Identifying Users with Logon Agent: Implementation and Troubleshooting

Websense Support Webinar May 2012

TRITON™

- Web security
- Email security
- Data security
- Mobile security

Webinar Presenter

Greg Didier

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

Goals And Objectives

- How Logon Agent works
- Deployment considerations
- Configuring the logon and logoff scripts
- Script parameters
- Troubleshooting
- Demonstrations
- Best practices

Why Use Logon Agent?

- Logon Agent provides user names to Filtering Service
  - Allows filtering by users and groups-based directory objects
- Logon Agent
  - Identifies users transparently
  - Works in Active Directory environments
  - Maximizes accuracy
  - Real time identification
    - Identifies users as they log “on” to the domain
    - Identifies users as they log “off” to the domain (optional)
  - Monitor IP address changes for wireless users (optional)

Deployment Considerations

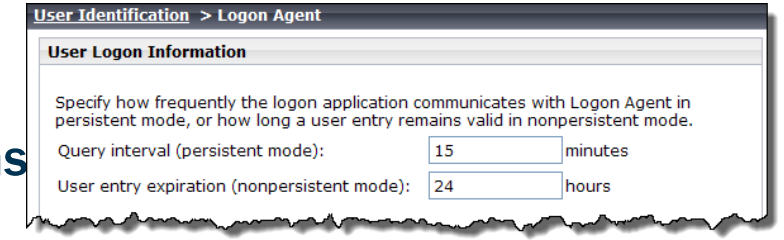
- Websense transparent identification agents:
  - Logon Agent, DC Agent, RADIUS Agent, eDirectory Agent
- Logon Agent may be used in conjunction with:
  - DC Agent and RADIUS Agent
  - Logon Agent takes precedence over names submitted by DC Agent
- Logon Agent may “not” be used in conjunction with:
  - eDirectory Agent
- Deploying multiple Logon Agents
  - Best practice in med-large networks
  - Must be installed on separate servers

Components

- **Logon script**
  - Enforced via Group Policy Object (GPO)
  - Invokes the Logon Application
  - Specifies the Logon Agent's location
- **Logon Agent**
  - Receives user names from multiple Logon Applications
  - Builds a *user-name-map* of authenticated users
  - Sends user names to Filtering Service
  - Runs on Windows or Linux servers

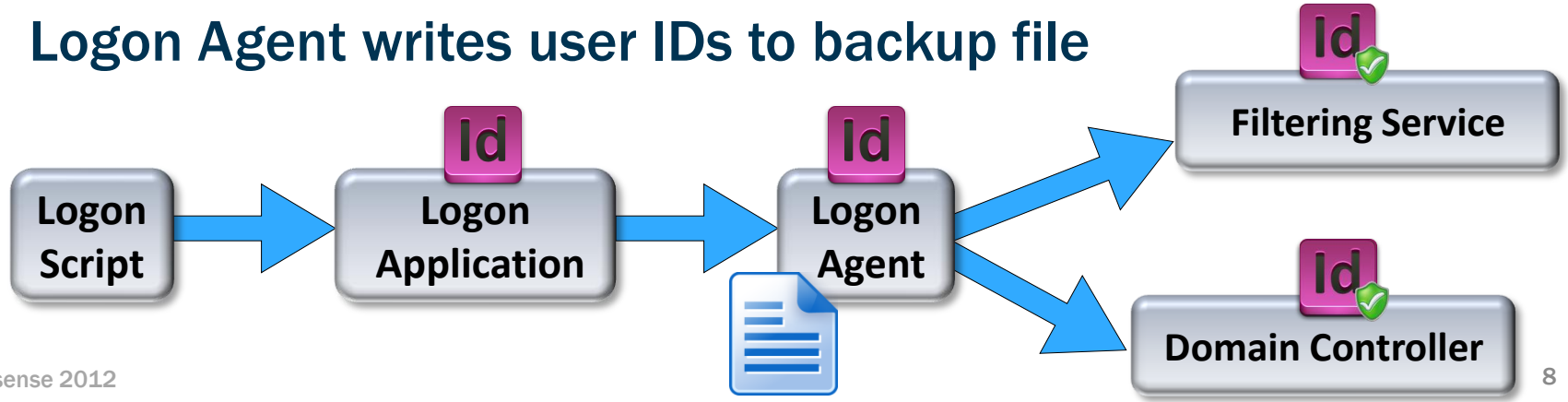
Components

- **Logon Application**
  - Sends user logon information to Logon Agent
  - Activated via a logon script
  - Activated via a logoff script (optional)
  - Runs only on Windows operating systems
  - **Persistent mode** (default)
    - Sends logon information to Logon Agent at specific intervals
      - Configured via “Query Interval” setting in TRITON - Web Security
  - **Nonpersistent mode** (optional)
    - Sends logon information to Logon Agent once, “only” at logon
      - “User Entry Expiration” interval setting in TRITON - Web Security determines the user names are removed



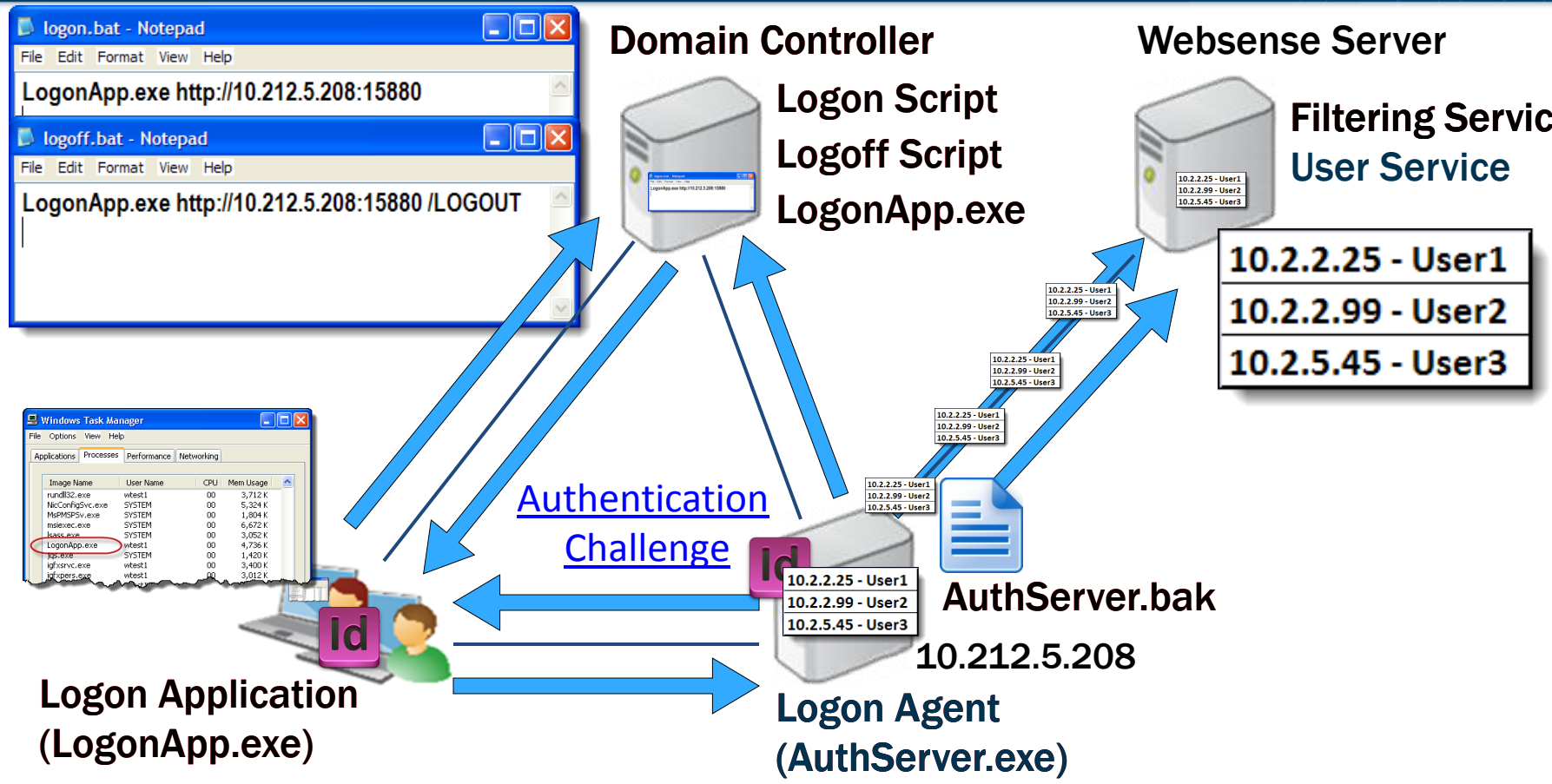
User Identification Process: Overview

1. A logon script invokes the Logon Application
2. Logon Application acquires the user ID
3. Logon Application sends user ID to Logon Agent
4. Logon Agent verifies credentials with Doman Controller
5. Logon Agent sends verified user IDs to Filtering Service
6. Logon Agent writes user IDs to backup file



User Identification Process: Detailed View

websense



Recap: Components

- **Logon Agent**
  - Authentication Server (service name)
  - AuthServer.exe (executable name)
  - \Program Files\Websense\Web Security\bin\
- **Logon Application**
  - LogonApp.exe (client side executable/process name)
- **Logon script**
  - Enforced via GPO
- **AuthServer.bak**
  - Logon Agent's backup file containing the entire user name map
  - \Program Files\Websense\Web Security\bin\
- **Websense User Service**
  - Provides discovery of domain controllers

Creating The Scripts

- Logon script syntax:
  - `LogonApp.exe http://<server>:<port> [/parameter]`

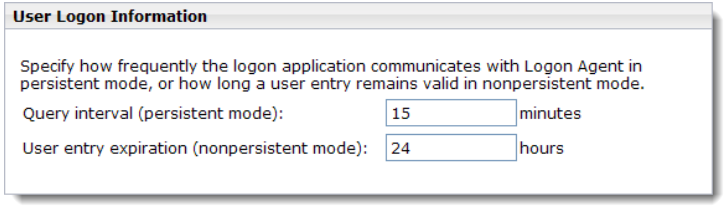
The Logon Agent script is very simple. It can be added to any existing GPO that you may already have established within your existing network environment.

Creating The Scripts

- Logon script syntax:
  - `LogonApp.exe http://<server>:<port> [/parameter]`
    - <server>
      - IP address or hostname of the machine running Logon Agent service
      - Best practice: Use an IP address
    - <port>
      - The port number used by Logon Agent (default 15880)
  - NOTE: Ensure a space character precedes the parameter
- Where will the LogonApp executable be hosted?
  - Hosted with the script file:
    - `LogonApp.exe http://x.x.x.x:15880`
  - Not host with the script file:
    - `\\<IP_address>\<folder>\LogonApp.exe http://x.x.x.x:15880`

Creating The Script

- Persistent mode?
  - `LogonApp.exe http://x.x.x.x:15880`
  - "Query Interval" setting
- Nonpersistent mode?
  - `LogonApp.exe http://x.x.x.x:15880 /NOPERSIST`
  - "User Entry Expiration" setting
- Do you have mobile users?
  - `LogonApp.exe http://x.x.x.x:15880 /DHCP`
- Remove user names?
  - `LogonApp.exe http://x.x.x.x:15880 /LOGOUT`



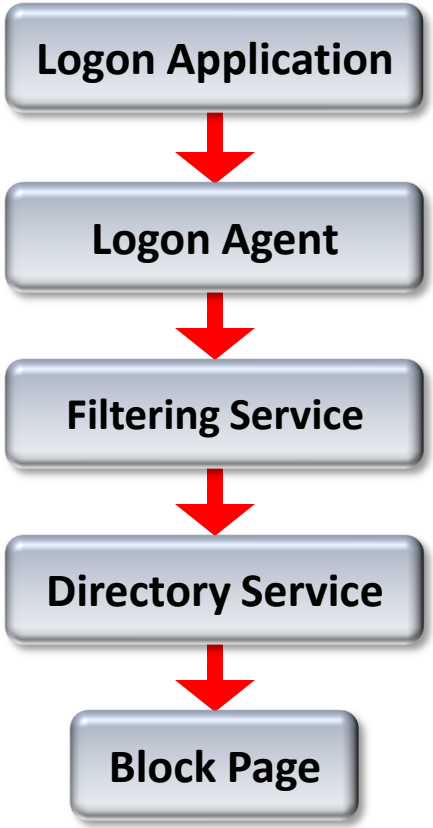
Demonstration: Implementing Logon Agent

websense

- Scenario:
  - Run Logon Application (LogonApp.exe) continuously
  - Copy LogonApp.exe to client machines
  - Watch for IP address changes for wireless users
  - Remove user names when logging off the domain
- **Task 1:** Prepare the scripts
- **Task 2:** Configure the scripts to run
- **Task 3:** Configure Logon Agent in TRITON - Web Security
- Host Logon Application on a shared folder
- Demonstration

Troubleshooting Logon Agent

- Filtering polices are not applying as expected
- Troubleshooting steps:
  - Is Logon Application running
  - Pull Logon Agent user ID map
    - Tracing and debugging
  - Pull Filtering Service user ID map
  - Check Directory Service settings
    - TRITON –Web Security
  - Check block page hidden information
- Follow the traffic slow…



Demonstration

websense

- Testing—are user names seen?
  - Logon Agent user map
    - `ConsoleClient <Logon Agent IP> 30603`
  - Filtering Service user map
    - `ConsoleClient <Filtering Service IP> 15869`
  - TestLogServer utility
    - `TestLogServer –file log.txt`
    - No user names indicates a User Service / Directory Service issue
  - Investigative Reports should show user names
  - Block page
    - Check the hidden view source information

Troubleshooting Logon Application

- Optional logon script parameters:
  - /VERBOSE
    - Debugging parameter
      - Writes messages to a DOS window when errors occur
  - /COPY
    - Copies LogonApp.exe to client machine and then runs locally
      - *\Documents and Settings\<user_account>\Local Settings\Temp*
      - Helpful if a DOS window remains open after logon
      - Can only be used in persistent mode
  - /LEGACY
    - Use the latest Logon Application release without upgrading Websense
      - Allows v7.6 LogonApp.exe instances to communicate with Logon Agent versions 7.5 and earlier

Troubleshooting Logon Application

- Optional logon script parameters (continued):
  - /T
    - Enables tracing of information sent to Logon Agent
    - The “logon_app_trace.txt” file is created in the root (C:\) directory
  - /D
    - Sends messages to the “Ws_LogonAppLog.txt” debug file located in the current user’s default “temp” directory
      - *\Documents and Settings\<user_account>\Local Settings\Temp*

Troubleshooting Logon Application

websense

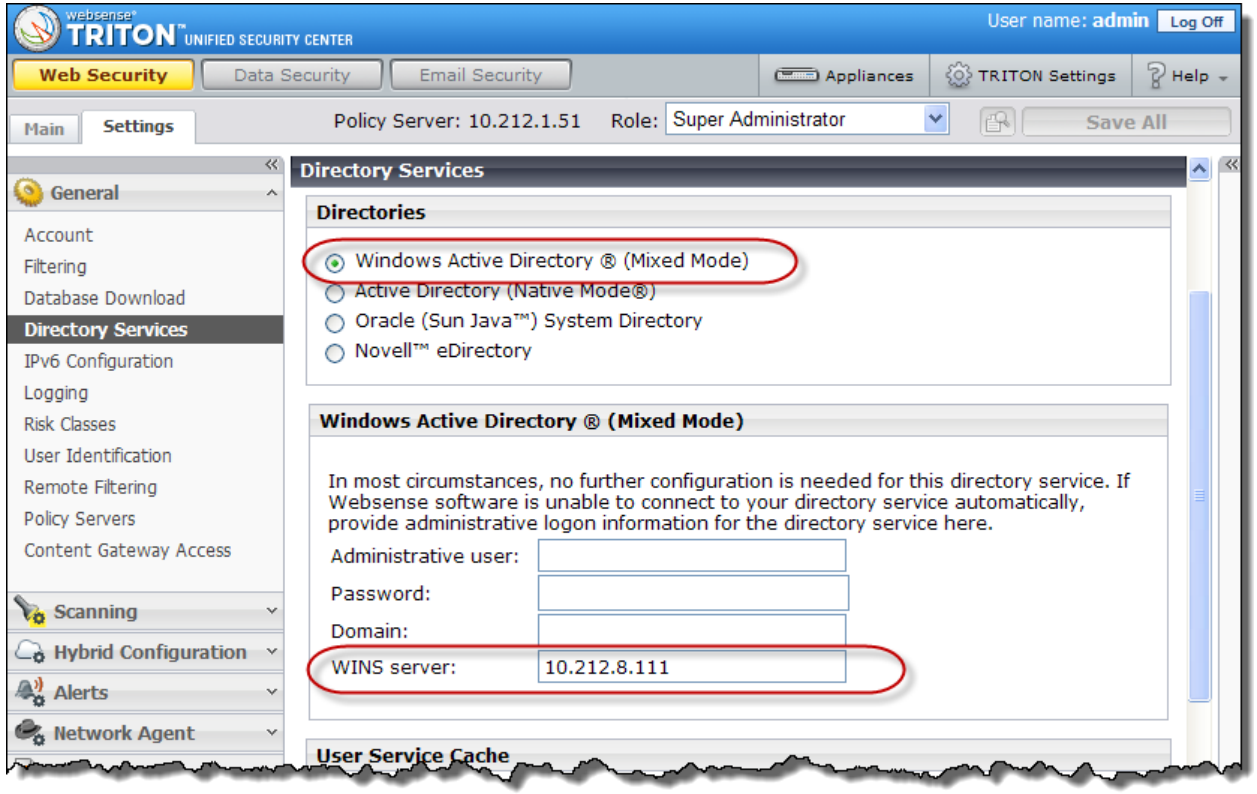
- Verify the script deployed Logon Application
  - Task Manager displays LogonApp.exe process (persist mode)
- All clients must be able to connect to shared resources
  - Client must connect to the shared drive hosting the logon script
    - `net view /domain:<domain name>`
  - Client must connect to the shared drive hosting LogonApp.exe
    - `\\<server_name>\<folder>`
- Script must include a hard return
- A space must precede script parameters
- Manually run logon script and LogonApp on client machine

Troubleshooting Logon Application

- Corrupt user profile on the client machine
  - Logon script that invokes LogonApp.exe does not run properly
- 401 error “during final handshake”
  - Could indicate Logon Agent cannot communicate with domain controller to verify user credentials
- Verify Group Policy Objects are applied to users
- TIP: To determine if your script is running as intended, configure manual authentication.
  - If transparent authentication with Logon Agent fails for any reason, users are prompted for a user name and password when opening a browser. Ask your users to notify you if this problem occurs.

Troubleshooting Logon Agent

- On V-Series appliance and Linux servers, indentify WINS



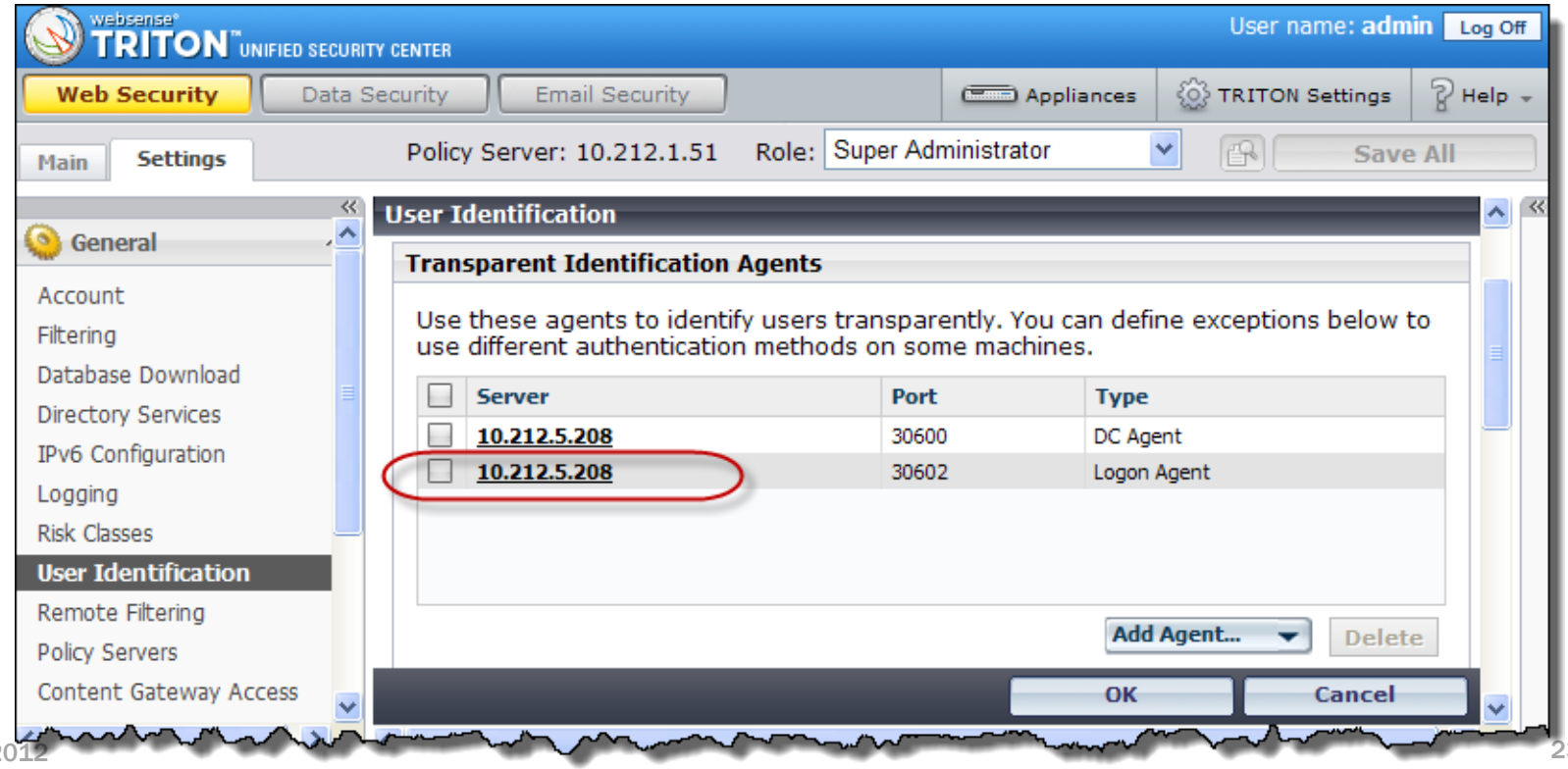
Troubleshooting Logon Agent

websense

- On V-Series appliance and Linux servers, indentify WINS
- Ensure the Logon Agent service is running
- NetBIOS for TCP/IP must be enabled
  - If disabled, LogonApp.exe may not run and Logon Agent may not communicate with domain controllers
- TCP/IP NetBIOS Helper service must be running clients
  - If not running, LogonApp.exe cannot deploy
- Clocks/time must be correct on all machines
- Run packet capture using Wireshark
- Run Logon Agent service using a service account with domain admin privileges

Troubleshooting Filtering Service

- Identify Logon Agent as an IP addresses, not a hostname



Troubleshooting Filtering Service

- Identify Logon Agent as an IP addresses, not a hostname
- As configured in TRITON - Web Security, can Filtering Service connect to Logon Agent via its communication port
  - Logon Agent default communication port is 30602
    - `telnet <Logon_Agent_IP> 30602`

Troubleshooting User Service

- If Logon Agent and Filtering Service user maps are correct, but the user remains unidentified, it may be a User Service problem
  - Verify Directory Service settings
    - Are you able to add clients in TRITON - Web Security manager?
  - Verify the User Service is running and restarts successfully
  - Verify User service can resolve WINS
    - Article: LogonApp cannot reach the AuthServer in the final attempt
  - Run a trace to debug Websense User Service (advanced troubleshooting)
    - How do I enable DSTrace for User Service?
    - Look for specific users names in the trace logging file

Additional Information: NTLM

- Client machines must use NTLM (v1 or v2) when authenticating users; however, when a Windows Server 2008 domain controller exists, client machines must NTLMv1 only
  - This can be done individual on each client machine by modifying the local security policy or on all machines in a domain by modifying the security policy of a Group Policy Object
  - For instructions, see Creating and running the script for Logon Agent
- How to check the NTLM version for Logon Agent compatibility?

Additional Information

- Transparent Identification of Users (white paper)
  - Web document or PDF
- Creating and running the script for Logon Agent
- Configuring Logon Agent for roaming users
- Troubleshooting Transparent Identification Agents with ConsoleClient
- How to debug the Websense LogonApp.exe
- How to run a debug trace on Websense Logon Agent
- Where can I find information about why Filtering Service is blocking a page?

Webinar Announcement

websense

Webinar Update

Title: **Introducing Websense Web Security version 7.7**

Date: **June 27th, 2012**

Time: **8:30 A.M. PDT (GMT -8)**

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 offer classes online and onsite at your location.
- For more information, please send email to: readiness@websense.com