FortiConverter - Release Notes

Version 6.0.1

TABLE OF CONTENTS

Introduction

This document provides installation instructions and caveats, resolved issues, and known issues for FortiConverter 6.0.1, build 0068.

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, McAfee, 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.

FortiConverter 6.0.1 provides a browser/server-based application. Since the last version, we no longer provide the legacy application. As a web application design, the database allows you to save conversions and support large source-firewall configurations. The new GUI design is intended to improve usability and provide a framework for new functionality.

The installer is available on the support site:

`FortiConverterSetup_6.0.1_Build0068.py.exe` is the new application.

The new applications use the same license key as a legacy tool and should install on the same host. **In 6.0.1, FortiConverter can also run on different windows users on the same machine.**

The FortiConverter 6.0.1 application now supports FortiOS from 6.0 to 6.4, Cisco Firepower conversions and IBM PAM IPS Sensor conversion, the new obfuscator tool to obfuscate your FortiGate configuration settings, and dozens of enhancements and bug fixes.

In FortiGate migration, the old design is adding back. Now, it runs on two modes: device, and offline mode. For device mode, the device connection is necessary for conversion and REST-API install; For offline mode, you have to input both the source and target default configuration, and manually upload the configuration to the device after conversion. Despite this, we still recommend using device mode to run FortiGate migration for a better user experience.

For all conversions, you can complete conversion and view the results on the tuning page. All other functionality is disabled until you upload the full license. In most cases, this limited functionality is sufficient to allow you 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 visithttps://docs.fortinet.com/product/forticonverter/.

What's new

This release contains the following new features and enhancements:

- Migration to FortiOS 6.4 is supported.
- Add support of **IBM PAM** IPS Sensor conversion.
- Add back the **offline mode** to FortiGate migration.
- Improve the Fortinet import wizards, including user interface, new tags filter, and new function to export the encrypted origin password.
- Add the **obfuscation tool** page to obfuscate FortiGate configuration settings.
- Add support for **WatchGuard IPsec VPN** and **NAT conversion**.
- New feature to split the interface pair view on the tuning page.
- Add ability to run the conversion of different windows users on the same host.
- **Cisco Firepower** conversion is now supported. The firewall objects and NAT are converted like Cisco ASA while the converter will deal with the different syntax in Policies between ASA and Firepower.

System requirements

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

- Microsoft Windows 10
- Microsoft Windows 8
- Microsoft Windows 7
- 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

The new application for FortiConverter has no special upgrade requirements. You may overwrite an existing installation with a different version.

If you want to upgrade the embedded PostgreSQL version, you may have to uninstall the tool and reinstall, the conversion data would not be lost.

*Note that FortiGate-to-FortiGate REST-API install is not backward compatible. You won't be able to enter the FortiGate conversion page, which was run by the old version of FortiConverter.

For additional support, contact fconvert_feedback@fortinet.com.

Supported vendors & configuration objects

FortiConverter can translate configurations from the following vendors and models.

- In some cases, FortiConverter can't translate some parts of the configuration because of dependencies or unsupported syntax and you must manually convert them.
- If the number of objects exceeds the maximum valid length for FortiGate or FortiManager, FortiConverter trims them.
- FortiConverter comes with two different applications, each capable of a different set of conversions. The Converter Application column shows which FortiConverter application to use for each conversion.

Unless noted as an exception below, conversions only support IPv4 unicast policy.

Vendor	Models	Versions	Convertible Objects
Alcatel-Lucent	Brick	ALSMS v9.x	• Interface (physical, logical, loopback, PPPoE) • Addresses & Address Books • Partitions • Services & Service Books • Static Routes • Zone rule set
Bluecoat	SGOS	6.5.10 6.7.4	• Addresses & Address Groups • Proxy Address (group) • Service • Proxy Policy
CheckPoint	SmartCenter	NGFP1 (4.0) to NGX R80	• 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

Vendor	Models	Versions	Convertible Objects
Cisco	Provider-1	NGX R65 to R80	• VPN communities (IPSec site-to-site)
	ASA	7.x/8.x/9.x	• 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/4.x	
	IOS	10.x to 12.x	
		15.x	
	PIX	5.x/6.x/7.x/8.x	
	Firepower	6.x	
	IOS XR	4.x/5.x/6.x	• 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	FortiGate configuration can be converted based on the version of the target FortiGate device (We suggest to migrate to FortiOS 6.0 and above). However, note that • Older features might be deprecated and may not be fully converted over. • The review is necessary. After

Vendor	Models	Versions	Convertible Objects
			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" and "Reviewing errors after FortiGate import "sections in admin guide.
Huawei	USG Series		• 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	• 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

Vendor	Models	Versions	Convertible Objects
			• Zones
	SRX	JunosOS 10.x to 18.x	• 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	• Addresses & Address Groups & FQDNs • Interfaces • IP Pools • Policies • Services & Service Groups • Static Routes
McAfee	Sidewinder	7.x, 8.x	• Addresses & Address Groups & FQDNs • Interfaces • IP Pools • Policies • Services & Service Groups • Static Routes
Forcepoint	Stonesoft	5.7	• Addresses & Address Groups • Interfaces • Policies/ Sub-policy • Alias • Services & Service Groups

Vendor	Models	Versions	Convertible Objects
			• Static Routes • NAT
Palo Alto Networks	PAN OS	PAN-OS 1.x to 8.x	• Addresses & Address Groups & FQDNs • Interfaces • Local Users & Groups • NAT • Policies • Schedules • Static Routes • Services & Service Groups • Zones • VPN • Panorama
Snort			IPS rules
SonicWall	TZ Series NSA Series	SonicOS 4.x, 5.x, 6.x	• 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
Sophos	XG Series	SFOS 17.0	• Interface • Zone • Addresses & Address Groups • Service & Service Groups • Users & User Groups • Policy
	Cyberoam	Cyberoam OS 10.6	
Tipping Point	IPS	4.5	• Addresses & Address Groups

Vendor	Models	Versions	Convertible Objects
			• Policies • Services & Service Groups
Vytta	VyOS	5.2 to 6.7	• Interface • Zone • Addresses & Address Groups • Services & Service Groups • Policy • Route
WatchGuard	Firebox Series XTM Series	Fireware 11.3 to 12.1	• 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.
- Juniper (Junos only) can support converting the consolidated policy to FortiOS v6.2 configuration.

Resolved issues

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

Bug ID	Description
640648	Vlan interface mappings not reflected in output.
638741	Checkpoint service objects to FGT default service objects.
636974	BIT - Checkpoint DCE service conversion.
634716	Cisco Firepower: Converter failed in root.
633549	F models are not listed in the dropdown menu while selecting Fortigate device.
643173	Cicso ASA: NAT rule getting incorrectly converted.
640254	Checkpoint: Getting "NAT tuning job initiation failed" after selecting policy for "ZF_AMERICA_internal" domain.
639674	Cisco: Static routes fail because of incorrect interface names.
638950	Firewall policy conversion could not find IPv6 address/address groups.
638234	Sonicwall: DNS Server settings are not converted.
638037	Checkpoint Schedules do not convert as expected.
637534	Cisco-IOS: DHCP server settings are not getting converted.
636876	Cisco: Blank value for Destination in Static routes.
636868	Cisco: Phase2 parameters has an undefined DST name that contains XSS vulnerable characters.
634588	NFR Obfuscate IP addresses etc on FortiConverter option.
634442	Improving Trimming logic for over length objects containing similar names.
634094	Palo Alto: Trimming VPN phase 1 object fails as it enforces to add proposal parameters.
634083	PaloAlto: Error message contains quotes that fails the config import.
638977	Cisco SSL VPN group-url conversion.
638976	Site-to-Site VPN migration is not happening sequentially based on the Cisco configuration.
638633	Checkpoint - Service object conversion issue.
638238	Cisco: SSL VPN Pool is incorrectly assigned.

Bug ID	Description
637478	SonicWall static IPs in DHCP are not converted..
634195	Please add visibility of "Negate" in FortiConverter Tuning Policy view.
633877	NewLine on Policy comments when selecting multiple Policy comments.
630782	Add "set send-deny-packet enable" where CP action is reject.
629997	Virtual IP conversion from Cyberoam-Sophos config to FortiGate.
629568	Huawei - Static route Interfaces to be determined by the Interface IP settings.
628240	Central NAT rules are not converted when the output format is FortiManager.
628097	FortiConverter does not create rule with DST "all" as expected.
627312	Huawei - Any policy which has "LOCAL" zone shall be converted as Local-in policy on FGT.
627301	Huawei - HRP zone to be ignored.
627246	Huawei - NAT Block Size IPPOOLS should be converted.
639649	Watchguard: Static routes fail due to blank interface.
639646	Watchguard: IPSec tunnel interfaces are not getting converted.
608516	Support Cisco ASA user-group keyword in ACL.
631131	Support IBM IPAM signatures.
642927	Cisco ASA 5505 conversion interface configuration.
607271	Cisco ASA Convert User VPN Configuration.
573255	PAN sometimes generate duplicate interfaces.
608516	Support Cisco ASA user-group keyword in ACL.
631131	Support IBM IPAM signatures.
642927	Cisco ASA 5505 conversion interface configuration.
607271	Cisco ASA Convert User VPN Configuration.
573255	PAN sometimes generate duplicate interfaces.

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
645199	Sonicwall: DHCP settings causes the Fortigate to enter a loop which renders it inaccessible.
607831	Stonesoft:Duplicate IP pools should be removed after conversion.
607885	Stonesoft: Incorrect VDOM association.
607869	Stonesoft: Undefined address referenced.
640768	Cisco: SSL VPN port is incorrectly mapped.
624008	Cisco IOS: VLANs don't have any physical interface associated with them.
550192	[FortiConverter] System admin account & trusted hosts shall be converted properly while FGT to FGT conversion.
607123	FGT-FGT conversion cannot parse out FOS version and build info.
642395	[Service Ticket] Check Point conversion central NAT interface issue.
600386	CVE-2019-9193 postgresql allows run system commands through COPY SQL command.
580729	The Check Point original policy is still there after central NAT merge.
640726	Getting "Fail to prepare output directory" after IPSEC VPN page.