WEBSENSE JUMPSTART KIT CHECKLISTS: TOOLS AND INFORMATION FOR A SMOOTH PILOT V1.7

Contents

Purpose of the Document

The purpose of this document is to provide guidance to the Channel Partner utilizing check lists during the deployment, installation, maintenance, disaster recovery process review of Websense Web Security Suite 6.3.

Who Should Use this Document

This document should be used by Websense Channel Partner Personnel (e.g. Systems Engineers or Security Specialists) to provide onsite customer installations of the Websense Web Security Suite 6.3 product. The Channel Partner must have thorough Websense product knowledge and product certification training provided by Websense.

Overview

Use the checklists within this document in conjunction with your Customers' needs or the service you are providing. You can print this document and provide specific sections to your Customer as a check list of objectives for a successful deployment of the pilot or evaluation of the Websense software.

Customer requirements or product integrations may require the review of additional product documentation. See references to product documents that will facilitate your research for additional product information in the appendix of this document.

Objective

This document contains several sections that will assist you with preparation, installation, maintenance, and disaster recovery for your Customers. If your intent is to provide maintenance service for an existing installation, see the maintenance section.

This document is a supplement to the current Websense product documents that are required for a complete installation of the Websense Web Security Suite product. The checklists within this document do not replace the Websense product documents.

Technical Support

Websense Technical Support is available to all Channel Partners by phone and from the Websense website.

For best results, search the Knowledgebase first. If a Solution is not found, open a support request online while you dial the support number. That way, by the time your call is answered, you can refer the Support Engineer to your new case you have created that contains the necessary details. Be sure to include your office and mobile phone numbers to expedite resolution. Make sure your spam filter permits email from 'websense.com', and be sure to respond to all support replies by phone, email, or using the online form to prevent your case from being closed for unresponsiveness. If your case is closed prematurely, ask that it be reopened; otherwise, you may be asked to start troubleshooting from the beginning.

Knowledgebase -- http://ww2.websense.com/global/en/SupportAndKB/SearchKB/
Technical Support Online -- http://ww2.websense.com/global/en/SupportAndKB/CreateRequest/
Technical Support Phone -- 5 a.m. to 5 p.m. Pacific Time (858) 458-2940

About Websense Web Security Suite

Websense Web Security Suite is a leading web security solution that protects organizations from known and new web-based threats. Based on the industry-leading Websense ThreatSeeker™ technology, Websense Web Security Suite protects against spyware, malicious mobile code, phishing attacks, bots, and other threats. Unlike some other solutions, it also blocks spyware and keylogger backchannel communications from reaching their host servers. In addition, only Websense Web Security Suite offers the Websense Web Protection Services that help protect organizations' websites, brands, and web servers.

Websense Web Security Suite protects the enterprise network at the gateway, while promoting employee productivity through behavior reinforcement. Gateway enforcement includes blocking access to dangerous and offensive websites, limiting time spent on unproductive sites, blocking undesirable protocols from exiting the corporate gateway, and restricting the use of network protocols to desirable purposes. In addition, Websense Web Security Suite offers additional services that can monitor for certain fraudulent use of an organization's brands (BrandWatcher™) as well as unauthorized changes made to its websites (SiteWatcher™), additionally it allows you to specify one public facing web server to be vulnerability scanned (ThreatWatcher™). Websense Web Security Suite promotes productivity by applying immediate feedback to users' behavior while enforcing the company's Internet policies. This behavior reinforcement is achieved through hard blocks, time quota-limited blocks, blocks with a "continue" option, and through the users' knowledge that their activity is being monitored and logged.

Why a Pilot versus an Evaluation

Websense Web Security Suite can be deployed as a “pass-by” technology, meaning … when configured in “monitor only” mode there is no impact to users or equipment on the Customer’s production network. In this configuration, Websense software is completely transparent while it is operational and when it is offline. You can apply policies to a small number of users and workstations for testing. Deployment on the Customer’s production network ensures that the test conditions and results are true to their actual environment, not obscured by unusual configurations and unsupervised changes made in a lab. Converting the pilot deployment to production simply requires replacing the pilot evaluation key with a subscription key. Generally, no additional effort is needed.

Pilot Schedule

For the smoothest transition from pilot to production, Websense recommends adopting the following schedule to facilitate a successful pilot, where management can review and approve the product acquisition, and a PO is received within the 30-day evaluation key time limit. If the time limit is reached, filtering will either fail open (default, all traffic is allowed to the Internet) or fail closed (optional, all traffic is blocked).

Pilot Deployment Date:	Day 1 (Pre-Deployment Checklist completed.)
Status Review:	(recommended no later than Week 2)
Present Results to Management on:	(recommended no later than Week 3)
Submit Order Requisition by:	(recommended no later than end of Week 3)
PO Received by Websense on:	Day 30 (a production key will be sent via email)

Questions to Ask Your Customer

Listed below are general questions you could ask your Customer. These questions are grouped into several sections; Preparation, Installation, and Maintenance. Added to the bottom of the list are general questions typically asked by a Customer. However, the questions you receive may vary considerably. Additional questions for information gathering may be required, depending on the type of service you are providing for your Customer.

The **Preparation Questions** are provided to assist you with the preparation for an onsite installation of the Websense Web Security Suite product. These questions will also assist your Customer with preparing for the installation.

The **Installation Questions** are provided to assist you while you are onsite to ensure the Customer's environment is set up to meet the requirements for the installation.

Maintenance Questions are typically used during follow up visits to ensure the integrity of the product. By definition, this is not a performance or tuning process. If assistance is needed, contact Websense Technical Support.

Customer Questions can vary depending on their needs or requirements, so a sampling has been provided. If assistance is needed to respond to their questions, contact Websense Technical Support.

Preparation Questions

- ❑ What is the Customer's experience with Websense?
- ❑ What is the Customer currently doing for Web Filtering?
- ❑ What security concerns are foremost in the minds of the executive staff right now?
- ❑ How many total users and total computers?
- ❑ How many different Points of Presence are there to the internet? Will all connections need to be filtered? (This is critical for transparent authentication. The customer will have to have a service account set up for directory service and XID functionality. If allowed by the customer, it's always a good idea to use the same service account ID for the SQL server also.)
- ❑ How many different firewall/proxy/cache products are being used and what types?
- ❑ What product (feature) preference does the customer have?
- ❑ What is the intent for using URL Filtering?
- ❑ Will there be more than one policy?
- ❑ Is there a written internet usage policy? If no, who would be involved in creating this policy; IT, HR, Legal?
- ❑ Are Directory Services going to be used with the filtering solution? If yes, which service and what version?
- ❑ Will there be any product integration? If yes, what platform?
- ❑ Provide the Customer the Websense hardware and software requirements.
  - ❑ If there is an existing server, ensure the Operating System and patch levels are current.
  - ❑ If there is an existing server, ensure the hardware configuration meets the requirements.
- ❑ What is the IP address of the servers where the Websense components will be installed?

- ❑ What is the IP range that the Customer wants filtered?
- ❑ Are there any requirements where SQL database or logging needs to run on a separate server?
- ❑ Is the Customer going to run Reporting on Unix or Windows?
  - ❑ If Unix, does the customer have the correct version of MySql installed?
- ❑ If the system is under 1000 users with Windows, is SQL or MSDE preferred?
- ❑ If the system is over 1000 users with Windows, will SQL be installed on a dedicated system or on a shared SQL server/cluster?
- ❑ If Network Agent is to be involved, do we have access to someone who will configure a span/monitor port for us, or is there space on the switch where the egress point for the inside interface of the firewall is located? We need 1 span/monitor port, and 1 normal port on this switch to do blocking

Installation Questions

- ❑ Has someone verified the configuration of the span/monitor port?
- ❑ If the span port has not been configured, do we have access to configure?
- ❑ What is the IP address and NIC configuration?
- ❑ A username and password is required for integrating Websense to your chosen directory structure. Do you have the full context for the username to be used in the directory structure setup?
- ❑ Have all patches and security updates been applied to the server?
  Note: Microsoft's Knowledgebase article KB294054 for Windows 2003 server. This Hotfix is required for customers who have installed the 08-08-2006 Microsoft Security Update. It resolves the Websense Manager GUI crash when remotely accessing the Filtering Server via RDP.
- ❑ Do you have access (username/password) to configure the integration, if needed, or will someone be available to assist? This is critical if you are integrating Websense software. Without this step you won't see the integrations traffic.
- ❑ Has the SQL server had all patches and security updates applied to the system?
- ❑ Are you using the SQL SA account, or has the customer created another SQL account for Websense?
- ❑ What rights does the SQL account have on the SQL server? Where is the SQL server located in the network?
- ❑ Is IIS or Apache installed? Can we use the IIS Default website for our Web Reporting Tools?
- ❑ Is this Web Server running other applications that may conflict with our Web Reporting Tools?
- ❑ Are you using Anonymous Access with the built-in IUSR account for IIS or another user account? Does this account have permissions on the Websense\webroot directory?

Maintenance Questions – (use during installation or as a post installation service)

- ❑ Reporting- Do you need to record all traffic (hits) or are the visits sufficient? This will reduce the amount of disk space needed for the SQL database. Hits or Visits show how much bandwidth or browse time was used by an activity.
  Note: All internet access requests pass through Filtering Service. These requests are analyzed to determine the actual sites a user views (visits), or the images, text blocks, ads, and other files (hits) acquired during a page request. The default setting is Visits.

- ❑ Reporting - Do you want to consolidate user activity records or do you want a record for each visit? (Consolidating will reduce SQL database size but will result in some loss of granularity and precision of database records.)

- ❑ WebCatcher captures and sends anonymous data records for "uncategorized" and "security related" sites to Websense for review and classification. Use of this functionality helps reduce the Customers administrative time and costs and also increases the accuracy of user related URL sites seen by the Customers organization. Is it allowable to enable this feature?

- ❑ Are you currently using the Websense Database Administration tool to archive, purge, auto "roll" and create databases, or is this done by an in house DBA? The Websense Database Administration tool can be located within the Websense Reporting Tools.

- ❑ Have you run the Websense Reporting Tool and reviewed the category and protocol usage since the installation to possibly refine your initial policies? Customers traditionally say they want to allow a category or protocol at first, but once they see the reports related to its actual usage/possible abuse, they typically want to refine the policies to better control usage (category/protocol/network bandwidth.)

Customer Questions with Answers

- ❑ Why do I have to give you a domain admin account?

  Answer: The Websense DC Agent uses domain administrator privileges. On Windows, the domain administrators group used must be a member of the Administrators group on the current machine. This is required for DC Agent to retrieve user logon information from the domain controller. If you cannot install DC Agent with such privileges, configure administrator privileges for these services after installation.

- ❑ If the integration only passes Websense HTTP traffic, how does Websense filter all other protocols?

  Answer: Network Agent filters all other protocols via a port span mirroring all outbound/inbound traffic from the firewall.

- ❑ Can I distribute Websense components on different operating systems?

  Answer: Yes, Websense components can be distributed between Solaris, Linux and Windows. The Websense Reporting components must be installed on a Windows OS with the exception of Unix Log Server/Unix Explorer. See the Websense Deployment Guide for details.

- ❑ If the Websense Server goes down, do my users lose access to the internet?

  No, configure the integration to fail open. In StandAlone mode, Network Agent fails open by default.

- ❑ What happens if we exceed the subscription count?

  Answer: Requests that exceed the user subscription go unfiltered unless Websense Manager is configured to “Block users when subscription expires or is exceeded”.

- ❑ Can we customize the Websense Block page with our company logo, security policy information?

  Answer: Yes. Websense software lets you modify portions of the default block messages, using a text editor. Refer to Chapter 3, Filtering Basics, in the Websense Administrator’s Guide for details on how to customize the Websense Block page.

- ❑ How can we restrict some users’ internet usage to only a few websites?

  Answer: Configure the Websense Policy using the Yes List feature. A Yes List allows users to access only URLs in the list, blocking access to all other websites.

- ❑ Won't my SQL database grow into an unmanageable size if it logs everyone’s internet traffic?

  Answer: No, in Websense v6.3 the database will roll into a new partition (.mdf & .ldf) based on a predefined size. A “Catalog Database” will have views into new and existing partitions, giving full reporting access to all data. You can also recommend that your Customer move the archive data to another storage server (online or offline) to make space.

Preparation Checklist

This Preparation Checklist is provided as an outline of the major activities necessary to prepare you for a successful evaluation of the Websense Web Security product.

Review Product Documentation

- ❑ Websense Evaluation Guide
- ❑ Websense Deployment Guide

Review the following criteria to establish objectives

- ❑ **Mitigate Legal Liability**
  Examples: Block pornographic websites ("hostile workplace" compliance), pornographic image searches on Google and Yahoo!, peer-to-peer file sharing (potential copyright infringement and a potential source of porn), Instant Messaging (potential source of information leaks), Instant Messaging Attachments (potential source of information leaks and a security risk).

- ❑ **Mitigate Productivity Loss.**
  Examples: Block pornographic websites, pornographic image searches on Google and Yahoo!, advertisements, peer-to-peer (P2P) file sharing protocols, streaming media protocols, Internet radio and TV sites, Instant Messaging (IM) sites and protocols, MP3 sites and file type downloads, Internet storage sites. Set quota limits on shopping websites, news, and sports sites. Block the launch of IM, P2P, and streaming media applications on the desktop.

- ❑ **Mitigate Security Threats**
  Examples: Block spyware infection and back channel sites (payload delivery and re-infection), malware infection and back channel sites, phishing and other Internet fraud sites, keyloggers, proxy avoidance sites and protocols, Internet storage sites, and IM attachments. Block the launch of hacking tools, spyware, and malware on the desktop. Block the silent install of applications on the desktop. Block network access for all unknown applications. Automatically generate reports on these activities for follow-up. Automatic, real-time updates on security-related threats, and automatic email notification of new web-based threats. Notify on detected fraudulent uses of brand and corporate image, and on unauthorized website changes.

- ❑ **Mitigate Bandwidth Loss**
  Examples: Block streaming media protocols, Internet radio and TV sites, MP3 sites and file type downloads, peer-to-peer file sharing. Set quota limits on shopping websites, news, and sports sites. Block streaming media and Voice Over IP (VOIP) applications on the desktop.

- ❑ **Demonstrate Ease of Use**
  Examples: 100% GUI-driven management interface; user-friendly reporting tools; automatic categorization and feedback loop for URLs, protocols, and applications; automatic nightly database updates.

Procure Appropriate Hardware

- ❑ Customer should have the following minimum required hardware for the evaluation process. These should be considered minimum requirements for any evaluation.
- ❑ Hardware requirements for actual deployment will vary depending on amount of users and traffic. Please consult the Websense Deployment Guide for actual Hardware requirements.
- ❑ Single CPU P4 3GHz processor or better, with 2GB Ram minimum
  85GB Hard Drive
  Two (2) Network Interface Cards (NICs)
  Windows 2000/2003 server Operating System (with current Service Packs)
  Windows SQL server (2000 or 2005) or MSDE
  IIS or Apache
- ❑ Change Control – Clear the installation activities with the customer change control process.

Request Evaluation Key and Download the Software

- ❑ Go to Websense website to register and request an evaluation key, and then download the software to the server. The evaluation key will arrive via email within a few minutes.
  http://ww2.websense.com/global/en/Downloads/
  http://www.websense.com >> Downloads >> Full Release Trial

Switch Configuration for Websense Network Agent

- ❑ Configure your switch to mirror (or SPAN) the firewall port to Websense Network Agent. The mirrored port needs to be between the users and ahead of any device that does network address translation.
- ❑ Run one Ethernet cable from the SPAN port to the Websense server.
- ❑ Run a second Ethernet cable from the switch to the Websense server.
- ❑ Alternatively, place a hub between the switch and firewall, and connect Network Agent to the hub. Network Agent is required for multi-protocol monitoring and filtering, IM Attachment Blocker, and Bandwidth Optimizer.

Pre-Installation

- ❑ Determine which directory services are being used.
  Active Directory (native/mixed), LDAP, eDirectory, Radius.
- ❑ If Windows environment, make the Websense server a member server with desired machine name.
- ❑ One static IP address
- ❑ Identify the *internal* SMTP mail server for sending email alerts and reports. If mail relay is disabled for security reasons, set up an email account for sending mail alerts.
- ❑ Install IIS or Apache prior to installation of Websense Components.
- ❑ Ideally, your database engine will reside on its own server, such as an enterprise SQL server.
  If not, install the database engine (SQL, MySQL, or MSDE) on the Log Server.
- ❑ Install all the latest patches for the OS, IIS, and SQL (or MSDE). On Solaris or Linux, get the Websense installer download, gunzip, from mywebsense.com. Make note to run the Websense installer with the "check patch levels" option, and then get the patches listed for the install.

Network Access

You have several options for port configuration and you will need to plan in advance of the installation. Refer to the Network Ports section in the Pre-Installation Checklist.

Note: Additional default ports are listed in Knowledgebase Article 604:
http://www.websense.com/support/knowledgebase/Display.php?faq=604

Passwords

The following passwords are needed to deploy Websense software.

- ❑ IP address, username, and password to configure the switch
- ❑ IP address, username, and password to configure the integration device
- ❑ Username and password for the integration software
- ❑ Admin account and password for the various Websense servers
- ❑ An account with 'domain admin' privileges to read user accounts
- ❑ SQL account to create/manage databases (e.g., 'sa' login and password)
- ❑ Name / IP of internal SMTP server (specify *internal* mail server)
- ❑ Email account (for alerts and reports, if open relay is disabled internally)
- ❑ Proxy IP, port, and account (for the nightly database download)

Personal Resources - Specialist

You may need the assistance from the following specialist during the deployment:

- ❑ Integration Device (Firewall/Proxy) Engineer scheduled to be on duty on deployment day
  Integration Device Engineer name and cell phone:
- ❑ Switch Engineer scheduled to be on duty on deployment day
  Switch Engineer name and cell phone:
- ❑ Directory Services Engineer scheduled to be on duty on deployment day
  Directory Services Engineer name and cell phone:
- ❑ Websense Operator scheduled to be on duty on deployment day
  Websense Operator name and cell phone:
- ❑ Database Administrator scheduled to be on duty on deployment day
  Database Administrator name and cell phone:
- ❑ Desktop Security Engineer scheduled to be on duty on deployment day
  Desktop Security Engineer name and cell phone:

Installation Checklists

This section of the document serves as a guide for deploying Websense Web Security Suite**,** and will ensure the success of your deployment. There are references to multiple server configurations if this is a preference by your Customer. This section is not intended to replace the Websense product documents. References to these documents are provided in the Appendix of this document.

Pre-Installation Checklist

Environment	**Deployment Date:**

- ❑ Production network
- ❑ Laboratory (Note: Lab results are not certifiable.)
- ❑ Internet connections at this facility: ❑One ❑more (specify) Type: (specify)
- ❑ Remote branches supported: (specify number and location)
- ❑ Remote branches use ❑their own Internet access ❑corporate Internet access
- ❑ Remote branches will connect to Websense via ❑VPN ❑private circuit

Integration

- ❑ Standalone
- ❑ Integrated (with)
- ❑ Embedded (on)
- ❑ IP address of integration/embedded device:

Switch Configuration

- ❑ Hardware brand: model:
- ❑ Configure a bi-directional mirror/SPAN of the firewall port. http://www.securitywizardry.com/switch.htm
- ❑ Run one Ethernet cable from the SPAN port to the Websense server.
- ❑ Run a second Ethernet cable from the switch to the Websense server.

Directory Services

- ❑ NT/AD mixed
- ❑ AD native
- ❑ LDAP
- ❑ eDirectory (❑ with NMAS)
- ❑ RADIUS
- ❑ **Optional**: Account with domain read privileges: (specify dom/account)

Websense Server

- ❑ Hardware brand: Model: CPU: RAM:
- ❑ OS: ❑ Windows 2000 ❑ Windows 2003 ❑ Linux RH Enterprise 3.0
  ❑ Linux RH Enterprise 4.0 ❑ Solaris 9 ❑ Solaris 10

- ❑ Size server according to Websense specifications
- ❑ Configure two NICs (one for monitoring, one for management/blocking)
- ❑ Configure static IP address for management NIC:
- ❑ Install IIS web server (or accept Apache during Websense install)
- ❑ Apply all service packs and critical updates
- ❑ Add server to the domain (or a trusted domain)
- ❑ Configure network time service
- ❑ Document any security modifications made (for troubleshooting)

Reporting Server

- ❑ Reporting Server is on the Websense server its own server
- ❑ Hardware brand: Model: CPU: RAM:
- ❑ OS: ❑ Windows 2000 ❑ Windows 2003 ❑ Linux RH Enterprise 3.0
  ❑ Linux RH Enterprise 4.0 ❑ Solaris 9 ❑ Solaris 10

- ❑ Size server according to Websense specifications
- ❑ Install IIS or Apache web server
- ❑ Configure static IP address: (specify IP)
- ❑ Apply all service packs and critical updates
- ❑ Configure network time service
- ❑ Document any security modifications made (for troubleshooting)

Database Server

- ❑ Database Engine is on:
  ❑ Websense Policy Server & Reporting Server
  ❑ Websense Dedicated Reporting Server
  ❑ Dedicated SQL server server name or IP
- ❑ Hardware brand: Model: CPU: RAM:
- ❑ OS: ❑ Windows 2000 ❑ Windows 2003 ❑ Linux RH Enterprise 3.0
  ❑ Linux RH Enterprise 4.0 ❑ Solaris 9 ❑ Solaris 10

- ❑ Size server according to Websense specifications
- ❑ Use separate spindles, one for OS and apps, and one for database
- ❑ Install DB engine: ❑ MSSQL 2000 ❑ MSSQL 2005
  ❑ MSDE 2K (no SQLExpress) ❑ MySQL 5.0

- ❑ Recommended: Use SQL authentication type SQL (not Windows)
- ❑ Configure static IP address: (specify IP)
- ❑ Apply all service packs and critical updates
- ❑ Document any security modifications made (for troubleshooting)

Network Ports	Reference this table for multiple server installations

- ❑ Open HTTP and FTP from the Websense Filtering Server to the internet to download the install files and patches from MyWebsense.com
- ❑ Open HTTP and FTP from the Websense Filtering Server to the internet for database updates to the Policy Server
  - download.websense.com
  - ddsdom.websense.com
  - ddsint.websense.com
  - portal.websense.com
- ❑ Open 15868/TCP from the integration device to the Filtering server. (Port 18182/TCP for the UFP filter with CheckPoint FW-1.)
- ❑ Open 55805/TCP from the Filtering Server to the Log Server
- ❑ Open SQL ports from the log server to the SQL Database Server
- ❑ Open NetBIOS ports between DC Agent and all Domain Controllers
- ❑ Open NetBIOS bi-dir between DC Agent and User Service
- ❑ Open NetBIOS bi-dir between User Service and domain controllers
- ❑ Open HTTP/S to the Filtering and Reporting Servers (for RTA and Explorer)
- ❑ Open 25/TCP from the servers to your internal mail relay
- ❑ Open 40000/TCP between all Websense Components
- ❑ Review KB 604 for other requirements (LDAP, eDirectory, etc.) http://ww2.websense.com/support/knowledgebase/Display.php?faq=604

Installation Checklist

Uncompress the Download Package

- ❑ Windows: Double-click the downloaded executable
- ❑ Solaris/Linux:
  - 'gunzip' the downloaded file
  - 'tar xvf' the gunzipped tar file

Install Websense

- ❑ Run the installer, following the onscreen prompts for Websense
  - Windows: run c:\temp\WebsenseSecuritySuite63Setup\Setup.exe
  - Solaris/Linux: ./install.sh

Install Reporting

- ❑ Run the installer, following the onscreen prompts for Reporting Tools
  - Windows: run c:\temp\WebsenseSecuritySuite63Setup\Setup.exe
  - Solaris/Linux: ./install.sh
  - **Note**: The filter and reporting versions must match
  - **Note**: Use the same SQL authentication method used during SQL setup

Verify Installation

- ❑ Check Real-Time Analyzer's Protocol Trends
  - HTTP/HTTPS/FTP may come from the integration device (if any)
  - IM/P2P/Streaming Media will come from Network Agent (if deployed)
- ❑ Check /var/adm/messages or Windows Event Viewer – Applications
  Check <install path>\Websense\bin\Websense.log
- ❑ Check that Websense services are running
  - Windows: Use the Windows Services dialog box
  - Solaris/Linux: './WebsenseAdmin status'
- ❑ Check <install path>\Websense Reporting\LogServer\Cache
  - You should see files created and deleted, no more than 10 at any time
- ❑ Use SNMP to test for active NICs and a live OS
- ❑ Set up alerts in case a Websense service fails to start or re-start
  - Windows: Set the recovery options to "restart>restart>run a program
- ❑ Set up automated weekly spyware reports. Reference the Reporting Administrator's Guide for details.
  - Send the desktop support group a message to clean infected systems.

Maintenance Checklists

Health Assessment

Performing a Quick Health Assessment
❑ In Real Time Analyzer (RTA), the default view (Risk Classes) should have data, typically displaying data in all five risk classes. ❑ In RTA, click “Protocol Trends”. Normally, you would expect to see six or more protocols (HTTP, HTTPS, some streaming media protocols, etc.) ❑ In RTA, click “Running Detail”. You should see usernames in the source column. ❑ On the machine running Log Server, check the <install path>\Websense\bin\cache directory. The .tmp files should have time stamps within one minute of the current system clock, and there should be less than a dozen files total (three is normal). ❑ Check for free space on the install disk. 2GB free is recommended minimum. ❑ Check for free space on the disk supporting the Log Database file (e.g., wslogdb63.mdf). DB_Administration requires 2x to 3x the .mdf size to create archives.

Automating the Websense Health Assessment
❑ Make sure all Websense services are running, and investigate any sudden stops. ❑ Check to make sure the <install path>\Websense\bin\cache directory contains at least one .tmp file within the current minute of the system clock, and no more than a dozen files total. During peak user activity, the file size should be greater than 1KB up to about 4MB (depending on seats). ❑ Keep at least 2GB free disk space on the application drive for nightly updates. ❑ Keep 2x to 3x the .mdf file size in free disk space for creating log data archives. ❑ Monitor the Websense.log file for sudden rapid growth or excessive size, and monitor the Event Viewer or similar system log files for repetitive errors. ❑ Make sure the bin\Websense file (no extension) is less than three days old. ❑ Monitor CPU and RAM utilization to maintain within acceptable limits of the OS.

Detailed Maintenance Checklist

Websense Filtering Server Maintenance

- ❑ Check the current patch levels
  - ❑ Operating System, Browser, Web Server
- ❑ Check the Websense version installed
  - ❑ Websense Manager, navigation pane, expand Filtering Services, select IP
  - ❑ Websense Manager > Help > About
- ❑ Check the Event Viewer – Applications log (or var/adm/messages or var/log/messages)
  - ❑ User Service errors contacting domain controllers
    - ❑ If the server is not a member of the domain, set User Service's logon properties using a valid domain account.
    - ❑ If the server is a member of the domain, or logon properties are valid, check to make sure network firewall ports are open between User Service and the domain controllers.
  - ❑ Filtering Service failed to connect to the Policy Server
    - ❑ Check to see if the Policy Server service is running
    - ❑ Check for open ports (telnet <PolicyServerIP> 15869)
    - ❑ Start Filtering Service if stopped
  - ❑ DC_Agent errors connecting to a domain controller
    - ❑ If the domain controller is not valid, edit Websense\bin\dc_config.txt and set the domain controller to =off. Restart DC Agent service.
    - ❑ If the domain controller is valid, set the logon properties of DC_Agent Service to a valid domain login, or add the server itself to the domain.

- ❑ Use the Event Viewer to check the System log for W32Time errors or NTP errors. Accurate reporting requires time services to be functioning correctly. Keep written records of any time discrepancies (for accurate forensics), and correct errors as soon as possible.
- ❑ Check <install path>\Websense\bin\Websense.log
  - ❑ Correct Warnings and Fatal Errors
  - ❑ Make sure the nightly database "transferred", followed in 30 minutes or so by "database loaded" with an incremented number and yesterday's date.
    - ❑ If the database number and date are not incrementing, check for scripts interrupting the update process.

- ❑ Check to make sure Websense services are running: (On Solaris or Linux, use the command *ps –ef* or opt\Websense\bin*WebsenseAdmin status*.)
  - ❑ Websense Policy Server (Note: Multiple Filtering Services can communicate to a single Policy Server. All Filtering Services are listed in the management console and in config.xml. Inspect those servers as well.)
  - ❑ Websense Filtering Service (also called "Websense EIM Service")
  - ❑ Websense Network Agent (optional, required for dynamic protocol filtering and monitoring, bytes transferred, Bandwidth Optimizer, Instant Messenger Attachment blocking, and all stand-alone environments).
  - ❑ Websense Real-Time Analyzer (RTA) (optional but highly recommended, requires either IIS or Apache web server)
  - ❑ Websense User Service (optional, required for user ID and/or creating user and group policies)[1]
  - ❑ Websense XID Authentication Server (optional, for user ID)[1]
  - ❑ Websense DC Agent (optional, recommended for user ID in Active Directory or NT domains)[1]
  - ❑ Websense Logon Agent (optional, recommended for user ID in Active Directory)[1]

[1] This service might be running on another machine. In v5.5.x, check the Websense Management console > Server > Settings > User Identification, edit settings, to locate it. In all 5.x versions and higher, the IP address of every installed service will be listed in the config.xml file.

- ❑ Websense eDirectory Agent (optional, recommended for user ID in Novel environments)[1]
- ❑ Websense RADIUS Agent (optional, for user ID in RADIUS environments)[1]

❑ Set Recovery options on Websense services (Windows OS only):
Right-click Websense services, select Properties > Recovery tab, set recovery options to restart—restart—run a program. Follow KB775 to create a VBScript, the program to run, which sends an email alert if the service cannot restart.
Notes:
- ❑ The SMTP server must allow mail relay, usually enabled on an internal NIC only.
- ❑ A real email account to send from is not necessary if relay is enabled.
- ❑ To speed identification make the "from" address the server name.
- ❑ Send alerts to an email alias for the on-duty engineer, or separate names with a comma. Consider sending alerts to your pager or text-enabled cell phone.
- ❑ Test the VBScript by double-clicking. Most errors are caused by mail relay disabled on the interface specified. Check your spelling!
- ❑ If the NIC is unplugged or the OS blue-screens, no alert will be sent. Use an SNMP mechanism to test for a live OS.

❑ Open RTA to confirm Filtering Service is receiving data. (Alternatively, use Reporter, Websense Explorer, or Websense\bin\testlogserver.)
- ❑ For any Risk Classes showing fewer than 100 visits, check:
  - ❑ The integration device or Network Agent configuration
  - ❑ Filtering Service is running
  - ❑ Filtering Service is listening on port 15868 or 15869
  - ❑ Network communication between devices is not blocked
- ❑ If Protocol Trends shows only HTTP, HTTPS and FTP or no traffic
  - ❑ On Network Agent > Local Settings > monitor NIC > panel four:
    - ❑ Enable "protocols" and "bytes transferred"
    - ❑ Specify the non-monitor NIC for sending messages
  - ❑ Check that Network Agent service is running
  - ❑ Check that the monitor NIC is enabled and receiving data
  - ❑ Check that the switch monitor port is properly configured and that the lights are blinking on your switch AND the local NIC
- ❑ If Protocol Trends shows no HTTP traffic but others are listed
  - ❑ On Network Agent > Local Settings > monitor NIC > panel four, disable "log HTTP requests" and "log and filter HTTP"
  - ❑ Check that the integration device is properly configured
  - ❑ Check for network interruptions or blocked ports
- ❑ Check the settings page:
  - ❑ The average response time should be between 2.5 and 35ms. If response times are above 35ms:
    - ❑ Inspect server CPU and RAM utilization (see below).
    - ❑ Consider reconfiguring PIX firewall to communicate via UDP instead of TCP, if applicable.
    - ❑ Consider upgrading the ICAP filter, if applicable (NetCache or NetScreen)
    - ❑ Consider upgrading the UFP filter, if applicable (CheckPoint).
- ❑ Confirm Filtering Service has been running the expected length of time. For example, if you believe it was running for several days but shows only four hours, it might have failed and been restarted via SNMP tools.

❑ Check filter settings
- ❑ Identify Websense version and integration type
  - ❑ In Websense Manager, expand Filtering Services, select the IP address of the current server
- ❑ Cleanup policies
  - ❑ Prune unused policies: right-click > "View Assigned Clients"

- ❑ Make sure the Global Policy is not assigned (it automatically applies when no other policy applies)
- ❑ Review the order of precedence that policies are enforced
  - ❑ A user-specific policy applies first, if one exists
  - ❑ An IP policy applies ahead of others
  - ❑ A "group" policy applies if no IP policy applies
  - ❑ Global Policy applies if no other is assigned

❑ Cleanup "Recategorized" and "Not Filtered" URLs (copy to a text editor)
- ❑ Remove www. from listed URLs
- ❑ Remove unnecessary modifiers: Anything to the left or right of the domain name Websense interprets as more restrictive. Most URLs should be entered in the form "Domain.com"
- ❑ Re-enter HTTPS sites as https:**//**<IP_address>:443
- ❑ Remove duplicates (sort in a text editor for easier viewing)
- ❑ To maintain "risk class" accuracy in the reporting tools when recategorizing, add the new category under the original category

❑ Prune unused "Yes Lists"[2]
- ❑ Check each policy to see if a Yes List is specified under "Category Set". If not, move the contents to "Custom URLs - Recategorized" or "Not Filtered" – or just delete it.

❑ Cleanup Keywords, keeping in mind:
- ❑ Keywords are string literal "sex" will match "Essex" and "sexual" but "=sex&" will not
- ❑ A keyword, when blocked, also recategorizes the blocked URL to the category specified. So: "=porn&" might better be in the category "adult material"
- ❑ Keyword blocking must be enabled (Edit > Category Set) to function

❑ Inspect Network Agent configuration
- ❑ In Websense Manager under Servers > Settings > Network Agent > Connections, make sure at least one filtering services and Network Agent is listed, and both are marked with a green icon.
  - ❑ Blanks and errors in either column can be edited from the config.xml file[3]
  - ❑ If either service shows "not connected", check that the services are running and there are no network blocks
- ❑ Check that two NICs are configured[4] under Servers > Settings > Network Agent > Global Settings. The IP address or how many IPs are listed doesn't matter as long as two NICs are listed.
  - ❑ If only one NIC is listed, check to make sure the second NIC is installed, enabled in the OS, plugged into the same switch[5], and receiving link up (lights are blinking). If any condition is false, correct it, restart the Network Agent service, and re-open the management console.
  - ❑ If the above requirements are already met, uninstall and reinstall Network Agent for it to recognize the second NIC.
- ❑ Select the NIC whose info panel shows it is Monitor "Yes". (With some rare exceptions[6], the other NIC is Monitor "No".) On the Monitor "Yes" NIC, confirm that the 'Activities & Communications' section should specify block messages are to be sent by the other NIC (not this NIC).
- ❑ Then click 'Monitoring' button to review the following:
  - ❑ 'Monitor List' will normally be "All".
  - ❑ 'Monitor List Exceptions' will be blank (recommended).

[2] A "Yes List" is **not** a white list of globally acceptable sites. A "Yes List" is meant as an alternative to a Category Set in a policy. The difference is that "Yes Lists" specify permitted URLs rather than categories.
[3] Stop the Filtering Service, edit config.xml in Notepad, save, start the Filtering Service.
[4] The assumption is that most switch ports cannot be configured to "monitor" at the same time as they communicate. Refer to your switch documentation.
[5] Both NICs servicing the Network Agent must be plugged into the same switch or the spoofed RST block packets will be dropped.
[6] Most switches can't support monitoring and transmitting from the same port. That's why two NICs are needed, one for monitoring, one for sending blocks and for management.

Websense Reporting Server Maintenance

- ❑ Check the current patch levels
  - ❑ Operating System, Browser, Web Server

- ❑ Check the Websense version installed
  - ❑ Websense Manager, navigation pane, expand Filtering Services, select IP
  - ❑ Websense Manager > Help > About

- ❑ Check the Event Viewer – Applications log (or var/adm/messages)
  - ❑ Websense Log Server errors
    - ❑ Confirm Log Server service runs under a valid account (default is Local)
    - ❑ Confirm that ODBC settings to the database match the authentication type configured on the SQL server
    - ❑ Confirm the username/password match
    - ❑ Apply Log Server patches if available from mywebsense.com
    - ❑ Check SQL server event viewer log for errors

- ❑ Use the Event Viewer to check the System log for W32Time errors or NTP errors. Accurate reporting requires time services to be functioning correctly. Keep written records of any time discrepancies (for accurate forensics), and correct errors as soon as possible.

- ❑ Confirm these services are running:
  - ❑ Websense Log Server
  - ❑ Websense Explorer Report Scheduler
  - ❑ Websense Reporter Scheduler
  - ❑ Websense Information Service for Explorer

- ❑ Set Recovery options on Websense services (Windows OS only):
  Right-click Websense services, select Properties > Recovery tab, set recovery options to restart—restart—run a program. Follow KB775 to create a VBScript, the program to run, which sends an email alert if the service cannot restart.
  Notes:
  - ❑ The SMTP server must allow mail relay, usually enabled on an internal NIC only.
  - ❑ A real email account to send from is not necessary if relay is enabled.
  - ❑ To speed identification make the “from” address the server name.
  - ❑ Send alerts to an email alias for the on-duty engineer, or separate names with a comma. Consider sending alerts to your pager or text-enabled cell phone.
  - ❑ Test the VBScript by double-clicking. Most errors are caused by mail relay disabled on the interface specified. Check your spelling!
  - ❑ If the NIC is unplugged or the OS blue-screens, no alert will be sent. Use an SNMP mechanism to test for a live OS.

- ❑ Check the Websense Reporter\LogServer\Cache directory. Normally, tmp files are written, processed, and deleted every minute. (Ignore the state file.)
  - ❑ If no files are being written within the last two minutes
    - ❑ Check that the Log Server service is running
    - ❑ Check that Filtering Service is running
    - ❑ Check that Logging is configured to the correct server IP
    - ❑ Use RTA to see if any data is coming in (see above)
  - ❑ If more than ten files remain after five minutes
    - ❑ Check that the Log Server service is running
    - ❑ Check that SQL server is alive (open SQL manager)
    - ❑ Check CPU and RAM utilization on the SQL server
      - ❑ Under SQL properties > Memory, increase available RAM
      - ❑ Add more RAM if utilization exceeds 80% average

- ❑ If no files are being deleted after five minutes
  - ❑ Check that the Log Server service is running
  - ❑ Make sure there is free space available for the LogServer cache
    - ❑ If needed, move the most recent tmp files to another disk. Once processing resumes, move them back.
  - ❑ Move the oldest tmp file in the LogServer cache directory to another directory
    - ❑ If files begin to process again, check our website for a LogServer patch, apply the patch, restart LogServer, copy the file back into the cache directory. If there is no patch, or it still chokes after patching and making free space (see above), open a ticket with Websense Tech Support using the online form and attach the corrupted file.
  - ❑ Make sure there is free space available to the SQL log file
  - ❑ Verify the ODBC connection to the database log file. If it fails
    - ❑ Check that SQL server is alive (open SQL manager)
    - ❑ Make sure the ODBC authentication type matches SQL
    - ❑ Check that MSSQLSERVER service is running on the SQL server, and is listening (telnet to 1433, or netsat -an)
  - ❑ Check that the database log file is listed in the SQL manager
    - ❑ Select All Tasks > Attach Database if it is not listed

- ❑ Configure DB Administration for archiving and/or purging data
  - ❑ Follow the customer's established policy for data retention
  - ❑ Consider how much free space is available (2x to 3x the active data file is needed for performing archives and purges)
  - ❑ Consider the amount of historical data needed to remain online for forensics and management reporting; move the rest to tape or SAN
  - ❑ Consider the amount of data needed in the 'active' database for analysis

- ❑ Enable LogServer > WebCatcher (to submit uncategorized data for analysis)

- ❑ Open Websense Explorer and click through some reports
  - ❑ Recommended: Show the customer how to drill down to a useful report, then save and/or email the URL.
  - ❑ If pages generate slowly:
    - ❑ Check CPU and RAM utilization (add RAM if >80%)
    - ❑ Check for runaway or excess processes
    - ❑ Check for runaway or excess processes
    - ❑ In the ODBC connection, use the IP address of the SQL server instead of the server name
    - ❑ Follow the steps for SQL Server (below)

- ❑ Open Websense Reporter and generate some reports
  - ❑ Recommended: Setup automated spyware reports
  - ❑ If reports generate slowly:
    - ❑ Check CPU and RAM utilization (add RAM if >80%)
    - ❑ Check for runaway or excess processes
    - ❑ If SQL runs on a separate server, copy ntwdblib.dll from SQL Server into the Winnt\System32 directory on the Reporter machine
    - ❑ In the ODBC connection, use the IP address of the SQL server instead of the server name
    - ❑ Follow the steps for SQL Server (below)

Websense SQL Server Maintenance

- ❑ Check that the OS is patched to current levels
- ❑ Check the SQL patch level against MS recommendations
- ❑ Check CPU and RAM utilization
  - ❑ Add more RAM if utilization exceeds 80%
- ❑ Confirm these services are running:
  - ❑ MSSQLSERVER
  - ❑ SQLAGENTSERVICE
- ❑ Inspect the running processes
  - ❑ End non-essential process
  - ❑ If possible, reboot to clear hung processes and unused sockets
- ❑ Setup a maintenance plan to reindex the active Websense database
  - ❑ In SQL Enterprise Manager, All Tasks > Maintenance
- ❑ Check free space for the data drives (Note: It is normal for the data file size to grow in spurts, as SQL grows the table space in 10% increments (default).
  - ❑ The OS and program files should be on one spindle, data files on a separate spindle (or array).
  - ❑ Websense needs 2x to 3x the amount of active data to perform archives or purges.
  - ❑ Database files:
    - ❑ The active log for Websense URL/protocol data is wslogdb63.mdf
    - ❑ Archives include date/time: wslogdb63_20050517124321.mdf

Disaster Recovery Checklist

Backup and Restoration of a Websense Environment

Introduction

Disaster Recovery (DR) depends on careful planning, especially for those subtle variations that creep into every deployment. Use these checklists as a guide to prepare your own DR Plan customized to your environment.

Linux/Solaris Note:

The paths listed below conform to a default installation on Windows. The default location on Linux is opt/Websense/bin. Not all components can be installed on Linux or Solaris, so be sure to stay informed about your particular deployment.

Integration Note:

Websense supports over 65 different integration partners, each with specific requirements that vary depending on the device, software, and Websense version. Keep the Websense Installation Guide for your integration device and version on hand specific to your Websense version. Our documentation site only maintains the latest version online.

Upgrades versus Fresh Install:

A fresh install of Websense places some configuration files in a different location than an upgrade, because upgrading preserves the older file locations. When recovering using a fresh install, some configuration files may need to be copied to the new location.

Preparation Checklist

- ❑ Keep these information items handy
  - ❑ IP address of your integration device (firewall, cache, etc.)
  - ❑ Hostnames and IP addresses of all Websense servers and the network port used for the integration and reporting tools if not the default ports (also stored in the ini or xml files).
  - ❑ Physical connections of cables and ports on the switch used for the management NIC versus monitoring NIC
  - ❑ Your SQL account and password for the Log Database
  - ❑ Your Websense subscription key
  - ❑ Password for the Websense management console
  - ❑ Password for RTA and user/password for Reporting Tools
  - ❑ Proxy credentials (if needed) for the nightly database download
  - ❑ Username and password used to configure logon properties for Websense services, if your environment requires privileges higher than ‘local system’.
  - ❑ Passphrase and custom ports used for Remote Filtering Server
  - ❑ Configuration of switch, router, and firewall in support of Websense communication ports and filter integration.
  - ❑ Websense Installation Guide for your integration. Each integration partner has specific software components and/or configuration elements, which might change with each version. Keep a copy on hand specific to your Websense version.
  - ❑ Websense Deployment Checklist for your installed version
  - ❑ Websense Maintenance Checklist for your installed version (for troubleshooting)

Backup Checklist

- ❑ Back up your switch configuration. If using Websense Remote Filtering, back up your router and firewall settings.
  Note: Restoring from tape backups can be time-consuming Consider backing up to SAN or DVD. A complete backup (configuration and data files, plus the application installer) is about 1-1.5 GB.
  Note: To prevent accidental loss of the configuration data, retain older backups until you can verify that the most recent backups are valid. If the backup files are corrupted, you will have to re-create your policies and server configuration manually.
  Note: The actual directory depends on the version installed. It also depends on whether the later version was installed fresh or was done as an upgrade to an earlier version. Use the paths below as a guide.

- ❑ Shut down the Websense services - stop them in this order (assuming they are all present) starting with DC Agent and finishing with Policy Server. After the files are backed up, restart them in reverse order, starting with Policy Server and finishing with DC Agent:
  - ❑ DC Agent
  - ❑ XID Logon Agent
  - ❑ E-Directory Agent
  - ❑ Radius Agent
  - ❑ Network Agent
  - ❑ Filtering Service
  - ❑ User Service
  - ❑ Policy Server

- ❑ Back up the following files, if present, on the Websense server.
  - ❑ C:\Program Files\Websense Enterprise\ ws.cfg (v4.4)
  - ❑ C:\Program Files\Websense\EIM\bin\ config.xml (v5.0-5.2)
  - ❑ C:\Program Files\Websense\bin\ config.xml (v5.5-6.3)
    Note: The config.xml file changes whenever changes are made through the Websense management console, whenever Websense components are moved, whenever IP addresses change, and sometimes when hardware changes are made such as removing or disabling a NIC. For this reason, make sure you maintain current backups.

  Note: All directories below assume v5.5-6.3.
  - ❑ C:\Program Files\Websense\bin\ Websense.ini
  - ❑ C:\Program Files\Websense \bin\ eimserver.ini
  - ❑ C:\Program Files\Websense\EIM\bin\ dc_config.txt

  Note: New domain controllers are added automatically to this file.
  - ❑ C:\Program Files\Websense\bin\ ignore.txt
  - ❑ C:\Program Files\Websense\bin\ transid.ini
  - ❑ C:\Program Files\Websense\bin\ Websense (with no extension, the master URL database)

  Note: The master database must be under 14 days old to be re-usable
  - ❑ C:\Program Files\Websense\webroot\ Websense.ini
  - ❑ C:\Program Files\Websense\BlockPages\en\Custom*.* (your custom block pages)
  - ❑ C:\Program Files\Websense\Manager\wsmanager.ini
  - ❑ C:\temp\WebSecuritySuite63setup*.* (Or appropriate version this is the WS install package, unpacked)

- ❑ Stop the Log Server service, information service for explorer, and Real Time Analyzer in order to backup these files, there is no order dependence on these services.
  - ❑ On the Reporter / Log Server backup:
    - ❑ C:\Program Files\Websense\bin\LogServer.ini
    - ❑ C:\Program Files\Websense\bin\websense.ini
    - ❑ C:\Program Files\Websense\reporter\wsreporter.ini
    - ❑ C:\temp\WebSecuritySuite6.3*.* (Or appropriate version this is the Reporter/Explorer install package, unpacked)

- ❑ SQL Server must either be stopped, or the databases taken off-line in order to copy these files.
  - ❑ On the SQL database server, back up:
    - ❑ C:\Program Files\Microsoft SQL Server\MSSQL\data\wslogdb63.mdf (WS log data) These Files may also path into the Websense directory depending upon the install
    - ❑ C:\Program Files\Microsoft SQL Server\MSSQL\data\wslogdb63_log.ldf
    - ❑ C:\Program Files\Microsoft SQL Server\MSSQL\data\wslogdb63_1.mdf (grab ALL wslogdb63_*.mdf files)
    - ❑ C:\Program Files\Microsoft SQL Server\MSSQL\data\wslogdb63_1_log.ldf (grab ALL wslogdb63_*_log.ldf files)
    - ❑ C:\Program Files\Microsoft SQL Server\MSSQL\data\wscamil_log.ldf

Restoration Checklist

- ❑ To restore the Websense Web Security server environment, follow this order:
  - ❑ Restore port mirroring on the switch where Websense Network Agent is used.
  - ❑ Restore the router and firewall configuration to support Websense Remote Filtering, if it is used.
  - ❑ Restore the integration device and settings.
  - ❑ Install OS, IIS, SQL and then patch to latest revision.
  - ❑ Configure the server to use the SAME static IP address, the same hostname, and the same domain membership. If it is necessary to change the IP address, you may have to manually edit the restored Websense configuration files. If the hostname or IP changes, be sure to update your DNS.
  - ❑ Restore the Websense mdf and ldf file(s) to the SQL Server (and 'attach' the database)
  - ❑ Install the SAME Websense version as backed up
    Note: If your backup master database is less than 14 days old, select “do not download the database” during installation.
  - ❑ Check MyWebsense.com for patches and hotfixes
  - ❑ Configure the ‘log on’ properties of Websense services, if needed.
  - ❑ After installing all the software, stop all Websense services, Policy Server LAST
    Note: In Windows use the Services applet. In Linux/Solaris use the command */opt/Websense/WebsenseAdmin stop*.
  - ❑ Backup the *newly installed* files (same list above) for safekeeping
  - ❑ Restore the *production* backup files to replace the newly installed files
  - ❑ Start Websense services, Policy Server FIRST
    Note: In Windows use the Services dialog box. In Linux/Solaris use the command */opt/Websense/WebsenseAdmin start*.
    Note: Filtering resumes when the master database has loaded successfully (5 to 30 minutes after starting Filtering Service).
  - ❑ Optional: To download the latest database updates and to resync the key (and features attached to the key), start a database download (Websense management console > Server > Database Downloads, “download all”).
    Note: You must first wait for the database to load successfully (5 to 30 minutes); otherwise it will start a complete download (30-60 minutes).
    Note: The resync / update process may take 10 to 20 minutes, versus 30-60 if a complete database download is required.
  - ❑ Install any integration-specific software plug-ins according to the Websense Installation Guide for your specific integration device. Most software plug-ins are installed by running Websense setup and selecting “Custom” install.
  - ❑ If restoring a Remote Filtering Server (v6.1+), run the Websense installer, select “Custom” > Remote Filtering Server.
  - ❑ Consult the Websense Maintenance Checklist to identify and resolve problems, and check our online Knowledgebase for up to date information

- ❑ Check for errors:
  - ❑ Windows Event Viewer > Applications
  - ❑ Windows Services (all 'automatic' Websense services started)
  - ❑ <install path>\websense\bin\websense.log or /opt/Websense/bin/Websense.log

- ❑ Real-Time Analyzer > Protocol trends (see more than HTTP, HTTPS, FTP)
- ❑ Websense Reporter launches ok and contains data (v5.x+ only)
- ❑ Websense Explorer launches ok and contains data

Troubleshooting

- ❑ **Error: Can't Locate Service or Service Doesn't Exist**
  - ❑ Websense software components are identified within the config.xml and INI files by a GUID. These GUIDs must match. To resolve, stop the affected service AND Filtering Service, edit the config.xml and any related ini, restart both services. To edit, use Notepad or any text editor that does not add formatting codes.

- ❑ **Database Not Found**
  - ❑ Check the SQL server to make sure the path is correct

Additional Help and Support

- ❑ Websense Technical Support, online 24/7 and by phone M-F 5am-5pm: 858-458-2940
- ❑ Websense Knowledgebase online
- ❑ MyWebsense.com – access to patches, online tech support, software downloads

Appendix

Top 22 Technical Support Solutions

The Websense Knowledge Base Solutions listed below can be viewed in detail by entering the Reference Number on the following site. The order of the list is sorted by the most frequently asked question when this document was created.

http://ww2.websense.com/global/en/SupportAndKB/SearchKB/

Websense Knowledge Base Reference Number and Description		
❑	4404	Minimum system requirements for Websense web filtering and CPM
❑	493	How do I troubleshoot transparent user identification when I am using DC Agent
❑	242	How to configure PIX to fail open
❑	604	What are the Websense default ports
❑	678	Using TestLogserver or FakeLogServer
❑	353	How do I configure Cisco PIX Firewall to integrate with Websense
❑	473	How do I start, stop, and/or restart Websense services
❑	352	How do I identify the IP address for Websense Filtering Service
❑	342	Why would I want to use a Domain Name System (DNS) with my Cisco PIX integration
❑	6805	Installation of Websense software on VMWare is supported
❑	574	How do I detach and attach my database in MSDE
❑	805	How do I troubleshoot empty web filtering reports
❑	225	How do I allow sites to go unfiltered through a PIX Firewall
❑	326	Password Override and Continue timeouts not being enforced
❑	156	Can Websense function in a Terminal Server - Citrix Server - Thin Client environment
❑	8	What is Cisco PIX URL caching and why would I use it
❑	336	What url-server host command options do I need for PIX
❑	41	Why won't Cisco PIX allow HTTP access when I stop Websense Enterprise
❑	3904	What are the component and file names for different versions of Websense products
❑	39	What statistics can I monitor for my integrated Cisco PIX Firewall
❑	6431	Websense Manager will not load after Microsoft Security Update 921883 is applied
❑	7	What versions of Cisco PIX Firewall can be integrated with Websense Enterprise

Websense 6.3 Product Documentation

For additional product specific information, visit our website using the link below to view our online documentation. The Websense online documentation is updated regularly. The Websense 6.3 Product Documentation reference list below may not correctly reflect what is currently online.

http://www.websense.com/global/en/SupportAndKB/ProductDocumentation/

Getting Started
Deployment Guide for Websense Enterprise and Web Security Suite
10 Steps to an Easy Websense Installation
Stand-Alone Edition Installation Quick Start
Websense Enterprise and Web Security Suite Installation Checklist
Websense Enterprise Evaluator's Guide and Quick Start Guide
Getting Started with Delegated Administration
Quick Start for Network Agent
Reporting Installation Checklist
CPM Installation Checklist
CPM Evaluation Guide
CPM Quick Start Guide
CPM Risk Evaluation Worksheet
CPM Policy Configuration

Administrator and User Guides for Websense Enterprise and Web Security Suite
Administrator’s Guide for Websense Enterprise and Web Security Suite, v6.3
Reporting Administrator’s Guide, v6.3
Explorer and Real-Time Analyzer User Guide, v6.3
Reporter User Guide, v6.3
Explorer for Unix Administrator’s Guide, v6.3

Websense Client Policy Manager
Websense v6.3, CPM Installation Guide
Websense v6.3, CPM Administrator's Guide
Websense v6.3, CPM Reporter Administrator's Guide
Websense v6.3, CPM Explorer Administrator's Guide
Websense v6.3, CPM Release Notes
Websense v6.3, CPM 10-Step Easy Install Guide
Websense v6.3, CPM Master Index

Installation Documents for Websense Enterprise and Web Security Suite v6.3
Deployment Guide for Websense Enterprise and Web Security Suite v6.3
Installation Checklist for Websense Enterprise and Web Security Suite v6.3
Installation Guide For Stand-Alone Edition of Websense Enterprise and Web Security Suite v6.3
Installation Checklist for Reporting v6.3
Reporting Installation Guide v6.3
Explorer for Unix Administrator’s Guide v6.3
Getting Started with Delegated Administration
Quick Start for Network Agent

Integration-specific Installation Guides
3Com SuperStack Firewall
3Com Webcache
Blue Coat Systems (CacheFlow)
Check Point FireWall-1
Cisco Catalyst 6000 Switches with PIX Firewall
Cisco PIX Firewall
Cisco Routers
Cisco Content Engine

Citrix Servers
Configuring Websense to Work with Citrix and a Second Integration
CyberGuard Firewall

Embedded installations

- Websense Enterprise v6.3, v6.1, or v5.2 Embedded on Blue Coat: Reporting Installation
- Release notes for Websense Enterprise v5.5.2 Embedded on Cisco Content Engine ACNS 5.4
- Websense Enterprise v5.2 Embedded on Cisco Content Engine ACNS 5.3
- Release notes for Websense Enterprise v5.2 Embedded on Cisco Content Engine
- Websense Enterprise v5.2 Embedded on Cisco Content Engine ACNS 5.2
- Installation Guide for Websense Enterprise v5.0.1 Embedded on Cisco Content Engine
- Installation Guide for Websense Enterprise v4.4.1 Embedded on Cisco Content Engine
- Websense Enterprise v6.3, v6.1, or v5.2 Embedded on NetCache: Reporting Installation

iMimic DataReactor
Inktomi Traffic Server
Juniper Networks NetScreen
Microsoft ISA Server
Microsoft Proxy Server
Network Appliance NetCache
Nortel GGSN
ServGate
SonicWALL Firewall
Squid Web Proxy Server
Stratacache
Sun Java™ System Web Proxy Server

Websense Enterprise v6.3 Release Notes
Websense Enterprise v6.3
Websense Enterprise v6.3, Reporting

Technical White Papers for Websense Enterprise and Web Security Suite
Internationalizing Explorer for Unix
Transferring Configuration Settings to a v6.3 System Without Upgrading
Transparent Identification of Users in Websense Enterprise