Exposure Notification Server Configurations

Version 1 • August 5, 2021

www.aphl.org

APHL supports the exposure notification system in its hosting of the National Key Server on the Azure Cloud and the Multi-tenant Verification Server on the Google Cloud Platform. These servers are available to all US states and territories.

This document includes a description of some of the server configurations that may affect user experience when using the Exposure Notification System. The configurations are chosen based on best practices and in accordance with APHL policy. Changes to these configurations will be reflected here. Please reach out to en@aphlinformatics.atlassian.net if you have any questions.

Multi-Tenant Verification Server (MVS) Configurations

- Issuing APIs (/issue and /bulk-issue) can be requested up to 240 times in a minute before the requests are rate limited and rejected.
- Verification tokens given to devices by the /verify API are valid for 24 hours. This token is exchanged for a verification certificate before sharing keys.
- MVS audit logs are kept for 30 days, and realm stats are kept for 90 days.

National Key Server (NKS) Configurations

- The key server must reach a minimum threshold of 10 publish requests per day to collect and export that day's key server statistics.
- A user can publish keys if their symptom onset date is a maximum of 14 days ago.
- Keys can be up to 15 days old, or they are rejected by the key server. Valid keys will still be accepted even if some are rejected. Up to 30 keys can be published at once.
- A maximum of three keys can be published with the same creation time. Normally, this scenario happens if a user tries to re-publish their keys multiple times after an initial failure.
- Key exports are available for download for 14 days after their initial publication.
- Keys are held (embargoed) before they are exported for a minimum of two hours after they are published.

Log Retention Configurations

- MVS infrastructure and application logs are stored for 14 days.
- NKS infrastructure logs are stored for 14 days.
- NKS application logs are stored for 30 days.