# Release Notes

**FortiRecon 26.1.0**

**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

February 20, 2026
FortiRecon 26.1.0 Release Notes
75-261-1254425-20260220

# TABLE OF CONTENTS

# Change log

| Date | Change Description |
| --- | --- |
| 2026-02-20 | Initial release of 26.1.0. |

# 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 *Overview* module provides a centralized view of your organization's digital risk posture across *Attack Surface Management (ASM)*, *Brand Protection (BP)*, and *Adversary Centric Intelligence (ACI)* 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 | 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. |
| | 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. |
| 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. |

| | |
|---|---|
| Security Orchestration | The *Security Orchestration* 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. |

# What's new

The following new features and enhancements are included in the FortiRecon 26.1.0 release.

| Module | Feature | Description |
|---|---|---|
| **FortiRecon Portal** | Support for External IdPs | FortiRecon now supports external identity providers (IdPs). You can configure external IdPs to allow users to sign in to FortiRecon portal using their existing corporate credentials. |
| | Licensing: Security Orchestration Playbooks Add-on | You can now purchase a new stackable *Security Orchestration Playbooks Add-on* license to increase your monthly playbook capacity. Each add-on license provides *2000* playbooks per month. By default, all FortiRecon solution bundles include *100* playbooks per month. |
| **Attack Surface Management (ASM) > Web Application Assessment** | Proof of Exploit | The *Web Application Assessment* page now includes *Proof of Exploit* details for supported vulnerability categories. These details include vulnerability description, endpoint request and response data, and a preview of the response body. |
| | WAF detection | The *Web Application Assessment* page now detects the presence of *Web Application Firewalls (WAF)* and displays warnings based on the WAF status and identified injection vulnerabilities. |
| | Vulnerability review | You can now review vulnerabilities on the *Web Application Assessment* page and update their status. This feature supports bulk actions and provides status categories such as *Active*, *Resolved*, *Risk Accepted*, and *False Positive*. |
| | Enhanced CSV Export | The vulnerability download file now includes a *Description* column. For known vulnerabilities, this column also specifies the affected library name and version. |

| Module | Feature | Description |
|---|---|---|
| **Attack Surface Management (ASM) > Internal Attack Surface Management (IASM)** | Automated OT and IoT tagging | FortiRecon now automatically classifies and tags discovered *OT* and *IoT* assets during IASM scans for improved visibility and filtering in the *ASM* > *Asset Discovery* > *IASM* and *ASM* > *Security Issues* > *IASM* pages. |
| | IASM Agent and Proxy auto-upgrade | FortiRecon now supports automatic upgrades for *IASM Agents* and *Proxy* binaries for all minor version updates. The system automatically updates the agents to the latest version. |
| **Attack Surface Management (ASM) > External Attack Surface Management (EASM)** | HTTP Header | EASM scan requests now include the *X-Fr-Scanner* HTTP header to help you distinguish FortiRecon traffic from other network activity. The header value is an *MD5* hash of your unique *Organization ID*, allowing you to recognize and permit these requests. |
| **Profile Settings** | Access Templates | The *Profile Settings* > *Access Templates* page now includes permission settings for the *Web Application Assessment* and *Security Orchestration*. |
| **User Interface** | UI enhancements | The following UI enhancements have been added.<br>• On the *Brand Protection* > *Domain Threats* page you can now use the *Copy* button to quickly copy domains. A new *Actions* menu has also been added to the threat list.<br>• A new *Release Notification* window displays the latest features upon login. You can also access this information, along with links to the *User Guide* and *Release Notes*, via the new *Help* icon in the top navigation bar. |

For details, see the FortiRecon User Guide.

www.fortinet.com