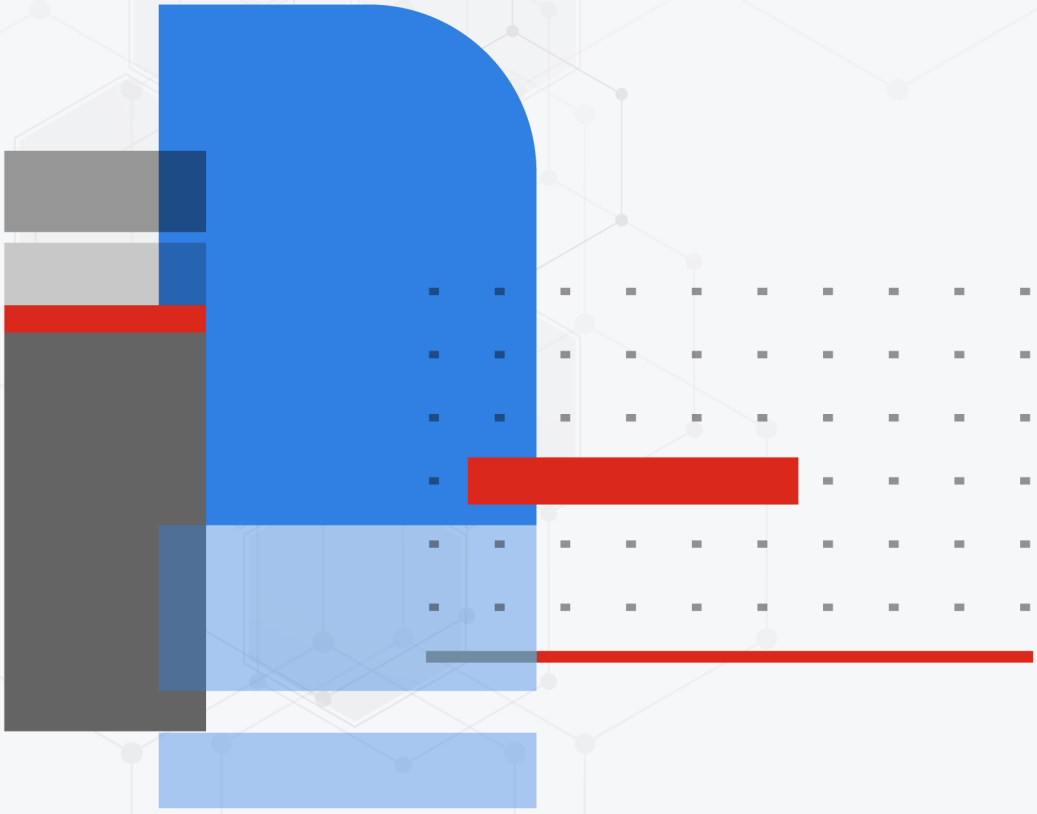
Release Notes

FortiProxy 7.4.14



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

May 28, 2026
FortiProxy 7.4.14 Release Notes
45-7414-1295030-20260528

TABLE OF CONTENTS

Change log

Date	Change Description
2026-05-28	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 7.4.14 supports upgrade from 7.4.x only. Refer to Deployment information on page 10 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 FortiProxy7.4.14:

PQC support

FortiProxy 7.4.14 adds support for TLS 1.3 hybrid Post-Quantum Cryptography (PQC) key exchanges in SSL deep inspection, enabling secure traffic inspection. This enhancement ensures compatibility with modern browsers and PQC-enabled servers that utilize algorithms such as X25519MLKEM768.

CLI changes

FortiProxy 7.4.14 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.
- `diagnose sys logdisk usage`—Use this new command to show log disk stats.
- `config web-proxy url-match`—Use the new `include-subdomains` option to configure whether to enable matching subdomains for simple-type entries.

Product integration and support

The following table lists product integration and support information for FortiProxy 7.4.14 build 748:

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

Type	Product and version
	• 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
Web browsers	• Microsoft Edge • Mozilla Firefox version 87 • Google Chrome version 89  Other web browsers may work correctly, but Fortinet does not support them.
Virtualization environments	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.
Hyper-V	• Hyper-V Server 2008 R2, 2012, 2012R2, 2016, 2019, and 2022
Linux KVM	• RHEL 7.1/Ubuntu 12.04 and later • CentOS 6.4 (qemu 0.12.1) and later
Xen hypervisor	• OpenXen 4.13 hypervisor and later • Citrix Hypervisor 7 and later
VMware	• ESXi versions 6.5, 6.7, 7.0, and 8.0
Openstack	• Ussuri
Nutanix	• AHV
Cloud platforms	• AWS (Amazon Web Services) • Microsoft Azure • GCP (Google Cloud Platform) • OCI (Oracle Cloud Infrastructure) • Alibaba Cloud

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 8 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 8 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 8 for a list of supported VM platforms.

Upgrading the FortiProxy

FortiProxy 7.4.14 supports upgrade from 7.4.x only.

If Security Fabric is enabled, all FortiProxy units must be upgraded to the same version. For example, if Security Fabric is enabled in FortiProxy 7.4.14, all FortiProxy devices in the Security Fabric must run FortiProxy 7.4.14. 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 7.4.14:

If you are using a RADIUS server that does not support the message-authenticator attribute, upgrading to 7.4.14 is not recommended.

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 2.0.x, 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 7.4.14. For example, to upgrade from 2.0.12 to 7.4.14, upgrade to 7.0.11 or later first, and then 7.2.5 or later (reboot before upgrading to 7.2.x), and then 7.4.0, and then 7.4.14.

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 7.4.14 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 7.4.14, all FortiProxy devices in the Security Fabric must run FortiProxy 7.4.14. 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 7.4.14 to 7.2.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 7.4.14 to 7.0.x or 2.0.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 7.4.14 to 2.0.12, downgrade to 7.2.5 or later first, and then 7.0.11 or later, and then 2.0.12.

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 7.4.14. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
1222883	Enabling "certificate inspection" on a policy breaks traffic and causes browser certificate error.
1226848, 1227043	Toggling FortiSandbox status causes the blocklist option to unset after FortiProxy upgrade.
1224024	FortiGuard Web Filtering categories does not work in ICAP server.
1224684	ICAP server configuration should not be allowed to be saved when address type is FQDN but no FQDN is set.
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.
1134552, 1226921	Incorrect length of resulting formatted JSON text output.
1213796, 1214768, 1221476	CMDB crashes.
1210702	Replacement message should always be sent if deep inspection is configured in the matched policy even if SSL-exempt is true.
1223406	Connection to websites with redirection is slow.
1225436	FortiProxy scheduled update failur ewith multiple log events "FortiProxy update failed".
1223145	SAML authentication fails when user-database is configured in the SAML authentication scheme.
1223615	Connection to ICAP secure server with TLS 1.3 fails.
1223712	ICAP secure server does not support TLS1.2+DHE cipher.
1218507	SAML authentication cannot proceed when captive-portal-ssl-port is set to 443.
1220573	FortiProxy SAML SSO login failed with Azure.
1236592	WAD fails to return replacement message when tp fwd_svr is down and ssl is deep-inspection.
1235968	"diag wad filter process-type" does not work as expected.

Bug ID	Description
1232698	Antiphish does not block usernames containing the "." character.
1226196	HTTP transaction log shows IP instead of URL/hostname on early request close.
1232661	Improve policy test GUI/CLI usability by normalizing HTTP request header input.
1233964	Inline IPS should be disabled by default.
1232659	"HTTP 500 Internal Error" when DLP profile is applied to the ICAP local server.
1210941	Cannot choose IPv6 address pool in explicit proxy policy.
1213836	FortiView sources do not include all sessions in aggregated results.
1233437	No TLS downgrade protection.
1225658	Web filter cannot block host in HTTP header if SSL has no SNI.
900911, 1232764	wad crashed with signal 11 at wad_port_fwd_peer_shutdown.
1223904	Error "Access Denied - The maximum web proxy user limit has been reached" while the limit of licenses are not reached.
1242590	No event log is generated when an external resource is updated and the downloaded item is within the limit after an overflow.
1245586	Deny policy fails to block FTP request.
1243552	heap-use-after-free is detected @wad_timer_list_renew.
1234160	Incorrect formatted printing of array in JASON parser.
1237357	Proxy rule not matching if host-regex type address value is more than 40 characters.
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.
1120494	Unauthorized traffic bypassing authentication on virtual server.
1215764	Unable to add remote LDAP user to FortiProxy while user group addition works normally.
1230642	Key share mismatch error message against tls1.3 with ecdsa certificate in server load balance type VIP.
1232296	FortiProxy-400E shows abnormal PSU voltage value.
1211668	Add additional warnings when configuring certificate authentication.
1204371, 1250962, 1260927	ICAP crash in "wad_hmsg_strm_reset" and chunked error.
1258666	Policy test should match tp-connect when tp-connect has no inspection.
1249061	ZTNA HTTP/3 traffic does not pass when using ciphers 0x1301 (ECC-256), 0x1302 (RSA-2048), and ECC-521.

Bug ID	Description
1237516	Increase header length limit from 4k to 16k for access management of SaaS applications that require longer values.
1234284, 1248324	Group match cache is not updated when the groups are changed on LDAP server.
1254103, 1256426, 1256564	Deamon 'wad_algo' crash.
1252671	ICAP local server resets packet in non-root VDOM.
1214017	FortiProxy becomes unresponsive after an external threat feed is added with more than 4,000,000 entries.
1223433, 1223447, 1236782, 1237405	ICAP client health check and status issues after boot.
1251663	Inline IPS crashes when visiting townscript.com.
1249069	Error with WAD when running debug command "dia wad worker ut".
1243569	FortiProxy booted with firewall policy that does not enable webcache.
1244554	FortiProxy should be able to use non-root VDOM interface to connect to FortiSandbox.
1265039	“504 Gateway Timeout: remote server did not respond to the proxy.” error after upgrade.
1262480	GUI freezes and keeps loading LDAP group.
1263851	SNMP response returns 0 when querying policy-related OID
1259573	Unintended subnet added during GUI search.
1250976	No validation for duplicate explicit-outgoing-ip.
1265395	The kernel HA primary shown in the CLI does not match the debug zone group primary on the secondary device.
1266880	The device encounters an issue when connecting to a website with an IP address, as the ephemeral certificate is generated with a DNS type IP address in the SAN instead of an IPADD type.
1196434	SAML authentication may stop working due to mandatory response signing in SAML auth response verification. An option is needed to allow SAML auth response without response signature while preserving security.
1261184,1261205	Authentication failure due to remote server renaming.
1264570	CLI script is not executed by automation stitch when triggered.
1255325	When FortiProxy blocks an expired server certificate in VIP, the certificate information does not show CN.
1252947	Web proxy does not replace or reject existing X-Authenticated-User header from original request.

Bug ID	Description
1256952, 1261976	No support for TLS1.3 HRR in proxy 1way server.
1224090, 1252573	Reject deprecated elliptic curves per RFC 8422.
1252221, 1252783, 1255206	ICAP crash and abort on ICAP server group config flush.
1272393	Kerberos authenticated user not matching with correct user group.
1202928	Video filter does not work as expected after YouTube API update.
1254558, 1261311, 1266707	ICAP remote server FQDN config lost and config update issue.
1273009	Add explicit-web-proxy name to http-transaction log for proxy traffic.
1272628	Prevent QUIC socket file descriptor leak during scheduler event teardown.
1252787, 1264976	A few issues with QUIC.
1262906, 1265904	When web filter profile is applied in the ICAP server, and when the Action of FortiGuard Web Filtering categories is set to Block, web traffic still passes through the ICAP server.
1251833	The authentication rule for certificate authentication is lost after upgrade.
1227469, 1257924	Crash at wad_http_scan_handle_unblock.
1243551	WAD crashes @wad_http_session_scan_done.
1223904, 1275635	User access denied when the limit of licenses has not been reached.
1266546	Prevent saving protocol change for forward server when object is in use.
1254420	Sporadic errors when browsing sites: "504 DNS lookup failed" when multiple dns proxy instances start to show high CPU utilization.
1266983	UDP port-forward VIP works for traffic but is not shown correctly in the GUI and do not update policy/log byte counters.
1284868	WAD crash at wad_ssl_port_caps_initiator_key_shares().
1282023, 1282589	HA fails to sync config due to different ssl.root snmp-index if no interface is assigned to ssl.root after deployment.  If you are using 7.6.0-7.6.6 and want to downgrade to 7.4.14+ for this fix, you must downgrade to 7.4.13 first and then upgrade to 7.4.14+. Downgrading from 7.6.0-7.6.6 to 7.4.14 directly will not resolve the issue.
1278274	Secondary HA unit becomes inaccessible (GUI/SSH/PING) after failover from primary to secondary.
1277701	Failure in adding an empty policy by selecting Insert empty policy.
1046504, 1268904	Various loopback issues including deletion and management.

Bug ID	Description
1286260	Cannot choose proxy addresses (URL-List type) as destination on Authentication Rules via GUI.
1286767	The device only checks the first certificate when multiple certificates are defined in an SSL profile in replace mode, causing issues with certificate validation.
1287642	TLS 1.2 secure renegotiation fails with handshake failure when reusing session ticket.
1207834	Remove table size enforcement changes due to large decreases in table size.
1286238	port7 and port8 do not detect 1G SFP FN-TRAN-SX.
1277552	LDAP cache: user entry is not removed when user object is deleted on the domain controller.
1276292	Interface not available on GUI.
1279792, 1280772	wanopt PSK length truncation issue.
1288916	External connector search field does not filter results. It only highlights entries.
1051088, 1264398, 1266177, 1268094	Fix FortiProxy conserve mode and a potential auth dead loop.
1118701, 1289354	Connection issues for Kentik application using http2 gRPC occur with proxy and deep inspection.
1244480, 1290307	WAD crashes when accessing HTTP/3 website with FSSO enabled
1010829	FortiProxy cannot mount FAT USB drives.
1276400	Forticron failed to learn dynamic sdn address list config change.
1281302 , 1283666, 1288106, 1288118	ICAP issues.
1124132	Cloning of access-proxy firewall policies fails in CLI.
1284883, 1291729	forticldd crash for NULL-terminated buffer issue when handling response from server.
1290852, 1290920	crashes in wad_quic_conn_rx_1rtt_pkt and wad_quic_conn_rx_hspkt caused by assigning negative value to unsigned int.
1285943	Incorrect source IP for deep inspection traffic when client IP header exists only in CONNECT.
1291175 , 1291909	WAD SOCKS and web-proxy fwd-svr related read-block handling issues.
1292129	Add upgrade code to ensure application matching continues working after upgrade.
1292767	VLAN interfaces in non-root vdom are not working.
1098087 , 1289354	HTTP2 traffic with two HEADERS frame cannot pass through policy.

Common vulnerabilities and exposures

FortiProxy 7.4.14 is no longer vulnerable to the following CVE references. Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE reference
1278217	• CVE-2025-31514 • CVE-2025-54821

Known issues

FortiProxy 7.4.14 includes the known issues listed in this section. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
1108489	Safe search does not work when configured in webfilter-profile and image-analyzer-profile in local ICAP server.
1096536	FortiProxy stop processing traffic after VIP modification.
996875	Traffic is failing because the replacement certificate created by FortiProxy during DPI does not contain CRL or OCSP.
1005060	Ingress traffic shaper hits a bandwidth throttle that cannot be more than 2.5 Gbps. **Workaround:** Use egress shaper for better scalability.

www.fortinet.com