

# Identifying and Solving the Most Common Web Security Issues: User Identification, Reporting, and Network Agent

WebSense Tech Talk Webinar April 2010

1. Common problem areas with Websense installations.
  - Reporting
  - User Identification
  - Network Agent Protocol Filtering
2. Technical question and answer session.
  - Websense Web Filter
  - Websense Security Gateway
  - Websense V10000





**Nathan McClean**

- **Title:** Technical Account Manager
- **Accomplishments:**
  - 4 years supporting Websense products
- **Education / Certifications:**
  - AA Computer Systems and Networks
  - CCNA
  - WSG and V10000 Certified
- **Qualifications:**
  - V10000 & WCG Training
  - Technical Support Mentor
- **For additional information:**  
[www.websense.com/support/](http://www.websense.com/support/)



**Greg Didier**

- **Title:** Technical Support Specialist
- **Accomplishments:**
  - 6 years supporting Websense products
- **Qualifications:**
  - WSG & WWF Training
  - Technical Support Mentor
- **For additional information:**  
[www.websense.com/support/](http://www.websense.com/support/)

## ■ Symptoms:

- No Qualifying Data on Today Page

**Today's Value**

Blocked:	Counters:
Malicious: 0	Requests: 0
Adult: 0	Blocked: 0
Spyware: 0	Scanned: 0
	RTSU: 42

- Logserver Health Alert Message

**Health Alert Summary**

**The Log Server at 10.212.5.47 is not running**

- Blank Reports

**Warning: the summary tables used by Investigative Reports are empty!**

If you have just installed Investigative Reports, the installation program may be preparing your database right now. Please wait 30 minutes and try again.

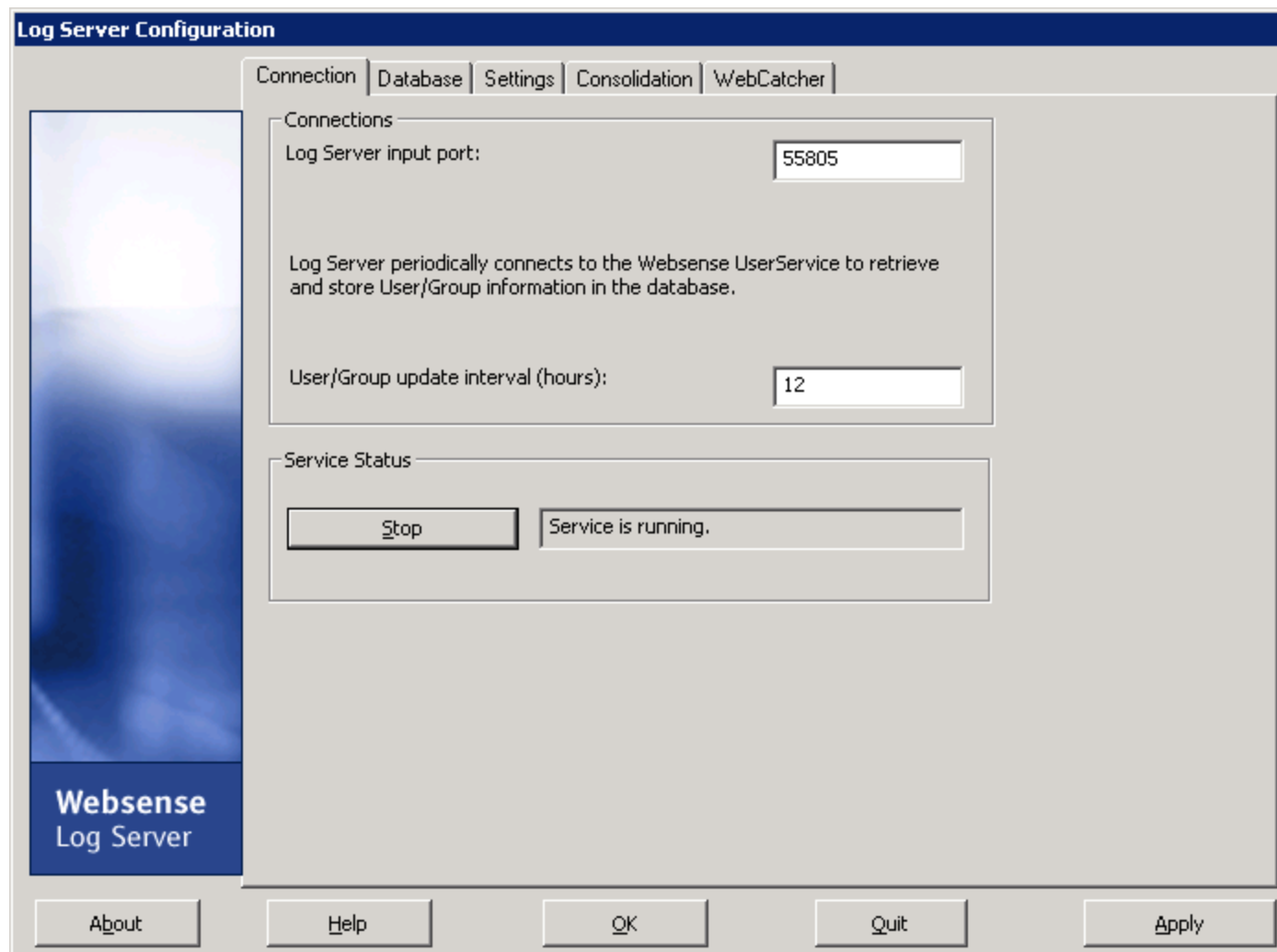
Please contact your Websense administrator.  
If you are the administrator, [edit your Investigative Reports options here.](#)

- Logserver location set to localhost

The screenshot shows the WebSense WebSecurityGateway Manager interface. The top navigation bar includes 'Main', 'Settings', and 'Logging'. The left sidebar lists various settings categories, with 'Logging' highlighted. The main content area is titled 'About Logging Settings' and contains the following text: 'Websense software lets you determine what information should be logged. Information that is n included in Internet usage reports.' Below this is a section titled 'Reporting Log Records' with the text: 'These settings determine what user information is logged and available in your Internet usage reports. If you deselect both check boxes, no user data will appear in your reports. For all logged categories and protocols:'. There are two checked checkboxes: 'Log IP addresses' and 'Log user names'. Below these are two input fields: 'Log Server IP address or name:' with the value '192.168.1.105' (highlighted with a red box) and 'Port:' with the value '55805'. A 'Check Status' button is located at the bottom of the form.

- Update Websense Logserver IP address

# Reporting Issues - Logserver Service



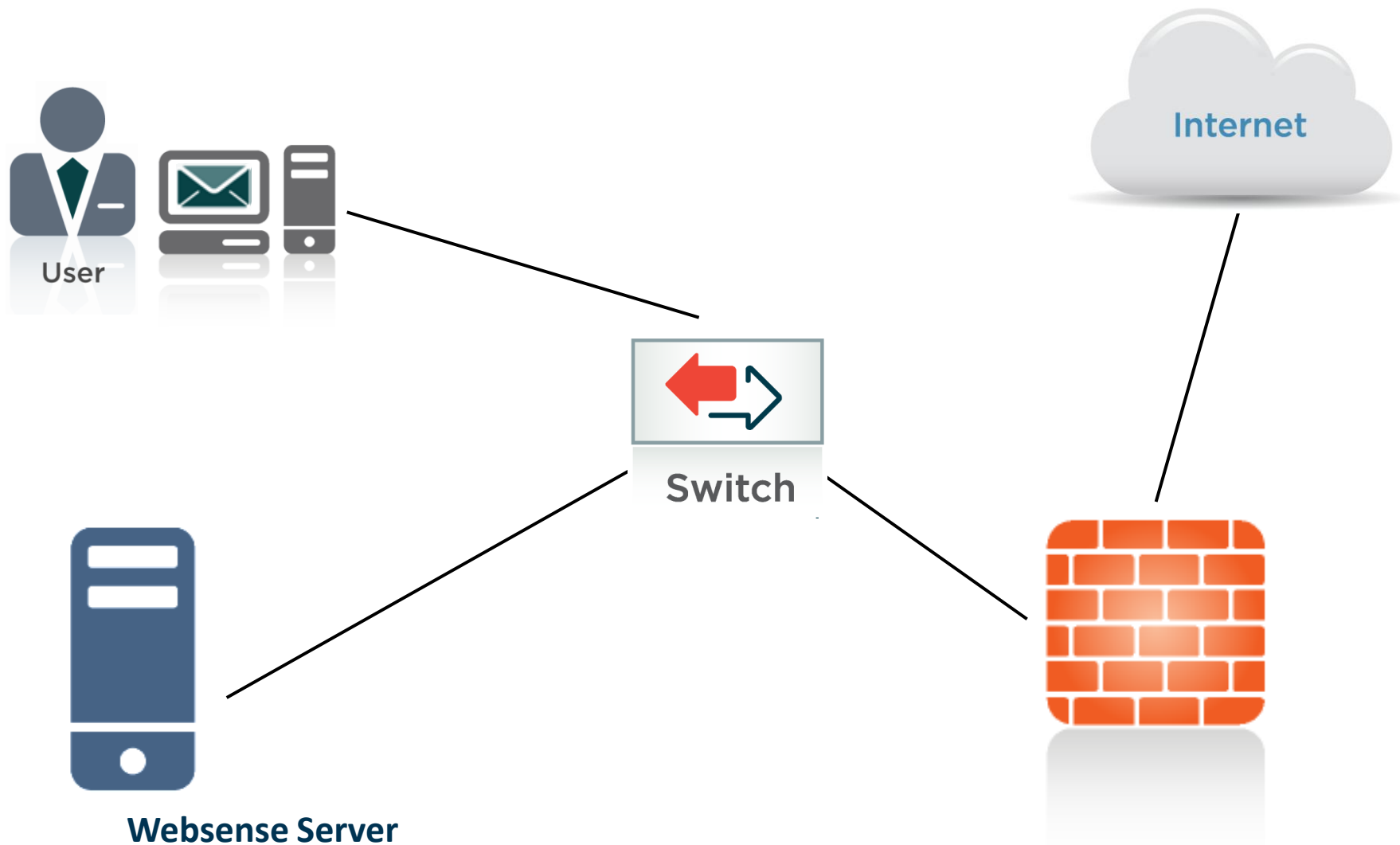
- Websense Knowledge Base Article 3663

- v7: Why is Log Server not recording data?

- <http://kb.websense.com/article.aspx?article=3663&p=12>



# DC Agent – Acquires User Names





- Packet contains only
  - Source IP address
  - Destination IP address
- No user names
- Filtering, on User and Groups, requires...
  - User Map
    - Pairs user names to source IPs



**Websense Server**

# DC Agent – Acquires User Names

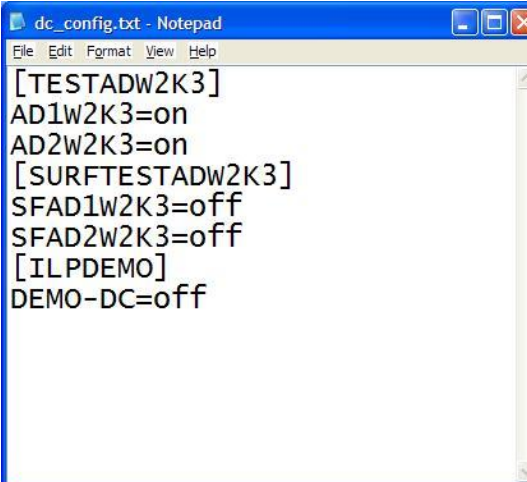
- For successful identification
  - DC Agent build user name/IP map
  - Filtering Server service ask DC Agent for map
  - Websense polls your Directory Services
- Reports show user names



**Websense Server**

## ■ Websense DC Agent service

- Installed and running
- Domain Administrator account
- Poll Domain Controllers
  - C:\>net view /domain > list.txt
- \Program Files\Websense\bin\dc\_config.txt
  - Domain Controller list, which filtered users authenticate
- KB # 3602 - DC Agent does not see some or all users



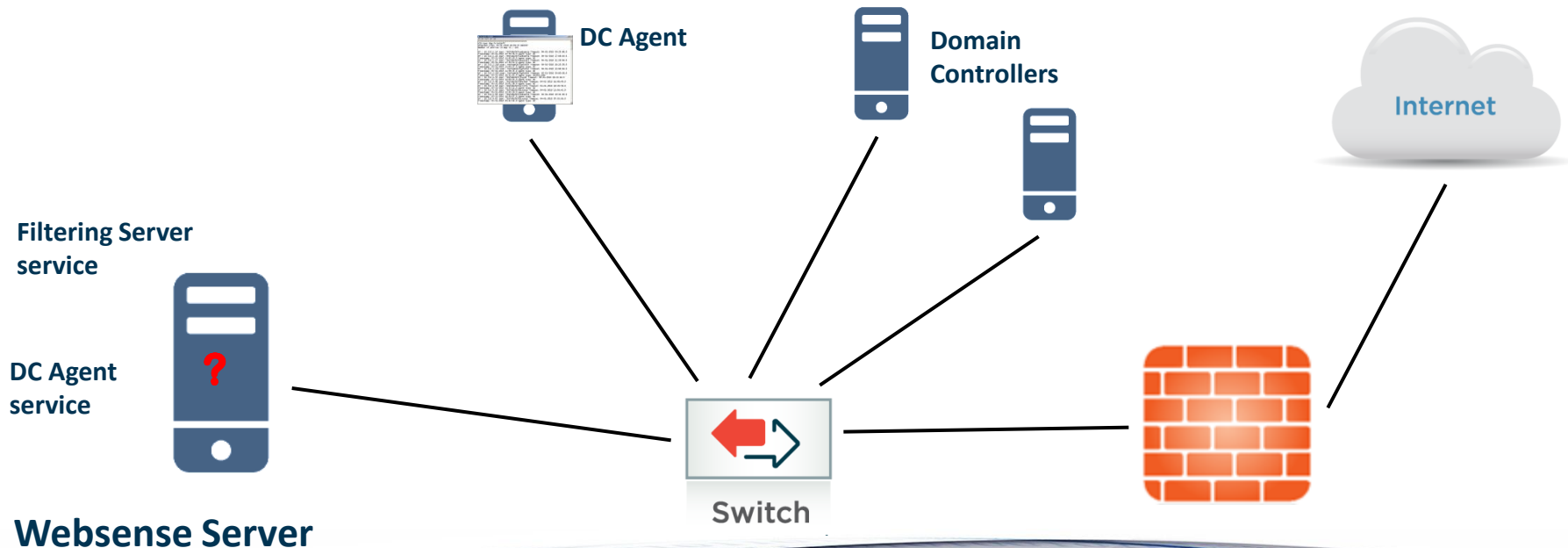
```
dc_config.txt - Notepad
File Edit Format View Help
[TESTADW2K3]
AD1W2K3=on
AD2W2K3=on
[SURFTESTADW2K3]
SFAD1W2K3=off
SFAD2W2K3=off
[ILPDEMO]
DEMO-DC=off
```



**Websense Server**

# DC Agent - Recap

- DC Agent polls domain controllers
- Domain controllers must be visible to DC Agent
- *dc\_config.txt* file must exist and be populated
- Filtering Server service gets IP\User map from DC Agent



**WebSecurity** WEBSSENSE<sup>®</sup> Policy Server: 10.212.2.215 Role: Super Admin

Main **Settings**

- General
- Account**
- Filtering
- Database Download
- Directory Services
- Logon Directory
- Logging
- Risk Classes
- User Identification >>>**
- Remote Filtering
- Policy Servers
- Alerts and Notifications
- Network Agent
- Reporting

### Basic Agent Configuration

Indicate where this instance of DC Agent is installed, and whether communication between the agent and Filtering Service is password protected.

Server IP or name: 10.212.2.210

Port: 30600

Enable authentication

Password:

### DC Agent Communication

Customize the port used for communication between DC Agent and other Websense components, and the port used for troubleshooting.

\*Communications port: 30600

\*Diagnostic port: 30601

### Domain Controller Polling

Define how often DC Agent queries the domain controller for user logon information, and how often it removes entries from its user map.

Enable domain controller polling

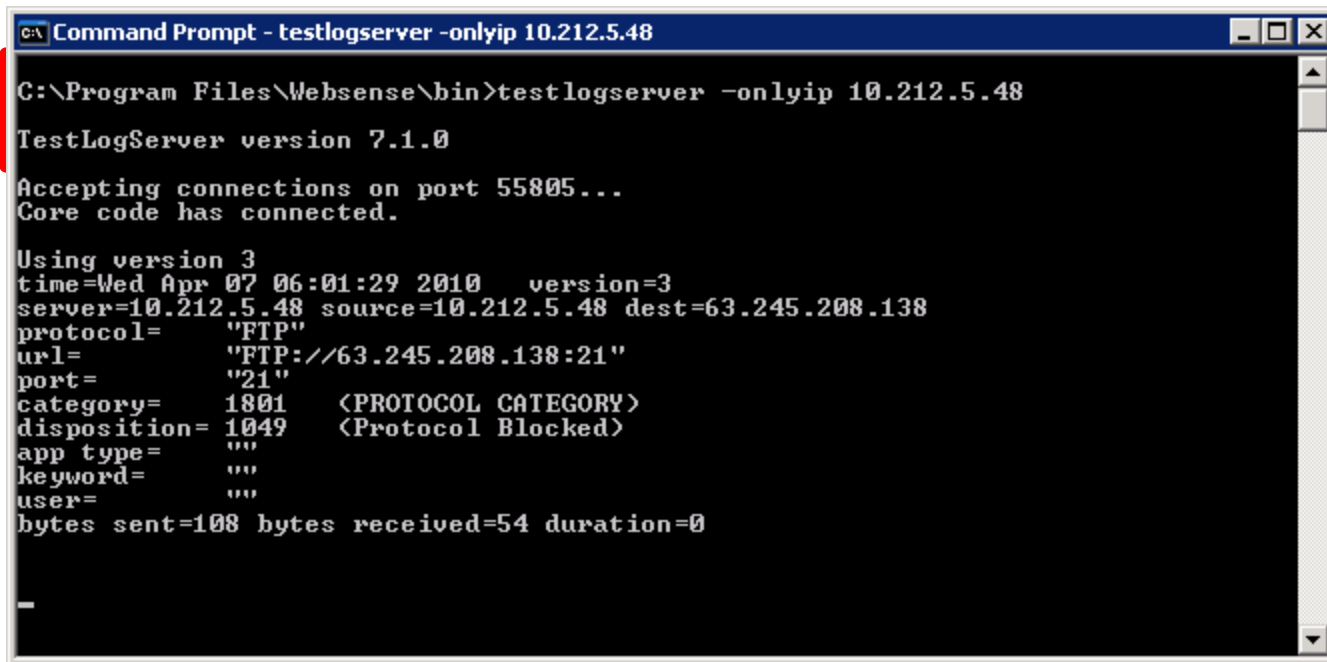
\*Query interval: 10 seconds

\*User entry timeout: 24 hours

### Computer Polling

OK Cancel

# Protocol Filtering – Filtering Issues



```
C:\> Command Prompt - testlogserver -onlyip 10.212.5.48

C:\Program Files\WebSense\bin>testlogserver -onlyip 10.212.5.48

TestLogServer version 7.1.0

Accepting connections on port 55805...
Core code has connected.


Using version 3
time=Wed Apr 07 06:01:29 2010    version=3
server=10.212.5.48 source=10.212.5.48 dest=63.245.208.138
protocol= "FTP"
url= "FTP://63.245.208.138:21"
port= "21"
category= 1801 <PROTOCOL CATEGORY>
disposition= 1049 <Protocol Blocked>
app type= ""
keyword= ""
user= ""
bytes sent=108 bytes received=54 duration=0

-
```

[Testlogserver Utility: See Websense Knowledge Base Article 3002](#)

## ■ Websense Network Agent

### – Service Installed and Running?

	websense information se...	Started	Automatic	Local System
	Websense Log Server	Started	Automatic	Local System
	Websense Network Agent	Started	Automatic	Local System
	Websense Policy Broker	Started	Automatic	Local System
	Websense Policy Database	Started	Automatic	.\WebsenseDBUser

### – Monitoring Correct NIC?

Network Interface Cards		
Name	IP Address	Description
<u>NIC-1</u>	10.212.5.48	Intel(R) 82566DC Gigabit Network Connection
<u>NIC-2</u>	192.168.132.1	Intel(R) 82566DC Gigabit Network Connection

### – Internal Network Definition Correct?

Internal Network Definition	
Identify the machines in your network. By default, Network Agent ignores requests coming in to these machines.	
<input type="checkbox"/>	<b>IP Addresses</b>
<input type="checkbox"/>	<u>10.0.0.0 - 10.255.255.255</u>
<input type="checkbox"/>	<u>192.168.0.0 - 192.168.255.255</u>
<input type="checkbox"/>	<u>172.16.0.0 - 172.31.255.255</u>
<input type="checkbox"/>	<u>224.0.0.0 - 239.255.255.255</u>



## ■ Knowledge Base Articles

- 3627 “Where does Network Agent fit in my network?”
  - <http://kb.websense.com/article.aspx?article=3627&p=12>
- 3628 “Configuring Network Agent behavior”
  - <http://kb.websense.com/article.aspx?article=3628&p=12>

## Knowledge Base

- Search or browse the knowledge base for documentation, downloads, top knowledge base articles, and solutions specific to your product.

## Support Forums

- Share questions, offer solutions and suggestions with experienced Websense Customers regarding product Best Practices, Deployment, Installation, Configuration, and other product topics.

## Tech Alerts

- Subscribe to receive product specific alerts that automatically notify you anytime Websense issues new releases, critical hot-fixes, or other technical information.

## [ask.websense.com](https://ask.websense.com)

- Create and manage support service requests using our online portal.

# Customer Training Options

- To find Websense classes offered by Authorized Training Partners in your area, visit:  
<http://www.websense.com/findaclass>
- Websense Training Partners also offer classes online and onsite at your location.
- For more information, please send email to:  
[readiness@websense.com](mailto:readiness@websense.com)

**WEBSense®**  
**Authorized Training  
Partner**

**WEBSense®**  
**Certified Instructor**



## Webinar Update

Title: Deployment and Installation of Websense  
Web Security Gateway Anywhere v7.5

Date: May 19, 2010

Time: 8:30 AM PDT (GMT -8)

How to register:

[http://www.websense.com/content/  
SupportWebinars.aspx](http://www.websense.com/content/SupportWebinars.aspx)

# Questions?

---

