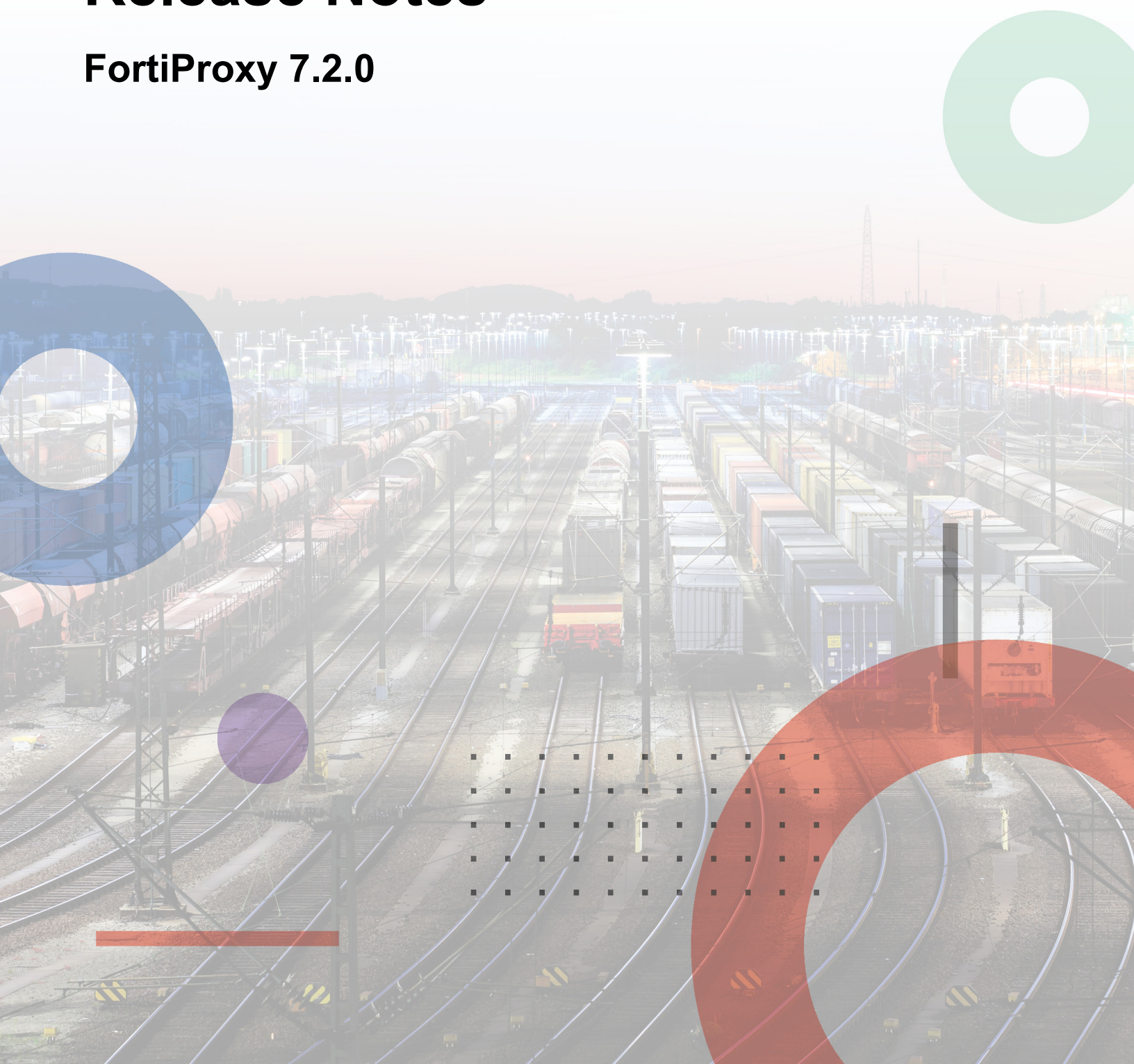
FORTINET

Release Notes

FortiProxy 7.2.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

February 6, 2024
FortiProxy 7.2.0 Release Notes
45-720-839840-20240206

TABLE OF CONTENTS

Change log

Date	Change Description
2022-09-19	Initial release.
2023-04-21	Updated Introduction on page 5.
2023-06-14	Added the *Correlation log support* section in What's new on page 7.
2023-06-23	Updated Product integration and support on page 13.
2023-06-27	Updated Product integration and support on page 13.
2023-10-26	Updated Product integration and support on page 13.
2024-02-05	Updated What's new on page 7.
2024-02-06	Updated What's new on page 7.

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. 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.
Data Leak 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.

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.

Supported models

The following models are supported on FortiProxy 7.2.0, build 0298:

FortiProxy	• FPX-2000E • FPX-4000E • FPX-400E
FortiProxy VM	• FPX-AZURE • FPX-HY • FPX-KVM • FPX-KVM-AWS • FPX-KVM-GCP • FPX-KVM-OPC • FPX-VMWARE • FPX-XEN

What's new

The following sections describe new features and enhancements:

Browser isolation

Client-based native browser isolation (NBI) uses a Docker container to isolate the browser from the rest of the computer. As browsers are one of the biggest windows to external networks, they are one of the biggest attack vectors. Isolating, or sandboxing, the browser in a container helps decrease the attack surface.

The endpoint must use FortiProxy as the network gateway for the internet. The FortiNBI installer installs the Chrome browser extension, a Docker image with a preloaded Chrome browser, a local server to invoke the dockerized browser instance, and a GUI for monitoring the status of the components and changing the IP address of the FortiProxy that it is connecting to.

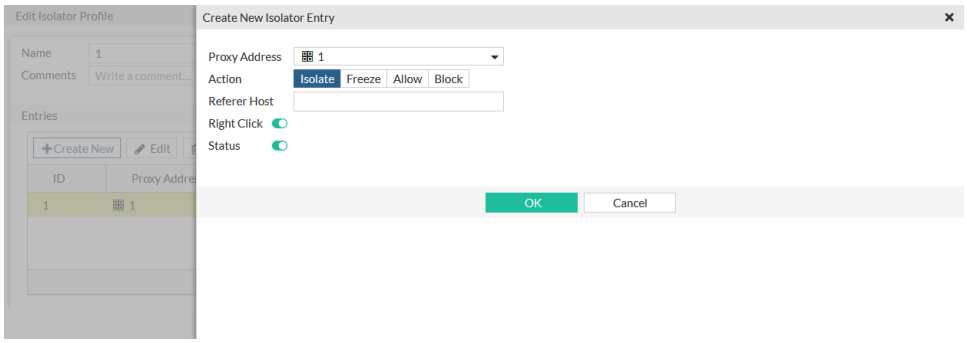
The browser extension monitors each browser tab, and reports every new tab invocation to FortiProxy over the communication channel that it maintains, with FortiProxy acting as a secure web gateway.

Browser isolation is currently supported on Microsoft Windows 10 in Google Chrome and requires the new Isolator license.

For more information, see Browser isolation.

To configure browser isolation:

1. Configure an HTTP portal for the client to download the isolator image.
2. Enable and configure Captive Portal in the Proxy authentication settings.
3. Enable captive portal on the interface.
4. Configure a firewall proxy address.
5. Configure an isolator profile that uses the proxy address.



6. Configure an SSL/SSH profile.
7. Configure a firewall policy that uses the isolator and SSL/SSH profiles.

License sharing

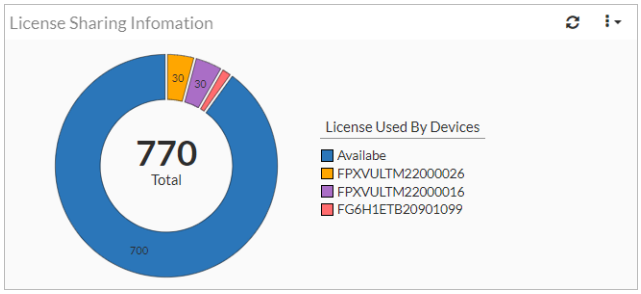
Seat licenses can be shared across multiple units (hardware and VM), while the license limit is maintained for each unit. A cluster is created that licenses are shared in. The primary FortiProxy manages the licenses, and can then share them with multiple other units. When a member joins the cluster, its associated entitlements are added to the license pool.

For more information, see the FortiProxy 7.2 License Sharing Guide.

To enable license sharing:

```
config system csf
    set status enable
    set group-name <string>
    set downstream-access enable
    set license-sharing enable
    ...
end
```

The *License Sharing Information* widget shows the total number of available licenses, and the numbers used by the devices in the license pool.



HA license sharing behavior change

In HA active-passive mode, FortiProxy 7.2.0 shares all available seats (as opposed to 50% of available seats in previous versions) among the HA cluster (hardware and VM) by default. With this change, seat license variation across HA devices is no longer a concern in case of failure.

The primary FortiProxy unit automatically claims all license entitlements from all members in the HA cluster (hardware or VM). When a member joins the cluster, its associated entitlements are added to the primary unit. When a member leaves the cluster, its associated entitlements are removed from the primary unit. When the primary unit goes down, the secondary device with the highest priority becomes the primary and assumes all the license entitlements.

VDOM support

Virtual Domains (VDOMs) are used to divide a single FortiProxy into two or more virtual units that function independently. VDOMs can provide separate firewall policies and security profiles. In NAT mode, they provide separate routing configurations. When multi VDOM mode is enabled, the default VDOM is the *root* VDOM, and it cannot be deleted.

Multiple VDOMs allow users to combine NAT and transparent mode on a single FortiProxy; VDOMs can be independently configured to operate in NAT or transparent mode.

By default, FortiProxy hardware and VM devices support 5 VDOMs; a license key can be purchased to increase the maximum number.

For more information, see Virtual domains in the FortiProxy Administration guide, and the FortiProxy data sheet.

Correlation log support

Under *Log & Report*, you can now view correlation log which shows the correlation of forward traffic log(s) and HTTP transaction log(s) that have a common session ID.

VXLAN support

FortiProxy supports VXLAN.

To configure VXLAN:

```
config system vxlan
    edit <name>
        set interface <interface>
        set vni <vxlan_network_id>
        set ip-version {ipv4_unicast | ipv6_unicast}
        set remote-ip <ipv4_address>
        set remote-ip6 <ipv6_address>
```

```
        set dstport <port>
    next
end
```

`interface <interface>`	Outgoing interface for VXLAN encapsulated traffic.
`vni <vxlan_network_id>`	VXLAN network ID (default = 0).
`ip-version {ipv4_unicast | ipv6_unicast}`	The IP address version to use for the VXLAN interface, and for communication over the VXLAN (default = ipv4_unicast).
`remote-ip <ip_address>` `remote-ip6 <ipv6_address>`	The IPv4 or IPv6 address of the VXLAN interface on the device at the remote end of the VXLAN.
`dstport <port>`	The VXLAN destination port (1 - 65535, default = 4789).

To view the VXLAN forwarding database list for an interface:

```
diagnose sys vxlan fdb list <interface>
```

Certificate validation for external resources

Certification is verified before fetching data from the external connectors that have SSL enabled.

To configure certificate verification:

```
config system external-resource
    edit "test"
        set server-identity-check {none | basic | full}
    next
end
```

`none`	No certificate verification (default).
`basic`	Check server certificate only.
`full`	Check server certificate and domain match server certificate.

Detect HTTPS in HTTP request

In an explicit web proxy, you can enable detecting SSL in the HTTP request line. When enabled, HTTP get/post requests sent to the FortiProxy will be passed instead of blocked.

To enable detecting SSL in the HTTP request line:

```
config web-proxy explicit-proxy
    edit "web-proxy"
        set status enable
        set interface "any"
```

```
        set http-incoming-port 8080
        set detect-https-in-http-request enable
    next
end
```

Auto-script password encryption

When configuring an automatic script, the new `password` attribute can be set. It will replace the password in the script when the script uses the `%%PASSWD%%` tag. When the configuration is downloaded or viewed in the CLI, the password is encrypted.

To configure then view an automatic script with a password:

1. Configure the automatic script:

```
config system auto-script
    edit "autobackup"
        set interval 60
        set repeat 0
        set start auto
        set script "execute backup config sftp 10.0.0.1 admin %%PASSWD%%
/home/user/proxy.config"
        set password 1234567890
    next
end
```

2. View the script:

```
# show system auto-script
config system auto-script
    edit "autobackup"
        set interval 60
        set repeat 0
        set start auto
        set script "execute backup config sftp 10.0.0.1 admin %%PASSWD%%
/home/user/proxy.config"
        set password ENC
Dz6s2235D+GkaND0zptzOUQH2ptR2M4v5VEP3v3/NvB2So/yBat/tUGEavP71pUdn38HKFXUPeZ802C8+exOjDat
MSo5YVebkkDnL01J4EtGzcrJuQKl97+ekrHXMzkyxA/yxtkKURuVBlhKRqBFn03DleaR7vcbj4HnLLIY73WRI018
NDfPgOS3non02OqfFv9Oew==
    next
end
```

   The password is encrypted.

Automation stitches

Automation stitches automate the activities between the different components in the Security Fabric, which decreases the response times to security events. Events from any source in the Security Fabric can be monitored, and action

responses can be set up to any destination. Automation stitches can only be created on the root device in a Security Fabric. Automation stitches can also be used on FortiProxy devices that are not part of a Security Fabric.

An automation stitch consists of two parts: the trigger and the actions. The trigger is the condition or event on the FortiProxy that activates the action, for example, a specific log, or a failed log in attempt. The action is what the FortiProxy does in response to the trigger.

Automation stitches that use cloud-based actions (AWS Lambda, Azure Function, Google Cloud Function, and AliCloud Function) have the option to delay an action after the previous action is completed.

Diagnose commands are available in the CLI to test, log, and display the stitch history and settings.

Go to *Security Fabric* > *Automation* to configure automation stitches, triggers, and actions. On the *Security Fabric* > *Automation* page, there are tabs for *Stitch*, *Trigger*, and Action. The *Stitch* tab is the default view that lists the trigger and actions used in each stitch. Individual triggers and actions can be created or edited in the corresponding tabs.

For details about configuring automation stitches, see Automation stitches in the FortiProxy Administration guide.

Remove quotes from external resource

When a URL is entered for an external resource, the leading and tailing quote strings are automatically removed from the URL. This includes the following characters: `&quot;`, `&apos;`, `&39;`, `&34;`, and `&96;`.

For example: "`https://docs.fortinet.com`" will be changed to: `https://docs.fortinet.com`.

Product integration and support

Web browser support

The following web browsers are supported by FortiProxy 7.2.0:

- Microsoft Edge
- Mozilla Firefox version 87
- Google Chrome version 89

Other web browsers might function correctly but are not supported by Fortinet.

Fortinet product support

- 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.

Fortinet Single Sign-On (FSSO) support

- 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
  - 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

Virtualization environment support

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.

HyperV	• Hyper-V Server 2008 R2, 2012, 2012R2, 2016, and 2019
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, and 7.0
Openstack	• Ussuri

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 13 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 13 for a list of supported VM platforms.

Upgrading the FortiProxy

You can upgrade FortiProxy appliances or VMs from 7.0.x to 7.2.0 by following the steps below:

1. In the GUI, go to *System* > *Firmware*.
2. Click *Browse* in the *File Upload* tab.
3. Select the file on your PC and click *Open*.
4. Click *Confirm and Backup Config*.
5. Click *Continue*.
   The configuration file is automatically saved and the system will reboot.

If you are currently using FortiProxy 2.0.x, Fortinet recommends that you upgrade to 7.0.x first by following the same steps above before attempting to upgrade to 7.2.0.

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.

After you upgrade from 2.0.x to 7.0.x, click *Reset All Dashboards* in the GUI to avoid any issues with FortiView.

Downgrading the FortiProxy

You can downgrade FortiProxy appliances or VMs from 7.2.0 to 7.0.x by following the steps below:

1. In the GUI, go to *System* > *Firmware*.
2. Click *Browse* in the *File Upload* tab.
3. Select the file on your PC and click *Open*.
4. Click *Confirm and Backup Config*.
5. Click *Continue*.
   The configuration file is automatically saved and the system will reboot.

To downgrade from FortiProxy 7.2.0 to 2.0.x, Fortinet recommends that you downgrade to 7.0.x first by following the same steps above before attempting to downgrade to 2.0.x.

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.

After you downgrade from 7.0.x to 2.0.x, click *Reset All Dashboards* in the GUI to avoid any issues with FortiView.

Resolved issues

The following issues have been fixed in FortiProxy 7.2.0. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
604172	Webfilter cannot communicate with FortiGuard through proxy.
728311	FortiProxy bypassed FTP MODE command when protocol option configuration was set to block.
734909	ICAP error messages use the correct replacement messages rather than the existing, hard-coded 502 response.
764817, 786194, 789150, 796489, 796574, 800013, 802841, 806595, 807653, 808091, 808203, 808454, 817881, 817995, 827721, 829497, 829543, 830074, 832716, 833174, 835163, 835638, 836141, 836142, 837089, 840519, 840525, 842519	Fix GUI issues.
752001	Ensure route entry removal whenever system.ha.unicast-gateway updates.
763951	Speed up policy learning by using a delta config.
766102	Change name from FortiAI to FortiNDR.
768980, 770178, 773671, 777370, 777718, 788697, 789520, 789600, 789982	Implicitly enforce deepscan when HTTP CONNECT request or TLS SNI partially matches to a policy.
776989	Fixed overflow when adding VDOM.
777032, 803217	Improve url-rating by FortiGuard URL rating raw-flag, fix isolate does not work.
778766, 783072, 783811	Port bug fix from FOS: wad forward-server monitor doesn't work.
780182	WAD crash at wad_http_fwd_msg_body.
781891	Add upgrade code to handle lost LDAP search filter option value.
781943	Disable default firewall policy action for explicit proxy on ZTNA rules.
783201	Memory usage tunning for webcache.
783837	Primary FortiProxy license status is changing from "Valid" to "Warning" after a successfull upgrade under an HA cluster fix.

Bug ID	Description
784337	OVF contains wrong VMDK for HW15 and FortiGate-label fix.
784338	OVF files contain FortiGate-VM references fix.
784797	Fix SSH over HTTP policy matching issue and ICAP server failures.
784891	Fix UTM features list is missing on policy page of type ssh/ssh-tunnel/wanopt/ftp.
785232	Comment out unwanted references to SD-WAN.
785912	Some fields (e.g. utm features) are not valid or missing according to the policy type fix.
787027	Fix antivirus profile content disarm options are not rendered correctly.
787496	Fix WAD memory leak on matching shaping policy.
787895	Fix potential memory corruption in wad_stats.
787977, 805228	Fix several issues related to dedicated-to option.
788822	Update kernel to v5.10.109.
789422	Fix missing ICAP request for CONNECT.
791235	Fix ssl exempt check condition for nontp policy.
791668	Traffic Shaping match fix
792065	DLP block an email with multi attachments via MAPI, but the log cannot show all the blocked files.
792579	Fix implicit deny policy logs and HTTP transaction logs not working.
793251	Unable to add IPv6 address group objects to policies fix.
793687	The source port range is not changed in kernel according to the CLI configuration fix.
794165, 803452	Fix fast match generation update after config change.
794753	Fix the issue authz header line is removed for HTTP basic authentication request.
795159	Add traffic log.action as 'pending' for not full matched policy.
795621	Fix data corruption on SSL traffic.
795970	As long as the ICAP function is turned on, the website front will be abnormal.
796019	Access issue with Application Control or IPS.
796152	Fix key_share leak on HRR.
796664	Fix domain-fronting conflict with HTTP2 connection coalescing.
797270	Fix ha-mgmt interface binding.
797609	IPv6 gateway route is not installed fix.
797809	Fix super_admin is not prompted to select between RO and RW access.

Bug ID	Description
798027	Rollback multiple session-base users check under ip-base authenticate and rollback userquery logic at http-get-user.
798054	Fix SSL layer data flow-control.
798118	WAD process crashes at wad_async_queue_time_out.
798745	Fix delayed CRLF 204 handling in ICAP.
799171	Fix shaping policy match crash by pol_ctx double free.
799214	Follow-up enforce deepscan when HTTP CONNECT: enforce fwdsvr, except host-cate not match.
799278	Transparent mode "set dedicated-to management" not working as expected fix.
799718	When to-pol with auth(group/user) is set to action isolate, request fails to be redirected to WAD.
800243	Dedicated to management interfaces allow incoming connections on extra ports.
800262	Access of NULL pointer in sslvpnd fix.
800921	HTTPS request via tp-policy + fw server and authentication, crashes @__wad_http_policy_category_notify.
801174	Add multiple HTTP request headers and extract .tar.gz file for external resource.
801492	If the icap remote server is abnormal, the service connected through FortiProxy will be abnormal.
802222	FSSO traffic log has group info but no user information. Add save guard when calling af->make().
802303	ICAP - correct ICAP server max_conn and health check server IP leak issue.
802333	Add sec_profile when matched implicit policy on HTTP traffic.
802866	Fix certificate ha sync related issues.
803159	FortiProxy blocks uncompressed oversize file, the AV UTM log does not cache the correct information.
803217	Fix policy matching with multiple category type proxy-address.
803380, 807332	WAD does not forward 302 HTTP redirect to end-client. WAD memory leak when convert explicit proxy to captive portal.
803794	Custom upgrade code to handle the loss of local certificate data during upgrade.
804689	ICAP "respmod-forward-rules" should AND "header-group" entries.
804853	Fix SSL traffic occasionally fail.
805210	Fix NTLM agentless authenticate fail due to user-restriction after FSSO service down.

Bug ID	Description
805819	FortiProxy as explicit web proxy did not block file transfer via ftp-over-http which has same hash value from ems-threat-feed.
806066	Avoid Syncing Outgoing-ip in webproxy.global.
806130	Fix proxy-address with host-regex match for IP URL.
806224	Execute ha manage does not work in FortiProxy cluster when trusted host is configured fix.
806595	Add License Sharing Information Widget on GUI.
807090	Upgrade IA Engine to Version 8.
807280	Fix proxy the certificate error when no policy matched.
808040	Kerberos authentication failed when upgrade FortiProxy.
808043	Fix disclaimer page is redirecting to incorrect URL.
808074	Allow content-encoding: UTF-8 passthrough.
808598, 809201, 809341	Local-ICAP Server Response does not contain Virus Response Header names and values, like X-Virus-ID or X-Infection-Found.
808769	Prevent HA Syncing of gui-dashboard and ems-tag to fix ICAP local server sync issue.
809813	Prefetch URLs report crawl for http://www.<whatever>.com failed (error: 255).
809832	Adding local-in rules for NTD server.
810570, 811995	Fixed several WebCache issues.
810571	Fix SSL exempt check condition for non-transparent policy.
811259	Fix WAD leak on IPS session objects.
813261	With learn-client-ip enable policy able to control based on the learn-client-ip but logs not reflecting.
813317	In transparent mode, implement srcaddr-negate, dstaddr-negate, and service-negate.
813348	Failure to access HTTPS virtual server after the flow control in SSL port improved.
813693	Event type of "infected" instead of "ems-threat-feed" logged when cached ems-threat-feed scan result used in FTP download.
813769	Fix WAD memory leak after enable ICAP profile 'respmod-forward-rules'.
814199	Change FortiGate reference to FortiProxy in "update-server-location" of "config sys fortiguard".
814266	Fix TP Policy displaying explicit proxy service list and vice-versa.
814569	Physical FortiProxy keeps killing usbmuxd.
815203	Traffic forwarded to fw-server is always rebind with outgoing interface/ip despite of the masquerade configuration.

Bug ID	Description
815313	Fix WAD crash on wad_ssl_cert_check_auth_status().
816205	Fix uninitialized ses_ctx usr_addr.
817056	The inactivity timer is 30 minutes, and renewed any time it is given out by the pool for ICAP traffic, or when any traffic flows through the connection in either direction.
817173	Fix an issue where dst-addr iptables rules are incorrect.
817722	Second try to a URL using prefetch failed.
817750	Fix WAD crash when web-proxy.forward-server-group does not have server-list.
817770	Change default source port range to 1024-65001.
817979	Explicit-outgoing-ip is not learned when config changes fix.
818406	Client got 304 response if a cached object with vary headers and got expired.
819700	Fix traffic shaping on VLAN interface.
820084	Fetch IPsec tunnel status from strongSwan and display it in the GUI.
821242	ICAP bypassing yields to web traffic corrupted upon ICAP_server failure to response.
822015	Add support for ACI dynamic address in WAD.
823247, 823829	WAD user_info process memory leak.
824259	Too many redirections error with session based authenthication and web-auth-cookie.
825349	WAD crashed at wad_http_req_finished with signal 11.
826088	Agent-based NTLM authentication resulted in blank user entry and allowed traffic.
826385	Add missing file.
826441	Fix WAD firewall schedule config change does not take effect.
827900	Fix empty FortiView monitor pages.
830907	WAD can crash when building a proxy policy if an address group has no member.
831428	Corrupted forward-server caused WAD crash.
832041	Filter wad log messages by process type or process ID.
832905	Crash when trying to access uninitialized array member.
833372	WAD crash due to long line reponse from server and SSH filter vulnerability.
833798	CID bug FORWARD_NULL in user info inventory.
834684	Configuring SNMP wiped kernel SNAT settings.
835180	Fix traffic shaping on newly configured VLAN interface.
835623, 837608	Embed base64 string images instead of URLs for WAD blocking page.
835625	Add kernel flow messages to help with kernel debugging.

Bug ID	Description
835739	Website will not reply if `Connection` uses the wrong letter case
836286	ICAP infection headers could not show the correct file name.
836464	The mac address type removed from firewall addresses, as it is not supported.
836723	HTTP/HTTPS requests that match a policy with an L7 address are not forward to the isolate server.
836915	DNS queries fail with dnsfilter applied.
837598	cloudinitd crash when deploying FortiProxy on AWS.
837729	Bypass interface kernel driver reset after rebooting.
838888	Fix HA sequential upgrade.
838910	WAD crashes on attaching history traffic stats to NULL tcp_port from session.
840189	Rare case in HA configuration caused kernel panic.
840680	Fix SSLVPN connection issue.
841632	Add bypass URLs to HTTP isolator check .
842338, 842826	Fix VPN widgets in the GUI.
842469	ZTNA access stuck when going through TCP-fwd towards HTTPS with a deep-inspection profile.
842840	Fix kernel panic when form HA A/P mode.
842926	Failure to perform SNAT when creating an FTP PASSIVE mode data channel.

www.fortinet.com