



# ZTNA Reference Guide

FortiOS 7.6



**FORTINET DOCUMENT LIBRARY**

<https://docs.fortinet.com>

**FORTINET VIDEO LIBRARY**

<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>

**FORTINET TRAINING INSTITUTE**

<https://training.fortinet.com>

**FORTIGUARD LABS**

<https://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

<https://www.fortinet.com/doc/legal/EULA.pdf>

**FEEDBACK**

Email: [techdoc@fortinet.com](mailto:techdoc@fortinet.com)



January 30, 2026

FortiOS 7.6 ZTNA Reference Guide

01-76-1051154-20260130

# TABLE OF CONTENTS

<b>Introduction</b> .....	<b>4</b>
<b>Endpoint posture check</b> .....	<b>5</b>
Recommended posture checks .....	5
Other posture checks .....	6
<b>CASB SaaS application support</b> .....	<b>27</b>
<b>Error codes and replacement messages</b> .....	<b>30</b>
<b>ZTNA object maximum values</b> .....	<b>33</b>
<b>Change log</b> .....	<b>37</b>

# Introduction

Zero trust network access (ZTNA) is an access control method that uses client device identification, authentication, and security posture tags to provide role-based application access. It gives administrators the flexibility to manage network access for on-net local users and off-net remote users. Access to applications is granted only after device verification, authenticating the user's identity, authorizing the user, and then performing context based posture checks using security posture tags. Furthermore, security posture tags can be used in VPN connections for enforcement before tunnel establishments.

This document provides references to ZTNA-related information such as security posture tags, CASB applications, and error codes.

# Endpoint posture check

The following are different context-based posture checks that FortiClient EMS 7.2 supports as part of the Zero Trust solution:

## Recommended posture checks

For vulnerable devices, checking for devices with high-risk vulnerabilities and above is recommended.

Rule type	Posture check	Supported operating systems
Vulnerable devices	Critical	
	High or higher	
	Medium or higher	
	Low or higher	
Antivirus software	AV software is installed and running. For Windows, this feature supports third party AV applications. For macOS and Linux, this feature can only check if FortiClient AV protection is enabled and does not recognize third party AV applications.	Windows, macOS, Linux
	AV signature is up-to-date	
Windows security	Windows Defender is enabled	Windows
	Bitlocker Disk Encryption is enabled on all disks	
	Bitlocker Disk Encryption is enabled on OS disk	
	Exploit Guard is enabled	
	Application Guard is enabled	
	Windows Firewall is enabled	
	Automatic Updates are enabled	
Security	FileVault Disk Encryption is enabled	macOS
EMS management	FortiClient installed and Telemetry is connected to EMS	Windows, macOS, Linux, iOS, Android

Rule type	Posture check	Supported operating systems
Common vulnerabilities and exposures (CVE)	Presence of [CVE]	Windows, macOS, Linux
Firewall threat	Presence of [firewall threat ID]	Windows, macOS

## Other posture checks

Rule type	Posture check	Supported operating systems
User in Active Directory (AD) group	Member of [AD Group]	Windows, macOS, Linux
Certificate	Certificate contains [Subject CN] and [Issuer CN]	Windows, macOS, Linux
CrowdStrike ZTA Score	Zero trust assessment (ZTA) score within configured range/equal to configured value	Windows
File	Presence of [File]	Windows, macOS, Linux
IP range	Device in the [IP Range]	Windows, macOS, Linux, IOS, Android
Logged in domain	Member of [Domain]	Windows, macOS, Linux
On-Fabric status	On-Fabric	Windows, macOS, Linux, IOS, Android

<b>Rule type</b>	<b>Posture check</b>	<b>Supported operating systems</b>
OS version	Windows Server 2022	Windows

Rule type	Posture check	Supported operating systems
	Windows Server 2019	Windows

Rule type	Posture check	Supported operating systems
	Windows Server 2016	Windows

Rule type	Posture check	Supported operating systems
	Windows Server 2012 R2	Windows

<b>Rule type</b>	<b>Posture check</b>	<b>Supported operating systems</b>
	Windows Server 2012	Windows

Rule type	Posture check	Supported operating systems
	Windows Server 2008 R2	Windows

Rule type	Posture check	Supported operating systems
	Windows 11	Windows

Rule type	Posture check	Supported operating systems
	Windows 10	Windows

Rule type	Posture check	Supported operating systems
	Windows 8.1	Windows

Rule type	Posture check	Supported operating systems
	Windows 8	Windows

Rule type	Posture check	Supported operating systems
	Windows 7	Windows

Rule type	Posture check	Supported operating systems
	Mojave	macOS

Rule type	Posture check	Supported operating systems
	High Sierra	macOS

Rule type	Posture check	Supported operating systems
	Sierra	macOS

Rule type	Posture check	Supported operating systems
	Catalina	macOS

Rule type	Posture check	Supported operating systems
	Big Sur	macOS

Rule type	Posture check	Supported operating systems
	Monterey	macOS

Rule type	Posture check	Supported operating systems
	Ventura	macOS

Rule type	Posture check	Supported operating systems
	Sonoma	macOS
	CentOS Stream 9	Linux
	CentOS Stream 8	Linux
	CentOS 8	Linux
	CentOS 7.5	Linux
	CentOS 7.4	Linux
	Red Hat 9	Linux
	Red Hat 8.5	Linux
	Red Hat 8.1	Linux
	Red Hat 8	Linux
	Red Hat 7.6	Linux
	Red Hat 7.5	Linux
	Red Hat 7.4	Linux
	Ubuntu 22.04	Linux
	Ubuntu 21.10	Linux
	Ubuntu 21.04	Linux
	Ubuntu 20	Linux
	Ubuntu 18.04	Linux
	Ubuntu 16.04	Linux
	Fedora 34	Linux
	Fedora 33	Linux
	Fedora 32	Linux
	Fedora 31	Linux
	Fedora Linux 37	Linux
	Fedora Linux 36	Linux
	Fedora Linux 35	Linux
	iOS 9, 10, 11, 12, 13, 14, 15, 16	iOS
	Android 5, 6, 7, 8, 9, 10, 11, 12, 13	Android

Rule type	Posture check	Supported operating systems
Registry key	[Registry key]	Windows
Running process	Presence of [Running process]	Windows, macOS, Linux
Sandbox detection	Sandbox detected malware in last seven days	Windows, macOS
User identity	User-specified	Windows, macOS, Linux, iOS, Android
	Social network login	
	Verified user	
FortiEDR	FortiEDR is installed and running	Windows, macOS, Linux
FortiClient version	Presence of [Specified FortiClient version]	Windows, macOS, Linux, iOS, Android
Security status	Device fulfills configured security status, such as being jailbroken or having passcode or biometrics protection enabled.	iOS, Android

# CASB SaaS application support

You can configure the FortiGate zero trust network access (ZTNA) access proxy to act as an inline cloud access security broker (CASB) by providing access control to software-as-a-service (SaaS) traffic using ZTNA access control rules. A CASB sits between users and their cloud service to enforce security policies as they access cloud-based resources. FortiOS 7.2.1 and later versions support ZTNA inline CASB for SaaS application access. This topic provides information on the supported applications.

The inline CASB database, as of version 1.00045, supports the following SaaS applications:

ZTNA access proxy application name	SaaS application
adobe	Adobe services domains
adp	ADP
atlassian	Atlassian
aws-s3	AWS S3
azure	Azure
box	Box
citrix	Citrix
confluence	Confluence
docusign	DocuSign
dropbox	Dropbox
egnyte	Egnyte
github	GitHub
gmail	Gmail
google-cloud	Google Cloud
google-drive	Google Drive
google-office	Google Office
google-web	Google Web Search domains
jira	Jira
ms-excel	Microsoft Excel
ms-exchange	Microsoft Exchange
ms-onedrive	Microsoft OneDrive
ms-outlook	Microsoft Outlook
ms-powerpoint	Microsoft PowerPoint

ZTNA access proxy application name	SaaS application
ms-teams	Microsoft Teams
ms-word	Microsoft Word
oracle-cloud	Oracle Cloud
salesforce	Salesforce
sap	SAP
Servicenow	ServiceNow
sharepoint	SharePoint
twilio-video-cloud	Twilio video cloud
webex	Webex
workplace	Workplace
youtube	YouTube
zendesk	Zendesk
zoom	Zoom

The inline CASB database, as of version 1.00045, supports the following SaaS access control:

ZTNA access proxy access control name	SaaS access control
box-download	Box download
box-upload	Box upload
dropbox-download	Dropbox download
dropbox-upload	Dropbox upload
gmail-getAttach	Gmail download attachment
ms-onedrive-download	MS OneDrive download
ms-outlook-getAttach	MS Outlook download attachment

The inline CASB database, as of version 1.00045, supports the following SaaS application groups:

ZTNA access proxy application name	SaaS application group
Google	Google SaaS
MS	Microsoft SaaS

For a complete list, use the following CLI commands to retrieve the corresponding lists.

#### Display the list of applications:

```
# diagnose saas show apps
```

**Display details of each application:**

```
# diagnose saas show details
```

# Error codes and replacement messages

The following table summarizes the replacement message errors based on error code and category available in FortiOS 7.4.1 and later.

Error code	Error category	Error message	Description
1	Invalid ZTNA Certificate	The page you requested has been blocked because the ZTNA certificate is invalid.	The client endpoint has an invalid certificate that the FortiGate cannot recognize.
2	Invalid ZTNA Certificate	The page you requested has been blocked because the ZTNA certificate is empty.	The client endpoint did not provide a client certificate for the FortiGate to verify and empty-client-cert is set to block.
3	Invalid ZTNA Certificate	The page you requested has been blocked because the device is manageable but with an empty ZTNA certificate.	The client endpoint is manageable (non-mobile), but did not provide a client certificate for the FortiGate to verify.
21	ZTNA Application Not Found	The page you requested has been blocked because no API gateway was matched.	The client endpoint is looking for a page or service that is not configured in the FortiGate's ZTNA settings.
22	ZTNA Application Not Found	The page you requested has been blocked because the real server in the API gateway cannot be found.	The FortiGate is unable to serve the requested page or service because it cannot find the real server.
23	ZTNA Application Not Found	The page you requested has been blocked because ZTNA FQDN DNS failed.	The FortiGate cannot resolve the FQDN in the client endpoint's request.
26	ZTNA Connection Error	There is a connection issue when attempting to reach the destination website.	Real server certificate's CN field does not match FQDN in access proxy.
27	ZTNA Connection Error	There is a connection issue when attempting to reach the destination website.	Real server certificate is expired.
28	ZTNA Connection Error	There is a connection issue when attempting to reach the destination website.	Real server certificate is revoked.

Error code	Error category	Error message	Description
29	ZTNA Connection Error	There is a connection issue when attempting to reach the destination website.	Real server certificate verification has timed out.
30	ZTNA Connection Error	There is a connection issue when attempting to reach the destination website.	Real server certificate verification failed.
31	ZTNA Connection Error	There is a connection issue when attempting to reach the destination website.	Untrusted real server certificate.
41	ZTNA Portal Error	The page you requested has been blocked because SSL VPN bookmark address failed.	The FortiGate is unable to match a bookmark in the SSL VPN web portal used by the ZTNA application gateway.
61	ZTNA Policy Deny	The page you requested has been blocked because no policy was matched.	There is no ZTNA policy that matches the destination page that the client endpoint is requesting.
62	ZTNA Policy Deny	The page you requested has been blocked because a policy with action deny was matched.	The traffic matched a ZTNA deny policy.
63	ZTNA Policy Deny	The page you requested has been blocked because the client cert has been revoked.	The endpoint client is using a client certificate issued by FortiClient EMS that has been revoked.
64	ZTNA Policy Deny	The page you requested has been blocked because the tags matched a deny policy.	The endpoint client has a ZTNA tag that matches a ZTNA deny policy.
65	ZTNA Policy Deny	The page you requested has been blocked because the tags didn't match any policy.	The endpoint client's ZTNA tags did not match any ZTNA policies, and its traffic is implicitly denied.
66	ZTNA Policy Deny	The page you requested has been blocked because no device info was found.	The FortiGate cannot find any device information for the client endpoint, resulting in a failed verification of the client.
67	ZTNA Policy Deny	The page you requested has been blocked because the device is offline.	The client endpoint is not connected to FortiClient EMS, hence is considered offline and blocked by the FortiGate.

Error code	Error category	Error message	Description
68	ZTNA Policy Denied	The page you requested has been blocked because the device is unknown or unmanaged.	The client endpoint is blocked because it is unmanaged, and the policy does not allow unmanaged devices.
69	ZTNA Policy Denied	The page you requested has been blocked because authorization failed.	The client endpoint failed authorization due to unmatched user group.

# ZTNA object maximum values

For various zero trust network access (ZTNA) object types, FortiOS may limit the number of each object type that you can create. To verify the maximum number of objects for each object type, run the following command on your FortiGate:

```
# print tablesize
```

The following provides example output for ZTNA (access proxy)-related objects from a FortiGate-VM04:

```
# print tablesize
firewall.access-proxy-virtual-host: 0 256 512 1
firewall.access-proxy-virtual-host:ssl-certificate: 0 0 0 1
firewall.access-proxy-ssh-client-cert: 0 256 512 0
firewall.access-proxy-ssh-client-cert:cert-extension: 0 0 0 0
firewall.access-proxy: 0 256 512 3
firewall.access-proxy:api-gateway: 0 0 0 3
firewall.access-proxy:api-gateway:realservers: 0 0 0 3
firewall.access-proxy:api-gateway:realservers:ssh-host-key: 0 0 0 0
firewall.access-proxy:api-gateway:application: 0 0 0 0
firewall.access-proxy:api-gateway:ssl-cipher-suites: 0 0 0 0
firewall.access-proxy:api-gateway6: 0 0 0 0
firewall.access-proxy:api-gateway6:realservers: 0 0 0 0
firewall.access-proxy:api-gateway6:realservers:ssh-host-key: 0 0 0 0
firewall.access-proxy:api-gateway6:application: 0 0 0 0
firewall.access-proxy:api-gateway6:ssl-cipher-suites: 0 0 0 0
firewall.access-proxy6: 0 256 512 0
firewall.access-proxy6:api-gateway: 0 0 0 0
firewall.access-proxy6:api-gateway:realservers: 0 0 0 0
firewall.access-proxy6:api-gateway:realservers:ssh-host-key: 0 0 0 0
firewall.access-proxy6:api-gateway:application: 0 0 0 0
firewall.access-proxy6:api-gateway:ssl-cipher-suites: 0 0 0 0
firewall.access-proxy6:api-gateway6: 0 0 0 0
firewall.access-proxy6:api-gateway6:realservers: 0 0 0 0
firewall.access-proxy6:api-gateway6:realservers:ssh-host-key: 0 0 0 0
firewall.access-proxy6:api-gateway6:application: 0 0 0 0
firewall.access-proxy6:api-gateway6:ssl-cipher-suites: 0 0 0 0
ztna.web-portal: 0 256 512 0
ztna.web-portal-bookmark: 0 256 512 0
ztna.web-portal-bookmark:users: 0 0 0 0
ztna.web-portal-bookmark:groups: 0 0 0 0
ztna.web-portal-bookmark:bookmarks: 0 0 0 0
```



These values may vary between FortiGate models.

---

The four columns of values provide the following information, respectively:

1. Maximum number of variables allowed for this object type
2. Maximum number of objects of this type allowed per virtual domain (VDM)
3. System global limit for maximum number of objects of this type
4. Current total number of objects of this type existing in FortiOS

A value of 0 indicates that there is no maximum value limit.

The following presents the example output in a table format, showing each object type and its associated maximum and current values:

Object	Maximum variables allowed	Maximum per VDOM	Global maximum	Current total objects in use
firewall.access-proxy-virtual-host	0	256	512	1
firewall.access-proxy-virtual-host:ssl-certificate	0	0	0	1
firewall.access-proxy-ssh-client-cert	0	256	512	0
firewall.access-proxy-ssh-client-cert:cert-extension	0	0	0	0
firewall.access-proxy	0	256	512	3
firewall.access-proxy:api-gateway	0	0	0	3
firewall.access-proxy:api-gateway:realservers	0	0	0	3
firewall.access-proxy:api-gateway:realservers:ssh-host-key	0	0	0	0
firewall.access-proxy:api-gateway:application	0	0	0	0
firewall.access-proxy:api-gateway:ssl-cipher-suites	0	0	0	0
firewall.access-proxy:api-gateway6	0	0	0	0
firewall.access-proxy:api-gateway6:realservers	0	0	0	0
firewall.access-proxy:api-gateway6:realservers:ssh-host-key	0	0	0	0
firewall.access-proxy:api-gateway6:application	0	0	0	0
firewall.access-proxy:api-gateway6:ssl-cipher-suites	0	0	0	0
firewall.access-proxy6	0	256	512	0
firewall.access-proxy6:api-gateway	0	0	0	0
firewall.access-proxy6:api-gateway:realservers	0	0	0	0
firewall.access-proxy6:api-gateway:realservers:ssh-host-key	0	0	0	0

Object	Maximum variables allowed	Maximum per VDOM	Global maximum	Current total objects in use
firewall.access-proxy6:api-gateway:application	0	0	0	0
firewall.access-proxy6:api-gateway:ssl-cipher-suites	0	0	0	0
firewall.access-proxy6:api-gateway6	0	0	0	0
firewall.access-proxy6:api-gateway6:realservers	0	0	0	0
firewall.access-proxy6:api-gateway6:realservers:ssh-host-key	0	0	0	0
firewall.access-proxy6:api-gateway6:application	0	0	0	0
firewall.access-proxy6:api-gateway6:ssl-cipher-suites	0	0	0	0
ztna.web-portal	0	256	512	0
ztna.web-portal-bookmark	0	256	512	0
ztna.web-portal-bookmark:users	0	0	0	0
ztna.web-portal-bookmark:groups	0	0	0	0
ztna.web-portal-bookmark:bookmarks	0	0	0	0

For example, consider the values for firewall.access-proxy-virtual-host:

Object	Maximum variables allowed	Maximum per VDOM	Global maximum	Current total objects in use
firewall.access-proxy-virtual-host	0	256	512	1

You can interpret this as follows for the virtual host object type:

- For each VDOM, FortiOS allows a maximum of 256 virtual hosts used within a ZTNA server definition.
- Globally, FortiOS allows a maximum of 512 virtual hosts used within a ZTNA server definition.
- Currently, FortiOS has one virtual host object defined.

For another example, consider the values for firewall.access-proxy:api-gateway:realservers:

Object	Maximum variables allowed	Maximum per VDOM	Global maximum	Current total objects in use
firewall.access-proxy:api-gateway:realservers	0	0	0	3

You can interpret this as follows for the real server object type:

- There is no per-VDOM or global limit on the number of real servers associated with ZTNA servers.
- Currently, FortiOS has three real servers defined.

For other maximum values, see [Maximum Values Table](#).

# Change log

Date	Change description
2024-07-25	Initial release.
2025-02-04	Added <a href="#">ZTNA object maximum values</a> on page 33.
2025-02-05	Updated <a href="#">ZTNA object maximum values</a> on page 33.
2025-07-28	Updated <a href="#">Endpoint posture check</a> on page 5.
2026-01-30	Updated <a href="#">Error codes and replacement messages</a> on page 30.



[www.fortinet.com](http://www.fortinet.com)

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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 Chief Legal Officer, 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. 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.