

A decorative pattern of concentric hexagons in a light blue color, scattered across the top dark blue header area.

FortiConverter - Release Notes

Version 7.0.1

TABLE OF CONTENTS

Introduction	3
What's new	4
System requirements	5
Upgrading	6
Supported versions and conversions	7
Resolved issues	13
Known issues	14

Introduction

This document provides installation instructions and requirements, resolved issues, and known issues for FortiConverter 7.0.1, build 0145.

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 can also convert Snort IPS rules to custom signatures; Also, the Bluecoat proxy, and IBM IPS sensor.

In this version, FortiConverter allows users to select multiple firewalls in Check Point SmartCenter conversions, and convert the selected firewalls into FortiGate VDOMs. Also JSON configs exported by the tool "ShowPolicyPackage" can be used as the input file of SmartCenter conversions.

Since Fortinet offers a more comprehensive and reliable config migration product named FortiConverter Service, product team decided to stop the support of the FortiGate migration "Device" mode feature from the FortiConverter tool.

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:

- Enable selecting multiple firewalls in Check Point SmartCenter conversion, and convert the selected firewalls into FortiGate VDOMs.
- JSON configs exported by the tool "ShowPolicyPackage" can be used as the input file of SmartCenter conversions.
- "Device" mode feature has been removed from FortiGate migration.

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 7
- 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

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 Static Routes Traditional IPSec site-to-site VPN (Support only before R80.10) Simplified IPSec site-

Vendor	Models	Versions	Convertible Objects
			to-site VPN
	VSX		
	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 • IPPools • Policies • Services & Service Groups • Static Routes
	Nexus	5.2/6.x/7.x	
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 converted over. • The review is necessary. After

Vendor	Models	Versions	Convertible Objects
			<p>importing the converted configuration, any CLI commands that have not successfully imported can be reviewed on the page.</p> <ul style="list-style-type: none"> 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 RADIUS & LDAP Zones
	SRX	JunOS 10.x onward	<ul style="list-style-type: none"> Addresses & Address

Vendor	Models	Versions	Convertible Objects
			Groups & FQDNs <ul style="list-style-type: none"> • 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 • Services & Service Groups • Static Routes

Vendor	Models	Versions	Convertible Objects
			<ul style="list-style-type: none"> 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.

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
856329	Zones are set to dstaddr instead of dstint
856224	Conversion From PAN to FGT - SSLVPN didn't convert to FGT and FGT Policy service missing from PAN config
854429	Duplicate vpn phase-1 name in different vdoms is not handled in forticonverter for cisco ASA
854395	# Warning: comment length overflowed:' for comment which doesn't exceed the comment limit
854192	FortiConverter not able to parse the interface members from the vsys -> vrouter block.
849833	Cisco FTD FQDN conversions
848712	Palo-alto ticket, ip addresses of logical interface associated with aggregate int. failed to convert over on Converter tool
846633	Add multiple interfaces in single firewall policy
843636	Unable to import config firewall proxy-address for bluecoat conversion
843453	NFR: Static route to be converted for bluecoat conversion
839046	For CISCO IOS conversion, Converter tool ignores some objects from central-snat-map
838744	Convert Disabled NAT rules
826098	Support for multiple policy.csv files import for Checkpoint VSYS
776890	When source config has interface with pppoe mode and has no reference, that interface drops in conversion when "Discard interface" is enabled
852838	"set vdom-mode multi-vdom" not getting deleted when converting a multi-vdom config into a single-vdom config
859286	Set proposal limitation for vpn phase1 and phase2 interface
859576	Sophos route interfaces are missing

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
853136	Rest Api import is failed for service object/interface in Forticonverter Tool
855315	Issues: firewall address6, addrgrp6, schedule recurring, policy are not generated correctly
856946	Dynamic Address Groups Migrated from Palo Alto to Fortinet
858087	gui-theme changed from 6.2.2 onwards for color red & from 7.0.0 for color blue
859986	10-config firewall service group script failed with no Error message given in the file.
859995	17-config-firewall-central-nat.txt contained objects reference which customer choose 'Do not Migrate'
838725	Palo Alto App mapping to FGT equivalent
824012	[Fortinet PS] FCON Option for VIP/IPPool pairs with Policy NAT
824458	6.2 or older versions, we shall add 'set feature-set proxy'.
847541	Add a conversion option to control generated source nat IP pool arp-reply status
838033	Failures of firewall vip, firewall address, vpn objects
857519	netmask line missing under dhcp server block
861849	CKP VSX Policy issues
861765	VPN interface to be migrated by tool for checkpoint conversion
861278	The alias name was not populated in WatchGuard conversions



Copyright© 2022 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.