Installation Guide Supplement

for use with

Universal Integrations

Websense® Web Security
Websense Web Filter

v7.5

Published 2010
Printed in the United States of America and Ireland

Trademarks

WinPcap

Contents

1 Universal Integrations

This supplement to the Websense Web Security and Websense Web Filter *Installation Guide* (*Installation Guide*) provides information specific to integrating Websense software with your firewall, proxy server, caching application, or network appliance (referred to as the "integration product"). For general installation instructions, refer to the *Installation Guide*.

Separate installation supplements are available for these specific integration products or vendors:

- Cisco®
- Check Point®
- Citrix®
- Microsoft® Internet Security and Acceleration (ISA) Server or Forefront TMG
- Squid Web Proxy Cache

If your integration product is not listed here, go to www.websense.com/global/en/Partners/TAPartners/SecurityEcosystem/. Check the list of Technology Partners to see if Websense software supports an integration with your firewall, proxy server, caching application, or network appliance. If your integration product is listed, that product has been specifically enhanced to integrate with Websense software.

Integrating Websense software with another product or device affects the following components:

- **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.
- **Network Agent**: Internet protocols that are not managed by your integration product are managed by Network Agent. It can detect HTTP network activity and instructs the Filtering Service to log this information.

  If Network Agent is installed, you must define the IP addresses of all proxy servers through which computers route their Internet requests. See the Network Configuration topic in TRITON - Web Security help for instructions.

  If Network Agent is installed separately from other filtering components, be sure to install Filtering Service in integrated mode (universal integration). This ensures that bandwidth filtering can be applied in the integrated environment.

How Websense filtering works with your integration

When the integration product receives an Internet request, it queries Websense Filtering Service to find out if the requested site should be blocked or permitted. Filtering Service consults the policy assigned to the client to determine which categories are blocked, and then checks the Websense Master Database to find out how the requested site is categorized.

- 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 the integration product that the site is not blocked, and the client is allowed to see the site.

Installation

Follow the installation instructions in the *Installation Guide* to install the Websense components you want. The steps below provide specific options to select or alternate instructions to be used as you follow the instructions in the *Installation Guide*. Unless a specific option or alternative instruction is provided here, you should follow the steps as described in the *Installation Guide*.

1. Start the Websense installer, and follow the prompts.

   See the *Installation Guide* for instructions on downloading and starting the installer.
2. On the **Integration Option** screen, select **Integrated with another application or device**.
3. On the **Select Integration** screen, select **Other (Universal Integration)**.
4. On the **Transparent User Identification** screen you can choose whether to install a Websense transparent identification agent. Transparent identification agents identify users without prompting them for logon information. This enables filtering via user and group-based policies.

   Select **None** if you plan to configure authentication of users through your integration product, or if you plan to assign policies to computers and networks (IP addresses or IP address ranges) only.

   See the *Installation Guide* for more information about this installer screen.

   See the *Deployment Guide* for Websense Web Security Solutions (*Deployment Guide)* for more information about transparent identification agents.
5. Follow the remaining installer prompts to complete the installation.

See the *Installation Guide* for instructions on the prompts.

Note

To prevent users from circumventing Websense filtering, configure your firewall or Internet router to allow outbound HTTP, HTTPS, FTP, and Gopher requests only from your integration product.

Contact your router or firewall vendor for information about configuring access lists for that product.

Important

If Internet connectivity of Websense software requires authentication through a proxy server or firewall for HTTP traffic, the proxy server or firewall must be configured to accept clear text or basic authentication to enable the Websense Master Database download.

Upgrade

Refer to the Websense Web Security and Websense Web Filter *Installation Guide Supplement for Upgrading* for instructions on upgrading Websense software. After the upgrade, Websense software and your integration product should continue to work together as before.

Initial setup

Depending on the integration product you are using, you may need to configure client computers to access the Internet through it to enable Websense filtering. Consult your integration product's documentation to make this determination.

Migrating to a different integration after installation

You can change your integration product or version after installing Websense software without losing any of your configuration data.

Note

If you are installing on of the integration products listed on page 5, refer to the *Installation Guide* supplement for that product.

1. Install and configure your new integration product. See your integration product documentation for instructions.

   Ensure that it is deployed in your network such that it can communicate with Filtering Service and Policy Server.
2. Use the Websense Backup Utility to backup the Websense configuration and initialization files. See TRITON - Web Security Help for instructions
3. Ensure that Websense software is running. The installer looks for Policy Server during the installation process.
4. Remove Filtering Service using the procedures for removing components in the *Installation Guide*.

   Warning
   Remove Filtering Service only. Do **not** remove the associated Policy Server.
5. Restart the machine (Windows only).
6. Close any open applications, and stop any antivirus software.
7. Run the Websense installer again.
8. Add Filtering Service using the procedures for installing individual components in the *Installation Guide*.
9. On the **Integration Option** screen, select **Integrated with another application or device**.
10. On the **Select Integration** screen, select **Other (Universal Integration)**.
11. Follow the installer prompts to complete the installation.

    The installer adds the new integration data, while preserving the previous configuration data.
12. Restart the machine (Windows only).
13. Verify that Filtering Service has started.
    - **Windows**: Open the Services dialog box (Start > Programs > Administrative Tools > Services) and check to see if **Websense Filtering Service** is started.
    - **Linux**: Navigate to the Websense installation directory (/opt/Websense, by default), and enter the following command to see if **Websense Filtering Service** is running:

      ```
      ./WebsenseAdmin status
      ```

    To start a service, follow the instructions in the *Installation Guide*.

14. Open TRITON - Web Security to identify which Filtering Service instance is associated with each Network Agent.
    a. Open the **Settings** tab.
    b. Go to the **Settings > Network Agent**, then choose the appropriate IP address to open the **Local Settings** page.
    c. Under **Filtering Service Definition**, select the IP address for the machine running Filtering Service. During the migration, the setting may have been reset to None.
    d. Log out of TRITON - Web Security.

    For more information, see the Network Configuration > Local Configuration topic in the TRITON - Web Security Help.
15. If you stopped your antivirus software, be sure to start it again.

Index