Websense®
Web Security Gateway Anywhere

Getting Started Guide

v7.5

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

Published September 8, 2010
Printed in the United States of America and China.

Trademarks

Contents

1 Introducing Web Security Gateway Anywhere

Overview

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

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

You can decide which method to use for which users. For example, you may use our robust on-premises Web filtering for your corporate office (business) or main campus (education), and filter your regional offices or satellite locations through our hybrid service.

Unlike alternate approaches, hybrid filtering gives you the flexibility to choose the platform or mix of platforms that best meets your operational requirements without incurring the cost of managing multiple systems

In addition, Web Security Gateway Anywhere protects you from data loss over the Web, providing security for outbound content as well. You identify sensitive data and define whether you want to audit or block attempts to post it to HTTP, HTTPS, FTP, or FTP-over-HTTP channels.

And finally, Web Security Gateway Anywhere provides flexible solutions for users who travel or work from a location outside of your network, such as a home office. You can install a Web filtering client on remote users' machines, or you can monitor remote activity using our hybrid Web filtering service.

Web Security Gateway Anywhere includes Websense Web Security and Websense Content Gateway as well as hybrid Web and DLP features.

Because it includes the real-time analytics of the Websense Content Gateway, you can can protect your users from Web 2.0 threats no matter where they reside.

Web Security Gateway Anywhere is available on the V-Series appliance or as software. The appliance configuration reduces your network footprint and improves latency. Appliance setup is described in Chapter 2*: Setting Up the V-Series Appliance*. Software installation is described in Chapter 3*: Installing Software*.

For even more robust enterprise security, consider adding Websense Email Security or data loss prevention over additional channels, such as email, endpoint applications, instant messaging, and printers.

Websense® TRITON™ Unified Security Center

The interface that you use to manage Websense Web Security Gateway Anywhere is called the **TRITON Unified Security Center**. TRITON has modules for Web, data, and—coming soon—email security. TRITON is a Web-based user interface that enables you to perform basic setup, system maintenance, policy creation, reporting, and incident management for both modules in the same location.

> **Note**
>
> TRITON Unified Security Center supports Internet Explorer 7 and 8 and Firefox 3.0.x - 3.5.x. If you have another browser version, unexpected behavior may result.

To access the TRITON security center, log onto either TRITON - Web Security or TRITON - Data Security as described in Chapters 4 and 6.

If you log onto TRITON - Web Security and configure linking before logging onto TRITON - Data Security—as described in this document—the password for TRITON - Web Security is automatically applied to the data security module. This is the case whether you configure the TRITON - Web Security password during installation or with the appliance first-boot script.

The TRITON module tray

The TRITON module tray indicates which module is active.

When you log onto TRITON - Web Security, the Web Security module is active and the Web Security button in the module tray is yellow. To enable the Data Security button, you must install Data Security software, configure linking between TRITON - Web Security and TRITON - Data Security, and create identical administrator accounts in both the Web and data modules. (See *Configuring linking between Web and data security*, page 93 for instructions on configuring this option.)

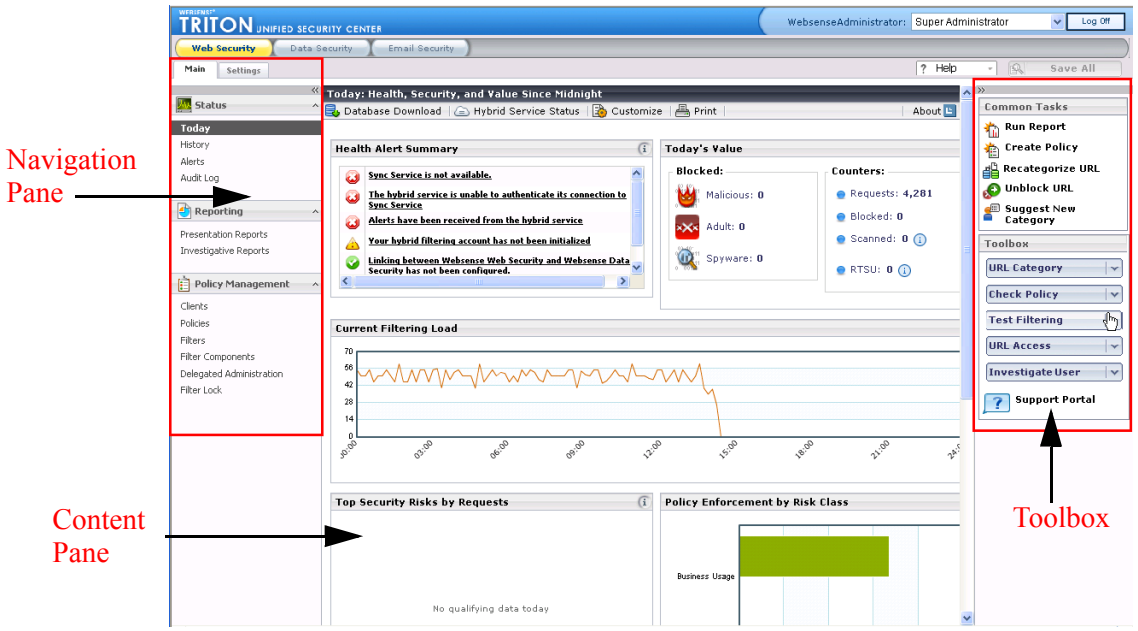
After you have configured linking, you can click Data Security in the module tray to open TRITON - Data Security. When in TRITON - Data Security, the Data Security button is yellow, and the Web Security button is grey.

> **Note**
> Once you have opened both management consoles in the TRITON security center, use the operating system task bar to switch between the two.

Until you configure linking, clicking the Data Security button opens a Web page describing the benefits of Websense data security solutions.The Email Security button displays a similar Web page.

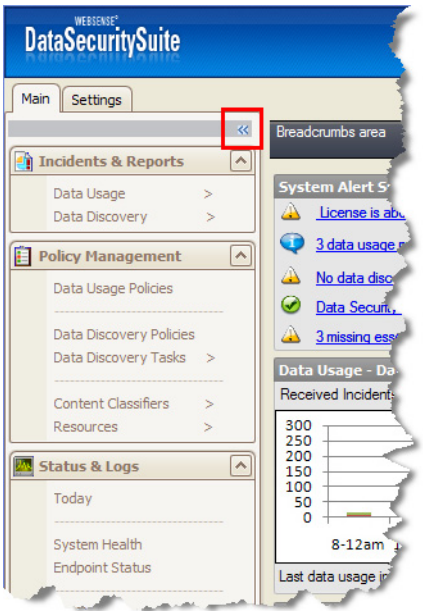
Collapsible navigation and content panes

The left pane of the TRITON Unified Security Center is known as the **navigation** pane. The navigation pane is organized with tabs and buttons, some of which offer a menu of options. The center pane (Web Security) or right pane (Data Security) is known as the **content** pane. The content in this pane varies according to the selection in the navigation pane. In the Web Security module, the far right pane offers a **toolbox** and links to common tasks.



The navigation and toolbax panes are collapsible to enable larger working space and a wider display area for all TRITON pages.

To collapse a pane, click the arrows in the upper corner of the pane. To expand it, click the arrows again. You can do this on any page in the TRITON security center.



Hybrid Web filtering

Web Security Gateway Anywhere supports on-premises appliance as well as hybrid on-premises/Security-as-a-Service (SaaS) platforms, while managing the entire environment from a single policy and reporting infrastructure. Unlike alternative approaches, you have the flexibility to choose the platform or mix of platforms that best meets your operational requirements without incurring the cost of managing multiple systems.

For enterprises with multiple branch offices or remote locations, there are several ways to provide Web filtering for the branch office. You can deploy a V-Series appliance with Websense Web Security Gateway at the branch location; have traffic back-hauled to the headquarters; or have the branch office be filtered by the hybrid service in the cloud. With Web Security Gateway Anywhere, you can define clients and create policies for on-premises and hybrid filtering in the same interface.

Here are some of your options:

- On-premises Web Security Gateway for head office users
- On-premises Web Security Gateway for the larger branch office
- Traffic from branch office 1 back-hauled to Web Security Gateway at the head office
- Hybrid filtering for branch office 2 and roaming users
- Remote filtering is still available for roaming users with corporate laptops

Sample hybrid deployment

Following is a sample scenario where you might adopt hybrid filtering.

You have 2 large headquarter offices—one in the United States and another in Europe. Between the 2 offices, there are around 1800 users, and as a result, there are sufficient users to justify deployment of the Websense on-premises product in each office. You also have a number of other satellite sales offices, with 10-30 people. You do not want the additional expense of having to source and support separate Websense enterprise installations in these offices; it is more cost-effective to adopt hybrid filtering. With hybrid filtering, you configure the policy that you want to apply to these remote offices, and push the policy to the hybrid infrastructure..

Once the policy information (and optionally user and group information from a directory service) is pushed into the hybrid service, it is validated and checked for consistency, and then pushed out to all data centers worldwide. The hybrid environment provides a customer-specific PAC file URL and client browsers should be configured to use this in their connection settings. Client requests coming from the branch offices (or off-site users) are automatically routed to the closest hybrid datacenter for URL filtering using a geographical IP lookup.

Logs from the hybrid service are downloaded by the on-premises software, and integrated into the main on-premises database for you.This enables your to monitor and report on your entire user base.

The branch office can be configured as a filtered location for the hybrid service. It is defined and recognized by its externally facing IP addresses. Because the branch office is a trusted location, it is possible for users who are logged onto a directory service to supply identification to the hybrid environment. This allows user, group and domain-based policies to be applied.

Hybrid Sync Service

Communication between the on-premises and hybrid side is handled by the Websense Sync Service, which resides on-premises, and the Websense Sync Server, which resides in the cloud. All communications are initiated by the on-premises side. The hybrid side never tries to initiate communication or push information to the on-premises side. This is to protect customer information and to comply with typical customer firewall configuration.

Sync Service traffic is encrypted using HTTPS. Account information, policies, and user information are pushed from the on-premises side to the hybrid side as part of the syncrhonization process.

- Account information includes the administrator contact information as well as user and group details from any configured directory services.
- Policy information includes proxy and filtering information.
- Log information is pulled from the hybrid side into the local log database for monitoring, reporting and analysis.

Websnese Directory Agent is used to extract user and group information from configured directories so that it may be exported to the hybrid environment by the Sync Service.

With directory synchronization in place, it becomes possible to provide transparent identification for users who are logged onto a directory service. The browser can provide their identity (as part of the HTTP header information) when making a request to the hybrid (cloud-based) proxy.

Filtered locations

Filtered locations are used to define a location (like a branch office, remote site, or satellite campus) filtered by the hybrid portion of the Websense software.

The filtered location should be assigned a time zone—this is used in applying policies, to ensure that the correct filters are applied at the appropriate time. Each filtered location can have a different time zone setting.

Filtered locations may be defined using an IP address, an IP address range, or a subnet. This must relate to the egress identity of the filtered location—for example, the external IP address of the branch office firewall. If a range of IP addresses is used, it must *not* include the address of the Websense Content Gateway.

Users who connect from a filtered location are recognized by the IP address. If they have provided user credentials, the browser can provide these to the hybrid service as part of the HTTP headers. This allows users to be identified for filtering purposes without requiring them to enter explicit authentication details. Their identity can be trusted because they are connecting from a location that should have corporate security policies in place.

Unfiltered destinations

Unfiltered Destinations may be used for sites to which users should be granted unfiltered access. Users can access these sites directly, without sending the request to the hybrid service.

Unfiltered Destinations may be defined as an IP address, domain (or FQDN) or subnet.

Destinations listed here are added to the Proxy Auto-Configuration (PAC) file that defines how filtered users' browsers connect to the hybrid service.

By default, the PAC file excludes all non-routable and multicast IP address ranges from filtering. Therefore private IP address ranges defined in RFC 1918 or RFC 3330 do not need to be entered here.

Authenticating off-site users

Off-site users are those who connect from an untrusted location—in other words, not a filtered location. The location may be a home network, hotel, or Internet café. The

identification passed by the browser cannot be trusted and the user must therefore authenticate with the proxy.

Remote filtering

Remote filtering offers an alternative to hybrid filtering if you prefer to manage all filtering through your on-premises deployment.

Remote filtering is deployed by installing client software onto users' laptops and providing a remote filtering server in the corporate DMZ.

Web data loss prevention (DLP)

Web mail, Instant Messaging and personal networking sites are some of the most common means by which corporate data is leaked. The Web DLP functionality included in Web Security Gateway Anywhere is able to detect and block such leaks—even if the connection is encrypted. The Websense PreciseID technology provides accurate fingerprinting of content to support this process.

PreciseID™ fingerprinting

Originally developed to meet the exacting security requirements of the Israeli military, the patented PreciseID technology at the heart of Websense Data Security Suite has now been extended to provide Web DLP within Websense Web Security Gateway Anywhere.

PreciseID takes a data-centric approach to protecting essential information. It provides accurate identification and classification of content in more than 370 different file types and format—from source code binaries to CAD drawings to Verilog code, and beyond—even if that content is cut and pasted from one format to another. PreciseID technology uses multiple detection methods to help organizations discover organizational compliance risk and automatically enforce content use policies, including fingerprinting technology, rules, dictionaries, exact and partial matching, statistical analysis, and natural language processing. Natural language processing enhances the granularity and accuracy of the PreciseID detection and classification capabilities, providing unparalleled protection for a broad range of content.

PreciseID enables Web Security Gateway Anywhere to accurately secure confidential data, efficiently preventing information loss over the Web.

What is Web DLP?

Web DLP provides all the DLP capabilities of the full Websense Data Security Suite but for the Web channel only. It includes all of the detection capabilities, all of the reporting capabilities, all of the incident management and workflow capabilities of the full Websense Data Security solution the Web, but only for HTTP, encrypted Web (HTTPS), and FTP.

All the DLP analysis capabilities are built into Web Security Gateway Anywhere and performed on the Content Gateway machine, most commonly the V-Series appliance. The only additional requirement to deploy Web DLP is a Data Security Management Server.

Web DLP cannot be purchased as a separate module; it is available as part of the Websense Web Security Gateway Anywhere package only.

If you decide to upgrade the solution to include other DLP modules (such as Data Discover or Data Endpoint), you can use the same management server for the entire solution.

Enterprise-class Web DLP

To help you prevent data loss and achieve compliance, Websense has integrated enterprise-class DLP for Web traffic. This not a simple keyword and regular expression utility, but a full implementation of our market leading DLP solution for Web traffic (HTTP, HTTPS, and FTP) that's natively integrated with the Web Security Gateway.

It includes:

- Predefined data patterns to accurately detect hundreds of the most common compliance data types like credit card numbers, tax IDs, financial data, and healthcare data worldwide.
- Comprehensive policy wizards and reporting
- Integration of the patented PreciseID fingerprinting so that customers create their own custom data patterns for documents and database records.

What all of this does is dramatically simplify DLP deployment when compared to alternative approaches.

- Single-box solution - Native integration with the Web Security Gateway eliminates the need to deploy multiple Web and DLP boxes at each site. This reduces up front licensing costs, hardware costs, hardware deployment costs, and the cost of integrating technology from multiple vendors.
- Predefined data patterns for hundreds of common compliance data types ensure automated detection accuracy.
- Policy wizards translate vague or complex regulatory requirements into detailed, well-documented DLP best-practice policies automatically. You can simply select the industry, region, and regulation and a best-practice policy is automatically applied.
- Web security and DLP capabilities are managed centrally from our TRITON Unified Security Center interface.

Do this first!

Before installing and configuring Websense Web Security Gateway Anywhere, you must have Microsoft SQL Server installed and running. (This applies to both appliance and software deployments.)

Once you have an installation of SQL Server, make note of the following:

- The IP address or host name of the SQL Server machine
- A user name and password of a SQL Server administrator

You'll be prompted for this information when you install Websense Web Security components.

Resources

The following additional resources are available to help you tailor your Web security solution and to answer questions that may arise as you work with Websense software.

Documentation

Documentation is available in the Websense knowledge base (http://kb.websense.com). It is also available on the **Support by Product** page of Websense.com.

In addition, help systems are included with the product. To access help, click the Help icon on the TRITON toolbar. Help for the active module opens. Click **Help > Explain This Page** to access context-sensitive help—that is, help on the current page; or click **Help > Contents** to access the entire help system.

Following are the documentation modules that pertain to Websense Web Security Gateway Anywhere.

Websense Web Security

- Websense Web Security Gateway Anywhere Getting Started Guide - this guide
- Websense Web Security Installation Guide - in knowledge base
- Websense Web Security Deployment Guide - in knowledge base
- TRITON - Web Security Help - in product
- Log Server Help - in product
- New User's Quick Start Tutorial - in product
- Upgrading User's Quick Start Tutorial - in product

Websense Data Security

- TRITON - Data Security Help - in product

- Websense Data Security Deployment and Installation Guide - in knowledge base

Websense Content Gateway

- Websense Content Gateway Installation Guide - in knowledge base
- Websense Content Gateway Administrator Guide - in knowledge base
- Content Gateway Manager Help - in product

Websense V-Series Appliances

- Websense Appliance Manager Help - in product
- Websense V-Series Getting Started Guide - in knowledge base

Knowledge Base

For Websense Web Security knowledge base articles and FAQs, go to http://kb.websense.com.

Technical Support

Technical information about Websense software and services is available 24 hours a day at:

www.websense.com/support/

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

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

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

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

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

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

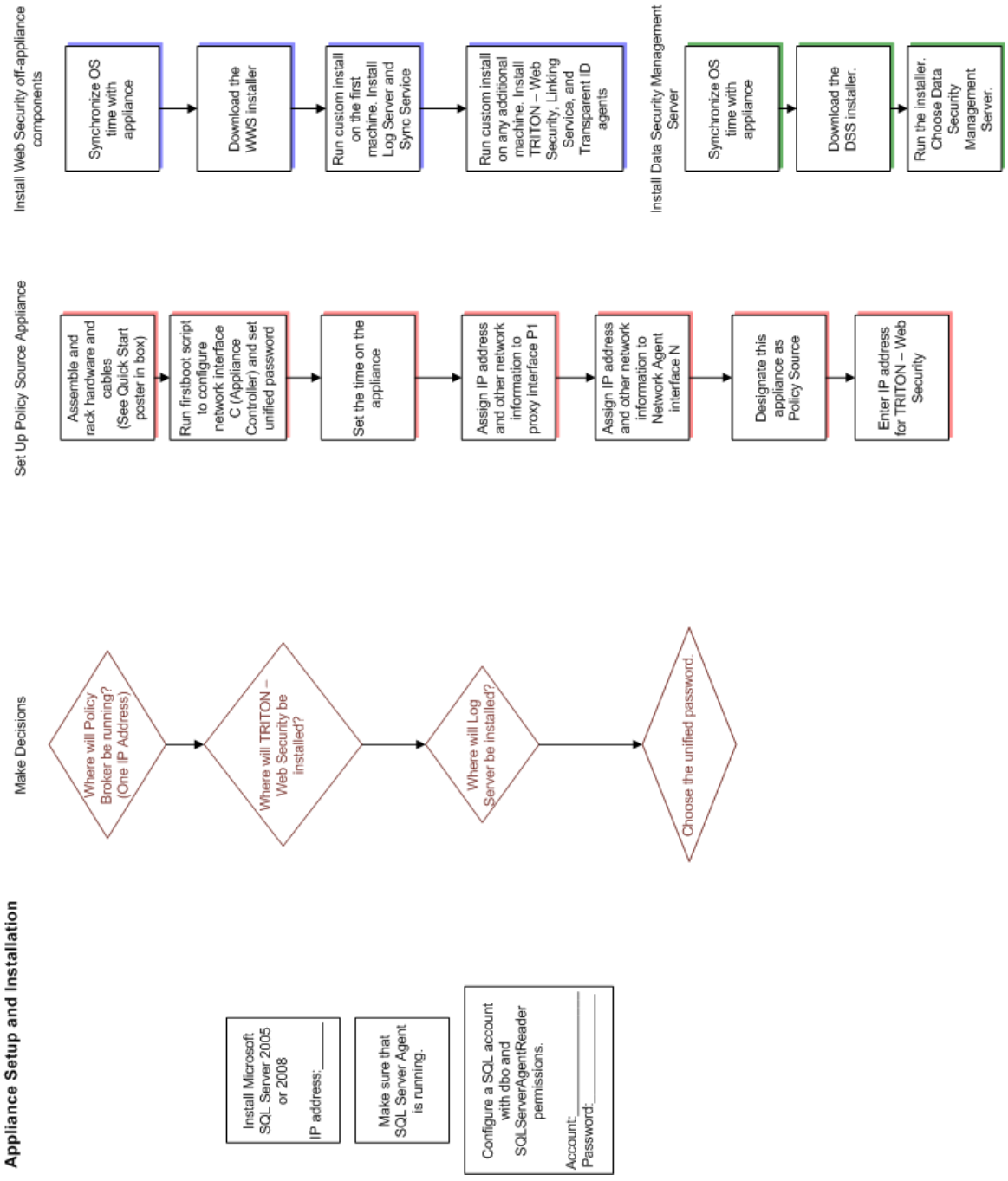
For telephone requests, please have ready:

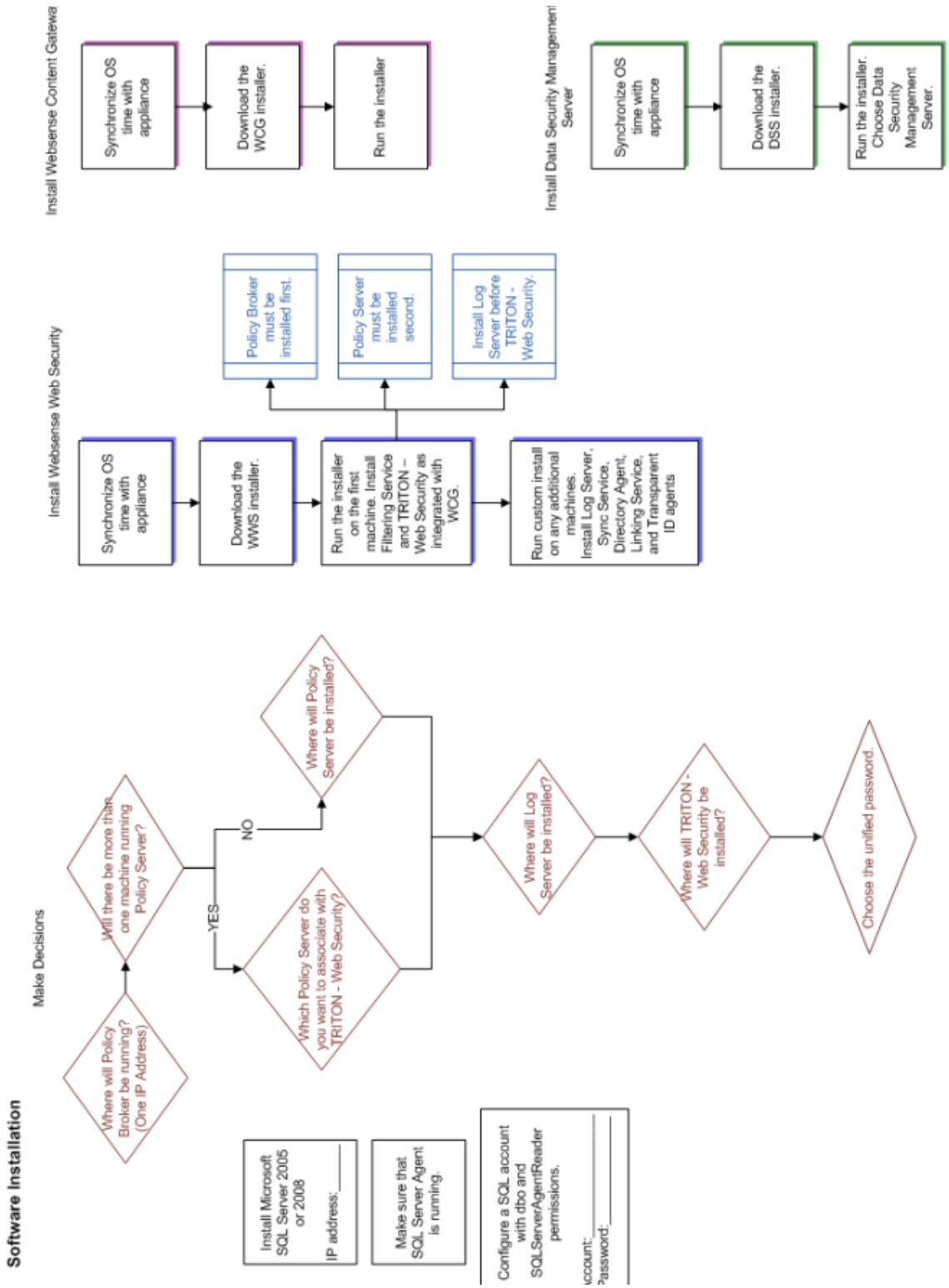
- Websense subscription key
- Access to TRITON Unified Security Center.
- Access to the machine running reporting tools and the database server (Microsoft SQL Server or MSDE)
- Familiarity with your network's architecture, or access to a specialist

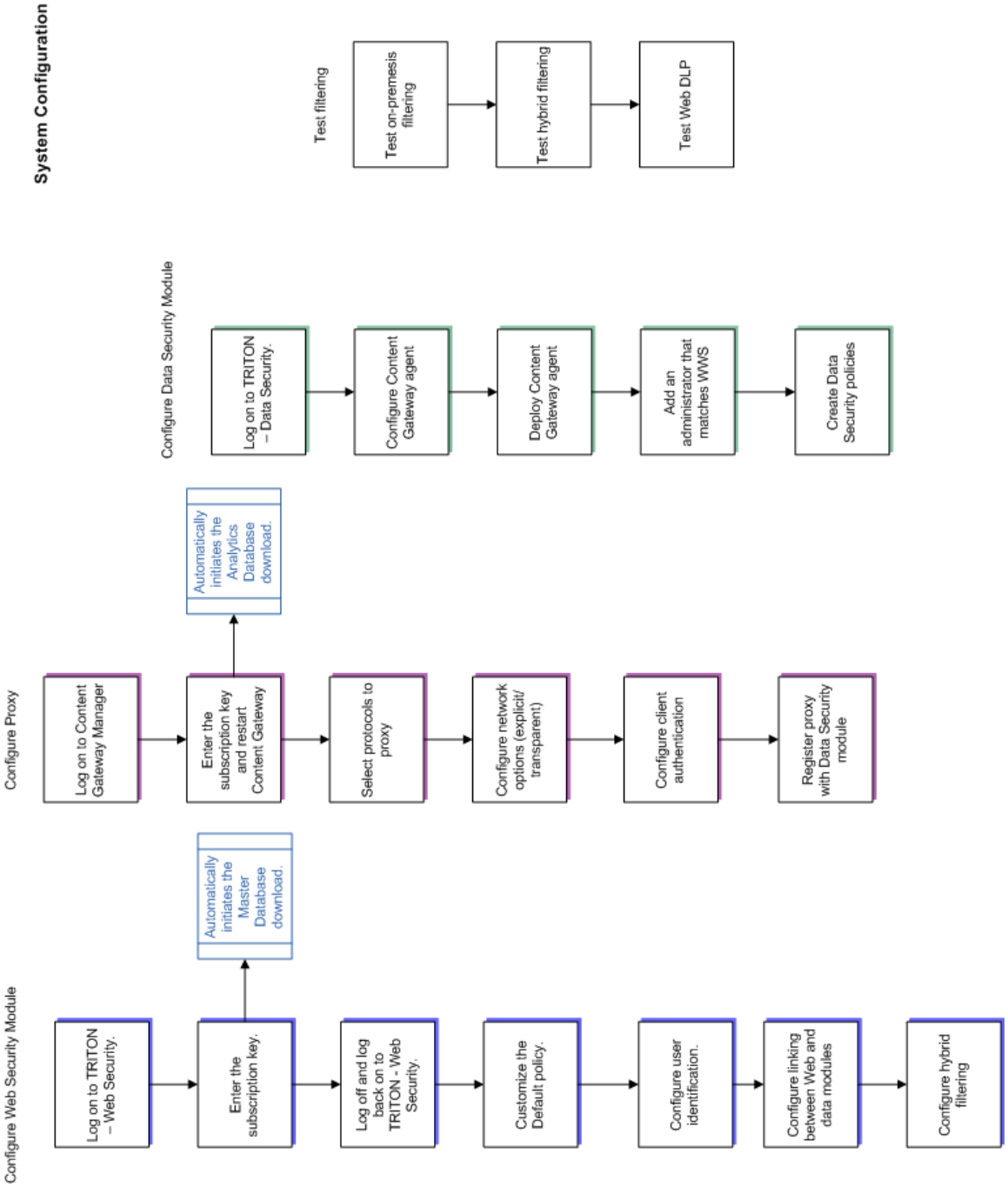
Setup diagrams

The following diagrams offer a graphical, at-a-glance presentation of the steps involved in establishing your Web Security Gateway Anywhere installation. Each step in the diagrams is discussed in detail in other locations in this guide.

- If you have a V-Series appliance, use diagrams 1 and 3 and refer to the following chapters:
  - Chapter 2: *Setting Up the V-Series Appliance*
  - Chapter 4: *Configuring the Web Security Module*
  - Chapter 5: *Configuring the Content Gateway Module*
  - Chapter 6: *Configuring the Data Security Module*
- If you have a software-only version of Web Security Gateway Anywhere, use diagrams 2 and 3 and refer to the following chapters:
  - Chapter 3: *Installing Software*
  - Chapter 4: *Configuring the Web Security Module*
  - Chapter 5: *Configuring the Content Gateway Module*
  - Chapter 6: *Configuring the Data Security Module*


Appliance Setup and Installation
Make Decisions
Where will Policy Broker be running? (One IP Address)
Where will TRITON – Web Security be installed?
Where will Log Server be installed?
Choose the unified password.
Set Up Policy Source Appliance
Assemble and rack hardware and cables (See Quick Start poster in box)
Run firstboot script to configure network interface C (Appliance Controller) and set unified password
Set the time on the appliance
Assign IP address and other network information to proxy interface P1
Assign IP address and other network information to Network Agent interface N
Designate this appliance as Policy Source
Enter IP address for TRITON – Web Security
Install Web Security off-appliance components
Synchronize OS time with appliance
Download the WWS installer
Run custom install on the first machine. Install Log Server and Sync Service
Run custom install on any additional machine. Install TRITON – Web Security, Linking Service, and Transparent ID agents
Install Data Security Management Server
Synchronize OS time with appliance
Download the DSS installer.
Run the installer. Choose Data Security Management Server.
Install Microsoft SQL Server 2005 or 2008
IP address:_____
Make sure that SQL Server Agent is running.
Configure a SQL account with dbo and SQLServerAgentReader permissions.
Account:_____
Password:_____


Software Installation
Make Decisions
Where will Policy Broker be running? (One IP Address)
Will there be more than one machine running Policy Server?
YES
NO
Which Policy Server do you want to associate with TRITON - Web Security?
Where will Policy Server be installed?
Where will Log Server be installed?
Where will TRITON - Web Security be installed?
Choose the unified password.
Install Microsoft SQL Server 2005 or 2008
IP address:_____
Make sure that SQL Server Agent is running.
Configure a SQL account with dbo and SQLServerAgentReader permissions.
Account:_____
Password:_____
Install Websense Web Security
Synchronize OS time with appliance
Download the WWS installer.
Run the installer on the first machine. Install Filtering Service and TRITON – Web Security as integrated with WCG.
Run custom install on any additional machines. Install Log Server, Sync Service, Directory Agent, Linking Service, and Transparent ID agents
Policy Broker must be installed first.
Policy Server must be installed second.
Install Log Server before TRITON - Web Security.
Install Websense Content Gateway
Synchronize OS time with appliance
Download the WCG installer.
Run the installer
Install Data Security Management Server
Synchronize OS time with appliance
Download the DSS installer.
Run the installer. Choose Data Security Management Server.


System Configuration
Test filtering
Test on-premesis filtering
Test hybrid filtering
Test Web DLP
Configure Data Security Module
Log on to TRITON – Data Security.
Configure Content Gateway agent
Deploy Content Gateway agent
Add an administrator that matches WWS
Create Data Security policies
Configure Proxy
Log on to Content Gateway Manager
Enter the subscription key and restart Content Gateway
Automatically initiates the Analytics Database download.
Select protocols to proxy
Configure network options (explicit/ transparent)
Configure client authentication
Register proxy with Data Security module
Configure Web Security Module
Log on to TRITON – Web Security.
Enter the subscription key.
Automatically initiates the Master Database download.
Log off and log back on to TRITON - Web Security.
Customize the Default policy.
Configure user identification.
Configure linking between Web and data modules
Configure hybrid filtering

2 Setting Up the V-Series Appliance

Deployment options

The Websense V-Series Appliance is a security gateway appliance with an operating system optimized for analyzing Web traffic and content. If you purchase an appliance-based Web Security Gateway Anywhere solution, the following components are pre-loaded for your convenience:

- Websense Web Security core components, including:
  - Policy Database
  - Policy Broker
  - Policy Server
  - Filtering Service
  - User Service
  - Usage Monitor
  - Control Service
  - Directory Agent
  - TRITON - Web Security (optional; can be run on separate Windows server)
    - Investigative Reports Scheduler
    - Manager Web Server
    - Reporting Web Server
    - Reports Information Service
- Websense Content Gateway
  - Content Gateway Manager
  - Content Cop
  - Download Service
- Network Agent (optional)

Larger enterprises might use 2 or more Websense appliances, with one designated as the *policy source* machine (the only machine to run Policy Broker and Policy Database, along with other components). All other appliances point to the *policy*

source machine for policy updates. Alternatively, you can add a Windows or Linux server and designate it as the *policy source*.

In all cases, Network Agent and Websense Content Gateway run as separate modules on each appliance, if they are enabled.

Regardless of how many appliances you have, the following Websense Web Security components must be installed separately. Most are Windows-only components.

- Log Server
- Sync Service
- Linking Service
- (optional) Transparent identification agents
  - DC Agent
  - Logon Agent
  - eDirectory Agent
  - RADIUS Agent

Note that TRITON - Web Security can be installed on one or more machines in addition to the appliance. TRITON - Web Security on the appliance is enabled by default. For production use, Websense recommends running it off the appliance. (You configure which manager to use in the Appliance Manager.)

In addition, the Websense Data Security Management Server must be installed on a Windows server. This includes:

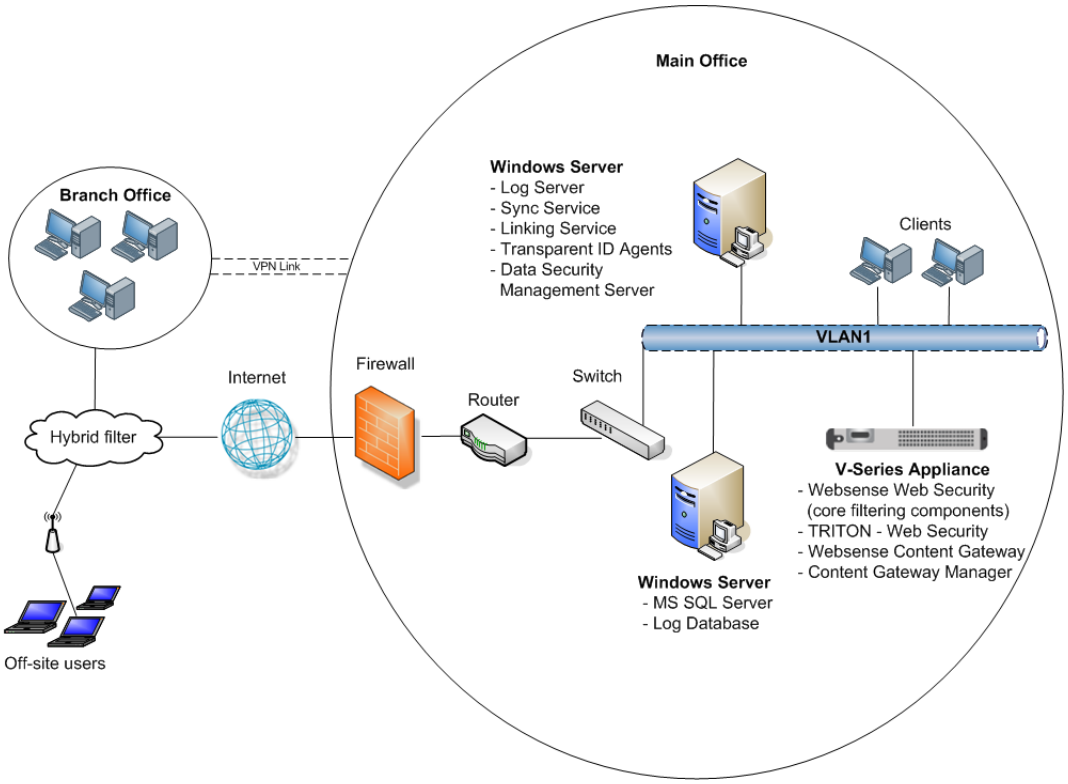
- Policy Engine
- Crawler
- PreciseID Fingerprint Repository
- Forensics Repository

The off-box Web and data security components can be installed on the same Windows machine using VMWare, if desired. (See *Installing on a virtual machine*, page 69 for more information.)

Finally, you're required to have a Windows database server running Microsoft SQL Server. This is where the Log Database is built. It does not matter whether SQL Server is installed in a virtualization environment or not, or whether it's on the same hardware as the Web and data security components.

This is what a Web Security Gateway Anywhere deployment might look like when deployed on a V-Series appliance in a small network. Larger networks typically install

and run **TRITON - Web Security** on Windows and might have 2 or more appliances and 2 or more Windows machines.



Preparing the appliance

Many components of Web Security Gateway Anywhere are pre-loaded on the appliance, while others require manual installation and set up.

To prepare an appliance for production use, you must:

1. *Set up the appliance hardware*
2. *Perform initial command-line configuration*
3. *Configure the appliance*
4. *Installing Windows components of Websense software*

Once you've done this, you can configure Websense software as described in sections 4 through 6.

Set up the appliance hardware

The Quick Start guide, which comes in the shipping box with your appliance, shows you all items included in each Websense appliance shipping box. The 2-page Quick

Start explains how to set up the hardware and shows how to connect the cables to the appliance and to your network.

Network interface C and the proxy interface (typically P1) must be able to access a DNS server. Both interfaces typically have continuous access to the Internet. Essential databases are downloaded from Websense servers through these interfaces.

- Ensure that interfaces C and P1 are able to access the download servers at **download.websense.com**. (As an alternative, some sites configure the P1 proxy interface to download the Websense Master Database as well as other security updates. In that situation, interface C does not require Internet access.)
- Make sure that this address is permitted by all firewalls, proxy servers, routers, or host files that control the URLs that the C and P1 interfaces can access.

After hardware setup, connect directly to the appliance through the serial port or the monitor and keyboard ports. For serial port activation, use:

- 9600 bits per second
- 8 data bits
- no parity

The activation script, called firstboot, runs when you start the appliance.

Perform initial command-line configuration

The first time you start a Websense appliance, a brief script (firstboot) prompts you to supply settings for the network interface labeled C and a few other general items. You can run the script again if you want to examine your settings or change settings. You can also change settings through the Appliance Manager (user interface) after firstboot has been executed.

Gather the following information before running the script. Some of this information may have been written down on the Quick Start during hardware setup.

Hostname	
IP address for network interface C	
Subnet mask for network interface C	
Default gateway for network interface C (IP address) *Optional*	NOTE: If you do not provide access to the Internet for interface C, then you must configure either P1 or P2 to receive Master URL Database downloads from Websense. This extra step must be done through the Appliance Manager (to configure P1 and P2) and through the TRITON - Web Security console (to configure the proxy for database downloads).
Primary DNS server for network interface C (IP address)	

Secondary DNS server for network interface C (IP address) *Optional*	
Tertiary DNS server for network interface C (IP address) *Optional*	
Unified password to be used for these consoles: Appliance Manager; TRITON - Web Security; and Content Gateway Manager. (8 to 15 characters, at least 1 letter and 1 number)	

When you have gathered the necessary information, run the initial command line configuration, as follows.

1. Access the appliance through a USB keyboard and monitor or a serial port connection.

   Note

   To configure the appliance, connect through the serial port or the keyboard/video ports and complete the firstboot script. For serial port activation, use:

   - 9600 bits per second
   - 8 data bits
   - no parity

2. Accept the subscription agreement when prompted.
3. When asked if you want to begin, enter **yes** to launch the firstboot activation script.

   NOTE: To rerun the script manually, enter the following command:

   ```
   firstboot
   ```

4. Follow the onscreen instructions to provide the information collected above.

After the activation script has been completed successfully, use the **Logon Portal** to access the Appliance Manager. To reach the **Logon Portal**, open a supported browser, and enter this URL in the address bar:

```
http://<IP address>
```

Replace <IP address> with the address assigned to network interface C during initial configuration of the appliance.

Configure the appliance

The Appliance Manager is the Web-based configuration interface for the appliance. Through it you can view system status, configure network and communication settings, and perform general appliance administration tasks.

After completing the initial configuration required by the firstboot script, use the Appliance Manager to configure important settings for network interfaces N and P1 (and optionally P2), which are used for communications by Network Agent and

Websense Content Gateway. Appliance model V10000 and model V10000 G2 also offer expansion interfaces (E1 and E2) that can be bonded with P1 and P2, respectively, either for load balancing or standby.

If you use the P2 interface, the P1 interface is bound to eth0, and the P2 interface is bound to eth1. Keep this in mind when you configure Websense Content Gateway.

For example, suppose you are using a transparent proxy deployment, and the P1 interface is connected to a WCCP router. In this case, you must configure Websense Content Gateway to use eth0 for WCCP communications (in Content Gateway Manager, see **Configure > Networking > WCCP**, WCCP version tab).

Gather the following information before running the Appliance Manager. Some of this information may have been written on the Quick Start during hardware setup.

Primary NTP server, (domain) *Optional* Be sure that interface C can access the NTP server. If interface C does not have Internet access, you can install an NTP server locally on a subnet that can be accessed by interface C.	
Secondary NTP server, (domain) *Optional*	
Tertiary NTP server, (domain) *Optional*	
IP address for network interface P1	
Subnet mask for network interface P1	
Default gateway for network interfaces P1 (and P2); (IP address) If you use both P1 and P2, the default gateway is automatically assigned to P2 (which is bound to eth1). To ensure that outbound packets can reach the Internet, do not locate the IP addresses of P1 and P2 in the same subnet.	
Primary DNS server for network interfaces P1 (and P2); (IP address)	
Secondary DNS server for network interfaces P1 (and P2); (IP address) *Optional*	
Tertiary DNS server for network interfaces P1 (and P2); (IP address) *Optional*	
IP address for network interface P2 *Required only if P2 is enabled*	
Subnet mask for network interface P2 *Required only if P2 is enabled*	
Choose interface for transporting blocking information for non-HTTP and non-HTTPS traffic. (interface C or interface N)	
If interface N transports blocking information, N must be connected to a bidirectional span port.	Ensure that interface N has been set up appropriately, if N will transport blocking information.

IP address for network interface N	
Subnet mask for network interface N	
Default gateway for network interface N (IP address) *Required only if network interface N carries blocking information*	
Primary DNS server for network interface N (IP address)	
Secondary DNS server for network interface N, (IP address) *Optional*	
Tertiary DNS server for network interface N, (IP address) *Optional*	
Bond expansion interface E1 to P1? Yes or No *Optional*	If Yes, choose one: Active/standby or Load balancing
Bond expansion interface E2 to P2? Yes or No *Optional*	If Yes, choose one: Active/standby or Load balancing
Policy Source IP address	Choose one: This appliance is the policy source. This appliance runs User directory and filtering (specify policy source IP address). This appliance runs filtering only (specify policy source IP address).
TRITON - Web Security (user interface for Websense Web Security) IP address	TRITON - Web Security runs on this appliance. *or* TRITON - Web Security runs at the specified IP address. *Organizations with high traffic volume or large reporting needs are encouraged to install and* *run TRITON - Web Security on a separate Windows server, to optimize performance.*

After collecting the information needed, access the Appliance Manager through a supported browser.

Follow these steps to enable default proxy caching and filtering. See the Appliance Manager Help for detailed instructions on any field or area, or for information about other available settings.

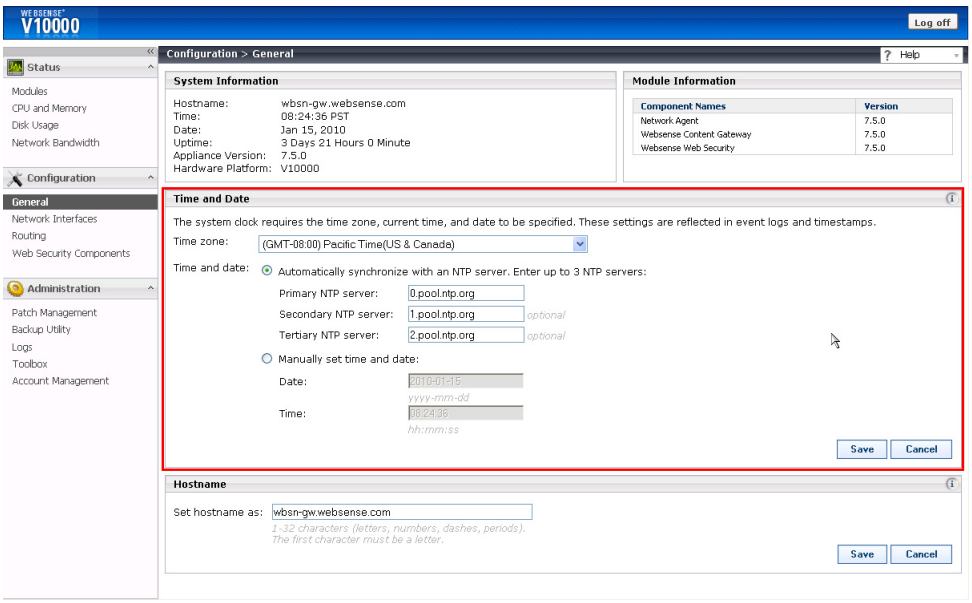
1. Open a supported browser, and enter the following URL in the address bar:

   ```
   https://<IP address>:9447/appmng
   ```

   Replace <IP address> with the address assigned to network interface C during initial configuration of the appliance.

   (See *Perform initial command-line configuration*, page 20.)

2. Log on with the user name **admin** and the password set during initial appliance configuration.
3. In the left navigation pane, click **Configuration > General**.

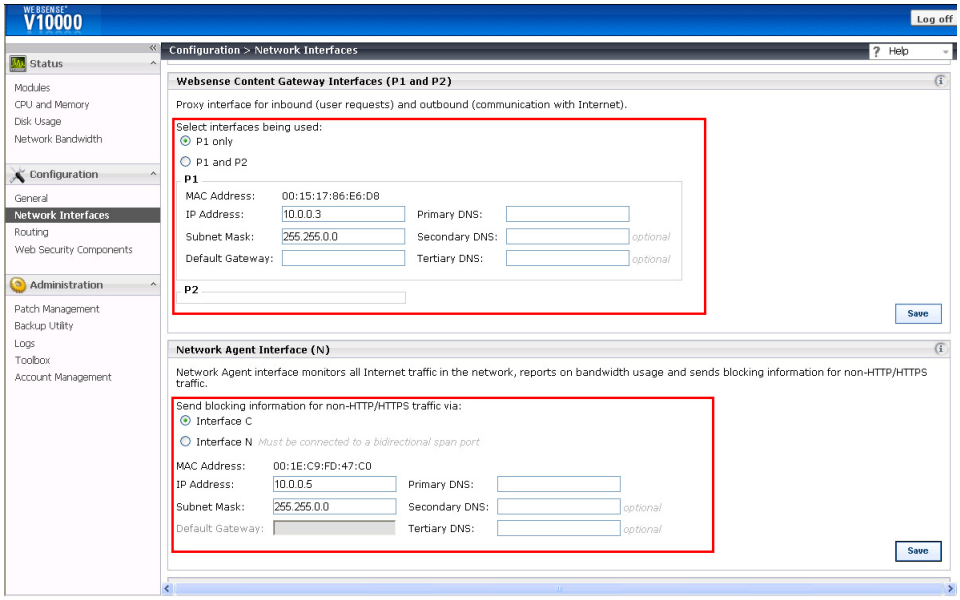


   a. Set the time zone.

   b. Select Internet Network Time Protocol (NTP) servers for time synchronization, or specify the system time and date. (Use of an NTP server is recommended, to ensure that database downloads and time-based policies are handled precisely.)

   c. Click **Save** in the Time and Date area.

4. In the left navigation pane, click **Configuration > Network Interfaces**.



a. Configure network interfaces P1 (and optionally P2) for Websense Content Gateway. Then, click **Save** in the Websense Content Gateway Interface area.

Important

When you use the P2 interface, the P1 interface is bound to eth0, and the P2 interface is bound to eth1. Keep this in mind when you configure Websense Content Gateway.

For example, suppose you are using transparent proxy, and the P1 interface is connected to the WCCP router. In this case, you must configure Websense Content Gateway to use eth0 for WCCP communications (in Content Manager, see **Configure > Networking > WCCP**, WCCP version tab).

These network interfaces can accept users' Internet requests (inbound traffic) and communicate with Web servers (outbound traffic).

One common configuration is to use P1 for traffic into and out of the proxy module. Another common configuration uses P1 for inbound traffic and P2 for outbound traffic. To enable this configuration, be sure to set appropriate routing rules for P1 and P2 on the **Configuration > Routing** page. For example, you might set outbound traffic to go through P2.

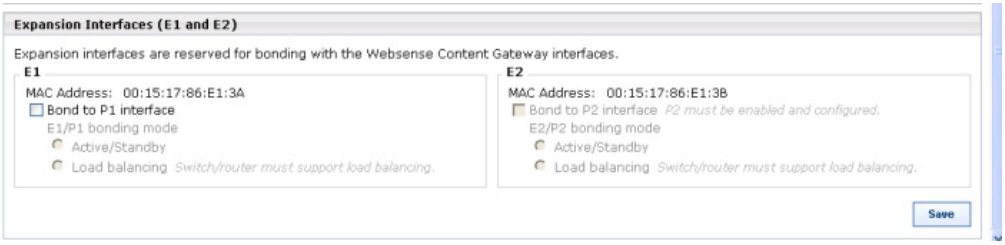
Additionally, you can use P2 as a communication channel for multiple proxy servers in a cluster. In this scenario, P2 cannot be used for outbound traffic. For additional information on clusters, see the Websense Content Gateway *Administrator's Guide*.

b. Decide whether network interface N (for Network Agent) will transport blocking information for non-HTTP/HTTPS traffic. Enter all required IP addresses and enter the subnet mask. Then, click **Save** in the Network Agent Interface area.

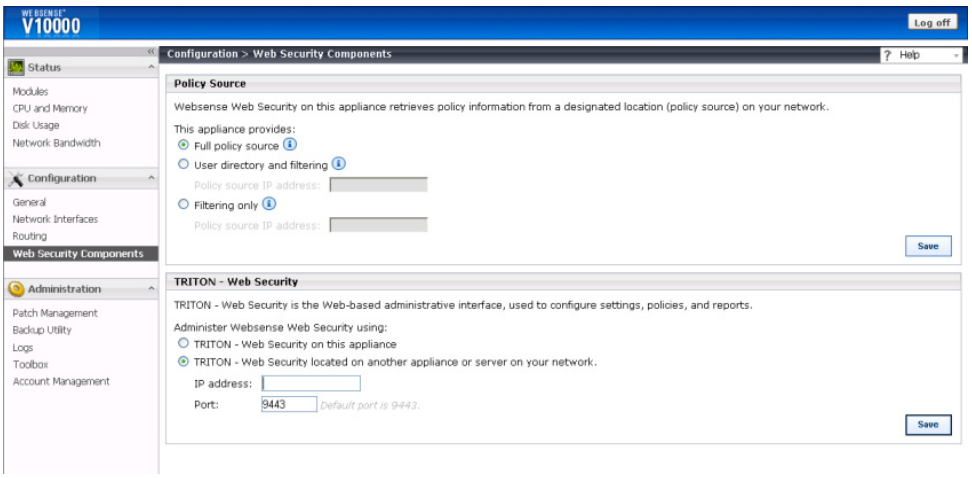
Network interface N monitors all Internet requests, and can enforce policy for protocols other than HTTP and HTTPS.

> **Note**
> The appliance does not send block messages to users who are blocked from non-HTTP and non-HTTPS protocols.

5. Configure expansion interfaces, if desired. Then, click **Save** in the Expansion Interfaces area.



6. In the left navigation pane, click **Configuration > Routing**.
   a. Use the **Add Route** button to specify customized, static routes.
   b. Use the **Edit** and **Delete** buttons to modify existing routes, as needed.
7. In the left navigation pane, click **Configuration > Web Security Components**.



   a. Specify the role of this appliance with respect to Websense Web Security policy information.
      - Choose **Full policy source** if Websense Policy Broker and Policy Database for your deployment will run on the appliance being configured. (Only one appliance in the network runs these two components, as well as the other filtering components.) Policy Server must also be run on the *policy source* appliance; Policy Server can run in multiple locations.

- Choose **User directory and filtering** if the appliance currently being configured is *not* the location of the policy information, but will run Policy Server and User Service. Then, enter the **IP address** of the server that is used as the policy source. (If the policy source is another appliance, enter the IP address of its network interface C.)
- Choose **Filtering only** if the appliance being configured will not run any policy components. (There are some disadvantages to this reduced role, as explained in the Appliance Manager help system.) Then, enter the **IP address** of the server that is used as the policy source. (If the policy source is another appliance, enter the IP address of its network interface C.)

b. Click **Save**.

c. Identify the location where you want to run **TRITON - Web Security. TRITON - Web Security** is the Web-based console for Websense Web Security software. It is pre-installed on the appliance, and is enabled there by default. Organizations with high traffic volume or large reporting needs are encouraged to install and run **TRITON - Web Security** on a separate Windows server, to optimize performance.

d. Click **Log Off**, at the top right, when you are ready to log off Appliance Manager.

Components running off the appliance

The following Websense Web Security components must be installed separately and can run on the same Windows server. Most are Windows-only components. The installer for all Websense Web Security components can be downloaded from the downloads page at www.websense.com.

- Log Server (required for reporting)
- Sync Service (for sites using hybrid Web security)
- Linking Service (for sites using any Data Security features)
- (optional) Transparent identification agents (for filtering by user or group)
  - DC Agent
  - Logon Agent
  - eDirectory Agent
  - RADIUS Agent

In addition, the Websense Data Security Management Server must be installed on a Windows server, for sites using any Data Security features. This includes:

- Policy Engine
- Crawler
- PreciseID Fingerprint Repository
- Forensics Repository

In addition, organizations with high traffic volume or large reporting needs are encouraged to install and run **TRITON - Web Security** on a separate Windows server, to optimize performance.

The off-appliance Web security and data security components can be installed on virtual machines that you create on a Windows server with a supported version of VMware, if desired.

Finally, you're required to have a Windows database server running Microsoft SQL Server. This is where the Log Database is built. Log Database provides the information for Web security reporting.

See *Installing Windows components of Websense software*, page 29 for instructions.

Logon portal

The **Logon Portal** provides V-Series administrators with access to the management consoles from a central Web page.

- Appliance Manager
- TRITON - Web Security
- Content Gateway Manager (for Websense Content Gateway)
- TRITON - Data Security

To reach the **Logon Portal**, open a supported browser, and enter this URL in the address bar:

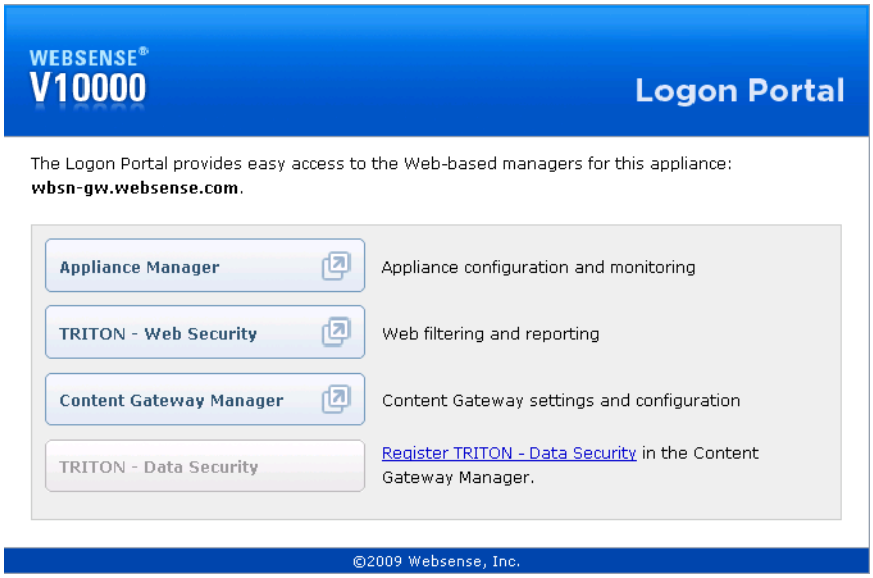
```
http://<IP address>
```

Replace <IP address> with the address assigned to network interface C during initial configuration of the appliance.

Note

The following (similar) URL does *not* provide access to the **Logon Portal**:

```
https://<IP address>
```



Installing Windows components of Websense software

Some Websense modules must be installed on Windows servers whether or not you have an appliance. This section describes what to install off-box.

Websense Web Security

Some Websense Web Security components are not included on the appliance. They must be installed separately.

Note that although TRITON - Web Security is included on the Linux-based appliance, you can install it on one or more other machines if you choose. TRITON - Web Security can also be installed on Windows servers.

The basic steps you need to perform are:

1. Ensure you have Microsoft SQL Server 2008 installed on the machine where you will be installing Websense off-box components.
2. Verify that you can ping to the IP address of the P1 and C network interfaces.
3. Synchronize your operating system time with the time on the V-Series appliance.
4. Download the Websense Web Security installer package from mywebsense.com.
5. Extract the installer files. To do so, double-click the downloaded file, and click **Run** when prompted.

   The installer files are extracted to a temporary directory (by default, C:\Documents and Settings*<user name>*\Local Settings\Temp*<generated name>*.tmp). Once the installer has completed, this directory is deleted. You can retain these extracted files, for example to perform script-based

installations, by copying the contents of the temporary directory (including all sub-directories) to another location. Launching **setup.exe** starts the installer.

After extraction, the installation program starts automatically.

6. On the **Introduction** screen, click **Next**.
7. On the **Subscription Agreement** screen, choose to accept the terms of the agreement and then click **Next**.
8. On the **Installation Type** screen, select **Custom** click **Next**.
9. On the **Select Components** screen, choose the following components to install and then click **Next**:
   - Log Server
   - Sync Service
   - Linking Service
   - Optionally, TRITON - Web Security
   - Optionally, the following transparent identification agents:
     - DC Agent
     - Logon Agent
     - eDirectory Agent
     - RADIUS Agent

   Do not choose Directory Agent. It is installed on the appliance and can cause issues if installed off of the appliance as well. (If you must have multiple Directory Agent instances, make sure they use a unique, non-overlapping root context to search for user data. You can have only one Directory Agent instance per Policy Server.)

   See Topic 3 for component-specific installation instructions.
10. Enter the IP address and port of the policy server when prompted. This is the IP of the appliance C interface. The default port is 55806. Click **Next**.
11. Enter the same IP address for the policy broker location.
12. Specify a database user name (sa) and password and click **Next**.
13. Enter the IP address and port for the filtering service. In appliance configurations, this is also the C interface IP. The default port is 15868.
14. Enter the log database location or accept the default.
15. When prompted, provide a user name and password for an administrator with user directory access.
16. Keep the default directory path and click **Next**.
17. On the **Pre-Installation Summary** screen, verify the information shown.
18. Click **Next** to start the installation. An **Installing** progress screen is displayed. Wait for the installation to complete.
19. On the **Installation Complete** screen, click **Done**.
20. Proceed to topic 4 for instructions on configuring the Web Security module.

Websense Data Security

Data Security software can be installed on the same Windows machine as TRITON - Web Security and Log Server—on a separate virtual machine—or it can be installed on its own Windows 2003 machine.

The machine where you install the software is called the *Data Security Management Server*. This machine provides Web Security Gateway Anywhere's core data loss prevention technology, capturing fingerprints of your data, applying policies, and storing incident forensics.

For instructions on installing Data Security software, refer to *Installing Websense Data Security*, page 69. For instructions on installing Data Security on a VM, see *Installing on a virtual machine*, page 72.

When you're done, proceed to topic 6 for instructions on configuring the Data Security module.

More information

For more information on the V-Series appliance, refer to the *Websense V-Series Appliance Getting Started Guide* and Appliance Manager Help.

3 Installing Software

If you purchase Websense Web Security Gateway Anywhere as software, you're required to install the various components. This chapter is your installation organizer. For ease of reference, installation tasks have been broken down into 3 main areas:

- *Installing Websense Web Security*, page 34
- *Installing Websense Content Gateway*, page 60
- *Installing Websense Data Security*, page 69

Deployment options

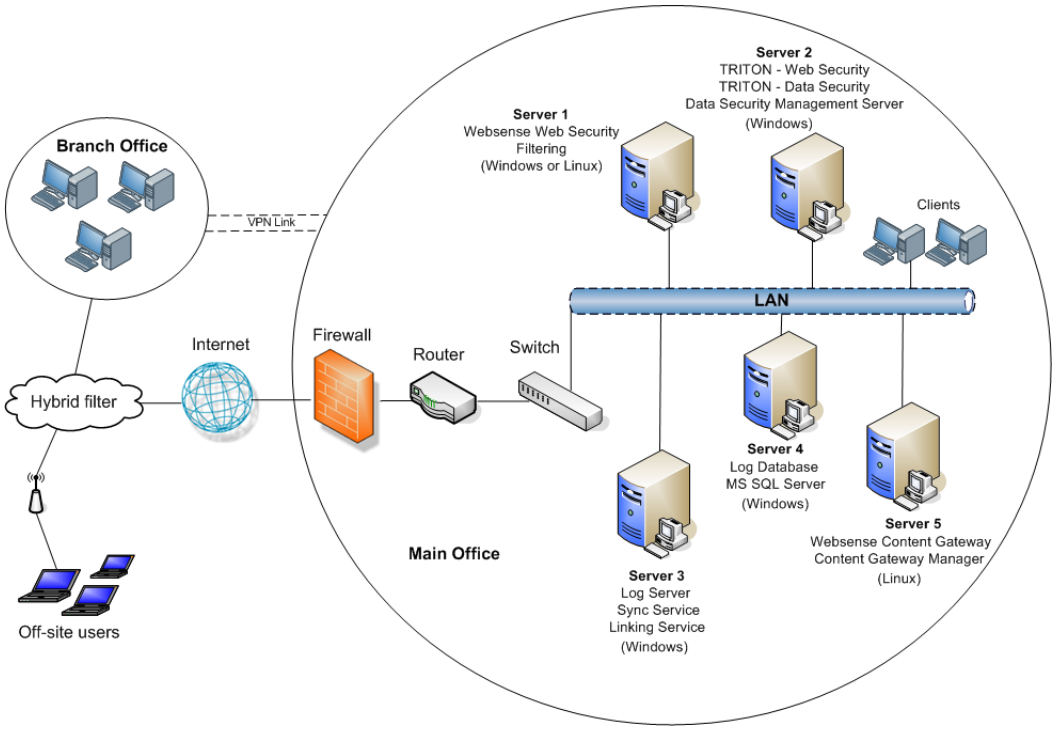
In Web Security Gateway Anywhere, a typical installation contains:

- Websense Web Security filtering components on a Windows or Linux machine.
- TRITON - Web Security and Data Security Management Server on a Windows machine in 2 virtual machines. See *Installing on a virtual machine*, page 72 for details.
- Log Server, Sync Service, Directory Agent, and Linking Service. Log Server and Linking Service much be installed on Windows. Websense recommends installing Sync Service on the same machine as Log Server. Directory Agent can be installed on a Windows or Linux machine.
- Log Database on your Microsoft SQL Server database engine.
- Websense Content Gateway on a Linux machine (includes Content Gateway Manager). (See *Hardware and software requirements*, page 60 for system requirements.)

Optionally, you may install transparent identification agents as needed.

> **Note**
> When installing manager components—TRITON - Web Security, Data Security Management Server, and TRITON - Email Security—make sure that the names of the machines you're installing on do not contain underscore characters or hyphens. Some browsers do not support these characters and cannot display TRITON screens as expected.

The following diagram illustrates what Web Security Gateway Anywhere deployment looks like when software is installed in a small to medium network. In larger networks, filtering components may be distributed across multiple machines. This is just an example of how the modules might fit together. You can arrange them in numerous ways to fit your needs.



Installing Websense Web Security

Following are instructions for installing Websense Web Security in Web Security Gateway Anywhere mode. For additional information, refer to the *Websense Web Security/Websense Web Filter Installation Guide*.

Note that you will be integrating Websense Web Security with Websense Content Gateway, so there are special instructions for selecting the integration option (this is not the default).

You will also be instructed to install custom Web DLP and hybrid components. The Websense Linking Service required for Web DLP is installed in a disabled state. You will enable this service when you link the Web Security and Data Security modules in Chapter 4. (See *Configuring linking between Web and data security*, page 93.)

Hardware and software requirements

Use the *Websense Web Security/Websense Web Filter Deployment Guide* before starting your installation to make sure that the installation machines meet or exceed system requirements, and that Websense components are distributed appropriately.

Components

Websense software is made up of several components that work together to provide user identification, Internet filtering, and reporting capabilities. Not all components are required to deploy the software.

Required components

- **Policy Broker**: Manages requests from Websense components for policy and general configuration information.
- **Policy Database**: Stores Websense software settings and policy information. This database is installed with Policy Broker, and cannot be installed separately.
- **Policy Server**: Identifies and tracks the location and status of other Websense components. Stores configuration information specific to a single Policy Server instance. Communicates configuration data to Filtering Service, for use in filtering Internet requests.
- **Filtering Service**: Interacts with your integration product and Network Agent to filter Internet requests. Filtering Service either permits the Internet request or sends an appropriate block message to the user.
- **TRITON - Web Security**: Configuration, management, and reporting interface to Websense software.
- **Apache2Websense**: Apache Web Server providing underlying functions required for Investigative Reports and client-browser communication in TRITON - Web Security.
- **ApacheTomcatWebsense**: Apache Tomcat service that hosts the management and reporting user interfaces of TRITON - Web Security.
- **User Service**: Communicates with your network's directory services to allow you to apply filtering policies based on users, groups, domains, and organizational units.
- **Network Agent** (required for stand-alone deployment only): In a stand-alone deployment, Network Agent manages the filtering of all protocols, including HTTP, HTTPS, and FTP.

Network Agent detects network activity to support the bandwidth filtering and protocol management features, and to log the number of bytes transferred.

In an integrated deployment, Network Agent is optional. In this case, Network Agent manages the Internet protocols that are not managed by your integration product. Network Agent can also be used to detect HTTP network activity and instruct Filtering Service to log this information.

- **Usage Monitor**: Tracks users' Internet activity and sends alerts to Websense administrators when configured threshold values are exceeded.
- **Websense Master Database**: A downloadable list of millions of categorized Internet sites. Protocol definitions are also included in this database.
- **Websense Control Service**: Tracks the installation, configuration, and removal of Websense components and services. This service should be left running at all times.

Optional user identification components

- **DC Agent**: With Microsoft Windows® directory services to transparently identify users so that Websense software can filter them according to particular policies assigned to users or groups.
- **Logon Agent**: Works with the Websense logon application (**LogonApp.exe**) to transparently identify users as they log on to Windows domains.
- **RADIUS Agent**: Works through a RADIUS Server to transparently identify users and groups who access your network using a dial-up, Virtual Private Network (VPN), Digital Subscriber Line (DSL), or other remote connection.
- **eDirectory Agent**: Works with Novell® eDirectory™ to transparently identify users so that Websense software can filter them according to particular policies assigned to users or groups.

Optional filtering components

- **Remote Filtering Server**: Provides Web filtering for clients located outside your organization's network firewall or Internet gateway. The Remote Filtering Server should be installed inside the outermost firewall, but in the DMZ outside the firewall protecting the rest of the corporate network.
- **Remote Filtering Client**: Is installed on client machines, such as laptop computers, that are used outside of the organization's network firewall or Internet gateway. This component connects with a Remote Filtering Server to filter the remote computers.

Optional reporting component

The following Windows-only component is required to enable the reporting features of TRITON - Web Security (including charts, presentation reports, and investigative reports). Before this component can be installed, Microsoft SQL Server or Microsoft SQL Server Desktop Edition (MSDE) must be installed.

- **Log Server**: Sends records of Internet activity to the Log Database. It also sends category names, protocol names, and risk class names from the Master Database to the Log Database.

Integration component

- **Filtering plug-in**: Enables communication between supported firewalls, proxy servers, caching applications, or network appliances and Filtering Service. See the *Installation Guide Supplement* for your integration product for more information.

> **Note**
> Not all supported integration products require a filtering plug-in. Only Microsoft ISA Server and Forefront TMG; Citrix Presentation Server and XenApp; and Squid Web Proxy Cache require plug-ins.

Interoperability components

The following components allow communication and synchronization between Web and data security components, and between on-premises components and the hybrid service in Websense Web Security Gateway Anywhere deployments.

- **Linking Service**: Enables communication between Websense filtering software and Websense Data Security. Linking Service gives Data Security access to user name information from User Service and URL categorization information from Filtering Service.
- **Directory Agent**: Collates user and group information for use by the hybrid service.
- **Sync Service**: Communicates policy and user information to the hybrid service. Retrieves log data for reporting from the hybrid service.

Preparing to install

1. Log on to the installation machine with administrative privileges:
   - **Linux**: log on as **root**.
   - **Windows**: log on with **domain** and **local** administrator privileges. If you will install Log Server, the installation machine must be joined to the same domain as the database engine machine.

   Using administrative privileges at installation ensures that User Service (and, optionally, DC Agent and Logon Agent) is able to apply user-based filtering. If necessary, you can apply administrator privileges after installation (see *Troubleshooting > User Identification* in TRITON - Web Security Help).

   If you will use a Windows trusted connection to communicate with the database engine to access the Websense Log Database, your logon account must also be a trusted account on the database engine machine with proper database privileges. Specify this same account in the Database Information screen (Step b, page 9) when choosing to use Windows trusted connection to access the Log Database.
2. Close all applications and stop any antivirus software.
3. On Linux, create a setup directory for the installer files. For example:

   ```
   /root/Websense_setup
   ```

4. Download the Websense Web Security or Websense Web Filter installer package from mywebsense.com:
   - Websense75Setup.exe (Windows)
   - Websense75Setup_Lnx.tar.gz (Linux)

   On Linux, place the installer tar archive in the setup directory you created.
5. Extract the installer files.
   - **Windows**: Double-click the downloaded file, and click **Run** when prompted. The installer usually starts automatically.

     The installer files are extracted to a temporary directory (by default, C:\Documents and Settings*<user name>*\Local Settings\Temp *<generated name>*.tmp). Once the installer has completed, this directory is deleted. You can retain these extracted files, for example to perform script-based installations, by copying the contents of the temporary directory (including all sub-directories) to another location. Launching setup.exe starts the installer.
   - **Linux**: In the setup directory, enter the following commands to uncompress and extract files:

     ```
     gunzip Websense75Setup_Lnx.tar.gz
     tar xvf Websense75Setup_Lnx.tar
     ```

     This places the following files into the setup directory:

File	Description
`install.sh`	Installation program
`Setup.bin`	Archive file containing installation files and documents

6. After extraction, the installation program starts automatically in Windows. It must be started manually in Linux.

   If the installation program is not running:
   - **Windows**: Download the installer package (Websense75Setup.exe) again. The initial download may not have completed successfully and resulted in a corrupted package. If double-clicking the re-downloaded installer package does not start the installer, delete all files from the **%temp%** directory (accessible by clicking Windows **Start**, selecting **Run**, and then entering **%temp%**) and then double-click the installer package again. If, at this point, the installer still does not start contact Websense Technical Support.
   - **Linux**: Use the following command to run the installation program from the setup directory:

     ```
     ./install.sh -g
     ```

     This launches a GUI-based installer and is available on English version of Linux only. A text-only, command-line version can be launched by omitting the -g switch:

```
./install.sh
```

Note

If the installation program displays error messages that it is having difficulty locating other machines, disable any firewall running on the installation machine.

Installing the software

Separate installers are available for Windows and Linux versions of Websense Web Security and Websense Web Filter.

For Websense Web Security Gateway Anywhere, you will need to run the installer twice:

- Once to install the default filtering, management, and reporting functions as part of a typical installation
- Another time to install the custom services required for Web DLP and hybrid filtering: Sync Service, Directory Agent, and Linking Service

When you select a typical installation, all core Websense filtering components are installed together. You are also given the option to install one or more transparent identification agents, used to apply user-based filtering without prompting users for logon information. See the *Deployment Guide* for more information about Websense software components, and about combining the transparent identification agents.

Which components are included in a typical installation depends on the operating system of the installation machine, as explained below. For a list of supported operating system versions, see the *Deployment Guide*.

Windows

The following core components are installed as part of a typical installation:

- Policy Broker
- Policy Database
- Policy Server
- TRITON - Web Security (includes required third-party components Apache HTTP Server and Apache Tomcat)
- Transparent identification agents (optional)
  - DC Agent
  - Logon Agent
  - eDirectory Agent
  - RADIUS Agent
- Log Server (generally installed separately from filtering components)
- Filtering Service
- User Service
- Network Agent
- Usage Monitor

Linux

The following core components are installed as part of a typical Linux installation.

- Policy Broker
- Policy Database
- Policy Server
- Web Security Manager (includes the required third-party component Apache Tomcat)
- Transparent identification agents (optional)
  - Logon Agent
  - eDirectory Agent
  - RADIUS Agent
- Filtering Service
- User Service
- Network Agent
- Usage Monitor

In order to enable the reporting features of Web Security Manager in a Linux deployment, the Log Server component (which is Windows-only) must also be installed on a Windows machine in the network.

Typical installation

Important

The installation supplement for your integration product contains additional information required to install and configure Websense software to run with your firewall, proxy server, caching application, or network appliance. Where indicated, refer to the supplement while performing the following procedures.

1. Make sure that you have followed the steps in *Preparing to install*, page 37.
   - Log on to the installation machine with appropriate permissions.
   - Close all applications and stop any antivirus software.
   - Download and start the installer, if needed.

Note

To cancel the command-line Linux installer, press Ctrl-C. However, do **not** cancel the installer after the **Pre-Installation Summary** screen, as it is installing components. In this case allow the installation to complete and then uninstall the unwanted components.

2. On the **Introduction** screen, click **Next**.

> **Note**
> These instructions refer to installer screens. In the command-line Linux installer, prompts are displayed that correspond to each screen. Instructions for a screen also apply to the corresponding command-line prompt. The main difference is how options are selected. Rather than clicking items in a screen, you will enter menu-item numbers or characters.

3. On the **Subscription Agreement** screen, choose to accept the terms of the agreement and then click **Next**.
4. On the **Installation Type** screen, select an installation type and then click **Next**:

   - **Filtering and Management**: Installs Filtering Service, Policy Broker, Policy Server, TRITON - Web Security, User Service, Usage Monitor, and Network Agent together on the same machine. The installer gives you the option of installing the following transparent identification agents: DC Agent (Windows only), eDirectory Agent, Logon Agent, and RADIUS Agent.

     This installation type is appropriate for:

     - Small networks (less than 500 users, or less than 25 Internet requests per second)
     - Medium networks (500-2500 users or 25-125 Internet requests per second), on a dedicated machine.

     For larger or distributed networks, select the **Custom** installation type instead.

> **Note**
> This installation type does not include remote filtering components, which provides filtering for remote users outside the network firewall. After installing core components, install remote filtering components on another machine, using a **Custom** installation.

> **Note**
> If you are installing on an ISA Server machine, you can select **Filtering and Management** only if ISA Server is used as a proxy server and not firewall. This type of installation includes Websense Network Agent which should not be installed on a machine running a firewall. If you want to install Websense components on this machine select the **Custom** installation type. Be sure not to install Network Agent. See *Installing individual components*, page 37.

> **Note**
> If you are installing on a Citrix machine, do not select this installation type. Only the Citrix Integration Service (i.e., filtering plug-in) should be installed on a Citrix machine, using the Custom installation type.

- **Filtering, Management, and Reporting**: Available for Windows only. Recommended only for evaluation or very small networks. Installs all filtering, management, and reporting components on a single machine.

  This installation type is appropriate for:

  - Non-production, evaluation environments
  - Small networks (less than 500 users, or less than 25 Internet requests per second), on a dedicated machine.

  For larger or distributed networks, select **Custom** installation type instead.

  > **Note**
  > Like Filtering and Management, this installation type does not include remote filtering components. See the note above, under Filtering and Management, for more information.

  > **Important**
  > Make sure the database engine is running before installing reporting components.

  > **Note**
  > If you are installing on a Citrix machine, do not select this installation type. Only the Citrix Integration Service (i.e., filtering plug-in) should be installed on a Citrix machine, using the Custom installation type.

- **Custom**: Allows you to choose individual Websense components to install.

  This installation type is suggested for:

  - Large networks (2500-10000 users or 125-500 Internet requests per second)
  - Enterprise networks (10000-25000 users or 500-1250 Internet requests per second)
  - Very large enterprise networks (more than 25000 users or more than 1250 Internet requests per second)

- Distributed enterprise networks (users distributed across regional offices or networks, connected together via the Internet)

> **Note**
> In these types of environments, Websense components are typically distributed across different machines in the network. Multiple instances of certain components are also installed to handle processing load. Run this installation program on each machine, select the **Custom** installation type, and install particular components. For information about distributing components, see the *Deployment Guide for Websense Web Security Solutions*.

5. If you are installing on Windows Server 2008 (the screens mentioned here appear only if Windows Server 2008 is detected by the installation program):
   a. On the **Active Directory** screen, indicate whether you are using Active Directory to authenticate users in your network and then click **Next**.
   b. If you select **Yes**, the **Computer Browser Service** screen appears if the Computer Brower service is not currently running. Choose whether to start this service and then click **Next**.

      The Computer Browser service is a Windows utility that must be set to Automatic and Start in the Windows Services dialog box for Websense components to communicate with Active Directory.

      > **Note**
      > If you choose to start the Computer Browser service now, make sure the Computer Browser service is enabled on this machine. In most cases, it is disabled by default. The installer will attempt to start the service and configure it to start up automatically from now on. If the service is disabled, the installer will be unable to start it.

      If you choose not to have the installer start the service, or if the installer is unable to start it, you must start it manually after installation. If you use Active Directory 2008 to authenticate users, you must also start the Computer Browser service on the Active Directory machine.
6. On the **WebsenseAdministrator Password** screen, enter a password for the WebsenseAdministrator user and then click **Next**.

   It is a best practice to enter a password that is *very strong* (at least 8-characters long, containing all of the following: uppercase characters, lowercase characters, numbers, and symbols).

   WebsenseAdministrator is the default TRITON - Web Security user with unconditional Super Administrator privileges (access to all administrative functions). This account cannot be removed and its permissions cannot be

changed. When logging on to TRITON - Web Security for the first time, do so as WebsenseAdministrator.

> **Important**
> Do not lose this password. Only other Super Administrator users can reset the WebsenseAdministrator password. If no other Super Administrator users exist, you must visit MyWebsense (www.mywebsense.com) and enter your subscription key to reset the password. For more information, see TRITON - Web Security Help.

7. On the **Multiple Network Cards** screen, select the IP address of the network interface card (NIC) to be used by Websense software on this machine.

   > **Note**
   > This screen appears even if the machine does not have multiple NICs. In this case, only one NIC is listed.

   This is the NIC that will be used to send block pages when a user requests filtered content.You will specify later whether this NIC is also used by Websense Network Agent to monitor Internet traffic and send protocol block messages.

   > **Note**
   > If the selected NIC will be used by Network Agent, it must support *promiscuous* mode.

8. On the **Integration Option** screen, select **Integrated with another application or device**, and then click **Next**.
9. The Select Integration screen appears. Select **Websense Content Gateway** and then click **Next**.
10. On the **Network Card Selection** screen, select the network interface card (NIC) to be used by Websense Network Agent and then click **Next**.

    > **Note**
    > This screen appears even if the machine does not have multiple NICs. In this case, only one NIC is listed.

    This is the NIC that Websense Network Agent will use to communicate with other Websense software components. All enabled NICs with an IP address are listed.

    > **Note**
    > For Network Agent to operate, this machine must be connected to a bi-directional span port (or mirror port) on a switch or hub that processes the network traffic to be monitored.

You may select multiple NICs. After installation, use TRITON - Web Security to configure how Network Agent will use each selected NIC (for more information, see TRITON - Web Security Help).

On Linux, NICs without an IP address are also listed. Do not choose a NIC without an IP address.

After installation, you can configure Network Agent to use NICs without an IP address to monitor Internet requests.

11. The following screens appear only if you are installing Websense reporting components:

    Note
    Reporting components can be installed on a Windows machine only.

    a. **Database Engine**: This screen appears only if a supported database engine (SQL Server or MSDE) is not detected on this machine. If a supported database engine is installed on another machine in the network, select **Connect to an existing database engine** and then click **Next**.

    If a supported database engine is not available, use the knowledge base link for more information about installing the free MSDE database, select **Exit the installation program**, and then click **Next**. The installation program is cancelled. After installing and configuring a supported database engine, run this installer again.

    Note
    For supported versions of SQL Server and MSDE, see the *Deployment Guide for Websense Web Security Solutions*.

    b. **Database Information**: Enter the hostname or IP address of the machine on which a supported database engine is running. If a supported database engine is detected on this machine, its IP address is already entered by default. To use a database engine on a different machine, enter its IP address instead.

    After entering the IP address of the database engine machine, choose how to connect to the database:

    - **Trusted connection**: use a Windows account to log into the database. Enter the domain\username and password of a trusted account with local administration privileges on the database machine. If you are using MSDE, it is a best practice to connect using a database account rather than trusted connection. If TRITON - Web Security is installed on a Linux machine, use a database account, rather than trusted connection, to connect to the database

    Important
    The account you specify for trusted connection here must be the same as that used to log onto this machine (Step 1, page 9).

If you choose trusted connection, be sure to configure the Apache2Websense and ApacheTomcatWebsense services, after installation, to log on as the trusted account specified here in the **Database Information** screen. See *Configuring Websense Apache services for trusted connection*, page 90.

If your organization uses ISA Server and a Windows trusted connection will be used to access the Log Database, remote SQL logging (on ISA Server) may need to be enabled and communication on the internal network allowed. See *Enabling Remote SQL Logging on ISA Server*, page 108.

- **Database account**: use a SQL Server account to log into the database. Enter the user name and password for a SQL Server account that has administrative access to the database. The SQL Server password cannot be blank, or begin or end with a hyphen (-). It is a best practice to connect to your database engine using a database account rather than a trusted connection.

Note

The database engine must be running to install Websense reporting components. The installer will test for a connection to the specified database engine when you click **Next** on the **Database Information** screen. The installer cannot proceed unless a successful connection can be made.

c. **Log Database Location**: Accept the default location for the Log Database, or select a different location. Then, click **Next**.

If the database engine is on this machine, the default location is the Websense directory (`C:\Program Files\Websense`). If the database engine is on another machine, the default location is `C:\Program Files\Microsoft SQL Server` on that machine.

It is a best practice to use the default location. If you want to create the Log Database in a different location (or if you already have a Log Database in a different location), enter the path to the database files. The path entered here is understood to refer to the machine on which the database engine is located.

Important

The directory you specify for the Log Database must already exist. The installer cannot create a new directory.

d. **Optimize Log Database Size**: The options on this screen allow you to control the size of the Log Database, which can grow quite large. Select either or both of the following options and then click **Next**.

Log Web page visits: Enable this option to log a record of each Web page requested rather than each separate file included in the Web page request. This creates a smaller database and allows faster reporting. Deselect this option to

log a record of each separate file that is part of a Web page request, including images and advertisements. This results in more precise reports, but creates a much larger database and causes reports to generate more slowly.

Consolidate requests: Enable this option to combine Internet requests that share the same value for all of the following elements, within a certain interval of time (1 minute, by default):

- Domain name (for example: www.websense.com)
- Category
- Keyword
- Action (for example: Category Blocked)
- User/workstation

12. On the **Filtering Feedback** screen, select whether you want Websense software to send feedback to Websense, Inc. to improve accuracy and then click **Next**.

    Choosing to allow feedback to Websense, Inc. helps improve the accuracy of Websense software for all customers. The feedback consists of any URLs that could not be categorized by Websense software. Such uncategorized URLs are evaluated by Websense, Inc. If warranted, they are investigated in more detail and put into an appropriate category. The Websense Master Database is updated with this information. When your Websense software downloads the updated database, it will be able to categorize those URLs and filter them according to the policies you have set.

    Important

    No information about users or your network is collected. The information is only about the visited URLs themselves. Only uncategorized URLs and the frequency of requests to them are collected. Uncategorized intranet URLs are not included in feedback.

    Note

    You can later choose to enable or disable feedback (the feedback mechanism is known as WebCatcher) using the Log Server Configuration utility. For more information, see Log Server Configuration Help.

13. On the **Transparent User Identification** screen, select whether to use Websense transparent identification agents to identify users and then click **Next**. This allows Websense software to apply user- or group-based filtering policies without prompting users for logon information.

    If Websense software is integrated with a third-party product (firewall, proxy server, cache, or network appliance) providing user authentication, a transparent identification agent may not be necessary. For more information, see the Websense installation supplement for your integration product.

To transparently identify remote users accessing the network via VPN, use Websense RADIUS Agent. Later in this installation process, you will be given the option to install RADIUS Agent.

It is possible to run multiple instances of the same transparent identification agent, or certain combinations of different transparent identification agents, in a network. (Note, however, you cannot run both DC Agent and eDirectory Agent, or Logon Agent and eDirectory Agent, in the same network.) To install another instance of a transparent identification agent or a different transparent identification agent, run this installation program on the other machine and use the Custom installation type. For information about multiple instances or combinations of transparent identification agents, see the *Transparent Identification of Users* technical paper.

- **Use DC Agent to identify users logging on to Windows domains** (*Windows only*): This option installs Websense DC Agent on this machine. DC Agent queries domain controllers and client machines at preset intervals to identify users currently logged on.

  Note
  Do not use DC Agent in a network that already includes eDirectory Agent.

- **Use Logon Agent to identify users logging on to local machines**: This option installs Websense Logon Agent on this machine. Logon Agent identifies users as they log onto Windows domains. Logon Agent is for use with Windows-based client machines on a network that uses Active Directory or Windows NT Directory.

  To use Logon Agent, you must modify the Group Policy on domain controllers so it launches a logon application (LogonApp.exe) as part of the logon script. Client machines must use NTLM (v1 or v2) when authenticating users (NTLMv1 only, in the case of Windows Server 2008; see note below).

  Note
  Do not use Logon Agent in a network that already includes eDirectory Agent.

  Note
  If using Logon Agent with a Windows Server 2008 domain controller, client machines must be configured to use NTLMv1 when authenticating a user. To do this, modify the security policy so **Network security: LAN Manager authentication level** is set to **Send NTLM response only**. This can be done on each individual client machine by modifying the local security policy, or on all machines in a domain by modifying the security policy of a Group Policy Object.

- **Use both DC Agent and Logon Agent** (*Windows only*): This option installs both DC Agent and Logon Agent on this machine. Running both agents may increase the accuracy of identification in some networks. If DC Agent is unable to identify certain users (for example, if it is unable to communicate with a domain controller due to network bandwidth or security restrictions), they would still be identified by Logon Agent at log on.
- **Use eDirectory Agent to identify users logging on via Novell eDirectory Server**: This option installs eDirectory Agent on this machine. Use this agent for a network using Novell eDirectory. eDirectory Agent queries the eDirectory Server at preset intervals to identify users currently logged on.

> **Note**
> Do not use eDirectory Agent in a network that already includes DC Agent or Logon Agent.

- **Do not install a transparent identification agent now**: Select this option if
  - Websense software will be integrated with a third-party product that provides user authentication.
  - You plan to install a transparent identification agent on another machine.
  - You do not want different filtering policies applied to users or groups.
  - You want users to be prompted for logon information when they open a browser to access the Internet.

> **Note**
> When integrated with Cisco products, Websense software cannot use Cisco Secure Access Control Server (ACS) for user authentication for more than 1 user domain. If there are multiple user domains, use a transparent identification agent instead.

14. On the **Directory Service Access** screen, specify an account to be used by User Service, DC Agent, or Logon Agent for transparent identification.

> **Note**
> User Service is included in a typical installation (i.e., **Filtering and Management** or **Filtering, Management, and Reporting**), which is why this screen appears even if you have not chosen to install DC Agent or Logon Agent.

Enter the domain, user name, and password of an account that is a member of the Domain Admins group on the domain controller. This must be the domain controller for the users you wish to apply user- or group-based filtering policies to.

The user identification components User Service, DC Agent, or Logon Agent (if installed) use this account to query the domain controller for user information.

> **Note**
> User information on domain controllers trusted by the domain controller in question will also be accessible.

If you choose not to specify a Domain Admin account now (by leaving the fields blank), you can specify it after installation:

- On Linux, specify a Domain Admin account to be used by Users Service, TRITON - Web Security. For more information, see *Troubleshooting* > *User Identification* in TRITON - Web Security Help.
- On Windows, configure the Websense User Service, Websense DC Agent (if installed), and Websense Logon Agent (if installed) services to **Log on as** a Domain Admin user, using the Windows **Services** dialog box:
  a. Start the Windows **Services** dialog box (typically, **Start** > **Administrative Tools** > **Services**).
  b. Right-click Websense User Service and select **Properties**.
  c. In the service properties dialog box, select the **Log On** tab.
  d. Under **Log on as**, select **This account** and enter the domain\username and password (twice) of the trusted account you specified during installation.
  e. Click **OK**.
  f. A message appears informing you the account you specified has been granted the Log On As A Service right. Click **OK**.
  g. A message appears informing you the new logon name will not take effect until you stop and restart the service. Click **OK**.
  h. Click **OK** to exit the service properties dialog box.
  i. Right-click Websense User Service and select Restart.
  j. Repeat this procedure (from Step b) for Websense DC Agent and Websense Logon Agent, if they are installed.

15. On the **RADIUS Agent** screen, select **Install RADIUS Agent** if you have remote users that are authenticated by a RADIUS server and then click **Next**. This allows Websense software to apply user- or group-based filtering policies on these remote users without prompting for logon information.
16. On the **Installation Directory** screen, accept the default installation path, or click **Choose** to specify another path, and then click **Next**.

    The installation path must be absolute (not relative). The default installation path is:

    - **Windows**: C:\Program Files\Websense\
    - **Linux**: /opt/Websense/

The installer creates this directory if it does not exist.

> **Important**
> The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

The installer compares the installation's system requirements with the machine's resources.

- Insufficient disk space prompts an error message. The installer closes when you click **OK**.
- Insufficient RAM prompts a warning message. The installation continues when you click **OK**. To ensure optimal performance, increase your memory to the recommended amount.

17. On the **Pre-Installation Summary** screen, verify the information shown.

    The summary shows the installation path and size, and the components to be installed.

18. Click **Next** to start the installation. An **Installing** progress screen is displayed. Wait for the installation to complete.

> **Note**
> If you are using the command-line Linux installer, do **not** cancel (Ctrl-C) the installer after the **Pre-Installation Summary** screen, as it is installing components. In this case, allow the installation to complete and then uninstall the unwanted components.

19. On the **Installation Complete** screen, click **Done**.

    On Windows machines, when the installer finishes running, a Web page provides instructions for launching TRITON - Web Security.

20. If you stopped your antivirus software, restart it.
21. If you stopped a firewall running on a Linux machine, open a command shell and enter:

    ```
    service iptables start
    ```

    To determine whether the firewall is running, enter:

    ```
    service iptables status
    ```

22. If your network uses Active Directory 2008 to authenticate users, you must enable and start the Windows Computer Browser service on the Active Directory machine.

Installing hybrid and Web DLP components

Custom installation

Once you're done with the typical install, you need to run a custom installation to install the following hybrid and Web DLP components:

- **Websense Linking Service** - gives Data Security software access to Master Database categorization information and user and group information collected by User Service. Enables shared administrative access to TRITON - Web Security and Data Security modules. Linking Service can be installed only on Windows machines.
- **Websense Sync Service** - transports policy, reporting, and user/group data between the on-premises and hybrid systems.
- **Websense Directory Agent** - collects user and group information from Directory Server and collates it for hybrid filtering.

To install these components:

1. If no Websense components have been installed on this machine:
   a. On the **Introduction** screen, click **Next**.
   b. On the **Subscription Agreement** screen, choose to accept the terms of the agreement and then click **Next**.
   c. On the **Installation Type** screen, select **Custom** and then click **Next**.
2. If there are Websense components already installed on this machine, the **Add Components** screen appears.

   Select **Install additional components on this machine** and then click **Next**.
3. On the **Select Components** screen, select components to install and then click **Next**.
4. If you are installing on Windows Server 2008 (the screens mentioned here appear only if Windows Server 2008 is detected by the installation program):
   a. On the **Active Directory** screen, indicate whether you are using Active Directory to authenticate users in your network and then click **Next**.
   b. If you select **Yes**, the **Computer Browser Service** screen appears if the Computer Brower service is not currently running. Choose whether to start this service and then click **Next**.

The Computer Browser service is a Windows utility that must be set to Automatic and Start in the Windows Services dialog box for Websense components to communicate with Active Directory.

> **Note**
> If you choose to start the Computer Browser service now, make sure the Computer Browser service is enabled on this machine. In most cases, it is disabled by default. The installer will attempt to start the service and configure it to start up automatically from now on. If the service is disabled, the installer will be unable to start it.

If you choose not to have the installer start the service, or if the installer is unable to start it, you must start it manually after installation. If you use Active Directory 2008 to authenticate users, you must also start the Computer Browser service on the Active Directory machine.

If you choose not to have the installer start the service, or if the installer is unable to start it, you must start it manually after installation. If you use Active Directory 2008 to authenticate users, you must also start the Computer Browser service on the Active Directory machine.

5. See the following sections for component-specific installation instructions, and then return to this procedure.
   - *Linking Service*
   - *Sync Service*
   - *Directory Agent*

6. On the **Installation Directory** screen, accept the default installation path, or click **Choose** to specify another path, and then click **Next**.

   The installation path must be absolute (not relative). The default installation path is:

   - **Windows**: C:\Program Files\Websense\
   - **Linux**: /opt/Websense/

   The installer creates this directory if it does not exist.

   > **Important**
   > The full installation path must use only ASCII characters. Do not use extended ASCII or double-byte characters.

   The installer compares the installation's system requirements with the machine's resources.

   - Insufficient disk space prompts an error message. The installer closes when you click **OK**.
   - Insufficient RAM prompts a warning message. The installation continues when you click **OK**. To ensure optimal performance, increase your memory to the recommended amount.

7. On the **Pre-Installation Summary** screen, verify the information shown.

   The summary shows the installation path and size, and the components to be installed.

8. Click **Next** to start the installation. An **Installing** progress screen is displayed. Wait for the installation to complete.

   > **Note**
   > If you are using the command-line Linux installer, do **not** cancel (Ctrl-C) the installer after the **Pre-Installation Summary** screen, as it is installing components. In this case, allow the installation to complete and then uninstall the unwanted components.

9. If you chose to install the ISA Server filtering plug-in, the **Stop Microsoft Firewall Service** screen appears. Do the following:

a. Stop the Microsoft Firewall service and then click **Next**.

> **Note**
> Leave the Websense installer running as you stop the Microsoft Firewall service. Then return to the installer and click **Next** to continue installation.

> **Important**
> In order to correctly install the ISA Server filtering plug-in, the Microsoft Firewall Service must be stopped. Installation of the plug-in files and registration of the plug-in in the system registry cannot occur while the Microsoft Firewall Service has certain files locked. Stopping the Microsoft Firewall Service unlocks these files.

To stop the Firewall service, go to the Windows Services management console (**Administrative Tools > Services)**. Right-click Microsoft Firewall, and then select **Stop**. When the service has stopped, return to the Websense installer and continue the installation process. The Firewall Service may also be stopped from the ISA Server Management console or Command Prompt (using the command `net stop fwsrv`). See Microsoft's documentation for more information.

> **Important**
> When the Microsoft Firewall service is stopped, ISA Server goes into lockdown mode. Depending on your network configuration, network traffic may be stopped. Typically, the Firewall service needs to be stopped for only a few minutes as the ISA Server filtering plug-in is installed and configured.

b. When the following message appears, start the Microsoft Firewall service and then click **OK**:

The Websense ISAPI Filter has been configured, you can now start the Microsoft Firewall Service.

To start the Firewall service, go to the Windows Services management console (**Administrative Tools > Services)**. Right-click Microsoft Firewall, and then select **Start**.The Firewall Service may also be started from the ISA Server Management console or Command Prompt (using the command `net start fwsrv`). See Microsoft's documentation for more information.

10. On the **Installation Complete** screen, click **Done**.

    If you stopped your antivirus software, restart it.

11. If you stopped a firewall running on a Linux machine, open a command shell and enter:

```
service iptables start
```

To determine whether the firewall is running, enter:

```
service iptables status
```

12. If your network uses Active Directory 2008 to authenticate users, you must enable and start the Windows Computer Browser service on the Active Directory machine.

Linking Service

Websense Linking Service makes it possible for Websense Data Security to access user information and URL categorization details from Websense Web Security.

When installing Linking Service separately, be sure that Filtering Service, User Service, and a transparent identification agent (DC Agent, Logon Agent, or RADIUS Agent) are already installed and running.

When Linking Service is selected, the following screens appear during installation:

- **Policy Server Connection**

  This screen appears if Policy Server is not found on this machine and is not selected for installation at the same time as Linking Service. It is assumed Policy Server is installed on another machine. Enter the IP address of the machine and the port Policy Server uses to communicate with other Websense components (default is 55806).

  The port used by Policy Server to communicate with other Websense components must be in the range 1024-65535. Policy Server may have been automatically configured to use a port other than the default 55806. When Policy Server is installed, if the installation program finds the default port to be in use, it is automatically incremented until a free port is found. To determine what port is used by Policy Server, check the `websense.ini` file—located in `C:\Program Files\Websense\bin` (Windows) or `/opt/Websense/bin` (Linux)—on the Policy Server machine. In this file, look for the **PolicyServerPort** value.

  Important

  Do not modify the `websense.ini` file.

  If Policy Server is not installed yet, anywhere in your network, you must install it before installing Linking Service. To install it on this machine, click **Previous** and select **Policy Server** in addition to **Linking Service**. To install it on another machine, run this installation program on that machine (prior to installing components on this machine).

- **Filtering Service Communication**

Enter the IP address of the machine on which Filtering Service is installed and the port Filtering Service uses to communicate with integration products and Network Agent (default is 15868). If Filtering Service is installed on this machine, enter the IP address of this machine (note: actual IP address, not the loopback address, 127.0.0.1)

Note

The port used by Filtering Service to communicate with integration products and Network Agent must be in the range 1024-65535. Filtering Service may have been automatically configured to use a port other than the default 15868. When Filtering Service is installed, if the installation program finds the default port to be in use, it is automatically incremented until a free port is found. To determine what port is used by Filtering Service, check the `eimserver.ini` file—located in `C:\Program Files\Websense\bin` (Windows) or `/opt/Websense/bin` (Linux)—on the Filtering Service machine. In this file, look for the **WebsenseServerPort** value.

Important: Do not modify the `eimserver.ini` file.

If Filtering Service is not installed yet, anywhere in your network, you must install it before installing Linking Service. To install it on this machine, click **Previous** and select **Filtering Service** in addition to already selected components. To install it on another machine, run this installation program on that machine (prior to installing Linking Service on this machine).

Sync Service

Sync Service communicates policy and reporting data to the hybrid service. To install Sync Service, Policy Server must already be installed on this machine or a networked machine. Typically, Sync Service is installed on the same machine as Log Server.

Important

There must be only one instance of Sync Service in an entire deployment of Websense Web Security Gateway Anywhere. See the Deployment Guide for Websense Web Security Solutions for more information.

> **Note**
>
> If you have a distributed logging deployment (e.g., central office with Log Server and Log Database, branch offices with their own instances of Log Server that send data to the central office) be sure to install Sync Service so it communicates with the central Log Server instance and not one of the branch instances. Hybrid logging data cannot be passed to the central Log Server instance by branch instances.

When Sync Service is selected, the following screens appear during installation:

- **Policy Server Connection**

  This screen appears if Policy Server is not found on this machine and is not currently selected for installation. It is assumed Policy Server is installed on another machine. Enter the IP address of the machine and the port Policy Server uses to communicate with other Websense components (default is 55806).

  The port used by Policy Server to communicate with other Websense components must be in the range 1024-65535. Policy Server may have been automatically configured to use a port other than the default 55806. When Policy Server is installed, if the installation program finds the default port to be in use, it is automatically incremented until a free port is found. To determine what port is used by Policy Server, check the `websense.ini` file—located in `C:\Program Files\Websense\bin` (Windows) or `/opt/Websense/bin` (Linux)—on the Policy Server machine. In this file, look for the **PolicyServerPort** value.

  > **Important**
  >
  > Do not modify the `websense.ini` file.

  If Policy Server is not installed yet, anywhere in your network, you must install it before installing Sync Service. To install it on this machine, click **Previous** and select **Policy Server** in addition to already selected components. To install it on another machine, run this installation program on that machine (prior to installing components on this machine).

- **Policy Broker Connection**

  This screen appears if Policy Broker is not found on this machine and not currently selected for installation. It is assumed Policy Broker is installed on another machine. Enter the IP address of the machine and the port Policy Broker uses to communicate with other Websense components (default is 55880).

  The configuration port must be in the range 1024-65535. Policy Broker may have been automatically configured to use a port other than the default 55880 for communication with other Websense components. When Policy Broker is installed, if the installation program finds the default port to be in use, it is

automatically incremented until a free port is found. To determine what port is used by Policy Broker, check the `BrokerService.cfg` file—located in `C:\Program Files\Websense\bin` (Windows) or `/opt/Websense/bin` (Linux)—on the Policy Broker machine. In this file, look for the **listen_port** value.

Important

Do not modify the `BrokerService.cfg` file.

If Policy Broker is not installed yet, anywhere in your network, you must install it before installing Policy Server. To install it on this machine, click **Previous** and select **Policy Broker** in addition to already selected components. To install it on another machine, run this installation program on that machine (prior to installing components on this machine).

Important

There can be only one instance of Policy Broker in the entire deployment. Policy Broker must be installed first, before any other Websense component. If you select other components to install along with Policy Broker, they will be installed in the proper order.

Directory Agent

Directory Agent collates user and group information for use by the hybrid service. To install Directory Agent, Policy Server must already be installed on this machine or a networked machine.

Typically, only one instance of Directory Agent should be installed in an entire deployment. It is possible, however, to install multiple Directory Agent instances but specific configuration is necessary for them to operate properly. For more information see the TRITON - Web Security Help.

Important

If you are installing components as part of a Websense Web Security Gateway Anywhere deployment with a V-Series appliance, you typically should not install Directory Agent on a separate machine. Directory Agent is already installed on the appliance.

When Directory Agent is selected, the following screen appears during installation:

- **Policy Server Connection**

This screen appears if Policy Server is not found on this machine and is not currently selected for installation. It is assumed Policy Server is installed on another machine. Enter the IP address of the machine and the port Policy Server uses to communicate with other Websense components (default is 55806).

The port used by Policy Server to communicate with other Websense components must be in the range 1024-65535. Policy Server may have been automatically configured to use a port other than the default 55806. When Policy Server is installed, if the installation program finds the default port to be in use, it is automatically incremented until a free port is found. To determine what port is used by Policy Server, check the `websense.ini` file—located in `C:\Program Files\Websense\bin` (Windows) or `/opt/Websense/bin` (Linux)—on the Policy Server machine. In this file, look for the **PolicyServerPort** value.

Important

Do not modify the `websense.ini` file.

If Policy Server is not installed yet, anywhere in your network, you must install it before installing Directory Agent. To install it on this machine, click **Previous** and select **Policy Server** in addition to already selected components. To install it on another machine, run this installation program on that machine (prior to installing components on this machine).

Installing Websense Content Gateway

Following are instructions for installing Websense Content Gateway in Web Security Gateway Anywhere mode. For additional information, refer to the *Websense Content Gateway Installation Guide*.

Note that Websense Content Gateway has a native integration with Websense Data Security. A Data Security policy engine is built into Websense Content Gateway, but is installed in a dormant and unregistered state.

Hardware and software requirements

Hardware

CPU	Quad-core running at 2.8 GHz or faster
Memory	4 GB
Disk space	2 disks: • 100 GB for the operating system, Websense Content Gateway, and temporary data.

- 147 GB for caching
  If caching will not be used, this disk is not required.
  The caching disk:
  - Should have minimum size of 2 GB, maximum 147 GB for optimal performance
  - Must be a raw disk, not a mounted file system
  - Must be dedicated
  - Must *not* be part of a software RAID
  - For best performance, use a 10K RPM SAS disk on a controller that has at least 64MB of write-through cache.

Network Interfaces 2

To support transparent proxy deployments:

Router	WCCP v1 routers support redirection of HTTP only. If your deployment requires additional protocols, such as HTTPS, your router must support WCCP v2. A Cisco router must run IOS 12.2 or later. The clients, the destination Web server, and Websense Content Gateway must reside on different subnets.
—*or*—	
Layer 4 switch	You may use a Layer 4 switch rather than a router. To support WCCP, a Cisco switch requires the EMI or IP services image of the 12.2SE IOS release (or later). Websense Content Gateway must be Layer 2 adjacent to the switch. The switch must be able to rewrite the destination MAC address of frames traversing the switch. The switch must be able to match traffic based on the layer 4 protocol port (i.e., TCP port 80).

Software

Linux operating system:

- Red Hat Enterprise Linux 5, update 3 or later, base or Advanced Platform (32-bit only)
  - Only kernels shipped with the above Linux versions are supported by Websense Content Gateway. Visit www.redhat.com for kernel information. To display the kernel version installed on your system, enter the command:
    ```
    /bin/uname -r
    ```

Important

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

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

    ```
    rpm -qa |grep compat-libstdc
    ```
- GNU C library (glibc) version 2.5-42 or later
  - Note that Red Hat Enterprise Linux 5, update 3 ships with glibc version 2.5-34. Be sure to update it to version 2.5-42 or later.
  - Example command to update this library (running as `root`): `yum update glibc`.

Supported browsers:

- Websense Content Gateway is configured and maintained with a Web-based user interface called the Content Gateway Manager. Supported browsers include:
  - Internet Explorer 7 or 8
  - Mozilla Firefox 3.0.x - 3.5.x

Downloading the software

1. Download the installer tar archive to a temporary directory.

   Go to the Websense Knowledge Base, log in to the Web Security Gateway area, and search for the article titled *v7: Accessing Websense Content Gateway downloads*.
2. Create a directory for the tar archive, and then move the archive to the new directory. For example:

   ```
   mkdir wcg_v75
   mv <installer tar archive> wcg_v75
   ```
3. Change to the directory you created in Step 2.

   ```
   cd wcg_v75
   ```
4. Unpack the tar archive:

   `tar -xvzf` *`<installer tar archive>`*

Installing the software

Use the following procedure to install the software.

Note

Up to the configuration summary (Step 16 below), you can quit the installer by pressing CTRL-C. The installation will be cancelled. If you choose to continue the installation past the configuration summary and you want to quit, do **not** use CTRL-C. Instead, allow the installation to complete and then uninstall it.

If you want to change your answer to any of the installer prompts, you will be given a chance to start over at the first prompt once you reach the configuration summary; you do not have to quit the installer.

Important

If SELinux is enabled, disable it before installing Websense Content Gateway. Do not install or run Websense Content Gateway with SELinux enabled.

1. Make sure you have root permissions:

   ```
   su root
   ```

2. In the directory where you unpacked the tar archive, begin the installation, and respond to the prompts to configure the application.

   ```
   ./wcg_install.sh
   ```

3. If your system does not meet the minimum recommended requirements, you receive a warning. For example:

   ```
   Warning: Websense Content Gateway requires at least 2
   gigabytes of RAM.

   Do you wish to continue [y/n]?
   ```

   Enter **n** to end the installation, and return to the system prompt.

   Enter **y** to continue the installation. If you choose to run Websense Content Gateway after receiving a warning, performance may be affected

4. If you choose to continue, accept the subscription agreement. If you do not accept the subscription agreement, the installation stops.

   ```
   Do you accept the above agreement [y/n]? y
   ```

5. Specify the full path to the Websense Content Gateway installation directory. The default is **/opt/WCG**. Press **Enter** to accept the default.

   ```
   Enter the full path of the directory to install Websense
   Content Gateway: [/opt/WCG]
   ```

6. Enter and confirm the password for the administrator account. This account enables you to log on to the management interface for Websense Content Gateway, known as Content Gateway Manager. The default username is **admin**.

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

   ```
   Enter the administrator password for the Websense Content
   Gateway management interface.
   Username: admin
   Password:> (your password does not appear)
   Confirm password:> (your password does not appear)
   ```

   Important

   The password length must be 16 characters or less. Also, it cannot contain the following characters:

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

   Note

   As you type a password, the cursor does not move and masked characters are not shown. After typing a password, press **Enter**. Then repeat to confirm it.

7. Enter an email address where Websense Content Gateway can send alarm messages. Be sure to use @ notation. Do not enter more than 64 characters for this address.

   ```
   Websense Content Gateway requires an email address for alarm
   notification.
   Enter an email address using @ notation: [] > user@corp.com
   ```

8. Enter the IP address for Policy Server. Use dot notation. Press **Enter** to leave this field blank if this Websense Content Gateway deployment is with Websense Data Security only.

   ```
   Enter the Policy Server IP address (leave blank if
   integrating with Data Security only): [] >xxx.xxx.xxx.xxx
   ```

9. Enter the IP address for Filtering Service.The default is the same address as Policy Server. This field does not appear if you did not enter an IP address for Policy Server in Step 8.

   ```
   Enter the Filtering Service IP address: [xxx.xxx.xxx.xxx] >
   ```

10. Websense Content Gateway uses 13 ports on your server. Review a listing of these ports to determine if you will encounter any port conflicts.

    Ports preceded by numbers in the list are considered the 9 ports for Websense Content Gateway. Ports preceded by letters are needed if you have subscribed to Websense Web Security Gateway or Web Security Gateway Anywhere.

```
Current port assignments:
-------------------------------------------
'1'  Websense Content Gateway Proxy Port  8080
'2'  Web Interface port                   8081
'3'  Overseer port                        8082
'4'  Auto config port                     8083
'5'  Process manager port                 8084
'6'  Logging server port                  8085
'7'  Clustering port                      8086
'8'  Reliable service port                8087
'9'  Multicast port                       8088
'E'  HTTPS inbound port                   8070
'N'  HTTPS outbound port                  8090
'M'  HTTPS management port                8071
'D'  Download Service port                30900
```

11. If you do not want to use these ports for Content Gateway, or if the installation program indicates that a port conflict exists, indicate any necessary changes. Any new port numbers you assign must be between 1025 and 65535, inclusive. The default is that no changes are required. It is a best practice to accept the default port assignments unless a port conflict exists.

```
Enter the port assignment you would like to change:
'1-9,E,M,N,D' - specific port changes
'X'   - no change
'H'   - help
[X] >
```

12. If only one network interface is detected, the installation script indicates that two are required for clustering and prompts you to continue the installation.

    Otherwise, enter the number that represents your clustering environment.

```
'1' - Select '1' to configure Websense Content Gateway
        for full clustering. The nodes in the cluster will
        act as a single aggregate cache, including the
        functionality of a management cluster.
'2' - Select '2' to configure Websense Content Gateway
        for management clustering. The nodes in the cluster
        will share configuration/management information
        automatically.
'3' - Select '3' to operate this Websense Content Gateway
        as a single node.

Enter the cluster type for this Websense Content Gateway
installation:
```

```
[3] > 3
```

13. If you select 1 or 2, provide information about the cluster. Note that the listed interfaces are examples.

```
Enter the cluster type of this Websense Content Gateway
installation:
[3] >1
Enter the name of this Websense Content Gateway cluster.
>cluster_name

Enter a network interface for cluster communication.
Available interfaces:
eth0
eth1
Enter the desired cluster network interface:
>eth0

Enter a multicast group address for cluster cluster0.
Address must be in the range 224.0.1.27 - 224.0.1.254:
[224.0.1.37] >
```

14. Provide information about cache disks. If no raw disks are detected, Websense Content Gateway runs in proxy-only mode, and no Web pages are cached.

> **Note**
> If you choose to not enable raw disk cache now, cache disks may be added after Content Gateway has been installed. For instructions, search the Websense Security Gateway Knowledge Base for *Adding cache disks after installation*.

```
Would you like to enable raw disk cache [y/n]? y
```

a. Select available disks from the list. Selected disks become dedicated cache disks and cannot be used for any other purpose. Cache disks must be raw. Aggregate disk cache size should not exceed 147 GB.

```
Select available disk resources to use for the cache.
Remember that space used for the cache cannot be used for
any other purpose.

Here are the available drives
(1) /dev/sdb 146778685440 0x0
```

Note: The above drive is only an example.

> **Warning**
> Although it might be listed as available, do **not** use an LVM (Logical Volume Manager) volume as a cache disk.

b. Indicate if you want to add or remove disks individually or as a group.

```
Choose one of the following options:
'A'   - Add disk(s) to cache
'R'   - Remove disk(s) from cache
'S'   - Add all available disks to cache
'U'   - Remove all disks from cache
'X'   - Done with selection, continue Websense
        Content Gateway installation.

Option: > A
[ ] (1) /dev/sdb 146778685440 0x0
```

c. Specify which disk(s) to use for the cache.

```
Enter number to add item, press 'F' when finished:
[F] >1
Item '1' is selected
[F] >
```

d. Your selections are confirmed. Note the "x" before the name of the disk.

```
Here is the current selection
[X] (1) /dev/sdb 146778685440 0x0
```

e. Continue based on your choice in Step b, pressing **X** when you have finished configuring cache disks.

```
Choose one of the following options:
'A'   - Add disk(s) to cache
'R'   - Remove disk(s) from cache
'S'   - Add all available disks to cache
'U'   - Remove all disks from cache
'X'   - Done with selection, continue Websense
        Content Gateway installation.

Option: >X
```

15. You can elect to send Websense, Inc., information about scanned content. Individual users are never identified.

```
Websense Content Gateway can send information about scanned
content to Websense, Inc. This information helps Websense,
Inc. improve filtering and scanning technology and accuracy.

Websense software never includes information that would
identify specific users.

Do you want to enable the Websense Content Gateway Feedback
Agent [y/n]?
```

16. You are then shown the configuration options you entered, and prompted to complete the installation.

```
Configuration Summary
```

```
------------------------------------------------------------
Websense Content Gateway Install Directory : /opt/WCG
Admin Username for Content Gateway Manager: admin
Alarm Email Address                        : user@corp.com

Policy Server IP Address                   : 11.222.33.44
Filtering Service IP Address               : 11.222.33.44

Websense Content Gateway Cluster Type      : NO_CLUSTER

Websense Content Gateway Cache Type        : LRAW_DISK
  Cache Disk                               : /dev/sdb
  Total Cache Partition Used               : 1

                  ******************
                  *  W A R N I N G  *
                  ******************
    CACHE DISKS LISTED ABOVE WILL BE CLEARED DURING
    INSTALLATION!! CONTENTS OF THESE DISKS WILL BE
    COMPLETELY LOST WITH NO CHANCE OF RETRIEVAL.

    Installer CANNOT detect all potential disk mirroring
    systems. Please make sure the cache disks listed
    above are not in use as mirrors of active file
    systems and do not contain any useful data.

Do you want to continue installation with this configuration
[y/n]? y
```

If you want to make changes, enter **n** to restart the installation process at the first prompt. If the configuration is satisfactory, enter **y**.

> **Important**
>
> If you enter **y** to proceed but you decide you want to cancel the installation, do not attempt to quit the installer by pressing CTRL-C. Allow the installation to complete. Then uninstall it.

17. Wait for the installation to complete.

    Note the location of the certificate required for Content Gateway Manager: **/home/Websense/content_gateway_ca.cer**. See the Getting Started section of the Content Gateway Manager Help for information on importing this certificate.

    You may receive an email from Websense Content Gateway (to the address you specified during installation for receiving alerts) with “WCG license download failed” in the subject line. This does not mean a problem occurred with the installation; this alert is generated because a subscription key has not been entered yet. You will enter a key as part of post-installation tasks.

18. When installation is complete, reboot the Websense Content Gateway server.
19. Refer to Chapter 5: *Configuring the Content Gateway Module* for instructions on configuring Websense Content Gateway.

Installing Websense Data Security

In this section, you're instructed how to install the Data Security Management Server required for Web DLP. Websense Web Security Gateway Anywhere deployments do not make use of the Data Security Protector or any agents so none need to be installed or configured.

Refer to the *Websense Data Security Deployment Guide* for additional deployment and installation considerations.

Hardware and software requirements

Hardware

	Minimum Requirements	Recommended
CPU	2 Dual-core Intel Xeon processors (2.0 GHz) or AMD equivalent	2 Quad-core Intel Xeon processors (2.0 GHz) or AMD equivalent Note: The Management Server can **not** have more than 8 cores.
Memory	2 GB	4 GB
Hard drives	4 - 72 GB	4 - 146 GB
Disk space	144 GB	292 GB
Hardware RAID	1 + 0	1 + 0
NICs	1	2

Software

- Windows 2003 standard R2 edition with the latest SP.
- Windows installation requirements:
  - Set the partition to 1 NTFS Partition. For more information, see the Websense knowledge-base article: "File System Performance Optimization."
  - Regional Settings: should be set according to the primary location. If necessary, add supplemental language support and adjust the default language for non-Unicode programs.
  - Configure the network connection to have a static IP address.
  - Install the following Windows components by running **appwiz.cpl** from **Start > Run** and selecting **Add/Remove Windows Components**.
  - The Data Security Manager computer name must not include an underscore sign. Internet Explorer does not support such URLs.
- Application Server
  - ASP.NET

- Create a local administrator to be used as a service account.
- It's necessary to set the system time accurately on the server onto which you install the Data Security Server.

In addition, the Data Security Management Server requires the following to support the TRITON - Data Security user interface:

- Adobe Flash Player v8 or beyond

  This is required for the Data Security Today and System Health dashboards. All the other functions of TRITON - Data Security can operate without Flash.
- One of the following Web browsers:
  - Internet Explorer 7
  - Internet Explorer 8
  - Firefox 3.0.x - 3.5.x

If you have another browser or version, the user interface may behave in unexpected ways or report an error.

Domain considerations

The servers running the Data Security software can be set as part of a domain or as a separate workgroup. If you have multiple servers or want to perform run commands on file servers in response to discovery, we recommend you make the server(s) part of a domain.

However, strict GPOs may interfere and affect system performance, and even cause the system to halt. Hence, when putting Data Security servers into a domain, it is advised to make them part of organizational units that don't enforce strict GPOs.

Also, certain real-time antivirus scanning can downgrade system efficiency, but that can be relieved by excluding some directories from that scanning. Please contact Websense Technical Support for more information on enhancing performance.

Installing the software

1. Close all Windows programs on the management server before starting installation.
2. Synchronize your operating system time with the time on the TRITON - Web Security machine, or if you have a V-Series appliance, the time on the appliance.
3. Download the Websense Data Security installer package from mywebsense.com.
4. Unzip the installation package into the c:\websense directory. (If you choose a path with a longer name, problems may result.)

   There are several files in the package:
   - the msi installer file, **WebsenseDataSecurity75.msi**
   - the Oracle Database 10G folder
   - various other files and folders

5. Ensure that all of the installation folders, including the Database 10g folder, are in the same directory, at the same level as the **.msi** file.
6. Double-click the **WebsenseDataSecurity75.msi** file in the Websense Data Security directory..

   During the Data Security installation, the installer verifies that the .NET 2.0 server is installed. If not, it is installed.

   Follow the instructions on the screen. Click the **Next** button to proceed throughout the installation.
7. Read the license agreement carefully before selecting the "I accept the license agreement" radio button and clicking **Next** in order to proceed.
8. Select a folder on the server into which to install Data Security. By default, it's stored in C:\Program Files\Websense\Data Security.
9. For type of installation, select **Data Security Management Server** and click **Next**. (For Web Security Gateway Anywhere deployments, supplemental servers and agents are not required.)
10. Click **Next** on the Agent Selection screen. On the management server, no agents are required.
11. Click **Next** to continue with the installation process.
12. When prompted, click **OK** to indicate that services such as ASP.NET and SMTP are enabled.
13. On the Oracle Server Connection screen, indicate the location where you want the Data Security incident and policy database to be installed, and the credentials to use to access it. Browse to the location where the Oracle Table Space is to be stored.

    If a database is not already installed on the system, use the edit boxes on the bottom of the dialog box to define both the system and the SA passwords. The system account is a general master account for the database, while the SA account is an administrative account for the Data Security software.

    If, on the other hand, a database is already installed on the system (from a prior installation, for example), use the edit box on the left to enter the password for the system account, and the edit boxes on the right to define a password for the SA account.
14. The PreciseID Database Destination Folder screen enables you to set a destination location for the Data Security PreciseID database into which all fingerprints are stored. The PreciseID database stores and serves fingerprints to the Data Security application.
15. Enter the local administrator user name and password according to the instructions indicated.
16. If all the information entered is correct, click the **Install** button to begin installation.

    Installation may take a while. If the installation process is lengthy, do not assume that the installation has encountered an error unless a specific failure notification is displayed.

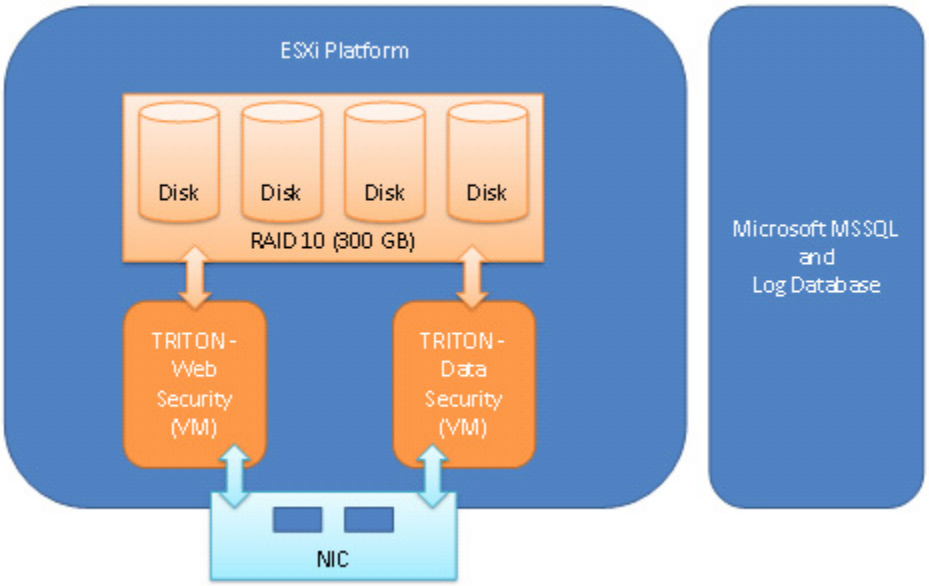
Once installation is complete, the Installation Successful screen appears to inform you that your installation is complete.

17. Refer to Chapter 6: *Configuring the Data Security Module* for instructions on configuring the Data Security module.

Installing on a virtual machine

With Websense Web Security Gateway Anywhere, you can install the Data Security Management Server and TRITON - Web Security on the same host on separate virtual machines (VMs).

The Data Security Management Server includes TRITON - Data Security and the Oracle database. TRITON - Web Security includes: Log Service, XID Agents, Linking Service, and Sync Service. Following is the standard profile:



The following VM platforms are supported. You can obtain them from the VMware site: *www.vmware.com*.

- VMware ESX 3.5i update 2
- VMware ESX 4i update 1

Note

While downloading ESXi, a license key is generated and displayed on the download page. Make a note of this license key for use during installation.

Before installing Websense modules on a VM via ESXi, ensure that your VMware tools are up to date. All of your hardware must be compatible with VMware ESXi. In addition, ensure that the following hardware specifications are met:

VMware Server	Requirements
CPU	• At least 4 cores 2.5 GHz (for example, 1 QuadXeon 2.5 GHz)
Disk	• 300 GB, 15 K RPM, RAID 10
Memory	• 8 GB
NICs	• 2*1000

VMware Infrastructure Client	Requirements
CPU	• At least 500 MHz
Disk storage	• 150 MB free disk space required for basic installation. • An additional 55 MB free on the destination drive during installation • 100 MB free on the drive containing the %temp% folder
Memory	• 512 MB
Networking	• Gigabit Ethernet recommended

Module	Requirements for VM installation
Data Security Management Server	• Windows Server 2003 Standard SP2 • 4 GB RAM • 150 GB Disk • 2 CPU cores
TRITON - Web Security machine	• Windows Server 2003 Standard SP2 • 2 GB RAM • 15 GB disk • 1 NIC (bridged) • 2 CPU cores (dedicated)

The steps for installing on a virtual machine are as follows:

- *Installing the ESXi platform*
- *Customizing ESXi*
- *Installing the VMware Client*
- *Installing the license and setting the time*
- *Configuring an additional NIC*

Installing the ESXi platform

To install ESXi:

1. Download the version of ESXi that you want to use from www.vmware.com.
2. Once the download is complete, burn the download file to a CD.
3. On the machine that will host your VMware server, insert the ESX Server CD into the CD drive
4. Set the BIOS to boot from the CD.
5. Follow the instructions in the installer to complete the installation process.
6. When the installation has finished, remove the CD and reboot the host machine.

Customizing ESXi

We recommend that you customize the ESXi platform as follows:

- Assign a password to the root account.
- Set up a management IP address for the ESXi server.

  By default the management IP address is dynamically obtained using DCHP. However, we recommend that you set up a static IP address.

To configure the ESXi platform:

1. Press **F2** to access the Customize System screen.
2. Select **Configure Password**, and enter a password for the root account.
3. To set up a static IP address, select the **Configure Management Network** menu.
4. Select **IP Configuration**, and on the screen that appears enter the following information:
   - Management IP address
   - Subnet mask
   - Default gateway
5. From the **Configure Management Network** menu, select **DNS Configuration**.
6. Configure static DNS information by entering the following:
   - Host name (fully qualified)
   - Primary and secondary DNS server addresses
7. Reboot the server.

Installing the VMware Client

> **Note**
> The VMware client for ESX 4i is called the vSphere Client. Although the instructions in this section refer to the VMware Infrastructure Client that is available with ESX 3.5i, all instructions also apply to the vSphere Client.

The VMware Infrastructure Client (VI Client) manages the ESXi platform. Install the client on a Windows machine with network access to the ESXi server.

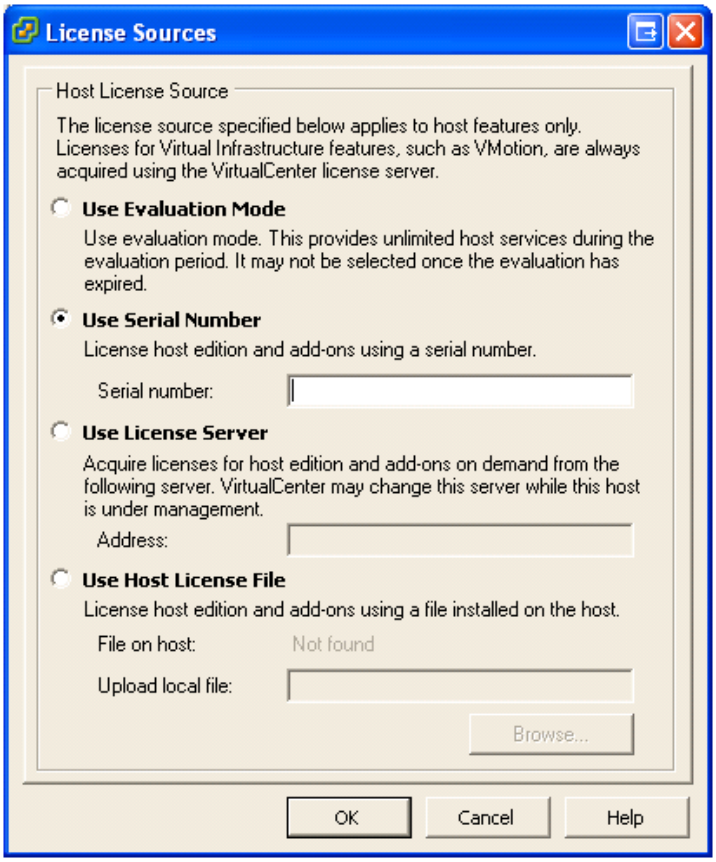
1. On the machine where you intend to install the client, open a browser and access the ESXi server using HTTPS and the management IP address you entered in the previous section (for example, https://10.15.21.100). If you see an error page, accept the server certificate.
2. On the VMware ESX Server Welcome page, click the **Download VMware Infrastructure Client** link.
3. Download and run the client installation program.

Installing the license and setting the time

You received your license number as part of the ESXi download.

1. Start the VI Client by selecting **Start > Programs > VMware > VMware Infrastructure Client**.
2. Connect to your ESXi server using the IP address you set up during configuration. For user credentials, enter the user name **root** and the password that you set up for the root account.
3. On the **Configuration** tab, select **Licensed Features**.

4. To the right of the **License Source** label, click the **edit** link.



5. Select **Use Serial Number**, and enter your license number in the field provided. Then click **OK**.
6. On the **Configuration** tab, select **Time Configuration**.
7. Select **Properties**, and then set your server's time. Click **OK** when done.

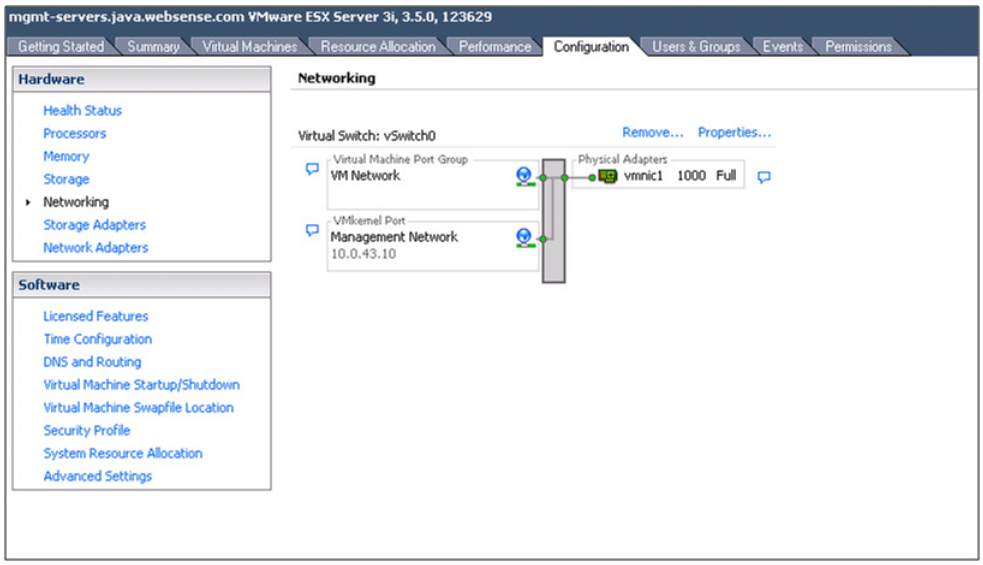
Configuring an additional NIC

When setting up the ESXi server, you configured one NIC as the ESXi platform management interface. This NIC can also be used by the virtual machines. However, this setup requires an additional NIC, for redundancy and to perform load balancing.

To set up an additional NIC:

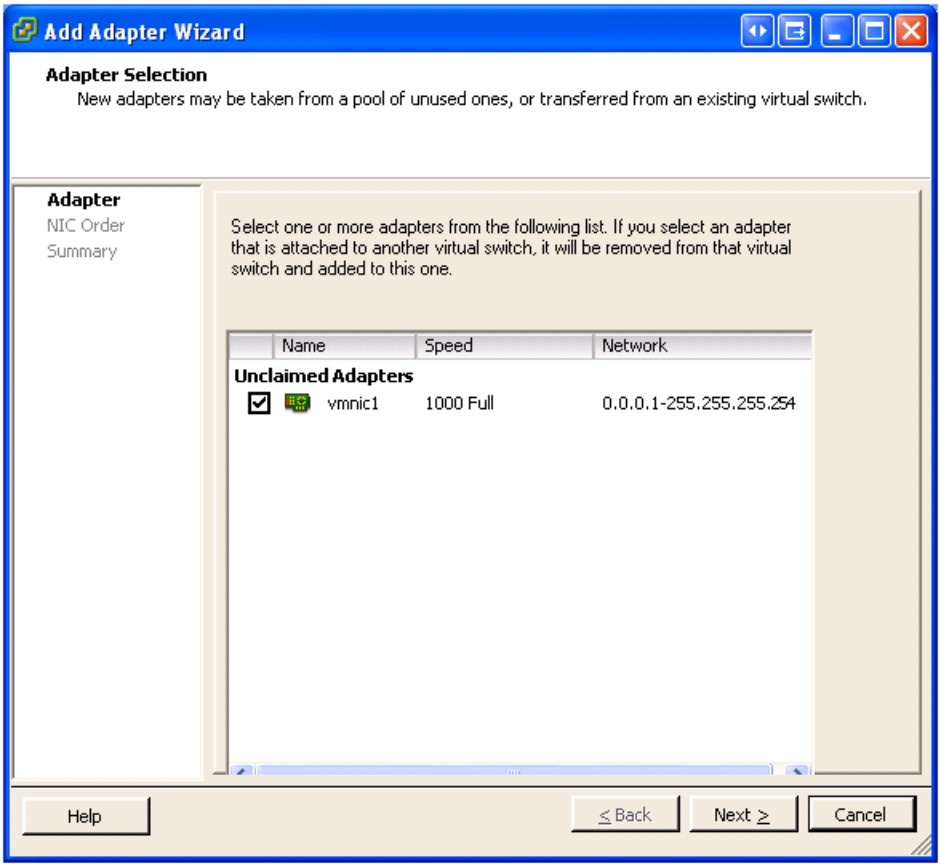
1. On the **Configuration** tab, select **Networking**.

When the system was started, the ESXi platform configured the server to have one virtual switch (vSwitch) using the management NIC. With this configuration, the Networking screen should look similar to the one below.



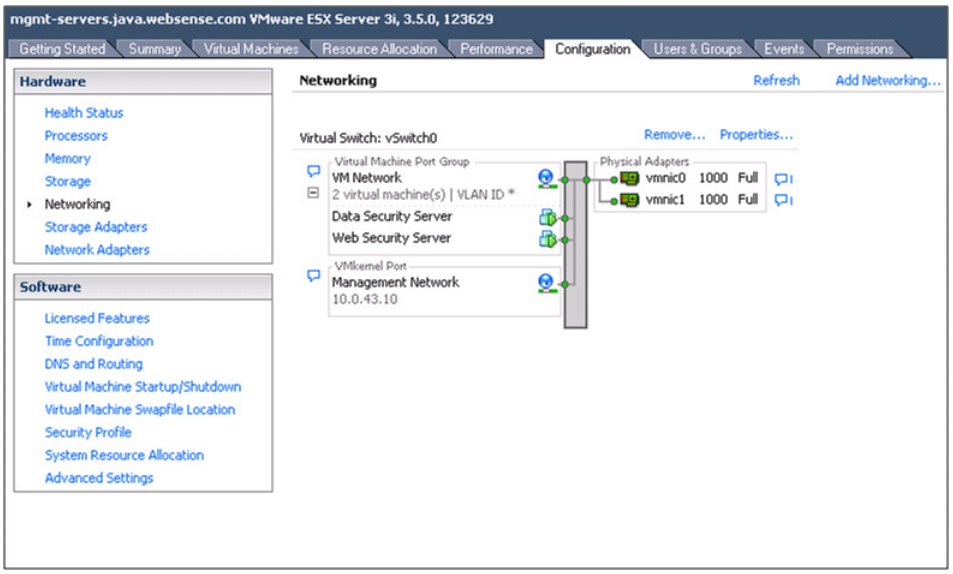
2. To add a new NIC to the virtual switch, select the **Properties** link.

3. In the Properties popup window, select the **Network Adapters** tab and click **Add**. The Add Adapter Wizard opens.



4. Select the adapter you want from the list, then click **Next** twice.
5. Click **Finish** to close the wizard, then close the Properties window.

After adding the additional network adapter to the virtual switch, the network layout should look similar to the one below:



Creating the virtual machines

This section describes how to create 2 virtual machines: one for the Data Security management server, and one for TRITON - Web Security.

Creating the Data Security virtual machine

1. In the VI Client, select the **Summary** tab and then select **New Virtual Machine**. The New Virtual Machine Wizard opens.
2. Select **Custom**, and click **Next**.
3. Set the machine name to be Data Security Server, and click **Next**.
4. Select the only available datastore (datastore1), and click **Next**.
5. Select Microsoft Windows as the guest operating system, and set the version to Microsoft Windows Server 2003, Standard Edition (32 bit). Then click **Next**.
6. Select 2 virtual processors, and click **Next**.
7. Set the virtual machine memory to 4096 MB (4 GB), and click **Next**.
8. Accept the defaults on the Network page and the I/O Adapters page, clicking **Next** to continue.
9. Select **Create a new virtual disk** and click **Next**.
10. Set the disk capacity to 150 GB.
11. Click **Next** to progress through the Advanced Options page without changing the defaults.
12. Review your configuration and then click **Finish**.

Setting the CPU affinity

Once you have configured the virtual machine, set its dedicated CPUs as follows:

1. In the VI Client, select the virtual machine you just created from the tree on the left.
2. Select the Summary view, and click **Edit Settings**.
3. Select the **Resources** tab.
4. Select **Advanced CPU**.
5. In the Scheduling Affinity group, select **Run on processor(s)**, then select processors zero and one.
6. Click **OK**.

Installing the operating system and VMware tools

Install the operating system on your virtual machine, and then reboot. We recommend that you also install the VMware tools before installing Data Security Manager. To do this:

1. Log on to the virtual machine.
2. From the VI Client, select **Inventory > Virtual Machine > Install/Upgrade VMware Tools**.
3. Follow the instructions on screen to install the tools.

Installing the Data Security management server

Follow the instructions earlier in this chapter to install Data Security. Note that you should install both the Data Security Server and Manager components.

Creating the TRITON - Web Security virtual machine

1. In the VI Client, select the **Summary** tab and then select **New Virtual Machine**. The New Virtual Machine Wizard opens.
2. Select **Custom**, and click **Next**.
3. Set the machine name to be Web Security Server, and click **Next**.
4. Select the only available datastore (datastore1), and click **Next**.
5. Select Microsoft Windows as the guest operating system, and set the version to Microsoft Windows Server 2003, Standard Edition (32 bit). Then click **Next**.
6. Select 2 virtual processors, and click **Next**.
7. Set the virtual machine memory to 2048 MB (2 GB), and click **Next**.
8. Accept the defaults on the Network page and the I/O Adapters page, clicking **Next** to continue.
9. Select **Create a new virtual disk** and click **Next**.
10. Set the disk capacity to 15 GB.
11. Click **Next** to progress through the Advanced Options page without changing the defaults.

12. Review your configuration and then click **Finish**.

Setting the CPU affinity

Once you have configured the virtual machine, set its dedicated CPUs as follows:

1. In the VI Client, select the virtual machine you just created from the tree on the left.
2. Select the Summary view, and click **Edit Settings**.
3. Select the **Resources** tab.
4. Select **Advanced CPU**.
5. In the Scheduling Affinity group, select **Run on processor(s)**, then select processors two and three.
6. Click **OK**.

Installing the operating system and VMware tools

Install the operating system on your virtual machine, and then reboot. We recommend that you also install the VMware tools before installing TRITON - Web Security. To do this:

1. Log on to the virtual machine.
2. From the VI Client, select **Inventory > Virtual Machine > Install/Upgrade VMware Tools**.

Follow the instructions on screen to install the tools.

Installing TRITON - Web Security

Follow the instructions in *Installing Websense Web Security*, page 34 to install TRITON - Web Security on your virtual machine.

4 Configuring the Web Security Module

This section describes how to perform basic configuration of the Web Security module so you can begin to use the hybrid filtering and Web DLP features.

Initial setup

The sections that follow guide you through the basic steps required to initialize the on-premises and hybrid filtering components of Websense Web Security Gateway Anywhere. Follow these steps to:

- Enter your subscription key and download the Websense Master Database
- Activate hybrid filtering
- Configure basic filtering account behaviors
- Enable communication between Web security components and your directory service
- Adapt the Default filtering policy for your organization

Further instructions for configuring hybrid filtering behavior are provided later in this chapter.

Logging on to TRITON - Web Security

Use the Web Security module of the TRITON Unified Security Center to customize filtering behavior, monitor Internet usage, generate Internet usage reports, and manage software configuration and settings for your Websense Web security software. This Web-based tool runs on the following fully supported browsers:

- Microsoft Internet Explorer 7 and 8 (not Compatibility View)
- Mozilla Firefox 3.0.x - 3.5.x

Tip

On Linux machines, for best results, use Firefox 3.5.x.

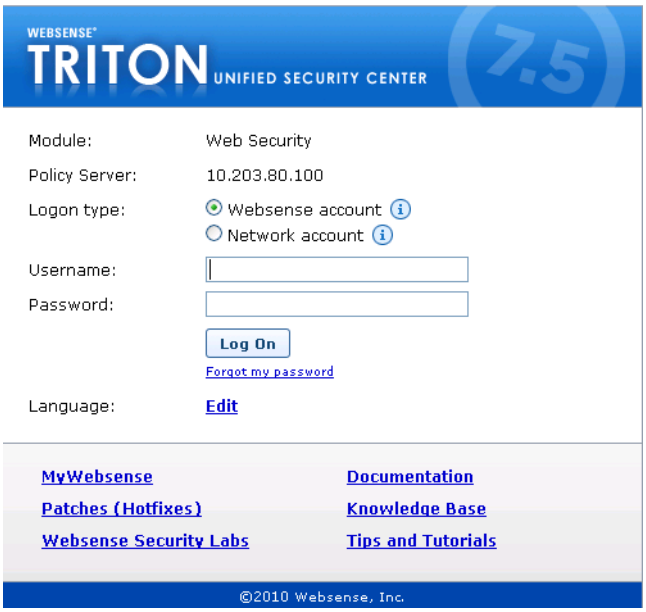
To launch TRITON - Web Security, do one of the following:

- From the appliance logon portal, click TRITON - Web Security.

- On Windows machines:
  - Go to **Start > Programs > Websense**, and then select **TRITON - Web Security**.
  - Double-click the TRITON - Web Security desktop icon.
- Open a supported browser on any machine in your network and enter the following:

  `https://<IP address>:9443/mng/`

  Substitute the IP address of the TRITON - Web Security machine.



An SSL connection is used for secure, browser-based communication with the TRITON Unified Security Center. This connection uses a security certificate issued by Websense, Inc. Because the supported browsers do not recognize Websense, Inc., as a known Certificate Authority, a certificate error is displayed the first time you launch TRITON from a new browser. To avoid seeing this error, you can install or permanently accept the certificate within the browser. See the Websense Knowledge Base for instructions.

After installation, the first user to log on to TRITON - Web Security has full administrative access. The user name is **WebsenseAdministrator**, and cannot be changed. The WebsenseAdministrator password is configured during installation.

To log on:

1. Select a **Policy Server** to manage.

   If your environment includes only one Policy Server, it is selected by default.
2. Under Account Type, select **Websense account** (default).

   You can later configure TRITON - Web Security to allow administrators to log on using their network credentials.

3. Enter the user name **WebsenseAdministrator**, and then enter the password created during installation.
4. Click **Log On**.

You are logged on to the Web Security module of the TRITON Unified Security Center and offered the option of launching a Quick Start tutorial.

If you are new to Websense software, or new to this version of Websense software, please consider completing a Quick Start tutorial once you have performed the initial configuration steps in this guide. You can uncheck the prompt if you do not want to see the tutorial again in the future.

Note

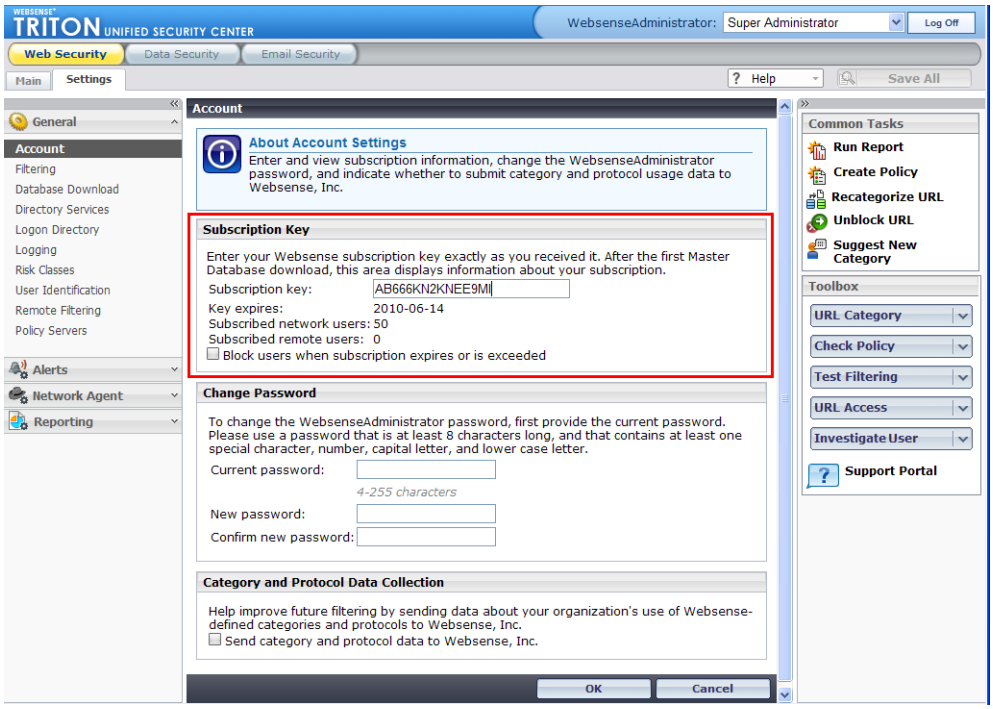
If you log onto TRITON - Web Security and configure linking before logging onto TRITON - Data Security—as described in this document—the password for TRITON - Web Security is automatically applied to the data security module.

Activating Websense Web Security Gateway Anywhere

In order to activate your Web security software, first enter your subscription key in TRITON - Web Security. This automatically initiates the process of downloading the Master Database, which contains the category and protocol information used in filtering Internet requests. Information included in this first database download also activates filtering and enables several TRITON - Web Security features.

1. In TRITON - Web Security, click the **Settings** tab of the left navigation pane.
2. Click the **Account** page (the first entry under General in the left navigation pane).
3. Enter your key in the **Subscription key** field.

   Once the key has been accepted and a Master Database download has occurred, this page will be updated to show the number of **Subscribed users** that can be filtered by any combination of on-premises components, remote filtering software, and hybrid filtering.

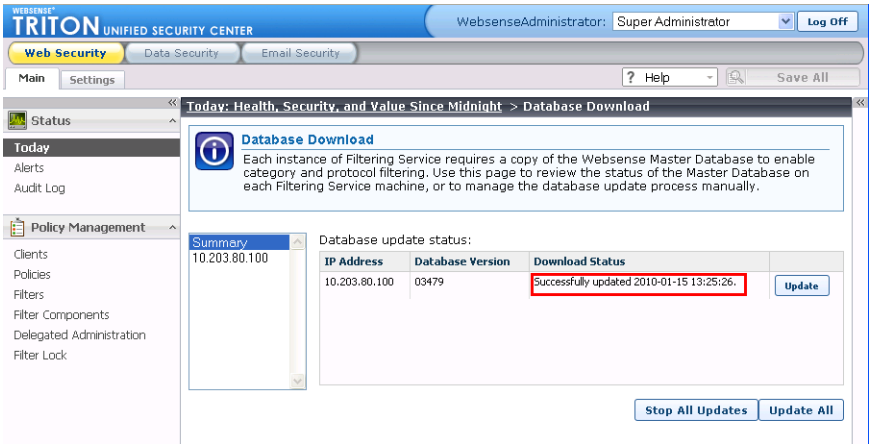


4. Click **OK**. The Master Database begins to download.
5. Do not perform any additional configuration until the Master Database download is complete. To monitor the download process, click the **Main** tab of the left navigation pane, go to the **Status > Today** page, and then click the **Database Download** button in the toolbar at the top of the content pane.
6. When the database download is complete, log off of TRITON - Web Security and then log back on.

Checking that the database download is completed

1. Select **Main > Status > Today**.
2. Click the **Database Download** button in the toolbar at the top of the content pane.

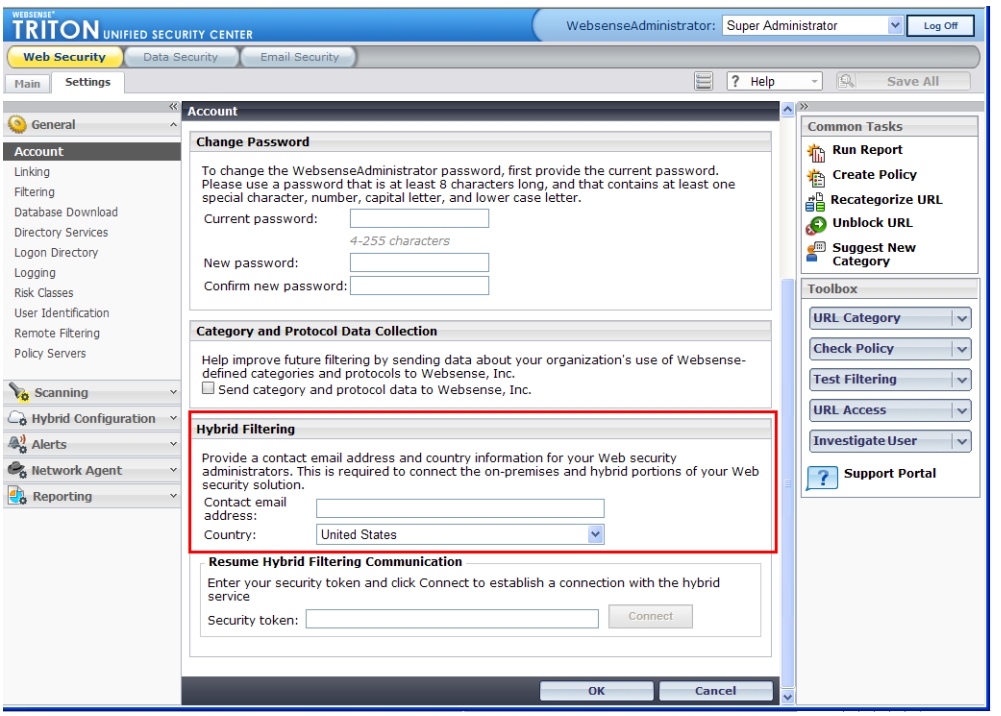
3. Verify that the database has successfully updated or that a download is in progress. (The download begins automatically when you install TRITON - Web Security.)



Activating hybrid filtering

After entering your subscription key and downloading the Master Database, provide the following information to activate hybrid filtering.

1. Go to the **Settings > General > Account** page in TRITON - Web Security. This is the same page you used to enter your subscription key.



2. Enter the **Contact email address** for your Web security administrators. This is typically a group email alias that is monitored frequently. Alerts about hybrid filtering issues are sent to this address. Failing to respond appropriately to an alert could lead to temporary disconnection of your hybrid service.

   Important

   This email address is not used to send marketing communications or other general information to your company. In the event that on-premises software loses its connection to the hybrid service, this email address must be active for you to reinitialize hybrid filtering.

   Users are not filtered by the hybrid service until this information has been provided and validated.

3. Select the **Country** where the majority of your filtering administrators and off-site users are located. This is used to select the hosted service that provides the most optimal performance.
4. When you are finished making changes, click **OK** to cache the changes, and then click **Save All**.

Configuring directory service settings

If your organization uses a supported directory service, you can configure Websense Web Security Gateway Anywhere to:

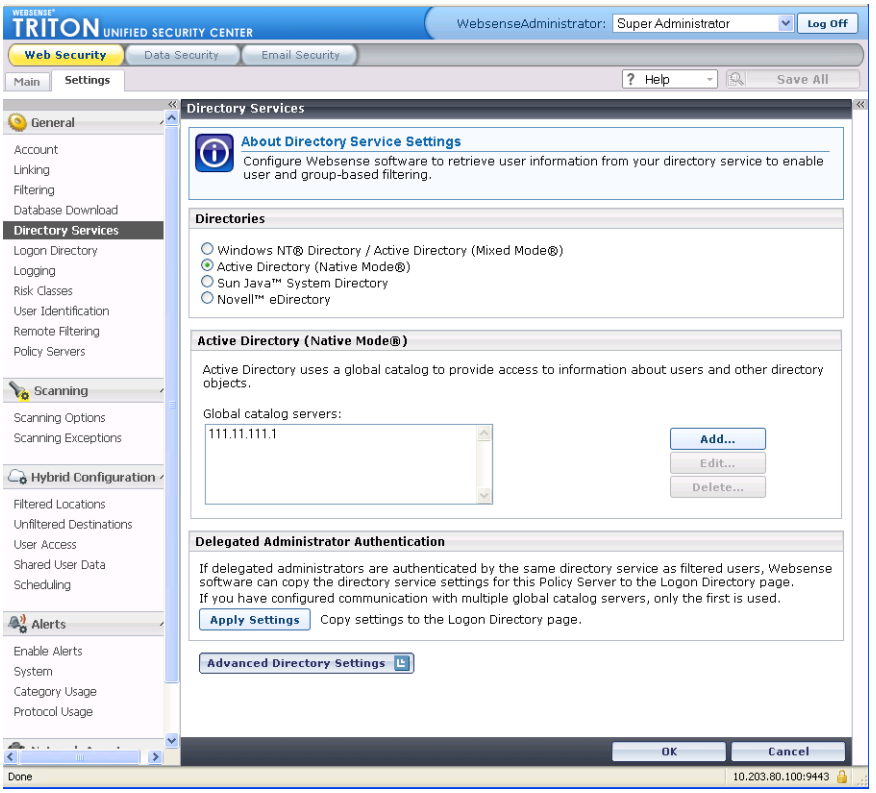
- Apply policies to directory clients (users, groups, and domains [OUs])
- Include information about directory clients in reports
- Allow administrators to log on to the TRITON Unified Security Center using their network accounts

The directory services supported by both on-premises components and the hybrid service are:

- Windows Active Directory (Native Mode)
- Novell eDirectory

To configure Websense software to communicate with your organization's directory service:

1. Go to the **Settings > General > Directory Service** page in TRITON - Web Security.



2. Select a supported directory service from the **Directories** list.

   Note that the default option—Windows NT Directory / Active Directory (Mixed Mode)—is not supported with hybrid filtering. Sun Java System Directory is also not supported. You can use these directory services to enable user and group-based filtering by on-premises components, but hybrid filtering will only be able to apply the Default policy or IP address-based policies.

3. See the appropriate section of the TRITON - Web Security Help for detailed instructions on completing your configuration. Go to the **Clients > Working with users and groups** topic, and then select the following subtopic:

   - Windows Active Directory (Native Mode)
   - Novell eDirectory and Sun Java System Directory

4. When you are finished making changes, click **OK** to cache them. Changes are not saved until you click Save All.

Editing the Default policy

Websense Web Security Gateway Anywhere uses policies to determine how and when Internet requests are filtered for *clients*: users, groups and domains (OUs) defined in a supported directory service, or IP addresses in your network.

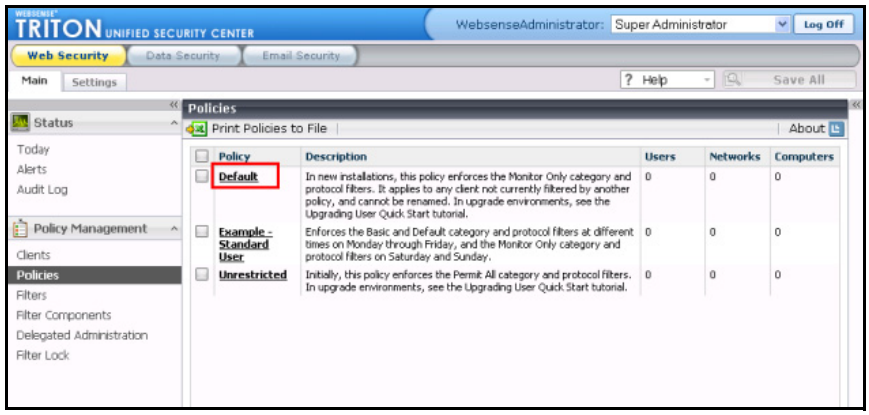
Each policy includes information about which Web sites and Internet communication protocols are blocked or permitted, and the days and times to enforce those rules.

Your Websense software includes a **Default** policy, in effect 24 hours a day, 7 days a week. Initially, this policy monitors Internet traffic without blocking. When you first install your Websense software, the Default policy applies to everyone in the network.

To review and edit the Default policy in TRITON - Web Security:

1. On the Main tab of the left navigation pane, under Policy Management, select **Policies**.

   A list of existing policies appears. In addition to the Default policy, there are 2 sample policies that you can use to learn how policies work.
2. Click **Default** to view policy details on the Edit Policy page.



3. Examine the area at the top of the content pane.
   - The policy name appears, followed by a short description of what the policy is intended to do.
   - A summary of the clients specifically governed by this policy is shown. Note that even if no clients are listed here, the **Default** policy applies to any client not currently governed by another policy.
4. Examine the **Schedule** box.
   - After a new installation, the Start, End, and Days columns show that the **Default** policy is in effect 24 hours a day, 7 days a week.
   - The Category / Limited Access Filter column shows that **Monitor Only** category filtering is in effect.

     A **category filter** is a list of categories and the actions (such as Permit or Block) assigned to them. The category filter enforced by a policy determines how user requests for Web sites are treated.

     The alternative to a category filter is a **limited access filter**, a list of specific Web sites (identified by URL or IP address) that users can access. When a limited access filter is enforced by a policy, users governed by the policy can access only sites on the list.
   - The Protocol Filter column shows that **Monitor Only** protocol filtering is in effect.

A **protocol filter** is a list of protocols (usually non-HTTP protocols) and the actions (such as Permit or Block) assigned to them. When Network Agent is installed, the protocol filter enforced by a policy determines how user attempts to access specific protocols (such as those used for instant messaging or peer-to-peer file sharing) are treated.

Note that hybrid filtering is applied only to HTTP, HTTPS, and in-browser FTP requests.

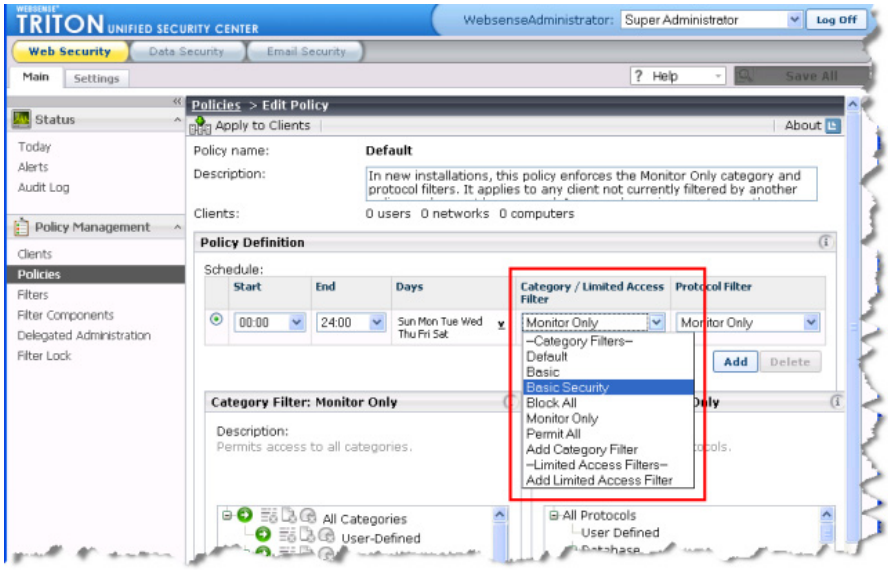
5. Two columns appear beneath the policy schedule. Examine the Category Filter column.
   - The name of the current category filter appears next to the column description.
   - You can scroll through the list to see which categories are permitted and blocked. A legend at the bottom of the page explains the icons that appear next to each category.

Because you have not configured the Content Gateway module, Internet requests are not yet being sent to Websense Web Security. If you would like an easy way to verify your filtering deployment once the other modules of Websense Web Security Gateway Anywhere have been configured, you can change the Default policy to use a category filter that blocks some sites.

As a first step, for example, you could configure the Default policy to enforce the **Basic Security** category filter. This category filter blocks sites in categories like Malicious Software and Phishing that present a security risk to your network.

To change the category filter enforced by the Default policy:

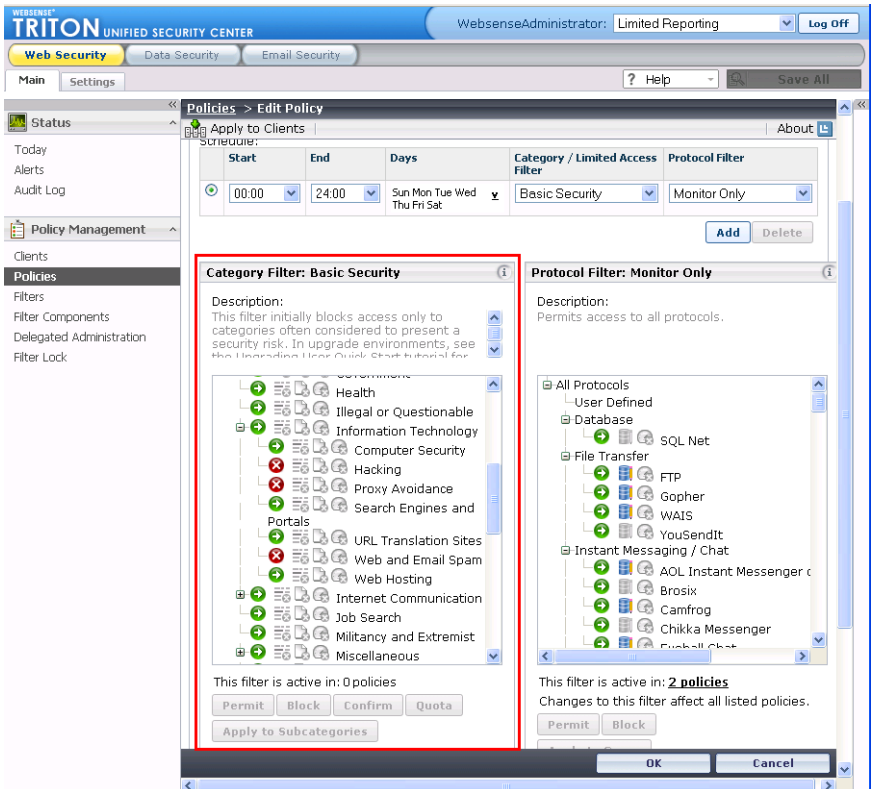
1. Under Policy Definition, open the Category / Limited Access Filter drop-down list.
2. Select a category filter, like **Basic Security**, from the --Category Filters-- portion of the list.



You can later refer to the New User Quick Start Tutorial or the TRITON - Web Security Help for detailed instructions to create your own category, protocol, and limited access filters; create custom policies; and apply different policies to different clients.

Note that if you select another category filter, like Default or Basic, many categories are blocked. The Basic Security category filter was chosen for this example because it increases network security without a large, immediate impact on end users' browsing experience.

3. Examine the Category Filter: Basic Security list in the bottom, left portion of the content pane.



- Expand the Security category to see some of the subcategories blocked by the new filter.
- Expand the Information Technology category to see additional subcategories blocked by the new filter.

4. If there is a category blocked that you believe should be permitted, select the category, and then click the **Permit** button just below the category tree.
5. When you are satisfied with your changes, click **OK**, and then click **Save All**.

Once you have configured the Content Gateway module, the basic filtering settings that you have established will be applied within your network.

In the Testing section of this guide, you will learn how to verify that filtering is being applied as expected.

Preparing for Web DLP

One of the key features of Websense Web Security Gateway Anywhere is that it includes Websense data security technologies to prevent data loss over the Web.

This means that you can protect whatever data you deem vital from leaving your organization by the Web—this includes HTTP, HTTPS, FTP, and FTP-over-HTTP.

For example, you may want to prevent employees from sending customer information to an FTP site where it can be retrieved by unauthorized users. Or you may be required to prevent social security numbers or credit card numbers from moving around your enterprise, even over secure HTTP. (Data compliance is a growing concern among enterprises across industries.)

Websense Web Security Gateway Anywhere provides such data loss prevention (DLP) capabilities. Depending on your needs, you can monitor or block the unwanted transmission of vital data, and you can send notifications and alerts when policy breaches occur.

In addition, you can create DLP policies that base rules on URL categories. For example, in TRITON - Data Security, you can define a rule that credit card numbers cannot be posted to known fraud sites.

You can also define rules based on users and computers rather than IP addresses. For example, Jane Doe cannot post financial information to FTP sites.

For those interested in monitoring email, removable media devices, printers, instant messages, or copy/paste operations for data loss, Websense Web Security Gateway Anywhere supports the following add-on modules:

- **Websense Data Monitor** - passive monitoring of business communications such as email, both external and internal.
- **Websense Data Protect** - active blocking of unauthorized data transmission.
- **Websense Data Discover** - discovery of all confidential information—on laptops, desktops, file servers, Exchange servers, and databases.
- **Websense Data Endpoint** - monitoring or blocking of endpoint computers for data loss. Protects removable media, LAN operations, and application operations. Includes local discovery.

This section describes how to enable DLP over Web channels. If you have a full subscription to Websense Data Security software, your steps are very similar.

Configuring linking between Web and data security

To get the full benefit of Web DLP, you need to configure linking between the Web and data security modules. *Linking* provides 2 benefits:

- It gives administrators access to TRITON - Web Security and TRITON - Data Security from the same unified console. (Identical administrator credentials must

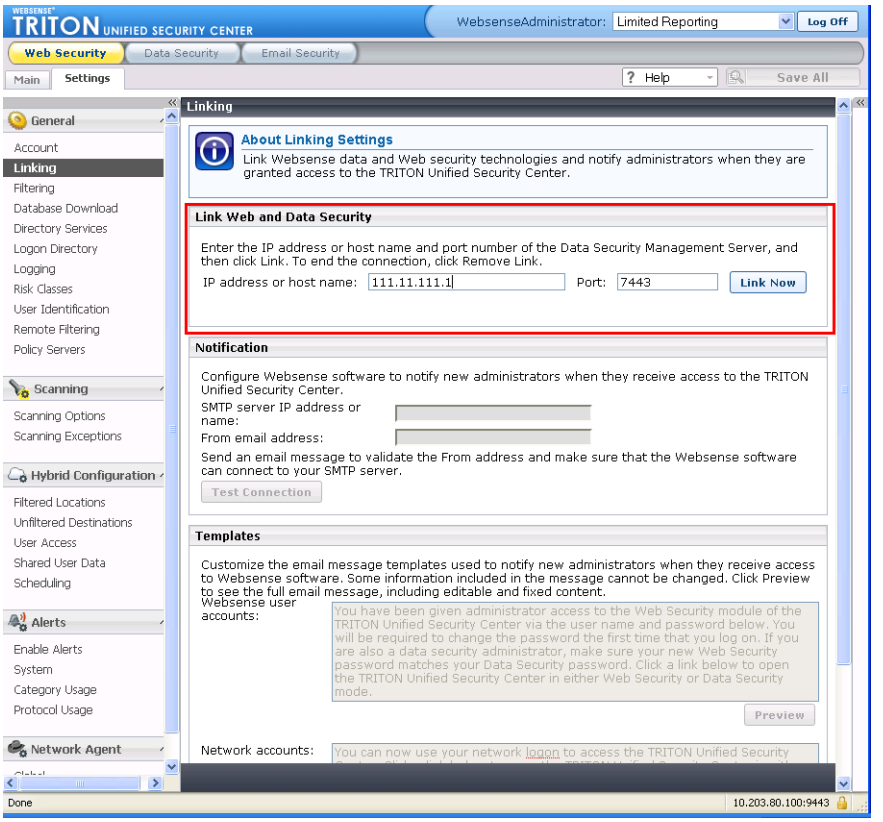
be configured in both managers for this to work. See *Creating a common administrator account*, page 96 for instructions.)

- Access to the *Websense Linking Service* that was installed on a Windows machine along with Web Security's other Windows-only components. The Websense Linking Service provides IP address to user name resolution for HTTP incidents. With this service, the Data Security module is able to display user names in incident reports rather than IP addresses.

  In addition, the Linking Service allows Data Security to import Web Security's preset and custom URL categories so you can add them as resources in your DLP policies.

To configure linking:

1. On the Settings tab of the left navigation pane, under General, select **Linking**.



2. Enter the **IP address** of the Data Security Management Server machine.
3. Enter the **Port** used for communication with Data Security Management Server (7443, by default).

4. Click **Link Now**. A message appears, indicating whether linking was successful. If linking failed, troubleshooting steps are suggested.

> **Note**
> Linking can also be configured in TRITON - Data Security, although this prevents the automatic transfer of the Web Security password to the data security module . To view the linking page in TRITON - Data Security, go to **Settings > System > Linking**.

The Websense Linking Service is enabled when linking succeeds. URL cateories are also imported from the Websense Master Database into the Data Security module.

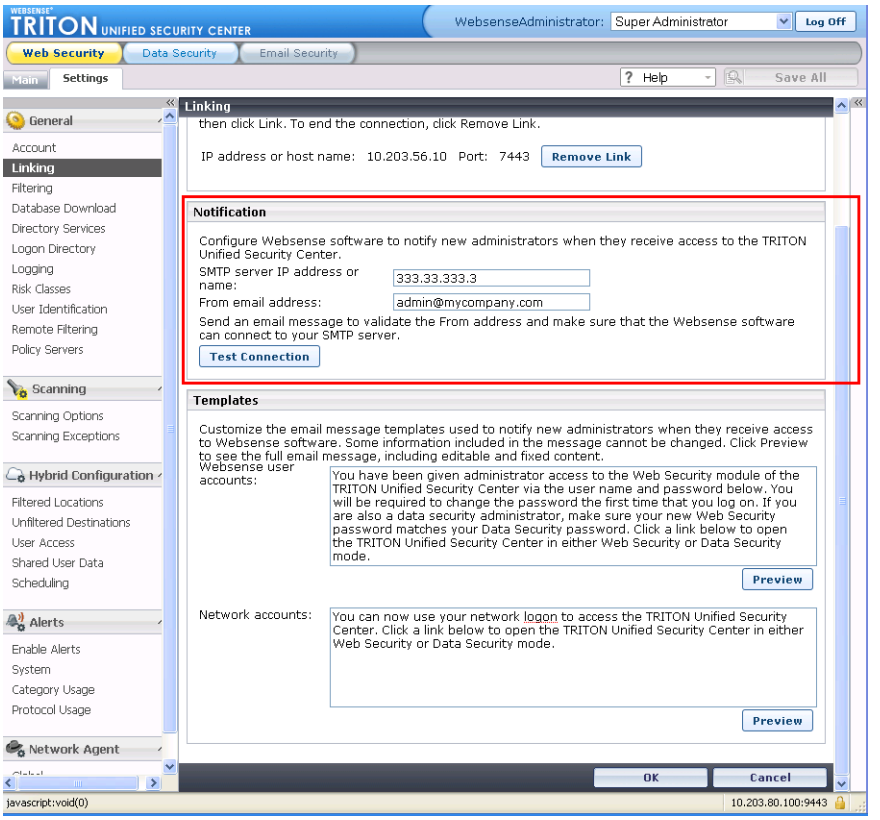
This allows the Data Security module to benefit from user name resolution and URL category mapping. If for some reason the Linking Service cannot be found, it is auto-installed at this time.

Email notification

If you want an email notification sent to new administrators with access to both TRITON - Web Security and TRITON - Data Security, configure the notification messages on the **Settings > Linking** page.

1. On the Linking page, scroll to the Notification section.

2. Enter the **IP address or name** of the SMTP Server machine.



3. Enter the **From email address** that will appear in notifications.
4. Click **Test Connection** to verify that Websense software can access the SMTP server, and that the From address is valid.
5. When you are satisfied with your changes, click **OK**, and then click **Save All**.

Next, review and modify the email message templates used for administrator notifications. Click **Preview** under either edit field to see the full message. Each message includes some required text (including links to TRITON - Web Security and TRITON - Data Security) that cannot be edited or removed.

A different message is sent to administrators who log on with Websense user accounts than administrators who log on with their network logon account. Typically, administrators using a Websense user account are both notified of their new logon name, and prompted to change their password the first time they log on. (The password prompt shows only if you checked “Prompt for password” when creating that administrator.)

Creating a common administrator account

If you’d like to use the buttons in the TRITON module tray to switch between the Web and data security modules, you must have an administrator account in both systems with the same user name and password.

All modules use WebsenseAdministrator as the default user name. If you log onto TRITON - Web Security and configure linking before logging onto TRITON - Data Security—as described in this document—the password for TRITON - Web Security is automatically applied to the data security module.

If this is not the case, for the module tray to function, you must log onto TRITON - Data Security and change the password of the WebsenseAdministrator user to the password you configured for TRITON - Web Security.

Once this is done, the buttons in the TRITON module tray become active, and the WebsenseAdministrator user can use them to switch between the Web and data security modules without having to enter credentials again.

If there are other administrators who will be accessing both modules, make note of their user names and passwords and add them to the data security module.

Configuring hybrid filtering

With Websense Web Security Gateway Anywhere, you can combine on-premises and hybrid (in-the-cloud) filtering as needed to manage Internet activity for your organization.

You decide which method to use for which users, but you might use robust on-premises Web filtering for your corporate office or main campus, and filter your regional offices or satellite locations through the hybrid service. Hybrid filtering also provides an option for users who are off-network, such as telecommuters and those who travel for business. (See the TRITON - Web Security Help for details.)

Hybrid filtering configuration tasks—including initial setup, defining clients and policies, and reporting setup—are performed in TRITON - Web Security.

Steps provided earlier in this chapter guided you through activating your hybrid filtering account. Now, use the instructions in the sections that follow to configure how the hybrid service filters Internet requests and shares data with on-premises components.

Define locations filtered by hybrid service

A **filtered location** is the external IP address, IP address range, or subnet from which browsers connecting to the hybrid service appear to be originating. Because the hybrid service is hosted outside your network, these must be external addresses, visible from the Internet. Filtered locations are:

- Public-facing IP addresses for offices filtered by the hybrid service
- Often the external address of your Network Address Translation (NAT) firewall
- Likely to be a branch office, remote site, or satellite campus

Filtered locations are NOT:

- IP addresses of individual client machines

- The IP address of any Content Gateway machine used by the on-premises portion of your Websense software

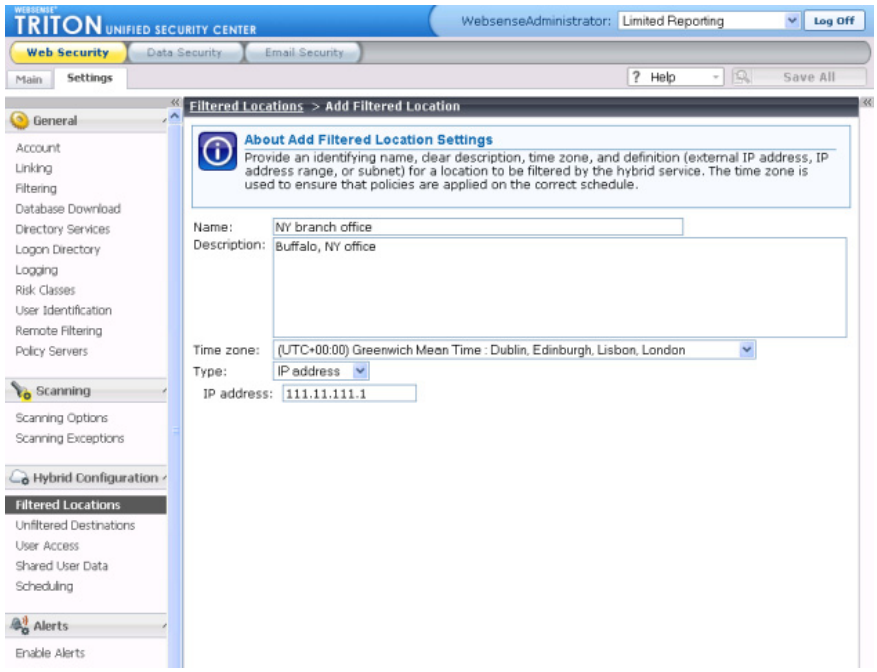
To define a filtering location:

1. Go to the **Settings > Hybrid Configuration > Filtered Locations** page in TRITON - Web Security.

   The page displays a table that will list a name and description for each filtered location that you define, as well as technical configuration details.
2. Click **Add**. The Add button is below the table.
3. Enter a unique location **Name**. The name must be between 1 and 50 characters long, and cannot include any of the following characters:

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   Names can include spaces, dashes, and apostrophes.



4. Enter a short **Description** of the location. This appears next to the location name on the Filtered Locations page, and should clearly identify the location to any administrator.

   The character restrictions that apply to names also apply to descriptions, with 2 exceptions: descriptions can include periods (.) and commas (,).
5. Select the **Time zone** of this location. Time zone information is used in applying policies, to ensure that the correct filters are applied at the appropriate time. Each location can have a different time zone setting.
6. In the **Type** field, indicate how you want to define this location: as an **IP address**, an IP address **Range**, or a **Subnet**.

   If you are providing a subnet, specify whether you are identifying it by **By bit range (CIDR)** or **By subnet mask**, and then select a bit range or mask.

7. Enter the external IP address, range, or subnet of the firewall or firewalls through which clients filtered by the hybrid service access the Internet.
   - These are external IP addresses, visible from outside your network, and not internal (LAN) addresses.

     Important

     Do not enter private IP addresses (in the ranges 10.0.0.0 - 10.255.255.255, 172.16.0.0 - 172.31.255.255, and 192.168.0.0 - 192.168.255.255) to identify locations filtered by the hybrid service. Because these addresses are not visible from outside your network, and are used within multiple local area networks, Websense software does not accept private IP addresses as valid entries.

   - Do not include the IP address of any Content Gateway machine used by the on-premises portion of your Websense software.
   - These IP addresses must be unique to your organization, not shared with any other entity, so that the hybrid service is able to associate requests originating from these locations with the policies belonging to your organization.
8. Click **OK** to return to the Filtered Locations page, and then click **OK** again to cache your changes. Changes are not implemented until you click **Save All**.

To make changes to a filtered location later, simply click the location name in the table on the Filtered Locations page. This opens an edit page that lets you make changes to the filtered location definition.

Specify sites that hybrid filtering users can access directly

An **unfiltered destination** is an site (defined by IP address, domain name, or subnet) that users can access directly, without sending the request to the hybrid service. Typical unfiltered destinations include organizational Web mail sites, internal IP addresses, and Microsoft update sites.

Tip

As a best practice, add your organization's Web mail address as an unfiltered destination. This ensures that:

- You can access messages from Technical Support in situations that cause the hybrid service to block all requests.
- Off-site users who have forgotten (or not created) their hybrid filtering password can retrieve it via email.

Destinations listed here are added to the Proxy Auto-Configuration (PAC) file that defines how filtered users' browsers connect to the hybrid service. By default, the PAC file excludes all non-routable and multicast IP address ranges from filtering. Therefore, if you are using private IP address ranges defined in RFC 1918 or RFC 3330, you need not explicitly define them as unfiltered destinations.

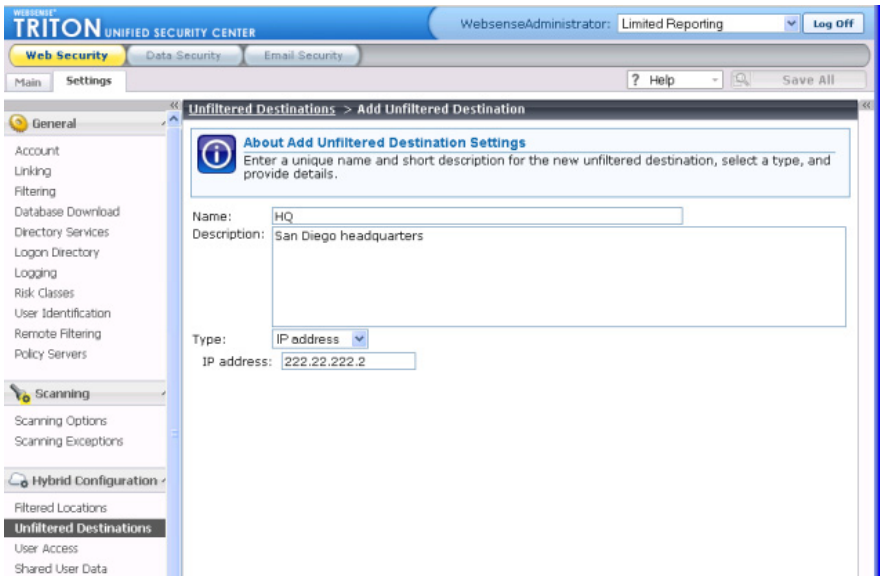
Each unfiltered destination that you define appears in a table that combines a name and description with technical configuration details, including how the destination is defined (as an IP address, domain, or subnet), and the actual IP address, domain, or subnet that users can access directly.

To define an unfiltered destination:

1. Go to the **Unfiltered Destinations > Add Unfiltered Destination** page.
2. Click **Add**. The Add button is below the table.
3. Enter a unique destination **Name**. The name must be between 1 and 50 characters long, and cannot include any of the following characters:

   ```
   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,
   ```

   Names can include spaces, dashes, and apostrophes.



4. Enter a short **Description** of the destination. This appears next to the unfiltered destination name on the Unfiltered Destinations page, and should clearly identify the unfiltered target site or sites to any administrator.

   The character restrictions that apply to names also apply to descriptions, with 2 exceptions: descriptions can include periods (.) and commas (,).

5. In the **Type** field, indicate how you want to define this destination: as an **IP address**, **Domain**, or **Subnet**.

   If you are providing a subnet, specify whether you are identifying it by **By bit range (CIDR)** or **By subnet mask**, and then select a bit range or mask.

6. Enter the IP address, domain, or subnet that you want users to be able to access without sending the request to the hybrid service.
7. Click **OK** to return to the Unfiltered Destinations page, and then click **OK** again to cache your changes. Changes are not implemented until you click **Save All**.

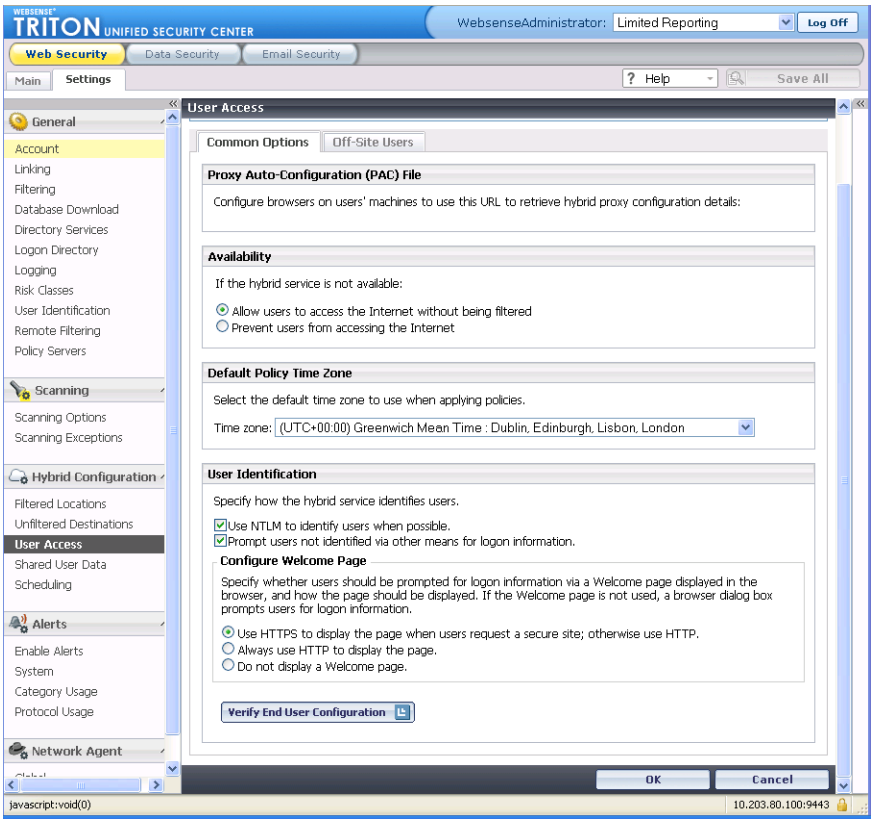
To make changes to an unfiltered destination later, simply click the destination name in the table.

Configure hybrid filtering behavior

Use the **Settings > Hybrid Configuration > User Access** page in TRITON - Web Security to:

- Find information about the default PAC file used to direct users' browsers to send Internet requests to the hybrid service.
- Provide basic information about how the hybrid service enforces filtering policies.
- Determine how users are identified, if hybrid filtering is configured to apply policies to users, groups, and domains (OUs).

  If you do not send directory service data to the hybrid service, hybrid filtering can only apply the Default policy, or policies applied to filtered locations (in other words, computer and network policies).



The **Proxy Auto-Configuration (PAC) File** section shows the URL from which browsers on filtered users' machines retrieve the default PAC file. The PAC file defines which requests the browsers send to the hybrid service, and which are sent

directly to the target site. Optionally, you can create your own PAC file, rather than using the default file generated for your account.

> **Note**
> The exact mechanism for configuring a user's browser to use the PAC file depends on the browser and your network environment. For example, if you are using Microsoft Active Directory and Internet Explorer or Mozilla Firefox, you might want to automate the process by using group policies.

Use the **Availability** section to specify whether all Internet requests should be permitted or blocked when the hybrid service is unable to access policy information for your organization.

Under **Time Zone**, use the drop-down list to select a default time zone to use when applying policies to:

- Users connecting to the hybrid service from an IP address that is not part of an existing filtered location

  The default time zone is used, for example, when applying policies to users who are off-site (remote or roaming).
- Whenever time zone information is not available for a filtered location

Use the **User Identification** section to configure how users are identified by the hybrid service, and to test and configure users' connections to the service.

1. Indicate how the hybrid service should identify users requesting Internet access:
   - Mark **Use NTLM to identify users when possible** to use directory information gathered by Websense Directory Agent to identify users transparently, if possible. This is used only for users connecting from a filtered location.

     If Directory Agent is sending data to the hybrid service, using NTLM to identify users is recommended.
   - Mark **Prompt users not identified via NTLM for logon information** to have users who could not be identified via another means see a logon prompt when accessing the Internet.

     Basic authentication is used to identify users who receive a logon prompt. Advise end users **not** to use the same password for hybrid filtering that they use to log on to the network.

   When both options are selected, the hybrid service first attempts to use NTLM to identify the user, and then, if identification fails, provides a logon prompt.

   When NTLM is used to identify users, **do not** use self-registration (configured on the Off-Site Users tab under Registered Domains).
2. Specify whether or not a Welcome page is displayed when users who have not been identified via NTLM open a browser to connect to the Internet. The Welcome page:

- Provides a simple selection of common search engines to get the user started
- Is used mainly by those who connect to the hybrid service from outside a filtered location (while working from home or traveling, for example)

If you choose to display the Welcome page, indicate whether or not the page should be sent via HTTPS when users request a secure site.

3. When you are finished, click **OK** to cache your changes. Changes are not implemented until you click **Save All**.

Once you have set up hybrid filtering and configured user browsers to access the PAC file, you can use the links provided under **Verify End User Configuration** to make sure that end user machines have Internet access and are correctly configured to connect to the hybrid service.

If your hybrid filtering account has not been verified (which may mean that no email address has been entered on the Settings > General > Account page), the URLs are not displayed.

Send user and group data to the hybrid service

If your organization uses a supported, LDAP-based directory service—Windows Active Directory (Native Mode) or Novell eDirectory—you can collect user and group data and send it to the hybrid service. This is accomplished using 2 Websense components:

- **Websense Directory Agent** - collects user and group information from Directory Server and collates it for hybrid filtering.
- **Websense Sync Service** - Transports policy, reporting, and user/group data between the on-premises and hybrid systems.

When hybrid filtering is configured properly, the information from Directory Agent can be used to apply user- and group-based filtering.

If your organization uses Windows NT Directory, Windows Active Directory (Mixed Mode), or Sun Java System Directory, user and group data cannot be collected and sent to the hybrid service.

If you have installed Directory Agent and configured your on-premises software to communicate with a supported directory service, you can review the default Directory Agent settings and configure custom settings in TRITON - Web Security.

- If your Websense software is configured to communicate with Active Directory (Native Mode), see *Directory Agent and Active Directory*, page 103.
- If your Websense software is configured to communicate with Novell eDirectory, see *Directory Agent and Novell eDirectory*, page 104.

Directory Agent and Active Directory

To configure how Directory Agent collects user and group information from Windows Active Directory and sends it to Sync Service for use by the hybrid service:

1. Navigate to the **Settings > Hybrid Configuration > Shared User Data** page.
2. A table lists the global catalog servers configured on the **Settings > General > Directory Services** page. Click an IP address or host name in the table to configure Directory Agent communication with that global catalog.

   A new page opens.
3. Under Root Context for Hybrid Filtering Users, provide a root **Context** to use when gathering user and group data from the directory. Narrow the context to increase speed and efficiency.

   It is best to provide a context that includes only users filtered by the hybrid service.
4. To verify that the context that you have entered uses valid syntax and exists in the directory, click **Test Context**.
5. Under Directory Search, indicate how far below the root context Directory Agent looks for users.
   - Select **One Level** to limit searches to the root context and one level below.
   - Select **All Levels** to expand searches to the root context and all levels below.
6. You can further refine the data that is sent to the hybrid service by defining patterns, or search filters, used to remove duplicate or otherwise unwanted **mail** entries from the directory search results. For more information, see the TRITON - Web Security Help.
7. Click **OK** to return to the Shared User Data page. Repeat steps 2 through 7 for any additional global catalog servers.
8. On the Shared User Data page, under **Synchronize User Data**, enter the **Name or IP address** of the Sync Service machine.
9. Enter the **Port** used for Sync Service communication (by default, 55832).
10. Click **Test Connection** to verify that Directory Agent can send data to Sync Service. The test may take a minute or more.
    - If the connection is made, a success message is displayed.
    - If the connection cannot be made, verify the IP address or host name of the Sync Service machine and the communication port. Also verify that the Sync Service machine is on, that Sync Service is running, and that your network firewall permits connections on the Sync Service port.
11. When you are finished, click **OK** to cache your changes. Changes are not implemented until you click **Save All**.

Directory Agent and Novell eDirectory

In environments that use Novell eDirectory, use the following steps to refine the way that Directory Agent searches the directory and packages results for the hybrid service:

1. Go to the **Settings > Hybrid Configuration > Shared User Data** page in TRITON - Web Security.

2. Under Root Context for Hybrid Filtering Users, provide a root **Context** to use when gathering user and group data from the directory. Narrow the context to increase speed and efficiency.

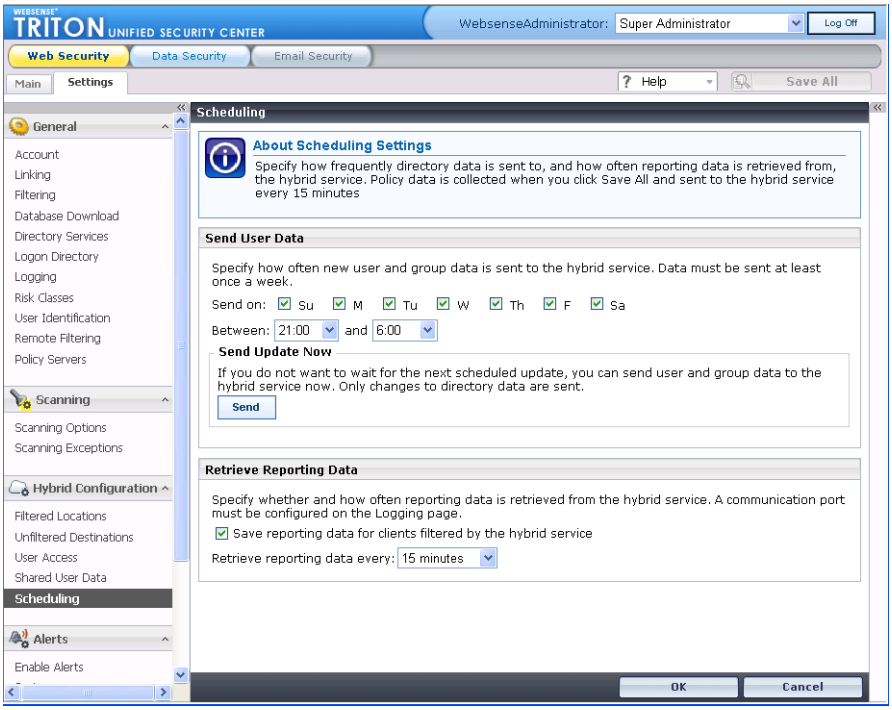
   It is best to provide a context that includes only users filtered by the hybrid service.

3. To verify that the context that you have entered uses valid syntax and exists in the directory, click **Test Context**.
4. Under Synchronize User Data, enter the **Name or IP address** of the Sync Service machine. (Sync Service is the component responsible for communicating with the hybrid service.)
5. Enter the **Port** used for Sync Service communication (by default, 55832).
6. Click **Test Connection** to verify that Directory Agent can send data to Sync Service. The test may take a minute or more.
   - If the connection is made, a success message is displayed.
   - If the connection cannot be made, verify the IP address or host name of the Sync Service machine and the communication port. Also verify that the Sync Service machine is on, that Sync Service is running, and that your network firewall permits connections on the Sync Service port.
7. Under Directory Search, indicate how far below the root context Directory Agent looks for users.
   - Select **One Level** to limit searches to the root context and one level below.
   - Select **All Levels** to expand searches to the root context and all levels below.
8. You can further refine the data that is sent to the hybrid service by defining patterns, or search filters, used to remove duplicate or otherwise unwanted **mail** entries from the directory search results. For more information, see the TRITON - Web Security Help.
9. When you are finished, click **OK** to cache your changes. Changes are not implemented until you click **Save All**.

Schedule communication with hybrid filtering

Go to the **Settings > Hybrid Configuration > Scheduling** page to specify how frequently directory data collected by Directory Agent is sent to the hybrid service, and how often reporting data is retrieved.

> **Note**
>
> Policy data is collected whenever your click **Save All** in TRITON - Web Security, and sent to the hybrid service at 15 minute intervals.



To configure how often directory information is sent to the hybrid service:

1. Under **Send User Data**, select one or more days of the week to send user and group information to the hybrid service. If you are using directory information to identify users, you must send Directory Agent data at least once a week.
2. Enter start and end times to define the time period during which Sync Service attempts to send directory data to the hybrid service. Typically, directory data is sent at a period of low traffic in your network.
3. If you have made an important update to your directory service data, and want to send user and group information right away, click **Send** under Send Update Now.

   If TRITON - Web Security receives confirmation from Sync Service, a success message is displayed. This means that Sync Service will send the data; not that the data has been received by the hybrid service.

To configure how often reporting data is retrieved from the hybrid service:

> **Note**
> In order for Sync Service to pass hybrid reporting data to Log Server, a hybrid communication port must be configured on the Settings > General > Logging page.

1. Under Retrieve Reporting Data, mark **Save reporting data for clients filtered by the hybrid service**.

   If you clear this check box, log data is not saved for hybrid filtering users. No information about these users' Internet activity will appear in reports.

2. Select how often you want Sync Service to request reporting data from the hybrid service (every 30 minutes, by default).

   Sync Service cannot download reporting data any more frequently than every 15 minutes. This means that there is a time delay between when hybrid filtering make Internet requests and when those requests appear in TRITON - Web Security reports.

When you are finished, click **OK** to cache your changes. Changes are not implemented until you click **Save All**.

5 Configuring the Content Gateway Module

This section describes how to set up the Content Gateway module in its minimum configuration so that you can quickly begin to protect your organization with Web Security Gateway Anywhere.

Initial Setup

The sections that follow guide you through the basic steps required to initialize the on-premises Content Gateway module (proxy) of Websense Web Security Gateway Anywhere. Follow these steps to:

- Log on
- Enter your subscription key
- Enable proxy features
- Configure protocols

Logging on

There are 2 ways to access the Content Gateway Manager user interface:

- From the appliance logon portal, click **Content Gateway Manager**.
- From an Internet Explorer or Firefox browser, open a window and enter the following URL into the address field:

  `https://<IP_or_hostname>:8081`

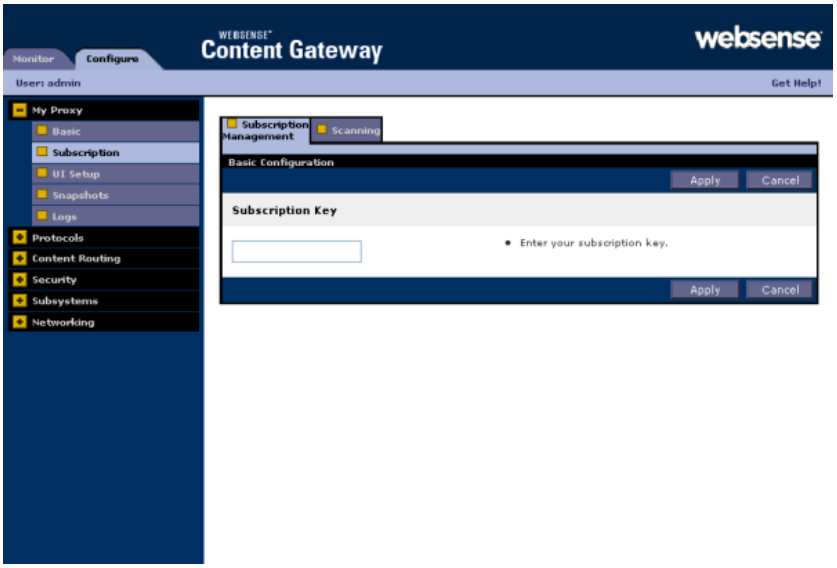
  where <IP_or_hostname> is the IP address or host name of the Linux machine where Content Gateway is installed.

Initially, your user name is “admin” (case-sensitive). Enter the password you set up during installation and click **OK**.

Entering your subscription key

When you first log onto Content Gateway Manager, you should enter your Web Security Gateway Anywhere subscription key.

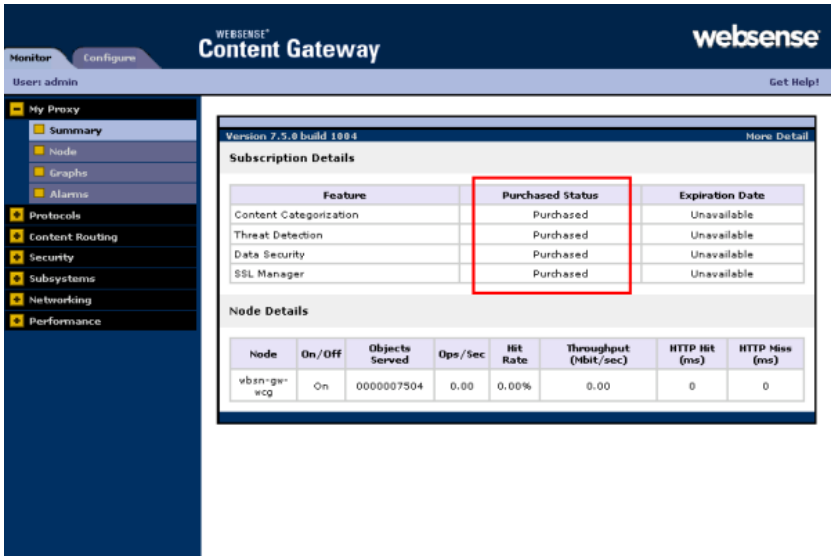
1. Navigate to **Configure > My Proxy > Subscription > Subscription Management**.



2. Enter the key for your Websense Web Security Gateway Anywhere subscription. This is the same key you entered into TRITON - Web Security.
3. Click the **Apply** button.
4. Select **Configure > My Proxy > Basic** and click **Restart** to restart the proxy.

5. Select **Monitor > My Proxy > Summary** and verify in the **Subscription Details** area that the 4 features have a status of "Purchased":
   - Content categorization
   - Threat detection
   - Data security

- SSL manager



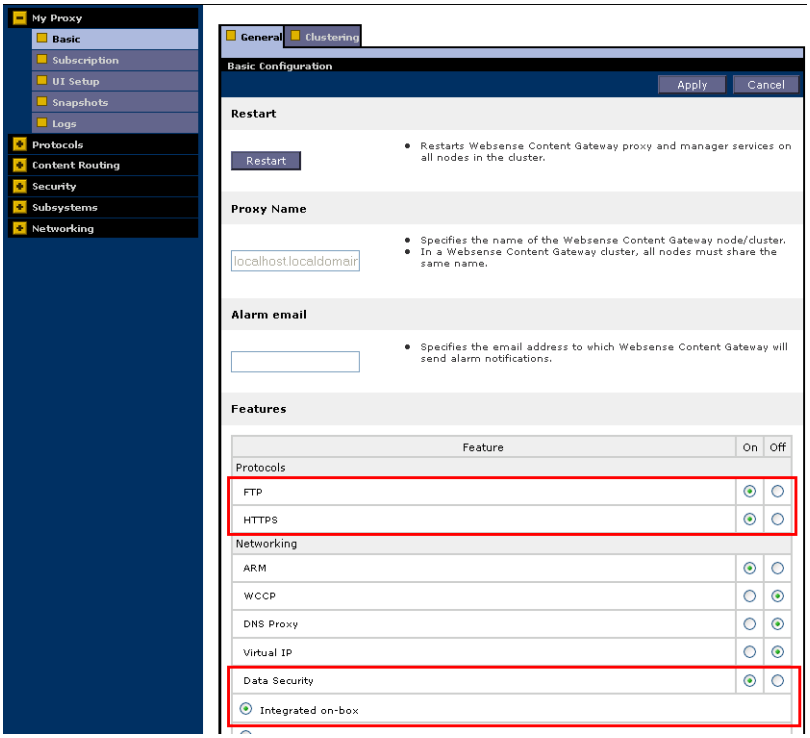
This demonstrates that your subscription is active. If the features do not show as purchased, verify your network settings, and again restart Content Gateway. If you have a V-Series appliance, go to the Appliance Manager and restart the Content Gateway services.

Enabling proxy features

Choose the basic proxy features you want to use:

1. Select **My Proxy > Basic > General**.
2. Under **Features**, click **On** to enable a feature.
   - HTTP is always enabled.
   - If you want to proxy HTTPS or FTP, select the associated **On** radio buttons.
3. If you plan to do transparent proxy routing with WCCP devices, select the WCCP **On** radio button in the Networking section. You will also have to configure your WCCP routers and switches. For detailed information, see Content Gateway Manager help.

4. Under **Networking**, turn Data Security on by selecting its **On** radio button, then select **Integrated on-box**.



5. Click **Apply**.
6. At the top of the **General** tab, click the **Restart** button to restart Content Gateway.

Configuring protocols

The default protocol configuration is suitable for most organizations. If you'd like to review and customize settings:

1. Select **Configure > Protocols**.
2. One at a time, select the protocols to proxy and review the screens. (Some have multiple tabs.) You can choose:
   - HTTP
   - HTTP responses
   - HTTP scheduled update
   - HTTPS (if you enabled the feature)
   - FTP (if you enabled the feature)
3. Confirm the ports listed on these screens. Make the changes you require.
4. Click **Apply**.
5. Go to **Configure > My Proxy > Basic > General** and click **Restart**.

Checking for alarms

Check to see if any alarms are indicated, view the message, and take any necessary corrective action. To remove an alarm from the list, select the box next to the alarm and click **Clear**.

Routing traffic to Content Gateway

For Content Gateway to proxy Internet request traffic, such traffic must be routed to Content Gateway. This section describes how to configure explicit and transparent Internet request routing.

Explicit request routing

If Internet requests are not transparently routed to Content Gateway via a Layer 4 switch or router (see *Transparent request routing*, page 112), traffic must be explicitly routed to the proxy by configuring the client's Internet browser.

Client Web browsers can be configured in 3 ways:

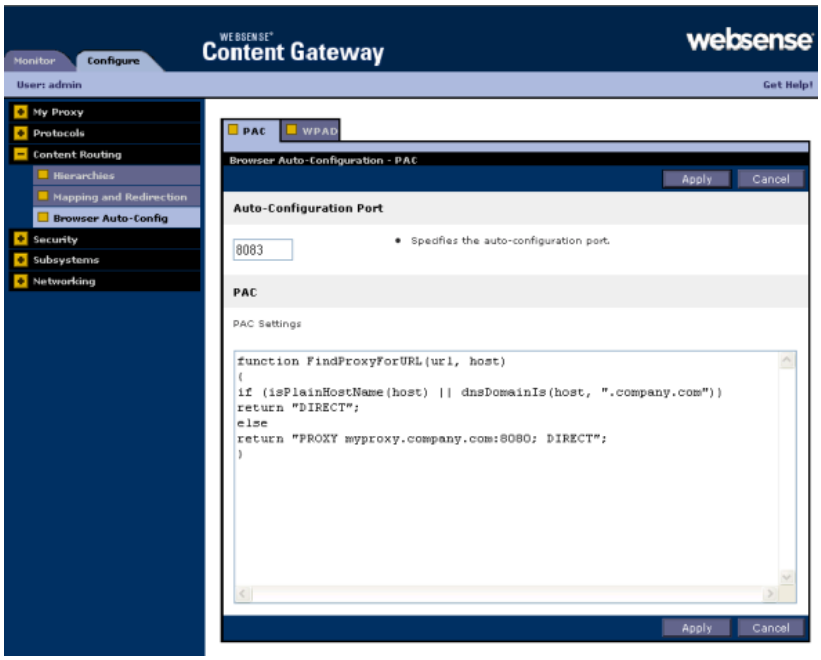
- By individually configuring browsers to send requests directly to the proxy. See the Web browser's documentation.
- By configuring browsers to download proxy configuration instructions from a PAC (Proxy Auto-Config) file. See *Using a PAC file*, page 111.
- By using WPAD (Web Proxy Auto-Discovery Protocol) to download proxy configuration instructions from a WPAD server (Microsoft Internet Explorer only). See Content Gateway Manager help.

If Content Gateway is configured to proxy FTP traffic, FTP applications, such as FileZilla or WS_FTP, must also be configured to explicitly send requests to the proxy. See the FTP application help and Content Gateway Manager help.

Using a PAC file

1. Select **Configure > Content Routing > Browser Auto-Config**.

2. On the **PAC** tab, enter the auto-configuration port and PAC settings. This includes the URL to the Proxy Auto-Configuration (PAC) file used to direct users' browsers to send Internet requests to the proxy. Sample PAC settings are shown below:



3. Click **Apply**.
4. Go to **Configure > My Proxy > Basic > General** and click **Restart**.

Transparent request routing

Transparent Internet request routing enables Content Gateway to respond to requests without requiring users to reconfigure their browser settings. It does this by redirecting the traffic flow to Content Gateway after the traffic has been intercepted, typically by a Layer 4 (L4) switch or router. For a complete discussion of transparent routing strategies, see Content Gateway Manager help.

In transparent interception:

1. The proxy receives client requests intercepted by a switch or router.
2. The Adaptive Redirection Module (ARM) changes the destination IP address of an incoming packet to the proxy's IP address and the destination port to the proxy port (if different). The ARM is enabled by default.
3. The proxy processes the intercepted client requests.

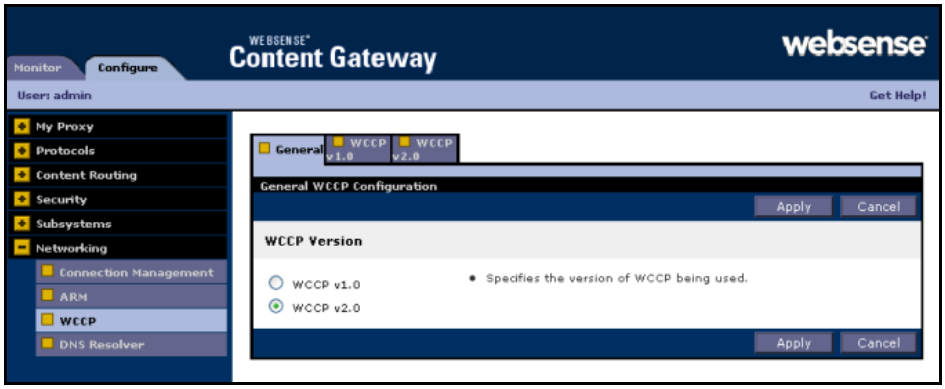
4. On the way back to the client, the ARM changes the source IP address to the origin server IP address and the source port to the origin server port.

> **Note**
> For transparent proxy configurations with multiple interfaces or gateways, Content Gateway must have proper routes to clients and the Internet in the operating system's routing table.

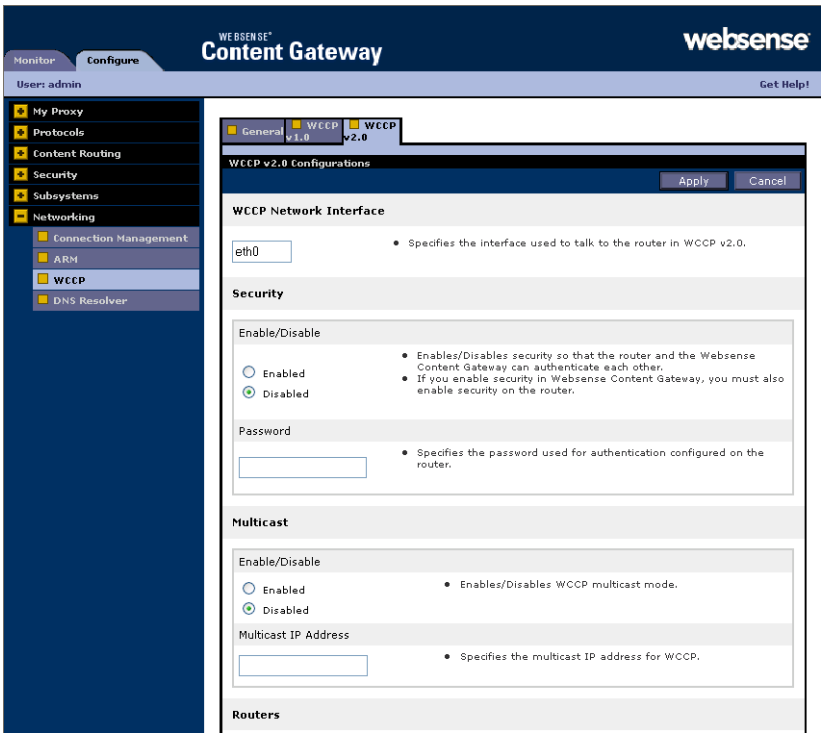
Enabling WCCP in Content Gateway

> **Warning**
> Before enabling WCCP transparent routing, you should be thoroughly acquainted with your network topology and the role of your WCCP devices in it. WCCP device configuration is discussed in detail in the Content Gateway Manager help.

1. Select **Configure > Networking > WCCP**.
2. On the **General** tab, select the version of WCCP to use. If you have enabled HTTPS or FTP, your WCCP devices must support v2.0 and you must select the v2.0 option.
3. Click **Apply**.



4. Click the tab corresponding to your selection.



5. Enter the network interface card to use to talk to the router (e.g., eth0).
6. Enter the IP address of the WCCP router(s).
7. Complete the remaining fields as required.
8. Click **Apply**.
9. Restart Content Gateway.

Configuring proxy user authentication

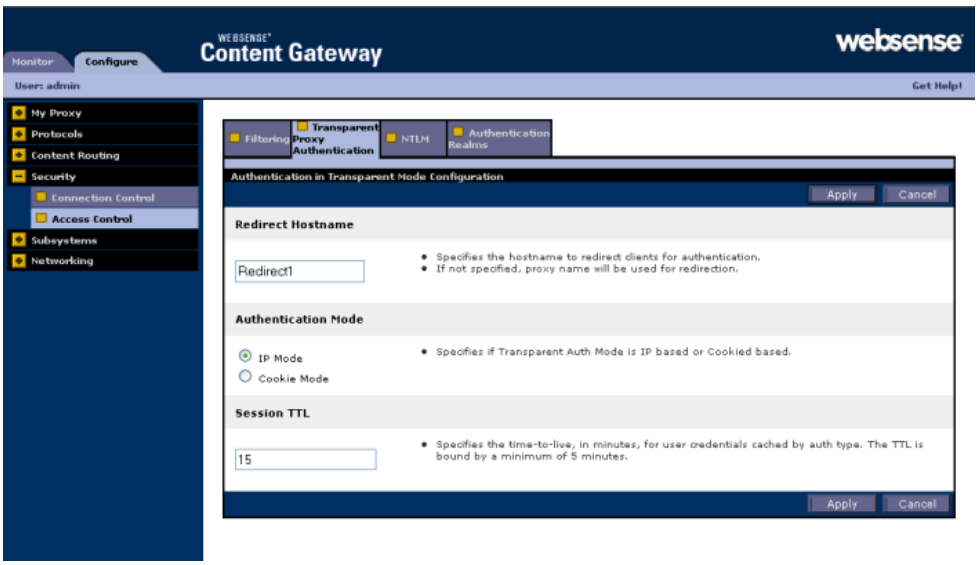
Content Gateway supports LDAP, RADIUS, and NTLM user authentication for both explicit and transparent request routing.

> **Important**
> Enable only one authentication option.

Transparent proxy authentication

When one of the NTLM, LDAP, or Radius authentication methods is enabled, Content Gateway performs user authentication for requests that are explicitly or transparently routed to Content Gateway.

Transparent proxy authentication settings are configured on the **Configure > Security > Access Control > Transparent Proxy Authentication** tab.



Specify the following values:

- **Redirect Hostname** (optional) — specifies an alternate hostname for the proxy.

  By default, authenticating clients are redirected to the hostname of the Content Gateway machine. If clients aren't able to resolve that hostname via DNS, or if an alternate DNS name for the proxy is defined, that hostname can be specified in the **Redirect Hostname** field.
- **Authentication Mode** — specifies the authentication mode. Content Gateway must be set to one of the following authentication modes:
  - In **IP mode** (the default), the client IP address is associated with a user name when the session is authenticated. Requests made from that IP address are not authenticated again until the **Session TTL** expires (time-to-live; default = 15 minutes). Requests made from that IP address within the time-to-live are considered to be made by the user associated with that IP address.
  - **Cookie mode** is used to uniquely identify users who share a single IP address, such as, for example, environments in which proxy-chaining is used or where network address translation (NAT) occurs.
- **Session TTL** — In either authentication mode, client authentication is valid for the duration of the time specified in **Session TTL** (default = 15 minutes). The supported range of values is 5-65535 minutes.

Click **Apply** to save your changes and click **Restart** on **Configure > My Proxy > Basic > General** to restart the proxy.

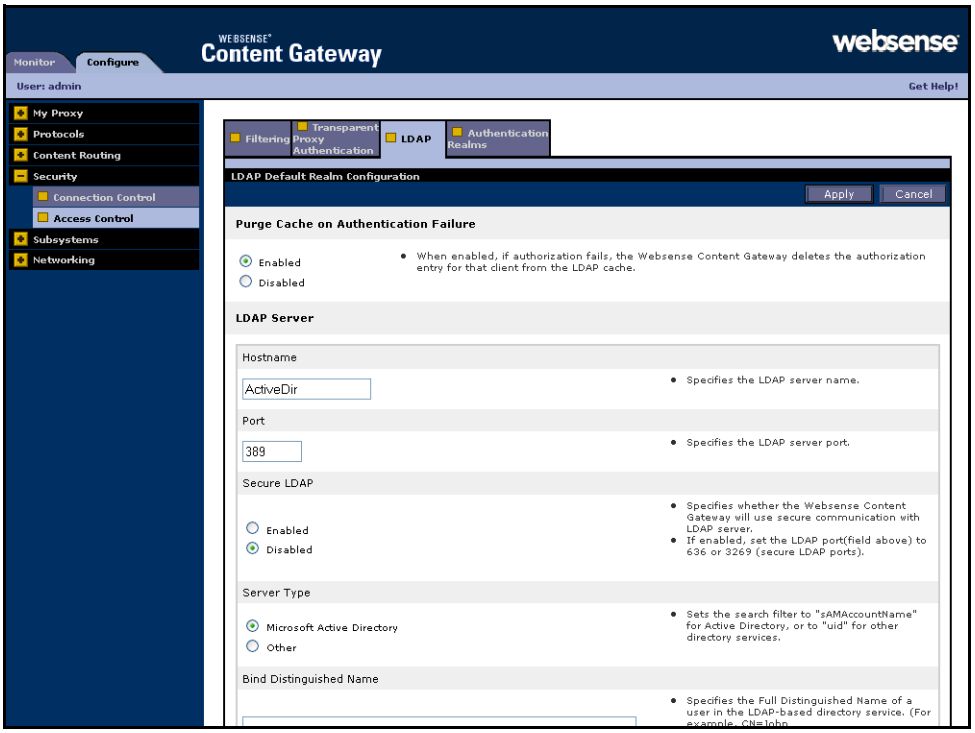
Using LDAP proxy authentication

When you enable the LDAP option, the proxy acts as an LDAP client and directly challenges users who request content for a user name and password. After receiving

the user name and password from a client, the proxy contacts the LDAP server to check that the credentials are correct. If the LDAP server accepts the user name and password, the proxy serves the client with the requested content and stores the user name and password entry in the Content Gateway LDAP cache; all future authentication requests for that user are served from the LDAP cache until the entry expires. If the LDAP server rejects the user name and password, the user's browser displays a message indicating that authorization failed and prompts again for a user name and password.

Configuring Content Gateway to be an LDAP client

1. Navigate to **Configure > My Proxy > Basic > General**.
2. In the Features table, click LDAP **On** in the Authentication section.
3. Click **Apply**.
4. Click **Restart** on **Configure > My Proxy > Basic > General**.
5. Navigate to **Configure > Security > Access Control > LDAP**.



6. Enable **Purge Cache on Authentication Failure** to configure the proxy to delete the authorization entry for the client from LDAP cache if authorization fails.
7. Enter the host name of the LDAP server.

8. Enter the port on which Content Gateway communicates with the LDAP server. The default is port 389.

> **Note**
> When the LDAP directory service is Active Directory, requests from users located outside the global catalog's base domain will fail to authenticate. This is because the default port for LDAP is 389 and requests sent to 389 search for objects only within the global catalog's base domain. To authenticate users from outside the base domain, change the LDAP port to 3268. Requests sent to 3268 search for objects in the entire forest.

9. Enable Secure LDAP if you want the proxy to use secure communication with the LDAP server. Secure communication is usually performed on port 636 or 3269. (Change the port value in the previous field, if necessary.)
10. Select the type of your directory service to set the filter for searching. The default is **sAMAccountName** for Active Directory. Select **uid** for eDirectory or other directory services.
11. Enter the Full Distinguished Name (fully qualified name) of a user in the LDAP-based directory service. For example:

    ```
    CN=John Smith,CN=USERS,DC=MYCOMPANY,DC=COM
    ```

    Enter a maximum of 128 characters in this field.

    If no value is specified for this field, the proxy attempts to bind anonymously.
12. Enter a password for the user specified in the previous step.
13. Enter the Base Distinguished Name (DN). Obtain this value from your LDAP administrator.
14. Click **Apply**.
15. Click **Restart** on **Configure > My Proxy > Basic > General**.

Optionally, you can:

- Change LDAP cache options.
- Configure multiple authentication realms in which certain IP addresses use specific LDAP servers.
- Configure Content Gateway to allow certain clients to access specific sites on the Internet without being authenticated by the LDAP server.

For details, see Content Gateway Manager help.

Using RADIUS proxy authentication

When you enable the RADIUS option, Content Gateway acts as a RADIUS client and directly challenges users who request content for a user name and password. After receiving the user name and password from a client, Content Gateway contacts the RADIUS server to check that they are correct. If the RADIUS server *accepts* the user name and password, the proxy serves the client with the requested content and stores

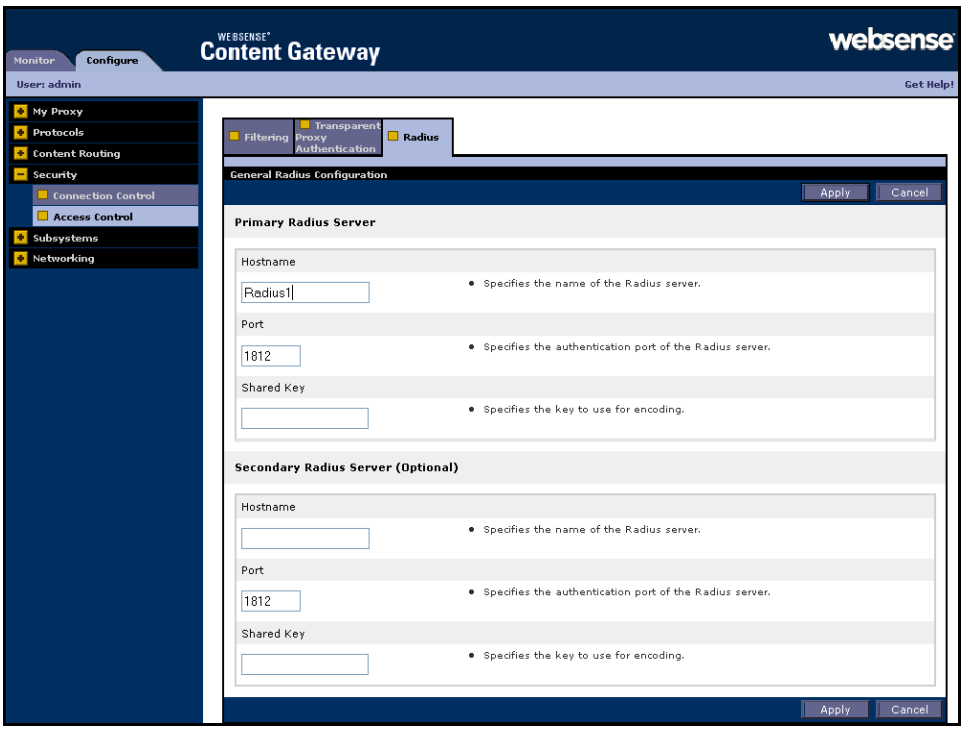
the user name and password entry in the RADIUS cache; all future authentication requests for that user are served from the RADIUS cache until the entry expires. If the RADIUS server *rejects* the user name and password, the user's browser displays a message indicating that authorization failed and prompts again for a user name and password.

Content Gateway supports a primary RADIUS server and a secondary RADIUS server for fail over. If the primary server does not respond to the proxy request within the specified timeout (60 seconds by default), Content Gateway tries to check the user name and password again. If a response from the primary RADIUS server is not received after the maximum number of retries (10 by default), the proxy contacts the secondary RADIUS server. If Content Gateway cannot contact the secondary RADIUS server, the user is prompted again for a user name and password.

The RADIUS cache is held in memory and stored on disk. Content Gateway updates the data on disk every 60 seconds. In addition, Content Gateway stores user name and password entries in the RADIUS cache for 60 minutes. If a password and user name entry is expired in the RADIUS cache, Content Gateway contacts the RADIUS server to accept or reject the user name and password.

Configuring Content Gateway to be a RADIUS client

1. Navigate to **Configure > My Proxy > Basic > General**.
2. In the Features table, click Radius **On** in the Authentication section.
3. Click **Apply**.
4. Navigate to **Configure > Security > Access Control > Radius**.



5. Enter the host name of your primary RADIUS server.

6. Enter the port number through which Content Gateway communicates with the primary RADIUS server.
7. Enter the key used for encoding.
8. If you are using a secondary RADIUS server, enter the host name, port, and shared key in the appropriate fields of the **Secondary Radius Server (Optional)** area.
9. Click **Apply**.
10. Click **Restart** on **Configure > My Proxy > Basic > General**.

> **Note**
> In addition to performing these procedures, you must add the Content Gateway machine as a trusted client on the primary and secondary RADIUS servers and provide the shared key you want to use for the Content Gateway machine (the shared key must be the same one you specify in the procedure below). See your RADIUS server documentation.

For more information about RADIUS options, see Content Gateway Manager help.

Using NTLM proxy authentication

When the NTLM option is enabled, the proxy challenges users who request content for proof of their credentials. The proxy then sends the proof of the user's credentials directly to the Windows domain controller to be validated. If the credentials are valid, the proxy serves the requested content and stores the credentials in the NTLM cache for future use. If the credentials are not valid, the proxy sends an *authentication failed* message to the user.

Content Gateway supports both transparent (Single Sign-On) and explicit authentication. Transparent authentication is supported with Microsoft Internet Explorer 7 and 8, and Mozilla Firefox 2 and 3. Single Sign-On allows users to sign on only once, so that they can seamlessly access all authorized network resources. Therefore, if a user has already logged on to the Windows network successfully, the credentials specified during Windows logon are used for authentication and the user is not prompted again for a username and password. Explicit (basic) authentication is supported for other browsers. With explicit authentication, users are prompted for a username and password before they can access the protected content.

Content Gateway supports the use of backup domain controllers for failover. If the primary domain controller does not respond to proxy requests, Content Gateway contacts the next domain controller in the list (the backup domain controller). For the next request, the proxy tries to contact the primary domain controller again and then contacts the backup domain controller if the connection fails. Content Gateway does this 5 times before considering the server unavailable. After marking the primary domain controller unavailable, the proxy waits 5 minutes before trying to contact it again.

Content Gateway supports access to Windows NT domain controllers and Windows 2000, 2003, and 2008 Active Directory.

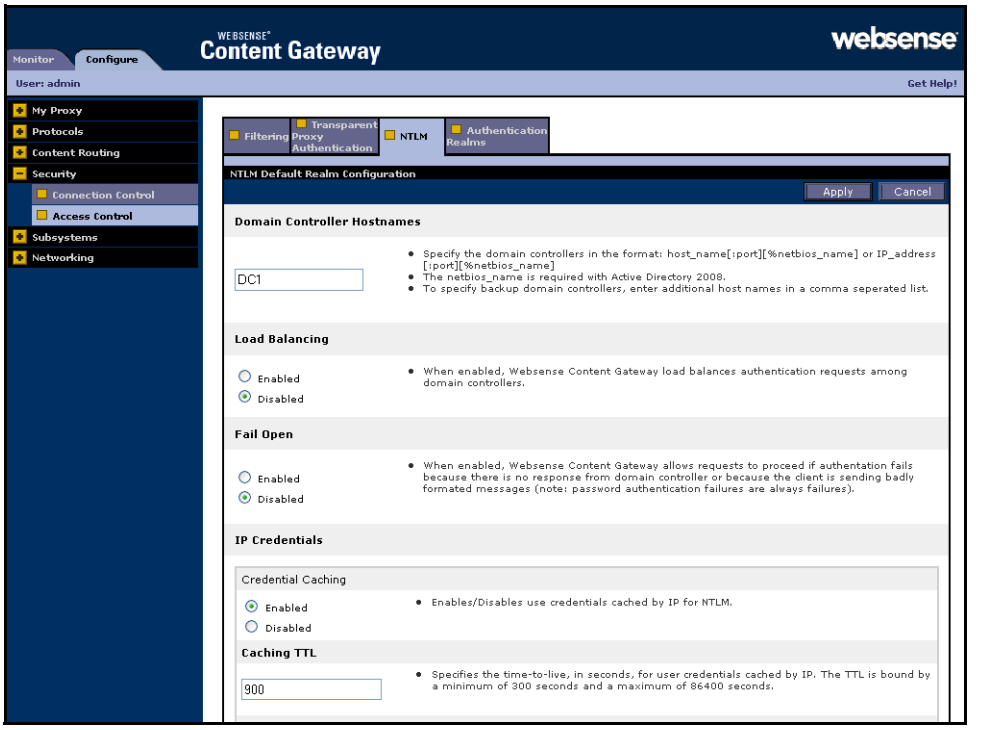
Restrictions:

1. **WINS resolution** is not supported. Domain controllers must have host names that can be resolved by a DNS server.
2. **Extended security** is not supported and cannot be enabled on the domain controller.
3. **NTLM2 session security** is not supported and cannot be enabled on clients. In the Security Settings area of the Windows operating system, inspect the **Network Security: Minimum session security** settings.
4. **NTLMv2** is not supported with Active Directory 2008. The required **Network Security: LAN Manager Authentication** setting is described in step 5 of *Configuring NTLM proxy authentication*, below.
5. Not all browsers support transparent NTLM authentication.
6. NTLM credential caching is performed when authentication is successful in explicit mode.Transparent proxy authentication caching is handled separately and is configured on the **Configuration > Security > Access Control > Transparent Proxy Authentication** tab.

Configuring NTLM proxy authentication

1. Navigate to **Configure > My Proxy > Basic > General**.
2. In the Features table, click NTLM **On** in the Authentication section.
3. Click **Apply**.

4. Navigate to **Configure > Security > Access Control > NTLM**.



5. In the **Domain Controller Hostnames** field, enter the host name of the primary domain controller, followed, optionally, by a comma separated list of backup domain controllers. The format of the host name must be:

   ```
   host_name[:port][%netbios_name]
   ```

   or

   ```
   IP_address[:port][%netbios_name]
   ```

> **Note**
>
> If you are using Active Directory 2008, you must include the netbios_name or use SMB port 445. If you **do not** use port 445, you must ensure that the Windows Network File Sharing service is running on the Active Directory server. See your Windows Server 2008 documentation for details.

> **Note**
>
> If you are using Active Directory 2008, in the Windows **Network Security** configuration, **LAN Manager Authentication level** must be set to **Send NTLM response only**. See your Windows Server 2008 documentation for details.

6. Enable **Load Balancing** if you want the proxy to balance the load when sending authentication requests to multiple domain controllers.

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

7. **Fail Open** is enabled by default. Fail Open allows requests to proceed when authentication fails due to:
   - No response from the domain controller
   - Malformed messages from the client
   - Invalid SMB responses

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

   Disable Fail Open if you want to stop requests from proceeding to the Internet when the above listed authentication failure conditions occur.
8. **Credential Caching** is enabled by default. To disable credential caching, select **Disable**.
9. **Caching TTL** sets the time-to-live from entries in the credential cache. The default TTL is 900 seconds (15 minutes). To change the TTL, enter a new value in the entry field. The range of supported values is 300 to 86400 seconds.
10. If some users use terminal servers to access the Internet through the proxy (e.g., Citrix servers), you must create a list of those servers in the **Multi-user Hostnames** field. Credentials for such users are not cached. Enter a comma separated list of host names. Names can include simple regular expressions to match multiple host names, such as “tserver*” to match all host names that start with “tserver”.
11. Click **Apply**.
12. Click **Restart** on **Configure > My Proxy > Basic > General**.

Optionally, you can:

- Configure multiple authentication realms in which certain IP addresses use specific NTLM servers.
- Configure Content Gateway to allow certain clients to access specific sites on the Internet without being authenticated by the NTLM server.

See Content Gateway Manager help.

Preparing for Web DLP

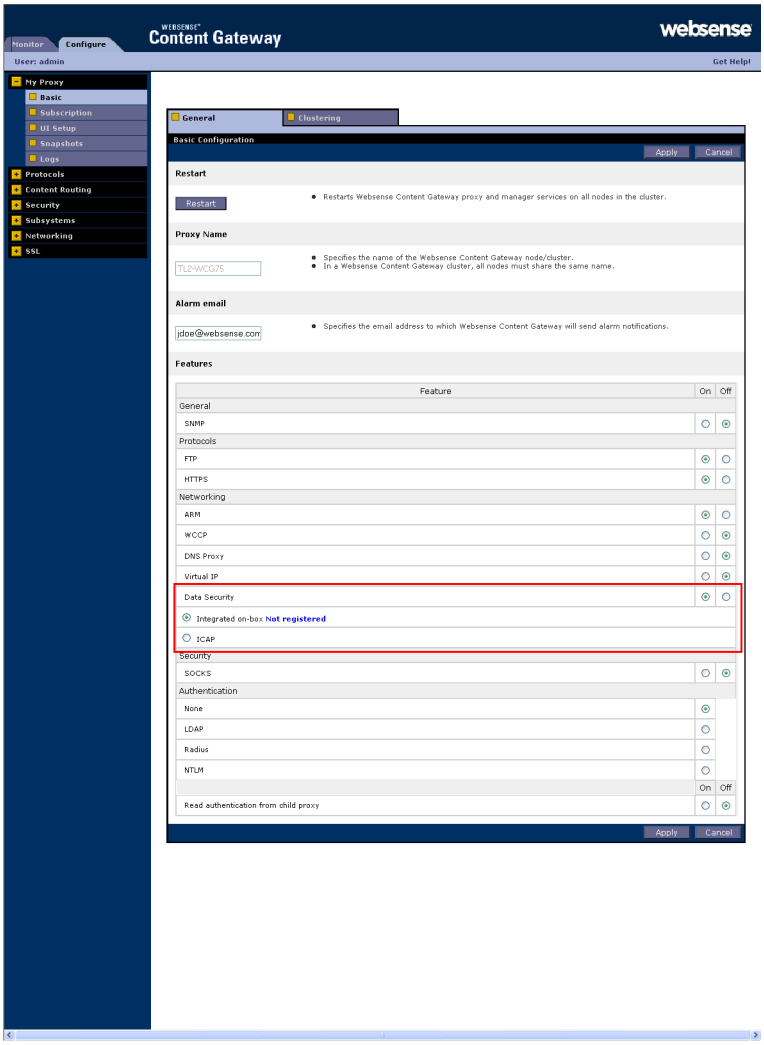
To enable data loss prevention over Web channels, you must connect the Content Gateway module of your Web security solution to the Data Security Management Server.

Registering with the Data Security Management Server

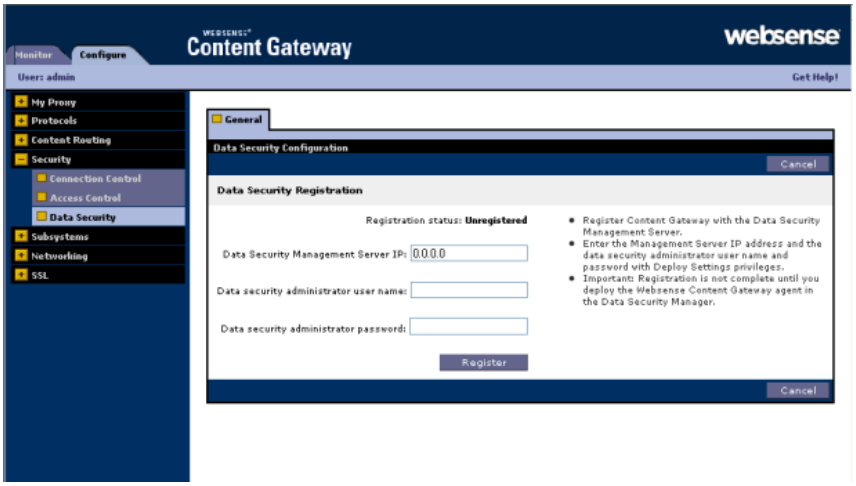
1. Ensure that Content Gateway and Data Security Management Server systems are running and accessible, and that their system clocks are approximately synchronized.
2. Ensure the Content Gateway machine has a fully qualified domain name (FQDN) that is unique in your network. Host name alone is not sufficient.
3. If Content Gateway is deployed as a transparent proxy, ensure that traffic to and from the communication interface ("C" on a V-Series appliance) is not subject to transparent routing. If it is, the registration process will be intercepted by the transparent routing and will not complete properly.
4. Make sure that the IPv4 address of the eth0 NIC on the Content Gateway machine is available (not required if Content Gateway is located on a V-Series appliance). eth0 is the NIC used by the Data Security Management Server during the registration process.

   After registration, the IP address can move to another network interface on the same machine; however, that IP address is used for configuration deployment and must be available as long as the 2 modules are registered.
5. From the Content Gateway Manager, select **Configure > Basic > General**.

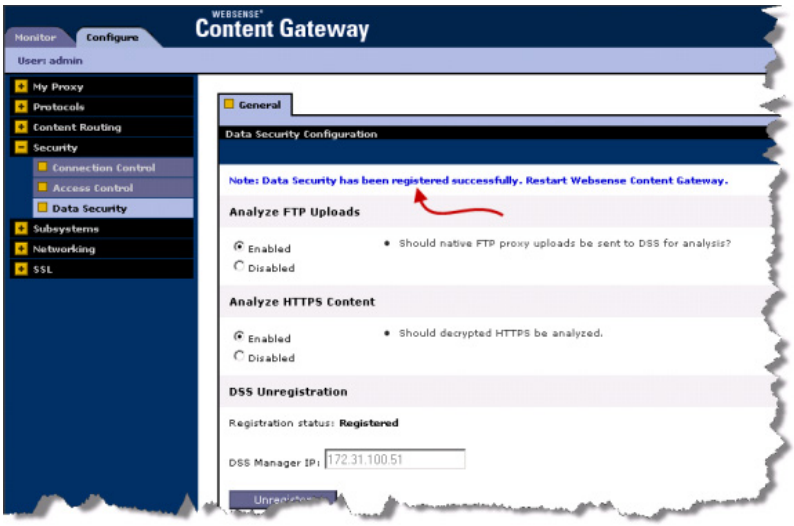
6. Earlier, you turned Data Security on by selecting its **On** radio button and selecting **Integrated on-box**. Now click the **Not Registered** link.



This opens the **Configure > Security > Data Security** registration screen.



7. Enter the IP address of the **Data Security Management Server**.
8. Enter a user name and password for a Data Security administrator with Manage System Modules privileges.
9. Click **Register**. You are reminded to synchronize the system time between the proxy machine and the Data Security Management Server.
10. If registration succeeds, a Data Security Configuration page displays.



Set the following configuration options.

a. **Analyze FTP Uploads**: Enable this option to send FTP uploads to Data Security for analysis and policy enforcement.

b. **Analyze Secure Content**: Enable this option to send decrypted HTTPS posts to Data Security for analysis and policy enforcement.

These options can be accessed whenever Data Security is registered by going to the **Configure > Security > Data Security > General** page.

11. Click **Apply**.
12. Restart Content Gateway.
13. Deploy the Content Gateway module as described in Chapter 6, *Deploying the Content Gateway module*, page 129.

6 Configuring the Data Security Module

This section describes the minimum steps required to set up the Data Security module for the Web DLP feature.

Logging on

There are several ways to access TRITON - Data Security:

- From the appliance logon portal, click TRITON - Data Security.
- Click the Websense TRITON - Data Security shortcut placed on the Data Security Management Server desktop during installation.
- Select **Start > Programs > Websense > Websense TRITON - Data Security** from the Windows **Start** menu of the Data Security Management Server.
- Open a browser window, and enter the following URL into the address field:

  `https://<IP_or_hostname>:8443/dlp/pages/mainFrame.jsf`

  where <IP_or_hostname> is the IP address or host name of the Data Security Management Server.

> **Note**
> Due to some browser limitations, the host name must not contain underscore characters.

Initially, your user name is **WebsenseAdministrator** (case-sensitive).

If you logged onto TRITON - Web Security and configured linking *before* logging onto TRITON - Data Security for the first time, the password for TRITON - Data Security is the same as that for TRITON - Web Security.

If this is not the case, your default password is also **WebsenseAdministrator**.

Enter your credentials and click **Log On**.

Changing passwords

If you entered the default credentials onto the log on screen, **WebsenseAdministrator/WebsenseAdministrator**, you are immediately prompted to change your password.

Type the old password, **WebsenseAdministrator**, then enter a new password and retype it for confirmation. Websense suggests you use the same password for the data security and Web security modules. This enables the administrator to access the Web and data security modules through the TRITON security center toolbar.

Click **Save & Log On**.

Note
A maximum of 20 users can be signed in simultaneously, each in a separate browser instance.

Note
Opening more than one session of TRITON - Data Security in the same browser results in unexpected behavior.

You do not have to enter a subscription key into the Data Security module, because it is automatically conveyed by the Web Security module when you configure linking. You need to enter a key only if you have data security add-on modules.

Troubleshooting log on

If you are unable to connect to TRITON - Data Security on the default port, refer to the **dlp-all.log** file on the Data Security Management Server (located by default in the C:\Program Files\Websense\data security\tomcat\logs\dlp directory) to verify the port.

If you are using the correct port, and are still unable to connect to TRITON - Data Security from a remote machine, make sure that your firewall allows communication on that port.

Deploying the Content Gateway module

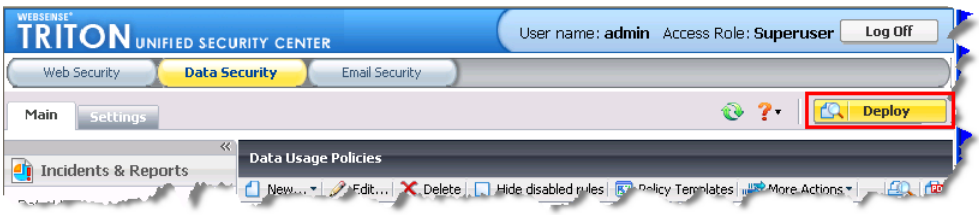
When you register the Websense Content Gateway policy engine with the Data Security Management Server, a Content Gateway module appears in the TRITON - Data Security System Modules screen. You can find this by clicking **Settings > Deployment > System Modules**.

By default, this agent is configured to monitor Web traffic, not block it, and for a default violation message to appear when an incident is triggered. If this is acceptable, you don't need to make changes to the Content Gateway configuration. You just need to deploy the new settings.

If you want to block Web traffic that breaches policy and customize the violation message, you can reconfigure the Content Gateway module. See *Configuring blocking versus monitoring*, page 129.

To deploy the Content Gateway module with its default settings:

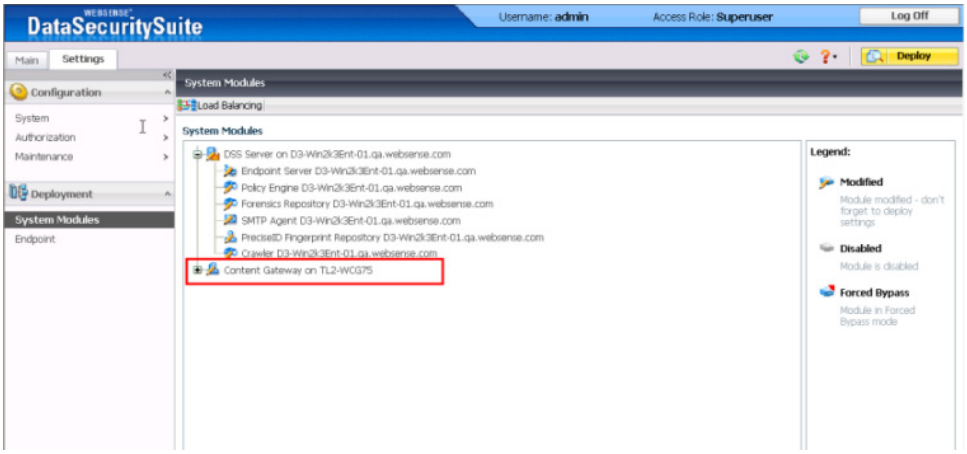
1. Log onto TRITON - Data Security.
2. Click **Deploy** to deploy your settings.



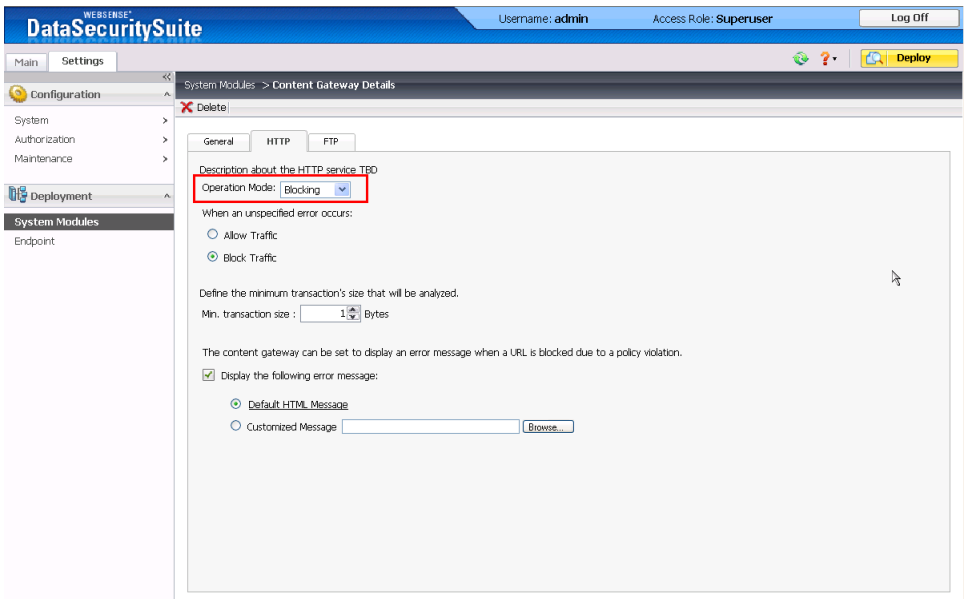
Configuring blocking versus monitoring

By default, the Content Gateway module is configured to monitor Web traffic. To block traffic:

1. From the TRITON - Data Security user interface, select **Settings > Configuration > System Modules**.
2. Select the Content Gateway module in the tree view.



3. Select the **HTTP** tab.
4. Switch **Mode** from Monitoring to Blocking**.**



5. Specify what to do in the event of an unspecified data analysis error: permit traffic or block traffic.
6. Optionally, define the smallest transaction size to be analyzed in bytes.
7. Click **Display the following error message**.
8. Click **Custom message** and browse to the message you want to display when a violation occurs.
9. Select the **FTP** tab.
10. Switch **Mode** from Monitoring to Blocking**.**
11. Define the smallest transaction size to be analyzed in bytes.

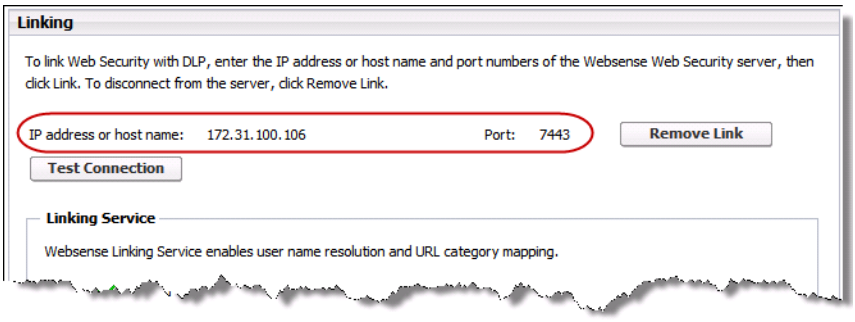
12. Click **OK** to save your changes.
13. Click **Deploy** to deploy your changes to the Websense Content Gateway.

> **Important**
> Remember that nothing is blocked until you configure policies in TRITON - Data Security with the block action. Please see *Creating data security policies*, page 134 for more information.

Verifying linking

In Chapter 4, you created a link between the TRITON - Web Security machine and the Data Security Management Server. To verify the link succeeded, navigate to **Settings > System > Linking**.

The top portion of the Linking screen should be populated with the IP address and port number of the TRITON - Web Security machine, and the button should say **Remove Link** rather than **Link**.



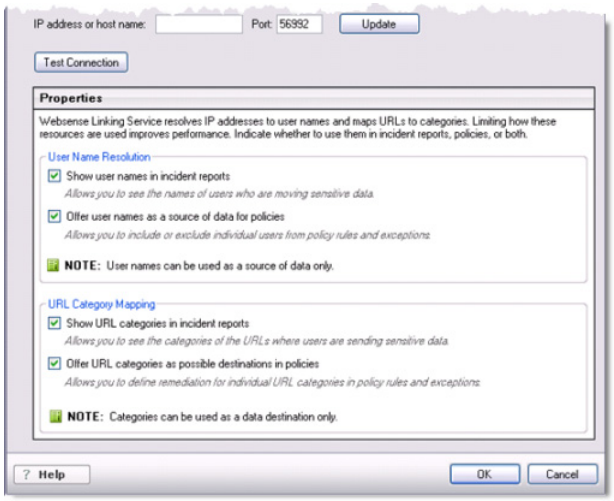
Verifying the Websense Linking Service

When you perform linking, the Data Security Management Server is automatically connected with the Websense Linking Service you installed on a Windows server. To confirm, look at the bottom portion of the Linking screen for the status **Enabled**.

The Websense Linking Service provides IP address to user name resolution. It takes advantage of the information that Websense Web Security has about users to provide IP address to user name resolution for HTTP incidents. After identifying the user, Data Security looks up that user's details in the user directory and adds that information to the incident details.

In addition, this feature allows Websense Data Security to make use of Web Security's preset and custom URL categories for accurate Web filtering.

To edit the properties of the Linking Service—for example, if it stops responding—click **Edit**. Here you can click **Update** to retrieve the latest IP address and port number for the service.



Note

If Linking Service information does not appear on this page as expected, refer to *Linking Service information is not shown in TRITON - Data Security*, page 146 for troubleshooting information.

Note that the dynamic user name resolution and category mapping that the Linking Service performs can cause latency when you are viewing reports or creating policies. To improve performance, you can limit its use to the most important functions by editing the properties below.

Resolved user names may be *sources* of data where URL categories may be *destinations*.

Field	Description
User name resolution	
Show user names in incident reports	Select this check box if you want user names to display in incident reports rather than IP addresses. This lets you determine more easily who is moving sensitive data.
Offer user names as a source of data for policies	Select this check box if you want to be able to select specific user names in rules. For example, block John Doe from posting the document MyDoc.doc to the Web.
URL category mapping	

Field	Description
Show URL categories in incident reports	Select this check box if you want URL categories to display in incident reports rather than URLs. For example, rather than displaying http://www.cnn.com, reports might display News and Media. This lets you see the type of Web site to which your sensitive data is being sent.
Offer URL categories as possible destinations in policies	Select this check box if you want to be able to select specific URL categories in rules. For example, block John Doe from posting the document MyDoc.doc to News and Media sites.

Verifying URL categories were imported

When Websense Linking Service is enabled, URL categories from the Websense Master Database are automatically imported into Data Security.This gives your DLP policies access to URL categories so you can monitor or block data leakage over Web sites. To verify that this occurred as expected:

1. Navigate to **Main > Policy Management > Resources > URL Categories**.
2. The category list should populate with the URL categories from the Websense Master Database.
3. If it does not, click **Update Now**.

Creating an administrator account

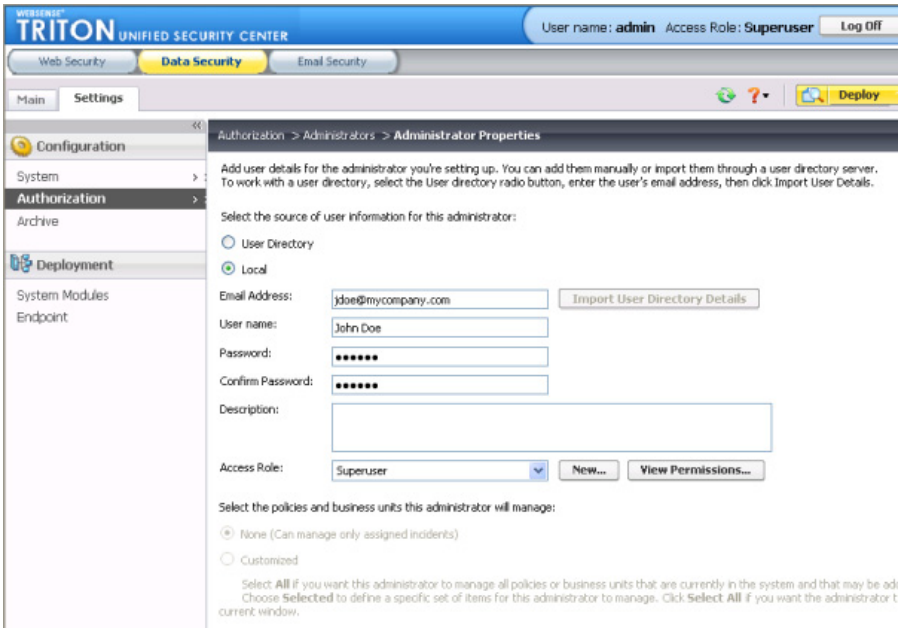
To enable joint administration (allowing a Data Security administrator to access the Web Security module and vice versa), the same administrator user name and password needs to be added to both TRITON - Web Security and TRITON - Data Security.

If you logged onto TRITON - Web Security and configured linking before logging onto TRITON - Data Security for the first time, the password for TRITON - Web Security is automatically applied to the data security module. Both have the user name, WebsenseAdministrator.

If you need to add Web Security administrators to the Data Security module:

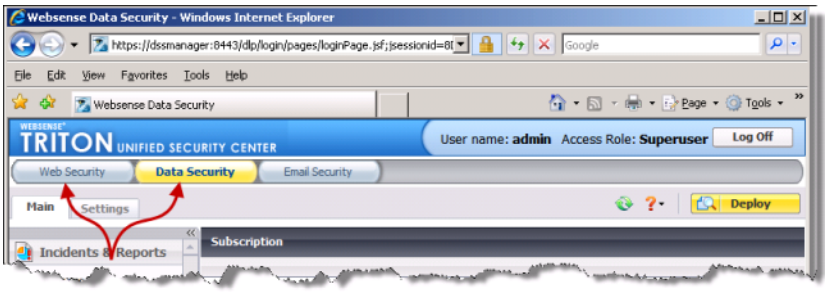
1. Go to **Settings > Configuration > Authentication > Administrators**.

2. Click **New**.



3. Follow the instructions in the TRITON - Data Security Help topic, "Adding a new Administrator" to complete this screen. Enter the credentials used in TRITON - Web Security.
4. Click **OK**.
5. Click **Deploy**.

The administrator can now access the Web Security module from the Web Security toolbar button.



Creating data security policies

In order to monitor your vital data, you must set up one or more data security policies. This is done in the TRITON - Data Security user interface. Most often, you use a policy wizard to create policies from predefined regulatory templates. This is a fast and accurate way to get started. Later, you may choose to create custom policies.

Data security policies typically define the source of the traffic to monitor (for example, the network or IP range), the conditions to watch for (for example, 5 or more

9-digit numbers with the text “SSN”), and the action to take in case of a breach (block or permit). By default, all HTTP, HTTPS, FTP, and FTP-over-HTTP destinations are monitored.

Policy creation is described in detail in the TRITON - Data Security Help. This section is designed to get you started.

Tip

To access data security help, log onto TRITON - Data Security and click the Help (**?**) button.

How data policies differ from Web policies

In the Web security portion of your Websense software, policies govern user Internet access. A Web policy is made up of:

- **Category filters** - Used to apply actions (permit, block) to Web site categories
- **Limited access filters** - Used to permit access to only a restricted list of Web sites
- **Protocol filters** - Used to apply actions to Internet protocols
- **Schedule** - Determines when each category or limited access filter and protocol filter is enforced

In the data security portion of your Websense software, policies govern data usage. Data policies contain:

- **Rules** - Provide the logic for the policy. They are the conditions that govern the behavior of the policy. When should something be blocked? When should managers be notified?
- **Exceptions** - Define the conditions that should be exempt from the rules.
- **Content classifiers** - Describe the data to be governed. You can classify data by file properties, key phrases, dictionaries, natural language processing (NLP), a database record fingerprint, a directory fingerprint, and/or a file fingerprint.
- **Resources** - Describe the source and destination of the data you want to protect, the endpoint device or application that may be in use, and the remediation or action to take when a violation is discovered (such as block or notify).

Websense Web Security Gateway Anywhere includes predefined policies for both Web and data security. You can use these policies or create custom policies as needed.

Save All versus Deploy

When you perform a task in TRITON - Web Security, and then click **OK**, your changes are cached. (Sometimes you must click **OK** both on a subordinate page and a main page to cache changes.) To save your changes and put them into use, you must click the **Save All** button.

This is different in TRITON - Data Security.

When you perform a task in TRITON - Data Security, and then click **OK**, your changes *are* saved. However, you must click **Deploy** to push the changes out to all of the data security components, including the Websense Content Gateway or V-Series appliance.

Be sure to click **Save All** when finished working in TRITON - Web Security. And be sure to click **Deploy** when finished working in TRITON - Data Security.

Getting started

There are 4 basic steps to get you started monitoring the Web for data usage. These are all done in TRITON - Data Security.

1. Configure user directory server settings. This lets you base your administrator login authentication on user directory credentials, resolve user details during analysis, and enhance the details displayed with the incident.
2. Set up alerts. This lets you configure the cases when administrators receive alerts from the system, such as when a subscription is about to expire or disk space is reaching its limit.
3. Run the first-time policy wizard. This helps you select from a rich set of predefined policies that cover the data requirements for a variety of regulatory agencies (such as GLBA, HIPAA, and Sarbanes-Oxley) all over the globe.
4. Deploy your initial settings.

These steps are described in the “Initial Setup” topic of the TRITON - Data Security Help. If you prefer to create a custom policy, you can do this as well. This is described in the “Creating Custom Policies” topic.

7 Testing Filtering

The procedures in this section assume that you have followed the steps in this guide without performing additional tasks, such as assigning custom policies to clients.

Verifying policy enforcement

You can use simple, graphical tools in TRITON - Web Security to determine which policy is enforced for a client, and whether a specific URL is permitted or blocked for a client.

1. Log on to TRITON - Web Security as WebsenseAdministrator.
2. In the right navigation pane, under Toolbox, click **Check Policy**.
3. Enter the IP address of any filtered machine in your network, and then click **Go**.
4. A pop-up window shows that the Default policy is assigned to this client.

   Once you have created custom policies and assigned them to specific clients, you can use this tool to verify that policies are being applied correctly.

   This may be especially useful when you want to find out which group or domain (OU) policies may affect a specific user.
5. Close the pop-up window, and then click the **Check Policy** tool title bar. The Toolbox once again shows a list of available tools.
6. Click **Test Filtering**.
7. Enter the IP address of a filtered machine, and then enter a URL.
   - You can get a list of test URLs from testdatabase.websense.com.
   - URLs are permitted or blocked based on the category filter enforced by the Default policy.
   - If the Default policy enforces the Monitor Only category filter, all requests will be permitted.

The Test Filtering tool shows the result returned by Filtering Service. To find out whether Content Gateway scanning would show a different result, continue to the next section.

Testing filtering through the explicit proxy

If you have modified the Default policy to enforce the Basic Security category filter, or any other category filter that blocks some requests, you can test whether Content Gateway is properly filtering client requests.

If the Default policy enforces the Monitor Only category filter (which is the default behavior), the requests attempted in step 11 will be permitted.

1. Log onto a client machine.
2. Navigate to **Control Panel > Internet Options**.
3. Click the **Connections** tab and click the **LAN Settings** button.
4. Select **Use a proxy for your LAN**.
5. Click **Advanced**.
6. Enter the IP address for the Websense Content Gateway machine and the port 8080. If you're using a V-Series appliance, enter the IP of the P1 interface.
7. Click **OK** 3 times.
8. Verify you can browse successfully.
9. If prompted, choose turn off automatic phishing filter.
10. Navigate to http://testdatabase.websense.com.
11. Try the following links in the Realtime Analysis section:
    - Malicious websites: file scanning

      This category is blocked by the Basic Security, Basic, and Default category filters.
    - Adult material: adult content

      This category is blocked by the Basic and Default category filters, but not by the Basic Security category filter.

Remember that which sites are blocked is entirely dependent on which category filter is enforced by the policy applied to the client.

Making sure that Internet activity is logged

Make sure that Filtering Service is sending correct and complete information about Internet activity to Log Server.

1. On Log Server machine, open a command prompt (**Start > Run > cmd**) and navigate to the Websense **bin** directory (C:\Program Files\Websense\bin, by default).
2. Start the **testlogserver** utility with the following parameters:

   ```
   testlogserver -port 5555 -forward <IP address>:55805
   ```

   Here, <*IP address*> is the IP address of the Log Server machine.

3. In TRITON - Web Security, navigate to the **Settings > General > Logging** page.
4. Make sure that the Log Server IP address is correct. This should be the actual IP address of the Log Server machine, and not the loopback address (127.0.0.1), even if Log Server and TRITON - Web Security are installed on the same machine.
5. Change the port to **5555**.
6. Click **Check Status** to verify the connection to testlogserver.
7. Click **OK** and then **Save All**.
8. Go (or open a remote desktop session) to a client machine configured to browse through the Content Gateway and open a Web browser.
9. Browse to a specific site, like **www.yahoo.com**.
10. On the Log Server machine, confirm that the activity is shown by testlogserver.
11. When you are finished, return to the **Settings > General > Logging** screen in TRITON - Web Security and change the logging port back to its original value (**55805**, by default). Remember to click **OK** and **Save All** to cache and then implement your change.

    Data stops flowing to testlogserver.
12. Return to the Windows command prompt and press **Ctrl+C** to stop testlogserver.

Testing hybrid filtering

Verify hybrid configuration

1. In TRITON - Web Security, navigate to the **Main > Status > Today** page.
2. Select **Hybrid Service Status**.
3. Verify that Sync Service has sent directory and policy information to the hybrid service.
4. If Internet traffic from your site has been sent through the hybrid service, also verify that Sync Service has received reporting information from the hybrid service.

   Note that there will be a lag between the time that traffic passes through the hybid service and the time that the reporting data is retrieved by Sync Service and recorded by Log Server.

Check that hybrid filtering is functioning

1. In TRITON - Web Security, navigate to the **Settings > Hybrid Configuration > User Access** page.
2. Expand the section at the bottom of the page: **Verify End User Configuration**.
3. Copy and paste the link from this section into a browser. The response confirms whether you are being filtered by the hybrid proxy or not.

4. From the top of the same page, make a note of the PAC file URL assigned to your organization. A unique PAC file is generated for each hybrid filtering account.
5. Open a remote desktop connection to a client machine at a remote location. This must be a location that you configured in TRITON - Web Security as a filtered location. (**Settings > Hybrid Configuration > Filtered Locations**.)
6. On the remote machine, open a Web browser and configure it to point to the PAC file. For example, if you are using Internet Explorer:
   a. Go to **Tools > Internet Options > Connections > LAN Settings**.
   b. Select U**se Automatic Configuration Script** and enter your PAC file URL.
   c. Enter the URL of the PAC file.
   d. Click **OK** until you have saved your settings change and closed the Internet Options dialog box.
7. Attempt to connect to a URL. The request should be filtered by your organization's Default policy or by a user policy (if you have synchronized users).
   - If you are connecting from an unknown location, a block page prompts you to identify yourself or self-register for the hybrid service.

Using reports to verify Web filtering

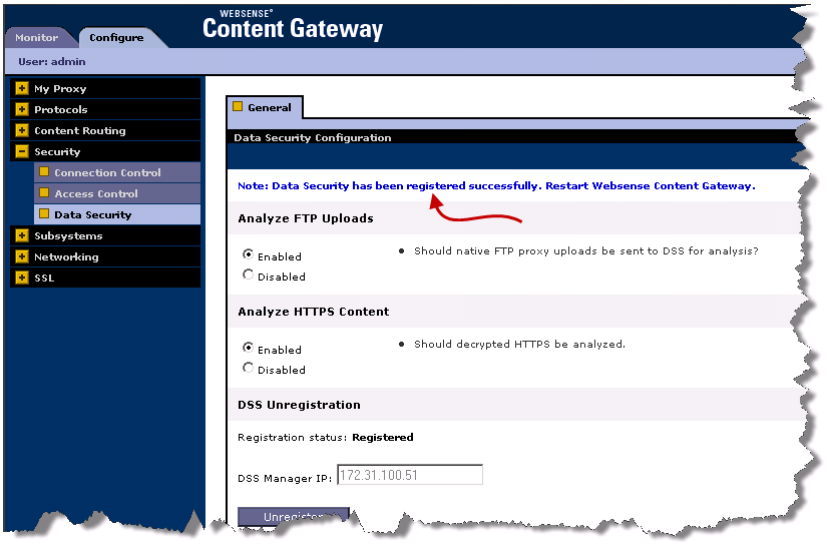
TRITON - Web Security includes both prenentation and investigative reports to help you assess security in your enterprise. These same reports can also be used to verify that your tests have been working properly. For example:

- Examine the "Source IP" column in detail reports. This lists the IP address of the machine from which the request was made. If the traffic came from a known filtered location, you know it's been filtered by the hybrid service.
  a. Select **Reporting > Investigative Reports**.
- Examine the scanning activity group in the Report Catalog for presentation reports. This displays your traffic flow and tells you whether something has been blocked or permitted.
  a. Select **Reporting > Presentation Reports > Report Catalog**.
  b. Expand the Scanning Activity group to see its corresponding templates and custom reports.
  c. Click on a template or report title to see a brief description of what it includes.
  d. Click **Run**.

Testing data loss prevention

Test that Content Gateway is properly registered

In Content Gateway Manager, navigate to **Configure > Security > Data Security**, and read the alert at the top of the screen.

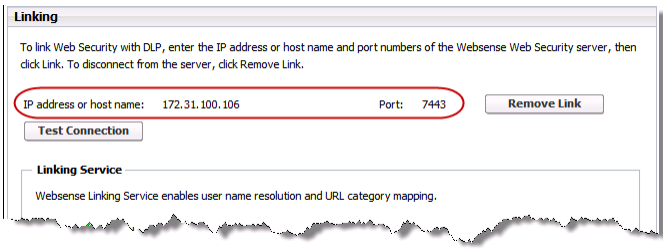


In TRITON - Data Security, go to **Settings > Deployment > System Modules**. If registration succeeded, there should be a Content Gateway module listed in the modules tree.

If registration fails, see *Cannot register the Content Gateway with Data Security*, page 145 for troubleshooting tips.

Verify that linking succeeded

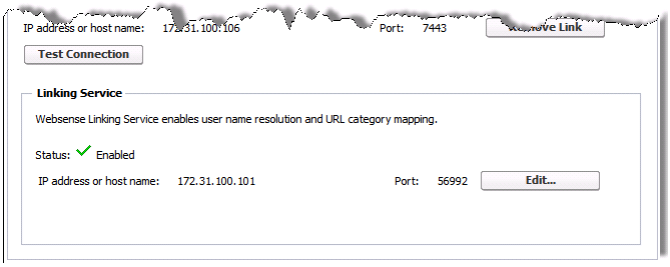
In topic 3, you established linking with the Data Security module from TRITON - Web Security. To verify that linking succeeded, log onto TRITON - Data Security and navigate to **Settings > System > Linking**. The top portion of the screen should be populated with the IP address of the TRITON - Web Security machine, and the button should say **Remove Link**, not **Link**.



Refer to *Linking has not been configured*, page 146 for tips on troubleshooting Linking issues.

Test that the Websense Linking Service is enabled

1. On the **Settings > System > Linking** page of TRITON - Data Security, confirm that the status of the Websense Linking Service is **Enabled**. If it is not, enable it and click **Edit**. Enter the IP address of the Windows machine where you installed the Linking Service and click **OK**.



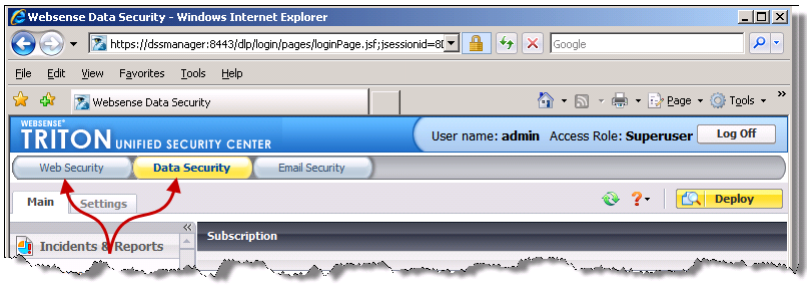
2. Navigate to **Main > Resources > URL Categories**.
3. Select the **Update Now** button. URL categories should be imported from the Websense Master Database and listed on the screen.

Refer to *Linking has not been configured*, page 146 for troubleshooting Linking Service issues.

Test that joint administration works

Once there is an administrator in both TRITON - Web Security and TRITON - Data Security, confirm that he or she can access both modules without re-entering credentials.

1. From TRITON - Web Security, click the **Data Security** button on the button bar.



2. From TRITON - Data Security, click the **Web Security** button.

You should not be prompted for logon credentials. If you are, go back and verify that the same user name and password are used for the administrator who is logged on.

Test that outbound HTTP data is detected

1. In TRITON - Data Security, create a policy containing a keyword classifier and deploy it to the Content Gateway module.
   a. Navigate to **Main > Content Classifiers > Key Phrases**.
   b. Select **New**.
   c. Create a key phrase classifier and click **OK**.
   d. When prompted to add the classifier to a rule in a policy, select **OK**.
   e. Enter a rule name, click **Add this rule to a new policy**, and enter a policy name.
   f. Click **OK** and **Deploy**.
2. From a client machine configured to go through the proxy, launch Outlook Express and send an email that uses the keyword. If you chose the action “Block” in TRITON - Data Security an error results. If you chose the action “Monitor”, the email is delivered normally.
3. Back in TRITON - Data Security, go to **Main > Today** to see if a new incident was added to the 24-hour graphical summary. If the incident appears, filtering is working properly.
4. Navigate to **Main > Data Usage > Incidents (last 3 days)**.
5. Select your incident and view the corresponding report.

Analyze traffic in Content Gateway Manager

1. In Content Gateway Manager, navigate to **Monitor > Security > Data Security**.
2. Confirm that traffic has been filtered through the proxy by analyzing statistics. You can see:

Statistic	Description
Total Posts	Total number of posts sent to Data Security.
Total Analyzed	Total number of posts analyzed by Data Security.
FTP Analyzed	Total number of FTP requests analyzed by Data Security.
Blocked Requests	Total number of requests blocked after analysis and policy enforcement.
Allowed Requests	Total number of requests allowed after analysis and policy enforcement.
Failed Requests	Total number of posts sent to Data Security that timed out or otherwise failed to complete.
Huge Requests	Total number of requests that exceeded the maximum transaction size.
Tiny Requests	Total number of requests that were smaller than the minimum transaction size.
Decrypted Requests	Total number of SSL requests decrypted and sent to Data Security.

8 Troubleshooting

This section includes troubleshooting tips that are specific to Websense Web Security Gateway Anywhere configurations—namely those relating to hybrid filtering and Web DLP.

Cannot register the Content Gateway with Data Security

If you cannot register Websense Content Gateway with the Data Security Management Server—you receive an error in Content Gateway Manager—be sure that you can ping the Data Security Management Server from the proxy machine. (Go to the Linux command line and ping the IP address of the Data Security Management Server.)

If the ping fails, make sure that you have the correct IP address for the Data Security Management Server by going to that machine and running **ipconfig** from the command line.

If the proxy is on a V-Series appliance, try pinging the IPv4 address of the appliance's C interface from the Data Security Management Server.

If the proxy is not on a Websense appliance, try pinging the IPv4 address of the Content Gateway host system eth0 network interface from the Data Security Management Server. The registration process requires that Content Gateway is reachable on eth0. After registration, the IP address may move to another network interface on the system, but that IP address must remain available while the 2 modules are being registered.

If Content Gateway is deployed as a transparent proxy and the communication interface ("C" on a V-Series appliance) is subject to transparent routing, the registration process was likely intercepted by the transparent routing and prevented from completing. Ensure that traffic to and from the communication interface is not subject to transparent routing.

If registration still fails, make sure that neither the proxy machine or the Data Security Management Server has a machine name with a hyphen in it. This has been known to cause registration problems.

And make sure the Content Gateway machine has a fully qualified domain name (FQDN) that is unique in your network. Host name alone is not sufficient to register the proxy with the Data Security Management Server.

Linking has not been configured

When your Websense software subscription includes both Web and data security, you have the option to link the 2 security solutions. A Health Alert appears on the Status > Today page in TRITON - Web Security when your subscription allows linking, but it has not been configured.

When you configure linking:

- Data security software gains access to user data gathered by Web security components.
- Data security software can access Master Database categorization information.
- Administrators can be given seamless access to both the Web Security and the Data Security modules of the TRITON Unified Security Center.
- To configure linking between your Web and data security solutions, go to the **Settings > Linking** page in TRITON - Web Security.

If you have trouble configuring linking, make sure that the TRITON - Web Security machine can access the Data Security Management Server. See *Unable to connect to TRITON - Data Security*, page 147 for instructions.

Linking Service information is not shown in TRITON - Data Security

If you do not see information about the Websense Linking Service on TRITON - Data Security's Linking page, it means that the Linking Service was never installed. Typically, the Linking Service is installed as part of a custom Web Security installation on a Windows machine.

When you configure linking, the system attempts to install the Linking Service automatically. If Web Security's Policy Server is running on Windows, the Linking Service is installed on this machine. If not, it is installed on the Log Server machine.

If the Policy Server is running on Linux and TRITON - Web Security does not have access to a Log Server with its own Policy Server, then the Linking Service cannot be auto-installed, and you will not see Linking Service information on the TRITON - Data Security Linking page.

To resolve this, you must add the Websense Linking Service manually to a Windows server (using the Web Security custom installation). Then, when you configure linking, TRITON - Data Security looks for the Websense Linking Service and enables

it. It displays the IP address and port number for the Linking Service that it found in the Linking Service section of the screen.

Alternatively, you can install Log Server, retry Linking, and auto-install the Linking Service as described above.

Websense Linking Service stopped responding

In TRITON - Data Security, take these steps:

1. Choose **Settings > Configuration > System > Linking**
2. Click **Edit** under Linking Service.
3. Make sure the **Enabled** check box is selected.
4. Click **Update** to retrieve the latest host and port settings of the linking service. These settings can change.

Unable to connect to TRITON - Data Security

If you receive an error when you try to connect to TRITON - Data Security from TRITON - Web Security, either a configuration or a communication problem is likely at fault.

To troubleshoot this problem, first check to see if you can open TRITON - Data Security directly. To do this, open a Web browser on the machine that you are currently using to access TRITON - Web Security, and then enter the TRITON - Data Security URL and port in the address bar. For example:

```
https://<IP address or name>:8443/dlp/pages/mainFrame.jsf
```

Replace *<IP address or name>* with the IP address or fully qualified domain name of the Data Security Management Server machine.

- If you are able to connect directly, go to the Settings > General > Linking page in TRITON - Web Security and verify that the IP address or host name provided matches the one that you used to connect directly to TRITON - Data Security.

  Note that the connection port entered on the Linking page (by default, 7443) is not the same port used when you access TRITON - Data Security directly.
- If you cannot connect directly, there may be a network communication problem, or a problem on the Data Security Management Server machine.
  - Make sure that the Data Security Management Server machine is on.
  - Use the Windows Services dialog box to verify that the Data Security Management Server service has started.
  - Check the Windows Event Viewer on the Data Security Management Server machine for errors from the Data Security Management Server.

- Use the **ping** utiliy to verify that the TRITON - Web Security machine can connect to the TRITON - Data Security machine.
- If ping shows that data can be passed between the machines, use the **telnet** utility to verify that the linking port (7443, by default) is open between the two machines.
- Check the Windows Event Viewer on the TRITON - Web Security machine for errors from Linking Service.

> **Note**
> If you move the location of TRITON - Web Security or TRITON - Data Security, linking breaks. You must remove the old link and create a new one, pointing to the new IP address.

Administrator unable to access TRITON - Data Security

If you receive an error when you click **Data Security** in TRITON - Web Security, the Websense user account or network account that you use to log on to TRITON - Web Security may not have been granted permission to access TRITON - Data Security. In order to change between TRITON Unified Security Center modules, an administrator must:

- Be given access to each module
- Have the same account type (Websense user or network) in each module
- Have the same user name in each module
- Use the same password to access each module

The default TRITON - Web Security account, **WebsenseAdministrator**, does not have TRITON - Data Security access by default. Likewise, the default TRITON - Data Security account, **admin**, does not have TRITON - Web Security access by default.

Unconditional Super Administrators can configure each administrator's level of access to modules and features of the TRITON Unified Security Center.

Unsupported Data Security Management Server version

Linking Websense Web Security and Websense Data Security, among other things, connects the Web Security and Data Security modules of the TRITON Unified Security Center.

In order for linking to succeed, your Websense Web Security version must match your Websense Data Security version. If you have not upgraded Websense Data Security to version 7.5, perform the upgrade first, and then use the Settings > General > Linking page in TRITON - Web Security to link your solutions.

Hotfix (patch) versions should not affect compatibility between Websense solutions.

Sync Service is not available

In Websense Web Security Gateway Anywhere deployments, Websense Sync Service is responsible for communication between the on-premises and hybrid services. Sync Service:

- Sends policy configuration data to the hybrid service
- Sends user information collected by Directory Agent to the hybrid service
- Receives reporting log records from the hybrid service

If you have not yet activated hybrid filtering, or if you have attempted to activate hybrid filtering, but have not been able to do so, note that your local Websense software components must be able to communicate with Sync Service before the connection to the hybrid service can be created.

To troubleshoot this issue, make sure that:

- Sync Service is running.
- Sync Service is successfully binding to the correct IP address and port.
  - The IP address and port that Sync Service is attempting to use are listed in the **syncservice.ini** file, located in the Websense **bin** directory on the Sync Service machine.
  - The IP address and port shown on the Settings > Hybrid Configuration > Shared User Data page in TRITON - Web Security must match those listed in the **syncservice.ini** file. If you update the configuration file, also manually update the Settings page.
  - The IP address and port in the **syncservice.ini** file must match the Sync Service IP address and port values in the **das.ini** file (located in the Websense **bin** directory on the Directory Agent machine).

  Verify that no other service on the Sync Service machine is binding to the IP address and port that Sync Service is attempting to use. If you suspect that Sync Service is unable to bind to the correct IP address and port, stop the service, open a command prompt, and try to start the service in console mode:

  ```
  syncservice -c
  ```

  In console mode, Sync Service displays the IP address and port that it is using, or displays an error, if it is unable to bind to the IP address and port.
- The Sync Service machine can communicate with the Policy Broker machine on port 55880.
- The Sync Service machine can connect to the Policy Server machine on ports 55806 and 40000, and receive data from Policy Server on ports 55830 and 55831.
- The TRITON - Web Security machine can create an HTTP connection to the Sync Service machine on port 55832.

Also check the Windows Event Viewer or **websense.log** file for errors from Sync Service.

Directory Agent is not running

In Websense Web Security Gateway Anywhere deployments, Websense Directory Agent gathers user information from your directory service and sends it to the hybrid service for use in applying filtering policies.

When Directory Agent is not available, the hybrid service's user data may become outdated.

Make sure that Directory Agent is installed, and that the service or daemon is running.

- Windows: Use the Windows Services dialog box to start the service.
- Linux: Use the /opt/Websense/WebsenseDaemonControl command to start the daemon.

If Directory Agent is running, but the alert message continues to appear, verify that:

- The Directory Agent machine can communicate with the Policy Server machine.
- The Directory Agent machine can communicate with the Sync Service machine.
- The firewall permits communication on the Directory Agent port.

If the service starts, but does not continue to run:

- Check the Event Viewer (Windows) or websense.log file (Linux) for errors.
- Navigate to the Websense **bin** directory (C:\Program Files\Websense\bin or /opt/Websense/bin/, by default) and verify that the **das.ini** file exists, and that it has not been corrupted or truncated.
- Make sure that there is enough disk space on the Directory Agent machine to store a full snapshot of your directory. For example, a snapshot of a 200,000 user directory requires about 100 MB of disk space.
- Make sure that there is enough available memory for Directory Agent to compare its current snapshot with the previous one. For example, comparing snapshots of a 200,000 user directory requires about 100 MB of memory.

Directory Agent cannot connect to the domain controller

Directory Agent must be able to connect to the domain controller to gather user information from the directory service. If there are communication problems between the Directory Agent machine and the domain controller, the hybrid service's user data may become outdated, leading to incorrect filtering.

To troubleshoot this problem:

- Make sure that the Directory Agent machine is bound to the domain, and that the firewall permits communication on the directory service port.
- Go to the Settings > General > Directory Services page and verify that your directory service configuration has not changed since you last updated your Directory Agent settings.
- Go to the Settings > Hybrid Configuration > Shared User Data page and verify that Directory Agent is attempting to search a valid context (path) for user and group information. To do this:
  - If you are using Windows Active Directory, click a directory server name or IP address, and then click Test Context. Repeat this process for each global catalog server.
  - If you are using Sun Java System directory or Novell eDirectory, click Test Context.
- On the Shared User Data page, also make sure that the context is not only valid, but appropriate. The context should be limited to include only those users and groups filtered by the hybrid service.
- Still on the Shared User Data page, make sure that the Directory Search option is set correctly, so that Directory Agent is searching only the relevant portion of your directory service.
- Verify that it is possible to connect to the directory service IP address and port from the Directory Agent machine.

Directory Agent does not support this directory service

Directory Agent is only able to retrieve user and group information from LDAP-based directory services. Windows NT Directory / Active Directory (Mixed Mode) is not supported. The supported directory services include:

- Windows Active Directory (Native Mode)
- Sun Java System Directory
- Novell eDirectory
- If you are not using a supported directory service, hybrid filtering can still be applied to filtered locations. User and group-based filtering, however, cannot be performed.

Alerts were received from the hybrid service

When the hybrid service encounters a problem that could affect your organization, it sends an alert to your installation of Sync Service. Alerts are sent for issues that affect either hybrid filtering as a whole, or that are specific to your account. When the alert is received:

- A general alert is displayed under Health Alerts on the Status > Today page in TRITON - Web Security.
- A more specific alert is shown on the Status > Alerts page under Hybrid Filtering Alerts.

If there are steps that you can take to correct the problem (for example, prompting Directory Agent to re-send user information, or clicking Save All to prompt Sync Service to re-send policy information), that information is included in the detailed alert message on the Status > Alerts page.

In many cases, alerts from hybrid filtering are informational, making sure that you are aware that a temporary issue may be preventing user or policy information from being received, or reporting data from being sent. No action on your part is required to address such issues.

When the condition causing the problem has been resolved, both the Health Alert on the Status > Today page and the alerts on the Status > Alerts page are cleared.

Unable to connect to hybrid service

The on-premises and hybrid portions of your Websense Web Security Gateway Anywhere solution must communicate regularly to ensure consistent filtering and accurate reporting.

Sync Service may be prevented from accessing the hybrid service due to network problems, either affecting Internet or internal network connections.

- Use a browser or the **ping** utility to verify that the Sync Service machine can connect to the Internet.
- Make sure that an HTTPS connection to the Internet can be established from the Sync Service machine. Sync Service uses port 443 to connect to the hybrid service.
- Make sure that Sync Service can communicate with other on-premises components in the network via ports 55830 and 55831.

Also verify that there is not a problem preventing the hybrid service from accepting the Sync Service connection.

- Check the Hybrid Filtering Alerts table on the Status > Alerts page for information from the hybrid service.
- Make sure that administrators have been monitoring the email account provided as a contact address on the Settings > General > Account page for messages from Websense Technical Support.

Missing key hybrid configuration information

In hybrid filtering environments, Sync Service provides an account identifier each time it connects to the hybrid service to send or retrieve information. This identifier is unique to your organization, and updated each time the WebsenseAdministrator password changes.

Under rare circumstances, possibly involving a serious problem with the Policy Database, the connection between your on-premises software and the hybrid service may be lost. In these cases, you must request a security token, used to generate a new identifier for your hybrid filtering account. The security token is sent to the **contact email address** specified on the Settings > General > Account page.

If you receive the alert message, “Missing configuration information; connection to hybrid filtering lost,” either no contact email address has been provided, or the contact email address is no longer valid.

Hybrid filtering data does not appear in reports

If Internet activity information for users filtered by the hybrid service does not appear in TRITON - Web Security reports, first make sure that:

- A hybrid logging port is configured on the **Settings > General > Logging** page.
- The **Have the hybrid service collect reporting data for the clients it filters** check box is selected on the **Settings > Hybrid Configuration > Scheduling** page.
- The **Status > Today > Hybrid Service Status** page shows that Sync Service has successfully connected to the hybrid service, and retrieved log records.
- No health alerts appear on the **Status > Today** page indicating Sync Service communication problems or Log Server errors.

Refer to TRITON - Web Security Help on assistance configuring these settings.

If your deployment uses distributed logging, in which multiple, remote Log Servers send data to a centralized Log Server instance, also make sure that Sync Service is configured to communicate with the central Log Server. Hybrid logging data cannot be passed to the central Log Server by remote Log Server instances.

APPENDIX A

Copyrights

For other copyright information, refer to:

- *Trademarks*
- *Open Source Copyrights*

Trademarks

Open Source Copyrights

The following trademarks are for open source software used by Websense.

7-Zip

License for use and distribution
7-Zip Copyright (C) 1999-2007 Igor Pavlov.
Licenses for files are:
1) 7z.dll: GNU LGPL + unRAR restriction
2) All other files: GNU LGPL
The GNU LGPL + unRAR restriction means that you must follow both GNU LGPL rules and unRAR restriction rules.
Note:
You can use 7-Zip on any computer, including a computer in a commercial organization.
You don't need to register or pay for 7-Zip.

Curl

MITX License
COPYRIGHT AND PERMISSION NOTICE
Copyright (c) 1996 - 2001, Daniel Stenberg, <daniel@haxx.se>.
All rights reserved.
Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software.

ehcache

Copyright 2003-2007 Luck Consulting Pty Ltd
Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License.
You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0
Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

GDChart

Portions copyright 1994, 1995, 1996, 1997, 1998, 1999, 2000 by Cold Spring Harbor Laboratory. Funded under Grant P41-RR02188 by the National Institutes of Health.
Portions copyright 1996, 1997, 1998, 1999, 2000 by Boutell.Com, Inc.
Portions relating to GD2 format copyright 1999, 2000 Philip Warner.
Portions relating to PNG copyright 1999, 2000 Greg Roelofs.
Portions relating to libttf copyright 1999, 2000 John Ellson (ellson@lucent.com).
Portions relating to JPEG copyright 2000, Doug Becker and copyright (C) 1994-1998, Thomas G. Lane. This software is based in part on the work of the Independent JPEG Group.
Portions relating to WBMP copyright 2000 Maurice Szmurlo and Johan Van den Brande.
Permission has been granted to copy, distribute and modify gd in any context without fee, including a commercial application, provided that this notice is present in user-accessible supporting documentation.
This does not affect your ownership of the derived work itself, and the intent is to assure proper credit for the authors of gd, not to interfere with your productive use of gd. If you have questions, ask. "Derived

works" includes all programs that utilize the library. Credit must be given in user-accessible documentation.

This software is provided "AS IS." The copyright holders disclaim all warranties, either express or implied, including but not limited to implied warranties of merchantability and fitness for a particular purpose, with respect to this code and accompanying documentation.

Although their code does not appear in gd 1.8.3, the authors wish to thank David Koblas, David Rowley, and Hutchison Avenue Software Corporation for their prior contributions.

GNU LGPT

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Libnet

$Id: COPYING,v 1.1.1.1 2002/08/05 22:26:04 route Exp $

libnet 1.1.x

Copyright (c) 1998 - 2002

Mike D. Schiffman <mike@infonexus.com>

http://www.packetfactory.net/libnet

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Net-SNMP

Various copyrights apply to this package, listed in 4 separate parts below. Please make sure that you read all the parts. Up until 2001, the project was based at UC Davis, and the first part covers all code written during this time. From 2001 onwards, the project has been based at SourceForge, and Networks Associates Technology, Inc hold the copyright on behalf of the wider Net-SNMP community, covering all derivative work done since then. An additional copyright section has been added as Part 3 below also under a BSD license for the work contributed by Cambridge Broadband Ltd. to the project since 2001. An additional copyright section has been added as Part 4 below also under a BSD license for the work contributed by Sun Microsystems, Inc. to the project since 2003. Code has been contributed to this project by many people over the years it has been in development, and a full list of contributors can be found in the README file under the THANKS section.

---- Part 1: CMU/UCD copyright notice: (BSD like) -----

Copyright 1989, 1991, 1992 by Carnegie Mellon University

Derivative Work - 1996, 1998-2000

Copyright 1996, 1998-2000 The Regents of the University of California

All Rights Reserved

Permission to use, copy, modify and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appears in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU and The Regents of the University of California not be used in advertising or publicity pertaining to distribution of the software without specific written permission.

CMU AND THE REGENTS OF THE UNIVERSITY OF CALIFORNIA DISCLAIM ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL CMU OR THE REGENTS OF THE UNIVERSITY OF CALIFORNIA BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM THE LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

---- Part 2: Networks Associates Technology, Inc copyright notice (BSD) -----

Copyright (c) 2001-2003, Networks Associates Technology, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 3: Cambridge Broadband Ltd. copyright notice (BSD) -----

Portions of this code are copyright (c) 2001-2003, Cambridge Broadband Ltd.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* The name of Cambridge Broadband Ltd. may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDER BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 4: Sun Microsystems, Inc. copyright notice (BSD) -----

Copyright © 2003 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara,

California 95054, U.S.A. All rights reserved.

Use is subject to license terms below.

This distribution may include materials developed by third parties.

Sun, Sun Microsystems, the Sun logo and Solaris are trademarks or registered trademarks of Sun Microsystems, Inc. in the U.S. and other countries.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the fol-

lowing disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Sun Microsystems, Inc. nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

---- Part 5: Sparta, Inc copyright notice (BSD) -----

Copyright (c) 2003-2004, Sparta, Inc

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* Neither the name of the Networks Associates Technology, Inc nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.Y OF SUCH DAMAGE.

MetaKit

LICENSE AND COPYRIGHT STATEMENT

==========

Copyright (c) 1996-1999 Jean-Claude Wippler

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

PCAP

License: BSD

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the

following disclaimer in the documentation and/or other materials provided with the distribution.

3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Quartz

All source code, binaries, documentation, and other files in this distribution are subject to the following copyright and license agreement, unless otherwise documented:

Copyright 2004-2005 OpenSymphony

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

OpenLDAP

The OpenLDAP Public License

Version 2.7, 7 September 2001

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain copyright statements and notices,

2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and

3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ``AS IS" AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

Copyright 1999-2001 The OpenLDAP Foundation, Redwood City,

California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

1. OpenSSL

OpenSSL

==========

Copyright (c) 1998-2002 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

6. Redistributions of any form whatsoever must retain the following acknowledgment:

"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are aheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

"This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence [including the GNU Public Licence.]

Sigar

Sigar is distributed under the terms of the GPL. Websense makes no modifications to any GPL copyrighted source code. Information about the GPL and code covered under this license can be found at http://www.gnu.org.

Jasper

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed. [This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Jasper is distributed under the terms of the GPL. Websense makes no modifications to any GPL copyrighted source code. Information about the GPL and code covered under this license can be found at http://www.gnu.org.

SPRING FRAMEWORK

Spring Framework/Apache License/Httpd server/commons

All Spring projects are licensed under the terms of the Apache License, Version 2.0.

Version 2.0, January 2004

http://www.apache.org/licenses/

JAVA

Sun Microsystems, Inc. Binary Code License Agreement
for the JAVA 2 PLATFORM STANDARD EDITION DEVELOPMENT KIT 5.0

STLPort

Copyright (c) 1994
Hewlett-Packard Company

Copyright (c) 1996-1999
Silicon Graphics Computer Systems, Inc.

Copyright (c) 1997
Moscow Center for SPARC Technology

Copyright (c) 1999, 2000, 2001, 2002
Boris Fomitchev

This material is provided "as is", with absolutely no warranty expressed or implied. Any use is at your own risk.

Permission to use or copy this software for any purpose is hereby granted without fee, provided the above notices are retained on all copies.

Permission to modify the code and to distribute modified code is granted, provided the above notices are retained, and a notice that the code was modified is included with the above copyright notice.

Samba

Samba is distributed under terms of the GPL. Websense makes no modifications to any GPL copyrighted source code. Information about the GPL and code covered under this license can be found at http://www.gnu.org.

Gzip

Gzip is covered under the LGPL. Websense makes no modifications to any LGPL copyrighted source code. Information about the LGPL and code covered under this license can be found at http://www.gnu.org.

Beecrypt

Beecrypt is distributed under terms of the LGPL. Websense makes no modifications to any LGPL copyrighted source code. Information about the LGPL and code covered under this license can be found at http://www.gnu.org. Information about Beecrypt can be found here - http://beecrypt.sourceforge.net/.

Tomcat

Apache License Version 2.0, January 2004
http://www.apache.org/licenses/

unRAR restriction

The decompression engine for RAR archives was developed using source code of unRAR program. All copyrights to original unRAR code are owned by Alexander Roshal.

The license for original unRAR code has the following restriction:

The unRAR sources cannot be used to re-create the RAR compression algorithm, which is proprietary. Distribution of modified unRAR sources in separate form or as a part of other software is permitted, provided that it is clearly stated in the documentation and source comments that the code may not be used to develop a RAR (WinRAR) compatible archiver.

Xerces

Apache License
Version 2.0, January 2004
http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document. "Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License. "Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived

from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, spe-

cial, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Index

W