



Release Notes

FortiDAST 25.2.0



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO LIBRARY

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD LABS

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com

May 09, 2025

FortiDAST 25.2.0 Release Notes

67-252-1155811-20250509

TABLE OF CONTENTS

- Change log 4**
- Introduction 5**
- Product integration and support 7**
- What's new 8**
- Known issues 9**
- Resolved issues 10**

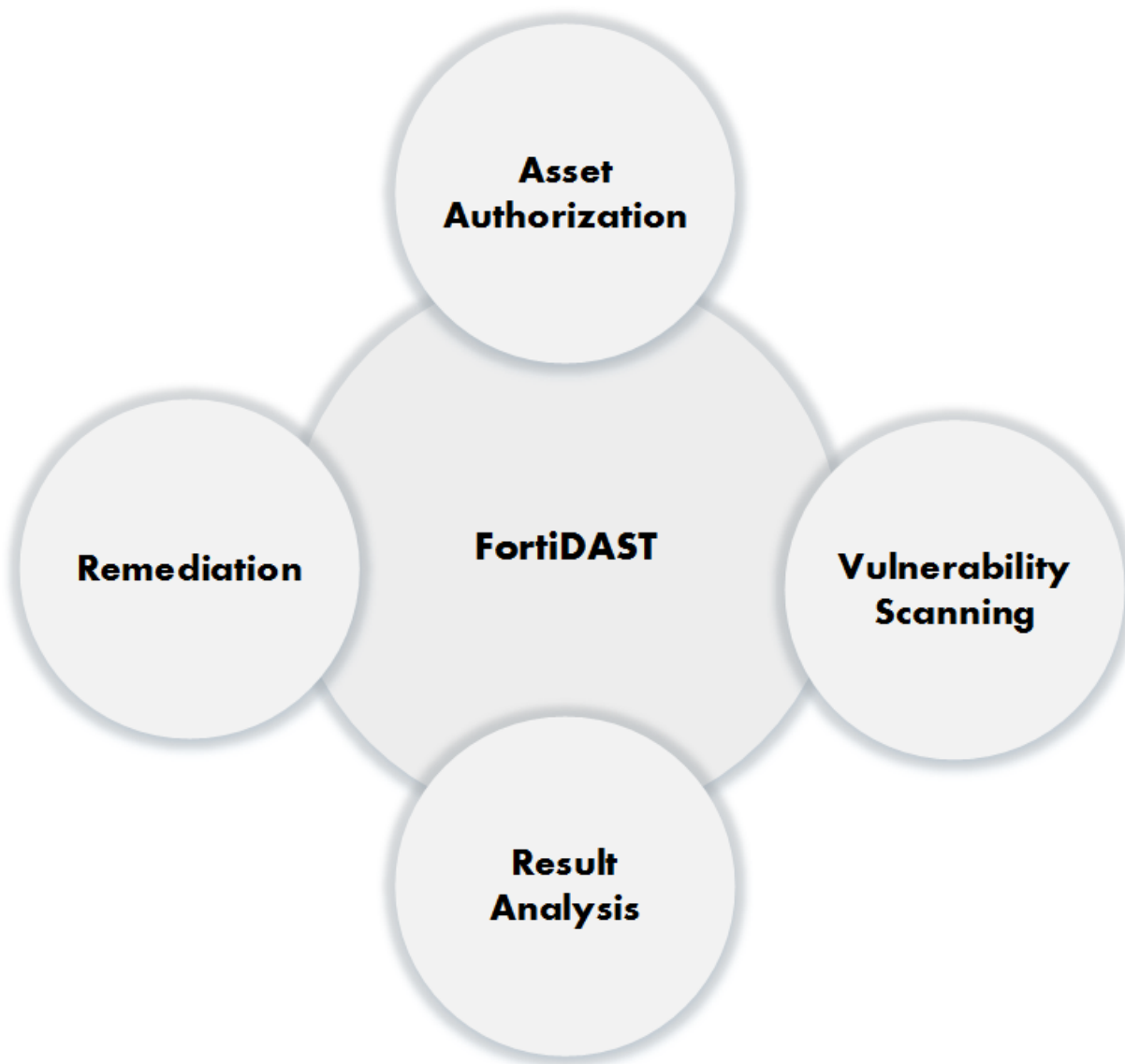
Change log

Date	Change description
2025-05-09	FortiDAST version 25.2.0 release document.

Introduction

FortiDAST is a cloud enabled service that performs vulnerability assessment and penetration testing through an intensive process of comprehensive and criteria based automated scanning and analysis. It adopts an organised technical approach of assessing your web applications running in an HTTP/HTTPS environment, to identify loopholes and vulnerabilities. Penetration testing (pen-testing) is the process to explore and exploit security vulnerabilities in an application using various malicious techniques to discover security gaps; securing your network and assisting in suitable remediation steps for the identified susceptibilities.

The goal of FortiDAST is to provide an easy-to-understand and non-intrusive evaluation of the security posture of your web applications. The outcome is an accurate and detailed vulnerability assessment report with a high vulnerability detection rate that facilitates appropriate measures for remediation and further network penetration testing.



This diagram lays down the building blocks of the FortiDAST vulnerability assessment and penetration testing service.

This document provides a list of new features and product integration information for FortiDAST version 25.2.0. Review all sections of this document before you use this service.

Product integration and support

The following table lists the latest supported/tested web browsers for FortiDAST version 25.2.0:

Item	Supported version
Web browser	• Microsoft Edge version 136.0.3240.50 (Official build) (64-bit) • Mozilla Firefox version 138.0.1 (64-bit) • Google Chrome version 136.0.7103.49 (Official Build) (64-bit) Other web browsers may work correctly but Fortinet does not support them.

What's new

The following table lists new features in FortiDAST version 25.2.0.

Feature	Description
Forced Browsing Enhancement	FortiDAST now expands forced browsing capabilities to include new technologies, improving scan accuracy when testing for access to restricted resources.
Context-sensitive Help	FortiDAST now includes direct links to relevant help content on every page. This provides quick and easy access to the information you need.
Feedback	FortiDAST now includes a feedback system across the platform. Share your ratings and comments to help us identify areas for improvement and enhance your experience.
Exploit Engine	Detection of additional CVEs is supported.

Known issues

The following issues are known in FortiDAST version 25.2.0. For inquiries about a particular issue, visit the [Fortinet Support](#) website.

Issue ID	Description
646320	Password protected reports do not have working links.
693579	The FortiWeb compatible reports contain Sensitive Data Exposure errors for queries blocked by FortiWeb.
820470	Modules that need to return the WAF Headers are not returning HTTP request headers.
820908	Partial URI rescan stops abruptly.
819333	Scans scheduled monthly are not working.
874324	[FortiDAST Proxy] C2 server is not working for FSE scripts.
876384	Failure in detecting Atlassian Jira and Confluence outbreak when using proxy in the Google Cloud Platform (GCP) configuration.
896907	False positive result for CSRF vulnerability.
860824	The FortiDAST plugin for Jenkins integration is unavailable for download through the Jenkins plugin manager
1137618	UI alignment issues occur when <i>Scans Policy > Automation</i> is clicked. To resolve refresh the page.

Resolved issues

The following issues have been resolved in FortiDAST version 25.2.0. For inquiries about a particular issue, visit the [Fortinet Support](#) website.

Issue ID	Description
1149778	Quick scans may fail with an <i>ERR_TEMP_DNS_LOOKUP</i> error when the target URL includes a <i>www</i> subdomain.
1141728	Sub-user accounts may be unable to log in to FortiDAST.

