

Release Notes

FortiRecon 24.4.b



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<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>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdoc@fortinet.com

December 19, 2024

FortiRecon 24.4.b Release Notes

75-244-1108936-20241219

TABLE OF CONTENTS

Change log	4
FortiRecon 24.4.b release	5
What's new	6

Change log

Date	Change Description
2024-12-19	Initial release of 24.4.b.

FortiRecon 24.4.b release

FortiRecon version 24.4.b is available.

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 External Attack Surface Management (EASM) 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 Internal Attack Surface Management (IASM) 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 Brand Protection (BP) 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 Adversary Centric Intelligence (ACI) 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.
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 24.4.b release.

Feature	Description
Reports	The <i>Adversary Centric Intelligence > Reports</i> page has been consolidated to include <i>Analyst Curated</i> , <i>Automated</i> , and <i>AI Insight</i> reports. Additionally, the new <i>FortiAI Assistant</i> has been added to provide AI-powered insights based on user queries about cybersecurity trends and insights, as well as to summarize reports.
Security Issues	The <i>Attack Surface Management > Security Issues</i> page now displays brief descriptions for identified CVEs.

