

A decorative pattern of overlapping, multi-lined hexagons in a light blue color, set against a dark blue background, located at the top of the page.

FortiConverter - Release Notes

Version 7.0.3

A decorative pattern of overlapping, multi-lined hexagons in a light blue color, set against a dark blue background, located at the bottom of the page.

TABLE OF CONTENTS

Introduction	3
What's new	4
System requirements	5
Upgrading	6
Supported versions and conversions	7
FortiGate Conversions	7
Exception	14
FortiADC conversions (Beta feature)	14
Resolved issues	15
Known issues	17

Introduction

This document provides installation instructions and requirements, resolved issues, and known issues for FortiConverter 7.0.3, build 0315.

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, PFSense 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, Cisco Meraki and PFSense conversion are added into FortiConverter. For both of them, FortiConverter supports the conversion of interfaces, addresses, services, policies and NATs into FortiGate configurations.

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 Cisco Meraki conversion.
- Supports converting PFSense conversion.

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
			<ul style="list-style-type: none">• Static Routes• Traditional IPSec sito-to-site VPN (Support only before R80.10)• Simplified IPSec sito-to-site VPN
	VSX		
	Provider-1		

Vendor	Models	Versions	Convertible Objects
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 • IPPools • Policies • Services & Service Groups • Static Routes
		Nexus	
Meraki	N/A	<ul style="list-style-type: none"> • Addresses & Address Groups • Interfaces • L3 firewall rules • NAT (Central NAT only) • Services & Service Groups 	
FortiGate	FortiOS	FOS5.2 and above	FortiGate configuration can be converted based on the version of the target FortiGate device. However, note that

Vendor	Models	Versions	Convertible Objects
			<ul style="list-style-type: none"> • Older features might be deprecated and may not be fully converted over. • 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

Vendor	Models	Versions	Convertible Objects
			<ul style="list-style-type: none"> • VPN • Local Users & Groups • 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

Vendor	Models	Versions	Convertible Objects
			<ul style="list-style-type: none"> • Policies/ Sub-policy • Alias • 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
PFSense		15+	<ul style="list-style-type: none"> • Addresses & Address Groups • Interfaces • NAT (Central NAT only) • Policies • Services & Service Groups • Static routes
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

Vendor	Models	Versions	Convertible Objects
			<ul style="list-style-type: none"> VPN (IPSEC site to site) SSLVPN
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
971775	Forcepoint conversion: config firewall VIP has mappedip set as name instead of IP which is incorrect
971349	PaloAlto: Generate username and password under config system external-resource from set resource of PaloAlto config
970573	Checkpoint: IPSec related conversion issues
969683	Router access-list is not converted as expected for OSPF config
968939	Under config firewall policy, Firewall addrgrp object is set as src interface, instead its interface must be set in srcint field.
968766	DNS Group Name are not converted correctly for Sophos Conversion.
968477	Cisco Conversion-Under config user LDAP block, set dn '' is not set by tool though it is present in source.
967401	Juniper SSG : Duplicated policies are present in config firewall policy in the tool
967371	Juniper SSG: Tool is not able to trim the space at end of firewall address and its references are failing in policy
966202	Checkpoint: 'set name' for rules created by fconv for DNAT
966196	Checkpoint: VLAN IDs not converted for version R77
965434	URI can be supported as external threat feed for checkpoint
962468	PAN : In the config file, config firewall policy block is duplicated.
962466	PAN : Tool is showing wrong no. of policies in the table after conversion from NGFW policy mode to profile mode.
962465	Palo Alto - Source to NGFW policy mode---->policy to profile conversion.
962142	syntax change of set authentication 'md5' to 'message-digest' under router OSPF
962042	Checkpoint: VDOMs not listed correctly
961324	IPv6 addresses need to be categories under 'config firewall address6' for ForcePoint conversion.
960717	set set-community '4273472578', set set-weight 90, set set-local-preference can be added in config router route-map
960190	Loopback IP addresses are not pulled out from source config in the Forticonverter tool

Bug ID	Description
959790	config vpn ipsec phase2-interface duplicate entries are shown in the tuning page for Cisco ASA
958392	set ip6 in config firewall address6 needs to be in correct format for Sophos config
957849	Juniper: Convert static blackhole routes
957845	Juniper: BGP route-map conversion
957419	Check Point IPSec conversion issue
957161	Sonicwall: To change objects definition from iprange to subnet under firewall address to support in config router static
956450	Checkpoint: DNAT output needs adjustment for Policy Target and all
956438	Checkpoint: ALL_VDOMs output for firewall policy is not merged correctly
954976	config system accprofile should be present in global VDOM
954680	Static routes are not migrated for one vdom in PALO ALTO conversion
951399	Checkpoint: Need to create additional No NAT rules for SNAT
951134	NFR- High availability config conversion for Sophos SG firewall
950026	[NFR]-config firewall schedule onetime can be supported for third-party Palo-Alto
949212	Cisco: network address should be replaced with host address range under config vpn l2tp
961853	To disable target config upload when 'Convert from Policy mode to Profile mode' option is enabled for Fgt conversion
958993	Enhance FortiGate to FortiGate conversion by adding a warning message when operation modes are different
957830	Juniper: BGP community list not created
942611	Bluecoat url extension object conversion
862298	Bluecoat enhancements with FortiProxy on Bluecoat Layers
960706	"set set-aspath" prepend is not valid inconfig router route-map

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
958992	FortiGate to FortiGate conversion switch port speed and status settings not migrated
957817	Juniper: Prefix list IPs are not converted
884822	Sonicwall NAT behavior fine tuning on FCONV
880817	SRX5600 to FGT 6500F conversion and found that the converter is not converting certificate auth'd IPSec
865907	Bluecoat enhancements with FortiProxy on Bluecoat Objects
927460	Policy based ipsec policy is failing for cisco ASA
968771	Huawei (USG Series)- To convert local admin user accounts to fortigate
968394	Huawei conversion: Tool support for custom services 'echo-tcp' and 'msn-stun'
962055	Checkpoint: Split up DNAT rules where subnet is used in load-balance type
961095	NAT policy conversion issue
956445	Change naming convention of SNAT
889498	Checkpoint: Merge output of FortiConverter for different VDOM output in FMG
861765	VPN interface to be migrated by tool for checkpoint conversion
855315	Issues: firewall address6, addrgrp6, schedule recurring, policy are not generated correctly



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.