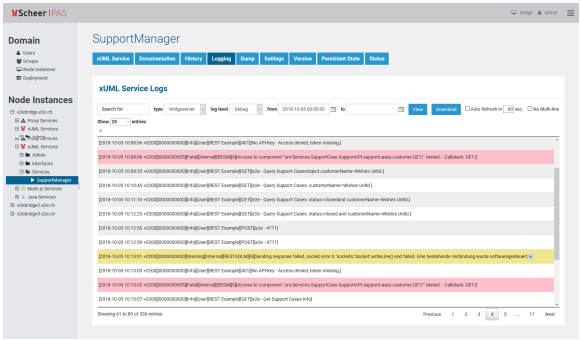
Logging of xUML Services

Switch to the **Logging** tab in the information/working area. All users have access to logged information.

The logged information is categorized as follows:

Log	Technical Name	Description
Standard Log	**bridgeserver**	Contains logging information logged by the Bridge process that is running the selected xUML service.
Transaction Log	**transaction**	Contains transactional logging information logged by the Bridge process that is running the selected xUML service. The logged information is usable for performance measurements or statistical evaluations (how often has the transaction been called, in which context, etc.).
Start Log	**start**	Contains information about the selected xUML service, environment variables, and errors logged by the Bridge process at startup.
Stop Log	**stop**	Contains information about the selected xUML service and errors logged by the Bridge process when stopping it. A stop log is available, if the service could not be stopped regularly but if errors occurred upon stopping, or if the service had to be killed.
Custom Logs	**<your name>**	The Bridge can also display custom logfiles. To be able to access this custom logfiles via the Bridge, they must meet certain conditions that are explained in detail further below.



Custom Logs

The Bridge can also display custom logfiles. To be able to access this custom logfiles via the Bridge, they must meet the following conditions:

Condition	Description	
Save Location	Custom log files of a service must be saved to the **/logs** folder of the service data directory.	
Naming Scheme	Names of custom log files must conform to the following naming scheme:	
	`<custom name part>.log`	for logs that do not rotate
	`<custom name part>_yyyy-mm-dd.log`	for logs that rotate per day
	`<custom name part>_yyyy-mm-dd-hh.log`	for logs that rotate per hour
	The custom name part of the logfile must not contain underscores and must not be one of the reserved log types mentioned above.	

On this Page:

Related Pages:

- xUML Service Standard Log
- xUML Service Transaction Log
- xUML Service Start Log
- xUML Service Stop Log
- xUML Service Dump

- Bridge Server Log Levels of an xUML Service
- Java Regular Expressions

Log File Content Format	The log files can be in text or in JSON (Bridge 7.7.0) format. If the log files are in JSON format, they must contain the following properties which will be displayed: • **timestamp:** Timestamp • **message:** Log message Log files in JSON format can be filtered in the same way as text log files. See Filtering the Log Entries below.	

Filtering the Log Entries

Logs may contain big amounts of data and in these cases it may be difficult to find the piece of information you are looking for. Therefore, you can filter the logfile entries by log level, date/time and a regular expression.

Filter Element	Description	Default
Search for	Insert a string or a valid regular expression to search the log entries for. Only log entries that match the expression will be displayed. Refer to Java Regular Expressions for more information on which regular expressions you can use here. Pressing **Enter** in this field triggers the search.	empty
in type	Select the type of logfile you want to display: bridgeserver, start, stop, transaction, custom log types. See top of this page for more information on the log types. The log types in this list are displayed in alphabetical order, and the first log type of this list will be the default. So, if you add a custom log named aa.log, this log will be displayed on going to the **Logging** page.	first available log type
with log level	Select the log level of the log entries you want to inspect. Refer to Bridge Server Log Levels of an xUML Service for more information on log levels and what information they contain. This filter is available for the xUML service standard log (bridgeserver) and the transaction log.	Debug
from	Select the date/time range you want to inspect. • Upon opening the logging tab, **from** is set to (now - 10 minutes) if there are log entries existing within this range of time. If not, **from** will be set to the point of time the first entries are found. • An empty **to** field displays all log entries from the **from** date/time until the most recent entries. An empty **from** field triggers a search backwards until the first entries are found. • You can remove the time part of the **to** field to search until the end of the day, and of the **from** field to search from the beginning of the day. Pressing **Enter** in these fields triggers the search. To enter the dates, you can use a date picker next to the input fields:  Refer to section The Date Picker for more information on this. The timestamp must follow one of the following patterns if you want to use this filtering feature for your **custom logs**: • `YYYY-MM-DD HH:MI:SS` or `[YYYY-MM-DD HH:MI:SS` • `HH:MI:SS` or `[HH:MI:SS` It is allowed to put the timestamp in square brackets.	actual timestamp - 10 min
to		empty

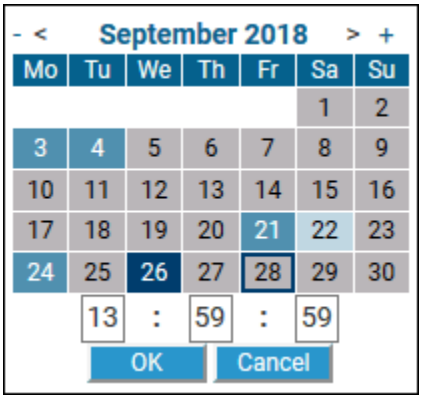
Click **View** to update the displayed logging information.
As per default, for logs with a time stamp the log entries are displayed latest first in the search results. Click the tiny arrow in the table header to change the order to oldest first.

The date filter settings will be kept as long as your Browser tab is open. They will be reset to default as soon as you open the **Logging** tab in a new Browser tab.

If you close your Browser with the **Logging** tab open, and start your Browser again with restoring all recent tabs (session restore), your date filter settings will be reloaded from your previous search.

The Date Picker

When filtering the log entries of a service by date and time, you can use a date picker to select a date from/to. Click the date picker icon  next to the input fields to open the a tiny calendar to pick the dates from.



The time part will be only visible if the related log entries contain a time part in format "HH:MM:SS". In all other cases, it is not possible to select log entries by time.

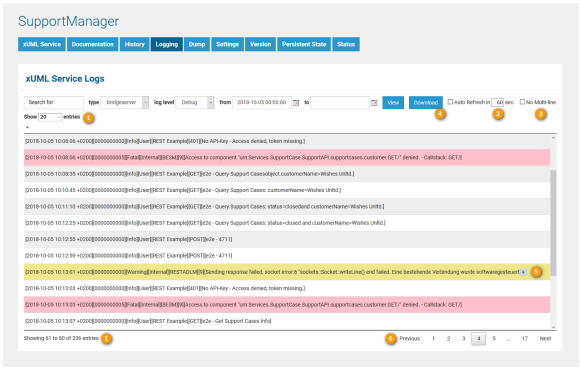
Some dates within the calendar are colored to help you finding the appropriate date:

Color	Meaning
dark blue border	Today.
dark blue	The selected date.
bright blue	A weekday on which data has been logged.
light blue	A weekend day on which data has been logged.
grey	A day on which no data has been logged.

Select a day, enter a time (if necessary), and click **OK** to apply the selected date to the search field.

The Search Results

The results according to your search conditions are displayed in a paged list.



1. You can define how many results should be displayed on one page by selecting on of 20, 50, 100, 250 and 1000 from the **Show entries** dropdown.
   At the bottom of the log table, you can see how many log entries have been found and how many of them are displayed: **Showing 1 to 9 of 9 entries**.

2. You can auto refresh the search results by checking the **Auto Refresh** checkbox. Specify an interval in seconds, or leave the default (60 seconds).
3. By ticking **No Multi-line** you can flatten the output to an unstructured view. This may be necessary if a multi-line log message contains more than 100 sub-messages (see also 5).
4. By clicking **Download**, you can download the search result (all pages) as a simple flat file that resides in a ZIP archive.
5. Multi-line log messages are collapsed to not clutter the list of results. You can expand those multipart lines by clicking the plus sign at the end of the visible message part.

   > For all logs except bridgeserver log: Mult-line log messages can only hold up to 100 sub-messages - the rest will be cut. If you get a hint that there are more then 100 messages, use **No multi-line** to flatten the output and display all messages (see also 3).

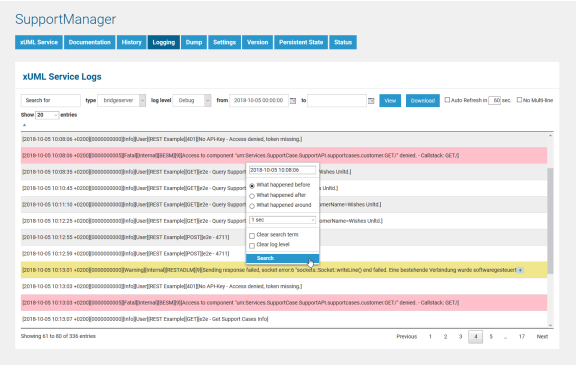
6. Use the buttons **Previous** and **Next** to browse through the results, or select a result page by clicking on a page number.

The lines of search results are colored in relation to their log level:

- Error/Fatal messages are colored in red.
- Warnings are colored in yellow.
- All other messages are white or gray, alternating for a better readability.

Refining the Search

Once you have identified problems in the bridgeserver or transaction log, you can refine the search with the help of the context menu.



Click a log entry with the right mouse button to activate the context menu. Then, make your selections:

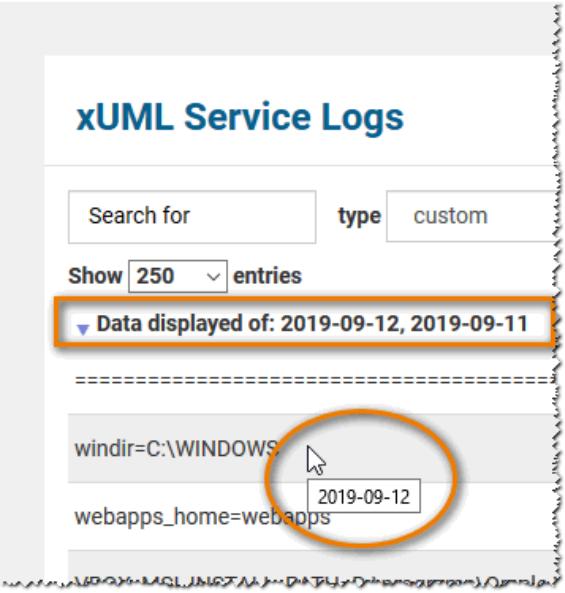
Filter Element	Description	Default	
timestamp	Enter a timestamp you want to analyze in more detail. As per default, this is prepopulated with the timestamp of the selected log entry.	Timestamp of the selected log entry.	
time focus	To analyze what happened around the selected time stamp, you can choose between: • What happened before the selected **timestamp**? • What happened after the selected **timestamp**? • What happened around the selected **timestamp**?	What happened before	
time frame	Set a **time frame** in relation to your selected **focus**: What happened within the specified **time frame** before/after/around the selected **timestamp**?	1 second	
clear search term	Remove a specified search term from the search filter for this refinement to get more search results.	false	
clear log level	Remove a specified log level from the search filter for this refinement to get more search results.	false	

Custom Logs

The Bridge can also display custom logfiles. If a service produces log files that

- have a date part in the log file name (scheme **<custom name part>_yyyy-mm-dd.log**.log or **<custom name part>_yyyy-mm-dd-hh.log**),
- but the log messages do not contain a timestamp

the Bridge allows nevertheless to search logs by date. In this case, the search results will display the dates in the table header:



A tooltip for each log entry displays the date it belongs to.