# Configuring and Troubleshooting Websense Solutions for Filtering Off-Site Users

## Websense Support Webinar August 2010

**Support Webinars**

web security | data security | email security

# Goals And Objective

websense®
ESSENTIAL INFORMATION PROTECTION™

- Understanding Websense filtering options for off-site users
- Remote Filtering Server and Client Deployment considerations
- Installing and configuring Remote Filtering Server and Client
- Firewall Configuration for Remote Filtering
- Remote filtering software upgrade information and compatibility guidance
- Troubleshooting remote filtering software
- Configuring hybrid filtering of off-site users
- Configuring client browsers to use a PAC file
- Identification methods for off-site users
- Tips for applying hybrid filtering to off-site users

# Webinar Presenter

**Ravi Desai**

- Title: Technical Support Specialist
- Accomplishments:
  - Over 3 years supporting Websense products
- Education / Certifications:
  - B.Eng (Hons) Computer Systems and Networks
  - CCNA
  - WCWSA – Websense Certified Web Security Associate

# Filtering options for off-site users

- Websense Remote Filtering

  - Requires **Remote Filtering Server that resides inside your firewall, and acts as a proxy to** Websense Filtering Service

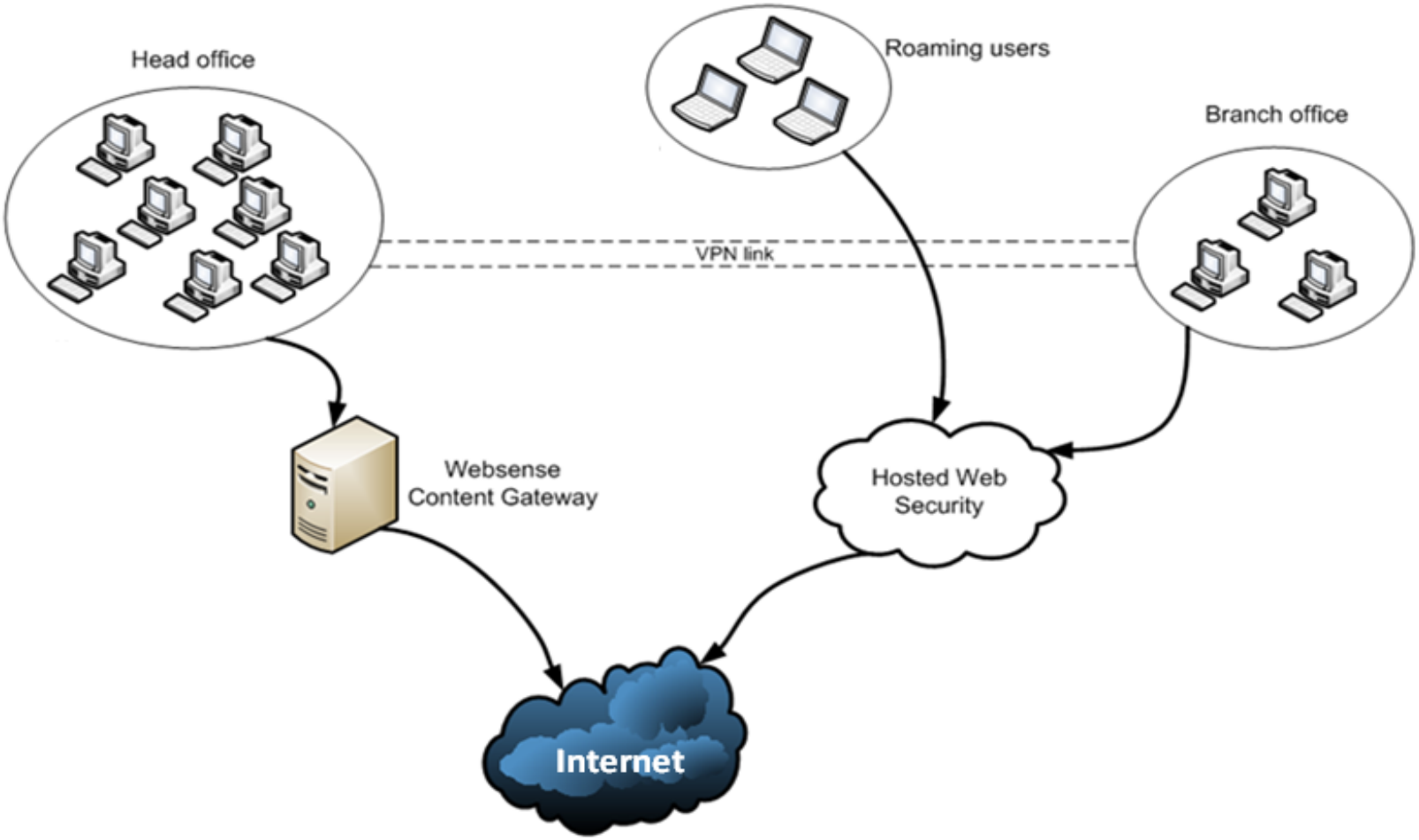
  - Also requires **Remote Filtering Client that is installed on each machine that will be filtered when** used outside the network.

  - Client communicates with Remote Filtering Server

  - Communication between RF client and RF server is encrypted.

# Filtering options for off-site users

- Websense Hybrid Filtering



# Remote Filtering Requirements

Remote Filtering Server 7.5 Requirements

- Supported operating systems
- Red Hat Enterprise Linux 5, update 3 (32-bit)
- Red Hat Enterprise Linux 4, update 7 (32-bit)
- Windows Server 2008 SP2 (32-bit x86 only)
- Windows Server 2003 SP2 or R2 SP2

Remote Filtering Client 7.5 is supported only on Microsoft Windows operating systems:

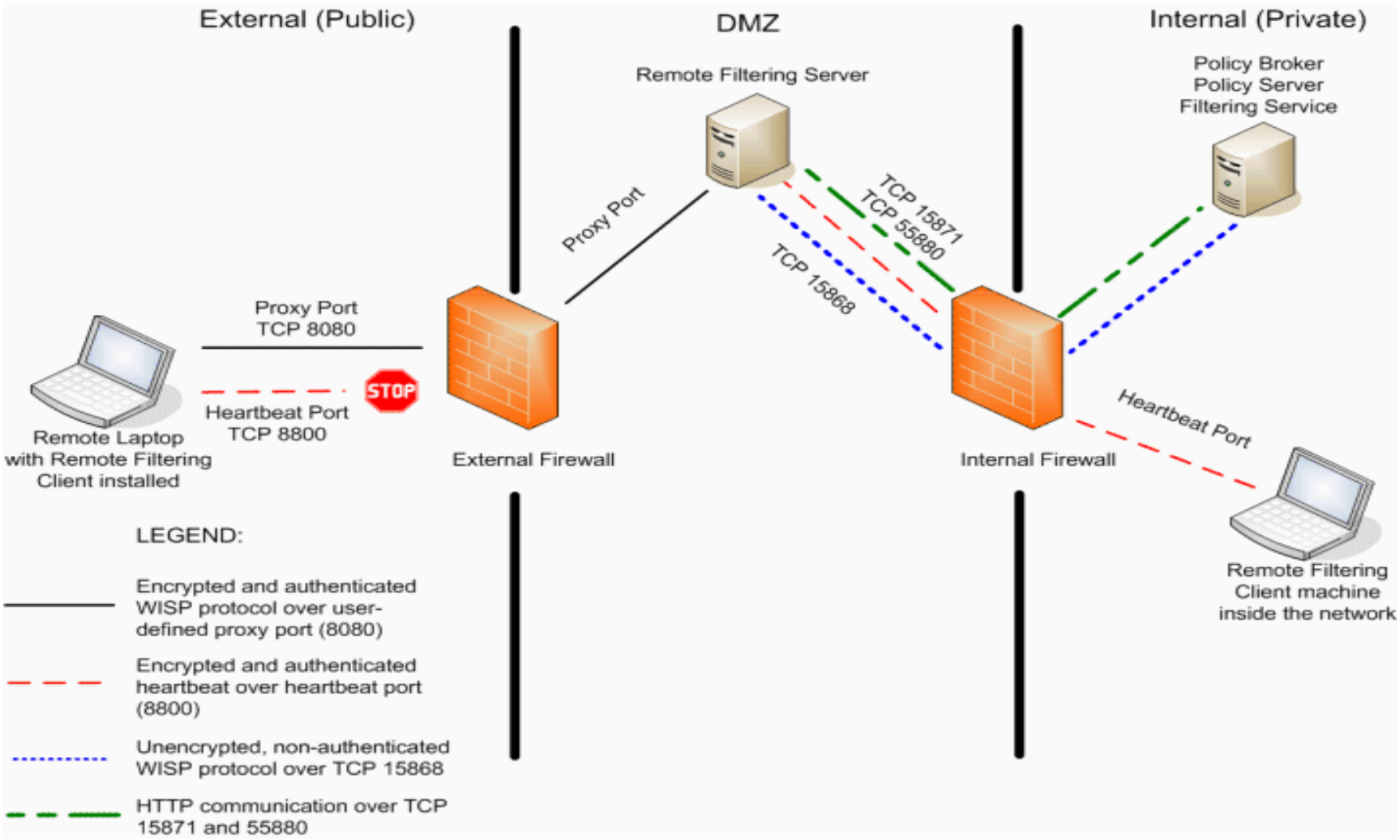
- Windows 7 (32-bit only)
- Windows XP SP3
- Windows Vista SP2

# Remote Filtering Server Deployment

Install the RFS server

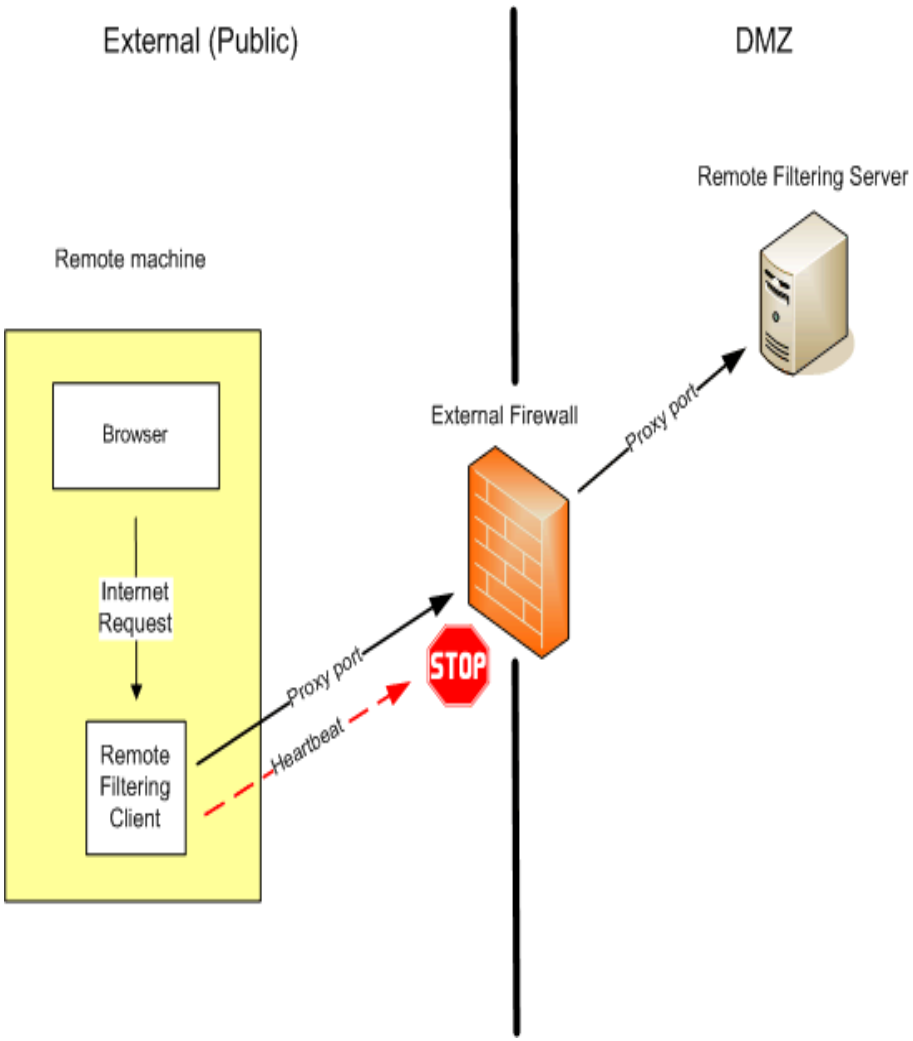
- Inside your organization's outermost network firewall
- In the DMZ outside the firewall that protects the rest of the network
- On its own, dedicated machine
- Do not install Remote Filtering Server on the same machine as Filtering Service or Network Agent.
- Install only one primary Remote Filtering Server for each Filtering Service in your network.
- Secondary and Tertiary RF Servers can be installed to provide failover.
- Remote Filtering clients should be configured to connect to backup servers in case of server failure.

# Remote Filtering Server Deployment



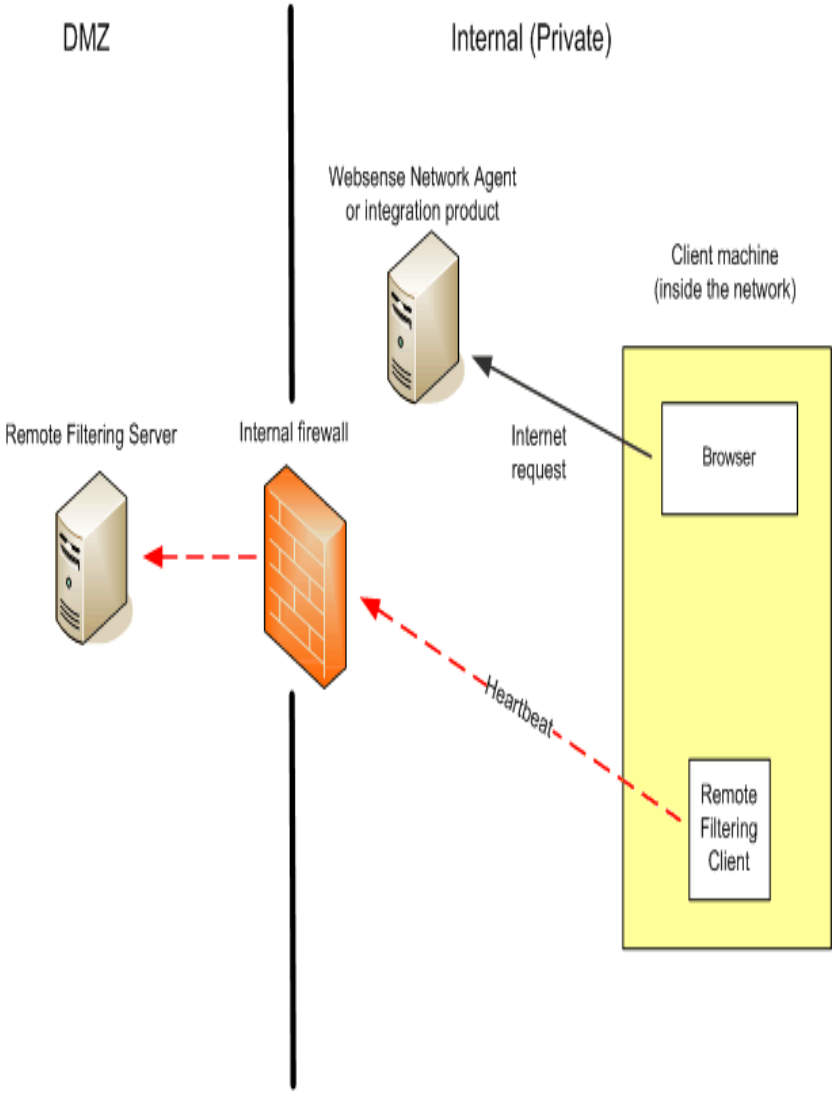
# How Remote Filtering works

- Remote Filtering client determines whether client is inside or outside the network
- If client is outside the network, request is sent to Remote Filtering Server
- External Clients attempt to connect to the Remote Filtering Server on the heartbeat port
- This port should be blocked on the external firewall
- Client will then connect using the proxy port to the RF Server in the DMZ.
- RF Server then forwards the request to Filtering service



# How Remote Filtering works

- Filtering Service evaluates the request and sends response to RF server.
- If site is blocked, RF client requests and receives the appropriate block page.
- When client is inside the network, the Remote filtering client attempts to connect on heartbeat port.
- This is successful hence client becomes passive and does not query Remote Filtering server.
- These requests are served by the integration partner as normal.



# Remote Filtering User Identification

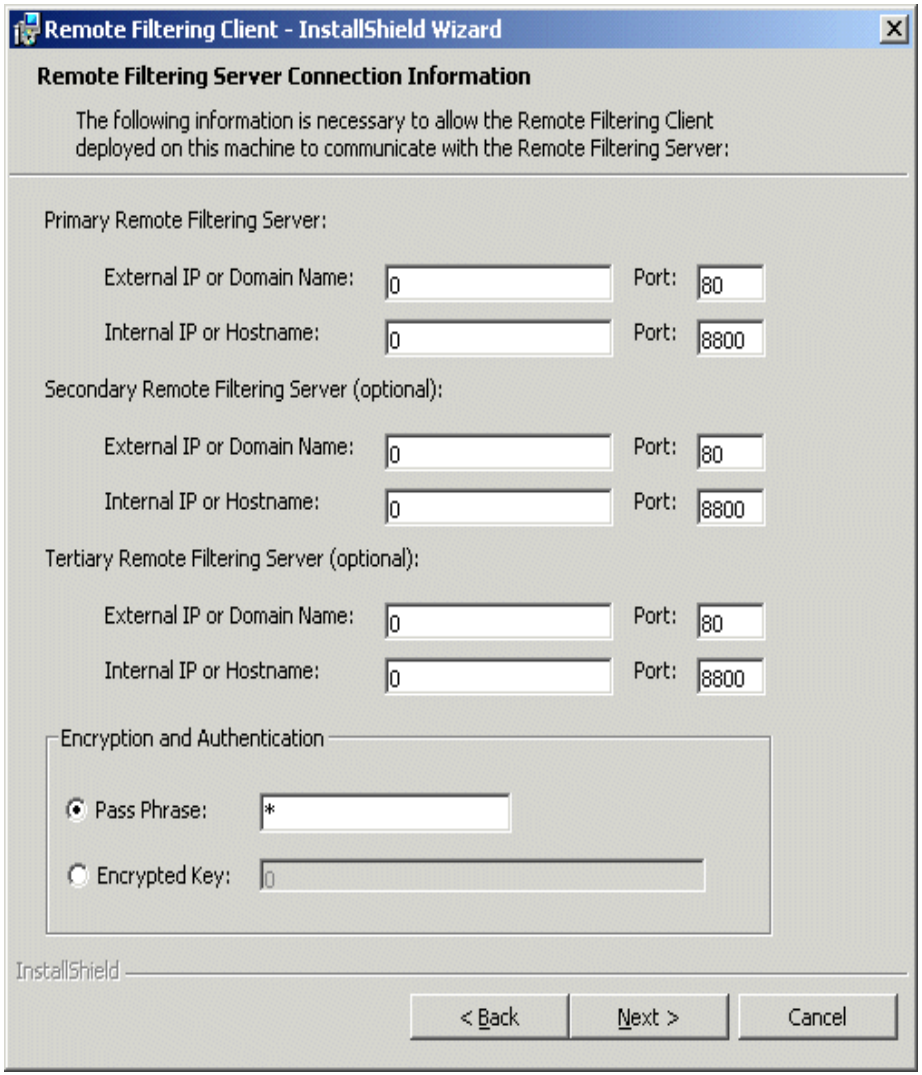
- If a user logs on using cached domain credentials, Filtering service is able to resolve the user name
- If users log on with a local user account then Filtering service cannot resolve the username and Default Policy will be applied
- Manual Authentication can be enabled to prompt users for entering user information. In this situation correct user based policy will be applied
- If user logs on using local account and manual authentication is not enabled Default Policy applies.
- Remote filtering cannot filter based on IP or networks.

# Remote Filtering Server Installation

- Run the installer, select Custom install and select Remote Filtering Server.
- Enter Policy Server IP and port number
- Enter External IP of Remote Filtering Server and port number.
- Enter Internal Communication port (HeartBeat)
- Enter and confirm passphrase
- Enter the Filtering service IP. If there is a firewall in between the RF server and Filtering service then enter the translated IP or clear the check box.
- Enter installation path and finish install

# Remote Filtering Client Installation

- Run the CPMclient.msi file to begin installation
- Enter the External IP and port number for Primary RF Server
- Enter the Internal IP and port number
- If any Secondary or Tertiary servers are installed enter the details.
- Enter the passphrase.



# Remote Filtering Client Installation

- Client can also be deployed using third party tools. Refer to installation document for more information
- Before installing the client on Windows Vista machines, User Account Control (UAC) must be disabled.

# Firewall Configuration

- On the External firewall, Remote Filtering proxy port must be opened for clients to communicate from outside with the Remote filtering server
- Heartbeat port should be blocked
- On the Internal Firewall, ports allowing communication between Remote Filtering server and Filtering server and Policy Server must be opened
- 15868, 15871 for filtering and block page
- 55806, 55880 for Policy Server and Broker. Also port 40000 for secure communication.

# Upgrade and Compatibility Guidance

- Before upgrading the Remote Filtering Server to 7.5 ensure that the Websense Filtering Service has been upgraded
- Remote Filtering Server is backwards compatible with the previous 2 versions of Remote Filtering Client
- So v7.5 Remote Filtering Server is compatible with Remote Filtering Client versions v7.1 and 7.0.x
- We recommend that clients should also be upgraded to the same version to ensure clients can use filtering enhancements available in the latest version

# Upgrade and Compatibility Guidance

- To upgrade Remote Filtering Server, run the installer and select option to upgrade. Follow on screen instructions
- To upgrade Remote Filtering Client, the following methods can be used

  **Manual upgrade:** Use the v7.5 Remote Filtering Client Pack installer on each client machine to upgrade the Remote Filtering Client. This upgrade method preserves existing Remote Filtering Client configuration settings.

  **Automatic upgrade with third-party tool:** Use the v7.5 Remote Filtering Client Pack and a third-party deployment tool to upgrade the Remote Filtering Client on client computers.

  For more information on the above methods please see Remote Filtering document on

  http://www.websense.com/content/support/library/web/v75/remote_filtering/remote_filtering.pdf

  For Manual procedure, see page 32.

  For Automatic upgrade using Third-party deployment tool, see page 33.

# Troubleshooting Remote Filtering

- No Remote Filtering clients are being filtered
  - Verify that the correct Passphrase is being used while installing the clients
  - Verify the parameters on Securewispproxy.ini file, this can be located in C:\Program Files\Bin directory on the RF Server
  - Parameters entered on the RF client should match with what is entered in this file.
  - The client parameters can be verified from registry by checking the following registry key

    HKLM\Software\Websense\Desktop Client\Desktop Filtering

# Troubleshooting Remote Filtering

securewispproxy.ini - Notepad

File Edit Format View Help

```
[SecureWISPProxy]

# The protocol used to for wrapping WISP requests
raw|http|secure
WispMode=secure

# Proxy Server parameters
ProxyIP=10.3.131.1
ProxyPort=8082
ProxyMaxConnections=10000
ProxyPublicAddress=195.244.17.11

# Time to wait for WISP requests, handshake, etc., seconds
ProxyTimeout=120

# HeartBeat Server Parameters
HeartBeatPort=8800
HeartBeatTimeout=5

# Web-Filtering connection parameters
WebFilterIP=10.3.131.16
WebFilterPort=15868
WebFilterMaxConnections=50

# Time to wait for WISP lookup responses, seconds
WebFilterTimeout=10

# Object Model connection parameters
objectModelIP=10.3.131.16
objectModelPort=55880
objectModelToken=6B9A07396664793EB7D38AC907E7999B6B8951DE6E
4090D0B3F3AE1865C0D0A60E55A159BDE4186874FF167E9FDAB21861270
B4A333867CC5D725DE64BFC03C698680FAC26F3555EAAC28BCB16781318
6CE18F5B3A292BE5CD301A6C339F1EEC0C8BBC7C99955E799AE85AF4923
219E7FE09B10E5D0677BE3DFB6BDE46CDB107A01996E0074566B06AE7A
12D362F8E7582763E789585B919EE4DEBE4BE1904CD926F4E341D6157E
objectModelRetryTime=10
objectModelWaitTime=180

# Blockserver connection parameters
BlockServerIP=10.3.131.16
BlockServerPort=15871

# Time to wait for BlockPage responses, seconds
BlockServerTimeout=10

#Trace type to trace All|WISP|BlockPage|HeartBeat
TraceType=none
TraceFile=traceFile.log
TraceFileSize=1
```

Private Remote Filtering Server IP address, used for internal communication with Filtering Service.

TCP port used by Remote Filtering Clients for the filtering of Web requests.

Public IP Address of the Remote Filtering Server. This is the IP address that Remote Filtering Clients connect to.

TCP port used for internal heartbeat communication between the client and server.

Internal IP address and port of the Filtering Service that handles Remote Filtering requests.

IP address and port of the server that sends block pages to Remote Filtering Clients.

# Troubleshooting Remote Filtering

websense
ESSENTIAL INFORMATION PROTECTION™

- Remote Filtering Server logs errors in the RFSErrors.log file in the Websense installation directory (C:\Program Files\Websense or /opt/Websense, by default).
- To enable more detailed tracing:

1. Open the Remote Filtering Server **SecureWispProxy.ini file**
2. Set **TraceType=All.**
3. Restart the Remote Filtering Server service or daemon.
4. A trace file called **traceFile.log is created in the Websense installation directory**

# Troubleshooting Remote Filtering

- Remote Filtering client trace can also be useful in troubleshooting problems

  1. Open the Windows Registry and navigate to: **HKLM\Software\Websense\Desktop Client**
  2. Add a new string variable and called **Trace Target with a value of 2.**
  3. Restart the machine.
  4. A trace file called trace.log is created in C:\Program Files\Websense\WDC\Debug, by default.

# Troubleshooting Remote Filtering

websense
ESSENTIAL INFORMATION PROTECTION™

- Remote Clients do not receive Block page

  - Ensure that the firewall between Remote Filtering Server and the Filtering Service machine is correctly configured. Port 15871 must be allowed on the internal firewall.

  - Make sure Remote Filtering Client is not installed on the Remote Filtering Server machine. This can use up all available connections meaning remote clients cannot connect to RF Server.

- Clients with mobile data cards are not filtered on the default port (80)

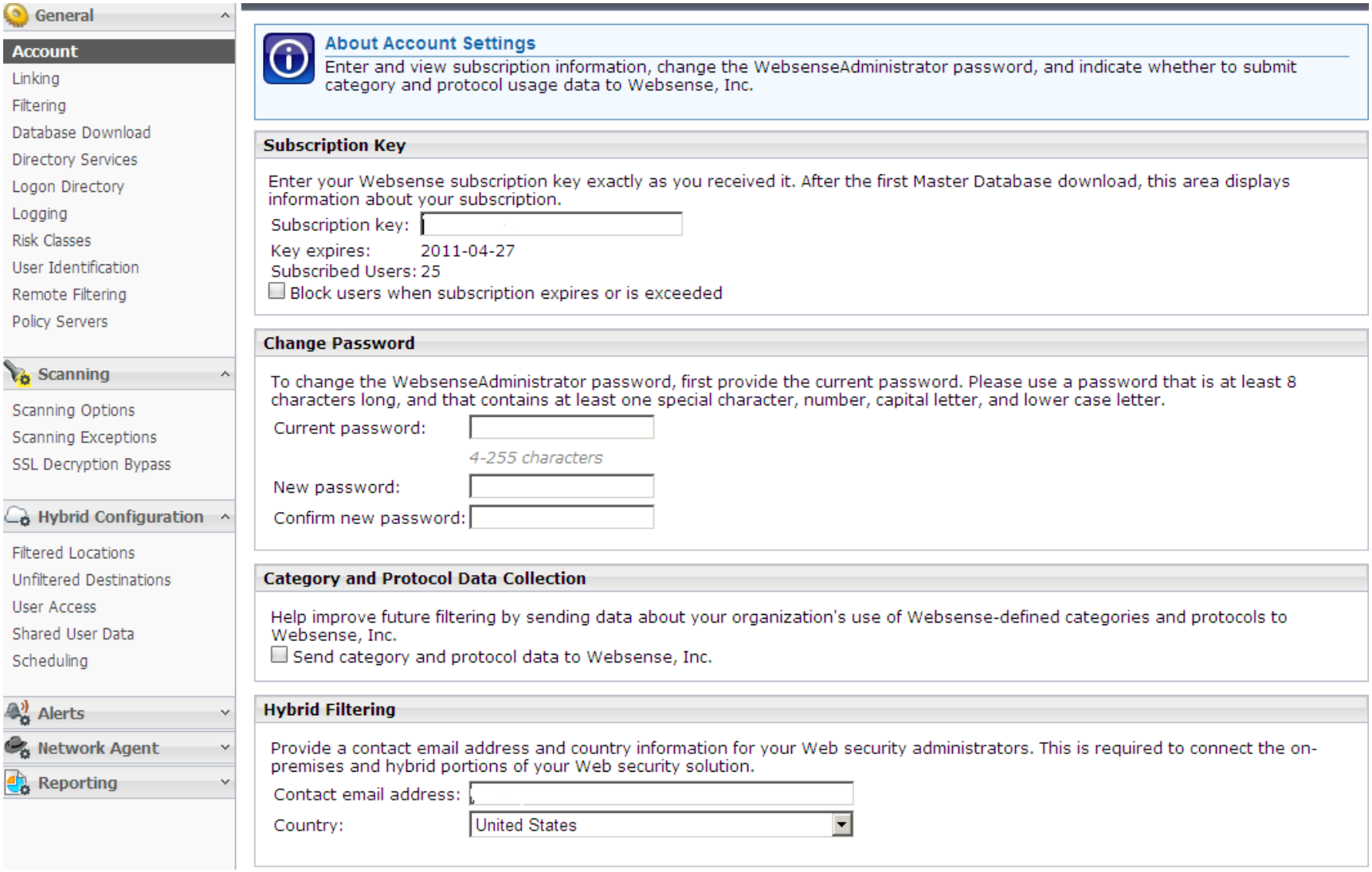
  – Select another proxy port (such as 81 or 8082).

  – Modify the **ProxyPort parameter in the Remote Filtering Server SecureWispProxy.ini file to reflect the new port.**

  – Install Remote Filtering Client using the new port or modify the registry key related to Proxyport

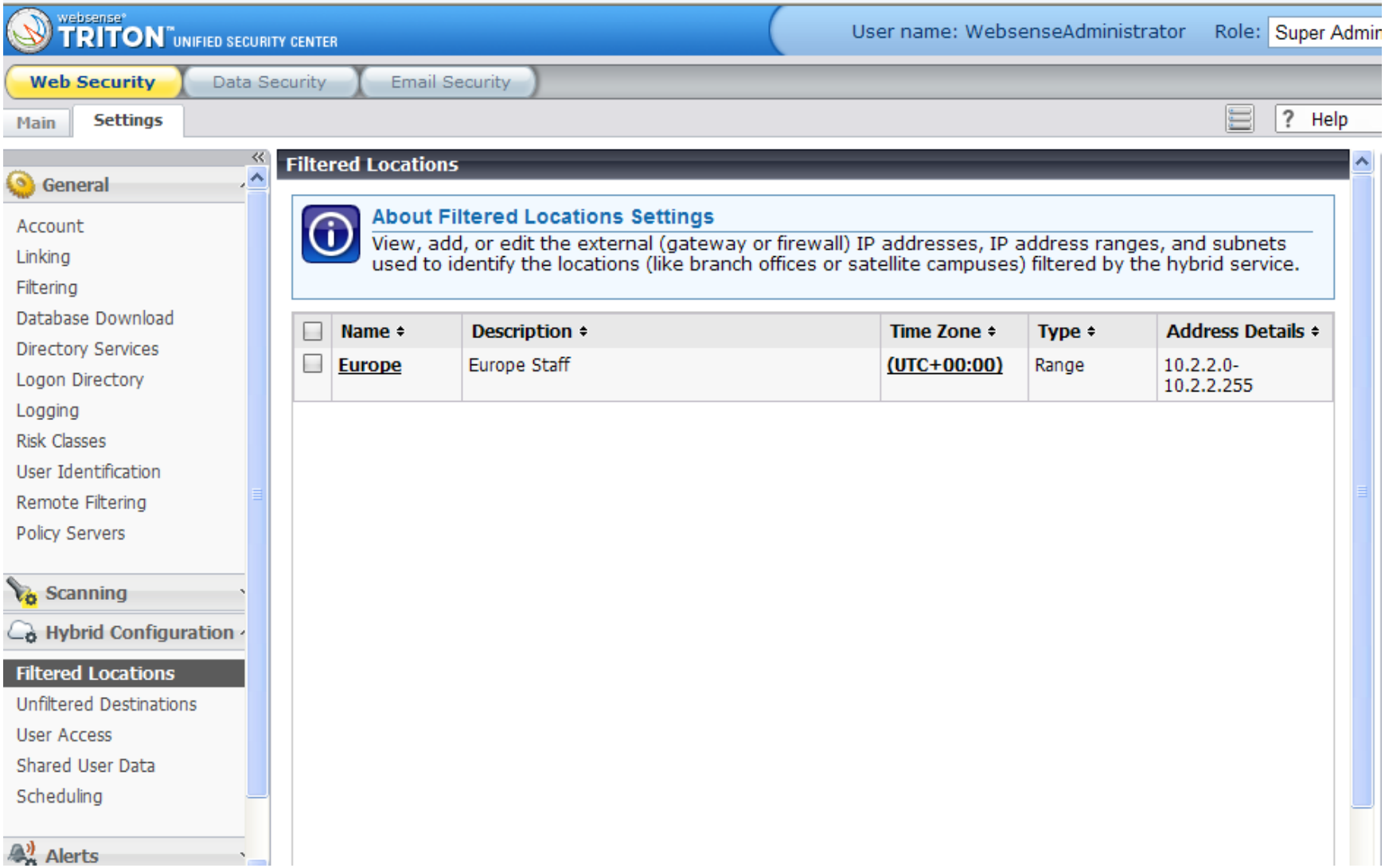
  – Modify firewall rules to allow the port.

# Configuring Hybrid Filtering



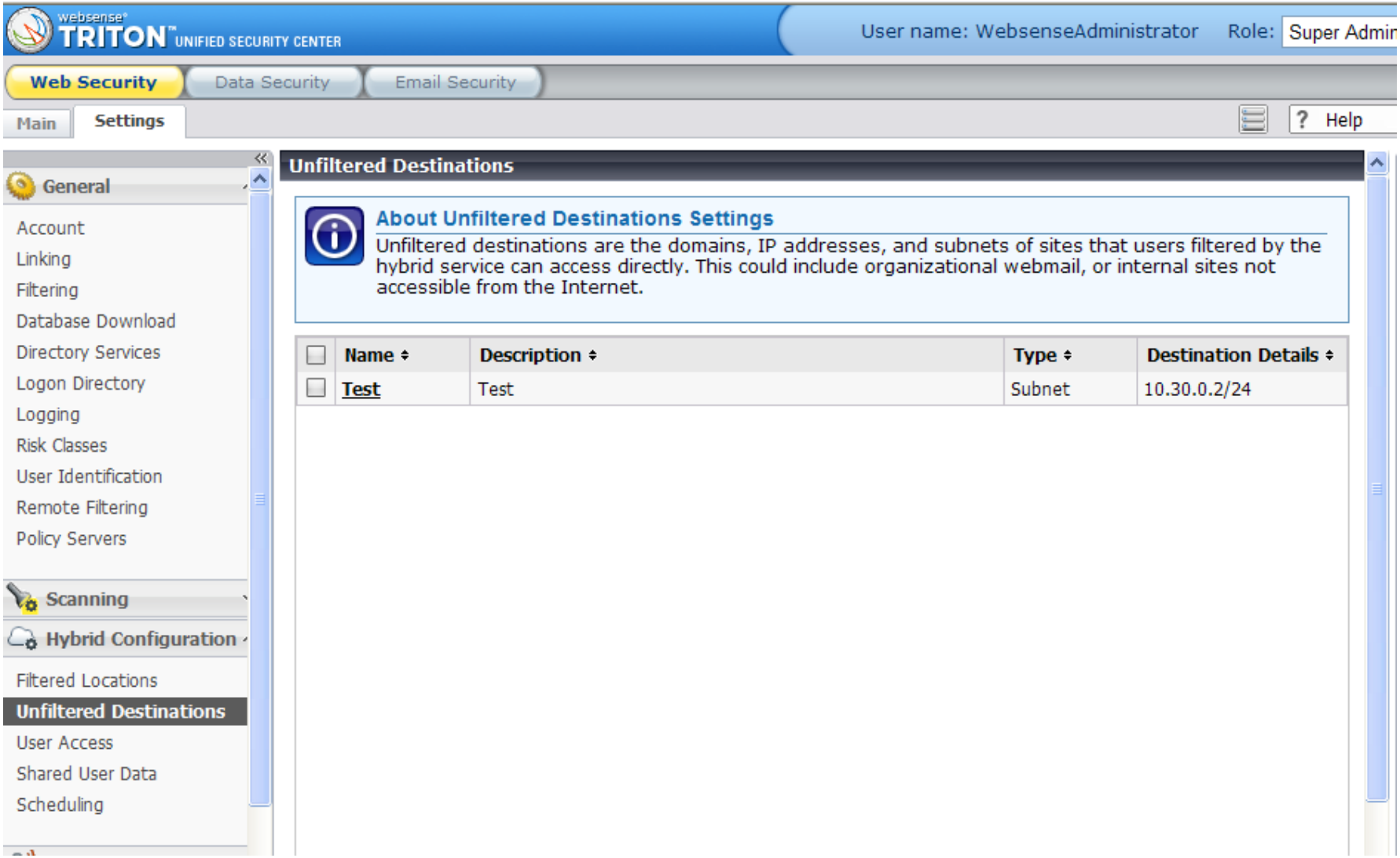
# Hybrid Filtered Locations

websense
ESSENTIAL INFORMATION PROTECTION™



# Hybrid Unfiltered Destinations

websense
ESSENTIAL INFORMATION PROTECTION™



# Hybrid User Access Settings

websense
ESSENTIAL INFORMATION PROTECTION™

TRITON UNIFIED SECURITY CENTER

User name: WebsenseAdministrator Role: Super A

Web Security | Data Security | Email Security

Main | Settings

? Help

**General**

- Account
- Linking
- Filtering
- Database Download
- Directory Services
- Logon Directory
- Logging
- Risk Classes
- User Identification
- Remote Filtering
- Policy Servers

**Scanning**

**Hybrid Configuration**

- Filtered Locations
- Unfiltered Destinations
- User Access
- Shared User Data
- Scheduling

**Alerts**

**Network Agent**

**Reporting**

## User Access

Common Options | Off-Site Users

### Proxy Auto-Configuration (PAC) File

Configure browsers on users' machines to use this URL to retrieve hybrid proxy configuration details:
http://hybrid-web.global.blackspider.com:8082/proxy.pac?p=32skvwb6

### Availability

If the hybrid service is not available:

- (●) Allow users to access the Internet without being filtered
- ( ) Prevent users from accessing the Internet

### Default Policy Time Zone

Select the default time zone to use when applying policies.

Time zone: (UTC+00:00) Greenwich Mean Time : Dublin, Edinburgh, Lisbon, London

### User Identification

- [x] Use NTLM to identify users when possible.
- [x] Prompt users not identified via other means for logon information.

#### Configure Welcome Page

Specify whether users should be prompted for logon information via a Welcome page displayed in the browser, and how the page should be displayed. If the Welcome page is not used, a browser dialog box prompts users for logon information.

- (●) Use HTTPS to display the page when users request a secure site; otherwise use HTTP.
- ( ) Always use HTTP to display the page.
- ( ) Do not display a Welcome page.

Verify End User Configuration

Access the link below from an end user's machine to confirm that the browser is configured properly.

# Hybrid User Access Settings

websense
ESSENTIAL INFORMATION PROTECTION™

TRITON UNIFIED SECURITY CENTER

User name: WebsenseAdministrator Role: Super A

Web Security | Data Security | Email Security

Main | Settings

? Help

General
- Account
- Linking
- Filtering
- Database Download
- Directory Services
- Logon Directory
- Logging
- Risk Classes
- User Identification
- Remote Filtering
- Policy Servers

Scanning

Hybrid Configuration
- Filtered Locations
- Unfiltered Destinations
- User Access
- Shared User Data
- Scheduling

Alerts

Network Agent

Reporting

## User Access

Common Options | Off-Site Users

### Filtering Users Outside Your Network

**Generate User Passwords**

If the hybrid service receives an Internet request that does not originate from locations filtered by the hybrid service, the user is prompted for a password. The password can be automatically generated, or be manually created by the user.

☐ Automatically generate and email passwords for users identified by Directory Agent

**Combine Filtering Methods**

If some users are filtered by the hybrid service when they are at home or on the road, but otherwise use on-premises filtering, enter a host name that can only be resolved from outside your network.

Host name:

If Internet requests from within your network pass through an explicit proxy, enter the proxy location and port to ensure optimized filtering.

Host name/IP address: Port:

### Registered Domains

If you want users to be able to connect to the hybrid service from outside a filtered location, enter the domains belonging to your organization. Users with email addresses in these domains can self-register with the hybrid service.

| ☐ | Domain | Description | Include Subdomains |
|---|---|---|---|

Add | Delete

# Hybrid Shared User Data

websense
ESSENTIAL INFORMATION PROTECTION™

TRITON UNIFIED SECURITY CENTER — User name: WebsenseAdministrator — Role: Super Admini

Web Security | Data Security | Email Security

Main | Settings | Help

General
- Account
- Linking
- Filtering
- Database Download
- Directory Services
- Logon Directory
- Logging
- Risk Classes
- User Identification
- Remote Filtering
- Policy Servers

Scanning

Hybrid Configuration
- Filtered Locations
- Unfiltered Destinations
- User Access
- Shared User Data
- Scheduling

Alerts

Network Agent

Reporting

Shared User Data > Directory Agent

About Directory Agent Settings

Review and configure the Directory Agent settings that determine how the agent collects directory service (user and group) information for the hybrid service.
Configure directory service types and locations on the Directory Services page.
Note: Directory Agent does not support Windows NT Directory / Active Directory (Mixed Mode) or Sun Java System Directory.

**Active Directory (Native Mode)**

Click a name or IP address to configure how Directory Agent collects user data from the selected directory server.

| Name or IP Address | Port | Context | User Search | Group Search | Filters |
|---|---|---|---|---|---|
| 10.5.144.100 | 3268 | None | All levels | All levels | None |

Go to the Directory Services page to change a directory server name or IP address.

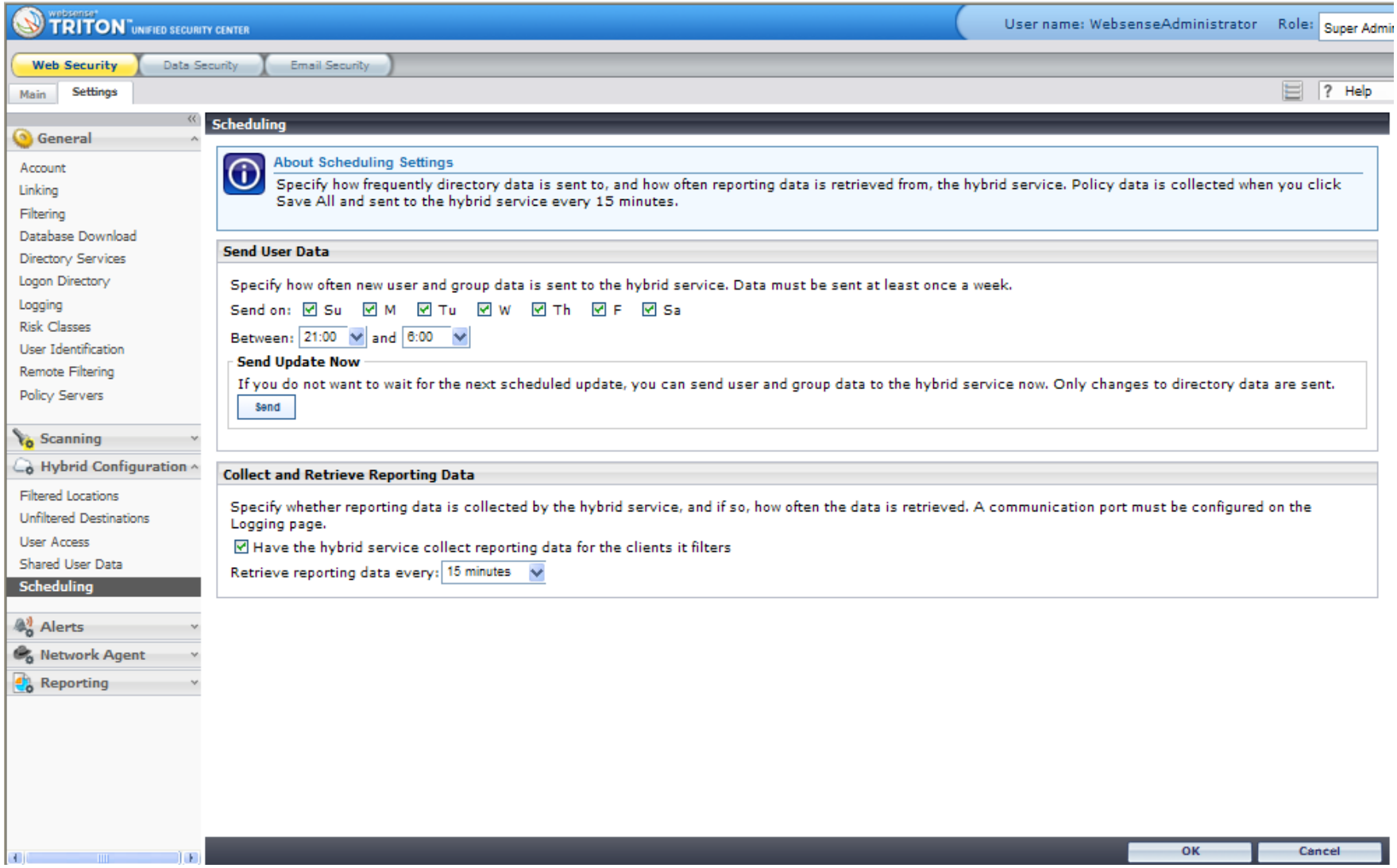
**Synchronize User Data**

Provide the name or IP address of the Websense Sync Service machine and the port used to communicate with the hybrid service.

Name or IP address: Port: 55832 Test Connection

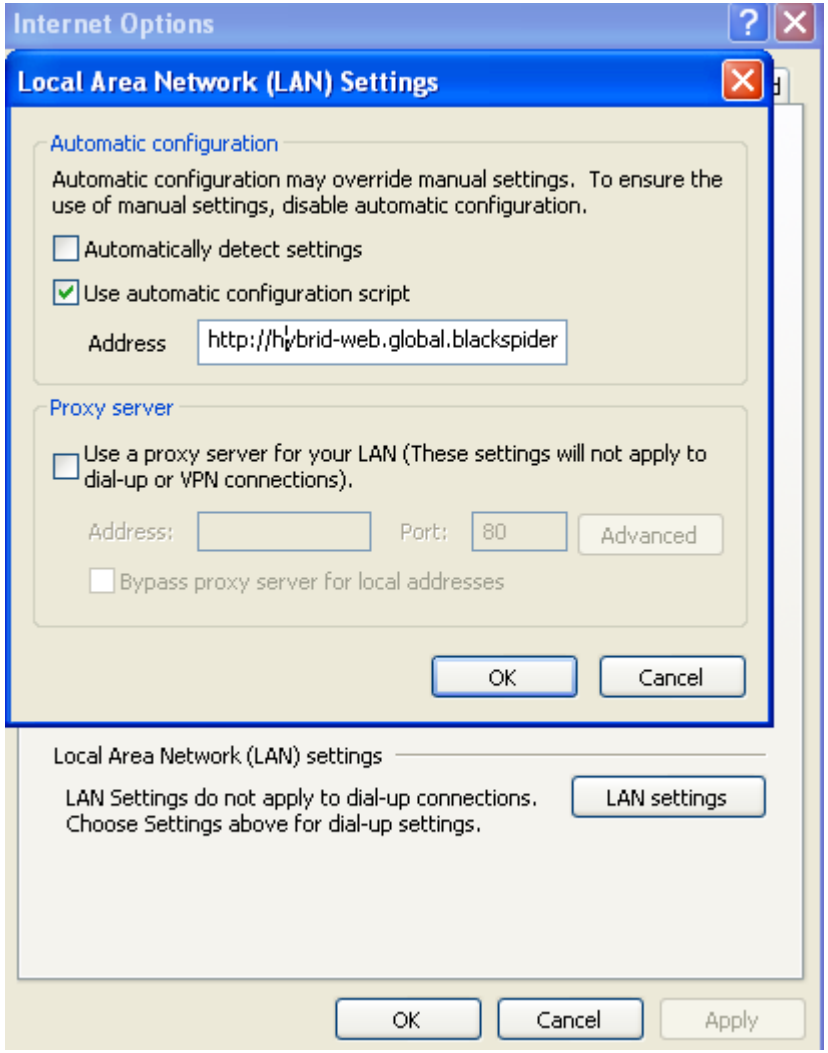
# Hybrid Scheduling

websense®
ESSENTIAL INFORMATION PROTECTION™



# PAC file configuration

- Client browsers need to be configured with the PAC file URL found on the Hybrid Configuration options on the manager.
- Can be configured manually from Internet Options->Connections->LAN settings
- Configuration can also be done via GPO



# Identification for Off site Users

websense
ESSENTIAL INFORMATION PROTECTION™

- If users are coming from a filtered location they will be identified via NTLM.
- If hybrid service receives an internet request from an unfiltered location users will be prompted for a password.
- The password can be automatically generated or manually created by the user by clicking on forgot password option.
- Authentication for roaming users supports basic authentication method.

# Tips for applying Hybrid Filtering

websense
ESSENTIAL INFORMATION PROTECTION™

- Make **certain** that the administrator email address for your account is correct, and that messages sent to that address are read and acted on quickly.
- If you have multiple Directory Agent instances, make sure each is configured to use a unique, non-overlapping directory context.
- Make sure that you have only one Sync Service instance, and that it is configured to send user information to the hybrid service at appropriate intervals.
- Add your organization's webmail address as an unfiltered destination.

# Support Online Resources

websense®
ESSENTIAL INFORMATION PROTECTION™

## 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

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

# Webinar Announcement

**Webinar Update**

Title: v7.5 Websense Web Security Jump Start: Configuration and Setup

Date: September 15, 2010

Time: 8:30 AM PDT (GMT -7)

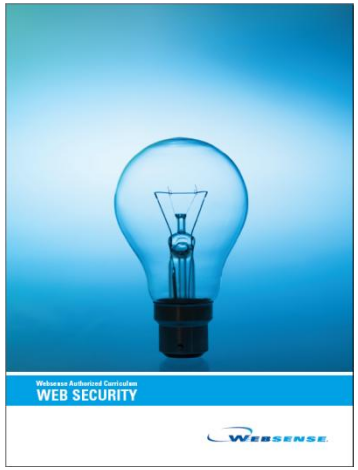
How to register:
http://www.websense.com/content/SupportWebinars.aspx

# 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

WEBSENSE® Authorized Training Partner

WEBSENSE® Certified Instructor



# Questions?