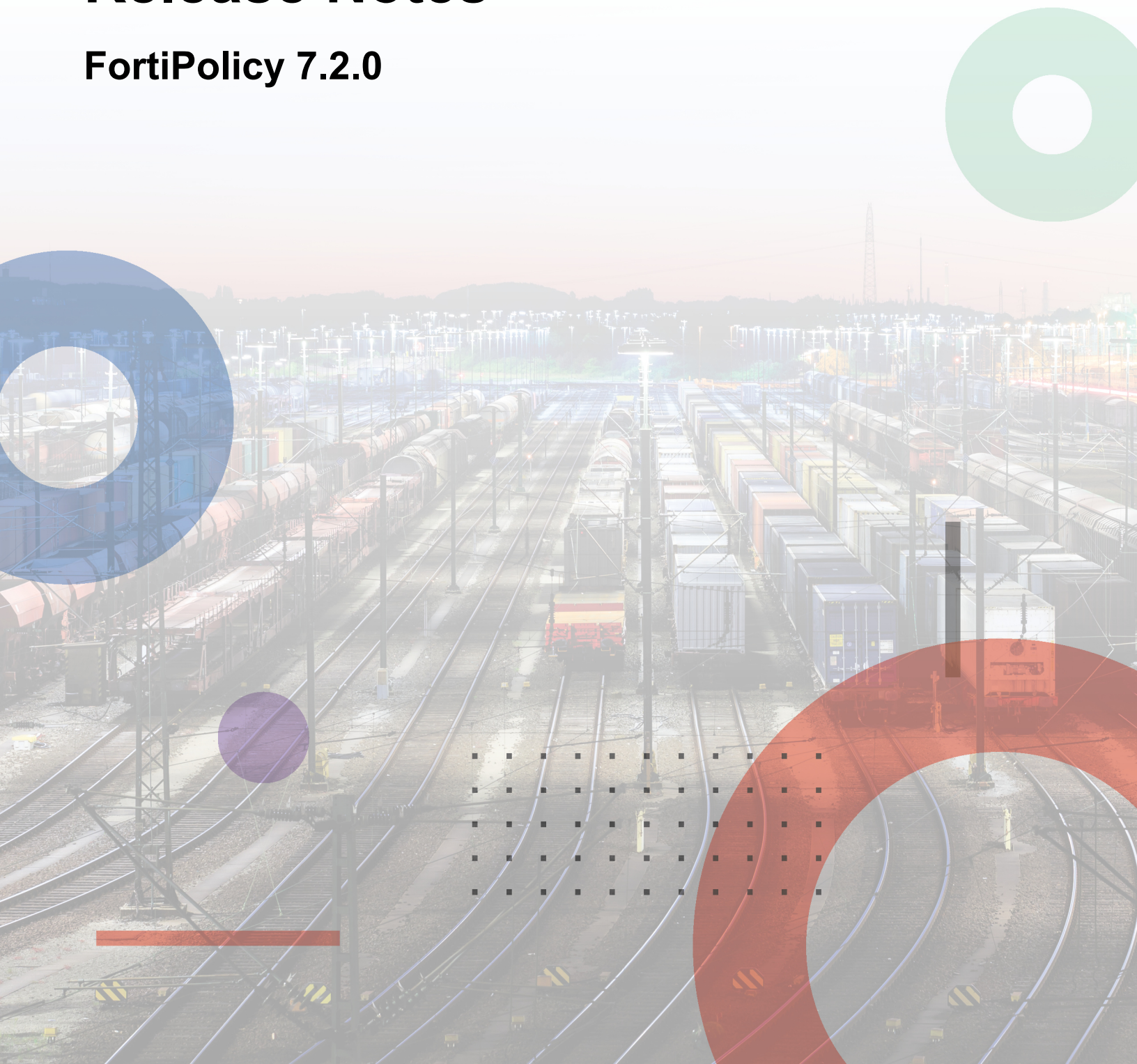
FORTINET

Release Notes

FortiPolicy 7.2.0



FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

July 21, 2022
FortiPolicy 7.2.0 Release Notes
64-720-796172-20220721

TABLE OF CONTENTS

Change log

Date	Change Description
July 20, 2022	Initial release
July 21, 2022	Added the release build number and bug 828039.

Introduction

FortiPolicy is the first containerized security platform that implements and automates security orchestration with full-flow inspection and segmented and microsegmented policy enforcement while auto-scaling to accommodate infrastructure changes.

This document provides the following information for FortiPolicy 7.2.0 build 0021:

Product integration and support

The following table lists FortiPolicy 7.2.0 integration and support information:

Web browsers	Latest version of Google Chrome
FortiGate	Running FortiOS 7.0.6 and higher
FortiSwitch	One or more managed FortiSwitch units running FortiSwitchOS 7.0.0 or higher

Virtualization environment

VMware vCenter Server	Version 6.0 or 6.5
VMware vSphere	Version 6.5 and higher
VMware ESXi	Version 6.x and above

ESX resource requirements

FortiPolicy component	vCPU requirements	VM requirements
FortiPolicy management plane	10 vCPUs	1 VM

Open ports

The following table lists the ports that FortiPolicy needs for communication through a firewall.

Service or program	Protocol	Incoming ports	Outgoing ports	Internal ports
SSHD	TCP	22		
DNS	TCP, UDP		53	
NTP	UDP		123 outbound queries to NTP servers from FortiPolicy	123 to FortiPolicy
Web access	UDP	80, 443		FortiPolicy port 5601
Connection between FortiPolicy and Security Fabric	TCP		8013 and 443	
Connection between FortiGate and FortiPolicy	UDP 4739	Syslog port for NetFlow	Syslog port for NetFlow	
For telemetry uploads to fortipolicy.fortinet.com	TCP	sxti.shieldx.com:443	sxti.shieldx.com:443	

Required management ports

The following table lists the required management ports.

Service or program	Protocol	Incoming ports	Outgoing ports	Internal ports
Web access	TCP	80		FortiPolicy port 5601
Web access	TCP	443		FortiPolicy port 5601

Services available

- Automated firewall policy
- Application-level visibility

- Complete user control
- Microsegment FortiSwitch traffic
- All FortiGate architectures
- Block east/west traffic

Known issues

The following known issues have been identified with FortiPolicy 7.2.0. For inquiries about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

Bug ID	Description
—	FortiGate devices are supported only in NAT mode.
—	FortiLink mode over a layer-3 network is not supported.
—	The FortiPolicy icon is not supported with 7.0.6.
—	For your security, the FortiPolicy window locks after a period of inactivity. By default, this period is 15 minutes. Any unsaved work will be lost when the FortiPolicy window locks. **Workaround:** Save your work before leaving FortiPolicy tasks.
—	Security events from the Security Fabric are not supported in the 7.2.0 release; they will be supported in a future release.
—	The deployed ACL rules displayed in the *Policy* > *Access Control* table are a read-only summary of all the rules that have been deployed. FortiPolicy does not support editing ACL rules after they are deployed to the FortiGate devices. All edits to the ACL rules must be done in the ACL tables on the FortiGate devices. The *Policy* > *Access Control* table allows you to add new rules, but, after they are saved and therefore deployed, they can only be edited on the FortiGate devices.
770259	Custom virtual domains (VDOMs) are not supported.
810391	In the 7.2.0 release, FortiPolicy does not provide data for *Risky Domains*, *Malware*, and *Sensitive Data* on the *Insights* > *Detections* page. The *Malware* widget will be supported in a future release.
810393	Exploit events in the *Insights* page are only available between any two workloads when traffic is evaluated by a FortiGate device and the “Exploit” filter is enabled in the FortiGate security profile.
814565	FortiPolicy supports a maximum of 600 workloads with FortiOS 7.0.6.
821065	Setting up the SMTP server so that faults are sent by email does not work. **Workaround:** Go to *Workspace* > *Logs* > *Faults* in the FortiPolicy UI to see any faults.

Bug ID	Description

828039	After the default user password expires in 90 days, the user cannot change the password when prompted.
	Workarounds:
	• Go to *Users* > *Login Rules* to disable the local password expiration.
	• Go to *Users* > *Login Rules* to change how many days before the password expires to a larger value.
	• Use the FortiPolicy REST API to change the password for an expired account:
	a. Get the REST API token:
	`curl -I -H 'X-Password: <password>' -H 'X-Username: <username>' -XPOST https://<IP_address>/shieldxapi --insecure`
	a. Change the password:
	`curl -X POST "https://<IP_address>/shieldxapi/v1/manage/users/changepassword?api_key=<key>" -H "accept: */*" -H "Content-Type: application/json" -d "{ \"newPassword\": \"<newpassword>\", \"oldPassword\": \"<oldpassword>\"}"`

www.fortinet.com