



FortiConverter - Release Notes

Version 7.0.2

TABLE OF CONTENTS

Introduction	3
What's new	4
System requirements	5
Upgrading	6
Supported versions and conversions	7
FortiGate Conversions	7
Exception	12
FortiADC conversions (Beta feature)	13
Resolved issues	14
Known issues	15

Introduction

This document provides installation instructions and requirements, resolved issues, and known issues for FortiConverter 7.0.2, build 0240.

FortiConverter provides a solution for the conversion of numerous firewall configurations into a FortiOS-compatible format. It currently supports the conversion of Cisco, Check Point, Juniper, SonicWall, Palo Alto Networks, Forcepoint, Trend Micro, Vyatta, Sophos, WatchGuard, Huawei, Alcatel-Lucent Brick, and FortiGate configurations.

FortiConverter also supports the conversion of load balancers into FortiADC configurations. Currently F5 and Radware load balancers are supported.

In addition, FortiConverter can convert Snort IPS rules to custom signatures, Bluecoat proxy, and IBM IPS sensor.

In this version, FortiConverter supports converting configurations into FortiOS v7.4. It also supports converting transparent mode configurations of Cisco and Check Point. Multiple firewalls can be selected in Check Point Provider-1 conversion.

Some features about application conversion are added. Policy-based FortiGate configurations can be converted into profile-based conversions now. In Palo Alto conversions, users can map Palo Alto applications into FortiGate applications and apply them into converted policy-based firewall policies.

For all conversions, you can complete conversion and view the results on the tuning page. All other functionality is disabled until you upgrade to the full license. In most cases, this limited functionality is sufficient to evaluate the product.



If your license expires and you do not renew the license, the functionality reverts to the trial version.

FC-10-CON01-401-01-12 1-year multi-vendor configuration migration tool for building FortiOS configurations, Windows OS is required.

FC-10-CON01-401-02-12 1-year renewal multi-vendor configuration migration tool for building FortiOS configurations, Windows OS is required.

For additional documentation, please visit: <https://docs.fortinet.com/product/forticonverter/>.

What's new

This release contains the following new features and enhancements:

- Supports converting configurations into FortiOS 7.4.
- Supports converting policy-based FortiGate configurations into profile-based configurations.
- Supports import CSV mapping from Palo Alto applications into FortiGate applications.
- Supports dynamic address groups in Palo Alto conversions.
- Supports transparent mode in Check Point and Cisco conversions.
- Supports converting multiple firewalls in Check Point Provider-1 conversions.
- Supports FortiADC conversions from F5 and Radware. (Beta feature)

System requirements

FortiConverter is tested to run on the following Microsoft Windows 64-bit platforms:

- Microsoft Windows 11
- Microsoft Windows 10
- Microsoft Windows 8
- Microsoft Windows Server 2022
- Microsoft Windows Server 2019
- Microsoft Windows Server 2016
- Microsoft Windows Server 2012

If your Windows OS or Windows Server version isn't listed above, contact FortiConverter support at fconvert_feedback@fortinet.com.

Upgrading

FortiConverter has no special upgrade requirements. You may overwrite an existing installation with a different version. However, please do not uninstall the existing version, as the original DB binaries are required during database migration.

For additional support, contact fconvert_feedback@fortinet.com.

Supported versions and conversions

FortiConverter can translate configurations from the following vendors and models. Unless noted as an exception below, conversions only support IPv4 unicast policy.

If FortiConverter cannot properly translate some of the supported configurations listed from below table, please kindly contact our product support email alias fconvert_feedback@fortinet.com

FortiGate Conversions

Vendor	Models	Versions	Convertible Objects
Alcatel-Lucent	Brick	ALSMS v9.x	<ul style="list-style-type: none"> Interface (physical, logical, loopback, PPPoE) Addresses & Address Books Partitions Services & Service Books Static Routes Zone rule set
Bluecoat	SGOS	6.5.10 6.6.4.2 6.7.4 7.0	<ul style="list-style-type: none"> Addresses & Address Groups Proxy Address (group) Service Proxy Policy
CheckPoint	SmartCenter	NGX R65 onward	<ul style="list-style-type: none"> Interface Addresses & Address Groups Local Users & Groups NAT Negate Cell Policies (rulebases.fws/*.csv) RADIUS, TACACS+, LDAP Rules (rulebases.fws/*.csv) Schedules Services & Service Groups

Vendor	Models	Versions	Convertible Objects
	VSX		<ul style="list-style-type: none"> Static Routes Traditional IPSec site-to-site VPN (Support only before R80.10) Simplified IPSec site-to-site VPN
	Provider-1		
Cisco	ASA	7.x onward	<ul style="list-style-type: none"> ACLs Addresses & Address Groups DHCP Servers DNS Servers Interface IP Pools Local Users & Groups NAT (Central NAT) RADIUS, TACACS+, LDAP Services & Service Groups Static Routes VPN
	FWSM	3.x onward	
	IOS	10.x to 12.x	
		15.x	
	PIX	5.x onward	
	FTD (LINA)	6.x onward	
	IOS XR	4.x/5.x/6.x	<ul style="list-style-type: none"> Addresses & Address Groups & FQDNs Interface IP Pools Policies Services & Service Groups Static Routes
		Nexus	
FortiGate	FortiOS	FOS5.2 and above	<p>FortiGate configuration can be converted based on the version of the target FortiGate device. However, note that</p> <ul style="list-style-type: none"> Older features might be deprecated and may not be fully

Vendor	Models	Versions	Convertible Objects
			<p>converted over.</p> <ul style="list-style-type: none"> The review is necessary. After importing the converted configuration, any CLI commands that have not successfully imported can be reviewed on the page. For more details, please see "FortiGate configuration migration" section in the admin guide.
Huawei	USG Series		<ul style="list-style-type: none"> Interface Zone Addresses & Address Groups Services & Service Groups Policy Route Zone IPSec Policy (VPN) Security Context Nat Policy (SNAT) Nat Server (VIP)
IBM	PAM		IPS Sensor
Juniper	SSG/ISG	ScreenOS 4.x, 5.x, 6.x	<ul style="list-style-type: none"> Addresses & Address Groups & FQDNs DHCP Servers & Clients & Relays Interfaces Static Routes Services & Service Groups Policies VIPs/MIPs NAT IP Pools VPN Local Users & Groups

Vendor	Models	Versions	Convertible Objects
			<ul style="list-style-type: none"> • RADIUS & LDAP • Zones
	SRX	JunOS 10.x onward	<ul style="list-style-type: none"> • Addresses & Address Groups & FQDNs • DHCP Servers & Client & Relay • Interfaces • IP Pools • Local Users & Groups • NAT • Policies • RADIUS & LDAP • Services & Service Groups • Static Routes • VIPs/MIPs • VPN (IPSec site-to-site) • Zones • Routing-instances (virtual-router)
	MX	Juno OS 10.x to 12.x	<ul style="list-style-type: none"> • Addresses & Address Groups & FQDNs • Interfaces • IP Pools • Policies • Services & Service Groups • Static Routes
Forcepoint	Sidewinder	7.x onward	<ul style="list-style-type: none"> • Addresses & Address Groups & FQDNs • Interfaces • IP Pools • Policies • Services & Service Groups • Static Routes • NAT (Policy NAT only)
	Stonesoft	5.7 onward	<ul style="list-style-type: none"> • Addresses & Address Groups • Interfaces • Policies/ Sub-policy • Alias

Vendor	Models	Versions	Convertible Objects
			<ul style="list-style-type: none"> • Services & Service Groups • Static Routes • NAT
Palo Alto Networks	PAN OS	PAN-OS 1.x onward	<ul style="list-style-type: none"> • Addresses & Address Groups & FQDNs • Interfaces • Local Users & Groups • NAT • Policies • Schedules • Static Routes • Services & Service Groups • Zones • VPN (GlobalProtect VPN not supported) • Panorama
Snort			IPS rules
SonicWall	TZ Series NSA Series	SonicOS 4.x onward	<ul style="list-style-type: none"> • Addresses & Address Groups & FQDNs • DHCP Servers & Clients & Relays • Interfaces • Local Users & Groups • NAT • Policies • Schedules • Services & Service Groups • Static Routes • Zones • VPN (IPSEC site to site) • SSLVPN

Vendor	Models	Versions	Convertible Objects
Sophos	XG Series	SFOS 17.0 - 17.5 MR3	<ul style="list-style-type: none"> Interface Zone Addresses & Address Groups Service & Service Groups Users & User Groups Policy NAT (XG supports traditional NAT merge and SG model supports central NAT mode only)
	Cyberoam	Cyberoam OS 10.6.3 onward	
	SG Series	6.6 onward	
Tipping Point	IPS	4.5	<ul style="list-style-type: none"> Addresses & Address Groups Policies Services & Service Groups
Vytta	VyOS	5.2 to 6.7	<ul style="list-style-type: none"> Interface Zone Addresses & Address Groups Services & Service Groups Policy Route
WatchGuard	Firebox Series XTM Series	Fireware 11.3 onward	<ul style="list-style-type: none"> Interfaces Addresses & Address Groups Services & Service Groups Policies Static Routes IPSec VPN NAT

Exception

- Check Point to FGT conversion can support IPv4 multicast policy.
- Check Point, Cisco, and Juniper (Junos only) to FGT conversion can support IPv6 unicast policy.

- Bluecoat conversion supports FortiProxy mode which the generated CLI would be slightly different to FortiGate mode.

FortiADC conversions (Beta feature)

Vendor	Models	Versions	Convertible Objects
F5	BIG-IP	TMSH 12.x	<ul style="list-style-type: none">• Nodes• Pools• Virtual addresses• Virtual servers
Radware	Alteon	30.x	<ul style="list-style-type: none">• Real servers• Server groups• Virtual servers

Resolved issues

The resolved issues listed below don't list every bug that has been corrected with this release. For inquiries about a particular bug, please email support at fconvert_feedback@fortinet.com.

Bug ID	Description
912057	Checkpoint: Address Groups not converted
911075	Checkpoint: IPSEC VPN not converted
889498	Checkpoint: Merge output of FortiConverter for different VDOM output in FMG
897904	Blue Coat Address Object Conversion enhancements (X-Forwarded-For header)
880265	Checkpoint: Objects with IPv6 and IPv4 configured together are not converting.
900631	Checkpoint: Service Object not converting as expected.
880252	Checkpoint: Provider-1 section should allow selection of multiple VSYS in a domain
886311	Checkpoint: FortiManager conversion does not have 'set scope' for NAT policies
887185	User groups with No members in Sophos config file
882650	Sonicwall Conversion: Policy comment - Preserve the original comment
880261	Translate PAN's firewall application layer firewall policy issue
881269	One PAN policy is translated into two or three FGT duplicates policy
867852	Checkpoint VPN settings not converted in FortiConverter tool.
880825	NetScreen address group object not converted
909249	In Cisco conversion VIP objects with protocol UDP missing from the settings
880227	Cisco: Cannot convert object-group referenced policy
894850	Service ticket 8499164 Cisco ASA to FGT service object conversion issue
911918	'FGR60F' device needs to add in the FortiConverter Tool target device list
880269	Checkpoint: FortiManager conversion has error for command 'set _scope'
908333	Checkpoint: Parent-Child policy attributes

Known issues

The issues listed below do not include every known bug. For questions about a particular bug, please email FortiConverter support at fconvert_feedback@fortinet.com.

Bug ID	Description
908330	Checkpoint: Listed VDOMs are not accurate when Checkpoint version is R77.x
905512	To remove deleted interfaces of tuning page from the csv file
870590	Attribute dhgrp under vpn objects are not converted correctly
915225	"Split-tunneling-routing-address" is set to all for Cisco conversion for config vpn ssl web portal
914721	Mapped ip is not converted for Twice NAT
913414	Hard switch does not contain members even after correct mapping in the tool for Cisco
912365	Static router is not pulled out from the source config by FortiConverter tool for Sophos
906850	Sonicwall: Converted Zones are not referenced in NAT
888933	Remove # Error: Undefined srcaddr object '_ipv6' comment for valid ip6 firewall addresses
884822	Sonicwall NAT behavior fine tuning on FCONV
886265	Central NAT toggle button should be present for Watchguard conversion
880817	SRX5600 to FGT 6500F conversion and found that the converter is not converting certificate auth'd IPSec
875690	User missing firewall policy in Cisco conversion
870286	FortiGate upgrade not working as expected
870968	Half proposal set for vpn ipsec phase2-interface in Juniper ticket
871349	Converter tool fails to trim vpn ipsec phase1-interface names present in config router policy
913573	Cisco FTD: Merged rules are not correct
914222	Incorrect warning generated by tool for dhcp server ip range
912699	Cisco: Incorrect encryption algorithms set for vpn ipsec phase2 interface
909556	Sophos: 'Error' should be replaced as 'Warning' for user groups with empty members
909549	Sophos: To update the code for replacing the '(' with '[' brackets under user group objects naming convention

Bug ID	Description
909248	In Cisco conversion where in some policies dstaddr field not updated to internal IP
904563	Tool is not proceeding after Cisco ASA vdom config upload
889526	Checkpoint: Color code interface output



Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. 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 General Counsel, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.