

AXA



AXA Migration Overview



There is an update to the AXA system for users who access the Security Information Exchange (SIE) data sets via SIE Remote Access. Release notes can be found on github at <https://github.com/farsightsec/axa/releases/>. A few highlights of this include:

- Authentication now uses an AXA-specific apikey credential rather than former legacy authentication methods.
- Consistency with DNSDB formatting conventions has been improved. RRnames now include the formal trailing dot, and RRtypes are now capitalized, as has been the norm in DNSDB.
- Formerly, sratool would display its output in a non-standard "presentation-like" format. sratool output is now in standard JSON Lines (JSONL) format only. If you relied on the prior output format used by sratool for data collection or analysis, you will need to update your process to use the new format.
- Command line tool changes
 - You can now add the `sratunnel -K kickfile` option to allow rotating new output files based on `-C` packet count, `-T` elapsed seconds, or `-Z` file size.
 - We now allow `sratunnel -k (kickfile)` to work with `-i (interval)`.
 - `sratunnel` has a new `-Z` option to clamp an output file size.
 - `sratunnel` has a new `-T` option to stop output after elapsed seconds.
 - The `-S certs` option has been removed.
 - The `axa config` file is now optional.
 - The missed packet display now uses UTC time (instead of local time)
- A per-user client configuration file may be used to setup convenience aliases for connections.
- `sratunnel` has NMSG JSONL output support.
- Accounting messages include ISO 8601 timestamps.
- Tools have an option to disable NMSG output buffering. This will write NMSG payloads as quickly as possible instead of waiting for the container to be full.
- On supported platforms like NetBSD and MacOS, CTRL-T (SIGINFO) may be used to report brief session information while `sratunnel` is running.

Upgrading to the new AXA release

Upgrading to the new AXA release will involve installing updated software and reconfiguring your access to the SIE data servers.

You will need a new API key to connect with the updated AXA software. Please contact Technical Support to be issued your new key.

It may make sense to create a new installation of AXA rather than update your existing setup and then switch to it when it's functional. This will allow you to continue using the old AXA system during installation and testing.

The AXA software is available as: <https://github.com/farsightsec/axa>. See the README for installation instructions. **IMPORTANT:** to use the new release you will need to install the updated software. It is strongly recommended you do so to take advantage of the many fixes and improvements in the updated system.

AXA documentation has been updated and can be found here:

- [AXA Technical Overview](#)
- [AXA User Guide](#)
- [AXA API Reference](#)

IMPORTANT: The host name and configuration syntax for connecting to the SIE data sources has changed. It previously looked something like this:

alias:sra-ssh=ssh:sra-service@sra.sie-remote.net,1021

It will now look like this:

alias:sra-staging=apikey:your_api_key_here@axa-sie.domaintools.com,49500

Testing the new Installation

Once the software is installed and configured, you should verify you can connect to the service and verify that you can access and download some data. Please verify that all of the channels you have subscribed to are available from the new server.

If you have any questions or see any issues with your provisioning, please contact Enterprise Support