject to compliance with the terms of this Agreement, Subscriber may relocate or transfer the Product for use on a different server within its location. Websense may terminate this Agreement at the end of a Subscription Term unless Subscriber continues to pay Subscription Fees for the Products. Subscription Fees are nonrefundable. Websense may audit its systems to confirm Subscriber's authorized use of the Products at any time or, upon reasonable notice, at Subscriber's site. Subscriber may not rent, lease or timeshare the Products or provide subscription services for the Products or permit others to do so. Subject to the terms of this Agreement, Subscriber may allow its agents and independent contractors to use the Products solely for the benefit of Subscriber; provided, however, Subscriber remains responsible for any breach of this Agreement. Any other use of the Products by any other entity is forbidden and a violation of this Agreement. Any source code provided to Subscriber by Websense is subject to the terms of this Agreement. Evaluation subscriptions to the Products are provided by Websense subject to the terms and conditions of this Agreement. Evaluation subscriptions are available for a period of up to thirty (30) days, and may be used only to evaluate and facilitate Subscriber's decision to purchase a subscription to Products, and at the end of the evaluation period, Subscriber must either pay the applicable Subscription Fees or this Agreement terminates as related to the evaluation. Subscriber's continued use of the Products after an evaluation period is subject to this Agreement.

3. Provision of the Products.

3.1 Websense will use commercially reasonable efforts to provide Anywhere Web and Anywhere Email for the Subscription Term. Service levels for Anywhere Web and Anywhere Email may be found at: http://www.websense.com/global/en/ProductsServices/HostedSecurity/servicedescriptions/WHS_SLA_Final.pdf. Websense makes no service level commitments for email that is determined by Websense to be Bulk Mail.

3.2 If Websense determines that the security or proper function of Anywhere Web and Anywhere Email would be compromised due to, hacking, denial of service attacks or other activities originating from or directed at Subscriber's network, Websense may immediately suspend Anywhere Web and Anywhere Email until the problem is resolved. Websense will promptly notify and work with Subscriber to resolve the issues.

3.3 If Anywhere Web and Anywhere Email are suspended or terminated, Websense will reverse all configuration changes made during Anywhere Web and Anywhere Email enrollment. It is Subscriber's responsibility to make the server configuration changes necessary to reroute email for Anywhere Email and reroute Web Content for Anywhere Web.

3.4 Websense may modify, enhance, replace, or make additions to the Products. Websense may use Malware, Spam, and other information passing through the Products for the purposes of developing, analyzing, maintaining, reporting on, and enhancing the Websense Products and services.

3.5 Prior to enrollment in Anywhere Email and at any time during the Subscription Term, Websense may test whether Subscriber's email system is acting as an Open Relay. If Websense finds the system to be acting as an Open Relay, Websense will inform Subscriber and may suspend Anywhere Email until the problem is resolved.

3.6 If Subscriber is using the Products to distribute Spam or Malware, Websense may immediately suspend Anywhere Web and Anywhere Email until the problem is resolved.

3.7 If in any one (1) calendar month the Average Emails per Seat is greater than thirty thousand (30,000), Websense may terminate Anywhere Email Subscription upon thirty (30) days prior written notice to Subscriber.

3.8 If in any one (1) calendar month the Average Bandwidth Per Seat is greater than 0.02Mbps, Websense may terminate Subscriber's Anywhere Web Subscription upon thirty (30) days prior written notice to Subscriber.

4. Subscriber Obligations.

4.1 Subscriber will (a) comply with all applicable laws, statutes, regulations and ordinances, (b) only use the Products for legitimate business purposes which may include sending and receiving business and personal email or Web Content by its employees, and (c) not use the Products to transmit Spam, Malware, or excessive email.

4.2 Subscriber must (a) have the authority, rights, or permissions to use all domains registered to the Products, (b) obtain any necessary consents from its employees, and (c) not use the Products to filter, screen, manage or censor Internet content for consumers without permission from the affected consumers and Websense's express prior written approval which may be withheld in Websense's sole discretion.

4.3 For Anywhere Web, Subscriber agrees to comply with the reasonable standards and protocols published on the Internet from time to time and adopted by the majority of Internet users.

4.4 If in any one (1) calendar month the Average Emails Per Seat is greater than ten thousand (10,000), Subscriber will make reasonable efforts to implement and maintain an accurate list of all valid email addresses belonging to Subscriber for which Anywhere Email scans inbound or outbound email.

4.5 Subscriber will defend, indemnify and hold Websense harmless against any loss, damage or costs (including reasonable attorneys' fees) incurred in connection with any claims, demands, suits, or proceedings ("Claims") made or brought against Websense by a third party alleging or related to Subscriber's (i) violation of its obligations in this Section 4; (ii) infringement of intellectual property rights; (iii) civil or criminal offenses; (iv) transmission or posting of obscene, indecent, or pornographic materials; (v) transmission or posting of any material which is slanderous, defamatory, offensive, abusive, or menacing or which causes annoyance or needless anxiety to any other person; or (vi) transmission of information through the Products.

5. Technical Support.

Standard technical support includes online website and/or portal access, telephone support during business hours, and Software Upgrades for the Products during the Subscription Term upon payment of the Subscription Fees. Standard technical support is provided pursuant to the terms of this Agreement and the then-current technical support policies which are available at http://www.websense.com/content/Assets/PDF/Websense_Global_Technical_Support_Users_Guide.pdf. Websense may require Subscriber to install Software Upgrades up to and including the latest release. Enhanced support offerings and services are available for additional cost and are also subject to the terms of this Agreement. Database Updates and Software Upgrades will be provided to Subscriber only if Subscriber has paid the appropriate Subscription Fees for all Seats and/or servers.

6. Intellectual Property Rights.

The Products and all related intellectual property rights are the exclusive property of Websense or its licensors. All right, title and interest in and to the Products, any modifications, translations, or derivatives thereof, even if unauthorized, and all applicable rights in patents, copyrights, trade secrets, trademarks and all intellectual property rights in the Products remain exclusively with Websense or its licensors. The Products are valuable, proprietary, and unique, and Subscriber agrees to be bound by and observe the proprietary nature of the Products. The Products contain material that is protected by patent, copyright and trade secret law, and by international treaty provisions. Subscriber may not remove any proprietary notice of Websense or any third party. All rights not granted to Subscriber in this Agreement are reserved to Websense. No ownership of the Products passes to Subscriber. Websense may make changes to the Products at any time without notice. Except as otherwise expressly provided, Websense grants no express or implied right under Websense patents, copyrights, trademarks, or other intellectual property rights. Subscriber may make a sufficient number of copies of the Software for its authorized use and may maintain one (1) copy of the Software for backup purposes only. Subscriber may not remove any proprietary notice of Websense or any third party from any copy of the Products.

7. Protection and Restrictions.

7.1 Each party (the "Disclosing Party") may disclose to the other (the "Receiving Party") certain confidential technical and business information which the Disclosing Party desires the Receiving Party to treat as confidential. "Confidential Information" means any information disclosed by either party to the other party, either directly or indirectly, in writing, orally, electronically or by inspection of tangible objects (including without limitation documents, prototypes, equipment, technical data, trade secrets and know-how, product plans, Products, services, suppliers, customer lists and customer information, prices and costs, markets, software, databases, developments, inventions, processes, formulas, technology, employee information, designs, drawings, engineering, hardware configuration information, marketing, licenses, finances, budgets and other business information), which is designated as "Confidential," "Proprietary" or some similar designation at or prior to the time of disclosure, or which should otherwise reasonably be considered confidential by the Receiving Party. Confidential Information may also include information disclosed to a Disclosing Party by third parties. Confidential Information shall not, however, include any information which the Receiving Party can document (i) was publicly known and made generally available prior to the time of disclosure by the Disclosing Party or an authorized third party; (ii) becomes publicly known and made generally available after disclosure through no action or inaction of the Receiving Party in violation of any obligation of confidentiality; (iii) is already in the possession of the Receiving Party at the time of disclosure; (iv) is lawfully obtained by the Receiving Party from a third party without a breach of such third party's obligations of confidentiality; or (v) is independently developed by the Receiving Party without use of or reference to the Disclosing Party's Confidential Information.

7.2 Subscriber will take all reasonable steps to safeguard the Products to ensure that no unauthorized person has access and that no unauthorized copy, publication, disclosure or distribution, in any form is made. The Products contain valuable, confidential information and trade secrets and unauthorized use or copying is harmful to Websense. Subscriber may not directly or indirectly transfer, assign, publish, display, disclose, rent, lease, modify, loan, distribute, or create derivative works based on the Products or any part thereof. Subscriber may not reverse engineer (except as required by law in order to assure interoperability), decompile, translate, adapt, or disassemble the Products, nor shall Subscriber attempt to create the source code from the object code for the Software. Any third party software included in the Products may only be used in conjunction with the Products, and not independently from the Products. Subscriber may not, and shall not allow third parties to, publish, distribute or disclose the results of any benchmark tests performed on the Products without Websense's prior written approval. Additional charges may apply if Subscriber assigns more than twenty (20) administrators to administer certain Websense products.

8. Limited Warranty.

8.1 For the Subscription Term, Websense warrants that the Products will operate in substantial conformance with the then-current Websense published documentation under normal use. Websense does not warrant that: (A) the Products will (i) be free of defects, (ii) satisfy Subscriber's requirements, (iii) operate without interruption or error, (iv) always locate or block access to or transmission of all desired addresses, emails, Malware, applications and/or files, or (v) identify every transmission or file that should potentially be located or blocked; or (B) data contained in the Databases will be (i) appropriately categorized or (ii) that the algorithms used in the Products will be complete or accurate.

8.2 Websense will use reasonable efforts to remedy any significant non-conformance in the Products which is reported to Websense and that Websense can reasonably identify and confirm. Websense at its discretion will repair or replace any such non-conforming or defective Products, or refund a pro-rata portion of the unused Subscription Fees paid for the remainder of the then-current term. This paragraph sets forth Subscriber's sole and exclusive remedy and Websense's entire liability for any breach of warranty or other duty related to the Products. Any unauthorized modification of the Products, tampering with the Products, use of the Products inconsistent with the accompanying documentation, or related breach of this Agreement voids the warranty. EXCEPT AS EXPLICITLY STATED AND TO THE EXTENT ALLOWED BY LAW, THERE ARE NO OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, TITLE OR FITNESS FOR A PARTICULAR PURPOSE WITH RESPECT TO THE PRODUCTS.

9. Limitation of Liability.

UNDER NO CIRCUMSTANCES WILL WEBSENSE, ITS AFFILIATES, ITS LICENSORS OR RESELLERS BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, SPECIAL, PUNITIVE OR INCIDENTAL DAMAGES, WHETHER FORESEEABLE OR UNFORESEEABLE, ARISING OUT OF OR RELATED TO THIS AGREEMENT INCLUDING, BUT NOT LIMITED TO CLAIMS FOR LOSS OF DATA, GOODWILL, OPPORTUNITY, REVENUE, PROFITS, OR USE OF THE PRODUCTS, INTERRUPTION IN USE OR AVAILABILITY OF DATA, STOPPAGE OF OTHER WORK OR IMPAIRMENT OF OTHER ASSETS, PRIVACY, ACCESS TO OR USE OF ANY ADDRESSES, EXECUTABLES OR FILES THAT SHOULD HAVE BEEN LOCATED OR BLOCKED, NEGLIGENCE, BREACH OF CONTRACT, TORT OR OTHERWISE AND THIRD PARTY CLAIMS, EVEN IF WEBSENSE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. IN NO EVENT WILL WEBSENSE'S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT EXCEED THE TOTAL AMOUNT ACTUALLY PAID BY SUBSCRIBER TO WEBSENSE FOR THE APPLICABLE PRODUCTS OVER THE ONE YEAR PERIOD PRIOR TO THE EVENT OUT OF WHICH THE CLAIM AROSE FOR THE PRODUCTS THAT DIRECTLY CAUSED THE LIABILITY.

10. Termination.

This Agreement is effective until the end of the Subscription Term for such use as is authorized, or until terminated by either party. Subscriber may terminate this Agreement at any time upon notice to Websense however, Subscriber is not entitled to a refund of any prepaid or other fees. Websense may terminate this Agreement if Websense finds that Subscriber has violated the Agreement. Upon notification of termination by either party, Subscriber must uninstall any Software, cease using and destroy or return all copies of the Products to Websense, and to certify in writing that all known copies thereof, including backup copies, have been destroyed. Sections 1, 6-10, 13, and 15 shall survive the termination of this Agreement.

11. Data Privacy.

Subscriber warrants that it has complied with all applicable laws and regulations, including those of other jurisdictions that may apply to Subscriber, concerning the protection of personal data. Subscriber warrants that it has obtained any required employee consents addressing the interception, reading, copying or filtering of emails and their attachments. Neither party shall use, nor require the other party to use, any data obtained via the Products for any unlawful purpose.

12. Government Restricted Rights.

The Products are provided with "RESTRICTED RIGHTS." Use, duplication, or disclosure by the U.S. Government is subject to restrictions as set forth in FAR 52.227-14 and DFAR 252.227-7013 et seq. or its successor. Use of the Products by the U.S. Government constitutes acknowledgment of Websense's proprietary rights therein. Contractor or Manufacturer is Websense.

13. Third Party Products.

The Products include software products licensed from third parties. Such third parties have no obligations or liability to Subscriber under this Agreement but are third party beneficiaries of this Agreement.

14. Export.

Certain Products are subject to export controls administered by the United States and other countries ("Export Controls"). Export or diversion contrary to U.S. law is prohibited. U.S. law prohibits export or re-export of the software or technology to specified countries or to a resident or national of those countries ("Prohibited Country" or "Prohibited Countries"). It also prohibits export or re-export of the software or technology to any person or entity on the U.S. Department of Commerce Denied Persons List, Entities List or Unverified List; the U.S. Department of State Debarred List; or any of the lists administered by the U.S. Department of Treasury, including lists of Specially Designated Nationals, Specially Designated Terrorists or Specially Designated Narcotics Traffickers (collectively, the "Lists"). U.S. law also prohibits use of the software or technology with chemical, biological or nuclear weapons, or with missiles ("Prohibited Uses"). Subscriber warrants that it is not located in, or a resident or national, of any Prohibited Country; that it is not on any Lists; that it will not use the software or technology for any Prohibited Uses; and that it will otherwise comply with Export Controls.

15. General.

Websense may periodically send Subscriber messages of an informational or advertising nature via email. Subscriber may choose to "opt-out" of receiving these messages by sending an email to optoutlegal@websense.com requesting the opt-out. Subscriber acknowledges and agrees that by sending such email and "opting out" it will not receive emails containing messages concerning upgrades and enhancements to Products. However, Websense may still send emails of a technical nature. Subscriber acknowledges that Websense may use Subscriber's company name only in a list of Websense customers. Subscriber may not transfer any of Subscriber's rights to use the Products or assign this Agreement to another person or entity, without first obtaining prior written approval from Websense. Notices sent to Websense shall be sent to the attention of the General Counsel at 10240 Sorrento Valley Road, San Diego, CA 92121 USA. Any dispute arising out of or relating to this Agreement or the breach thereof shall be governed by the federal laws of the United States and the laws of the State of California, USA for all claims arising in or related to the United States, Canada, or Mexico; the laws of England and Wales for all claims arising in or related to the United Kingdom; and Dublin, Ireland for all other claims, without regard to or application of choice of laws, rules or principles. Both parties hereby consent to the exclusive jurisdiction of: (1) the state and federal courts in San Diego, California, USA, for all claims arising in or related to the United States, Canada or Mexico; (2) the competent courts in England and Wales for all claims arising in or related to the United Kingdom; or (3) the competent courts in Dublin, Ireland for all other claims. Both parties expressly waive any objections or defense based upon lack of personal jurisdiction or venue. Neither party will be liable for any delay or failure in performance to the extent the delay or failure is caused by events beyond the party's reasonable control, including, fire, flood, acts of God, explosion, war or the engagement of hostilities, strike, embargo, labor dispute, government requirement, civil disturbances, civil or military authority, disturbances to the Internet, and inability to secure materials or transportation facilities. This Agreement constitutes the entire agreement between the parties hereto regarding the subject matter contained herein and the parties acknowledge that they have not relied on any promise, representation, or warranty, express or implied, that is not contained in this Agreement. Any waiver or modification of this Agreement shall only be effective if it is in writing and signed by both parties or posted by Websense at http://www.websense.com/legal. If any part of this Agreement is found invalid or unenforceable by a court of competent jurisdiction, the remainder of this Agreement shall be interpreted so as reasonably to affect the intention of the parties. Websense is not obligated under any other agreements unless they are in writing and signed by an authorized representative of Websense.

Copyright and Trademarks

EAP2_050210_750

The products and/or methods of use described in this document are covered by U.S. Patent Numbers 6,606,659 and 6,947,985 and other patents pending.

Every effort has been made to ensure the accuracy of this document. 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 is a registered trademark 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, Windows NT, Windows Server, and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

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.

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.