FortiConverter - Release Notes

Version 5.6.3

TABLE OF CONTENTS

Introduction

This document provides installation instructions and caveats, resolved issues, and known issues for FortiConverter 5.6.3, build 0587.

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

FortiConverter can also convert Snort IPS rules to custom signatures and Bluecoat proxy.

FortiConverter 5.6.3 provides a new browser/server based application, in addition to the legacy application.

Designed as a web application, the database allows you to save conversions and support large source-firewall configurations. The new GUI designed is intended to improve usability and provide a framework for new functionality.

There are two installers available on the support site:

- `FortiConverterSetup_5.6.3_Build0587.exe` is the legacy application.
- `FortiConverterSetup_5.6.3_Build0587.py.exe` is the new application.

Both the legacy and the new applications use the same license key and should be installed on the same host.

The FortiConverter 5.6.3 new application supports Cisco ASA, PIX, FWSM, and IOS, Check Point, Juniper SRX, SSG, and MX, Sophos, Vyatta, SonicWALL, Palo Alto, McAfee(Stonesoft), WatchGuard, Huawei, conversions, FortiGate migration, Snort IPS, and Bluecoat proxy-policy conversion. Use release 5.6.3 of the legacy application for all other supported conversions.

FortiGate to FortiGate migration is redesigned in this release. With the new import page, it's able to import converted configurations directly to the target device with FortiOS 6.0 and 6.2.

FortiGate bulk conversion also supports simultaneously conversion for more than one source configuration with the same model to establish the restorable configurations.

For all 3rd party conversions, you can complete conversion and view the results on the tuning page. All other functionality is disabled until you upload to full license. In most cases, this limited functionality is sufficient for evaluation purpose.

*Note that FortiGate-to-FortiGate migration is no longer an extended support to tune or download the converted configuration on the import page.

If your license expires and you do not renew the license, 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:

- **Fortinet Conversion** has new designed REST API import page and now supports bulk conversion.
- **Huawei USG Firewall Conversion** is now supported.
- **Bluecoat (Beta) Conversion** is now supported to convert proxy-policy in the new application.
- Supports converting consolidated policy in **Juniper Junos Conversion**.
- Supports central NAT conversion for **Juniper ScreenOS Conversion**.
- Supports central NAT conversion for **Stonesoft Conversion**.
- New SSL VPN tuning page in **Cisco Conversion** and **SonicWall conversion**.

System requirements

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

- Microsoft Windows 10
- Microsoft Windows 8 (32-bit and 64-bit)
- Microsoft Windows 7 (32-bit and 64-bit)
- 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

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

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 applicat ion 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 • VPN communities (IPSec site-to-site)
	Provider-1	NGX R65 to R80	

Vendor	Models	Versions	Convertible Objects
Cisco	ASA	7.x/8.x/9.x	• Interface • ACLs • Addresses & Address Groups • DHCP Servers • DNS Servers • DNS Servers Interfaces • IPPools Local Users & Groups • NAT • RADIUS, TACACS+, LDAP • Services & Service Groups • Static Routes • VPN • SSLVPN (ASA only)
	FWSM	3.x/4.x	
	IOS	10.x to 12.x 15.x	
	PIX	5.x/6.x/7.x/8.x	
	IOS XR	4.x/5.x/6.x	• Addresses & Address Groups & FQDNs • Interface • IP Pools • 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 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.

Vendor	Models	Versions	Convertible Objects
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)
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 • 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)

Vendor	Models	Versions	Convertible Objects
			• 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
	Stonesoft	5.7	• Addresses & Address Groups • Interfaces • Policies/ Sub-policy • Alias • Services & Service Groups • 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

Vendor	Models	Versions	Convertible Objects
			• 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 • 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

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
592762	Cisco: Setting DNS-servers under "config vpn ssl web portal" fails
592760	Cisco: The index of "config match" duplicates under "config user group"
592753	Cisco: Setting URL for "VPN SSL web portal" objects fails because of incorrect command
594736	Cisco: Few SNAT rules are missing in the conversion output
595417	Cisco: NAT tuning job initiation failed
588735	Cisco: mapped-ip has a blank value under firewall VIP
588732	Cisco: Undefined interface DMZ1 referenced in firewall VIPs and SNAT
588729	Cisco: Blank value for extip for a firewall VIP object
592759	Cisco: tunnel-mode command failed under vpn ssl web portal
592748	Cisco: web-mode command failed under vpn ssl web portal
581791	Cisco: srcintf-filter to be added while converting static NAT (1 to 1 NAT) to VIP on FOS 6.2
577166	Cisco: DHCP Server configuration not completely migrated to FGT CLIs
566831	Cisco: NAT policy to perform source NAT for the Object group has to be CSNAT policy and not VIP
566869	Cisco: Granular options while converting Cisco NAT
564909	Cisco: VPN routes converted from Backup peer IP config should add a higher AD in routing configuration to sec int
585432	Cisco: setting usrgrp and authusrgrp fails in IPSec VPNs
590460	Cisco: IPv6 Firewall address and address group objects seems to be invalid
586096	Checkpoint: VPN Phase 1 setting proposal fails
581606	Checkpoint: Firewall VIP fails because of incorrectly placed "edit" command while setting src-fitler
581560	Checkpoint: Setting groups in firewall policy fails
580695	Checkpoint: Peer type is empty for vpn ipsec object during renaming the object on tuning page

Bug ID	Description
580688	Checkpoint: Firewall vipgroup setting fails because interface is not set
579056	Checkpoint: The command to set dst-addr under Firewall central-snat fails
586096	Checkpoint: VPN Phase 1 setting proposal fails
537433	Checkpoint: FortiOS v6.0 central nat conversion issues
568115	Checkpoint Provider-1: Conversion error - NAT tuning job initiation failed
570784	Fortinet: Migration security profile's statistics didn't convert properly
593626	Juniper SSG: Policy-based VPN not getting converted
595034	Juniper SRX: Import accprofile command errors
581786	Juniper SRX: Real interfaces should associated in VIP than a Zone
590609	Juniper SRX: Objects called in central-snat-map rules are not present in address database
590601	Juniper SRX: IP pools are not converted when SRX config has Routing instances
591498	Juniper SRX: Ability to convert policy annotate to comments
586382	Palo Alto: Many "tunnel" interfaces are referenced throughout the config but they are not defined anywhere
588498	Palo Alto: VIP incorrect interface and ip
586380	Palo Alto: src-subnet and dst-subnet do not have subnet mask set in phase2 interface objects
586375	Palo Alto: Many phase1 interface objects do not have remote-gw set which cause the object to fail
586370	Palo Alto: Phase2 interface objects don't seem to work in the system zones
584557	Palo alto: Loopback interface isn't defined
584554	Palo alto: Few interfaces have invalid IP addresses
584561	Palo alto: VPN IPSec phase2 contains undefined src and dst subnets
590772	SonicWall - MAC addresses objects not converted
587909	SonicWall: Router static and router policies have blank interface values
586889	SonicWall: Undefined destination address used in router static
581721	SonicWall: Invalid firewall IPPool
581720	SonicWall: vpn ssl web portal web mode value is blank
581698	SonicWall: Setting a VLAN interface as the dst-intf under Firewall central NAT fails

Bug ID	Description
581693	SonicWall: Remote gateway must be IP address under VPN IPsec phase1
581004	SonicWall: Blank interfaces showing up in system interface after conversion
561253	Vdom wrapper didn’t apply when Vdom enable and in using CLI feature

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	Description
Bug	Description
564891	Incorrectly firewall policy created for the new VPN tunnels
535354	Cisco ASA IPSEC VPN ACL conversion bug
592179	Checkpoint - wildcard fqdn objects not properly converted
569419	Fortinet wildcard FQDN address should not be used in the firewall policy.