

Release Notes

FortiRecon 25.4.0



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

November 27, 2025

FortiRecon 25.4.0 Release Notes

75-254-1229894-20251127

TABLE OF CONTENTS

Change log	4
Introduction	5
What's new	7

Change log

Date	Change Description
2025-11-27	Initial release of 25.4.0.

Introduction

FortiRecon is a Digital Risk Protection (DRP) service that operates alongside existing security solutions to provide you with the visibility that an adversary can have of your infrastructure. This early warning of any malicious activity targeted at your organization enables swift detection and mitigation. Operating purely from outside the organizational boundary, the service maps an organization's digital footprint and monitors it for abnormal activity. The service gives organizations the intelligence to mitigate credible security threats in a controlled manner as part of ongoing security efforts.

FortiRecon scans the organization's attack surface and identifies risks to assets while FortiGuard Threat Intelligence delivers early warning of risks to the organization through targeted, curated intelligence to provide an early warning of any malicious activity targeted to the organization.

The FortiRecon portal includes the following modules:

Overview	The <i>Overview</i> module provides a centralized view of your organization's digital risk posture across <i>Attack Surface Management (ASM)</i> , <i>Brand Protection (BP)</i> , and <i>Adversary Centric Intelligence (ACI)</i> modules. Discovered issues are mapped to relevant MITRE ATT&CK techniques and sub-techniques, providing a valuable framework for understanding attacker motivations and potential attack paths.
Attack Surface Management	<p>The <i>External Attack Surface Management (EASM)</i> module provides an adversary's view of the organization digital attack surface and prioritizes risks and exposures, enabling administrators to mitigate threats in a controlled manner before the threats become a problem.</p> <p>The <i>Internal Attack Surface Management (IASM)</i> module provides visibility into internal network, identifying vulnerabilities within the organization's perimeter. It helps administrators discover internal assets, assess associated risks, and take mitigation steps.</p>
Brand Protection	The <i>Brand Protection (BP)</i> module continually monitors the organization's public-facing visibility for unauthorized changes, including web-based phishing attacks, typo-squatting, rogue applications, credential leaks, and brand impersonation in social media, which may impact brand value, integrity, and trust.
Adversary Centric Intelligence	The <i>Adversary Centric Intelligence (ACI)</i> module leverages FortiGuard Threat Analysts to provide comprehensive coverage of dark web, open source, and technical threat intelligence, including threat actor insights. This information enables administrators to proactively assess risks, respond faster to incidents, better understand their attackers, and protect assets.
Security Orchestration	The <i>Security Orchestration</i> module helps you investigate and respond to security threat findings from Attack Surface Management, Brand Protection, and Adversary Centric Intelligence. This solution reduces the time responders require to prioritize and take appropriate actions by automating and streamlining security workflows. It provides preconfigured playbooks to help you get started quickly. You can also create playbooks using connectors, add playbook variables, and view execution logs. Install and connect agents if required.

Profile Settings

The Profile Settings module allows you to personalize your FortiRecon account and provide information on your organization.

For details, see the [FortiRecon User Guide](#).

What's new

The following new features and enhancements are included in the FortiRecon 25.4.0 release.

Module	Feature	Description
Attack Surface Management	Web Application Assessment	You can now export the vulnerability details list for the selected asset to CSV from the <i>Attack Surface Management > Web Application Assessment</i> page.
	Leaked Credentials	Administrators can now view associated passwords within leaked credentials details in <i>Attack Surface Management > Leaked Credentials</i> page.
Adversary Centric Intelligence	Intelligence Collection Lookup	The <i>Cyber-Crime Forum Posts</i> tab now includes content from various threat marketplaces.
Profile Settings	Audit Logs	<ul style="list-style-type: none">The <i>Audit Logs</i> page now displays the source IP address for all user login entries.The <i>More Information</i> window now includes entity details for log entries.Audit logs now include entries for failed or bounced email notifications.

