Release Notes

FortiProxy 7.6.3

October 15, 2025
FortiProxy 7.6.3 Release Notes
45-763-1143188-20251015

TABLE OF CONTENTS

Change log

Date	Change Description
2025-04-09	Initial release.
2025-04-10	Updated What's new on page 7.
2025-06-10	Added CVE-2025-22862 to Resolved issues on page 18.
2025-06-18	Added ticket 1159963 to Known issues on page 22.
2025-08-13	Added CVE-2025-25248 to Resolved issues on page 18.
2025-10-15	Added CVE-2025-57740 and CVE-2025-22862 to Resolved issues on page 18.

Introduction

FortiProxy delivers a class-leading Secure Web Gateway, security features, unmatched performance, and the best user experience for web sites and cloud-based applications.

FortiProxy 7.6.3 supports upgrade from 7.4.x or 7.6.x only. Refer to Deployment information on page 14 for detailed upgrade instructions.

All FortiProxy models include the following features out of the box:

Security modules

The unique FortiProxy architecture offers granular control over security, understanding user needs and enforcing Internet policy compliance with the following security modules:

Web filtering	The web-filtering solution is designed to restrict or control the content a reader is authorized to access, delivered over the Internet using the web browser. The web rating override allows users to change the rating for a web site and control access to the site without affecting the rest of the sites in the original category.
DNS filtering	Similar to the FortiGuard web filtering. DNS filtering allows, blocks, or monitors access to web content according to FortiGuard categories.
Email filtering	The FortiGuard Antispam Service uses both a sender IP reputation database and a spam signature database, along with sophisticated spam filtering tools on Fortinet appliances and agents, to detect and block a wide range of spam messages. Updates to the IP reputation and spam signature databases are provided continuously by the FDN.
CIFS filtering	CIFS UTM scanning, which includes antivirus file scanning and DLP file filtering.
Application control	Application control technologies detect and take action against network traffic based on the application that generated the traffic.
Inline CASB	The inline CASB security profile enables the FortiProxy to perform granular control over SaaS applications directly on policies.
Data Loss Prevention (DLP)	The FortiProxy DLP system allows you to prevent sensitive data from leaving your network.

Antivirus	Antivirus uses a suite of integrated security technologies to protect against a variety of threats, including both known and unknown malicious codes (malware), plus Advanced Targeted Attacks (ATAs), also known as Advanced Persistent Threats (APTs).
SSL/SSH inspection (MITM)	SSL/SSH inspection helps to unlock encrypted sessions, see into encrypted packets, find threats, and block them.
Intrusion Prevention System (IPS)	IPS technology protects your network from cybercriminal attacks by actively seeking and blocking external threats before they can reach potentially vulnerable network devices.
Zero Trust Network Access (ZTNA)	ZTNA is an access control method that uses client device identification, authentication, and Zero Trust tags to provide role-based application access. It gives administrators the flexibility to manage network access for users. Access to applications is granted only after device verification, authenticating the user's identity, authorizing the user, and then performing context based posture checks using Zero Trust tags.
Content Analysis	Content Analysis allow you to detect adult content images in real time. This service is a real-time analysis of the content passing through the FortiProxy unit.
Client-based native browser isolation (NBI)	Client-based native browser isolation (NBI) uses a Windows Subsystem for Linux (WSL) distribution (distro) to isolate the browser from the rest of the computer in a container, which helps decrease the attack surface.

Caching and WAN optimization

All traffic between a client network and one or more web servers is intercepted by a web cache policy. This policy causes the FortiProxy unit to cache pages from the web servers on the FortiProxy unit and makes the cached pages available to users on the client network. Web caching can be configured for standard and reverse web caching.

FortiProxy supports WAN optimization to improve traffic performance and efficiency as it crosses the WAN. FortiProxy WAN optimization consists of a number of techniques that you can apply to improve the efficiency of communication across your WAN. These techniques include protocol optimization, byte caching, SSL offloading, and secure tunneling.

Protocol optimization can improve the efficiency of traffic that uses the CIFS, FTP, HTTP, or MAPI protocol, as well as general TCP traffic. Byte caching caches files and other data on FortiProxy units to reduce the amount of data transmitted across the WAN.

FortiProxy is intelligent enough to understand the differing caching formats of the major video services in order to maximize cache rates for one of the biggest contributors to bandwidth usage. FortiProxy will:

- Detect the same video ID when content comes from different CDN hosts.
- Support seek forward/backward in video.
- Detect and cache separately; advertisements automatically played before the actual videos.

What's new

The following sections describe new features, enhancements, and changes in FortiProxy 7.6.3:

- Traffic shaping based on HTTP response on page 7
- OIDC enhancements on page 7
- ZTNA web portal enhancements on page 8
- Support for Securosys Primus HSM on page 8
- Support SHA-256 for digest authentication method on page 9
- Increase proxy-address configuration limit on page 9
- CLI changes on page 9

Traffic shaping based on HTTP response

FortiProxy 7.6.3 introduces the new response shaping policy, which is a specialized type of traffic shaping policy that works on the top of a traffic shaping policy to further match the traffic based on certain HTTP response header fields. When *Http Response Match* is enabled in a traffic shaping policy, any traffic that matches the traffic shaping policy is further evaluated against the list of response shaping policies. If a match is found, the traffic will be mapped to the traffic shaper or assigned to the class defined in the response shaping policy instead of the ones defined in the original matching traffic shaping policy.

See Traffic shaping based on HTTP response in the Administration Guide for an end-to-end configuration example.

OIDC enhancements

FortiProxy 7.6.3 includes the following enhancements to OIDC:

- **Support for multiple OIDC identity providers (IdPs) in one authentication scheme**
  When multiple IdPs are configured, users can select which IdP to use in the OIDC landing page, allowing for flexible authentication across different user groups. This feature is useful in the following scenarios:
  - The organization manages multiple IdPs for different user sets (e.g., Azure AD for employees, Google Identity for contractors).
  - A transition between identity providers is required (e.g., migrating from Okta to Azure AD).
  - Users need to choose their preferred IdP for authentication.
- **Support private and public key pairs during authentication communication between FortiProxy and the cloud IdP**
  FortiProxy generates a private key, uploads the public key to the IdP, and authenticate with JWT using the private key. This is recommended for high-security environments where secret-based

authentication is less desirable.

To do so, use the following new CLI options under `config user oidc`:

```
config user oidc
   edit <name>
      set auth-type private-key
      set auth-method private_key_jwt
      set private-key {string}
   next
end
```

- **Authentication with FortiAuthenticator groups**—You can now configure the OIDC server to be FortiAuthenticator using the group attribute name.
- **Disabling HTTPS certificate verification**—You can now configure FortiProxy to disable HTTPS certificate verification during OIDC authentication using the new `set verify-cert` subcommand under `config user oidc`.

ZTNA web portal enhancements

FortiProxy 7.6.3 includes the following enhancements to ZTNA agentless web-based application access:

- **Dynamic bookmarks using SAML attributes**—Administrators can define dynamic bookmarks to generate personalized application shortcuts using a SAML attribute within the user's SAML account so that bookmarks are auto-populated with the values defined in that attribute instead of static pre-defined IP or hostnames.
- **New login method using OIDC**—You can now log into the ZTNA web portal using OIDC.

Support for Securosys Primus HSM

FortiProxy 7.6.3 adds support for Securosys Primus HSM.

- Under `config system nethsm`, you can now configure the HSM vendor to be Securosys Primus and then configure the Primus-related settings:

```
config system nethsm
```

```
   set status enable
   set vendor primus
   set primus-cfg <primus.cfg file content>
   set secret-content <Encrypted Config>
   config partitions
      edit "PRIMUSDEV270"
         set slot-id 1
         set pkcs11-pin <Encrypted password>
   next
```

```
end
```

- When configuring local keys and certificates using the `config vpn certificate local` command, you can now configure the HSM vendor to be Securosys Primus HSM and configure the HSM key type.
- You can perform operations on Primus HSM using the new `execute nethsm primus` command.

Support SHA-256 for digest authentication method

FortiProxy 7.6.3 adds support for SHA-256, which is mandatory in RFC 7616.

To configure the digest algorithm to be SHA-256:

```
config authentication scheme
   edit "digest-scheme"
      set method digest
      set fsso-guest disable
      set digest-algo md5 sha-256
   next
end
```

Increase proxy-address configuration limit

FortiProxy 7.6.3 includes the following changes to the proxy-address configuration limit for VM04 and VM08:

Proxy address object	New configuration limit for 7.6.3
Proxy Address Object	80K
Proxy Address Group	4096
Proxy Address Group Member	30K

CLI changes

FortiProxy 7.6.3 includes the following CLI changes:

- `config system global`—Use the new `set tcp-random-source-port` subcommand to enable or disable (default) TCP IPv4 random source port.
- `config webfilter urlfilter`—Use the new `set include-subdomains` subcommand to enable (default) or disable (default) matching subdomains.

- `config vpn certificate local`—This command adds support for Securosys Primus HSM with the following changes:
  - Use the new `hsm-vendor` subcommand to configure the HSM vendor.

safenet	Safenet HSM.
primus	Securosys Primus HSM.

  - Use the new `hsm-keytype` subcommand to configure the HSM key type.

rsa	RSA key type.
ec	EC key type.

  - The `nethsm-slot` command is renamed `hsm-slot`.
  - The `execute nethsm` command is renamed `execute nethsm safenet`.

    Use the new `execute nethsm primus` command to perform operations on Primus HSM with the following options:

    ```
    # execute nethsm primus
       clear-pkcs-provider-log Clear logs from /tmp/pkcs11.log, generated by pkcs11.so, the
             OpenSSL provider.
       clear-primus-log Clear logs from /tmp/primus.log, generated by libprimusP11.so.
       delete-object Delete Hardware Security Module object(s).
       dump-pkcs-provider-log Dump logs from /tmp/pkcs11.log, generated by pkcs11.so, the
             OpenSSL provider.
       dump-primus-log Dump logs from /tmp/primus.log, generated by libprimusP11.so.
       inspect-primus-library-info Display information about the integrated libprimusP11.so
             library.
       list-objects List Hardware Security Module objects.
       upload-primus-cfg Upload nethsm primus.cfg file.
       upload-primus-cfg-raw Upload nethsm primus.cfg file.
    ```

  - `config system nethsm`—The `set vendor` parameter includes the new `primus` option to configure the HSM vendor to be Securosys Primus. You can then configure the Primus-related settings:

    ```
    config system nethsm
       set status enable
       set vendor primus
       set primus-cfg <primus.cfg file content>
       set secret-content <Encrypted Config>
       config partitions
          edit "PRIMUSDEV270"
             set slot-id 1
             set pkcs11-pin <Encrypted password>
       next
    end
    ```

- `config vpn certificate hsm-local`—The `set gch-cryptokey-algorithm` subcommand includes the following new options:

Option	Description
rsa-sign-pss-3072-sha256	3072 bit RSA - PSS padding - SHA256 Digest.

Option	Description
rsa-sign-pss-4096-sha256	4096 bit RSA - PSS padding - SHA256 Digest.
rsa-sign-pss-4096-sha512	4096 bit RSA - PSS padding - SHA256 Digest.
ec-sign-p256-sha256	Elliptic Curve P-256 - SHA256 Digest.

- `config icap remote-server` and `config user ldap`—The `set validate-server-certificate` subcommand is removed.
- `diagnose wad worker oidc refresh-server`—Use this new command to manually refresh OIDC discovery servers.

  The automatic refresh rate is once per minute for servers in error state and once per hour for servers in ready state.

Product integration and support

The following table lists product integration and support information for FortiProxy 7.6.3 build 1559:

Type	Product and version
FortiProxy appliance	• FPX-400E • FPX-2000E • FPX-4000E • FPX-400G • FPX-2000G • FPX-4000G
FortiProxy VM	• FPX-AZURE • FPX-HY • FPX-KVM • FPX-KVM-ALI • FPX-KVM-AWS • FPX-KVM-GCP • FPX-KVM-OPC • FPX-VMWARE • FPX-XEN
Fortinet products	• FortiOS 6.x and 7.0 to support the WCCP content server • FortiOS 6.0 and 7.0 to support the web cache collaboration storage cluster • FortiManager - See the FortiManager Release Notes. • FortiAnalyzer - See the FortiAnalyzer Release Notes. • FortiSandbox and FortiCloud FortiSandbox- See the FortiSandbox Release Notes and FortiSandbox Cloud Release Notes. • FortiIsolator 2.2 and later - See the FortiIsolator Release Notes.
Fortinet Single Sign-On (FSSO)	5.0 build 0301 and later (needed for FSSO agent support OU in group filters) • Windows Server 2019 Standard • Windows Server 2019 Datacenter • Windows Server 2019 Core • Windows Server 2016 Datacenter • Windows Server 2016 Standard • Windows Server 2016 Core • Windows Server 2012 Standard • Windows Server 2012 R2 Standard • Windows Server 2012 Core

<table>
<tr><th>Type</th><th>Product and version</th></tr>
<tr><td></td><td>
- Windows Server 2008 64-bit (requires Microsoft SHA2 support package)
- Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package)
- Windows Server 2008 Core (requires Microsoft SHA2 support package)
- Novell eDirectory 8.8
</td></tr>
<tr><td><b>Web browsers</b></td><td>
- Microsoft Edge
- Mozilla Firefox version 87
- Google Chrome version 89
Other web browsers may work correctly, but Fortinet does not support them.
</td></tr>
<tr><td><b>Virtualization environments</b></td><td>
Fortinet recommends running the FortiProxy VM with at least 4 GB of memory because the AI-based Image Analyzer uses more memory compared to the previous version.
<table>
<tr><td><b>Hyper-V</b></td><td>- Hyper-V Server 2008 R2, 2012, 2012R2, 2016, 2019, and 2022</td></tr>
<tr><td><b>Linux KVM</b></td><td>- RHEL 7.1/Ubuntu 12.04 and later
- CentOS 6.4 (qemu 0.12.1) and later</td></tr>
<tr><td><b>Xen hypervisor</b></td><td>- OpenXen 4.13 hypervisor and later
- Citrix Hypervisor 7 and later</td></tr>
<tr><td><b>VMware</b></td><td>- ESXi versions 6.5, 6.7, 7.0, and 8.0</td></tr>
<tr><td><b>Openstack</b></td><td>- Ussuri</td></tr>
<tr><td><b>Nutanix</b></td><td>- AHV</td></tr>
</table>
</td></tr>
<tr><td><b>Cloud platforms</b></td><td>
- AWS (Amazon Web Services)
- Microsoft Azure
- GCP (Google Cloud Platform)
- OCI (Oracle Cloud Infrastructure)
- Alibaba Cloud
</td></tr>
</table>

Deployment information

You can deploy the FortiProxy on a FortiProxy unit or VM. You can also upgrade or downgrade an existing FortiProxy deployment. Refer to Product integration and support on page 12 for a list of supported FortiProxy units and VM platforms.

Downloading the firmware file

1. Go to https://support.fortinet.com.
2. Click *Login* and log in to the Fortinet Support website.
3. From the *Support > Downloads* menu, select *Firmware Download*.
4. In the *Select Product* dropdown menu, select *FortiProxy*.
5. On the *Download* tab, navigate to the FortiProxy firmware file for your FortiProxy model or VM platform in the *Image Folders/Files* section. `.out` files are for upgrade or downgrade. `.zip` and `.gz` files are for new deployments.
6. Click *HTTPS* to download the firmware that meets your needs.

Deploying a new FortiProxy appliance

Refer to the FortiProxy QuickStart Guide for detailed instructions of deploying a FortiProxy appliance. Refer to Product integration and support on page 12 for a list of supported FortiProxy units.

Deploying a new FortiProxy VM

Refer to the FortiProxy Public Cloud or FortiProxy Private Cloud deployment guides for more information about how to deploy the FortiProxy VM on different public and private cloud platforms. Refer to Product integration and support on page 12 for a list of supported VM platforms.

Upgrading the FortiProxy

FortiProxy 7.6.3 supports upgrade from 7.4.x or 7.6.x.

If Security Fabric is enabled, all FortiProxy units must be upgraded to the same version. For example, if Security Fabric is enabled in FortiProxy 7.6.3, all FortiProxy devices in the Security Fabric must run FortiProxy 7.6.3. Otherwise, some devices may get stale or disconnected from the root, resulting in issues with fabric logging and address synchronization.

To upgrade FortiProxy units or VMs from 7.4.x to 7.6.3:

1. Reboot the FortiProxy.

   You must reboot the FortiProxy before the upgrade process. Otherwise, the device may be damaged due to upgrade failure during critical processing.

2. In the GUI, go to *System > Fabric Management*.
3. Select the device you want to upgrade in the table and click *Upgrade*.
4. Click *Browse* in the *File Upload* tab.
5. Select the file on your PC and click *Open*.
6. Click *Confirm and Backup Config*.
7. Click *Continue*.

   The configuration file is automatically saved and the system will reboot.
8. Click *Reset All Dashboards* in the GUI to avoid any issues with FortiView.

If you are currently using FortiProxy 7.0.x or 7.2.x, Fortinet recommends that you perform the upgrade procedure for each major version in between from low to high before attempting to upgrade to 7.6.3. For example, to upgrade from 7.0.17 to 7.6.3, upgrade to 7.2.5 or later first (reboot before upgrading to 7.2.x), and then 7.4.x, and then 7.6.3.

Upgrading a FortiProxy 2.0.5 VM to 7.0.x requires a different upgrade process with additional backup and configuration as FortiProxy 2.0.6 introduced a new FortiProxy VM license file that cannot be used by earlier versions of the FortiProxy VM.

To upgrade a FortiProxy 2.0.5 VM to 7.0.x:

1. Back up the configuration from the GUI or CLI. Make sure the VM license file is stored on the PC or FTP or TFTP server.
2. Shut down the original VM.
3. Deploy the new VM. Make sure that there is at least 4 GB of memory to allocate to the VM.
4. From the VM console, configure the interface, routing, and DNS for GUI or CLI access to the new VM and its access to FortiGuard.
5. Upload the VM license file using the GUI or CLI.
6. Restore the configuration using the CLI or GUI.
7. Click *Reset All Dashboards* in the GUI to avoid any issues with FortiView.

Downgrading the FortiProxy

Downgrading FortiProxy 7.6.3 to previous firmware versions results in configuration loss on all models. Only the following settings are retained:

- operation mode
- interface IP/management IP
- static route table
- DNS settings
- admin user account
- session helpers
- system access profiles

If Security Fabric is enabled, all FortiProxy units must be downgraded to the same version. For example, if Security Fabric is enabled in FortiProxy 7.6.3, all FortiProxy devices in the Security Fabric must run FortiProxy 7.6.3. Otherwise, some devices may get stale or disconnected from the root, resulting in issues with fabric logging and address synchronization.

You can downgrade FortiProxy units or VMs from 7.6.3 to 7.4.x by following the steps below:

1. In the GUI, go to *System > Fabric Management*.
2. Select the device you want to upgrade in the table and click *Upgrade*.
3. Click *Browse* in the *File Upload* tab.
4. Select the file on your PC and click *Open*.
5. Click *Confirm and Backup Config*.
6. Click *Continue*.

The configuration file is automatically saved and the system will reboot.

7. Click *Reset All Dashboards* in the GUI to avoid any issues with FortiView.

To downgrade from FortiProxy 7.6.3 to 7.2.x or 7.0.x, Fortinet recommends that you perform the downgrade procedure for each major version in between from high to low before attempting to downgrade to the target version. For example, to downgrade from 7.6.3 to 7.0.17, downgrade to 7.4.x first, and then 7.2.5 or later, and then 7.0.

Downgrading a FortiProxy 7.0.x VM to 2.0.5 or earlier requires a different downgrade process with additional backup and configuration as FortiProxy 2.0.6 introduced a new FortiProxy VM license file that cannot be used by earlier versions of the FortiProxy VM.

To downgrade a FortiProxy 7.0.x VM to FortiProxy 2.0.5 or earlier:

1. Back up the configuration from the GUI or CLI. Make sure the VM license file is stored on the PC or FTP or TFTP server.
2. Shut down the original VM.
3. Deploy the new VM. Make sure that there is at least 2 GB of memory to allocate to the VM.
4. From the VM console, configure the interface, routing, and DNS for GUI or CLI access to the new VM and its access to FortiGuard.
5. Upload the VM license file using the GUI or CLI
6. Restore the configuration using the CLI or GUI.
7. Click *Reset All Dashboards* in the GUI to avoid any issues with FortiView.

Resolved issues

The following issues have been fixed in FortiProxy 7.6.3. For inquiries about a particular bug, please contact Customer Service & Support.

Description	Bug ID
1105484, 1110873, 1116906, 1117622, 1118078, 1119366, 1120458, 1122890, 1123775, 1125661, 1126935, 1133638, 1134920, 1136622, 1138133, 1138194, 1143201, 1143616, 1144162, 1144435	GUI issues.
1115120	Incorrect service and URL in AV log when HTTP request via external proxy hit the AV infected URL cache.
1107113	SSL exempt logs "destination" and "destination-interface" fields are not correct.
1118101	ZTNA web portal should not have SSLVPN in the URL.
1118107	Non-HTTP traffic does not bypass application policy with deny and is dropped.
1074460	Crash due to buffer overflow issues related to corrupted traffic log files.
1118408	Crash when executing "dia wad license glob-usage".
1111239	The lock IP address function does not work in explicit proxy mode.
1054835, 1121171	Proxy HTTP2 single file transfer is slow when IPS/APP/SSL inspect-all is enabled.
924740	Improve WAD trace log precision of process-id-by-src filter.
1121444	Create custom SaaS applications for inline CASB causes HA to be out of sync.
1120460	Setting an Internet service as the destination in explicit web policies does not work.
1120660	Integer overflow in ZTNA web portal VNC bookmark.
1126226	FortiProxy OCR with DLP fails to block the uploading of sensitive images.
1080366	The FURL license seat does not control the inline CASB feature.
1122606	When web-auth-cookie is enabled in session-based kerberos authentication, the authentication window still appears after authentication is passed.
1109469	FortiProxy SOCKS5 traffic is denied when detect-https-in-http-request is enabled.
1119389	Explicit proxy does not work via IPsec tunnel.

Description	Bug ID
1103476	License leak.
1110668	Web filter using simple URL entries does not work as expected.
1118000	Crash during authentication with OIDC when no captive portal is set.
1128580	FortiSandbox connection status shows error "Unreachable or not authorized" after upgrade to 7.6.2.
1128371	Register authentication scheme failed.
1125415	Duplicate headers in ZTNA web portal error responses.
1127524	web-proxy forward-server monitor URL does not work with HTTP scheme.
1095093, 1092529	"utmref" and "utmaction" fields are missing in forward traffic log and long-tcp sessions are missing in http-transaction traffic log.
1127033	For a policy with IP pool enabled, IP pool change does not take effect unless you disable and enable IP pool in policy.
1127299	JSON parser returns invalid results.
1056498, 1075806, 1109306, 1110202	Proxy inline IPS performance on HTTP traffic is much worse than the IPS engine.
1071928	Duplicated UTM log when log-http-transaction is enabled.
1128154	"print tablesize" returns the wrong values.
1128283	Logs that should have duration 0 sometimes show wrong values.
1130067	HTTP/2 traffic cannot pass through the explicit-policy when web filter is enabled.
1131180	Error message on console when FPX-4000E is booting.
1034891	IdP applications are failing via SWG.
1129460	On-demand sniffer interface does not support interface names with more than 7 characters.
1045789, 1125827	Dynamic address does not work in transparent policy.
1129510	WANOpt secure-tunnel negotiation failure when PSK is configured.
1110321	Close p2s session if the last response does not support keep-alive.
1110904	Unable to see logs for traffic that matches transparent policy with action DENY.
1130522	wad_p2s_http_ses always use the default port(80/443) even if there is a non-standard port in URL.
1106807	With a configuration that blocks bats.video.yahoo.com, visiting tw.sports.yahoo.com triggers HTTP2 PROTOCOL_ERROR.
1123962	`diag wad policy` list does not show implicit deny/allow policy.

Description	Bug ID
985311, 1121357, 1110850	X-Forwarded-For header in webfilter log and "exec tac report" trace on console.
1133565	Password protected msofficex and msoffice files are bypassed when encrypted-file is set to inspect.
1127004	No automatic refresh for OIDC server, causing error state and recovery issues which can only be fixed by manually restarting the FortiProxy or updating the config.
1112756	Incorrect ztna-proxy and explicit-proxy policy byte information.
1127352	Inline IPS generates duplicate and conflicting app control logs with app list configured to block category 23.
1126749	Duplicate session ID in traffic logs across different connections.
1134204	JSON delete/detach/replace is not case-sensitive on object key.
1126862	Traffic is passed by transparent deny policy when log-http-transaction is enabled.
1137505	If the LDAP returns a user with group "a", it will match group "a1", "a2", which is incorrect.
1102925, 1118853, 1127366, 1131558, 1132833	WAD memory continuous increase due to memory leak.
1096529	WAD crash at wad_ctrl_workers_close_ips_db once.
1135706, 1135863	Domain matching issue caused by the "include_subdomains" flag not being initialized in some cases.
1138575	ZTNA webportal logout does not clear the session's authentication state.
1135253	OIDC should not print client_secret and access_token in log.
1135709	IP set is unable to handle maximum external resource size.
1125699	Inline IPS PCRE pattern matching issues.
1102796	Passive proxy member send LDAP requests to the LDAP servers.
1104821	WAD has signal 6 crash at wad_ftp_data_session_make.
1121249	CASB fails to block the HTTP request when CASB profile is enabled and the header name is a known header like "Accept", "Content-type", "User-Agent", or "Host" set header-name "user-agent".
1134310	SSL exemption does not work when the policy is a partial match.
1133422	Authentication challenge does not appear when authentication scheme is set to "form" in web portal settings.
1138209	Automatic firmware update should be disabled by default.

Description	Bug ID
1140047	Local user authentication fails when the authentication scheme includes both LDAP and local user DB.
1012742	With fast-policy-match enabled, proxy fails to match policy for traffic with SD-WAN logical interface index.
1135096	In HTTP transaction log, when certificate inspection is set, the URL filed lost protocol information if traffic passes through.
1139414	WAD signal 11 crash with "wad_mem_free".
1111368, 1129196, 1142863	Source IPs are banned without any quarantine features enabled.
1141119	FortiProxy deletes a physical port during installation.
1142196	Cannot perform DNS lookup in transparent policy mode unless a DNS server is specified.
1070388	FortiProxy does not respond to an ICMP request from directly connected interfaces.
1144280	HA becomes out-of-sync after upgrading and requires a reboot to force it to sync again.
1136537	Partial WAD crash logs are shown when verifying WAD memory statistics.
1121655	WAD http2 engine: integer overflow in wad_h2_learn_pad_opt.

Common vulnerabilities and exposures

FortiProxy 7.6.3 is no longer vulnerable to the following CVE references. Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE reference
1125742	CVE-2025-22862
1120660	CVE-2025-25248
1125742	CVE-2025-22862
1194891	CVE-2025-57740

Known issues

FortiProxy 7.6.3 includes the known issues listed in this section. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
1072072	Device identification detection is not yet supported in FortiProxy 7.6.
1103523	The ARM64 image for AWS cannot be deployed correctly.
1141275	The FortiProxy is shut down unexpectedly when Active Directory is used.
1144621	Unicast HA with transparent VDOM fails to sync. **Workaround**: Disable the unicast and re-enable it under HA configuration.
1159963	Expired server certificates are issued during deep inspection.

FortiNBI

The following issues have been identified in FortiNBI. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
N/A	WSL2 X11 output corruption. This is a known bug on Microsoft's WSLg graphics. **Workaround:** • Try running "wsl –shutdown" and then restarting the isolator. • Use the FortiNBI WSLg graphics, which has lower performance than the Microsoft's WSLg graphics.
975570	Certificate warning when starting up the isolator. **Workaround**: Ignore the certificate warning.
881957	Error in Google Chrome or Microsoft Edge login page when FortiNBI is on. **Workaround**: Use Firefox.

www.fortinet.com

Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's Chief Legal Officer, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.