Conversion Guide

Configuration Converter to ATP/FLEX series

Version 6.2.0 edition 1

June 30, 2026

Contents

Introduction

Key Benefits

The Configuration Converter helps organizations streamline platform upgrades and reduce migration complexity when moving to newer Zyxel security appliances.

Key benefits include:

- **Reduce Migration Time**
  Automatically converts supported configurations, eliminating the need to manually recreate network and security settings.
- **Minimize Configuration Errors**
  Reduces the risk of human errors commonly introduced during manual migration.
- **Preserve Existing Security Policies**
  Retains supported firewall, NAT, VPN, routing, and network configurations to help maintain service continuity.
- **Simplify Hardware Refresh Projects**
  Enables a smoother transition from legacy USG and ZyWALL platforms to newer ATP, VPN, USG FLEX, and USG FLEX H series devices.
- **Accelerate Deployment**
  Allows administrators to focus on validation and optimization rather than rebuilding configurations from scratch.
- **Provide Migration Visibility**
  Generates detailed conversion reports, warnings, and error messages to help identify configuration items requiring manual review.

Purpose of Configuration Converter

The Configuration Converter is designed to simplify the migration process between Zyxel security appliance platforms by automatically translating supported configuration settings from a source device to a target device.

The converter helps preserve existing network, security, and VPN configurations during hardware upgrades, reducing manual reconfiguration effort and minimizing migration time.

Because hardware architectures, firmware capabilities, and feature availability may differ between platforms, some settings may be modified, partially converted, or excluded during the conversion process. After the conversion is completed,

administrators should review the conversion report and verify the converted configuration before deployment.

The Configuration Converter is intended to assist migration projects and should be used as part of a planned migration process. Final configuration validation and testing remain the responsibility of the administrator.

Supported Migration Paths

The Configuration Converter supports migration between selected Zyxel security appliance product families, including legacy USG and ZyWALL platforms and newer ATP, VPN, USG FLEX, and USG FLEX H series devices.

Supported migration scenarios include:

- USG → ATP Series
- USG → USG FLEX Series
- USG → USG FLEX H Series
- ZyWALL → VPN Series
- ZyWALL → USG FLEX Series
- ZyWALL → USG FLEX H Series
- ATP → USG FLEX H Series
- USG FLEX → USG FLEX H Series
- VPN → USG FLEX H Series

The converter automatically maps supported configuration objects, interfaces, policies, and VPN settings based on the selected source and target platforms.

Please refer to the **Supported Upgrade Paths** section for the complete model compatibility matrix and recommended migration paths.

Wireless Model Considerations

When migrating between wireless and non-wireless models, WiFi-related configurations require special attention:

- **Wireless to Non-Wireless Models**

  Wireless settings, SSIDs, radio profiles, and related WiFi configurations are not migrated.

- **Non-Wireless to Wireless Models**

  Wireless functionality is supported on the target device; however, WiFi settings must be configured manually after migration.

Administrators should review wireless configurations separately after completing the conversion process.

Supported Upgrade Paths

The configuration converter supports converting Zyxel USG to ATP, ZyWALL to VPN or USG to USG FLEX. Please refer to the supported model correspondence table.

Source Model	★ Recommended Upgrade (Primary Path)	Alternative Upgrade Options
USG FLEX 50 (USG20-VPN)	USG FLEX 50H / 50HP	—
USG20W-VPN*	USG FLEX 50H / 50HP	—
USG FLEX 50AX*	USG FLEX 50H / 50HP	—
USG FLEX 100	USG FLEX 100H / 100HP	—
USG FLEX 100W*	USG FLEX 100H / 100HP	—
USG FLEX 100AX*	USG FLEX 100H / 100HP	—
USG FLEX 200	USG FLEX 200H / 200HP	—
USG FLEX 500	USG FLEX 500H	—
USG FLEX 700	USG FLEX 700H	—
ATP100	USG FLEX 100H / 100HP	—
ATP100W*	USG FLEX 100H / 100HP	—
ATP200	USG FLEX 200H / 200HP	—
ATP500	USG FLEX 500H	—
ATP700	USG FLEX 700H	—
ATP800	USG FLEX 700H	—
VPN50	USG FLEX 100H / 100HP	—
VPN100	USG FLEX 200H / 200HP	—
VPN300	USG FLEX 500H	—
VPN1000	USG FLEX 700H	—
USG40	USG FLEX 50H / 50HP	USG FLEX 100 / ATP100
USG40W*	USG FLEX 50H / 50HP	USG FLEX 100W / ATP100W
USG60	USG FLEX 100H / 100HP	USG FLEX 200 / ATP100
USG60W*	USG FLEX 100H / 100HP	USG FLEX 200 / ATP100W
USG110	USG FLEX 200H / 200HP	USG FLEX 500 / ATP200
USG210	USG FLEX 200H / 200HP	USG FLEX 500 / ATP200
USG310	USG FLEX 500H	USG FLEX 700 / ATP500
USG1100	USG FLEX 700H	ATP800 / ATP700
USG1900	USG FLEX 700H	ATP800 / ATP700
ZyWALL 110	USG FLEX 200H / 200HP	USG FLEX 500 / VPN100
ZyWALL 310	USG FLEX 500H	USG FLEX 700 / VPN300
ZyWALL 1100	USG FLEX 700H	VPN1000

* **Wireless Model Considerations**:

- Wireless → Non-Wireless: WiFi settings are not migrated.
- Non-Wireless → Wireless: WiFi settings must be configured manually.

Before You Start

Zyxel Converter is a migration tool, not a migration service. It is designed to assist a properly planned and verified migration process;

To ensure a successful conversion and prevent device lockout, please review and complete the following prerequisites before starting the conversion:

Please review the following requirements before starting the conversion:

1. **File Naming**
   The uploaded configuration filename must be **fewer than 40 characters**, as this name will be used for the converted policy package.
   File name format: {original file name 40 characters}_converted-XXXXXX.conf
   XXXXXX is a serial number that generated automatically.

Example: usg110-2026aprilproject_converted-123456.conf

   English only. The valid characters are [a-zA-Z0-9~_=-].

2. **Feature Compatibility**
   Some configurations include advanced or unsupported features that cannot be automatically migrated. These features must be **manually removed** from the configuration file **before starting** the conversion.

   For example: **Device HA, LAG**.

3. **Firmware Compatibility**
   For best results, use the **latest ZLD firmware**. ZLD V4.32 or later is strongly recommended.

4. **Configuration Parameter Limits**
   Ensure your configuration does not exceed system limits. If limits are exceeded, the conversion will fail and a detailed error log will be generated for troubleshooting.

Post-Conversion Notice

After conversion, please review the generated log file to verify all changes applied during the conversion process.

Static Port/Interface Mapping

ZLD Platform

The converter has a static mapping rule to convert USG ports to ATP/USG FLEX/VPN ports. Followings are the static port mapping rule used by converter.

Strategic Architectural Details:

- SFP Port Conversion Strategy

Four strategic approaches are adopted for SFP port handling:

1. **Convert to Optional Port (opt)** — maximize deployment flexibility
2. **Convert to Secondary WAN (wan2)** — standardize dual-WAN architecture
3. **Convert to RJ45 general Port** — preserve HA heartbeat architecture
4. **Bypass SFP Port Conversion (No Conversion)**— no conversion for the SFP port

- Interface Mapping

1. Fixed-Zone Models: Interfaces are automatically remapped to match the target platform's predefined interface layout.
2. Configurable-Zone Models: Original interface assignments are preserved using 1:1 port mapping whenever possible.

Pxx indicates to the physical ports.
(xxx) indicates to the port role- zone Interface.
if all the ports are configurable then there is no (xxx) specific zone interface.

USG40(W) to USG FLEX 100(W)/ ATP100(W)

USG40(W)		P1(wan1)	P2(lan1)	P3(lan2)	P4(dmz)	P5(opt)
USG FLEX 100(W)/ ATP100(W)	P1(sfp)	P2(wan1)	P3(lan1)	P4(lan2)	P5(dmz)	P6(opt)

USG60(W) to ATP100(W)

The USG60(W) port 2 (wan2) will be mapped to ATP100(W) port 1 (sfp). The wan2 configuration may not work on ATP100(W).

USG60(W)	P1(wan1)	P2(wan2)	P3(lan1)	P4(lan2)	P5(dmz)	P6(guest)
ATP100(W)	P1 sfp (wan2)	P2(wan1)	P3(lan1)	P4(lan2)	P5(dmz)	P6(guest)

USG60(W) to USG FLEX 200

USG60(W)		P1(wan1)	P2(wan2)	P3(lan1)	P4(lan2)	P5(dmz)	P6(guest)

USG FLEX 200	P1(sfp)	P2(wan1)	P3(wan2)	P4(lan1)	P5(lan2)	P6(dmz)	P7(Res.)

USG110/210 to ATP200

The port 3 (opt) of USG110/210 will be converted to port 1 (SFP port) on ATP200.
Port 3 will be removed from opt port grouping after conversion.

USG110	P1(wan1)	P2(wan2)	P3(opt)	P4(lan1)	P5(lan2)	P6(Res.)	P7(dmz)
ATP200	P1(opt)	P2(wan1)	P3(wan2)	P4(lan1)	P5(lan2)	P6(dmz)	P7(Res.)

USG110/210 to USG FLEX 500

USG110/210		P1(wan1)	P2(wan2)	P3(opt)	P4(lan1)	P5(lan2)	P6 (Res.)	P7(dmz)
USG FLEX 500	P1(sfp)	P2(wan1)	P3(wan2)	P4(lan1)	P5(lan2)	P6(dmz)	P7(opt)	P8(Res.)

USG310 to ATP500

By default, interface on port 7 of USG310 will become interface on port 1 (SFP port) of ATP500 as shown in the following table. Interface on port 1 of USG310 will become interface on port 2 of ATP500, and et cetera.

USG310	P1	P2	P3	P4	P5	P6	P7	P8
ATP500	P2	P3	P4	P5	P6	P7	P1	P8

USG310 to USG FLEX 700

USG310	P1	P2	P3	P4	P5	P6	P7	P8						
USG FLEX 700	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14

USG1100/1900 to ATP700/800

The port on USG1100/1900 will be converted to the same port on ATP700/800.

USG1100/1900	P1	P2	P3	P4	P5	P6	P7	P8						
ATP700/800	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14

ZyWALL 110 to VPN100

The port 3 (opt) of ZyWALL 110 will be converted to port 1 (SFP port) on VPN100.
Port 3 will be removed from opt port grouping after conversion.

ZyWALL 110	P1(wan1)	P2(wan2)	P3(opt)	P4(lan1)	P5(lan2)	P6(Res.)	P7(dmz)
VPN100	P1(opt)	P2(wan1)	P3(wan2)	P4(lan1)	P5(lan2)	P6(dmz)	P7(Res.)

ZyWALL 110 to USG FLEX 500

ZyWALL 110		P1(wan1)	P2(wan2)	P3(opt)	P4(lan1)	P5(lan2)	P6(Res.)	P7(dmz)
USG FLEX 500	P1(sfp)	P2(wan1)	P3(wan2)	P4(lan1)	P5(lan2)	P6(dmz)	P7(opt)	P8(Res.)

ZyWALL 310 to VPN300

By default, port 7 of ZyWALL 310 will be mapped to port 1 (SFP port) of VPN300.

ZyWALL 310	P1	P2	P3	P4	P5	P6	P7	P8
VPN300	P2	P3	P4	P5	P6	P7	P1	P8

ZyWALL 310 to USG FLEX 700

The port mapping from ZyWALL 310 to USG FLEX 700 is one-to-one mapping.

ZyWALL 310	P1	P2	P3	P4	P5	P6	P7	P8						
USG FLEX 700	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14

ZyWALL 1100 to VPN1000

The port mapping from ZyWALL 1100 to VPN1000 is one-to-one mapping.

ZyWALL 1100	P1	P2	P3	P4	P5	P6	P7	P8						
VPN1000	P1	P2	P3	P4	P5	P6	P7	P8	P9	P10	P11	P12	P13	P14

Conversion Scopes

Following are features will be converted or partial convert.
After completing the conversion, please review the log file to identify any changes made during the process.
Some manual review or post-conversion adjustments are required.

Supported Features

The converter supports migration of the following configuration items:

Interface

- Physical Interfaces
- Logical Interfaces
- PPPoE Interfaces

Objects

- Address Objects
- Address Groups
- Service Objects
- Service Groups
- Schedule Objects

Users

- Local Users
- User Groups

Policies
- NAT Policies
- Firewall Policies
- Routing Policies

Networking
- DHCP Server
- DHCP Client
- DHCP Relay

VPN
- IPsec Site-to-Site VPN

Partially Supported Features

Due to differences in platform architecture, the following features will be migrated with limitations and may require manual review or post-conversion adjustment.

Security Profiles

Content Filtering (CF)
- Content Filtering profiles will be migrated.
- URL Filtering category settings (URL Threat Filter) will not be migrated.

Anti-Virus (AV)
- Multiple AV profiles will be consolidated into the default single profile on USG FLEX / ATP platforms.

Unsupported Features

The following configurations are not migrated by the converter:

IPv6
- IPv6 objects, rules, and related configurations are not supported.
- IPv6-specific configurations will be ignored during conversion.

Credentials and Certificates
- Certificates will not be migrated.
- Private keys (for example, VPN pre-shared keys) will be removed.
- The system will use the default certificate after conversion.

Licenses Services
- License information and subscribed services will not be migrated.

LAG Interface
- LAG (Link Aggregation Group) interfaces will not be migrated.

*Remove LAG configurations before conversion.

Schedules

- Schedule configurations will be removed.

Authentication Portal

- Customized Web Authentication portal and User Authentication (UA) portal files will not be migrated.
- Default portal profiles will be applied after conversion.

Other Unsupported Features

- Easy Mode*
- Device HA (Active-Passive mode)
- SSL VPN Application
- Application objects
- IDP (Intrusion Detection and Prevention)
- Facebook WiFi

*Easy Mode exception: When converting to VPN50, Easy Mode configuration will be migrated.

Platform-Specific Limitations

Some features supported on the source platform may not be available on the target platform. These features will be removed during conversion.

When Converting to ATP

The following USG/ZyWALL features are not supported on ATP platforms:

- ADP (Anomaly Detection and Prevention)
- Dynamic Guest
- Hotspot-related features:
  - Billing
  - Payment Service
  - Printer Manager
  - Free Time
  - Walled Garden
  - Advertisement

When Converting to VPN

The following USG/ZyWALL features are not supported on VPN platforms:

- Anti-virus
- IDP (Intrusion Detection and Prevention)

Configuration Parameter Limits

The converter validates configuration parameters to ensure they are within the supported limits of the target platform.

Configurations that exceed the supported limits may cause:

- Conversion failure
- Incomplete converted configuration files
- Failure when applying the converted configuration to the target device

Please review all warning and error messages generated during the conversion process.

Conversion Messages (Errors and Warnings)

During the conversion process, the converter generates messages to report the conversion status and any detected issues.

Warning Messages

Warnings indicate potential compatibility issues, unsupported limitations, or configuration conditions that may require attention.

The conversion process will continue, but manual review or post-conversion adjustment may be required before applying the converted configuration to the target device.

Error Messages

Errors indicate that the converter cannot complete the conversion successfully.

Example:
The configuration exceeds the supported or recommended limit for a specific parameter.

When an error occurs:

- The message will identify the related rule, object, or parameter that caused the issue.
- The generated configuration file may be incomplete and **must not be used on the target device**.

Source model 40 series

	Source	Target	Target	Target
Model	**USG40 series**	**USG FLEX 100 series**	**ATP100 series**	**VPN50**
Max. number of IPsec VPN tunnel	20	50	50	50

Max. bridge interface (physical port: Eth+ SFP /2)	2	2	2	2
Max. policy route rules	100	100	100	100
Max. user define trunk	4	4	4	4
Max. NAT virtual server number	128	128	128	128
Max. session limit per host rules (Firewall)	1000	1000	1000	1000
Max. address object number	300	300	300	300
Max. service object number	200	200	200	200
Max. schedule object number	32	32	32	32
Max. application object number	500	500	500	500
Max. LDAP server object number	2	2	2	2
Max. Radius server object number	2	2	2	2
Max. AD server object number	4	2	2	2
Max. A record number	32	64	64	64
Max. NS record number	8	8	8	8
Max. MX record number	4	8	8	4
Max. DHCP network pool (vlan+brg+ethernet)	14	15	15	15
Max. DHCP options (pre-defined + user defined) (per pool)	10	10	10	10
Max. number of Content Filtering profiles	16	16	16	16
Max. number of Application Patrol profiles	N/A	32	32	N/A
Max. URL Threat Filter allow list rule	N/A	1024	1024	N/A
Max. URL Threat Filter block list rule	N/A	1024	1024	N/A
Max. DNS Threat Filter allow list rule	N/A	1024	1024	N/A
Max. DNS Threat Filter block list rule	N/A	1024	1024	N/A

Source model 60 series

	Source	**Target**	**Target**
Model	**USG60 series**	**USG FLEX 200**	**ATP100 series**
Max. number of IPsec VPN tunnel	40	100	50

Max. bridge interface (physical port: Eth+ SFP /2)	4	8	2
Max. policy route rules	200	500	100
Max. user define trunk	4	8	4
Max. NAT virtual server number	256	256	128
Max. session limit per host rules (Firewall)	1000	1000	1000
Max. address object number	300	300	300
Max. service object number	200	500	200
Max. schedule object number	32	32	32
Max. application object number	500	500	500
Max. LDAP server object number	2	8	2
Max. Radius server object number	2	8	2
Max. AD server object number	4	8	2
Max. A record number	64	64	64
Max. NS record number	8	16	8
Max. MX record number	8	8	8
Max. DHCP network pool (vlan+brg+ethernet)	24	29	15
Max. DHCP options (pre-defined + user defined) (per pool)	10	15	10
Max. number of Content Filtering profiles	16	16	16
Max. number of Application Patrol profiles	N/A	32	32
Max. URL Threat Filter allow list rule	N/A	1024	1024
Max. URL Threat Filter block list rule	N/A	1024	1024
Max. DNS Threat Filter allow list rule	N/A	1024	1024
Max. DNS Threat Filter block list rule	N/A	1024	1024

Source model 110 series

	Source	**Target**	**Target**	**Target**
Model	**ZyWALL / USG110**	**USG FLEX 500**	**ATP200**	**VPN100**
Max. number of IPsec VPN tunnel	100	300	100	100

Max. bridge interface (physical port: Eth+ SFP /2)	8	16	8	8
Max. policy route rules	500	500	500	500
Max. user define trunk	8	16	8	4
Max. NAT virtual server number	256	1024	256	256
Max. session limit per host rules (Firewall)	1000	1000	1000	1000
Max. address object number	300	1000	300	300
Max. service object number	500	1000	500	500
Max. schedule object number	32	32	32	32
Max. application object number	500	1000	500	500
Max. LDAP server object number	8	16	8	8
Max. Radius server object number	8	16	8	8
Max. AD server object number	8	16	8	8
Max. A record number	64	128	64	64
Max. NS record number	16	16	16	16
Max. MX record number	8	16	8	8
Max. DHCP network pool (vlan+brg+ethernet)	29	88	29	29
Max. DHCP options (pre-defined + user defined) (per pool)	15	30	15	15
Max. number of Content Filtering profiles	16	32	16	16
Max. number of Application Patrol profiles	N/A	64	32	N/A
Max. URL Threat Filter allow list rule	N/A	1024	1024	N/A
Max. URL Threat Filter block list rule	N/A	1024	1024	N/A
Max. DNS Threat Filter allow list rule	N/A	1024	1024	N/A
Max. DNS Threat Filter block list rule	N/A	1024	1024	N/A

Source model 210

	Source	**Target**	**Target**
Model	**USG210**	**USG FLEX 500**	**ATP200**
Max. number of IPsec VPN tunnel	200	300	100

Max. bridge interface (physical port: Eth+ SFP /2)	8	16	8
Max. policy route rules	500	500	500
Max. user define trunk	8	16	8
Max. NAT virtual server number	512	1024	256
Max. session limit per host rules (Firewall)	1000	1000	1000
Max. address object number	500	1000	300
Max. service object number	500	1000	500
Max. schedule object number	32	32	32
Max. application object number	500	1000	500
Max. LDAP server object number	8	16	8
Max. Radius server object number	8	16	8
Max. AD server object number	8	16	8
Max. A record number	64	128	64
Max. NS record number	16	16	16
Max. MX record number	8	16	8
Max. DHCP network pool (vlan+brg+ethernet)	45	88	29
Max. DHCP options (pre-defined + user defined) (per pool)	15	30	15
Max. number of Content Filtering profiles	16	32	16
Max. number of Application Patrol profiles	N/A	64	32
Max. URL Threat Filter allow list rule	N/A	1024	1024
Max. URL Threat Filter block list rule	N/A	1024	1024
Max. DNS Threat Filter allow list rule	N/A	1024	1024
Max. DNS Threat Filter block list rule	N/A	1024	1024

Source model 310 series

	Source	**Target**	**Target**	**Target**
Model	**ZyWALL/USG 310**	**USG FLEX 700**	**ATP500**	**VPN300**
Max. number of IPsec VPN tunnel	300	500	300	300

Max. bridge interface (physical port: Eth+ SFP /2)	16	16	16	16
Max. policy route rules	1000	1000	500	500
Max. user define trunk	16	32	16	16
Max. NAT virtual server number	1024	1024	1024	1024
Max. session limit per host rules (Firewall)	1000	1000	1000	1000
Max. address object number	1000	2000	1000	1000
Max. service object number	1000	1000	1000	1000
Max. schedule object number	32	32	32	32
Max. application object number	1000	1000	1000	1000
Max. LDAP server object number	16	16	16	16
Max. Radius server object number	16	16	16	16
Max. AD server object number	16	16	16	16
Max. A record number	128	128	128	128
Max. NS record number	16	16	16	16
Max. MX record number	16	16	16	16
Max. DHCP network pool (vlan+brg+ethernet)	88	158	88	88
Max. DHCP options (pre-defined + user defined) (per pool)	30	30	15	30
Max. number of Content Filtering profiles	32	64	32	32
Max. number of Application Patrol profiles	N/A	96	64	N/A
Max. URL Threat Filter allow list rule	N/A	1024	1024	N/A
Max. URL Threat Filter block list rule	N/A	1024	1024	N/A
Max. DNS Threat Filter allow list rule	N/A	1024	1024	N/A
Max. DNS Threat Filter block list rule	N/A	1024	1024	N/A

Source model 1100 series

	Source	**Target**	**Target**	**Target**
Model	**ZyWALL/USG1100**	**ATP800**	**ATP700**	**VPN1000**

Max. number of IPsec VPN tunnel	1000	1000	500	1000
Max. bridge interface (physical port: Eth+ SFP /2)	16	16	16	16
Max. policy route rules	1000	1000	1000	1000
Max. user define trunk	32	32	32	32
Max. NAT virtual server number	1024	1024	1024	1024
Max. session limit per host rules (Firewall)	1000	1000	1000	1000
Max. address object number	2000	2000	2000	2000
Max. service object number	1000	1000	1000	1000
Max. schedule object number	32	32	32	32
Max. application object number	1000	1000	1000	1000
Max. LDAP server object number	16	16	16	16
Max. Radius server object number	16	16	16	16
Max. AD server object number	16	16	16	16
Max. A record number	128	128	128	128
Max. NS record number	16	16	16	16
Max. MX record number	16	16	16	16
Max. DHCP network pool (vlan+brg+ethernet)	152	158	158	158
Max. DHCP options (pre-defined + user defined) (per pool)	30	30	30	30
Max. number of Content Filtering profiles	64	64	64	64
Max. number of Application Patrol profiles	N/A	96	96	N/A
Max. URL Threat Filter allow list rule	N/A	1024	1024	N/A
Max. URL Threat Filter block list rule	N/A	1024	1024	N/A
Max. DNS Threat Filter allow list rule	N/A	1024	1024	N/A
Max. DNS Threat Filter block list rule	N/A	1024	1024	N/A

Source model 1900

	Source	Target	Target

Model	USG1900	ATP800	ATP700
Max. number of IPsec VPN tunnel	2000	1000	500
Max. bridge interface (physical port: Eth+ SFP /2)	16	16	16
Max. policy route rules	2000	1000	1000
Max. user define trunk	32	32	32
Max. NAT virtual server number	1024	1024	1024
Max. session limit per host rules (Firewall)	1000	1000	1000
Max. address object number	2000	2000	2000
Max. service object number	1000	1000	1000
Max. schedule object number	32	32	32
Max. application object number	1000	1000	1000
Max. LDAP server object number	16	16	16
Max. Radius server object number	16	16	16
Max. AD server object number	16	16	16
Max. A record number	128	128	128
Max. NS record number	16	16	16
Max. MX record number	16	16	16
Max. DHCP network pool (vlan+brg+ethernet)	152	158	158
Max. DHCP options (pre-defined + user defined) (per pool)	30	30	30
Max. number of Content Filtering profiles	128	64	64
Max. number of Application Patrol profiles	N/A	96	96
Max. URL Threat Filter allow list rule	N/A	1024	1024
Max. URL Threat Filter block list rule	N/A	1024	1024
Max. DNS Threat Filter allow list rule	N/A	1024	1024
Max. DNS Threat Filter block list rule	N/A	1024	1024