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

Presenter

Greg Didier

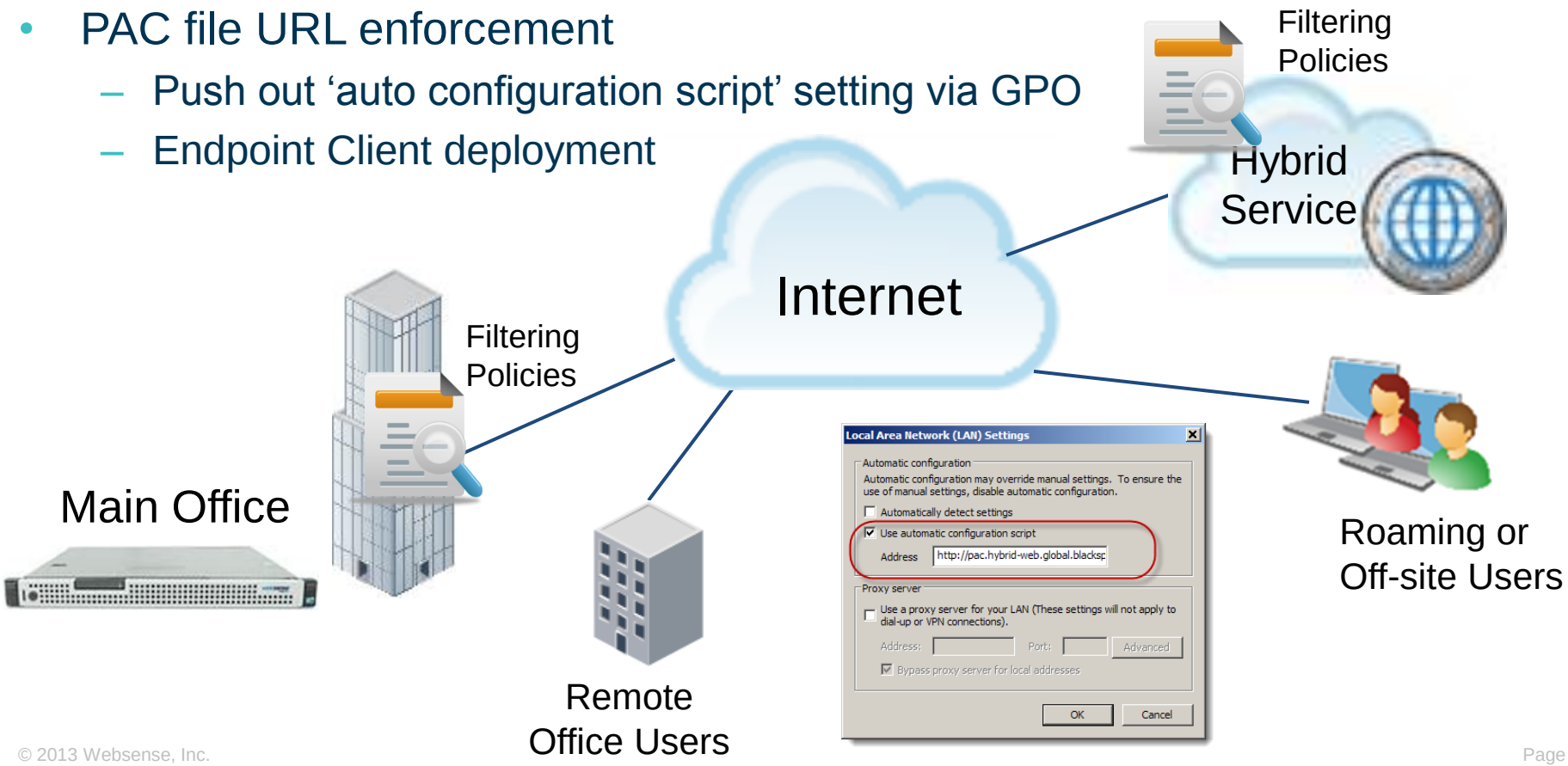
- Title:
  - Technical Trainer eSupport
- Accomplishments:
  - 10 years supporting Websense products
- Qualifications:
  - Technical Support mentor
  - Product trainer
  - Knowledge base writer

Objectives

- 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



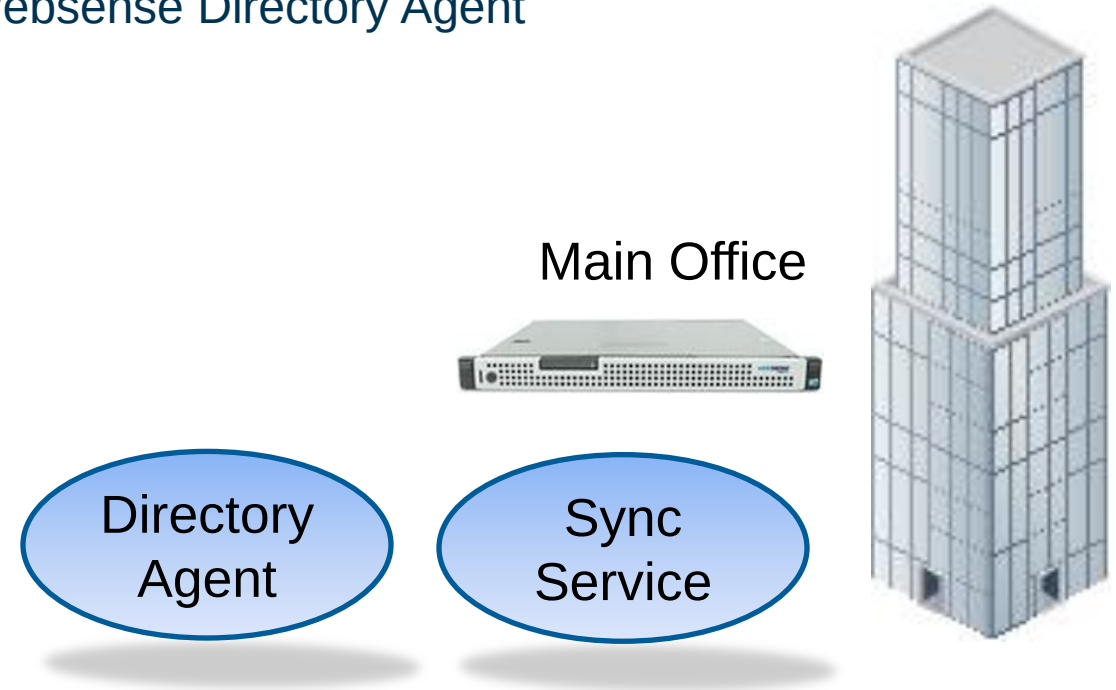
Hybrid Service Versus On-premises Filtering

- 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

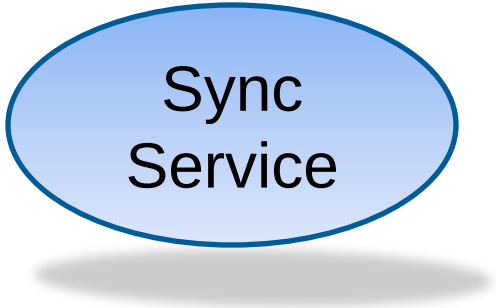
Hybrid Components

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



Websense Sync Service

- 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)



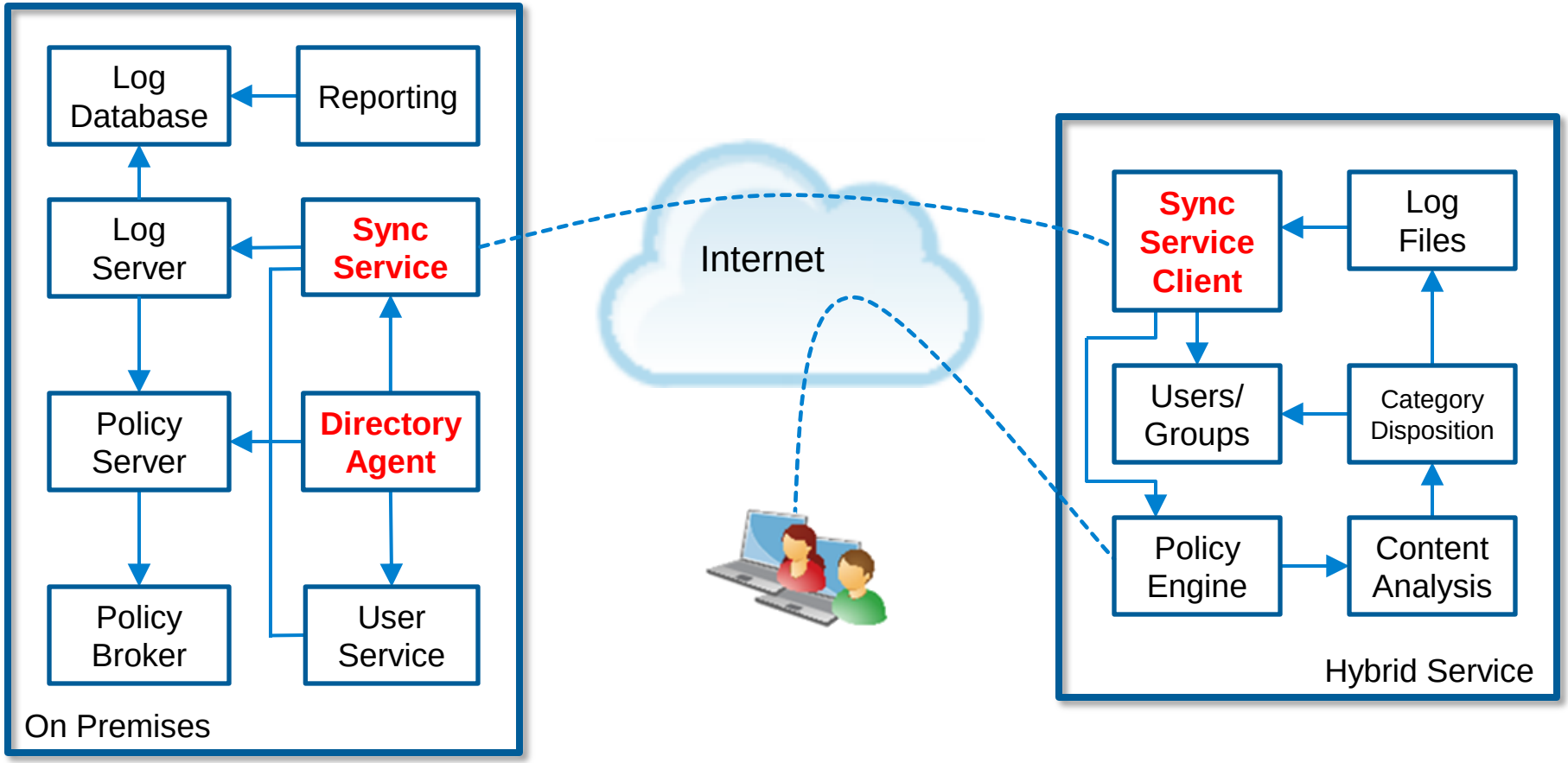
Websense Directory Agent

- 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

Websense 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

Websense Sync Service



Working With Hybrid Filtering Clients

- 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)

Hybrid Service Filtering Order

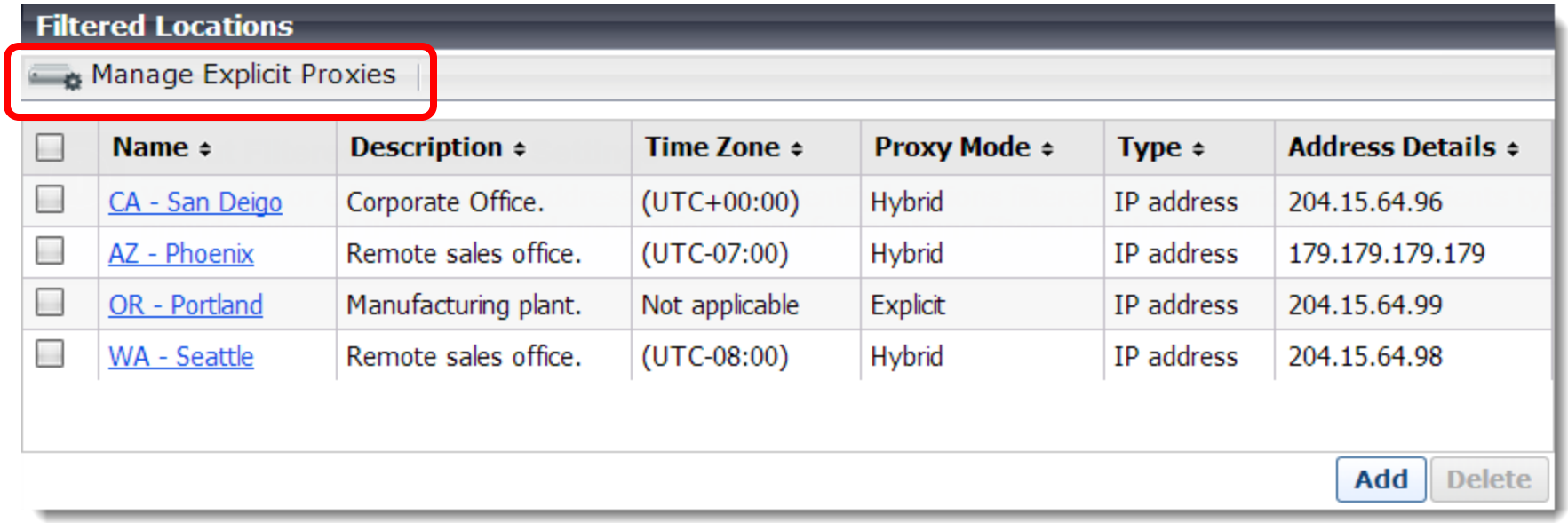
- For each request that the hybrid service receives:
  1. Verify subscription compliance (clients not exceeded)
  2. Determine which **exception** or **policy** applies (in the following order):
     a. **User**
     b. **Groups** the user belongs to
     c. The user's **domain** (OU)
     d. **External 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

Getting Started With Hybrid

- Hybrid configuration
  1. Activate your hybrid filtering account
     - **Settings > General > Account** page

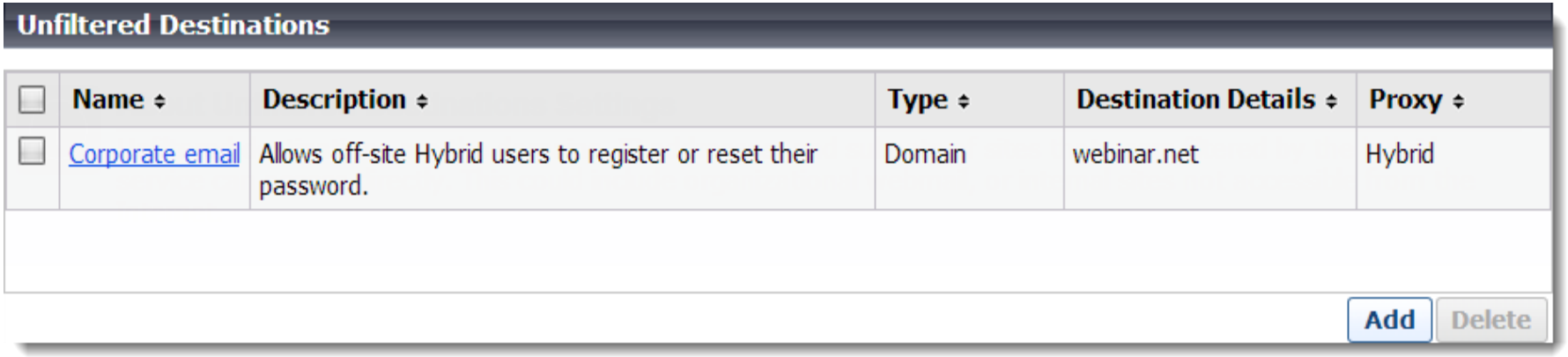
Getting Started With Hybrid

- Hybrid configuration
  2. Define filtered locations
     - **Settings > Hybrid Configuration > Filtered Locations** page



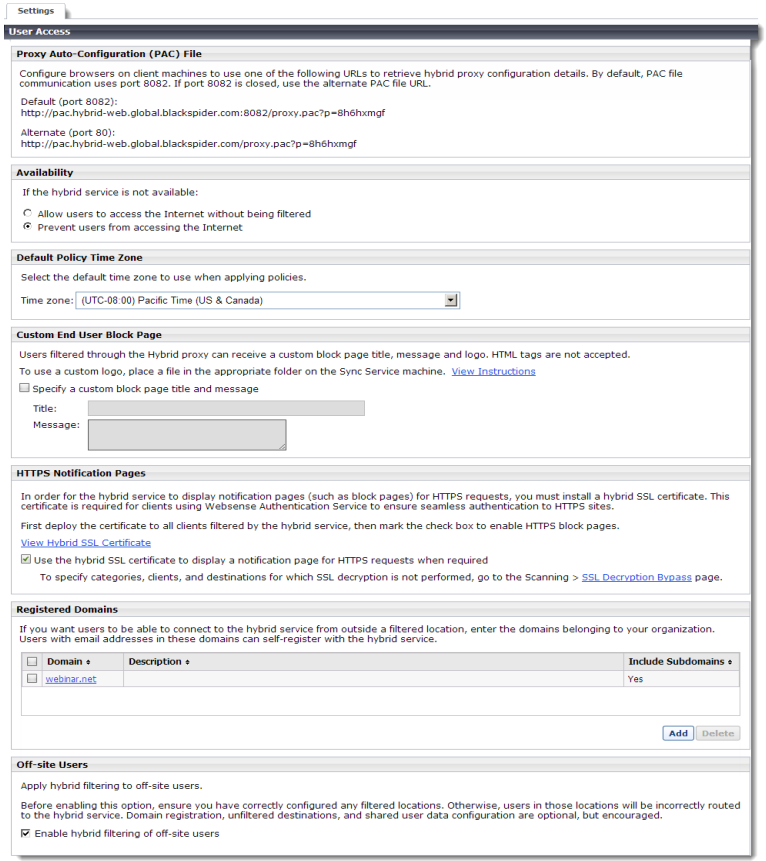
Getting Started With Hybrid

- Hybrid configuration
  3. Specify sites not filtered by hybrid service
     - **Settings > Hybrid Configuration > Unfiltered Destinations** page



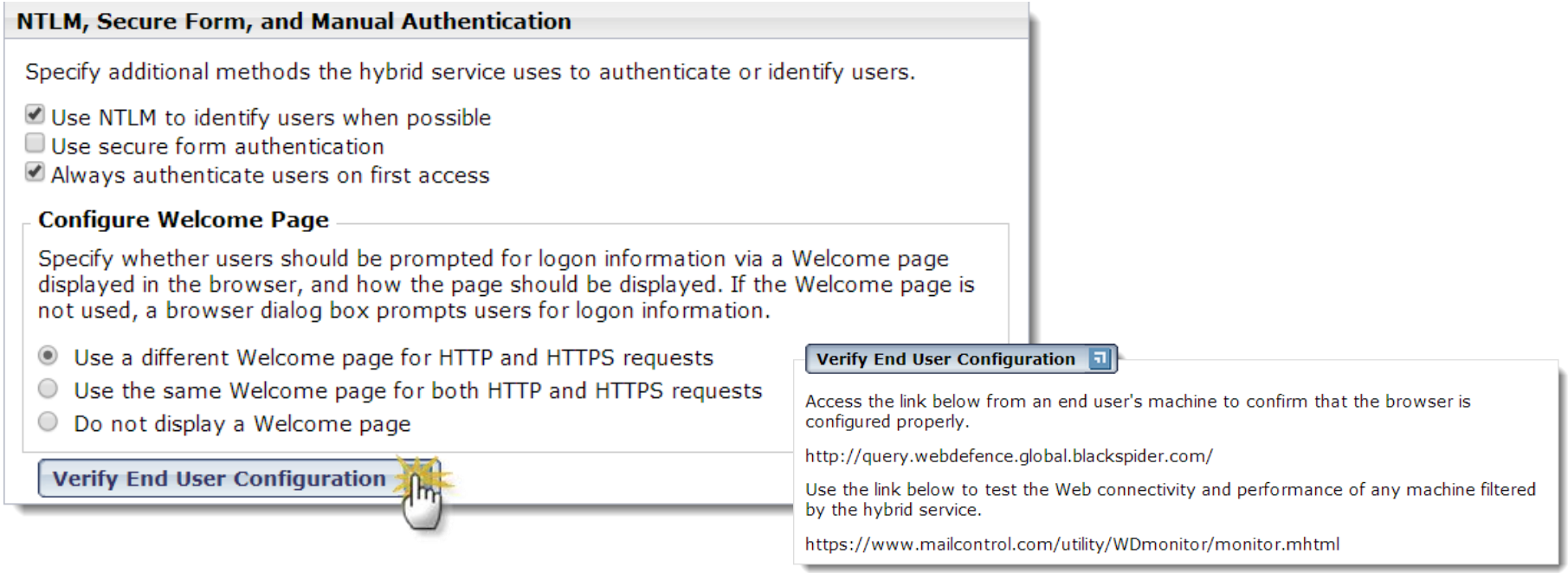
Getting Started With Hybrid

- 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



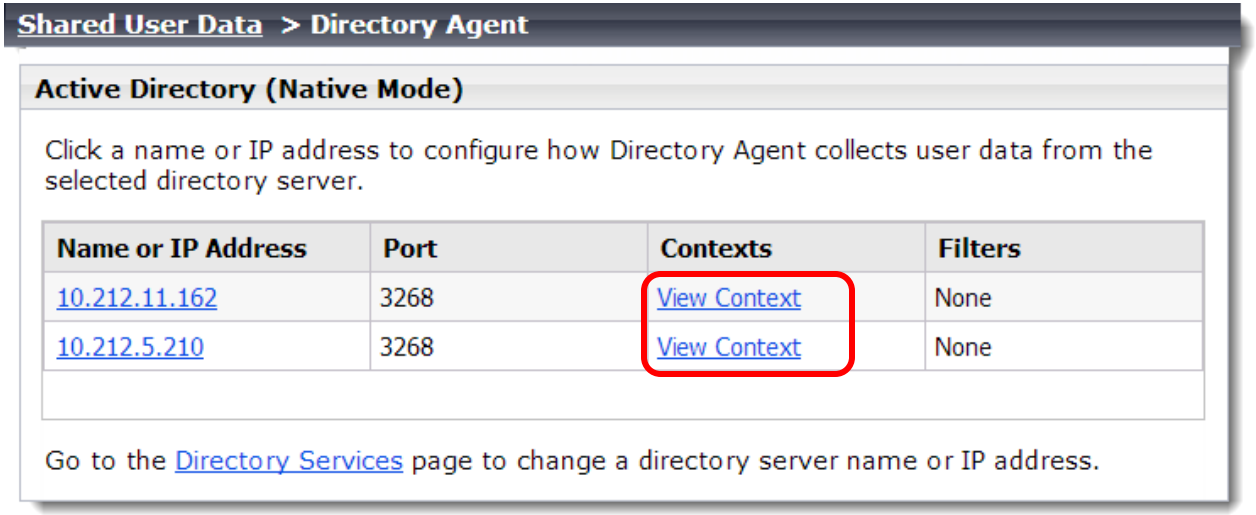
Getting Started With Hybrid

- Hybrid configuration
  5. Identification of hybrid filtering users
     - **Settings > Hybrid Configuration > Hybrid User Identification** page



Getting Started With Hybrid

- 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.

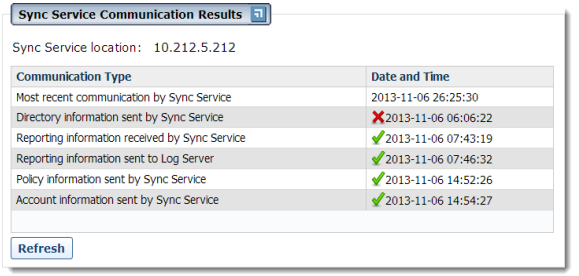


Demonstration - Hybrid User Synchronization

- 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

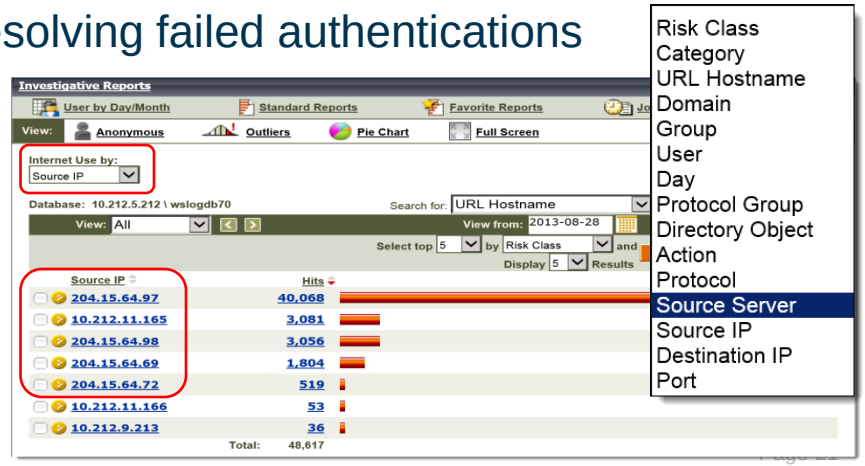
Troubleshooting

- **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



Hybrid Reporting

- 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



Additional Resources

- 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