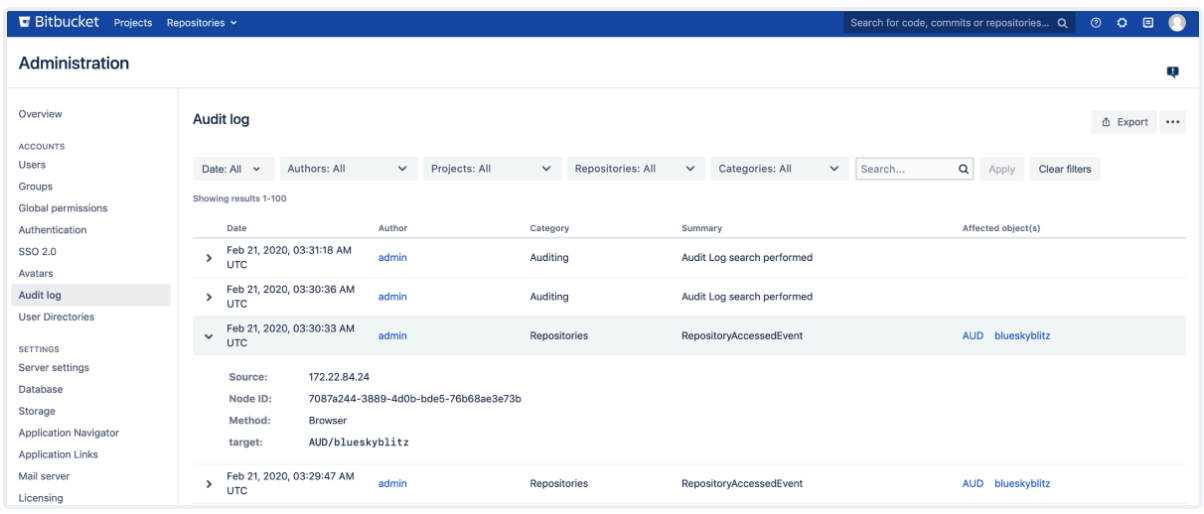
View and configure the audit log

The auditing feature tracks key activities in Bitbucket Data Center, allowing administrators to get an insight into the way Bitbucket is being used. The audit system can be used to identify authorized and unauthorized changes, or suspicious activity over a period of time. The audit log experience lets you search and filter the log for details, along with utilizing grouped coverage areas for clarity.



Viewing the audit logs for your instance

To view the global audit page:

1. In the administration area, go to **Audit log** (under Accounts).
2. **Expand** any event to get more details.

Information for each event may include:

- **IP address** - IP address of the user who performed the action (though not recorded for system-generated events) Can also show the node IP address.
- **Node ID** - unique ID of the node where the action was performed
- **Method** - depending on how the action was performed, will be either Browser (end user) or System (system process)
- **Target** - a legacy attribute that represents the target of an action
- **Details** - a legacy attribute containing additional information about event details
- **Load balancer/proxy** - shown while using a load balancer or proxy

Some of the information in each event is not available for events logged by Bitbucket 6.x.

Accessing audit logs

You can find the log file in the `<home directory>/log/audit` directory. On clustered Bitbucket Data Center deployments, each application node will have its own log in the local `<home directory>/log/audit` directory. The audit log file is used primarily for integrating with third-party logging platforms.
Refer to Audit log integrations for detailed information about the log file.

> All audit log events are stored in the database. There is a limit of 10 million events logged in the database. When that limit is reached, the oldest records will be deleted as necessary.

Audit log events from previous versions of Bitbucket

Any events that were logged before you upgraded to Bitbucket 7.x:

- won't be visible until after the migration task completes in the background
- will appear as two separate entries in the list
- won't contain details like Source, Node ID, and Method

Adjusting data retention and selecting which events to log

In the audit log settings, you can decide how long you want to retain the logged events in the database and the areas from which you want to collect the logs.

Setting the database retention period

You can decide to retain the data in the database for a maximum of 99 years, however, setting long retention periods can increase the size of your DB and affect performance.

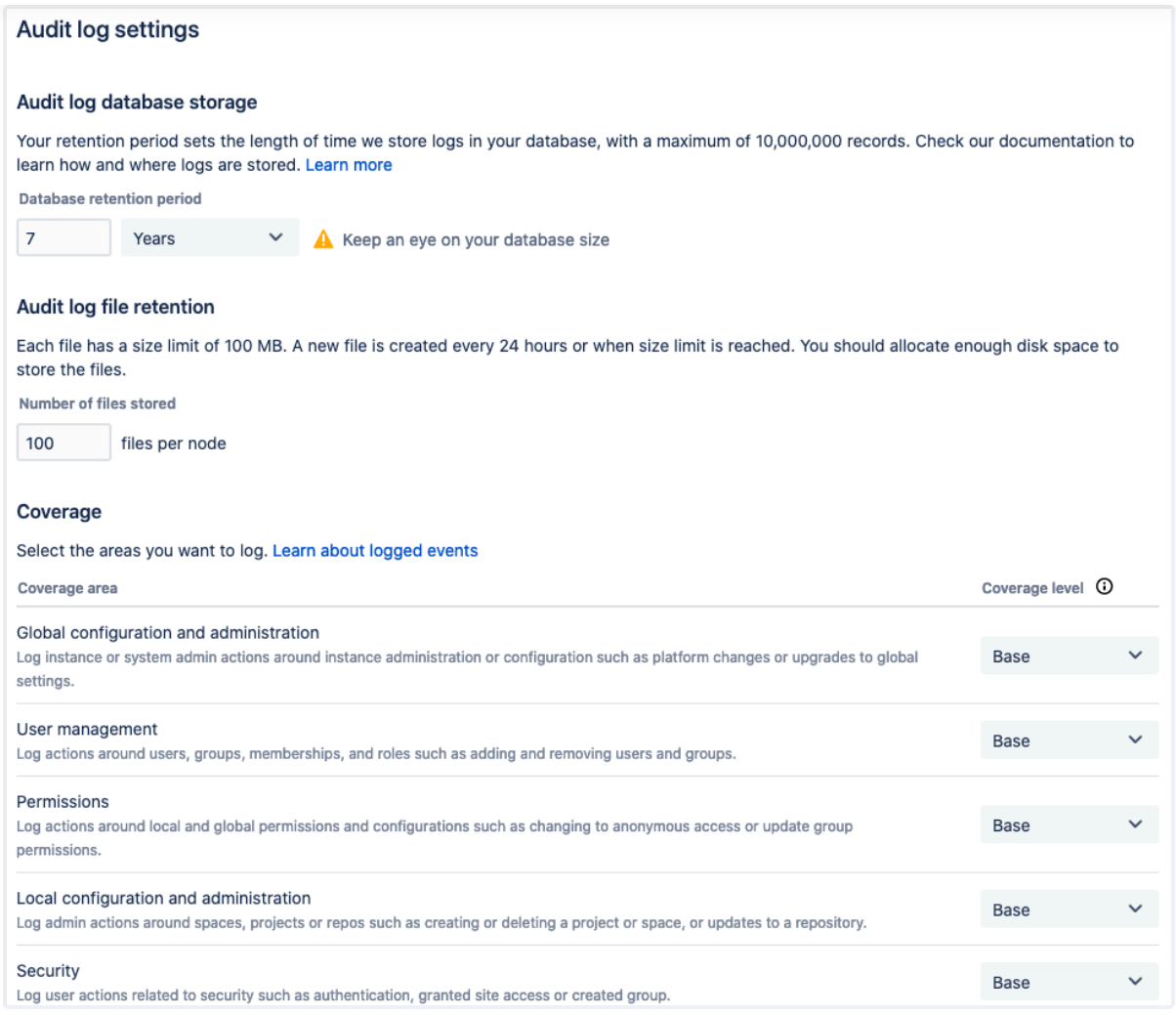
To set the retention period:

1. In the administration area, go to **...** > **Settings**.
2. Adjust the **Database retention period**.
3. **Save** your changes.

> If you limit the retention period, all the events that exceed the newly set period will be deleted from the database and from the UI, however, they will be retained in the audit log file.

Selecting events to log

The events that are logged are organized in categories that belong to specific coverage areas. For example, mirror-related events are logged in the Global administration category that belongs to the Global configuration and administration coverage area. For all coverage areas and events logged in each area, see Audit log events.



To adjust the coverage:

In the administration area, go to **...** > **Settings**.

In the **Coverage level** drop-down, choose **Base** to log the most important events or **Off** to stop collecting events from a particular area.

Coverage levels reflect the number and frequency of events that are logged.

Off: Turns off logging events from this coverage area.

Base: Logs low-frequency and some of the high-frequency core events from selected coverage areas.

Advanced: Logs everything in Base, plus additional events where available.

Full: Logs all the events available in Base and Advanced, plus additional events for a comprehensive audit.

Exporting audit log events

You can export up to 100,000 events as a CSV file. If you have more events than that, only the 100,000 newest events are included in the export. In Bitbucket Data Center, you can also export up to 100k filtered events based on your current search.

To export audit log events:

1. On the **Audit log** page, select **Export**.
2. Select **Filtered result**s (Data Center only) or the **Latest 100k events**.
3. Select **Export**.

Change the audit log file retention

You can choose how many audit log files to store in the local home directory on each node. By default, we store 100 files. Make sure you've provisioned enough disk space for these files, especially if you have set the logging level to Advanced or Full.

To change the file retention setting:

1. On the **Audit log** page, select ... **Settings**.

Last modified on Oct 4, 2023

Was this helpful? Yes No Provide feedback about this article

In this section

Audit log events

Audit log integrations

Push logs

Related content

Audit log integrations

Right to erasure in Bitbucket Server and Data Center

Configuration properties

Users and groups

Data pipeline

Mesh configuration properties

Monitor security threats

Event system