Getting Started

Websense® V5000 G2 Appliance
for Web Security

v7.5.4

Published 2011 Revision A
Printed in the United States of America and Ireland

The products and/or methods of use described in this document are covered by U.S. Patent Numbers 5,983,270; 6,606,659; 6,947,985; 7,185,015; 7,194,464 and RE40,187 and other patents pending.

Every effort has been made to ensure the accuracy of this manual. However, Websense, Inc., makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Websense, Inc., shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Trademarks

Websense is a registered trademark of Websense, Inc., in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

Contents

Topic 1 **Introducing the V5000 G2 Appliance 5**

Software provided on the appliance 6

Software that runs off the appliance 7

Database management software 7

TRITON - Web Security 7

Third-party integration software off the appliance 8

Microsoft ISA Server and Forefront TMG 8

How Websense filtering works with Microsoft ISA/TMG 8

Supported integration versions 9

Installation 9

Cisco PIX and Cisco ASA 10

How Websense filtering works with Cisco products 10

Supported Cisco integration product versions 11

Citrix Presentation Server and XenApp 11

Supported Citrix versions 11

Client computers 12

Installation 12

Windows Server requirements for Web security components 13

Hardware 13

Operating System 13

Additional software for accessing the TRITON manager 13

Database Engine 14

Directory Service. 14

Other servers 15

Network scenarios 15

Single appliance deployment 16

Multiple appliance deployment 17

Topic 2 **Setting up the V5000 G2 appliance 19**

Set up the appliance hardware 19

Perform initial command-line configuration 20

Configure the appliance 21

Database management software 25

TRITON - Web Security 25

Third-party integration software and Websense plug-in. 25

Recovering the appliance from DVD 26

Topic 3 **Installing Off-Box Components. 29**

Before installing off-box components 29

Configure TRITON - Web Security 39
Special directory service considerations 42
Test and refine your policies 43
Logon Portal 44

1 Introducing the V5000 G2 Appliance for Web Security

The Websense V5000 G2 appliance for Web Security v7.5.4 is a high-performance security appliance with a hardened operating system, optimized for detecting, categorizing, and managing Web traffic.

Working in conjunction with integration software, Websense software provides the engine and configuration tools to develop, monitor, and enforce Internet access policies.

Together, a series of Websense components provide Internet filtering, user identification, alerting, reporting, and troubleshooting capabilities.

After installation and setup, the V5000 G2 appliance applies the **Default** policy to monitor Internet usage without blocking requests. This policy governs Internet access for all clients in the network, until you define your own policies and assign them to clients. Even after you have created your custom filtering settings, the Default policy is applied any time a client is not governed by any other policy.

The process of creating filters, adding clients, defining policies, and applying policies to clients is described in the TRITON - Web Security Help system. The Help system is embedded in the TRITON console and is also available online at MyWebsense.com.

The appliance offers:

- Command Line Interface (CLI), to enter basic control commands for initial appliance setup. The CLI commands are entered from a USB keyboard and monitor or a serial port connection.
- Appliance Manager, a Web-based configuration interface that provides management features:
  - System dashboard, with up-to-the-minute status of the software modules and system resources on the appliance.
  - Appliance configuration and network settings.
  - System administration, including patch management; troubleshooting tools with basic command-line utilities; backup; and restore.
- Logging of events related to appliance configuration and patching. Log entries can be viewed in Appliance Manager, and the entire log file can be downloaded for later viewing.
- Integrated Web filtering after minimal initial configuration.

- Full customization of Web filtering, available through separate Web-based configuration interfaces.
- Optional integration with Microsoft ISA Server or Microsoft Forefront TMG; Cicso PIX or Cisco ASA; and Citrix Presentation Server or Citrix XenApp.

Software provided on the appliance

With the appliance-based Web Security 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
    - TRITON - Web Security (optional; can be run on separate Windows server)
        - Investigative Reports Scheduler
        - Manager Web Server
        - Reporting Web Server
        - Reports Information Service
- Network Agent (Network Agent can monitor all traffic, or can instead be used to monitor only non-HTTP protocols if a third-party integration product is used at your site.)

Larger enterprises might use 2 or more 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. In all cases, Network Agent runs as a separate module on each appliance.

Software that runs off the appliance

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

- Log Server (required for reporting)
- (optional) Transparent identification agents (for filtering by user or group)
  - DC Agent
  - Logon Agent
  - eDirectory Agent
  - RADIUS Agent
- (optional) Remote Filtering Server (required for filtering roaming users)
- (optional) Integration plug-in (required only for Microsoft or Citrix integration deployment, described later)

Database management software

You are required to have a Windows database server running a supported version of Microsoft SQL Server. This is where the Log Database of reporting data is built. Log Database provides the information for Websense Web Security reporting.

TRITON - Web Security

The **TRITON - Web Security** manager is pre-installed on the appliance as a convenience for evaluations and small installations. The manager is used to set up filtering policies, assign policies to users and groups, read alerts, and perform other management tasks.

The **TRITON - Web Security** manager provides filtering reports that can be used to create and schedule custom reports.

To optimize performance, organizations with high traffic volume or large reporting needs can install the **TRITON - Web Security** manager on a ***separate Windows server***.

TRITON - Web Security services include:

- Investigative Reports Scheduler
- Manager Web Server
- Reporting Web Server
- Reports Information Service

Third-party integration software off the appliance

At your option, Websense security software running on the V5000 G2 appliance can be integrated with the following third-party products running on another server. When used, the third-party product filters HTTP/HTTPS/FTP traffic, and Network Agent monitors all other protocols. If your site does not use an integration product, then Websense Network Agent manages all traffic.

- *Microsoft ISA Server and Forefront TMG*
- *Cisco PIX and Cisco ASA*
- *Citrix Presentation Server and XenApp*

Microsoft ISA Server and Forefront TMG

Full details about integrating Websense software with Microsoft® Internet Security and Acceleration (ISA) Server and Forefront™ Threat Management Gateway (TMG) are covered in the the Websense Installation Supplement for Microsoft ISA/TMG integrations at MyWebsense.com.

An integration with ISA/TMG affects the following Websense components:

- **Websense ISAPI Filter plug-in**: This additional Websense component is installed on the machine running ISA/TMG. The ISAPI Filter plug-in configures ISA/TMG to communicate with Websense Filtering Service running on the V5000 G2 appliance.
- **Websense Filtering Service**: Interacts with ISA/TMG and Websense Network Agent to filter Internet requests. Filtering Service either permits the Internet request or sends an appropriate block message to the user.

  After the V5000 G2 appliance is installed, the ISAPI Filter plug-in must be installed on every ISA/TMG machine in your network.
- **Websense Network Agent**: You must define the IP addresses of all proxy servers through which computers route their Internet requests. See *Network Configuration* in the TRITON - Web Security Help for instructions.
- **Transparent identification agents**: Generally, ISA/TMG provides user authentication information for Websense software. If ISA/TMG is not configured to provide user information to Websense software, install the appropriate Websense transparent identification agent. See the *Deployment Guide for Websense Web Security Solutions* or *Transparent Identification of Users* technical paper for more information about these agents.

How Websense filtering works with Microsoft ISA/TMG

To be filtered by Websense software in this integration, a computer must access the Internet through ISA/TMG.

When ISA/TMG receives an Internet request from a user, it queries Websense Filtering Service to find out if the requested site should be blocked or permitted. Filtering Service checks the policy assigned to the client. Each policy designates specific time periods and lists the category filters that are applied during those periods.

After Filtering Service determines which categories are blocked for that client, it checks the Websense Master Database.

- If the site is assigned to a blocked category, the client receives a block page instead of the requested site.
- If the site is assigned to a permitted category, Filtering Service notifies ISA/TMG that the site is not blocked, and the client is given access to the site.

Supported integration versions

Websense software can be integrated with the following Microsoft products.

- Microsoft ISA Server 2004, Standard Edition and Enterprise Edition
- Microsoft ISA Server 2006, Standard Edition and Enterprise Edition
- Microsoft Forefront TMG 2010

.

Important

The Websense ISAPI Filter plug-in for Microsoft Forefront TMG supports Windows Server 2008 (64-bit) only.

The Websense ISAPI Filter plug-in for Microsoft ISA Server supports the Windows versions supported by ISA Server 2004 and 2006, except Windows Server 2000.

Supported ISA/TMG clients are:

- Firewall Client/Forefront TMG Client
- SecureNAT clients
- Web Proxy clients

Installation

The only Websense component installed on the ISA Server or TMG machine is the Websense ISAPI Filter plug-in. Instructions for installing the plug-in are provided in the Microsoft Installation Supplement for Web Security version 7.5 at MyWebsense.com.

Cisco PIX and Cisco ASA

Full details about integrating Websense software with Cisco® Adaptive Security Appliance (ASA) and Cisco PIX® Firewall are provided in the Websense Installation Supplement for Cisco integrations at MyWebsense.com.

Integrating Websense software with a Cisco product involves the following components:

- **Filtering Service**: The integrated Cisco product and Network Agent work with Filtering Service to filter Internet requests. For redundancy, two or more instances of Filtering Service may be used. Only one instance is active at any given time—referred to as the primary server. URL look-up requests are sent only to the primary server.
- **Network Agent**: Manages Internet protocols that are not managed by your integrated Cisco product. **Network Agent** can also detect HTTP network activity and instruct the Filtering Service to log this information.
- **Configure your Cisco integration**: You must direct Internet requests through your Cisco integration product, and configure it for use with Websense software.
- **User authentication**: To work properly, Filtering Service must be installed in the same domain (Windows), or the same root context (LDAP), as Cisco Secure ACS.

  If you are using a Websense transparent identification agent or manual authentication, this configuration is not necessary.

How Websense filtering works with Cisco products

To be filtered by Websense software in a Cisco integration, a client's Internet requests must pass through the Cisco product. When Websense software is integrated with a Cisco PIX Firewall or ASA, browser requests must go through the PIX Firewall or ASA to reach the Internet.

When it receives an Internet request, the Cisco product queries Websense Filtering Service to determine if the requested Web site should be blocked or permitted. Filtering Service consults the policy assigned to the user. Each policy designates specific time periods and lists the category filters that are applied during those periods.

After Filtering Service determines which categories are blocked for that client, it checks the Websense Master Database.

- If the site is assigned to a blocked category, the user receives a block page instead of the requested site.
- If the site is assigned to a permitted category, Filtering Service notifies the Cisco product that the site is not blocked, and the client is allowed to visit the site.

> ✓ **Note**
>
> Before enabling Websense URL filtering, make sure there is not another URL filtering scheme configured, such as N2H2. There can be only one active URL filtering scheme at a time.

Supported Cisco integration product versions

Websense software is compatible with the following versions of Cisco products:

- Cisco PIX Firewall Software v5.3 and higher
- Cisco ASA Software v7.0 and higher

Citrix Presentation Server and XenApp

Full details about integrating Websense software with Citrix® MetaFrame® Presentation Server, Presentation Server™, or XenApp™ are provided in the Websense Installation Supplement for Citrix integrations at MyWebsense.com.

Integrating Websense software with a Citrix product involves the following components:

- **Websense Citrix Integration Service**: The Integration Service must be installed on each Citrix server to allow that server to communicate with Websense Filtering Service.
- **Websense Filtering Service**: Interacts with Citrix Presentation Server or XenApp and Websense Network Agent to filter Internet requests. Filtering Service either permits the Internet request or sends an appropriate block message to the user.
- **Websense Network Agent**: Manages Internet protocols that are not managed by your Citrix server integration. It can also detect HTTP network activity and instruct Filtering Service to log this information.

> ✓ **Note**
>
> If your Citrix server runs applications that use protocols other than HTTP, FTP, or SSL, Network Agent can apply protocol filtering to those applications based on a computer or network policy, or the Default policy. It cannot apply user- and group-based policies to protocol filtering of applications running on the Citrix server.

Supported Citrix versions

- XenApp 5.0 (Windows, 32-bit, only)
- Presentation Server 4.5 (Windows only)
- Presentation Server 4.0 (Windows only)
- MetaFrame Presentation Server 3.0 (Windows only)

✓ **Note**

For Presentation Servers, Websense Citrix Integration Service supports Windows 2000 Server (32-bit) and Windows Server 2003 (32-bit).

For XenApp, the Citrix Integration Service supports Windows Server 2008 (32-bit) and Windows Server 2003 (32-bit).

Client computers

- To be filtered by Websense software, Citrix client computers must access the Internet through a Citrix server.
- Non-Citrix clients in the network also may be filtered by the same installation of Websense Web Security.

Installation

Most Websense components must be installed on a separate machine from the Citrix server. Only the Citrix Integration Service is installed on each Citrix server machine.

If Websense Web Security will be filtering both Citrix and non-Citrix users, be sure to review the Citrix Installation Supplement at MyWebsense.com for deployment instructions.

Windows Server requirements for Web security components

In addition to the appliance, you must have one or more separate server machines that meet or exceed the requirements listed below for Websense Web Security components that run off-appliance.

To optimize performance, organizations with high traffic volume or large reporting needs are encouraged to install the **TRITON - Web Security** manager on a separate Windows server. Log Server (the component that receives Internet activity information and processes it into a Log Database) must be located off the appliance.

> **Important**
>
> Self-signed certificates are created to secure communications between Websense components. In order for these certificates to be valid, and for communication to succeed, all the machines running Websense components **must** have the same date.
>
> Please set the appliance time and the time on the Windows server machine before installing Websense components.
>
> If you need to reset the time and date, be sure to reset all machines.

Hardware

- Quad-Core Intel Xeon processor, 2.5 GHz or higher
- 4 GB RAM
- 100 GB free disk space utilizing a disk array
- High speed disk access

Operating System

- Windows Server 2008 SP2
- Windows Server 2003 R2 SP2
- Windows Server 2003 SP2

Additional software for accessing the TRITON manager

- Internet Explorer 7 or 8 or Firefox 3.0.x to 3.5.x
- Common Desktop Environment (CDE)
- Apache Tomcat (installed automatically with the TRITON manager)
- Adobe Flash Player 8 or later

Database Engine

One of the following supported database engines is required to store log data for reporting. Although this software can run on the same Windows server machine that runs Log Server, better performance is achieved when it runs on a dedicated server.

One of these database engines:

- Microsoft SQL Server 2008
- Microsoft SQL Server 2005 SP2 or SP3 (Workgroup, Standard, Enterprise, or 64-bit* edition)
- MSDE 2000 SP4

* If you are using 64-bit SQL Server, then Log Server must be installed on a machine separate from SQL Server, because Log Server does not support 64-bit operating systems.

The following recommendations apply to the machine running the database engine:

- You can improve I/O performance by installing the Log Database on a disk array running RAID level 1+0.
- The amount of required RAM depends on the total number of requests being stored and the number of requests per second being processed. To optimize RAM usage, use the Enterprise Edition of Microsoft SQL Server on a machine running Windows Server 2003 Enterprise Edition or Windows Server 2008 Enterprise Edition or Datacenter.

Directory Service

If your network includes one of the supported directory services listed below, you can apply Web filtering to individual users, groups, and domains (OUs). Additionally, you can install an optional transparent identification agent from Websense, to ensure that clients in a supported directory service are filtered without being prompted to log on when they open a browser. (If no directory service is installed, Websense Web Security uses IP addresses for Web filtering.)

✓ **Note**

If your network uses a Windows NTLM directory service, or Active Directory in mixed mode, you must create Websense accounts for any administrators who must log on to **TRITON - Web Security**. This configuration does not support logging on to **TRITON - Web Security** with network credentials.

- NTLM-based directory services
- Microsoft Active Directory 2003 or 2008 (specific permissions need to be granted to Websense Logon Agent to run with 2008)
- Novell eDirectory 8.51 or later

    - NMAS authentication is supported.
    - Recommend Novell Client v4.83 or v4.9 (v4.81 and later are supported)
- Other LDAP-based directory services
- Most standard RADIUS servers

  The following RADIUS servers have been tested:

    - Livingston (Lucent) 2.x
    - Cistron RADIUS server
    - Merit AAA
    - Microsoft IAS
    - NMAS authentication

Other servers

In some networks, additional machines may be used to deploy additional instances of Network Agent or other, optional components. For example, in a large, segmented network, you may need a separate Network Agent for each segment, and a separate Filtering Service for these Network Agents. Or, you might deploy the Remote Filtering Server to enable filtering of laptops and other computers that are outside the organization’s network.

Important

If you change the *policy source* (machine running Policy Broker and Policy Server) after deploying components on additional machines, you must reconfigure those components to communicate with the new *policy source*.

Go to the Websense Knowledge Base, and search for the article titled *Changing the Policy Server (or Policy Broker) IP address*.

For information about system requirements and appropriate placement of machines for additional or optional components, see the *Websense Deployment Guide*.

Network scenarios

One or more appliances can be deployed in a network, depending on the traffic volume and security goals.

Appliances can serve different roles, and thus all deployments should be well planned in advance. Please contact your Websense Sales Engineer, or your authorized Websense reseller, for assistance in planning your deployment.

Basic deployment scenarios are shown below:

- *Single appliance deployment*

- *Multiple appliance deployment*

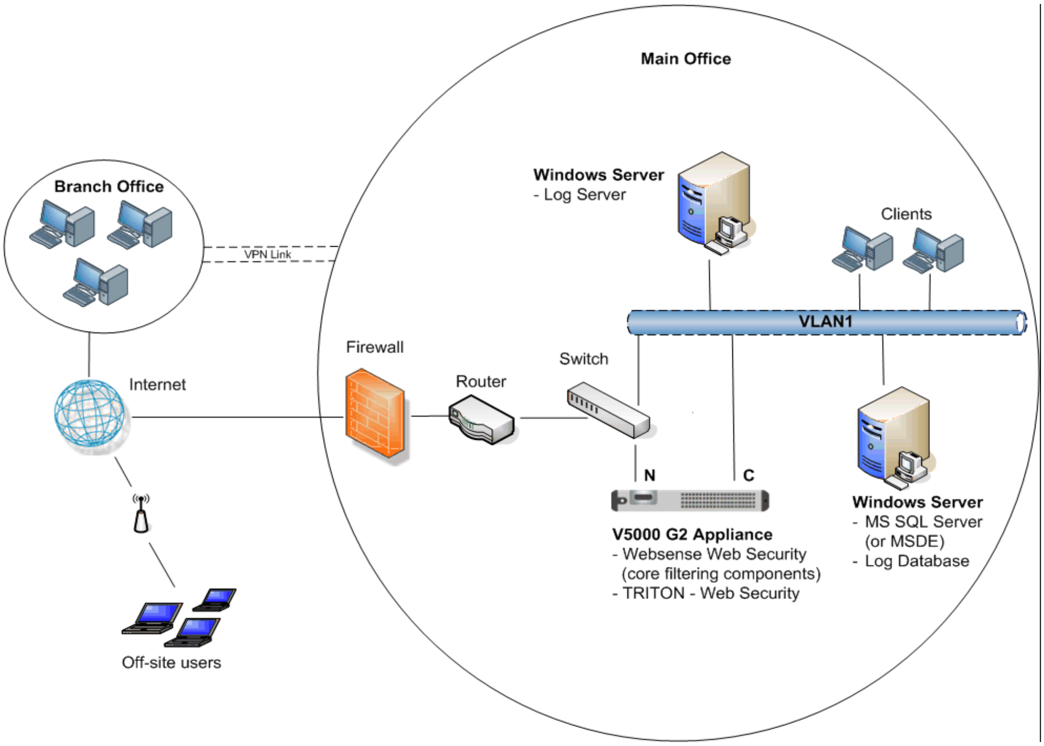
Single appliance deployment

When you deploy a single Websense appliance to host all major features, one additional Windows server is required to run Log Server. Organizations with high traffic volume or large reporting needs should install and run the **TRITON - Web Security** manager on a Windows server, to optimize performance.

In all environments, the cable for Network Agent interface N must be connected to a span port, monitor port, or mirror port on a router or switch. This enables it to see traffic from all clients being filtered.

If interface N is used to send blocking information, it must be connected to a bi-directional mirror port on the router or switch. In this configuration, Network Agent can montor all client traffic and send blocking information when needed.

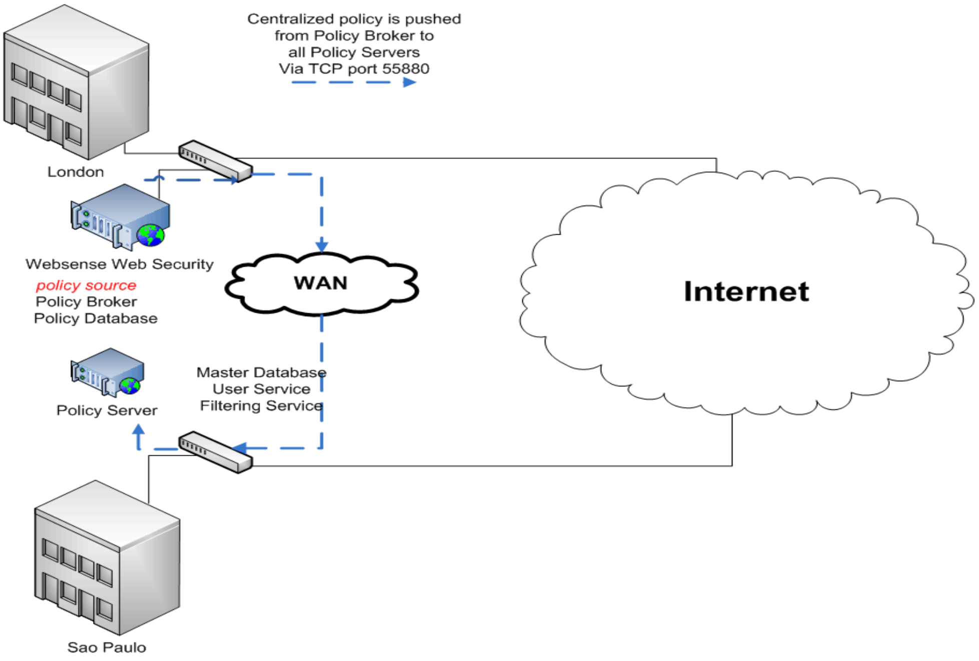
- Typically, the appliance controller interface C requires Internet access, to connect to the Websense download server for both subscription verification and database downloading.
- If interface C is used to send blocking information, as it is by default, it must be able to communicate with client machines.



Multiple appliance deployment

Organizations that need to filter a large number of users or a large volume of Internet traffic may deploy multiple Websense appliances. One appliance is designated as the *policy source*, and all others point to the *policy source* for policy and configuration settings.

The policy source appliance is configured first.



2 Setting up the V5000 G2 appliance

Follow this sequence.

1. *Set up the appliance hardware*
2. *Perform initial command-line configuration*
3. *Configure the appliance*
4. *Installing Off-Box Components*
5. *Test and refine your policies*

When setup is complete, you can use the Logon Portal to log on to any of the related management consoles.

Set up the appliance hardware

The 2-page Quick Start poster, in the appliance shipping box and at **www.websense.com**, shows the items included with each Websense appliance. The poster explains how to install the hardware, power on the appliance, and connect the appliance to your network.

The following are network requirements for the appliance:

- Interface C typically has a continuous connection to the Internet to access DNS servers.
- Interface C must be able to download essential databases from Websense servers at **download.websense.com**.
- The appliance address must be permitted by all firewalls, proxy servers, routers, or host files that control the URLs.
- Interface N must be connected to a mirror port on a router or switch.
- If interface N is used to send blocking information, then it must be connected to a *bi-directional* mirror port. Through the bi-directional mirror port, interface N not only monitors all client traffic but also sends blocking information if needed.

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.

See *Perform initial command-line configuration*.

Perform initial command-line configuration

The first time you start the appliance, a brief script (called 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 poster during hardware setup.

Hostname (example: appliance.domain.com)	
IP address for network interface C	
Subnet mask for network interface C	
Default gateway for network interface C (IP address) *Optional*	
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 and TRITON - Web Security console. (8 to 15 characters, at least 1 letter and 1 number)	
Integration method for this appliance (choose one): • Standalone (Network Agent only) • Microsoft ISA or TMG • Cisco PIX • Cisco ASA • Citrix	

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 on-screen 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 interface N, which is used for communications by Network Agent.

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*	
Choose interface for transporting blocking information for 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	
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*	
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 *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.*	TRITON - Web Security runs on this appliance. *or* TRITON - Web Security runs at the specified IP address.

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

Follow these steps to enable filtering. See the embedded 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*.)

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. The network interface N (for Network Agent) transports blocking information. Enter all required IP addresses and enter the subnet mask. Then, click **Save** in the Network Agent Interface area.

      In standalone mode (no third-party integration product), Network Agent (interface N) manages all Internet requests, and can enforce policy for all protocols. When a third-party product such as Microsoft ISA Server or Cisco PIX is integrated with Websense software, then Network Agent (interface N) manages only non-HTTP and non-HTTPS protocols.

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

5. In the left navigation pane, click **Configuration** > **Web Security Components**.

   Use the **Configuration** > **Web Security Components** screen to specify where the appliance gets Internet filtering policy information, and to define the location of your TRITON - Web Security manager.

   a. **Policy Source:** Whether you have one location or many, designate a single appliance to host a centralized Websense Policy Database. The other Websense appliances point to this server and receive regular updates from it. This appliance is called the *policy source*. All available Websense Web Security services run on the *policy source* appliance.

      With a centralized Policy Database on the *policy source* machine, you manage one set of filtering policies for all appliances and all domains in the network.

If the appliance being configured is not the *policy source* machine, then it must point to the *policy source*.

b. **TRITON - Web Security**: Use this panel to enter information that the Logon Portal needs to connect to the TRITON console, the management console for Web Security software.

For the *policy source* appliance, you can choose whether to use TRITON - Web Security on the appliance, or elsewhere on your network. The default for evaluations and small offices is to use TRITON - Web Security on the *policy source* appliance.

Production sites with heavy traffic or large reports are advised to download the Websense Web Security installer archive from www.mywebsense.com and install the TRITON - Web Security console on a separate Windows server.

To administer Websense Web Security on your *policy source* appliance, select **TRITON - Web Security on this appliance**.

To specify that **TRITON - Web Security** is installed elsewhere, select **TRITON - Web Security located on another appliance or server on your network**, and enter the IP address for the appliance or server where the manager is installed in your network. The default port is displayed. This option disables the on-appliance TRITON - Web Security console.

If you are configuring an appliance that is not a *policy source* machine, **TRITON - Web Security** settings are not needed. The manager does not run on *non-policy source* appliances.

Click **Save** to save and apply your changes.

Components running off the appliance

When you are ready to install components off the Websense appliance, refer to the *Installation Guide* for **Websense Web Security**. All Websense guides are available at MyWebsense.com. A summary from that guide is provided in the next chapter.

Most off-box components are Windows-only components.

- Log Server (required for reporting)
- (optional) Transparent identification agents (for filtering by user or group)
  - DC Agent
  - Logon Agent
  - eDirectory Agent
  - RADIUS Agent
- (optional) Remote Filtering Server (required for filtering roaming users)
- (optional) Integration plug-in (required only for Microsoft or Citrix integration deployment, described later)

Database management software

You are required to have a Windows database server running a supported version of Microsoft SQL Server. This is where the Log Database is built. Log Database provides the information for Websense Web Security reporting.

TRITON - Web Security

The **TRITON - Web Security** management console is pre-installed on the appliance as a convenience for evaluations and small installations. Organizations with high traffic volume or large reporting needs should install and run **TRITON - Web Security** on a ***separate Windows server***, to optimize performance.

TRITON - Web Security services include:

- Investigative Reports Scheduler
- Manager Web Server
- Reporting Web Server
- Reports Information Service

Third-party integration software and Websense plug-in

At your option, you can integrate Websense security software with a third-party integration product. See *Third-party integration software off the appliance* for details.

Recovering the appliance from DVD

The appliance comes with a recovery disk that can be used to restore the appliance to its factory image. You can use this DVD (after saving a Full configuration backup) to re-image the appliance and then recover your custom appliance and module settings. Note that all Websense components running off the appliance must be stopped before you use the recovery disk.

1. Stop all Websense components that are running off the appliance. For example, stop Log Server, transparent ID agents, **TRITON - Web Security**.
2. If possible, back up any information you want to preserve.
   a. Log on to the Appliance Manager for the primary appliance.
   b. Go to **Administration** > **Backup Utility**, and create a Full Configuration backup. See online Help for assistance. Save this backup file to another machine.
3. Go to the machine rack and insert the recovery disk into the appliance DVD drive.
4. Reboot the appliance. (An alternative is to turn off the power, and then turn it on again.)
5. Watch the terminal screen closely after the reboot starts. When a list of function keys appears at the upper right during reboot, press **F11.** Then select:
   - **Embedded SATA drive**
6. When asked whether you want to continue, enter **yes**.

   Restoring the image can take 20 minutes or more. When the DVD is ejected, be sure to remove it from the drive.
7. Press any key to view the subscription agreement.
8. Enter **yes** to accept the subscription agreement, and then enter **yes** to begin firstboot.

   This begins the firstboot script.
9. Follow the on-screen instructions at the terminal and provide the necessary information.

   See *Perform initial command-line configuration* for details of what information is requested.
10. Restore the backed up configuration via the Appliance Manager.
    a. Point a browser to the Logon Portal and log on to the Appliance Manager for the primary Websense appliance.
    b. Go to **Administration** > **Backup Utility**.
    c. Choose **Restore**.
11. Upload your Full Configuration backup file to the appliance, and then select **Restore**. The appliance will be rebooted automatically after the **Restore** is completed. Appliance and software module settings are restored.
12. Ensure that the appliance time and date are synchronized with other servers.
13. Restart the components that run off the appliance.

14. On occasion, a manual download of the Websense Web Security Master Database should be initiated after a Recovery. Do this in the TRITON - Web Security console if you receive a warning message about the Master Database.

3 Installing Off-Box Components

Deploying the Websense V5000 G2 appliance also requires installing:

- a SQL Server database engine
- the TRITON - Web Security management console (used off-box at larger sites)
- Log Server
- Filtering plug-in for use with Microsoft and Citrix integrations (only)

These components are installed on a separate Windows server machine in the network.

Start by downloading the Web Security installer for version 7.5 from the Downloads page at MyWebsense.com.

> **Important**
>
> Log Server receives records of Internet filtering activity and sends them to the Log Database, which is installed on a database engine. The SQL Server database engine must be installed and running before you install Log Server.

If you do not have a supported database engine, you can download and install the free Microsoft SQL Server (MSDE). The instructions are available from the Websense Support Portal in the Websense Knowledge Base (support.websense.com). Search for *Installing MSDE with Websense software, version 7*.

See the Websense *Installation Guide* for prerequisites and details on configuring the database engine, setting up user roles, and the database rights needed for the account specified during Log Server installation.

Before installing off-box components

Before installing the console and reporting components, ensure that the server meets the hardware and software requirements detailed in *Windows Server requirements for Web security components*, page 13.

Gather the following information before running the off-box installer. Some of this information may have been gathered on the Quick Start during hardware setup

Policy Server IP address (IP address of the policy source machine. Typically, this is the IP address for network interface C on the appliance)	
Database engine location (IP address or machine name)	
Database user name	
Database password	
Filtering Service IP address (typically, this is the IP address for network interface C on the V5000 G2 appliance)	

The following procedure summarizes the steps required to install the required components. See the Websense *Installation Guide* for more detailed instructions.

1. Log on to the installation machine with administrative privileges.

   If you will use a Windows trusted connection to communicate with the database engine, your logon user account must also be a trusted account with local administration privileges on the database machine.

2. Make sure the date and time are synchronized with the date and time on the V5000 G2 appliance.

   > **Important**
   >
   > Self-signed certificates are created to secure communications between Websense components. In order for these certificates to be valid, and for communication to succeed, all the machines running Websense components **must** have the same date.
   >
   > Please set the appliance time and the time on the Windows server machine before installing TRITON - Web Security and Log Server.

3. Download the Web Security version 7.5 installation package from the Downloads page at www.mywebsense.com.
4. Close all applications and stop any anti-virus software.
5. Double-click the installation package to extract the files and start the installation.
6. Follow the onscreen instructions to the Subscription Agreement screen.
7. Select **“I accept the terms of the Subscription Agreement,”** and click **Next**.
8. Select a **Custom** installation, and click **Next**.
9. In the list of components, mark the check boxes for **Log Server** and **TRITON - Web Security**.

See the Websense *Deployment Guide* and *Installation Guide* for descriptions of the available components, and associated installation requirements.

10. Clear all other check boxes, and then click **Next**.

Important

Be sure to **clear** the check boxes for these components:

- Policy Broker
- Policy Server
- Filtering Service
- Network Agent
- Usage Monitor
- User Service
- DC Agent
- eDirectory Agent
- RADIUS Agent
- Logon Agent
- Remote Filtering Server
- Remote Filtering Client
- Linking Service
- Directory Agent\
- Sync Service
- Filtering Plug-in

11. 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.

12. Install the TRITON - Web Security component.

    The TRITON - Web Security is the administration and reporting interface to Websense Web Security.

    In Windows environments, TRITON - Web Security and Log Server are typically installed together, which helps to minimize the impact of report processing on Internet filtering. See the *Deployment Guide for Websense Web Security Solutions* for a list of supported operating systems and deployment recommendations.

13. Policy Server Connection: This screen appears only 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. You are prompted to enter the IP address of the machine and the port Policy Server uses to communicate with other Websense components (default is 55806). When asked for the IP address of the Policy Server machine, enter the IP address of the policy source machine (typically, this is the IP address for network interface C on the V5000 G2 appliance).

14. Accept the default port number (55806), and click **Next**.

    Important

    Do not change the default port number if you are connecting to a Policy Server running on a V5000 G2 appliance.

15. Install the Log Server component.

    Log Server receives records of Internet filtering activity and sends them to the Log Database, which is installed on a database engine. Typically, Log Server is installed on the same machine as TRITON - Web Security.

    Note

    Log Server can be installed only on a Windows machine.

    The supported database engines are:

    - Microsoft SQL Server 2008
    - Microsoft SQL Server 2005 SP2 or SP3 (Workgroup, Standard, Enterprise, or 64-bit* edition)
    - MSDE 2000 SP4 (MSDE is not supported on Windows 2008 machines)

      * If you are using 64-bit SQL Server, then Log Server must be installed on a machine separate from SQL Server, because Log Server does not support 64-bit operating systems.

    See the *Deployment Guide for Websense Web Security Solutions* for specific service pack requirements for these database engines.

To be able to install Log Server, ensure that the database engine is running.

✓ **Note**

Log Server must be installed before you can see charts on the Status > Today and Status > History pages, or run presentation or investigative reports.

If you install Log Server on a machine separate from TRITON - Web Security, stop and restart the **ApacheTomcatWebsense** and **Apache2Websense** services after installation. These services are on the TRITON - Web Security machine.

Important

When Log Server is not installed on the same machine with TRITON - Web Security, you **must** stop and restart the Apache services on the TRITON - Web Security machine before creating scheduled jobs in presentation reports. You will be unable to create scheduled jobs until the services are restarted.

When Log Server is selected to be installed, the following screens appear during installation:

- **Policy Server Connection**

  Enter the IP address of the Policy Server machine (typically, this is the IP address for network interface C on the V5000 G2 appliance) and the port Policy Server uses to communicate with other Websense components (default is 55806).

- **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*.

- **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 user name and password of a trusted account with local administration privileges on the database machine. Note that the trusted account you specify here should be the same as that with which you logged onto this machine before starting the Websense installer. If you are using MSDE, it is a best practice to connect using a database account rather than trusted connection.

Important

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.

Note

If TRITON - Web Security is installed on a Linux machine, the Log Database must be on a SQL Server instance supporting database account authentication (i.e., mixed mode). Trusted connection authentication cannot be used in this case.

- **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.

- **Log Database Location**

  Accept the default location for the Log Database files, 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 files in a different location (or if you already have Log Database files in a different location), enter the path to them. 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 files must already exist. The installer cannot create a new directory.

- **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

16. Provide other information requested if you are installing any optional components.

    The information requested depends on the components being installed. See the Websense *Installation Guide* for details on optional components.

17. Accept the default installation path or click **Browse** to locate another path, and then click **Next**. The default installation path is:

    ```
    C:\Program Files\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 system requirements for the selected components with the machine's resources.

- Insufficient disk space prompts an error message. The installer quits when you click **OK**.

- Insufficient RAM prompts a warning message. The installation continues when you click **OK**. To ensure optimal performance, increase the machine's memory to the recommended amount after installation.

18. On the summary screen, click **Next**.
19. In response to the message stating that features like protocol management and Bandwidth Optimizer cannot be used unless Network Agent is installed, click **Next**.
20. A filtering plug-in is required only if you have certain third-party integration software in your network. When you install a Websense plug-in, you must place it on the same machine where your integration product is running. So, do not select a plug-in unless you are running the installer on the third-party integration machine.
    If appropriate, mark the checkbox for the filtering plug-in (optional) for your integration.
    - Microsoft ISA and TMG
    - Citrix

    No plug-in is needed if you are not integrating one of those filtering options.

    ✓ **Note**
    The filtering plug-in for Microsoft Forefront TMG is installed using a separate installer. See *Installation Guide Supplement for use with Microsoft ISA Server or Forefront TMG*.

    ✓ **Note**
    Other supported integration products (Cisco PIX and Cisco ASA) do not require a filtering plug-in.

    The filtering plug-in must be installed on the integration product machine itself. Select this component only if you are running the installer on the integration product machine.

    Filtering Service must already be installed before you install a filtering plug-in. (Filetring Service is pre-installed on the V5000 G2 appliance.)

    When a Filtering Plug-in is selected, the following screens appear during installation:

    - **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).

    - **Select Integration**

      Select your integration product and then click **Next**.

21. An optional Websense Transparent ID Agent (DC Agent, eDirectory Agent, RADIUS Agent, and Logon Agent) can be added later, if desired.

22. 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\

    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.

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

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

24. 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, because it is installing components. In this case, allow the installation to complete and then uninstall the unwanted components.

25. 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.

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

See the appropriate *Installation Guide* supplement for any additional setup instructions for your integration product.

Configure TRITON - Web Security

TRITON - Web Security is the central configuration and management interface for Websense Web Security. Use it to customize filtering behavior, monitor Internet usage, generate Internet usage reports, and manage Websense software configuration and settings. This Web-based tool runs on Microsoft Internet Explorer 7 or 8 and Mozilla Firefox 3.0.x to 3.5.x.

Gather the following information before configuring TRITON - Web Security. Some of this information may have been gathered on the Quick Start during hardware setup.

User name	WebsenseAdministrator (default)
Password	Unified password created when you configured the V5000 G2 appliance (during firstboot)
Subscription key	

Use the following steps to configure default filtering.

1. Access the TRITON - Web Security console by entering the following address in a supported browser:

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

   If you are using an off-box TRITON manager, replace <IP address> with the IP address of the server where you installed the TRITON manager. If you are using the on-box TRITON manager, specify the IP address of interface C on the appliance.

   Access to the TRITON - Web Security manager is secured with an SSL security certificate issued by Websense, Inc. Because the browser does not recognize Websense, Inc., as a known Certificate Authority (CA), a security warning is displayed.

2. To proceed to the TRITON - Web Security manager, do one of the following:
   - Select the option to ignore the warning and continue. (The exact phrasing of this option varies among browsers.)
   - Permanently accept or install the certificate.

3. Log on with the following credentials:

   User name: **WebsenseAdministrator**

   Password: (enter the unified password set up during V5000 G2 appliance configuration)

4. You are offered the option of launching a Quick Start tutorial. Quick Start tutorials provide an excellent method for becoming familiar with Websense software. To continue following the steps in this guide, click **Skip** to continue to TRITON - Web Security. You can view the tutorial later.

TRITON - Web Security opens, showing the **Status** > **Today** page. Because you have not yet entered a subscription key, the Health Alert Summary at the top of the page shows a series of errors and warnings.

5. Click the **Settings** tab of the left navigation pane. The **Settings** > **Account** page is displayed.
6. Enter your **Subscription key** exactly as you received it.
7. Create a new, secure password in the **Change Password** area, and then click **OK**.
8. Click **Save All** at the top of the right shortcut pane to save the key and the new password, and start downloading the Websense Master Database.

   No filtering occurs until you enter a subscription key. Downloading the database ensures full and accurate filtering.

   The Master Database, which contains the category and protocol definitions that provide the basis for Internet filtering, begins to download automatically.

   If Websense software must go through a proxy to perform the download, also use the **Settings** > **Database Download** page to configure proxy settings (see TRITON - Web Security Help for instructions).

   The process of downloading the full database may take a few minutes or more than 60 minutes, depending on factors such as Internet connection speed, bandwidth, available memory, and free disk space.

   For more information about Master Database downloads, see TRITON - Web Security Help.
9. If you plan to apply filtering policies to individual users, groups, and domains in your network:

   a. Go to **Settings** > **Directory Service**.

   b. Select the directory service used in your network, and configure its settings. See TRITON - Web Security Help for assistance.

   > **Important**
   >
   > If your network uses a Windows NT directory or Active Directory (Mixed Mode), or you use Logon Agent to transparently identify users in Active Directory (Native Mode), see *Special directory service considerations*, page 42, for important configuration steps.

10. Go to **Settings** > **Network Agent** > **Global**. After making any changes, click **OK**, and then click **Save All**.

    Initially, Websense Network Agent uses these guidelines to identify the machines in your network and start filtering requests.

    - Machines in the following IP address ranges are assumed to be internal machines. Requests sent **to** these machines, and messages sent between these machines, are ignored.

      ```
      10.0.0.0 - 10.255.255.255
      172.16.0.0 - 172.31.255.255
      192.168.0.0 - 192.168.255.255
      224.0.0.0 - 239.255.255.255
      ```

- Requests sent to the Internet **from** all internal machines visible to Network Agent are monitored.

If this basic configuration is adequate for your network, no additional configuration is necessary.

If, however, you want to configure Network Agent to monitor requests sent **to** some internal machines (like an internal Web server), or to ignore Internet requests sent **from** certain machines, you can make those changes in TRITON - Web Security, under **Settings** > **Network Agent** > **Global**. See TRITON - Web Security Help for details.

11. If you are using explicit proxy, click the IP address under **Settings** >**Network Agent** in the left navigation pane.
12. Click **Add** in the Proxies and Caches area.
13. Enter the IP address of the explicit proxy.

✓ **Note**

On the V5000 G2 appliance, Websense sends blocking information for non-HTTP protocols through the N network interface if it is connected to a bidirectional span port, and that port is identified and configured in the V5000 G2 appliance console. Otherwise, blocking information is sent through the C interface.

Configuration settings or changes for the blocking NIC in TRITON - Web Security are disregarded by the V5000 G2 appliance. (See the TRITON - Web Security Help topic on Configuring NIC settings for information about the blocking NIC.)

The V5000 G2 appliance for Web Security includes two interfaces for Network Agent: a virtual interface (NIC1: 169.254.254.x) and an interface to which you assign the IP address (NIC2). Both of these interfaces are displayed in the TRITON - Web Security console when you configure Network Agent. You need to configure only NIC2 for traffic monitoring and filtering; NIC1 is used internally and is not configured.

Enhanced logging with Network Agent is an option in some integration environments, and may be configured at this time.

14. Click **OK** to cache your changes. Changes are not implemented until you click **Save All**.
15. In any environment that includes reporting:
    - If TRITON - Web Security and Log Server are being installed on different machines, open TRITON - Web Security and verify the Log Server location on the **Settings** > **Logging** page.

- If TRITON - Web Security and Log Server arebeing installed on the same (Windows) machine, make sure that the machine IP address, rather than **localhost**, appears on the **Settings > Logging** page.

These are the steps required to configure Websense Web Security so that the Websense V5000 G2 appliance is ready for default operations. See the TRITON - Web Security Help for details on the variety of features and options available for Websense Web Security.

Special directory service considerations

If you plan to apply filtering policies to individual users and groups in your network, special configuration steps are required to assure that the Websense V5000 G2 appliance can identify users successfully in networks that:

- Use Windows NT Directory or Active Directory (Mixed Mode)
- Plan to use Websense Logon Agent to transparently identify users in Active Directory (Native Mode),

In these environments, the Websense V5000 G2 appliance must be configured to communicate with a Windows Internet Name Server (WINS) to resolve domain names to domain controller IP addresses. The precise steps vary, depending on your environment.

If your network uses Windows NT Directory or Active Directory (Mixed Mode):

1. In TRITON - Web Security, go to the **Settings > Directory Service** page.
2. Select **Windows NT Directory / Active Directory (Mixed Mode)**, which is the default.
3. Enter the name and password for the administrative user.
4. Enter the **Domain** name.

   If your organization uses multiple domains, enter the name of a domain that is trusted by all domains that authenticate your users.
5. Enter the IP address of a Windows Internet Name Server (WINS) that can resolve the domain name entered above to a domain controller IP address.
6. Click **OK** to cache your changes. Changes are not implemented until you click **Save All**.

If your network uses Active Directory (Native Mode), and uses Logon Agent to transparently identify users for filtering:

1. In TRITON - Web Security, go to the **Settings > Directory Service** page.
2. Provide administrative credentials and identify the Windows Internet Name Server (WINS), as follows.
   a. Select **Windows NT Directory / Active Directory (Mixed Mode)**, which is the default.
   b. Enter the name and password for the administrative user.
   c. Enter the **Domain** name.

If your organization uses multiple domains, enter the name of a domain that is trusted by all domains that authenticate your users.

d. Enter the IP address of a Windows Internet Name Server (WINS) that can resolve the domain name entered above to a domain controller IP address.

e. Click **OK** to cache your changes.

f. Click **Save All** to implement these changes.

3. On the Directory Service page, select **Active Directory (Native Mode)**.
4. Configure the global catalog servers and other settings for your directory service. See TRITON - Web Security Help for assistance.
5. Click **OK** to cache your changes. Changes are not implemented until you click **Save All**.

Test and refine your policies

After performing the procedures outlined in this document, run the following tests to verify that the system is configured and operating properly.

1. Go to another computer in the network that is monitored by the Websense V5000 G2 appliance.
2. Open a Web browser, and browse to several different sites to generate Internet traffic.

   If possible, browse to sites that would likely fall into several different categories; for example, Games, Education, Entertainment, Sports, Shopping, Travel, and Vehicles.

   ✓ **Note**
   Because the Default policy enforces the Monitor Only category filter, all sites are permitted.

3. Access TRITON - Web Security by entering the following address:

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

   Replace <IP address> with the IP address of the server where you installed the TRITON - Web Security console, if you are using an off-box TRITON manager. Specify the IP address of interface C on the appliance, if you are using the on-box TRITON manager.

4. Log on as WebsenseAdministrator, with the password you set during installation.

5. Observe the charts on the Today page to verify that they reflect the traffic you just generated.

> **Note**
>
> Charts on the Today page are refreshed every 2 minutes. If they reflect the sites that you browsed to after the next refresh, your configuration is correct.
>
> If the correct data is not shown, verify that you have correctly entered the configuration information, as described in this document.

After you verify that the system is operating according to the default settings:

1. In TRITON - Web Security, go to **Help** > **Quick Start Tutorials** > **New User**.

   Work through the lessons to become familiar with the TRITON - Web Security interface, and learn to configure and manage Web filtering policies.

2. Configure policies suitable to your organization's specific needs, and assign them to the appropriate clients.

   See TRITON - Web Security Help for detailed instructions.

3. Open the V5000 G2 Appliance Manager to view system status, modify the configuration, or manage the appliance itself.

   See the V5000 G2 Appliance Manager Help for detailed instructions.

Logon Portal

The **Logon Portal** provides V5000 G2 administrators with access to these management consoles from a central Web page.

- Websense V5000 G2 console
- TRITON - Web Security console (for Websense Web 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 V5000 G2

.

> **Note**
>
> The following (similar) URL does *not* provide access to the **Logon Portal**:
>
> ```
> https://<IP address>
> ```