

Troubleshooting and Best Practice Tips for Hybrid Web Endpoint Users

WebSense Support Webinar
December, 2013



TRITON STOPS MORE THREATS. WE CAN PROVE IT.



websense
TRITON®



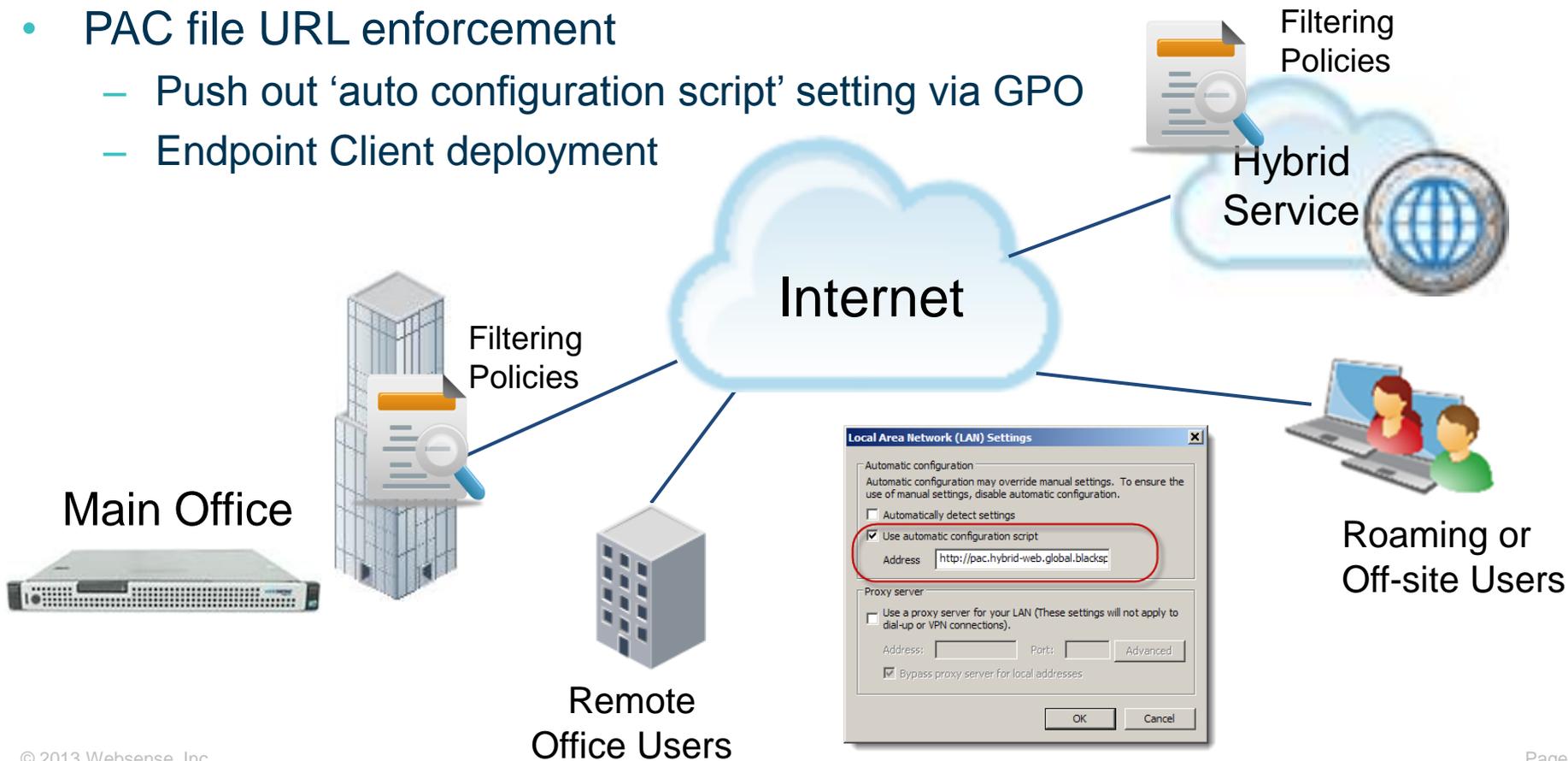
Greg Didier

- **Title:**
 - Technical Trainer eSupport
- **Accomplishments:**
 - 10 years supporting Websense products
- **Qualifications:**
 - Technical Support mentor
 - Product trainer
 - Knowledge base writer

- Explore hybrid features and settings in the Web Security console
- Hybrid components
- Directory service synchronization and configuration
- Troubleshooting directory synchronization
- Hybrid identification
- Hybrid reporting
- Best practice tips

Hybrid Filtering

- PAC file URL enforcement
 - Push out 'auto configuration script' setting via GPO
 - Endpoint Client deployment



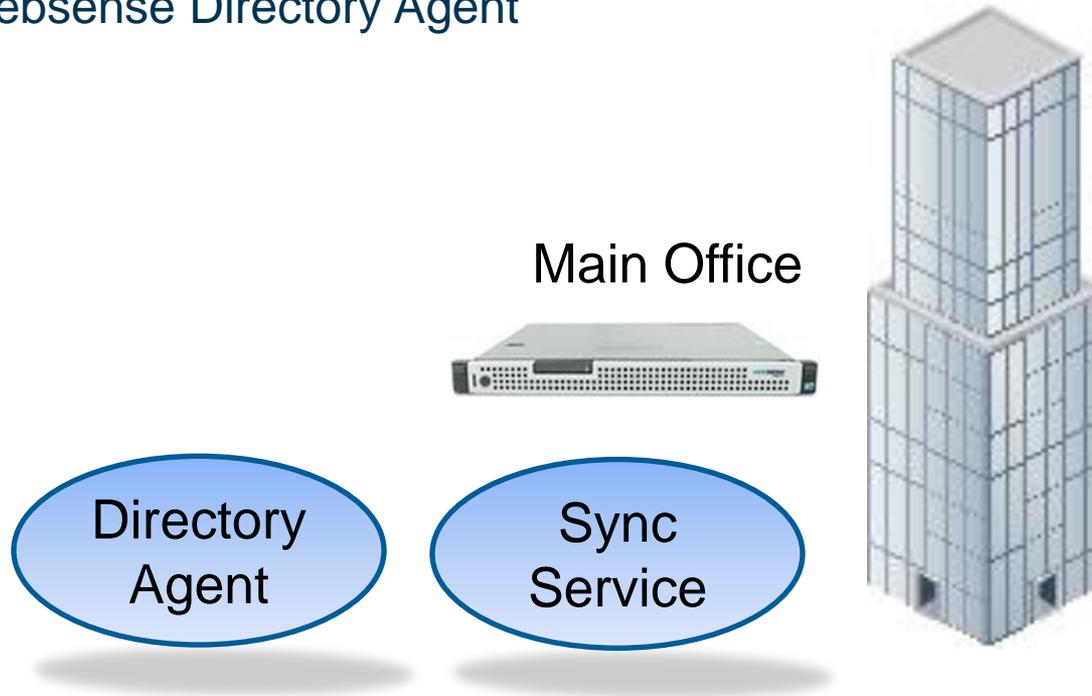
- Hybrid filtering does not enforce protocol filters
- Hybrid filtering does not use Bandwidth Optimizer settings
 - No bandwidth-based restriction enforcement
- On-premises custom block messages are not displayed
 - Hybrid solution: **Settings > Hybrid Configuration > User Access page > customize hybrid block page**
- ACEInsight link does not appear on hybrid block pages
- Hybrid filtering does not apply policies to computer IP addresses
 - You can apply policies to a defined Filtered Locations
- Windows Active Directory Mixed Mode not supported



On-premises



- Hybrid Web Security requires two 'on-premises' components:
 - Websense Sync Service
 - Websense Directory Agent



- On-premises service: sends and receives policies, custom PAC file, alerts, user/group and reporting data
- Deployment:
 - Only one Sync Service instance allowed
 - Best practice—install with Log Server
- Communicates with:
 - Hybrid (cloud) service on port 443
 - Log Server on port 55885 (outbound)
 - Directory Agent on port 55832 (inbound)
 - Web Security manager on port 55832 (inbound)
 - Policy Broker on port 55880 (outbound)
 - Policy Server on port 55830 (inbound) and ports 55806 and 40000 (outbound)



- Collects directory information and forwards it to Sync Service
- Directory Agent Deployment:
 - One instance per Policy Server
 - Policy Server must have an associated User Service instance
 - Communicates with the same directory service as User Service
 - You can only use one Directory Agent per domain
 - For each User Service that connects to a different directory service install a Directory Agent instance
 - All Directory Agent instances must connect to a single Sync Service
 - By default, Directory Agent is enabled on the V-series appliance
 - TIP: Disable Directory Agent and install with Sync Service (off the appliance)
 - Communicates with:
 - Your LDAP-based directory service
 - Sync Service on port 55832
 - Policy Server on ports 55806 and 40000



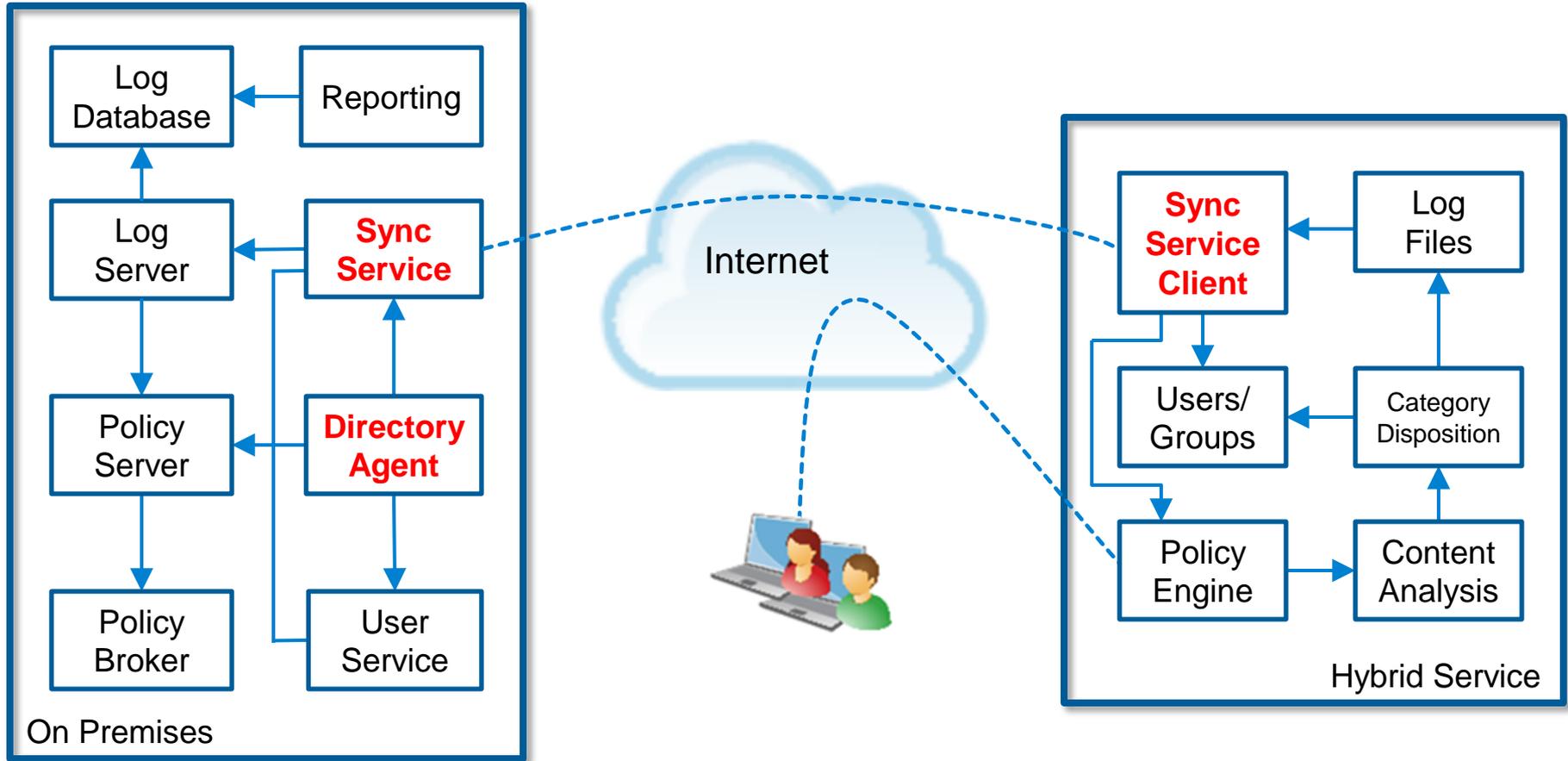
Directory
Agent

- Configuration:
 - Configure User Service first
 - The domain controllers you enter in User Service settings appear on the Directory Agent page
 - A User Service configuration change may require updating Directory Agent
 - **Settings > Hybrid Configuration > Shared User Data** page
 - Supplemental Directory Agent instances
 - Use a unique, non-overlapping root context
 - You must manually configure the Sync Service connection
 - This is automatic for the primary instance connecting to same Policy Server as Sync Service
 - Typically, Directory Agent uses a more restrictive root context than User Service

A blue oval callout with a dark blue border and a light blue fill, containing the text 'Directory Agent'. It is positioned to the right of the 'Supplemental Directory Agent instances' section of the list.

Directory Agent

Websense Sync Service



- Hybrid service filters Internet requests originating from recognized and unrecognized locations (off-site users)
- Hybrid filtering applies policies to:
 - Users, groups and domains (OUs)
 - Requires Directory Agent
 - Filtered Locations
 - Requires defining the external IP address
- To apply a policy to a Filtered Location:
 1. Add a location (**Settings > Hybrid Configuration > Filtered Locations**)
 2. Add a computer or network client (**Policy Management > Clients**)
 3. Apply a policy to the IP address or IP range (the location from step one)

- For each request that the hybrid service receives:
 1. Verify subscription compliance (clients not exceeded)
 2. Determine which **exception** or **policy** applies (in the following order):
 - a. **User**
 - b. **Groups** the user belongs to
 - c. The user's **domain** (OU)
 - d. **External IP address** (Filtered Location from which the request originates)
 - e. **Default** policy (no user, group, or location IP policy or exception applies)
 - The clean-up rule
- The first applicable exception or policy found is used
 - NOTE: Hybrid filtering applies a *group* policy before an *IP-based* policy

- [Hybrid configuration](#)
 1. Activate your hybrid filtering account
 - **Settings > General > Account** page

Hybrid Filtering

Provide a contact email address and country information for your Web security administrators. This is required to connect the on-premises and hybrid portions of your Web security solution.

Contact email address:

Country: 

Resume Hybrid Filtering Communication

Enter your security token and click Connect to establish a connection with the hybrid service

Security token:

- [Hybrid configuration](#)
 2. Define filtered locations
 - **Settings > Hybrid Configuration > Filtered Locations** page

Filtered Locations

 [Manage Explicit Proxies](#)

<input type="checkbox"/>	Name ↕	Description ↕	Time Zone ↕	Proxy Mode ↕	Type ↕	Address Details ↕
<input type="checkbox"/>	CA - San Deigo	Corporate Office.	(UTC+00:00)	Hybrid	IP address	204.15.64.96
<input type="checkbox"/>	AZ - Phoenix	Remote sales office.	(UTC-07:00)	Hybrid	IP address	179.179.179.179
<input type="checkbox"/>	OR - Portland	Manufacturing plant.	Not applicable	Explicit	IP address	204.15.64.99
<input type="checkbox"/>	WA - Seattle	Remote sales office.	(UTC-08:00)	Hybrid	IP address	204.15.64.98

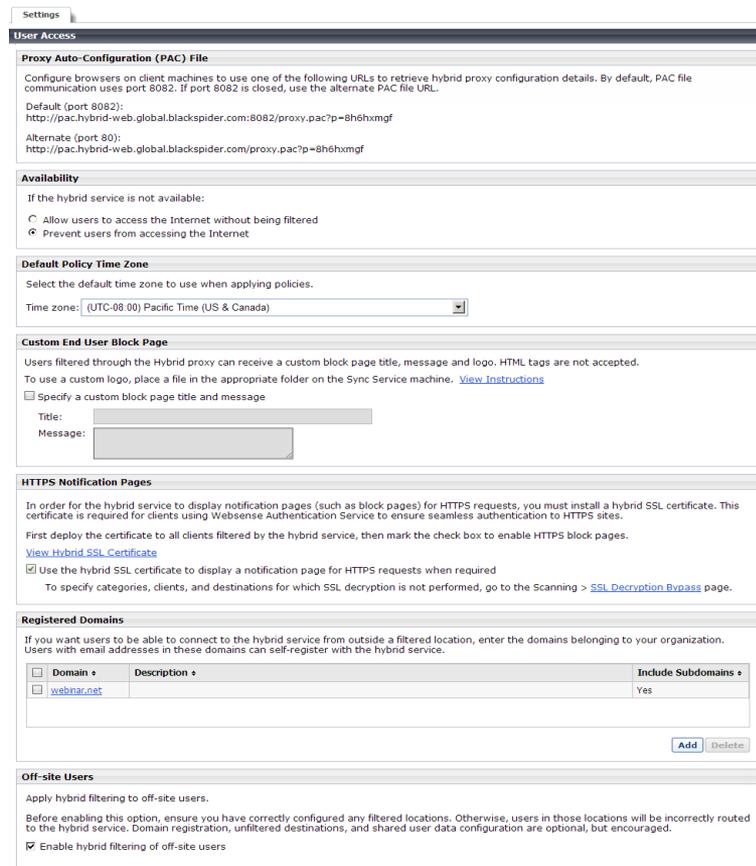
[Add](#) [Delete](#)

- [Hybrid configuration](#)
 3. Specify sites not filtered by hybrid service
 - **Settings > Hybrid Configuration > Unfiltered Destinations** page

Unfiltered Destinations					
<input type="checkbox"/>	Name ↕	Description ↕	Type ↕	Destination Details ↕	Proxy ↕
<input type="checkbox"/>	Corporate email	Allows off-site Hybrid users to register or reset their password.	Domain	webinar.net	Hybrid

[Add](#) [Delete](#)

- Hybrid configuration
 4. Configure user access to hybrid filtering
 - **Settings > Hybrid Configuration > User Access** page
 - Proxy Auto-Configuration (PAC) File
 - Availability
 - Default Policy Time Zone
 - Customer End Block Page
 - HTTPS Notification Pages
 - Registered Domains
 - Off-site Users



Settings

User Access

Proxy Auto-Configuration (PAC) File

Configure browsers on client machines to use one of the following URLs to retrieve hybrid proxy configuration details. By default, PAC file communication uses port 8082. If port 8082 is closed, use the alternate PAC file URL.

Default (port 8082):
`http://pac.hybrid-web.global.blackspider.com:8082/proxy.pac?p=8h6hxmfg`

Alternate (port 80):
`http://pac.hybrid-web.global.blackspider.com/proxy.pac?p=8h6hxmfg`

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:

Custom End User Block Page

Users filtered through the Hybrid proxy can receive a custom block page title, message and logo. HTML tags are not accepted. To use a custom logo, place a file in the appropriate folder on the Sync Service machine. [View Instructions](#)

Specify a custom block page title and message

Title:

Message:

HTTPS Notification Pages

In order for the hybrid service to display notification pages (such as block pages) for HTTPS requests, you must install a hybrid SSL certificate. This certificate is required for clients using Websense Authentication Service to ensure seamless authentication to HTTPS sites.

First deploy the certificate to all clients filtered by the hybrid service, then mark the check box to enable HTTPS block pages. [View Hybrid SSL Certificate](#)

Use the hybrid SSL certificate to display a notification page for HTTPS requests when required

To specify categories, clients, and destinations for which SSL decryption is not performed, go to the Scanning > [SSL Decryption Bypass](#) page.

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
<input type="checkbox"/>		
<input checked="" type="checkbox"/>	webnar.net	Yes

Off-site Users

Apply hybrid filtering to off-site users.

Before enabling this option, ensure you have correctly configured any filtered locations. Otherwise, users in those locations will be incorrectly routed to the hybrid service. Domain registration, unfiltered destinations, and shared user data configuration are optional, but encouraged.

Enable hybrid filtering of off-site users

- Hybrid configuration

- 5. Identification of hybrid filtering users

- **Settings > Hybrid Configuration > Hybrid User Identification page**

NTLM, Secure Form, and Manual Authentication

Specify additional methods the hybrid service uses to authenticate or identify users.

- Use NTLM to identify users when possible
- Use secure form authentication
- Always authenticate users on first access

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 a different Welcome page for HTTP and HTTPS requests
- Use the same Welcome page for both HTTP and HTTPS requests
- Do not display a Welcome page

Verify End User Configuration



Verify End User Configuration

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

<http://query.webdefence.global.blackspider.com/>

Use the link below to test the Web connectivity and performance of any machine filtered by the hybrid service.

<https://www.mailcontrol.com/utility/WDmonitor/monitor.mhtml>

- [Hybrid configuration](#)

- 6. Send user and group data to the hybrid service

- **Settings > Hybrid Configuration > Shared User Data** page
 - Incorrectly configuring or not optimizing the Directory Agent search context are the most common Tech Support issue.

Shared User Data > Directory Agent

Active Directory (Native Mode)

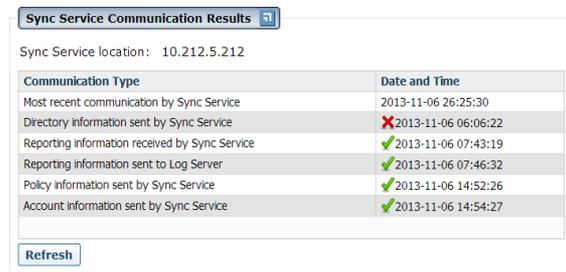
Click a name or IP address to configure how Directory Agent collects user data from the selected directory server.

Name or IP Address	Port	Contexts	Filters
10.212.11.162	3268	View Context	None
10.212.5.210	3268	View Context	None

Go to the [Directory Services](#) page to change a directory server name or IP address.

- Three phase implementation
 - a. Define your hybrid users and limit domain controller involvement
 - b. Define Explicit Proxies, Filtered Locations, Unfiltered Destinations, your domain and User Access/Hybrid Identification methods
 - c. Define your search context
- Demonstration
 - This article outlines and provides more details on the demonstration.
 - [Best practices suggestions for configuring hybrid](#)

- **Web Security > Main > Status > Hybrid Service** page
 - Last Directory Agent Sync Results
 - Sync Service Communication Results
- Hybrid Filtering Alerts table (**Status > Alerts** page)
 - Click the **View Details** button
- Determine why a request was blocked
 - Right-click anywhere in the block message and select **View Source**
- Sync Viewer web page info: http://<Sync_Service_IP>:55832/viewer
- Hybrid confirmation page: <http://query.webdefence.global.blackspider.com>
- You cannot resolve the 'Duplicate email addresses' sync failure when:
 - Reusing an email address from a prior deleted sync'd account (*Do not do this!*)
 - To display users in reports, hybrid service retains all sync'd email addresses

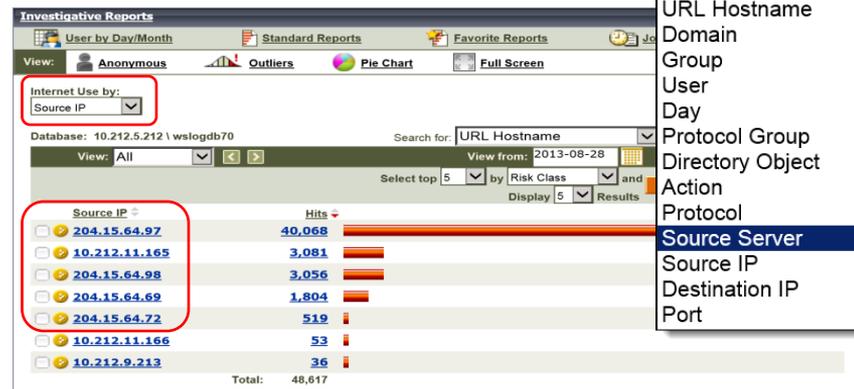


Sync Service location: 10.212.5.212

Communication Type	Date and Time
Most recent communication by Sync Service	2013-11-06 26:25:30
Directory information sent by Sync Service	✘ 2013-11-06 06:06:22
Reporting information received by Sync Service	✔ 2013-11-06 07:43:19
Reporting information sent to Log Server	✔ 2013-11-06 07:46:32
Policy information sent by Sync Service	✔ 2013-11-06 14:52:26
Account information sent by Sync Service	✔ 2013-11-06 14:54:27

Refresh

- To pass hybrid reporting data to Log Server, configure the hybrid logging port under the **Settings > General > Logging** page
- **Main > Status > Dashboard > System**
 - *Hybrid Bandwidth Trend*—shows bandwidth consumed by Internet requests
 - *Hybrid Requests*—shows the number of permitted and blocked requests
- **Main > Status > Hybrid Service**
 - *Hybrid Authentication Reports*—see how hybrid users are authenticating
 - *User Agent Volume Report*—useful for resolving failed authentications
- Column data in detail reports for hybrid data varies from on-premises data
 - **Source IP**
 - Identifies the external IP, of on-site (Filtered Location) and off-site users
 - **Source Server**
 - Identifies the hybrid Data Center



Investigative Reports

User by Day/Month | Standard Reports | Favorite Reports

View: Anonymous | Outliers | Pie Chart | Full Screen

Internet Use by: Source IP

Database: 10.212.5.212 \wsllogdb70 | Search for: URL Hostname | View from: 2013-08-28

View: All | Select top 5 | by Risk Class | and | Display 5 | Results

Source IP	Hits
204.15.64.97	40,068
10.212.11.165	3,081
204.15.64.98	3,056
204.15.64.69	1,804
204.15.64.72	519
10.212.11.166	53
10.212.9.213	36

Total: 48,617

- Risk Class
- Category
- URL Hostname
- Domain
- Group
- User
- Day
- Protocol Group
- Directory Object
- Action
- Protocol
- Source Server
- Source IP
- Destination IP
- Port

- [Deploying hybrid Web Security components](#)
- [Best practices suggestions for configuring hybrid](#)
- [How do I synchronize user and group data with the hybrid service?](#)
- [How to debug the Hybrid Sync Service](#)
- [How to test for latency when using Cloud Web or Hybrid services](#)
- [Define custom authentication settings](#)
- [Identification of hybrid filtering users](#)
- [Interoperability issues](#) (list of sixteen various hybrid related issues)
- [Prior Hybrid webcasts](#) (September and October 2013)
- [Configure how data is gathered for the hybrid service](#)
- [Adding and editing directory contexts](#)

- Websense training partners can offer classes online and on-site at your location.
- To find authorized training partners offering classes in your area:
 - www.websense.com/findaclass
- For additional training information:
 - readiness@websense.com
- To suggest a future Webinar topic:
 - eSupport@websense.com

Websense Customer Training

Designed for:

- ▶ System administrators
- ▶ Network engineers
- ▶ Other members of your organization as appropriate

Training locations:

All training is conducted at Authorized Training Centers (ATCs). Each ATC has information on costs, course schedules, and types of classes (in-person, virtual, or computer-based).