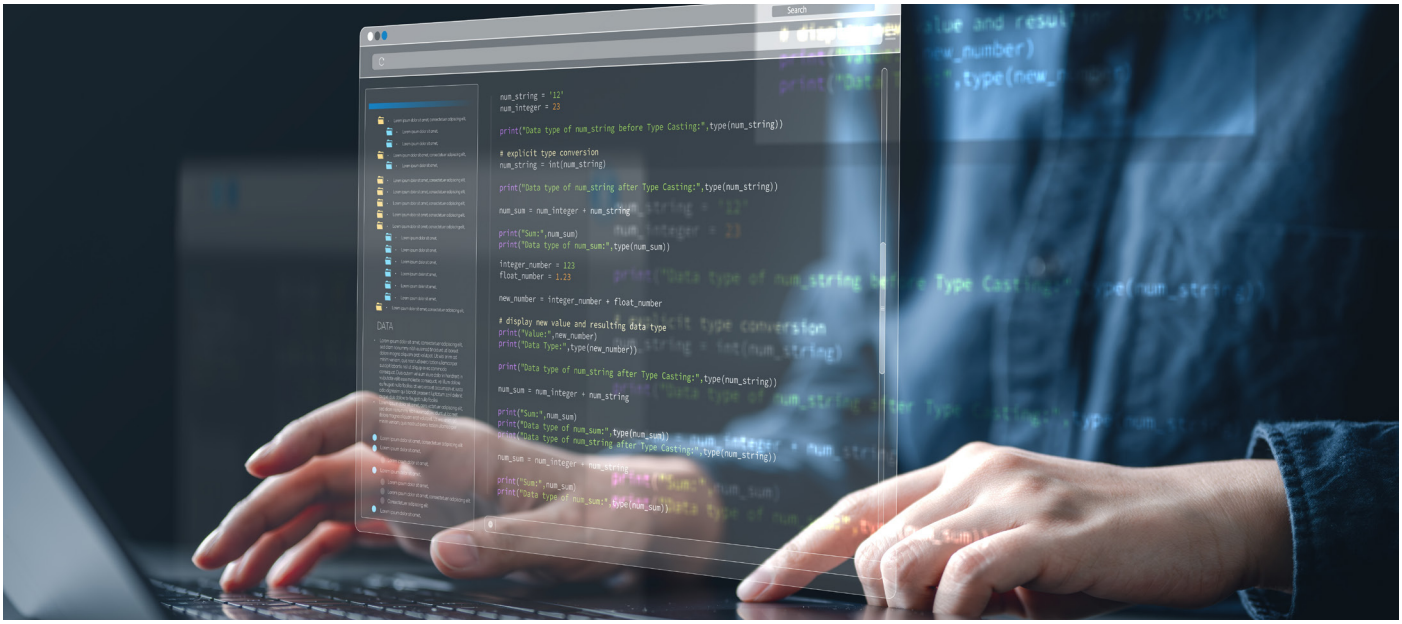
Automate login macros. Scale authenticated DAST.

OpenText™ Fortify™ DAST Aviator™ uses AI to automatically generate login macros, removing manual scripting and enabling authenticated DAST at DevSecOps scale.



Benefits

- Macro generation in seconds, not hours
- No scripting, no manual recording
- Parameterized macros for CI/CD at scale
- Credentials stay in your environment

As AI-assisted development accelerates code delivery, security teams face mounting pressure to scan every application in production. Authenticated dynamic application security testing (DAST) is the only way to uncover vulnerabilities behind a login. Yet creating login macros has long been one of the most time-consuming, error-prone, and manual steps in the DAST workflow.

AI-driven login macro generation

Fortify™ DAST Aviator™ removes the macro creation bottleneck entirely. Security teams provide a target URL, credentials, and optional MFA. An LLM browser agent, built on the proven object-detection capabilities of TruClient, analyzes the authentication flow for each unique application, identifies required fields, handles redirects, and builds a fully structured login macro using DOM, JavaScript, and image recognition. The result is a reusable, parameterized macro, generated in seconds and ready to attach to a scan.

Built for DevSecOps scale

Generated macros are parameterized, so credentials can be updated without recreating the macro. This is a critical feature for credential rotation and multi-environment scanning. Macros integrate directly into Fortify ScanCentral DAST and Software Security Center (SSC), drop into existing CI/CD pipelines, and scale horizontally with your scanning infrastructure. No external tooling. No specialized scripting knowledge. No manual recording.

Enterprise-grade data handling

Fortify DAST Aviator is engineered for regulated environments. Credentials never leave the customer environment—they are not transmitted to the underlying large language model or to any OpenText-hosted service. Beyond control and metric data, such as accounts, licenses, and usage telemetry, no application data is retained. Security teams get the benefits of AI automation without compromising their compliance posture.

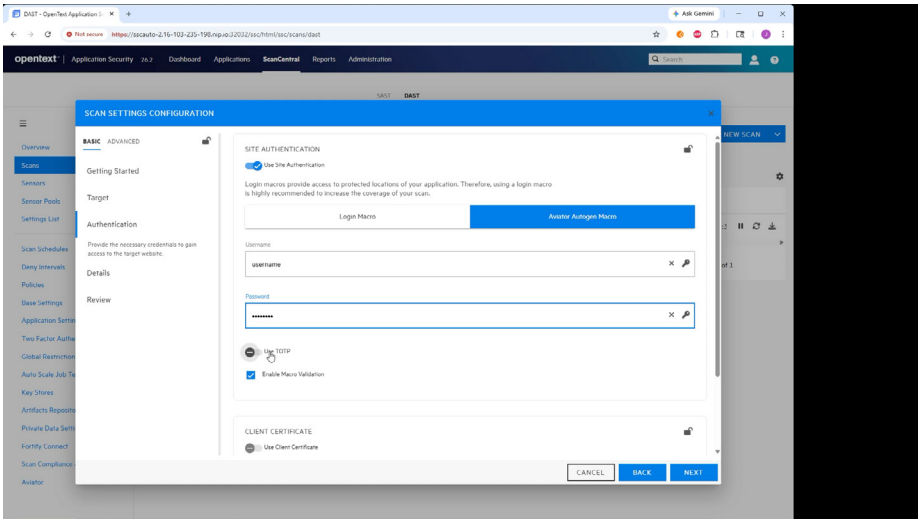
Feature	Description
AI macro generation	Uses a multi-model LLM to simulate human user actions and drive a recording of a macro without human intervention.
Built on TruClient	Object detection and action execution are powered by TruClient capabilities, driven by the LLM for accurate flow navigation.
Parameterized credentials	Update credentials without regenerating the macro. Supports credential rotation and multi-environment scanning.
TOTP support	Handles modern authentication flows including time-based one-time passwords. Optionally accepts a QR code or TOTP secret at setup.
Native Fortify integration	Built into Fortify ScanCentral DAST and Software Security Center. No external tooling required.
CI/CD ready	Parameterized macros plug directly into automated pipelines for continuous authenticated scanning at DevSecOps scale.
Isolated credential handling	Credentials remain in the customer environment and are never sent to the underlying LLM or to any OpenText-hosted service.

Resources

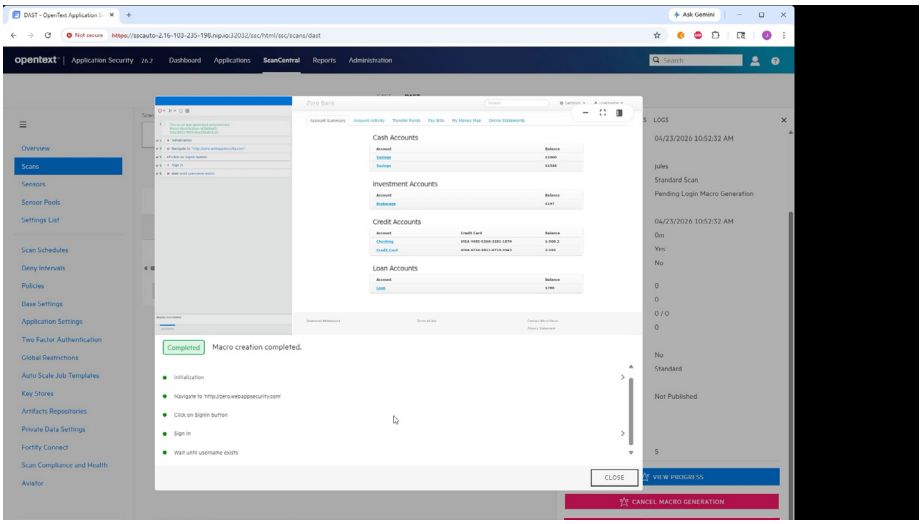
OpenText Fortify DAST ›

View demo video ›

Fortify AppSec portfolio ›



Configuring authentication in OpenText Fortify DAST Aviator



Macro generation complete

Authenticated DAST is no longer optional. Every application behind a login needs it. With Fortify DAST Aviator, OpenText eliminates the single biggest barrier to running DAST at scale, bringing AI-powered automation to the dynamic testing side of the application security lifecycle. Fortify DAST Aviator is part of the broader Fortify portfolio, the industry's most trusted application security suite and a Leader in the Gartner® Magic Quadrant™ for Application Security Testing for the 11th year in a row. It extends AI-native capabilities from static analysis and remediation through to dynamic testing.

opentext™