Quick Start 7: Websense® Cloud Web Security: Troubleshooting and Best Practices

Websense Support Webinar June 2013

TRITON STOPS MORE THREATS. WE CAN PROVE IT.

Presenter

Greg Didier

- Title:
  - Support Specialist
- Accomplishments:
  - 9 years supporting Websense products
- Qualifications:
  - Technical Support Mentor
  - Product Trainer

© 2013 Websense, Inc.

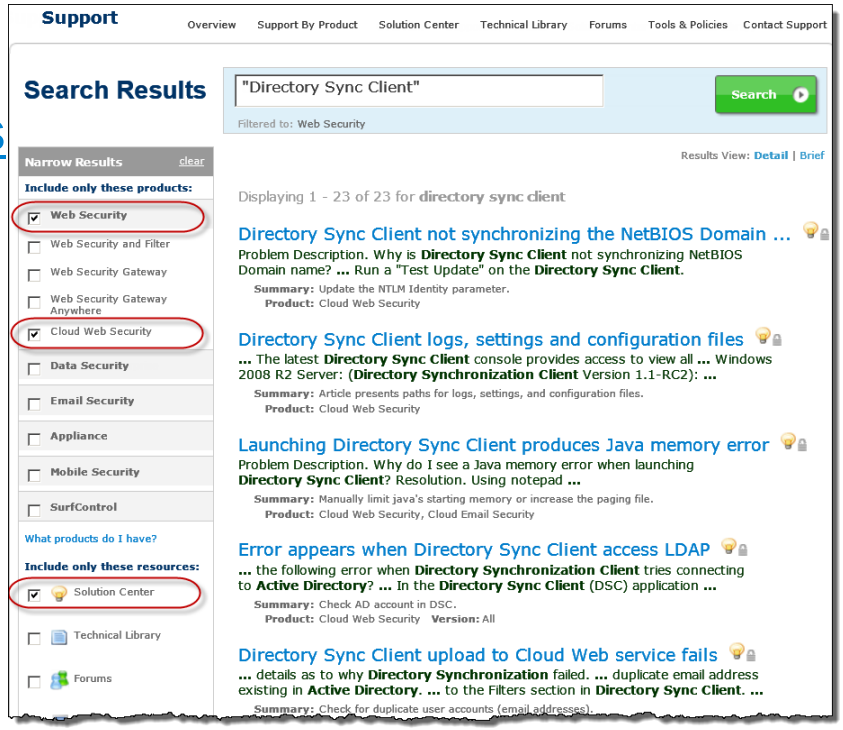
Goals And Objectives

- Troubleshooting procedures and diagnostics
  - Available resources
  - Directory Synchronization
  - Testing for latency
  - Endpoint client
  - Proxied Connections versus Non-Proxied Destinations
  - User authentication
  - Best practices and tips
- Demonstration resolving common filtering issues

© 2013 Websense, Inc.

Technical Support Resources

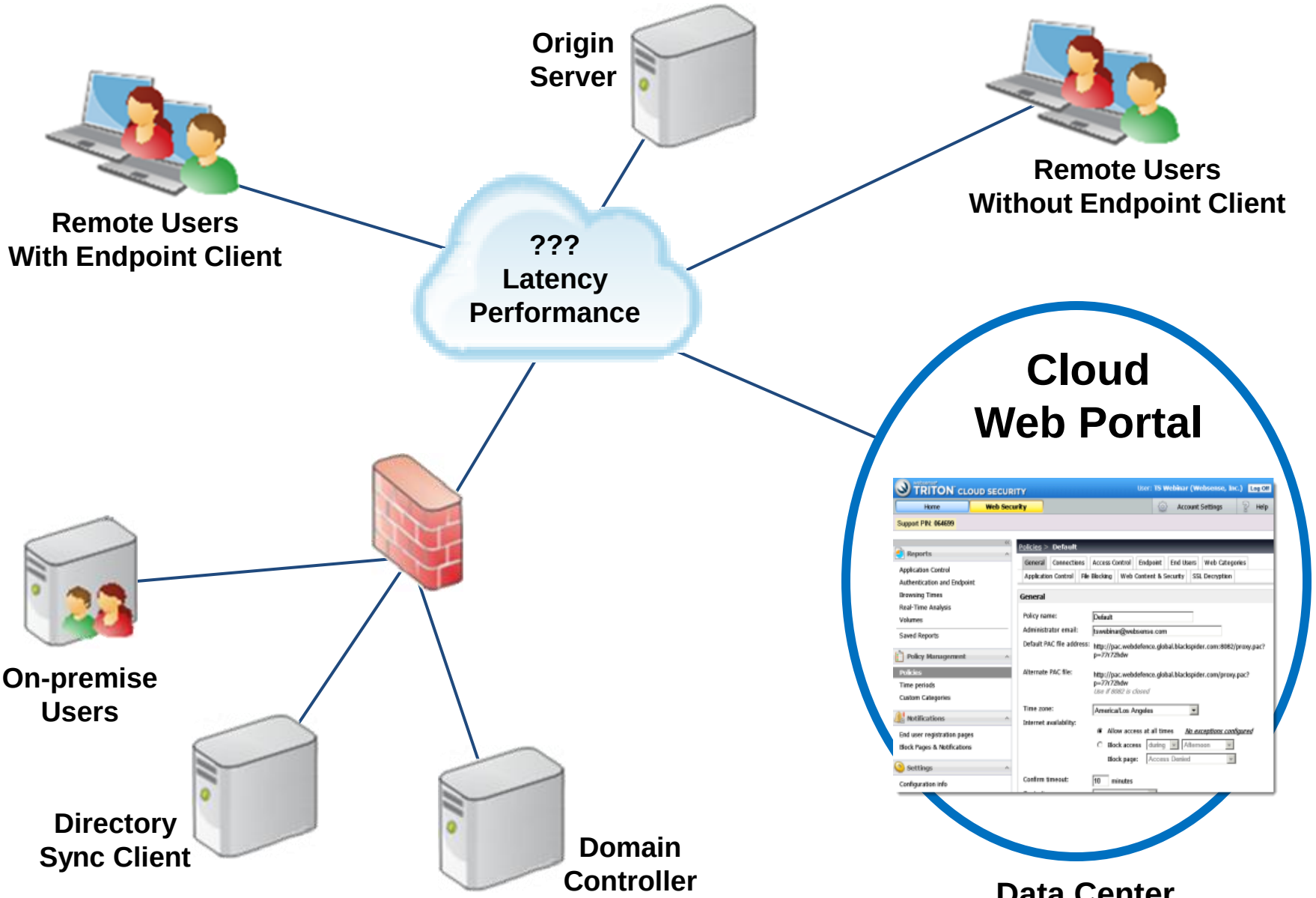
- Websense Technical Support site
  - Knowledge base articles
    - Limit search criteria to Cloud Web service
    - Wildcards versus explicit searching
      - Use quotes for *“exact match”*
  - Websense Technical Library
    - Cloud Web Security documents
- Portal
  - Home > Support > Summary
- Demonstration



© 2013 Websense, Inc.

Troubleshooting And Diagnostic Points

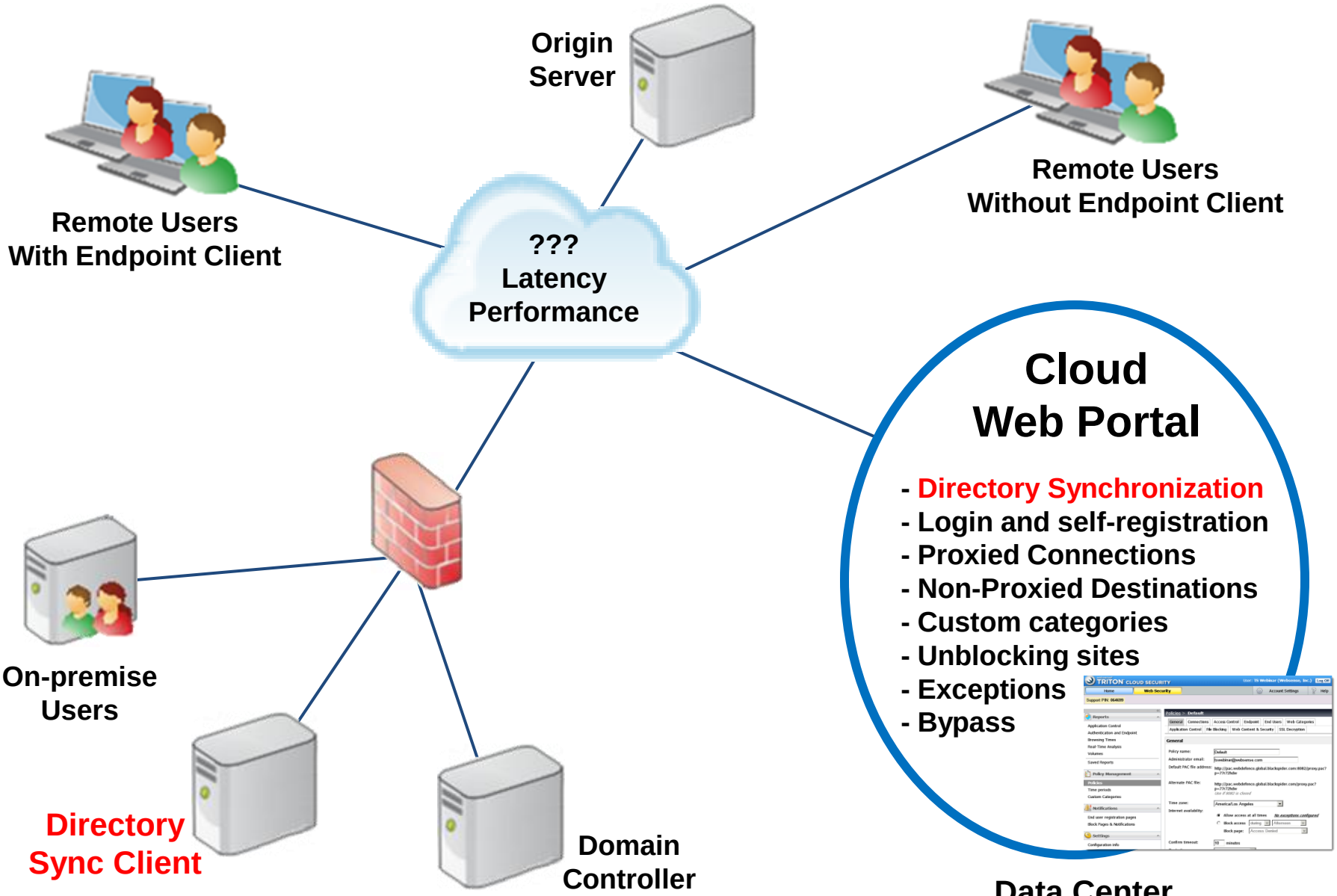
websense



© 2013 Websense, Inc.

Troubleshooting And Diagnostic Points

websense



© 2013 Websense, Inc.

Directory Synchronization

- Cloud Portal
  - Account Settings > Settings > Directory Synchronization
    - Cloud Sync settings
      - To remove objects, disable Synchronization and delete
    - Directory Sync Client application download
    - Directory Sync Client product Admin Guide
    - Synchronization activity details
  - Verify users
    - Account Settings > Settings > End Users > Search
  - Account Settings > Settings > Contacts > serv_acct
    - Directory Sync Client uses this contact to access the portal
    - Logging in to portal forces password expiration. DO NOT LOGIN!
  - Home > Reports > Services
    - Provides Sync *history log* and *time summary* reports
- Demonstration

© 2013 Websense, Inc.

Directory Synchronization

websense

- Directory Sync Client application
  - Buttons
  - Log file viewer
  - Repository, change from portal to local file
    - Repeat steps on *Groups* and *Users* tabs
      - Modify > Data Repository > Type > File > Next > File_Name > Location > Save
  - Directory Referral Checker
    - DSC > View > Directory Referral Checker > Start
  - Configuration file
    - C:\ProgramData\DirSyncClient\configurations\
  - Best practice
    - Configure SMTP to email directory synchronization notifications
    - Schedule directory synchronization twice daily
    - Set Threshold limits
- Demonstration

© 2013 Websense, Inc.

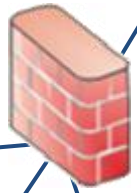
Troubleshooting And Diagnostic Points

websense

Remote Users
With Endpoint Client

Remote Users
Without Endpoint Client

???
Performance
Latency



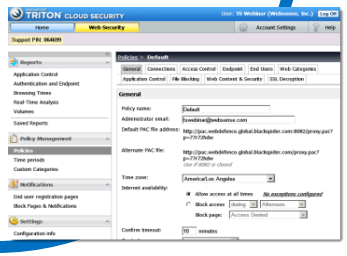
On-premise
Users

Directory
Sync Client

Domain
Controller

Cloud
Web Portal

- Directory Synchronization
- Login and self-registration
- Proxied Connections
- Non-Proxied Destinations
- Custom categories
- Unblocking sites
- Exceptions
- Bypass



Data Center

© 2013 Websense, Inc.

Performance And Latency

- Portal
  - Cloud Web Security monitoring tool
    - Web Security > Settings > Configuration Info
  - Report
    - Web Security > Reports > Volumes > Show > Web Performance - Detailed web response time data
- End user tests
  - Test for latency when using Cloud Web or Hybrid service
    - nslookup -query=TXT …
      - Geo IP Services and Websense Data Center IP addresses
    - tracert
    - ping
- Demonstration

© 2013 Websense, Inc.

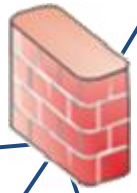
Troubleshooting And Diagnostic Points

websense

Remote Users
With Endpoint Client

Remote Users
Without Endpoint Client

???
Performance
Latency



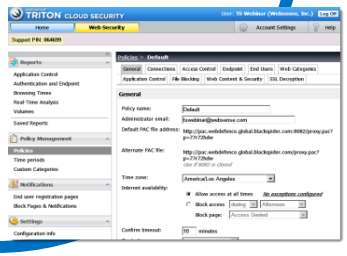
On-premise
Users

Directory
Sync Client

Domain
Controller

Cloud
Web Portal

- Directory Synchronization
- Login and self-registration
- Proxied Connections
- Non-Proxied Destinations
- Custom categories
- Unblocking sites
- Exceptions
- Bypass



Data Center

© 2013 Websense, Inc.

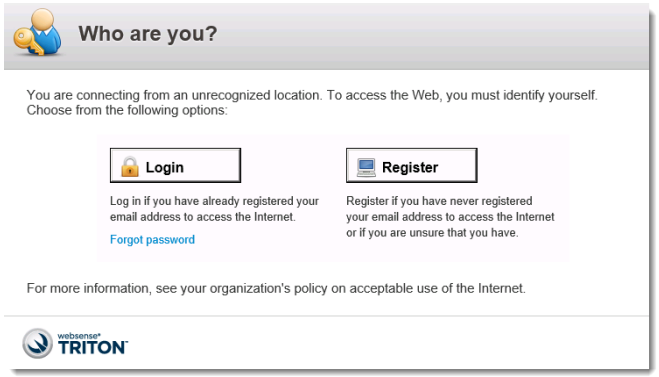
Endpoint Client

- Portal
  - Endpoint installer, use the latest build
    - Test, by pushing out new build with a temporary policy
    - NOTE: Firefox updates often, endpoint may not support latest release
  - Forgotten password
    - Reset anti-tampering password, endpoint clients update automatically
  - Reports
    - Web Security > Reports > Authentication and Endpoint
- Endpoint client
  - Verify installation registry key
  - Debug options
    - Websense\Websense Endpoint\ClientInfo.exe
    - Packet capture - Wireshark
  - Stop Web endpoint: *wepsvc -stop -password <password> wspxy*
- Demonstration

© 2013 Websense, Inc.

Endpoint Client

- Roaming users with endpoint client
  - Synchronized users using domain login are not prompted
    - Provides true transparent identification
  - Endpoint installed, but users still receive login request
    - User not synchronized
    - User logs in locally
    - Incorrect or no WSCONTEXT
      - Login failure
  - Avoid endpoint login request
    - Synchronize users with Cloud service
      - Directory Sync Client works perfectly for this
    - Users do not authenticate, they login with cached credentials
- Roaming users without endpoint client
  - Always prompted for login credentials



© 2013 Websense, Inc.

Troubleshooting And Diagnostic Points

websense

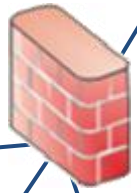
Unknown Site

Remote Users With Endpoint Client

Unknown Site

Remote Users Without Endpoint Client

??? Performance Latency



Known Site IP Address

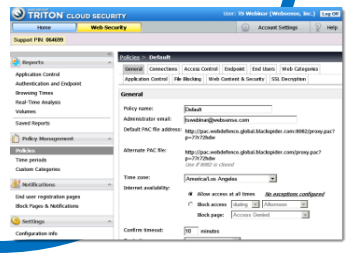
On-premise Users

Directory Sync Client

Domain Controller

Cloud Web Portal

- Directory Synchronization
- Login and self-registration
- Proxied Connections
- Non-Proxied Destinations
- Custom categories
- Unblocking sites
- Exceptions
- Bypass



Data Center

© 2013 Websense, Inc.

Connections

- Policy has defined Proxied Connections
  - Your external firewall IP address
  - A policy can have one or more Proxied Connections
  - A Proxied Connection can exist in only one policy
  - The Proxied Connection determines the applied policy
  - Transparent identification
    - End user's browser replies to 407 request with credentials
- Policy has NO defined Proxied Connections
  - All users are treated as remote users and must log in
  - The policy is determined by the user's email domain
- Non-Proxied Destinations
  - Destinations are added to your organization's PAC file
  - Can be a domain name, IP address or IP subnet
  - Avoids connecting to Cloud proxy service for certain sites

© 2013 Websense, Inc.

Filtering Order

- Filtering order for Standard or Custom **Web categories**:
  1. Security category blocking
  2. Application control blocking, File extension blocking, File type blocking, File Size blocking
  3. Allow access
  4. Require user authentication
  5. Confirm
  6. Quota
  7. Block access
  8. Do not block
- When per-time, per-user, or per-group **exceptions** exist:
  1. Per-time
  2. Per-user
  3. Per-group
  4. Default

© 2013 Websense, Inc.

Filtering

- Custom categories
  - Created at the account level—apply to all policies
- Exceptions apply to per-time, per-user, or per-group
  - Requires user authentication
  - Allow exception overrides only the Block action on URL categories, does not bypass authentication and antivirus
- Separate entries by commas
  - multiple email addresses, domains or user names
- Demonstration
  - Exceptions
  - Custom categories
  - Bypass for authentication, endpoint and certificates

© 2013 Websense, Inc.

Additional Resources

- Articles:
  - Directory Sync Client logs, settings and configuration files
  - Filtering actions and Filtering action order
  - Proxied Connections and Non-Proxied Destinations
  - Cloud service Data Center (cluster) IP addresses and port numbers
  - How can I deploy Web Endpoint?
  - How do I uninstall the Web Endpoint?
  - Verify using Cloud proxy and determine active policy
    - How do I query Cloud service for hidden connection info?
- Past Webinars:
  - May 2013: Administering the Cloud Web Security Solution
  - April 2013: Introducing and configuring Cloud Web Security solution

© 2013 Websense, Inc.

Upcoming Webinar

websense

Webinar Update

A note to our customers,

Our Technical Support site is undergoing a number of updates. We want to provide our customers with a wider range of topics and product groups.

Websense Technical Support will re-launch the support webinars in September 2013. Stay tuned for some great changes!

Your feedback helps us refine and improve our ongoing webinar series. If you have any questions or suggestions, please email the webinar team at esupport@websense.com.

Thank you,

© 2013 Websense, Inc.

Training

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

© 2013 Websense, Inc.