# Forcepoint

# Web Security On-prem and URL Filtering

**v8.5.x**

**Log Server Error Reference Guide**

**Contents**

# Introduction

When Log Server experiences logging problems, the service records errors in the Windows Event Viewer and the **Websense.log** file. The Websense.log file is located in the **bin** directory (`C:\Program Files\Websense\Web Security\bin`, by default) on the Log Server machine.

Use the information in this document to better understand the following error messages, and to troubleshoot the underlying problem or problems.

**Related concepts**

**Related tasks**

**Related information**

# Could not connect to the directory service...

## Full error message

```
Could not connect to the directory service. The groups for this user will not be resolved at this
time. Please verify that this process can access the directory service.
```

## Explanation

Log Server is unable to access the directory service, and therefore cannot update user information and user-to-group mappings for reports.

This can happen if Log Server and User Service are on different sides of a firewall that is limiting their communication. To resolve this problem, configure the firewall to permit access over port **55815**.

The default ports used for directory service communication are:

| 139 | NetBIOS communication: Active Directory |
|---|---|
| 389 | LDAP communication: Active Directory, Novell eDirectory, Oracle (formerly Sun Java) Directory Server |
| 636 | SSL port: Novell eDirectory, Oracle (formerly Sun Java) Directory Server |
| 3268 | Active Directory |
| 3269 | SSL port: Active Directory |

# Could not read...

## Full error messages

```
Could not read field name
Could not read v5 field ## [field name]
Could not read v6 field ## [field name]
Could not read WTG field name
```

## Explanation

Filtering Service:

1) Receives Internet usage information from Content Gateway, Network Agent, or third-party integration products.

2) Formats the data it sends to Log Server based on the source.

These informational errors indicate that Log Server found an invalid piece of data in a record forwarded by Filtering Service. Records with invalid data are not included in the temporary files Log Server creates and sends to the Log Database.

Although the error messages do not indicate a problem with Log Server:

- Large numbers of errors suggest that a large amount of Internet usage data is not being recorded in the Log Database.

- The errors suggest either an issue with Filtering Service, or with the component that sends URL request information to Filtering Service.

  To resolve the issue:

  1) Use the Windows Services tool or /opt/Websense/WebsenseDaemonControl command to stop and restart Filtering Service.

2)    Refer to the Deployment and Installation Center for the installation instructions for your product for information about correctly configuring Filtering Service communication with Content Gateway, Network Agent, or another integration product.

# Failed to delete...

## Full error messages

```
Failed to delete BCP file
```

```
Failed to delete cache file
```

## Explanation

Once Log Server moves the data from a BCP or cache file to the Log Database, it deletes the temporary file. If Log Server is unable to delete temporary files, they continue to collect, taking up disk space.

Make sure the Log Server account has read, write, and delete privileges for the cache folder, BCP folder, or both.

# Log Server dropped an invalid record

Log Server receives records from Filtering Service and moves them to the Log Database. When the contents of a record are not in the correct format, Log Server is not able to process the information accurately. As a result, the record is "dropped" (neither processed into temporary files, nor recorded in the Log Database).

This error message is informational only. If it occurs regularly and frequently, however, it could indicate a problem with the component or integration product that is sending the Internet usage information to Filtering Service. It could also indicate a problem with Filtering Service.

To resolve the issue:

1)    Use the Windows Services tool or `/opt/Websense/WebsenseDaemonControl` command to stop and restart Filtering Service.

2)    Refer to the Deployment and Installation Center for the installation instructions for your product for information about correctly configuring Filtering Service communication with Content Gateway, Network Agent, or another integration product.

If Log Server receives 4 consecutive invalid records, it drops its connection to Filtering Service and reconnects, in an attempt to correct the problem on its own.

When this occurs, the error "Connection from client xxx is reset due to bad log data" is recorded.

# LogServer failed 100 times while obtaining user full names from the UserService

This non-critical warning occurs when Log Server has been unsuccessful in re- verifying information for users who have generated Internet usage data. This message can occur when:

- Users were moved within or deleted from the directory service.
- Log Server or User Service cannot contact the directory service.

By default, Log Server tries to find user information for 90 days, then stops looking.

## To avoid flooding the Event Viewer or Websense.log file with these errors

### Steps

1) Use the Windows Services tool to stop the **Websense Log Server** service.

2) Navigate to the **bin** directory (`C:\Program Files\Websense\Web Security\bin`, by default) and open **LogServer.ini** in a text editor.

3) In the **[UserGroups]** section, find **CutOffDays**.

4) Change the default value of 90 to **3** (or some other value that works for your organization) to keep Log Server from looking for a user's information for more than the specified number of days.

5) Save and close **LogServer.ini**.

6) Start the **Websense Log Server** service.

# LogServer failed to save the group membership to the database

This warning appears when Log Server has been unable to move user information into the Log Database. This can happen if there is a problem with the database or the database server. Make sure:

- The Microsoft SQL Server machine is running and available on the network
- The SQL Server service is running

# Log Server stopped processing a corrupt cache file: %1

This informational message indicates that Log Server found one or more corrupt records in a cache file and stopped sending data from that particular file to the Log Database.

If you see this errors regularly and frequently, there may be a problem with Filtering Service or with the component or integration product that sends Internet requests to Filtering Service. See *Log Server dropped an invalid record*, for more information.

This message may also occur if Log Server stopped suddenly, leaving a cache file partially written.

The name of the problematic cache file is appended to the error message. To avoid the same error each time Log Server is started, delete that cache file.

> **Related concepts**
> Log Server dropped an invalid record on page 5

# Not enough disk space. Buffering stopped.

This warning message appears when Log Server is not able to create new cache files because there is no free disk space. The solution is to free up or add disk space.

Before this error appears, a health alert is displayed in the Web Security module of the Forcepoint Security Manager, warning that disk space on the Log Server machine is getting low.

# Service initialization failed

This warning indicates that Log Server cannot run. It is always accompanied by another error message explaining the underlying problem. Look for that error message to determine the problem and resolve it.

# The database may be down or unreachable

Log Server must remain connected to the Log Database to process log records. When the database connection is down, Log Server attempts to reconnect 20 times. If it is unable to establish a connection, the service stops.

See Log Server stops unexpectedly or will not start for information about correcting this problem.

# The Websense server was unreachable...

## Full error message

```
The Websense server was unreachable. The Log Server will shutdown. Please verify the IP and port of
the Websense server and that it is running, then restart the Log Server. The Log Server service must
be started after the Websense server.
```

## Explanation

When Log Server is unable to contact Policy Server, the service stops. To address this problem:

### Steps

1) Make sure that the Policy Server service associated with the stopped Log Server instance is running.

2) Verify that the Policy Server IP address and UID that appear in the **websense.ini** file on the Log Server machine are correct.

   - The **websense.ini** file is located in the **bin** directory (`C:\Program Files\Websense\Web Security\bin`, by default).
   - The UID in the **websense.ini** file should match the one that appears in the **config.xml** file in the **bin** directory on the Policy Server machine (`C:\Program Files\Websense\Web Security\bin or /opt/ Websense/bin/`, by default)

# This process does not have permission to access the directory service...

## Full error message

```
This process does not have permission to access the directory service.The groups for this user will
not be resolved at this time. Please verify that this process has permission to access the directory
service.
```

## Explanation

This message appears when Log Server attempts to retrieve user information from User Service, but User Service does not have permission to access the directory service.

Refer to the Administrator Help for your web protection product for information about configuring communication between User Service and the directory service used in your network.

# Unable to access LogServer.state file

This warning indicates a problem with the **LogServer.state** file, which is stored in the Log Server cache folder. To correct the problem:

## Steps

1) Use the Windows Services tool to stop the **Websense Log Server** service.

2) Navigate to the cache folder (`C:\Program Files\Websense\Web Security\bin\Cache\ or bin\Cache\BCP`, by default).

   If you have defined a custom directory, you can verify the path on the **Web** > **Settings** > **Reporting** > **Log Server** page in the Forcepoint Security Manager

3) Delete the **LogServer.state** file.

4) Start Log Server.

# To resolve the issue of accessing LogServer.state file

If cache file processing does not quickly resume, there may be a corrupted cache file. To resolve this:

## Steps

1) Use the Windows Services tool to stop the **Websense Log Server** service.

2) Navigate to the cache folder (see path in step 2 above).

3) Delete the **LogServer.state** file, if it has been recreated.

4) Delete the oldest cache (.tmp) file in the directory.

   If loss of reporting data is not a serious concern, you can alternatively delete all of the temporary files in the directory.

5) Start Log Server.

# Unable to communicate with the Websense Filtering Service...

## Full error message

Unable to communicate with the Websense Filtering Service. Make sure that the service is running and that configuration parameters are correct.

## Explanation

If Log Server is not able to communicate with Filtering Service, Log Server cannot receive Internet request information.

See Make sure Filtering Service is sending data for help resolving the issue.

# Unable to create the temp file

If Log Server can't create temporary (cache or BCP) files to store the data it receives from Filtering Service, Internet activity records are lost.

This warning typically indicates that Log Server does not have the necessary read, write, and delete permissions to the cache directory (`C:\Program Files\Websense\Web Security\bin\Cache\ or bin\Cache\BCP`, by default).

First verify the cache file location on the **Web** > **Settings** > **Reporting** > **Log Server** page in the Forcepoint Security Manager, then make sure the Log Server account has the permissions needed to create the folder and cache files.

This error occurs most often when Windows Authentication is used to connect to the database. When the trusted user changes in Microsoft SQL Server, Log Server must be configured to run with a new trusted user account. If the Log Server account is not updated, this warning is displayed.

# Unable to initialize the Directory Service. Websense Server may be down or unreachable

This warning indicates that Log Server is unable to get user and group information from the directory service.

See *Could not connect to the directory service...*, for more information.

> **Related information**
> Could not connect to the directory service... on page 3

# Unable to initialize the Log Database

When Log Server loses connection to the Log Database, Internet usage data, user information updates, and custom policy enforcement data cannot be sent to the database.

See Check for Log Database problems and Log Server stops unexpectedly or will not start for help resolving the issue.

# Unable to initialize the Policy Server connection...

## Full error message

```
Unable to initialize the Policy Server connection. Websense Policy Server may be down or unreachable.
```

## Explanation

The Log Server service cannot run without a connection to Policy Server. Any time Policy Server is stopped, or communication between the Log Server and Policy Server machines is blocked, Log Server stops.

Restart Log Server after making sure:

- Policy Server is running.
- The Policy Server IP address and UID in the **Websense.ini** file in the **bin** directory (`C:\Program Files \Websense\Web Security\bin`, by default) on the Log Server machine are correct.

  The UID in the Websense.ini file should match the one listed in the config.xml file on the Policy Server machine.

# Unable to receive. There was a previous I/O error

This informational message indicates that Log Server is having problems receiving data from Filtering Service. This may occur when Filtering Service is stopped and restarted.

If Filtering Service and Log Server are both running and this message continues to appear, see Make sure Filtering Service is sending data for help resolving the issue.

# Unable to write to log file

If Log Server has problems writing to the cache files, it cannot load the Internet usage data Filtering Service sends. If this message is displayed frequently, there could be a significant amount of data being lost.

Make sure:

- Log Server has permission to write to the cache folder defined on **Web** > **Settings** > **Reporting** > **Log Server** page in the Forcepoint Security Manager.

- There is sufficient disk space for Log Server to create a new file.