Release Notes

FortiProxy 7.6.6

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 05, 2026
FortiProxy 7.6.6 Release Notes
45-766-1229099-20260205

TABLE OF CONTENTS

Change log

Date	Change Description
2026-02-05	Initial release.

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 7.6.6 supports upgrade from 7.4.x or 7.6.x only. Refer to Deployment information on page 13 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 7.6.6:

- LLM security gateway as HTTP proxy on page 7
- Replacing iptables and ipset with netlink on page 9
- Logging for license sharing events on page 9
- HTTP QUERY method support on page 9
- CLI changes on page 9

LLM security gateway as HTTP proxy

FortiProxy 7.6.6 supports LLM security gateway as HTTP proxy with the following features:

- **Seamless user access via PAC file or explicit proxy settings**—Users can configure their browsers or devices with a PAC file (or manual proxy setting) to direct traffic for known LLM endpoints (for example, `api.openai.com`, `claude.ai`, `gemini.google.com`) through FortiProxy, removing the need for a dedicated access portal.
- **Automatic LLM traffic detection and classification**—FortiProxy inspects outbound HTTPS traffic and automatically classifies LLM API requests based on domain, URL patterns, and TLS fingerprinting, enabling vendor and model awareness without user intervention.
- **Inline policy enforcement on prompts & responses**—Requests and responses are scanned inline, allowing FortiProxy to apply DLP, keyword-based allow/deny lists, language filters, and rate limiting transparently during real-time usage.
- **Per-user attribution and API key control**—FortiProxy maps each request to a user identity (via FSSO or other authentication methods) and enforces API key usage policies (e.g., inject shared key, block if no key, per-user quota), maintaining traceability even without a web portal.
- **Real-time logging & analytics**—All interactions are logged with full context (user, time, model, prompt, response), feeding into FortiAnalyzer, FortiSIEM, or other logging systems for auditing, AI usage metrics, and compliance.
- **Optional redirect to policy page on first use or violation**—On first LLM use or policy violation, FortiProxy can redirect the user to a policy awareness page or disclaimer, replicating the portal’s policy visibility while keeping access frictionless.

Configuration example

```
config ztna web-portal
   edit "ztna_portal_fqdn"
      set vip "ztna_portal_fqdn"
      set host "10.20.20.220.xx.xx"
      set auth-rule "ztna"
      set cookie-age 50
      set llm-proxy enable
      set llm-profile "llm-profile-2"
      set ak-manager enable
   next
end
config firewall proxy-address
   edit "src-adv"
      set type src-advanced
      set host "all"
      config header-group
         edit 1
            set header-name "Authorization"
            set header ".*"
         next
      end
   next
end
config authentication scheme
   edit "bearer-scheme"
      set method bearer
      set user-database "ldap"
      set bearer-type access-token
   next
   edit "fac_ldap_scheme"
      set method basic
      set user-database "ldap"
   next
end
config authentication rule
   edit "bearer-session"
      set srcaddr "src-adv"
      set ip-based disable
      set active-auth-method "bearer-scheme" <--- new option
   next
   edit "ztna"
      set protocol ztna-portal
      set ip-based disable
      set active-auth-method "fac_ldap_scheme"
      set web-auth-cookie enable
   next
end
config user ldap
   edit "ldap"
      set server "10.120.1.120"
      set cnid "cn"
      set dn "dc=qa,dc=domaintest,dc=com"
      set type regular
      set username "qa\\administrator"
      set password ENC
            a2luZ8wb8C2sNYzMPmlPpntA2h3vFgz/F092WGNpwaoB7esnzD8G/Whg/Ph/VswTZ3OvFRWyNysni6sOp4kcWPTw
            Qo6k6iNzQFOEMAROqeV4+lFJ4JzYR1VQ8P6EC7kqJ2B3cZYmvU0o1DBr843pLe9+k4miy4pPHmg2qvPqmSThqF9d
            LjYa33JTrgHHsygbGkACcVlmMjY3dkVA
   next
end
config firewall policy
   edit 13
      set type ztna-proxy
      set ztna-proxy "ztna_portal_fqdn"
      next
```

```
        edit 16
        set name "test"
        set llm-profile "llm-profile-2"
    next
end
config llm profile
    edit "llm-profile-2"
        config chat
            set system-prompt-mode append
            set system-prompt "using emoji"
        end
        config response
        end
    next
end
```

Replacing iptables and ipset with netlink

FortiProxy 7.6.6 replace iptables and ipset with netlink to reduce dependency on third-party programs. As a result, the old `diagnose iptables` commands are replaced with the new `diagnose nft` commands with improved performance and scalability. See CLI changes on page 9 for more details.

Logging for license sharing events

FortiProxy7.6.6 adds logging for the following license sharing events:

- When a member becomes stale and recovers from stale status, the event is recorded on the root node.
- When a member node is promoted as root or reverts back as a member, the event is recorded on the member node.
- When the effective root node changes, the event is recorded on each member node.

See the License Sharing Deployment Guide for more details.

HTTP QUERY method support

FortiProxy 7.6.6 adds support for the HTTP QUERY method. You can now redirect to captive portal for QUERY, similar to a POST request. You can also use the new QUERY method in `config firewall proxy-address`, `config waf profile`, and `config icap profile`.

CLI changes

FortiProxy 7.6.6 includes the following CLI changes:

- `diag sys saml metadata`—Use this new command to test SAML metadata.
- `diagnose sys disk`—Use this new command to enable and view SMART support information for FPX-2000G/4000G/400G.
- `config firewall proxy-address`—The `set method` subcommand includes the new `query` option.
- `config waf profile`—The `config method > default-allowed-methods` and `config method-policy > allowed-methods` subcommands includes the new `query` option.
- `config icap profile`—The `set methods` subcommand includes the new `query` option.
- The old `diagnose iptables` commands are replaced with the new `diagnose nft` commands with improved performance and scalability:

Old	New
`iptables list`	`nft show`
`iptables list6`	
`ipset list`	
`iptables refresh`	`nft update`
`iptables dry-run`	`nft set log-show-ruledump enable', then 'update'`
`iptables shaper`	`firewall shaper reapply`
`iptables shaper-stats`	`firewall shaper`
`debug app iptables`	`nft log`

Product integration and support

The following table lists product integration and support information for FortiProxy 7.6.6 build 1628:

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>
<ul>
<li>Windows Server 2008 64-bit (requires Microsoft SHA2 support package)</li>
<li>Windows Server 2008 R2 64-bit (requires Microsoft SHA2 support package)</li>
<li>Windows Server 2008 Core (requires Microsoft SHA2 support package)</li>
<li>Novell eDirectory 8.8</li>
</ul>
</td></tr>
<tr><td><b>Web browsers</b></td><td>
<ul>
<li>Microsoft Edge</li>
<li>Mozilla Firefox version 87</li>
<li>Google Chrome version 89</li>
</ul>
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><ul><li>Hyper-V Server 2008 R2, 2012, 2012R2, 2016, 2019, and 2022</li></ul></td></tr>
<tr><td><b>Linux KVM</b></td><td><ul><li>RHEL 7.1/Ubuntu 12.04 and later</li><li>CentOS 6.4 (qemu 0.12.1) and later</li></ul></td></tr>
<tr><td><b>Xen hypervisor</b></td><td><ul><li>OpenXen 4.13 hypervisor and later</li><li>Citrix Hypervisor 7 and later</li></ul></td></tr>
<tr><td><b>VMware</b></td><td><ul><li>ESXi versions 6.5, 6.7, 7.0, and 8.0</li></ul></td></tr>
<tr><td><b>Openstack</b></td><td><ul><li>Ussuri</li></ul></td></tr>
<tr><td><b>Nutanix</b></td><td><ul><li>AHV</li></ul></td></tr>
</table>
</td></tr>
<tr><td><b>Cloud platforms</b></td><td>
<ul>
<li>AWS (Amazon Web Services)</li>
<li>Microsoft Azure</li>
<li>GCP (Google Cloud Platform)</li>
<li>OCI (Oracle Cloud Infrastructure)</li>
<li>Alibaba Cloud</li>
</ul>
</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 11 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 11 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 11 for a list of supported VM platforms.

Upgrading the FortiProxy

FortiProxy 7.6.6 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 7.6.6, all FortiProxy devices in the Security Fabric must run FortiProxy 7.6.6. 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 7.6.6:

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 7.6.6. For example, to upgrade from 7.0.17 to 7.6.6, upgrade to 7.2.5 or later first (reboot before upgrading to 7.2.x), and then 7.4.x, and then 7.6.6.

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 7.6.6 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 7.6.6, all FortiProxy devices in the Security Fabric must run FortiProxy 7.6.6. 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 7.6.6 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 7.6.6 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 7.6.6 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 7.6.6. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
1203968	Proxy HTTPS traffic bypasses authentication when SSL profile is cert-inspection.
1202644	Wildcard FQDN should not be allowed as source address in authentication rule.
1203616	Remove wcs socket console message.
1174407	external-resource download does not support IPv6 for FQDN.
1206970	ZTNA Web Portal crash when using ZTNA Web Portal and visit web bookmark then visit RDP.
962298, 1195020	Add support for panic logging on FortiProxy G-series generation 2.
1194046	When a web-filter blocks a QUIC initial packet, the QUIC CONNECTION_CLOSE frame is returned with an incorrect error code.
1187323, 1195493, 1200523, 1200528, 1207608, 1247091, 1247617, 1247662	GUI issues.
1197589	Explicit web HTTPS traffic fails to match policy if `set inspect-all deep-inspection` is configured under `ssl-ssh profile`.
1143184	Policy test does not working on service set on app-service-type app-id
1178204	FortiProxy lacks visibility of the performance of a shared traffic shaper.
1205399	FortiClient TCP forwarding times out when destination is configured as FQDN.
1202928	When a video filter profile is configured to block all videos except some YouTube channels, errors may occur with a "no internet" page when loading a video from the allowed channel.
1209116	Empty config in user group when creating remote SAML user account from GUI.
1212010	SAML idp-entity-id on GUI does not accept HTTP.
1211319	URLFilter regex pattern with perl style regex flags (e.g. /goo.*/gm) does not work after upgrade.
1210950	Crash in crypto_soft_key_signature_schemes when memory malloc failed.
1212765	HTTP-transaction logs show "deny" action while the traffic is allowed with the traffic log showing "allow" action.
1212053	Entry errors when upgrading FortiProxy on FPX-400E/G/F models due to wrong

Bug ID	Description
	limits for FPX-400E/G/F models.
1211406	"Agentforce" chat service on "help.salesforce.com" returns error messages when Appctrl is configured and inline IPS is enabled.
1197688	FortiSandbox setting in web filter prevents updates to URL list objects from taking effect.
1199969	ICAP: WAD keeps crashing with stress traffic.
1203869	Inline IPS performance issue with all-zero 44k HTTPS file.
1214773	Memory leak for web UI LDAP query causing crash or process freezing.
1216034	In config-sync HA mode, the primary shows as secondary.
1211845	TLS 1.3 and newer IANA-registered alerts are displayed as unknown with no numeric alert ID in WAD logs.
1210950	Crash in crypto_soft_key_signature_schemes when memory malloc failed.
1215948	LLM proxy session hangs when the HTTP request does not have a valid body.
1188271	HTTPS is deep scanned silently when it matches a shaping policy with group configured.
1210657	ICAP client should compress multiple cookie headers when converting H2 to H1 for ICAP request.
1214555	Forticron process crashes when too many failed connections occur when fetching external resources.
1219314	HTTP/2 server stream statistics are not displayed in WAD stats output.
1220427	FortiProxy only removes the first header from the HTTP response when multiple HTTP-predefined headers are configured to be removed from response in the web-proxy.profile entry.
1210356	Unable to create shaping profile on top of interface config.
1217947	Failure in adding VLAN interface in kernel.
1217944	Aggregate interface cannot be created in global scope.
1183724	Stream scan detects eicar as "FSA/RISK_MALICIOUS" while analytics-db is disabled.
1219985	FortiProxy fails to cache object with pnc no-cache indicated even with ignore-pnc set to enable.
1198336	Setting up SF-Root HA A/P cluster and the HA widget shows a negative value for uptime with state changed.
1219335	http3 does not jump to captive portal for cookie authentication.
1214773, 1215764	Unable to add remote LDAP user to FortiProxy while user group addition works normally.

Bug ID	Description
1215809	Maximum seats change for VM04, FPX-2000G, and FPX-4000G.
1215282	FortiProxy transparent policy does not pass traffic when both schedule "none" and webfilter-profile exist in the policy.
1216319	Web filter returns error-block when FortiGuard category resolution fails.
1214267	Performance issue for large file upload with http form.
1215438, 1210696	HTTPS traffic does not trigger authentication challenge when passing through forward proxy Internet.
1216128	Failure in matching URL list with external resource URL feed.
1192737	FPX-2000G and FPX-4000G generation 2 UID buttons are non-functional.
1215797	HA Status Widget shows negative value for uptime and state changed.
1104818	WAD crashes when FTP establishes passive data channel without snat and ips configured.
1226755	FortiProxy fails FortiGuard updates if it has CIDB001 license and FortiManager acting as a FDS.
1210702	Replacement message should always be sent if deep inspection is configured in the matched policy even if SSL-exempt is true.
1213796, 1214768, 1221476	CMDB crashes.
1226770, 1218198	WAD crash at wad_http_scan_unexpected().
1225436	FortiProxy scheduled update failur ewith multiple log events "FortiProxy update failed".
1222972	tcp-random-srcport setting does not take effect after reboot.
1223054	Cannot connect to FortiSandbox when "Verify FortiSandbox Certificate" is enabled.
1223145	SAML authentication fails when user-database is configured in the SAML authentication scheme.
1224090	"TLS Internal Error" when a TLS client sends ClientHello with an empty supported_group to FortiProxy TLS Server (like secure web proxy).
1223712	ICAP secure server does not support TLS1.2+DHE cipher.
1194462	GUI sensor view widget is unavailable.
1223615	Connection to ICAP secure server with TLS 1.3 fails.
1218507	SAML authentication cannot proceed when captive-portal-ssl-port is set to 443.
1186225	Microsoft Outlook certificate errors after FortiProxy upgrade.
1220573	FortiProxy SAML SSO login failed with Azure.

Bug ID	Description
1220551	Reports of nonsense sensor values.
1214466	Intermittent traffic via FortiProxy throws 403 Forbidden error.
1224937	Restoring configuration by VDOM causes static entries of proxy-address to lose host-regex.
1213247	504 Gateway Timeout error when accessing full mode HTTPS virtual server.
1228242	Captive portal does not support ECDSA cert + TLS 1.2 Client.
1224024	FortiGuard Web Filtering categories does not work in ICAP server.
1226921	Incorrect length of resulting formatted JSON text output.
1226782	HTTP/2 error when LLM profile prompt size is too small.
1213758	Crash when forward server is enabled and health check is enabled.
1223406	Connection to websites with redirection is slow.
1222883	Enabling "certificate inspection" on a policy breaks traffic and causes browser certificate error.
1226848	Toggling FortiSandbox status causes the blocklist option to unset after FortiProxy upgrade.
1224684	ICAP server configuration should not be allowed to be saved when address type is FQDN but no FQDN is set.
1223904	Error "Access Denied - The maximum web proxy user limit has been reached" while the limit of licenses are not reached.
1228552	The “compile took” value in diag wad deb ips-db status is incorrect.
1199626, 1232099	Unable to access the website after successful SAML authorization when using ZTNA TCP forwarding.
1229572, 1230697, 1230682	Rule is missing for policy when address contains proxy-address with host=all.
1226834	transparent-connect policies have higher priority than ZTNA access policies, which should not be the case.
1232934	After successful deployment on OCI, the FortiProxy OCI instance can be accessed through the OCI cloud platform console but FortiProxy service is not accessible externally
1232764	wad crashed with signal 11 at wad_port_fwd_peer_shutdown.
1225658	Web filter cannot block host in HTTP header if SSL has no SNI.
1090202	DoH/DoT client does not verify server certificate in TLS 1.3.
1210941	Cannot choose IPv6 address pool in explicit proxy policy.
1232659	"HTTP 500 Internal Error" when DLP profile is applied to the ICAP local server.

Bug ID	Description
1233437	No TLS downgrade protection.
1233755	Scanunit crash in fg_hs_realloc when using DLP.
1230902	Packet sniffer under a non-root VDOM captures and shows the packets on root VDOM.
1093617	Move nethsm certificate from "vpn certificate local" to "vpn certificate hsm-local".
1213836	FortiView sources do not include all sessions in aggregated results.
1233964	Inline IPS should be disabled by default.
1235057	The transparent policy traffic matches a policy with a mismatching schedule.
1233086	Invalid read due to type confusion in wad_h2_ses.
1182776	Missing result check for wad_str_copy_str in wad_http_parse_hostinfo.
1232661	Improve policy test GUI/CLI usability by normalizing HTTP request header input.
1236592	WAD fails to return replacement message when tp fwd_svr is down and ssl is deep-inspection.
1193993, 1194125, 1194197, 1218082	WAD memory chaos fixes.
1235968	"diag wad filter process-type" does not work as expected.
1232698	Antiphish does not block usernames containing the "." character.
1226196	HTTP transaction log shows IP instead of URL/hostname on early request close.
1120494	Unauthorized traffic bypassing authentication on virtual server.
1238298	"diag sys link-monitor" does not work on non-root VDOM.
1215764	GUI-only interfaces of root VDOM are shown on GUI regardless of which VDOM is selected.
1240478	TACACS+ authentication does not use HA-direct interface in an active-passive cluster.
1241868	FPX_2000G Gen2 hardware keeps rebooting and formatting HD2 disk.
1230642	Key share mismatch error message against tls1.3 with ecdsa certificate in server load balance type VIP.
1239501	DLP profile rules discrepancy between GUI and CLI.
1233331	Incorrect GUI behavior logic for Web Authentication Cookies button.
1242892	Certificate authentication fails when set ldap-user-cache enable.
1224664	ZTNA portal RDS websocket should implement maximum frame sizes per protocol on FortiProxy.

Bug ID	Description
1243698	HTTPS does not redirect for deep-inspection.
1237357	Proxy rule not matching if host-regex type address value is more than 40 characters.
1242183	FortiProxy fails to route replies to FortiProxy-originated traffic back to itself.
1244035	Wanopt server failed to establish tunnel.
1244480	WAD crashes when accessing HTTP/3 website with FSSO enabled.
1213283, 1243580	Web cache-related crashes.
1245976	Kernel-only traffic does not SNAT to IP pool.
1243552	heap-use-after-free is detected @wad_timer_list_renew.
1245769	Access-proxy traffic is rejected by redirect filter.
1234160	Incorrect formatted printing of array in JASON parser.
1245586	Deny policy fails to block FTP request.
1242590	No event log is generated when an external resource is updated and the downloaded item is within the limit after an overflow.
1175553	Unexpected "no route" error returned by policy lookup when no policy matches.
1223433, 1223447, 1236782, 1237405	ICAP client health check and status issues after boot.
1232296	FortiProxy-400E shows abnormal PSU voltage value.
1249069	Error with WAD when running debug command "dia wad worker ut".
1249419	App signature and group are not correctly created or displayed on GUI in non-root VDOM.

Known issues

FortiProxy 7.6.6 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.
1210368	FortiProxy in config-sync-only HA mode with the default certificate cannot establish stable connection to FortiManager. **Workaround**: **1.** Add central management configuration in backup mode on both FortiProxy devices in the HA cluster. **2.** Select both FortiProxy devices and authorize (instead of authorizing the devices one by one),

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.