Athena API Keys: Security

API keys provide secured access to the Athena Content Hub API. You should treat all API keys like you would treat a password or any other credentials. Keep it secret! Keep it safe!

- Don't store API keys in shared or public code bases (including Git/GitLab).
- Deactivate unneeded API keys to prevent unauthorized access.
- If you suspect an API key has been compromised, generate a new one (and be sure to update it in any connected apps).
- Regenerate API keys at least once a year along with database credentials.

If you suspect data has been compromised, follow your organization's information security policies accordingly.

Still need help?

If you have questions related to this article, please contact the LTS Help Desk at 715-836-5711 or helpdesk@uwec.edu.