User Guide

# AXA Migration Overview

June 2024

DomainTools

# Overview

There is an update to the access mechanisms for SIE Remote Access. Release notes can be found on github at https://github.com/farsightsec/axa/releases/. Changes 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 an 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.
- `sratunnel` has NMSG JSONL output support.
- 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 set up convenience aliases for connections.
- 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

The following actions are required to access the new AXA release.

# Implement a new API key

A new API key is required to connect with the updated AXA software. You will need a new API key to connect with the updated AXA software. Please contact enterprisesupport@domaintools.com for your new key.

# Install the updated software

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 at https://github.com/farsightsec/axa. See the repo README and the SIE User Guide for more information.

# Update connection syntax

The host name and configuration syntax for connecting to the SIE data sources has changed. Previously, it appeared like:

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

The updated syntax reads as follows:

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

# Verify your connection

Please verify that your subscribed channels are available, and contact enterprisesupport@domaintools.com if you experience any difficulties.