v7.1.1 Resolved and Known Issues

Applies To:	Websense Web Filter 7.1.1
	Websense Web Security 7.1.1

Resolved issues and *Known issues* specific to Websense Web Filter and Websense Web Security are listed here.

See the Release Notes for information about the upgrade process0

Resolved issues

Several hotfixes created for previous releases have been incorporated into this version. In addition, other changes requested by customers have been incorporated.

Websense Manager (general)

◆ The audit log no longer returns an internal error if you select the last 30 or 60 days. (v7.1 Hotfix 60, 69)

◆ An internal error message from Websense Manager no longer appears when you add a client in Firefox 3.0. (v7.1 Hotfix 60, 69)

◆ Websense Manager now features a scroll bar if there are additional Network Agents that are not shown on the screen. (v7.1 Hotfix 52, 69, v7.0 Hotfix 27, 35)

◆ An error message is no longer generated when a new Delegated Administrator attempts to look up clients or URLs in Websense Manager. (v7.0.1 Hotfix 01, 22, v7.0 Hotfix 08, 13, 21, 35)

◆ An issue that stopped some alert messages from being sent to the SNMP Trap when the SNMP alert setting was enabled in Websense Manager was resolved. (v6.3.2 Hotfix 68)

Websense Manager (Policy Management > Filter Components)

◆ URLs with certain characteristics (such as news.abc.gov.it) are no longer considered invalid hostnames when added as site exceptions. (v7.1 Hotfix 61, 69)

- Websense Manager now accepts user names containing periods (.) when it downloads the Master Database via a proxy. (v7.1 Hotfix 41, 69)

- Custom URLs (recategorized and unfiltered) and URLs added to limited access filters are now categorized properly when they contain uppercase letters. (v7.1 Hotfix 40, 69)

- Database download status for a Filtering Service instance located on a remote machine no longer takes several minutes to appear in Websense Manager. (v7.1 Hotfix 35, 69)

- URL recategorization no longer has errors with uppercase letters. (v7.1 Hotfix 35, 69)

- When unfiltered URLs are written to the Policy Database, duplicates are no longer created. A site with duplicate URLs already in the Policy Database should use Websense Manager to save unfiltered URLs again. This automatically removes any duplicates. (v7.1 Hotfix 20, 69)

- Websense Manager now consistently displays custom URLs. (v7.1 Hotfix 12, 33, 69)

- Administrators can now define non-qualified sites as unfiltered (example: http://wrprod). (v7.1 Hotfix 10, 12, 33, 69)

- When a site has a significant number (hundreds or thousands) of recategorized URLs or regular expressions, clicking OK on the Edit Categories page no longer results in a very long delay (many minutes) before the Filter Components page is loaded and changes can be saved. (v7.1 Hotfix 10, 12, 33, 69, v7.0.1 Hotfix 12, 22)

- The method used to add and remove custom URLs from categories has been improved. (v7.1 Hotfix 08, 12, 33, 69)

- Filtering is now compatible with custom URLs containing one or more capital letters. (v7.0.1 Hotfix 29)

- The load time for the Edit Policy page has been greatly reduced, especially for environments with a large number of custom URLs. (v7.0.1 Hotfix 22)

- The method used to add and remove custom URLs from categories has been improved. (v7.0.1 Hotfix 22)

- User names containing special characters are now filtered correctly. (v7.1 Hotfix 64, 69)

- User names containing a backslash (\) or a comma are now consistently filtered correctly. (v7.1 Hotfix 60, 69)

- You can now delete any custom category in Websense Manager. (v7.1 Hotfix 26)

- An error is no longer generated when an attempt is made to change category names that include a comma. (v7.0.1 Hotfix 01, 22, v7.0 Hotfix 08, 13, 21, 35)

Websense Manager (Policy Management > Clients)

- Custom LDAP groups identified in Websense Manager are now applied properly and user requests are filtered correctly. (v7.1 Hotfix 17, 28)

- Websense Manager's comparison of user domain name and OU domain name is no longer case sensitive. Users with the same domain name for both user and OU,

but with different case (upper/lower) can now be displayed to the Delegated Administrator who manages both. (v7.1 Hotfix 69)

◆ A backslash character is no longer added to user IDs that contain a comma when the user is added by the Search option on the Add Clients page in Websense Manager. (v7.1 Hotfix 52, 69)

◆ In Active Directory environments, when global catalog servers are identified by IP address rather than name, the Check Policy tool in the Websense Manager Toolbox no longer shows the Default policy being applied to clients that have a user, group, or OU policy assigned. (v7.1 Hotfix 50, 69)

◆ Manager now properly displays organizational units (OU) with plus signs (+) in the name. (v7.1 Hotfix 41, 69)

◆ Websense Manager no longer adds 'amp;' to the search context when the name of an OU contains an ampersand (&). (v7.1 Hotfix 38, 69)

◆ Users whose name includes a pound or hash symbol (#) in the LDAP path are now filtered when added to the Websense Manager. (v7.1 Hotfix 12, 33, 69)

◆ Administrators can now add a proxy user name containing a hyphen (-). (v7.1 Hotfix 10, 12, 33, 69)

◆ When a user whose name includes double quotation marks (") anywhere in the LDAP path is added in Websense Manager, the string '\22' is no longer displayed instead of double quotes. (v7.1 Hotfix 10, 12, 33, 69, v7.0.1 Hotfix 06, 22)

◆ Administrators can now add network ranges as clients. (v7.0.1 Hotfix 01, 22, v7.0 Hotfix 13, 21, 35)

◆ A Java error is no longer generated in the content pane when an administrator attempts to navigate to the Clients page in Websense Manager. (v7.0.1 Hotfix 01, 22, v7.0 Hotfix 08, 13, 21, 35)

◆ A warning is no longer generated in Websense Manager when an administrator attempts to add a network client, and the first value in the second IP address is greater than 127 (for example, 1.1.1.1 - 128.0.0.0). (v7.0.1 Hotfix 01, 22, v7.0 Hotfix 08, 13, 21, 35)

◆ Websense software can now query more than one global catalog server when an administrator adds directory clients in Websense Manager. (v7.0.1 Hotfix 01, 22, v7.0 Hotfix 08, 13, 21, 35)

◆ The Clients page now displays directory clients in alphabetical order, with domains appearing first, then groups, then individual users. (v7.0.1 Hotfix 01, 22, v7.0 Hotfix 13, 21, 35)

◆ Administrators who add a client to a role no longer receive an error message stating that the new client has a policy assigned when there are no policies assigned to that client. (v7.0 Hotfix 21, v7.0.1 Hotfix 22)

Websense Manager (Settings)

◆ Connection issues between Websense Manager and Websense Policy Server have been resolved. (v7.1 Hotfix 21, 33, 69)

◆ Duplicate entries no longer appear in the list of Policy Servers when an administrator makes changes to the Settings > Policy Servers page in Websense Manager. (v7.0.1 Hotfix 01, 22, v7.0 Hotfix 13, 21, 35)

- Latency was resolved in logon page loading and on the Settings > Policy page when many Policy Server instances appeared on the Settings > Policy Servers page in the Websense Manager. (v7.0.1 Hotfix 01, 22, v7.0 Hotfix 13, 21, 35)
- A complete list is now displayed on the Settings > Policy Servers page when more than 25 Policy Server instances are associated with one Websense Manager. (v7.0.1 Hotfix 01, 22, v7.0 Hotfix 13, 21, 35)
- When an administrator attempts to view the Settings > Risk Classes page, Websense Manager no longer displays an internal error in the content pane. (v7.1 Hotfix 10, 12, 33, 69)

Diagnostics

- The WebsensePing and TestLogServer tools now show custom URLs as recategorized. (v7.0.1 Hotfix 4, 29, v7.0 Hotfix 03, 20, 28)
- The WISP trace (used by Websense Technical Support for diagnostic purposes) now supports the Dynamic HTTP Lookup Request and Dynamic HTTP Lookup and Log Request messages. (v7.0.1 Hotfix 26, 29)

Reporting Tools (general)

- Log Server now successfully looks up full names and associated groups with User Service. (v7.1 Hotfix 05)
- The high value in the protocol field of Log Server records has been removed, allowing the information in these records to be saved to the Log Database and included in reports. (v7.1 Hotfix 18, 31)
- During startup, Log Server now tries to connect to the database only a specified number of times before recording a failure to connect. (v7.1 Hotfix 15, 31)
- Websense Log Server now supports all of Blue Coat's authentication realm types. User reports now show user names. User names are displayed correctly in group reports. (v7.0.1 Hotfix 32)
- Log Server no longer shuts down when renewing an SSL certificate. It successfully stores the certificate in the **LogServer.exe.p12 file**. (v7.0 Hotfix 31, 35)
- Attempting to report on source IP address and destination IP address no longer causes incorrect values in detail reports. (v7.0.1 Hotfix 03)

Today and History Reports

- Presentation reports and the Websense Manager Today and History charts now display properly in environments that use a non-standard port for Microsoft SQL Server. (v7.0.1 Hotfix 01, 22, v7.0 Hotfix 13, 21, 35)
- The Current Filtering Load line now plots data up to the current time, and the line does not drop to zero. (v7.0.1 Hotfix 01, 22, v7.0 Hotfix 08, 13, 21, 35)

Investigative Reports

- The length of the protocol field in Log Server records is now restricted, effectively preventing malformed protocol entries from appearing in investigative reports. (v7.1 Hotfix 31)

- More space is now allocated for concatenated investigative reports exported to PDF. (v7.1 Hotfix 45, 59)

- An issue that caused Administrators with long network account names to have problems accessing investigative reports has been resolved. (v7.1 Hotfix 45, 59)

- Investigative reports now use UTF-8 encoding. Any information passed using ISO-8859-1 encoding is now converted to UTF-8. (v7.0 Hotfix 14)

- Investigative reports showing the top <element> by <element> (for example, Top URL Hostnames by Category) can now be successfully exported to both PDF and XLS format. (v7.0 Hotfix 14)

Presentation Reports

- Presentation Reports Scheduler is now able to connect to the Policy Database when SQL Server is configured to use a non-standard port. (v7.1 Hotfix 12, 33, 69)

- An issue that generated an error when an administrator edited a copied presentation report was resolved. (v7.0.1 Hotfix 01, 22, v7.0 Hotfix 13, 21, 35)

- In presentation reports, it is now possible to specify up to Top 200. Note that the graph may not display in the report when you use a large Top N value. This is expected behavior. (v7.0.1 Hotfix 01, 22, v7.0 Hotfix 08, 13, 21, 35)

Filtering Service

- When the machine running Websense Filtering Service is shut down in a network where Websense filtering is integrated with a Squid proxy, client browser access now performs as expected. (v7.1 Hotfix 4)

- User data is now re-sent to Filtering Service, if a socket is busy during the first attempt to send it. (v7.1 Hotfix 42, 47, 51)

- An error encountered during the Master Database load process that reset the subscribed user count to 0 (or, the subscription key to expired) no longer occurs. (v7.1 Hotfix 68)

- Downloads of Real-Time Security Updates to the Master URL Database no longer fail as a result of a Microsoft C++ exception. (v7.1 Hotfix 67, 68)

- Issues with multi-threading no longer cause Websense Network Agent to stop running on Linux. (v7.1 Hotfix 32)

- An issue that caused Websense Master Database downloads to repeatedly fail and generated an AddFailure error message in Websense.log has been resolved. (v7.1 Hotfix 36)

- You can now configure Network Agent to ignore traffic and not show the IP addresses of interfaces in Websense Manager via settings in the **natuning.ini** file.

  Change the "IgnorePort80" parameter to "IgnorePorts" as shown below to have Network Agent ignore traffic on the specified ports. (v7.0.1 Hotfix 13, 29)

  For example:

      IgnorePorts = 80, 443

This fix also adds the "ShowNICsIP" to the natuning.ini file. When this parameter is set to false, Network Agent does not show the IP addresses of its interfaces in Websense Manager. The default value is true.

For example:

ShowNICsIP = false

◆ For sites running Websense Web Filter or Websense Web Security in a Stand-Alone deployment, an issue that caused Network Agent to occasionally stop with no error message has been resolved. (v7.0.1 Hotfix 35)

◆ An error message no longer appears occasionally when an administrator tries to recategorize a valid URL. (v7.0.1 Hotfix 01, 22)

◆ It is now possible to configure Websense Filtering Service to give Websense security risk categorization priority over custom categorizations, including limited access filters. (v7.0 Hotfix 28)

◆ CacheWISPUsers is an optional parameter in the Websense file **eimserver.ini**, used to cache user name/IP address pairs in HTTP requests. The User Map can no longer be corrupted by non-authenticated traffic when CacheWISUsers is enabled, and the Squid plug-in is in use. (v6.3.3 Hotfix 14, 27, 96)

◆ Administrators now receive an email alert when the Master Database download process fails. (v6.3.3 Hotfix 06, 27, 96)

◆ Filtering Service no longer occasionally shuts down when it receives a request to access a site defined as a custom URL. (v6.3.3 Hotfix 03, 27, 96)

◆ Filtering service now retries the connection to User Service (to obtain group information) until it is successful, for users filtered only by a group policy. (v6.3.3 Hotfix 96)

◆ Now Network Agent on Linux can handle more packets per second with a drop rate of less than 1%. (v6.3.2 Hotfix 59)

◆ Network Agent on Windows and Linux has now been updated to ignore exceptions caused by conflicts with Windows-based socket monitors. (v6.3.2 Hotfix 65)

◆ URLs containing a special byte sequence in the CGI portion of the URL on Windows machines no longer cause filtering to stop. (v6.3.1 Hotfix 136)

◆ All users discovered by DC Agent are now correctly transferred to the Filtering Service user map, and the correct filtering policy is now applied. (v7.1 Hotfix 29, 42)

◆ Websense Filtering Service with an integrated proxy now provides a valid HTTP block message string to the browser for explicit proxy clients, in compliance with a new HTTP protocol rule. (v7.1 Hotfix 19)

◆ Thumbnail images in Google search are now filtered correctly, even when the URL is requested from a link in investigative reports. (v7.1 Hotfix 39)

User Identification

◆ Users who log on to Novell eDirectory via Novell ZENWorks are now identified by Websense eDirectory Agent. (v7.1 Hotfix 30)

- Websense eDirectory Agent no longer connects to eDirectory Server through port 389, even though another port (such as port 636) had been selected for use. (v7.1 Hotfix 24, 30)

- NTLM v2 is now supported by Logon Agent and LogonApp.exe running with Windows 2000 and 2003. (v7.1 Hotfix 51)

- Microsoft software update KB960803 no longer causes the Websense logon application (**LogonApp.exe**) to fail to authenticate using NTLM on systems when the /dhcp option is used. (v7.1 Hotfix 13, 51)

- Websense Radius agent now has two optional configuration settings that you can specify in the initialization file **wsradius.ini**:

  - AcctDelayEnable

  - AcctDelayTime

  This intialization file resides in the Websense bin directory (by default, either C:\Program Files\Websense\bin\ or /opt/Websense/bin/).

  Websense RADIUS Agent now checks the initialization file to see if AcctDelayEnable is On or Off (default is Off). If it is On, then RADIUS Agent checks the value of the Acct-Delay-Time attribute in each Accounting-Request packet.

  When the value in the packet is larger than the predefined time set in wsradius.ini for AcctDelayTime (default is 0 seconds), then Websense RADIUS Agent ignores the packet.

  For example:

      AcctDelayEnable = On

      AcctDelayTime = 60 (v7.1 Hotfix 27, 51)

- An application event log has been added to provide alerts for any issues with transparent identification agents. (v7.1 Hotfix 47, 51)

- When no update is received from a transparent ID agent for 30 minutes, Filtering Service now reconnects to the agent. (v7.1 Hotfix 47, 51)

- An issue that caused administrators to sometimes be unable to browse the root domain when child domains were added to directory services has been resolved. (v7.1 Hotfix 10, 12, 33, 69)

- Websense user accounts that include hyphens (such as "report-auditor) can now be added to roles. (v7.0.1 Hotfix 01, 22, v7.0 Hotfix 08, 13, 21, 35)

- Results returned from the directory service are now alphabetized, as are pages, if paging is necessary. (v7.0.1 Hotfix 01, 22, v7.0 Hotfix 13, 21, 35)

- Websense User Service now retrieves only required attributes from Sun ONE. (v6.3.2 Hotfix 58)

- When Active Directory is the directory service, User Service now identifies all special characters and finds the user name correctly. (v6.3.2 Hotfix 16, 58)

- When Active Directory is the directory service, you now have the option of telling User Service to qualify the logon user with a user filtering string that you set in Websense Manager. (v6.3.2 Hotfix 16, 58)

- User Service now verifies user names in a Sun ONE Directory Server according to advanced Sun directory attributes. (v6.3.2 Hotfix 16, 58)

- An internal issue with Websense User Service no longer causes Novell eDirectory Server to lock up, behaving as if it had reached the maximum number of allowable connections. (v7.1 Hotfix 28)

- Logon now works as expected in situations where (a) the user was a member of a group that was a Delegated Administrator for a role and (b) the group name began with a special character (such as #). (v7.1 Hotfix 64, 69)

Delegated Administration

- The search mechanism for Delegated Administrators has been improved. (v7.1 Hotfix 48, 69)

- Delegated Administrators whose permissions do not include viewing user names can no longer use the Websense Manager Toolbox to search for users. (v7.1 Hotfix 43, 69)

- An issue that sometimes caused Delegated Administrators to be unable to log on to Websense Manager has been resolved. (v7.1 Hotfix 02)

Remote Filtering

- End users can no longer rename WDC.exe or delete driver files to bypass the protection of Remote Filtering. (v7.1 Hotfix 66)

- Remote Filtering Client can now identify Cisco non-split tunnel VPN traffic. (v7.1 Hotfix 66)

- PPP dial-in mode is now handled correctly, and client filtering occurs as expected. (v7.1 Hotfix 63, 66)

- Remote Filtering Client can now run on 32-bit Windows 7 machines. (v7.1 Hotfix 53, 66)

- Remote Filtering Server now checks the local initialization file (**securewispproxy.ini**) to obtain parameter settings, if Policy Broker cannot be reached, and the settings in that file determine whether HTTPS and FTP traffic is filtered. (v7.1 Hotfix 46, 66)

- Two new parameters in the file **securewispproxy.ini** make it possible to selectively disable or enable HTTPS and FTP filtering for Websense Remote Filtering client.

  This file is located in the Websense "bin" directory (C:\Program Files\Websense\bin or /opt/Websense/bin, by default).

  Add the appropriate entry to change the way HTTPS and FTP are filtered:

  - To disable FTP filtering, add the following line:

    FilterFTP=0

  - To disable HTTPS filter, add the following line:

    FilterHTTPS=0

  To return to the default behavior for either protocol, change the value of the parameter from "0" (disable) to "1" (enable). Save and close the

securewispproxy.ini file and restart Websense Remote Filtering to implement the changes. (v7.1 Hotfix 07, 66, v7.0.1 Hotfix 25, 34)

◆ Remote Filtering Client is now compatible with URLs containing a colon (:). (v7.0.1 Hotfix 34)

◆ Remote Filtering Client now detects if theclient has obtained an IP address from a wireless aircard. Quota time works as expected. (v6.3.2 Hotfix 62)

◆ Users can now visit the Web page for Live Search Cashback on MSN Live Search, from workstations where Remote Filtering Client is installed. (v6.3.2 Hotfix 47, 62)

◆ Users can now access Web pages by using quota time on workstations where Remote Filtering Client is installed. (v6.3.2 Hotfix 40, 62)

◆ Workstations where Remote Filtering Client is installed can now access application services that use the same IP address as the Remote Filtering Server. (v6.3.2 Hotfix 33, 62)

◆ Users can now add attachments in Outlook when Remote Filtering Client is installed. (v6.3.2 Hotfix 06, 62)

◆ Users can now compile .java files using IBM RAD when Remote Filtering Client is installed. (v6.3.2 Hotfix 06, 62)

◆ Users can now log on to their Windows Vista workstation when Remote Filtering Client is installed. (v6.3.2 Hotfix 06, 62)

◆ Copying and overwriting files to a mapped shared drive no longer lags when Remote Filtering client is installed. (v6.3.2 Hotfix 47, 62)

◆ Remote Filtering server no longer shuts down during peak traffic. (v6.3.3 Hotfix 18)

Services and Daemons

◆ Websense daemons no longer deadlock when signaled with SIGTERM for graceful shutdown (kill pid). (v7.0.1 Hotfix 4, 29, v7.0 Hotfix 15, 20, 28)

Integrations

◆ Customers using Websense Web Filter or Websense Web Security integrated with Citrix can now add a setting to the **wscitrix.ini** file to determine whether the user name from a Citrix session is returned from the Websense Citrix integration software.

The value of the new setting, DoNotSendUserName, is read by the Websense Citrix integration software.

If this flag is set to true, the Websense Citrix integration software does not return the user and domain name (only the client IP), so the user name entered during manual authentication in the browser is used for Websense logging.

The default value (false, or not set) causes the Websense Citrix integration software to send user names as well as user IP addresses.

A value of true prevents the user name from being sent:

> # By default is 'false', Citrix Integration sends user names to
>
> # EIMserver

If 'true', Citrix Integration does not send user names

DoNotSendUserName=false

(v7.1 Hotfix 22)

- For customers using Websense Web Filter or Websense Web Security integrated with Citrix, new parameters in the WsCitrix.ini file allow you to:

    a. Specify whether a protocol pop-up message is to be displayed when the SSL or FTP protocol is blocked.

    b. Set the minimum time interval between two sequential pop-up messages.

    The new parameters are:

    - DisplaySSLBlockMessage specifies if a pop-up message is displayed when the SSL protocol is blocked.

    - MinTimeBetweenSSLMessages defines the minimum time interval (in seconds) between 2 sequential pop-up messages when the SSL protocol is blocked.

    - DisplayFTPBlockMessage specifies if a pop-up message is displayed when the FTP protocol is blocked.

    - MinTimeBetweenFTPMessages defines the minimum time interval (in seconds) between 2 sequential pop-up messages when the FTP protocol is blocked. (v7.1 Hotfix 22)

- The Websense plug-in for Citrix integrations can now be configured to ignore specific IP addresses.

    To do this, add the parameter IgnoreIPList to the file wscitrix.ini. The value of this parameter is read by the Websense Citrix integration software.

    When the Websense Citrix plugin receives a browsing request, it determines if the destination IP address is in the ignore list.

    If it is, then the software allows the request; no filtering is performed. (v7.1 Hotfix 09, 22)

- Long URLs can no longer trigger an exception during filtering that caused an integrated Blue Coat appliance to close its connection with Websense Software. (v6.3.3 Hotfix 27)

- UFP server no longer shuts down unexpectedly when Websense software is integrated with CheckPoint Firewall-1. (v7.1 Hotfix 14)

SSL Issues

- Pages transmitted over SSL (assumed to contain sensitive information) are no longer cached by the browser. (v7.1 Hotfix 21, 33, 69)

- The Secure Attribute is no longer missing in an Encrypted Session (SSL) cookie. (v7.1 Hotfix 21, 33, 69)

Known issues

Upgrade

- When you upgrade to v7.1.1 from v6.3.x, configuration settings for Active Directory in Websense Manager cannot be saved. After upgrading, navigate to the **Settings** > **Directory Services** page and make sure the settings reflect your desired configuration.

- During the process of upgrading to or from v7.1.1, the parameter redirect_children, in the **squid.conf** file located by default in the /etc/squid directory, is reset to default.

- Warning messages in the installer log files are informative only and do not indicate an error condition or installer problem. There is nothing you need to do about these messages.

- Two new parameters in the file **securewispproxy.ini** make it possible to selectively disable or enable HTTPS and FTP filtering for Websense Remote Filtering client.

  This file is located in the Websense "bin" directory (C:\Program Files\Websense\bin or /opt/Websense/bin, by default).

  Add the appropriate entry to change the way HTTPS and FTP are filtered:

  - To disable FTP filtering, add the following line:

    FilterFTP=0

  - To disable HTTPS filter, add the following line:

    FilterHTTPS=0

  To return to the default behavior for either protocol, change the value of the parameter from "0" (disable) to "1" (enable). Save and close the **securewispproxy.ini** file and restart Websense Remote Filtering to implement the changes.

Websense Manager

- When using the **Add Clients** page, administrators must first expand the organizational unit (OU) that contains the clients, and then select it.

  If the OU is selected first, and then expanded, clients are not added successfully. This affects organizational units that contain a pound symbol (#). In this case, you must remove the old entries and add them again. (v7.1 Hotfix 12, 33, 69)

Other components

- To take advantage of some fixes for issues with incorrect user filtering, you need to delete the affected users, add them again, apply policy, and then select **Save All**. For example, filtering policy was not always applied correctly to users whose name included special characters. If the user could be identified with a group, the group policy was applied instead of the user policy. Otherwise, the default policy

was applied. To take advantage of the correction for this issue, delete the users, add them again, and reassign a filtering policy.

Windows

◆ On Windows, it is advisable to uninstall Windows socket monitoring software, because it may cause a conflict with Network Agent. (v6.3.2 Hotfix 65)

Remote Filtering

◆ If Remote Filtering Client is installed from the command line on a Windows machine, the REBOOT parameter, which defines whether the client computer is restarted automatically after installation or uninstallation, does not take effect. As a result, no automatic reboot occurs. This means that some Web sites or protocols that you expect to have blocked may not be blocked. You must manually restart the client machines after command-line installation or uninstallation of Remote Filtering Client.

◆ If you customize the the value of the Fail closed timeout field and also mark the Fail closed check box on the Settings > General > Remote Filtering page in Websense Manager, then the Remote Filtering Client service must be manually restarted at each client. Otherwise, the Fail closed setting does not take effect as expected. (Mark the Fail closed check box to block Remote Filtering Clients from all Internet access unless their computer is communicating with Remote Filtering Server. By default, this is not selected, which means remote users have unfiltered access to the Internet when their computers cannot communicate with the Remote Filtering Server.)

v7.1 Hotfixes not included in v7.1.1

The following v7.1.0 issues still exist in version 7.1.1. Corrections were made avialable as hotfixes for v7.1.0, but these corrections are not currently available in v7.1.1:

◆ In deployments that integrate Websense software with Microsft ISA Server, an out-of-memory sometimes causes ISA Server to shut down.

This can happen when an HTTP client in the network makes HTTP requests over the same TCP connection for a very long time (several days). (v7.1 Hotfix 44)

◆ Websense Manager supports secure HTTP methods. However, it is possible for a security scanner such as IBM App Scan to report that the machine running Websense Manager supports Insecure HTTP methods.

This is because the scanner encountered Web-based distributed authoring and versioning (WebDAV) methods listed in the response to an OPTIONS request made to the Websense Manager machine.

Other security scanners may report this as a vulnerability as well. (v7.1 Hotfix 55)

Upgrading to v7.5.0 from v7.1.1

◆ Some custom settings are reverted to their default values during a direct upgrade from v7.1.1 to v7.5.0. See the v7.5 upgrade guide for details.