

User Service and Directory Agent: Configuration Best Practices and Troubleshooting

Websense Support Webinar March 2011

Support Webinars

- Introduction to User Service and Directory Agent
- User Service configuration best practices
- Directory Agent deployment best practices
- Directory Agent configuration best practices
- Troubleshooting User Service issues
- Troubleshooting Directory Agent issues

- Communicates with a supported LDAP- or WINS-based directory service
 - Passes information from the directory service to Policy Server and Filtering Service for applying policies to users, groups, and organizational units (OUs).
 - Allows directory users to be assigned as delegated administrators.
- Only one User Service per Policy Server
- Use the Directory Services and Logon Directory pages in TRITON - Web Security to configure User Service settings.
- Duplicate user names are not supported for LDAP-based directories. Ensure that the same user does not appear in multiple domains.

- Directory Agent collects user and group information from an LDAP based directory service (Windows Active Directory or Novell eDirectory)
- Windows NT or Sun Java System Directory not supported
- Sends directory data to the Sync Service in LDIF format
- Policy Server must be installed before installing Directory Agent
- User Service must be configured to communicate with the directory before configuring Directory Agent

- Directory Agent configuration file is `das.ini` and is located in the Websense `bin` directory
- This file is used to configure additional parameters for Directory Agent
- Communicates to the Sync Service via port 55832
- Sync Service sends user and group information to the hybrid service, compresses large LDIFs before sending them

- Only one User Service per Policy Server
- The Settings > Directory Services page
 - Configure settings for Windows NT Directory / Active Directory (mixed mode), Active Directory (native mode), Sun Java System Directory, or Novell eDirectory.
 - Only one type of directory service can be selected per Policy Server.
 - Select the appropriate directory service from the list.
- **Windows NT Directory/Active Directory (Mixed Mode)**
 - If this option is selected, no further configuration is necessary.
 - Make sure that User Service runs with a service account that has enough rights to access the directory.
 - You will need to configure additional settings if User Service resides on a Linux machine.
 - Universal groups do not work with this option.

■ Windows Active Directory (Native Mode)

- In order for User Service to contact AD, you must provide information about the global catalog servers in your network.
- The best practice for this setting is to use the DNS domain name instead of the IP address
- Provides failover and can use DNS round robin functionality if configured on DNS server in case one domain controller fails to respond

■ Windows Active Directory (Native Mode) (*continued*)

- When using the full distinguished name option, ensure that the LDAP path for the user is correctly entered.
- Use the following command-line query on the domain controller to find the full LDAP path:

```
dsquery user -name UserName
```

For example, to find the full LDAP path for user Administrator:

```
dsquery user -name Administrator
```

This returns a result similar to the following:

```
CN=Administrator,CN=Users,DC=testlab,DC=com
```

■ Identifying Nested Groups

- User Service does not recursively search for nested groups
- Users must be direct members of the group with Universal Scope to which a group-based filtering policy has to be applied

Please refer to the following KB article for more information

<http://www.websense.com/support/article/kbarticle/Active-Directory-group-based-policies-with-multiple-domains-and-or-nested-groups>

- Add the following entry to the [DirectoryService] section of the **websense.ini** file to ensure that User Service filters users added to updated nested groups:

```
[DirectoryService]
```

```
SearchADNestedGroups=True
```

Restart Filtering Service and User service after making the change.

- **Novell eDirectory and Sun Java System Directory**
 - Enter the IP address of the directory server machine.
 - Enter **Port** used for directory communication (by default, 389).
 - If your directory requires administrator privileges for read-only access, enter the **Administrator distinguished name** and **Password**.
 - Optionally, enter the **Root context** to use when searching for user information. For example, o=domain.com.

- Supported Operating Systems
 - Windows Server 2008 SP2
 - Windows Server 2003 R2 SP2
 - Windows Server 2003 SP2
 - Red Hat Enterprise Linux 5, update 3
 - Red Hat Enterprise Linux 4, update 7
- In most cases, you need only one instance of Directory Agent in the entire deployment.
 - It is possible to install multiple instances of Directory Agent, but not recommended.

- Policy Server must be installed before installing Directory Agent.
- If you have a V-Series appliance, Directory Agent is already installed on the appliance. Do not install it on a separate machine.
- Sync Service must be installed to send data collected by the Directory Agent to the hybrid service.
- Communicates with Sync Service on port 55832

- Directory Agent configuration is done in TRITON - Web Security
- Navigate to the Settings > Hybrid Configuration > Shared User Data page
- User Service must be configured before configuring Directory Agent
- Select a global catalog server configured on the Directory Services page to configure Directory Agent communication with that server

- Specify a root context to use when collecting user/group information
 - Context should include only hybrid filtering users
 - To increase Directory Agent speed and efficiency, narrow the context.
- Select the appropriate level to indicate whether search is performed just one level below the context or all levels.
- Use search filters to remove duplicate or unwanted mail entries while searching.

Directory Agent Configuration

- Use the Test Connection button to verify that Directory Agent can communicate with Sync Service.
- Schedule how often collected data is sent to the hybrid service on the Settings > Hybrid Configuration > Scheduling page.

- Additional configuration of Directory Agent can be done using the **das.ini** file.
- To change the path where Directory Agent stores LDIF files, use:

```
DiffDir=./diffs/
```

- To set the number of times Directory Agent retries after a failed attempt to connect to the directory service:

```
DirServiceRetryCount=5
```

- Unable to add clients in TRITON - Web Security:
 - Verify your Directory Service settings.
 - If you are using Active Directory (native mode), make sure that you can telnet to the global catalog server on the port specified.
 - Ensure that the account details specified in the directory service settings are correct
 - Use an LDAP browser such as Softerra to replicate settings and check whether you can connect with that browser.
 - Use Wireshark to packet capture the communication

- User or group-based filtering is not working:
 1. Stop all Websense services
 2. Navigate to the Websense **bin** directory and open the **websense.ini** file in a text editor.
 3. Add the following lines:

```
[DirectoryService]
GroupLog=true
BindLog=true
CacheLog=true
```
 4. Start the Websense services. A **dstrace.txt** file is created in the **bin** directory. Send this file to Technical Support for further investigation.

- Sync Service not receiving user/group information
 - Ensure User Service is correctly configured and that Directory Agent is able to communicate with the global catalog to retrieve user/group information.
 - Verify that the Directory Agent can communicate with Sync Service via the Test Connection button.
 - If no connection can be made, verify the IP address or hostname of the Sync Service machine and ensure that Sync Service is running.
 - Also check the firewall to ensure communication is allowed.
 - Run the Sync Service viewer to see if it is receiving LDIFs from Directory Agent.

- Directory Agent debugging information can be generated using the **diagnostic.cfg** file located in the Websense **bin** directory:
 1. Open the **diagnostics.cfg** file.
 2. Look for the section:
`#log4j.threshold=OFF`
`log4j.threshold=ERROR`
#log4j.threshold=ALL
 3. Change this to:
`#log4j.threshold=OFF`
#log4j.threshold=ERROR
`log4j.threshold=ALL`
 4. Add the following line into the file:
log4j.logger.DAS=ALL, GUI, CONSOLE, FILE
 5. Save and close the file, then stop and start the Directory Agent service.

- When Directory Agent diagnostics are enabled, a detailed log file called WebsenseDAService.log is created in the Websense **bin** directory.
- After generating the necessary troubleshooting information, make sure to disable debugging in the **diagnostic.cfg** file, then restart Directory Agent.

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 Update

Title: Upgrading to Websense Web Security v7.6

Date: April 13, 2011

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

WEBSense®
**Authorized Training
Partner**

WEBSense®
Certified Instructor



Questions?

