Troubleshooting Transparent Identification Agents for Websense Web Security

Websense Support Webinar November 2010

Support Webinars

web security | data security | email security

Goals and Objectives

- What is a transparent identification agent?
- Deploying and combining transparent identification agents
- DC Agent troubleshooting
- Logon Agent troubleshooting
- RADIUS Agent troubleshooting
- eDirectory Agent troubleshooting

Transparent Identification Agents

websense
ESSENTIAL INFORMATION PROTECTION™

- What is a Transparent Identification Agent?
  - Used to transparently find user information
  - Maps an IP address to a Username for use by the Websense Filtering Service
  - Username information passed to User service when required to find group and OU membership for use with filtering policies.

Transparent Identification Agents

websense
ESSENTIAL INFORMATION PROTECTION™

- Websense Web Security includes 4 transparent identification agents:
  - **DC Agent** communicates with a Windows-based directory service. Can be installed on a Windows server in any domain.
  - **Logon Agent** communicates with a Windows-based directory service. Requires a logon application to be installed on client machines.
  - **RADIUS Agent** can be used with any supported directory service. Requires a RADIUS client and RADIUS server to identify remote users.
  - **eDirectory Agent** communicates with Novell eDirectory.
- Agents can be used individually, or in combination.

DC Agent

- Can work with Logon Agent and RADIUS Agent
  - On the same machine or in the same network
- If using multiple instances of DC Agent, install each instance on a separate machine.
- All instances of DC Agent must be able to communicate with Filtering Service.
- Cannot work with eDirectory Agent, either on the same machine or in the same network

Logon Agent

- Can work with DC Agent and RADIUS Agent
  - On the same machine or in the same network
- If using multiple Logon Agent instances, each instance must be installed on a separate machine.
- Cannot work with eDirectory Agent, either on the same machine or in the same network

RADIUS and eDirectory Agents

websense
ESSENTIAL INFORMATION PROTECTION™

- RADIUS Agent can work with any other transparent identification agent
  - On the same machine or in the same network
- eDirectory Agent can work only with RADIUS Agent.

DC Agent Troubleshooting

- The incorrect policy is being applied to users.
  - DC Agent could not identify a user.
  - A user is incorrectly associated with a particular IP address.
- Troubleshooting steps:
  - Make sure that DC Agent is running with an account that has access to poll domain controllers for user information.
  - Run **testlogserver** to see if user information is missing from filtering requests.
    - See www.websense.com/content/support/library/web/v75/ws_utilities/tl_75_testlogsvr.aspx.

DC Agent Troubleshooting

websense
ESSENTIAL INFORMATION PROTECTION™

- Troubleshooting steps (continued):
  - Run **ConsoleClient** on diagnostic port **30601**.
    - See websense.com/content/support/library/web/v75/ws_utilities/tl_75_consoleclient.aspx.
    - Use the **printself** option to review the user name map.
    - Check for user entries that don't have a corresponding IP address.
    - Check for blank user names.
    - If the user map is correct, but the user is not identified, there may be a User Service problem, or a communication issue between DC Agent and Filtering Service.
      - Enable directory service tracing (**dstrace**) to troubleshoot problems related to User Service.

DC Agent Troubleshooting

- Troubleshooting steps (continued):
  - Check the **websense.log** file and the Windows Event Viewer for errors.
  - Check the **dc_config.txt** file to make sure that all relevant domain controllers are listed, and set to **on**.

    ```
    [SANDIEGO]
    AD-SD=on
    ```

    If this file is empty, DC Agent does not know which domain controllers to poll.
  - If there is a problem identifying particular user, open a command prompt on the client machine and run the **set L** command to get the logon server name.

DC Agent Troubleshooting

- Troubleshooting steps (continued):
  - Make sure that NetBIOS is enabled between the DC Agent machine and domain controller.
  - Get additional diagnostic data:
    1. Add the following parameters to the **transid.ini** file in the Websense **bin** directory (C:\Program Files\Websense\bin, by default).

       ```
       UseFileTrace=true
       VerifyTracing=true
       ```

    2. Restart the DC Agent service.
    3. An **xid_trace.txt** file will be created with diagnostic information.

Logon Agent Troubleshooting

- If Logon Agent cannot get a user name/IP address pair from a client machine, Websense software does not apply the appropriate user or group policy.
- Troubleshooting steps for the logon application:
  - Verify that the script used to run the logon application (**LogonApp.exe**) is correctly applied.
  - Make sure the user profile on the client machine is not corrupt. A corrupt profile can keep LogonApp.exe from running.
  - Verify that the client machine is connected to the shared drive on the domain controller where LogonApp.exe and the logon script are stored.

Logon Agent Troubleshooting

- Troubleshooting for the logon application (continued):
  - Make sure the TCP/IP NetBIOS Helper service is running on the client machine. This service is required for proper deployment of LogonApp.exe.
  - Add the **/d** parameter to the logon script to print logon application messages to a file specified via the **/filename** switch.

Logon Agent Troubleshooting

- Troubleshooting steps for Logon Agent:
  - Run **ConsoleClient** on diagnostic port **30603**.
    - See websense.com/content/support/library/web/v75/ws_utilities/tl_75_consoleclient.aspx.
    - Use the **printself** option to review the user name map.
    - If the user map is correct, but the user is not identified, there may be a User Service problem, or a communication issue between Logon Agent and Filtering Service.
  - NetBIOS for TCP/IP must be enabled. If NetBIOS is disabled:
    - The logon application (logonapp.exe) may not be able to run
    - Logon Agent may not be able to communicate with domain controllers.

Logon Agent Troubleshooting

- Troubleshooting steps for Logon Agent (continued):
  - Run a packet capture using Wireshark.
  - Check for an **error 401** during final handshake. This could indicate that Logon Agent is not able to communicate with domain controller to verify user credentials.

RADIUS Agent Troubleshooting

- RADIUS Agent acts as a proxy that forwards RADIUS messages between the RADIUS client and server.
- Troubleshooting steps:
  - If remote users are not identified by RADIUS Agent, verify that RADIUS parameters are correctly configured in TRITON - Web Security.
  - Ensure that the communication ports between RADIUS clients and RADIUS Agent and between RADIUS Agent and the RADIUS server are correctly configured on the firewall.
  - Run **testlogserver** to see if user information is missing from filtering requests.
    - See www.websense.com/content/support/library/web/v75/ws_utilities/tl_75_testlogsvr.aspx.

RADIUS Agent Troubleshooting

- Troubleshooting steps (continued):
  - Enable RADIUS Agent diagnostics in the **wsradius.ini** file in the Websense **bin** directory (C:\Program Files\Websense\bin or /opt/Websense/bin, by default).
    1. Set **DebugMode** to **On**.
    2. Set **DebugLevel** to **3** for the highest level of debugging (includes all RADIUS transactions involved in a user logon).
    3. Use the **LogFile** parameter to specify a name for the output file.
  - Run a packet capture on the RADIUS Agent, RADIUS server, and client machines to verify that RADIUS and accounting information is being passed from the agent to the server.

RADIUS Agent Troubleshooting

- Troubleshooting steps (continued):
  - Check the RADIUS server log file to verify that the server is authenticating clients.
  - Ensure that the RADIUS server has the RADIUS Agent machine IP address added as a RADIUS client.
  - Check the RADIUS Agent log file for errors.
    - The message “Error receiving from server: 10060” (Windows) or “Error receiving from server: 0” (Linux) usually indicates that the RADIUS server does not recognize RADIUS Agent as a client (source of RADIUS requests).
    - Make sure your RADIUS server is configured as described in the TRITON - Web Security Help.

RADIUS Agent Troubleshooting

- Troubleshooting steps (continued):
  - Run **ConsoleClient** on diagnostic port **30801**
    - See websense.com/content/support/library/web/v75/ws_utilities/tl_75_consoleclient.aspx.
    - Use the **printself** option to review the user name map.
    - If the user map is correct, but the user is not identified, there may be a User Service problem, or a communication issue between RADIUS Agent and Filtering Service.

eDirectory Agent Troubleshooting

- If users are not identified by eDirectory Agent:
  - Make sure that users are logging onto the Novell eDirectory domain.
  - Run **testlogserver** to see if user information is missing from filtering requests.
    - See www.websense.com/content/support/library/web/v75/ws_utilities/tl_75_testlogsvr.aspx.

eDirectory Agent Troubleshooting

websense
ESSENTIAL INFORMATION PROTECTION™

- Troubleshooting steps (continued):
  - Run **ConsoleClient** on diagnostic port **30701**.
    - See websense.com/content/support/library/web/v75/ws_utilities/tl_75_consoleclient.aspx.
    - Use the **printself** option to review the user name map.
    - If the user map is correct, but the user is not identified, there may be a User Service problem, or a communication issue between eDirectory Agent and Filtering Service.
    - Enable directory service tracing (**dstrace**) to troubleshoot problems related to User Service.

eDirectory Agent Troubleshooting

websense
ESSENTIAL INFORMATION PROTECTION™

- To activate eDirectory Agent logging and debugging:
  1. Stop the **Websense eDirectory Agent** service or daemon.
  2. Navigate to the Websense **bin** directory (C:\Program Files\Websense\bin or /opt/Websense/bin, by default).
  3. Open the **wsedir.ini** file in a text editor and locate the **[eDirAgent]** section.
  4. Modify the **DebugMode** entry to read:

     ```
     DebugMode=On
     ```

  5. Modify the **DebugLevel** entry to read:

     ```
     DebugLevel=3
     ```

     Level 3 provides the highest level of debugging detail.

eDirectory Agent Troubleshooting

websense
ESSENTIAL INFORMATION PROTECTION™

- eDirectory Agent logging and debugging (continued):

6. Modify the **LogFile** entry to read:

   ```
   LogFile=eDirLog.txt
   ```

   This causes log output to be sent to a file called **eDirLog.txt**. You can enter a different file name, or leave the entry blank to send debugging information to the console.

7. Start the **Websense eDirectory Agent** service or daemon.

eDirectory Agent Troubleshooting

websense
ESSENTIAL INFORMATION PROTECTION™

- Additional note:
  - Check to see if the root context set in the **wsedir.ini** file is different from the one set for eDirectory Agent in TRITON - Web Security.

    In this case, although the user can be identified, Websense software may not be able to apply the correct filtering policy.

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

websense
ESSENTIAL INFORMATION PROTECTION™

Webinar Update

Title: **Jump Start Part 3: Web filtering with the V-Series proxy**

Date: December 15, 2010

Time: 8:30 AM Pacific Time

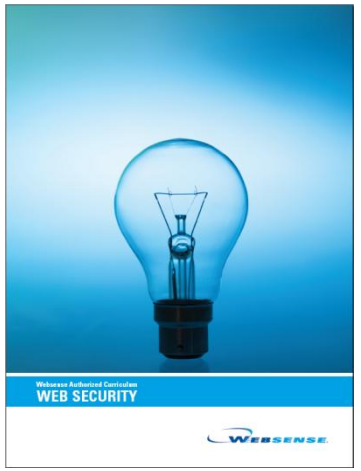
How to register:
http://www.websense.com/content/SupportWebinars.aspx

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 at your location.
- For more information, please send email to: readiness@websense.com

WEBSENSE® Authorized Training Partner

WEBSENSE® Certified Instructor



Questions?