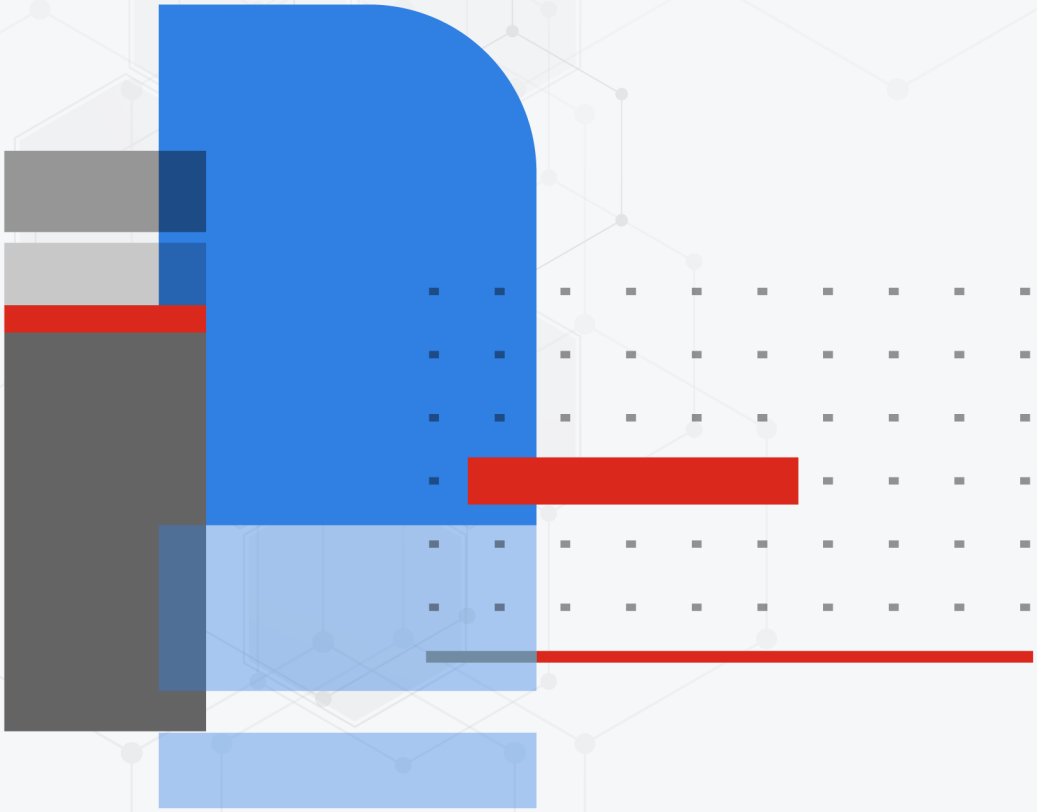
XML Reference

FortiClient 7.4.6



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

March 17, 2026
FortiClient 7.4.6 XML Reference
04-746-866071-20260317

TABLE OF CONTENTS

Change log **5**
Introduction **6**
What's new **7**
7.4.6 7
7.4.5 8
XML configuration file **9**
File structure 9
Configuration file sections 9
File extensions 10
Encrypted username and password 10
IP addresses 10
Boolean values 11
Metadata 11
System settings 11
UI settings 12
Log settings 16
Proxy settings 19
Update settings 20
FortiProxy settings 24
Certificate settings 25
User identity settings 26
Installer settings 27
Endpoint control 28
VPN 38
VPN options 38
SSL VPN 46
IPsec VPN 60
Antivirus 85
General options 85
Real-time protection 86
On-demand scans 91
Scheduled scans 95
Email 98
Quarantine 99
Antiransomware 100
SSOMA 102
Web filter 103
Video Filter 118
Application firewall 121
Vulnerability scan 125
Sandboxing 128
Anti-exploit detection 132
Removable media access 133

Cloud-based malware protection ... 134
ZTNA ... 137
PAM ... 140
Apple ... 141
Design considerations ... 142
Input validation ... 142
Handling password fields ... 142
Importing configuration file segments ... 142
Client certificate ... 143
Backing up or restoring the configuration file ... 144
Backing up the full configuration file ... 144
Restoring the full configuration file ... 144
Backing up and restoring CLI utility commands and syntax ... 144
Adding XML to advanced profiles in EMS ... 146
Advanced features ... 148
Advanced features (Windows) ... 148
Connecting VPN before logon (AD environments) ... 148
Creating a redundant IPsec VPN ... 148
Priority-based SSL VPN connections ... 149
Enabling VPN autoconnect ... 149
Enabling VPN always up ... 150
Advanced features (macOS) ... 150
Creating a redundant IPsec VPN ... 150
Priority-based SSL VPN connections ... 151
Enabling VPN autoconnect ... 151
Enabling VPN always up ... 151
VPN tunnel and script ... 152
Windows ... 152
macOS ... 153

Change log

Date	Change description
2026-03-17	Initial release.

Introduction

This document provides an overview of FortiClient version 7.4.6 XML configuration.

This document is written for FortiClient (Windows) 7.4.6. See What's new on page 7 for a list of new, changed, or removed XML options in version 7.4.5.

For information on FortiClient installation and configuration, see the FortiClient Administration Guide.

What's new

This section identifies new, changed, and removed XML configuration options in FortiClient 7.4.5 and later. For more information about new features in 7.4.6, please see the FortiClient 7.4 New Features Guide.

7.4.6

<table>
<tr><th>Category</th><th>New</th><th>Changed</th></tr>
<tr><td>VPN options on page 38</td><td>• <saml_auth_enable_proxy_server></td><td></td></tr>
<tr><td>IPsec VPN on page 60</td><td>• <resolve_to_ipv4_only></td><td></td></tr>
<tr><td>IPsec VPN on page 60 > IKE settings on page 70</td><td>• <no_vnic_dns_server>
• <modeconfig_type></td><td>• <implied_SPDO_timeout>—Default value is changed from 0 to 60.
• <proposal>—The default values have been changed as follows:
<table>
<tr><th></th><th>7.4.5 or earlier</th><th>7.4.6</th></tr>
<tr><td>phase 1</td><td><proposals>
<proposal>AES128|SHA1
</proposal>
<proposal>AES256|SHA256</proposal>
</proposals></td><td><proposals>
<proposal>AES128|SHA256
</proposal>
<proposal>AES256|SHA256</proposal>
</proposals></td></tr>
<tr><td>phase 2</td><td><proposals>
proposal>AES128|SHA1
</proposal
<proposal>AES256|SHA256</proposal>
</proposals></td><td><proposals>
proposal>AES128GCM|NONE
</proposal
<proposal>AES256|SHA256</proposal>
</proposals></td></tr>
</table></td></tr>
<tr><td>SSL VPN on page 46</td><td>• <splitdns_tcp_enabled></td><td></td></tr>
</table>

7.4.5

Category	New	Changed	Removed
VPN options on page 38	• <disconnect_password>		• <show_negotiation_wnd>
IPsec VPN on page 60	• <traffic_keep_strategy> • <traffic_keep_timer>		
IPsec VPN on page 60 > IKE settings on page 70	• <remove_password_for_unexpected_eap_failure>	• <dpd_retry_interval>—Default value is changed from 10 to 20. • <enable_ike_fragmentation>—Default value is changed from 0 to 1.	
SSL VPN on page 46	• <traffic_keep_timer>	• <traffic_keep_strategy>—Added option 2.	
Web filter on page 103	• <referrer>		
Cloud-based malware protection on page 134	• <notification_type>		
System settings on page 11 > Installer settings on page 27	• <remove_user_data>		
ZTNA on page 137	• <fqdn_exceptions>		
Antivirus on page 85 > Email on page 98			• <outlook>
Endpoint control on page 28	• **(Android only)** <auto_start>		

XML configuration file

FortiClient supports importation and exportation of its configuration via an XML file. The following sections describe the file's structure, sections, and provide descriptions for the elements you use to configure different FortiClient options:

File structure

This section defines and describes the format of the FortiClient XML configuration file:

Configuration file sections

The configuration file contains the following major sections:

Section	Description
Metadata on page 11	Basic data controlling the entire configuration file.
System settings on page 11	General settings not specific to any module listed or that affect more than one module.
Endpoint control on page 28	Endpoint control settings, including: enabling enforcement and off-net updates, skipping confirmation, disabling ability to unregister, and silent registration.
VPN on page 38	Global VPN, IPsec VPN, and SSL VPN settings.
Antivirus on page 85	Antivirus (AV) settings, including: FortiGuard Distribution Network (FDN) analytics, real-time protection (RTP), behavior when a virus is detected, and quarantining.
SSOMA on page 102	Single Sign-On (SSO) mobility agent settings.
Web filter on page 103	Web filter settings, including: logging, white list priority, maximum violations, rate IP addresses, profiles, safe search, and YouTube education filter.
Application firewall on page 121	Application firewall settings.
Vulnerability scan on page 125	Vulnerability scan settings.
Sandboxing on page 128	Sandbox detection settings.

Section	Description
Anti-exploit detection on page 132	Anti-exploit detection settings.
Removable media access on page 133	Removable media access settings.
Apple on page 141	Settings that only apply to FortiClient (iOS).

File extensions

FortiClient supports the following four file types:

File type	Description
.conf	Plain text configuration file.
.sconf	Secure encrypted configuration file.
.conn	Plain text VPN connection configuration file.
.sconn	Secure encrypted VPN connection configuration file.

You can generate a configuration file on the *Settings* pane in FortiClient or by using the FCConfig.exe command line program, which is installed with FortiClient.

Encrypted username and password

Several XML tag elements are named `<password>`. FortiClient always encrypts all such tags during configuration exports. For modified and imported configurations, FortiClient accepts encrypted or plain-text passwords.

Here is an example of an encrypted password tag element. The password starts with *Enc*:

```
<password>Enc9b4e1aae22c65e638aed4e47fbd225256a3b7a24b53f8370d6bc3b9aa90cecd5086c995f0549e944b4ac
      c951e4844529c71d81280de2b951</password>
```

Several `<username>` XML tags also follow this format.

IP addresses

IP address tag elements usually refer to IPv4 addresses. A fully qualified domain name (FQDN) may also be provided. Here are two examples:

- Single IP address: `74.196.82.243`
- FQDN: `www.fortinet.com`

Boolean values

Elements that determine if you have enabled or disabled a feature use Boolean values. The configuration file accepts `0` for false and `1` for true.

Metadata

The `<forticlient_configuration>` XML tag contains all of the XML tags and data in a configuration file. An empty configuration file looks like this:

```
<?xml version=”1.0” encoding=”utf-8”?>
<forticlient_configuration>
</forticlient_configuration>
```

The first line of the file includes an XML version number as well as the encoding. This is the standard XML start tag.

FortiClient supports the following metadata:

Metadata	Description
`<forticlient_version>7.4.6.xxx</forticlient_version>`	FortiClient version number if you exported the file from FortiClient.
`<version>7.4.6</version>`	Configuration file version.
`<exported_by_version>7.4.6.xxx</exported_by_version>`	FortiClient version number when the file was exported from FortiClient.
`<date>2026/08/30</date>`	Date the file was generated.
`<partial_configuration>0</partial_configuration>`	Controls whether the configuration is replaced or added in import/restore. Possible values are `0` or `1`.
`<os_version>windows</os_version>`	Indicates whether this configuration is generated from Microsoft Windows or macOS. Possible values are `windows` or `MacOSX`.
`<os_architecture>x64</os_architecture>`	Indicates the OS architecture. Possible values are `x64` or `x32`.

System settings

The `<system> </system>` XML tags contain system settings. System settings include the following subsections:

UI settings

The <ui></ui> XML tags contain user interface (UI)-related information.

```
<forticlient_configuration>
   <system>
      <ui>
         <ads>0</ads>
         <disable_backup>0</disable_backup>
         <allow_shutdown_when_registered>1</allow_shutdown_when_registered>
         <default_tab>AV</default_tab>
         <flashing_system_tray_icon>1</flashing_system_tray_icon>
         <hide_system_tray_icon>0</hide_system_tray_icon>
         <suppress_admin_prompt>0</suppress_admin_prompt>
         <show_host_tag>0</show_host_tag>
         <password>Encrypted/NonEncrypted_PasswordString</password>
         <lock>Encrypted/NonEncrypted_PasswordString/</lock>
         <hide_user_info>0</hide_user_info>
         <culture-code>os-default</culture-code>
         <gpu_rendering>0</gpu_rendering>
         <replacement_messages>
            <quarantine>
               <title>
                  <title>
                     <![CDATA[]]>
                  </title>
               </title>
               <statement>
                  <remediation>
                     <![CDATA[]]>
                  </remediation>
               </statement>
               <remediation>
                  <remediation>
                     <![CDATA[]]>
                  </remediation>
               </remediation>
            </quarantine>
         </replacement_messages>
         <avatars>
            <enabled>[0|1]</enabled>
            <providers>
               <google>
                  <clientid>
                     <![CDATA[]]>
                  </clientid>
                  <clientsecret>
                     <![CDATA[]]>
                  </clientsecret>
                  <redirecturl>
                     <![CDATA[]]>
                  </redirecturl>
               </google>
               <linkedin>
                  <clientid>
                     <![CDATA[]]>
```

```
                  </clientid>
                  <clientsecret>
                     <![CDATA[]]>
                  </clientsecret>
                  <redirecturl>
                     <![CDATA[]]>
                  </redirecturl>
               </linkedin>
               <salesforce>
                  <clientid>
                     <![CDATA[]]>
                  </clientid>
                  <clientsecret>
                     <![CDATA[]]>
                  </clientsecret>
                  <redirecturl>
                     <![CDATA[]]>
                  </redirecturl>
               </salesforce>
            </providers>
         </avatars>
      </ui>
   </system>
</forticlient_configuration>
```

The following table provides the XML tags for UI settings, as well as the descriptions and default values where applicable:

XML tag	Description	Default value
`<ads>`	Advertisements (dashboard banner) in the FortiClient do not display, even when set to `1`. FortiClient ignores this setting. Boolean value: `[0 | 1]`	`1`
`<disable_backup>`	Disallow users from backing up the FortiClient configuration. Boolean value: `[0 | 1]`	`1`
`<allow_shutdown_when_registered>`	Allows user to shut down FortiClient while registered to EMS. This feature is only available for FortiClient (Windows). Boolean value: `[0 | 1]`	`0`
`<default_tab>`	The tab selected by default in the FortiClient. Enter one of the following: • `AV`: Malware Protection • `WF`: Web Filter • `FW`: Application Firewall • `VPN`: Remote Access • `VULN`: Vulnerability Scan	`AV`
`<flashing_system_tray_icon>`	Enable the flashing system tray icon. The system tray flashes while FortiClient background processes are running. Boolean value: `[0 | 1]`	`1`
`<hide_system_tray_icon>`	Hide or display the FortiClient system tray icon.	`0`

XML tag	Description	Default value
	Boolean value: `[0 | 1]`	
`<suppress_admin_prompt>`	Do not ask for an administrator password for tasks that require superuser permissions to complete. Boolean value: `[0 | 1]`	`0`
`<show_host_tag>`	Display the applied host tag on the FortiClient. EMS applies host tags based on compliance verification rules. See the *FortiClient EMS Administration Guide* for details. Boolean value: `[0 | 1]`	`0`
`<password>`	Enter an encrypted or non-encrypted password to set the configuration lock upon connecting with a FortiGate. EMS uses MD5 to hash the lockdown password and encrypts the hash. This legacy element is meant to support FortiClient 7.0.6 and earlier versions.	
`<lock>`	Enter an encrypted or non-encrypted password to set the configuration lock upon connecting with a FortiGate. EMS uses SHA256 to hash the lockdown password and encrypts the hash. • If you configure `<lock>` with a value, FortiClient does not use the password configured in `<password>`. • If you do not configure `<lock>` with a value, FortiClient defaults to using the password configured in `<password>`. This element supports FortiClient 7.0.7 and later versions.	
`<hide_user_info>`	Hide the User Details panel where the user can provide user details (avatar, name, phone number, email address), and link to a social media (LinkedIn, Google, Salesforce) account.	`0`
`<culture-code>`	The localized language that FortiClient displays in. Enter one of the following: • `os-default`: Defaults to the OS language • `de-de`: German • `en-us`: English (United States) • `es-es`: Spanish (Spain) • `fr-fr`: French (France) • `ja-jp`: Japanese • `pt-br`: Portuguese (Brazil) • `kr-kr`: Korean • `zh-cn`: Simplified Chinese • `zh-tw`: Traditional Chinese	`os-default`
`<gpu_rendering>`	Enable GPU rendering. Boolean value: `[0 | 1]`	`0`
`<replacement_messages>`	Display a message in FortiClient when the endpoint is quarantined. You can customize the message.	

XML tag	Description	Default value
<avatars> elements	Contains the elements for configuring whether FortiClient retrieves an avatar picture for the endpoint user from web applications, such as Google, LinkedIn, or Salesforce.	
<enabled>	Enable FortiClient to retrieve an avatar picture for the user from web applications, such as Google, LinkedIn, or Salesforce. Boolean value: [0 | 1]	
<providers>	Identifies which cloud applications FortiClient uses to retrieve an avatar picture for the endpoint users.	
<google>	Settings that allow FortiClient uses to retrieve an avatar picture from Google. Integration with Google requires a Google API Console project.	
<clientid>	Enter your Google API Console project's client ID.	
<clientsecret>	Enter your Google API Console project's client secret.	
<redirecturl>	Enter your Google API Console project's redirect URL.	
<linkedin>	Settings that allow FortiClient uses to retrieve an avatar picture from LinkedIn. Integration with LinkedIn requires LinkedIn Developers knowledge.	
<clientid>	Enter your LinkedIn client ID.	
<clientsecret>	Enter your LinkedIn client secret.	
<redirecturl>	Enter your LinkedIn URL.	
<salesforce>	Settings that allow FortiClient uses to retrieve an avatar picture from Salesforce. Integration with Salesforce requires Salesforce Developers knowledge.	
<clientid>	Enter your Salesforce client ID.	
<clientsecret>	Enter your Salesforce client secret.	
<redirecturl>	Enter your Salesforce redirect URL.	

Following is an example replacement message:

```
<replacement_messages>
   <quarantine>
      <title>
         <![CDATA[Quarantined]]>
      </title>
      <statement>
         <![CDATA[Your system has been quarantined by %FortiGate% %serial number% (%ip
               address%).]]>
      </statement>
         <remediation>
            <![CDATA[Contact your system administrator for assistance.]]>
         </remediation>
   </quarantine>
</replacement_messages>
```

Log settings

The <log_settings> </log_settings> XML tags contain log-related information.

```
<forticlient_configuration>
   <system>
      <log_settings>
         <onnet_local_logging>[0|1]</onnet_local_logging>
         <level>6</level>
         <log_
               events>antiexploit,antiransomware,av,cloudscan,dblog,endpoint,firewall,fssoma,ipsecvp
               n,pam,proxy,removable_media_
               access,sandboxing,sslvpn,update,videofilter,vuln,webfilter,ztna,configd,scheduler,shi
               eld</log_events>
         <remote_logging>
            <log_upload_enabled>1</log_upload_enabled>
            <log_upload_server>12345.ca-west-1.fortianalyzer.forticloud.com</log_upload_server>
            <log_upload_ssl_enabled>1</log_upload_ssl_enabled>
            <log_retention_days>90</log_retention_days>
            <log_upload_freq_minutes>90</log_upload_freq_minutes>
            <log_generation_timeout_secs>900</log_generation_timeout_secs>
            <log_compressed>0</log_compressed>
            <log_protocol>syslog</log_protocol>
            <!-- faz | syslog -->
            <!-- server IP address -->
            <netlog_server>0.0.0.0</netlog_server>
            <netlog_categories>7</netlog_categories>
            <send_software_inventory>1</send_software_inventory>
            <send_os_events>
               <enabled>1</enabled>
               <interval>120</interval>
            </send_os_events>
            <send_ms_exch_events>
               <enabled>1</enabled>
               <interval>120</interval>
            </send_ms_exch_events>
         </remote_logging>
      </log_settings>
   </system>
</forticlient_configuration>
```

The following table provides the XML tags for log settings, as well as the descriptions and default values where applicable.

XML tag	Description	Default value
<onnet_local_ logging>	If you enabled client-log-when-on-net on EMS, EMS sends this XML element to FortiClient. Boolean value: [0 | 1]	
<level>	Configure the FortiClient logging level. FortiClient generates logs equal to and more critical than the selected level. Enter one of the following: • 0: Emergency. The system becomes unstable.	6

XML tag	Description	Default value
	• 1: Alert. Immediate action is required. • 2: Critical. Functionality is affected. • 3: Error. An error condition exists and could affect functionality. • 4: Warning. Functionality could be affected. • 5: Notice. Information about normal events. • 6: Info. General information about system operations. • 7: Debug. Debug FortiClient.	
<log_events>	FortiClient events or processes to log. Enter a comma-separated list of one or more of the following: • antiexploit: Anti-exploit detection events • antiransomware: Antiransomeware detection events • av: AV log events • cloudscan: Cloud-based malware scan events • dblog: Events for logging process • endpoint: Endpoint Control log events • firewall: Application firewall log events • fssoma: SSO mobility agent for FortiAuthenticator log events • ipsecvpn: IPsec VPN log events • pam: FortiPAM log events • proxy: FortiProxy log events • removable_media_access: Removable media access (RMA)-related log events • sandboxing: Sandbox detection events • sslvpn: SSL VPN log events • update: Update log events • videofilter: Video filter log events • vuln: Vulnerability scan log events • webfilter: Web filter log events • ztna: ZTNA-related log events • configd: Configuration log events • scheduler: Scheduler log events • shield: FortiShield log events	All events are enabled
<remote_logging> elements All elements for <remote_logging> apply only to remote logs. The elements do not affect the behavior of local logs.		
<log_upload_enabled>	Upload FortiClient logs to FortiAnalyzer or FortiManager. Boolean value: [0 | 1]	0
<log_upload_server>	Enter the FortiAnalyzer or FortiManager IP address or hostname/FQDN. If using a port other than the default, use <address>:<port>. With Chromebook profiles, use the format https://FAZ-IP:port/logging.	

XML tag	Description	Default value
	For FortiAnalyzer Cloud, enter the FQDN that you use to access the FortiAnalyzer Cloud instance (such as `1208151.ca-west-1.fortianalyzer.forticloud.com`). You must also configure the SNI for FortiAnalyzer Cloud using the `<log_uploadserver_sni>` tag.	
`<log_uploadserver_sni>`	Enter the SNI for FortiAnalyzer Cloud.	
`<log_upload_ssl_enabled>`	Enable using the SSL protocol when uploading logs to FortiAnalyzer or FortiManager. Boolean value: `[0 | 1]`	`1`
`<log_upload_freq_minutes>`	Enter the log frequency upload period in minutes.	`90`
`<log_generation_timeout_sec>`	Configure how often logs are created in seconds.	`900`
`<log_compressed>`	Enable log compression. Boolean value: `[0 | 1]`	
`<log_retention_days>`	Enter the number of days to retain the logs in the upload queue before being deleted in the event that the FortiClient cannot reach the server. This setting does not affect local logs.	`90`
`<log_protocol>`	Enter the remote server type: • `faz`: FortiAnalyzer • `syslog`: Syslog server	
`<netlog_server>`	Enter the syslog server's IP address. FortiClient uses this setting only when `<log_protocol>` is set to `syslog`.	

`<netlog_categories>`	Enter the bitmask of logs to upload.
	Bitmask:
	`1 = traffic logs`
	`2 = vulnerability logs`
	`4 = event logs`
	Since these are bitmasks, you may combine them as follows:
	`3 = 1 or 2 (traffic and vulnerability)`
	`5 = 1 or 4 (traffic and event)`
	`6 = 2 or 4 (vulnerability and event)`
	`7 = 1 or 2 or 4 (all logs)`
		`7`

`<send_software_inventory>`	Enable sending software inventory reports to FortiAnalyzer. Boolean value: `[0 | 1]`	`1`
`<send_os_events>` elements Send OS event logs to FortiAnalyzer.		
`<enabled>`	Enable sending OS event logs to FortiAnalyzer.	`1`
`<interval>`	Interval to send OS event logs to FortiAnalyzer in seconds.	`120`

XML tag	Description	Default value
`<send_ms_exch_events>` elements Send Microsoft Exchange server logs to FortiAnalyzer.		
`<enabled>`	Enable sending Microsoft Exchange server logs to FortiAnalyzer.	`1`
`<interval>`	Interval to send Microsoft Exchange server logs to FortiAnalyzer in seconds.	`120`

The FortiShield daemon protects FortiClient's own file system and registry settings from modification by unauthorized persons.

Proxy settings

The `<proxy></proxy>` XML tags contain proxy-related information. If a proxy server configuration is required for Internet access, use the fields here to specify that configuration so that FortiClient's functions can use Fortinet's Internet-based services. Only FortiClient-originated traffic uses these settings.

```
<forticlient_configuration>
   <system>
      <proxy>
         <update>0</update>
         <fail_over_to_fdn>0</fail_over_to_fdn>
         <online_scep>0</online_scep>
         <virus_submission>0</virus_submission>
         <type>http</type>
         <address></address>
         <port>80</port>
         <username>Encrypted/NonEncrypted_UsernameString</username>
         <password>Encrypted/NonEncrypted_PasswordString</password>
      </proxy>
   </system>
</forticlient_configuration>
```

The following table provides the XML tags for proxy settings, as well as the descriptions and default values where applicable.

XML tag	Description	Default value
`<update>`	Enable updates. You should enable updates if a proxy server exists between FortiClient and the Internet. Boolean value: `[0 | 1]`	`0`
`<fail_over_to_fdn>`	Enable failover to FDN servers. Boolean value: `[0 | 1]`	`0`

XML tag	Description	Default value
<online_scep>	Enable Simple Certificate Enrollment Protocol (SCEP). Enable if you are using an SCEP server and a proxy server exists between FortiClient and the SCEP server. Boolean value: [0 | 1]	0
<virus_submission>	Enable virus submission to FDN. Enable if an SMTP proxy server exists between FortiClient and Fortinet's virus submission servers. Used when you *submit for analysis* or *submit as false positive*. Boolean value: [0 | 1]	0
<type>	The type of proxy being specified. Enter one of the following: • HTTP • SOCKS4 • SOCKS5	HTTP
<address>	The proxy server's IP address or FQDN.	
<port>	The proxy server's port number. Port range: 1 to 65535	80
<username>	If the proxy requires authentication, specify the username. Enter the encrypted or non-encrypted username.	
<password>	If the proxy requires authentication, specify the password. Enter the encrypted or non-encrypted password.	

Update settings

The <update></update> XML tags contain update-related information. Use this field to specify how FortiClient performs updates from FDN servers.

```
<forticlient_configuration>
   <system>
      <update>
         <use_custom_server>0</use_custom_server>
         <restrict_services_to_regions/>
         <use_legacy_fdn>1</use_legacy_fdn>
         <server></server>
         <port>80</port>
         <fail_over_
               servers>server1.fortinet.com:8008;172.81.30.6:80;server2.fortinet.com:80</fail_
               over_servers>
         <timeout>60</timeout>
         <failoverport>8000</failoverport>
         <fail_over_to_fdn>1</fail_over_to_fdn>
```

```
            <use_proxy_when_fail_over_to_fdn>1</use_proxy_when_fail_over_to_fdn>
            <scheduled_update>
               <enabled>1</enabled>
               <type>interval</type>
               <daily_at>03:00</daily_at>
               <update_interval_in_hours>3</update_interval_in_hours>
            </scheduled_update>
            <submit_virus_info_to_fds>0</submit_virus_info_to_fds>
            <submit_vuln_info_to_fds>1<submit_vuln_info_to_fds>
            <ocsp_mode>0</ocsp_mode>
         </update>
      </system>
   </forticlient_configuration>
```

The following table provides the XML tags for update settings, as well as the descriptions and default values where applicable.

XML tag	Description	Default value
`<use_custom_server>`	Define a custom server for updates. When the Boolean value is set to `0`, FortiClient uses the default FDN server address. When the Boolean value is set to `1`, you must specify the address in `<update><server>`. This setting is typically used when specifying a FortiManager as your update server. Boolean value: `[0 | 1]`	`0`
`<restrict_services_to_regions>`	Define whether to restrict the FDN server location to U.S.-only, or to use the nearest FDN server. To restrict to U.S.-only FDN server locations, set to `USA`, as follows: `<restrict_services_to_regions>USA</restrict_services_to_regions>`. Otherwise, leave blank. This is the default configuration.	

`<use_legacy_fdn>`	When enabled, update tasks use HTTP to connect to myforticlient.fortinet.net. `<fail_over_servers>` and `<fail_over_to_fdn>` are valid.
	When disabled, the following occurs:
	• Update tasks use HTTPS to connect to:
	  • fctupdate.fortinet.net (global region)
	  • fctusupdate.fortinet.net (US region)
	  • fcteuupdate.fortinet.net (EU region)
	• FortiClient checks the FortiGuard certificate validity:
	  • Expires in the future
	  • Has a valid domain name
	  • Is signed by one of the three CAs: Verisign, Digicert, and Comodo
	• FortiClient checks that the certificate is not revoked. By default, FortiClient connects to FDS via HTTPS. You can configure strict mode to check the certificate before connecting to FDS servers.
		`1`

XML tag	Description	Default value
<server>	Enter the update server's IP address or FQDN. Use when <use_custom_server> is set to 1. Optionally, you can specify the port number.	
<port>	Enter the update server's port number. If a port number is not specified in <update><server>, FortiClient uses this port. Port range: 1 to 65535	80
<fail_over_servers>	Enter the update servers to try if FortiClient cannot reach the primary server (with specified port or failover port). This option works only if <use_legacy_fdn> is 1. Enter the IP address or FQDN, followed by a colon and the port number if applicable. Separate multiple servers with a semicolon. FortiClient tries each server specified in order until one works or they all fail.	
<timeout>	Enter the connection timeout, in seconds, when attempting to reach a custom update server. If a server is reachable but not responding to update requests, the actual timeout is longer. The timeout specified is applied three times to one <server>:<port> pair before FortiClient gives up on this pair. If <failoverport> is specified, and greater than 0, there are a total of six attempts (three attempts for <server>:<port>, three attempts for <server>:<failoverport>).	60
<failoverport>	Failover port number. If FortiClient cannot reach the update server via the port specified in <server> or <port>, FortiClient tries the same address with this port. Port range: 1 to 65535	8000
<fail_over_to_fdn>	Determines whether or not to use FDN servers if communication with custom <server> fails. This option works only if <use_legacy_fdn> is 1. If the Boolean value is set to 1, <use_custom_server> is set to 1, and the update server specified by <server> cannot be reached, then FortiClient tries the default public FDN server. This is tried only if FortiClient has exhausted all other custom update server options. Boolean value: [0 | 1]	1
<use_proxy_when_fail_over_to_fdn>	Supports failover to FDN servers if FortiClient uses a proxy server defined with <forticlient_configuration><system><proxy> and <fail_over_to_fndn> is set to 1. Set <use_proxy_when_fail_over_to_fdn> to 1 to fail over to FDN servers. This element is ignored when no proxy server is defined with <forticlient_configuration><system><proxy>.	1

XML tag	Description	Default value
	Boolean value: [0 | 1]	
<submit_virus_info_to_fds>	Enable submitting virus information to FDN. Boolean value: [0 | 1]	1
<submit_vuln_info_to_fds>	Enable submitting vulnerability statistics to FDN. When set to 1, send vulnerability detection statistics from the vulnerability scanner to FDN. When set to 0, do not send vulnerability statistics to FDN. Boolean value: [0 | 1]	1
<ocsp_mode>	Enable or disable OCSP. **0** (default) Enable OCSP. **1** Disable OCSP.	0
<scheduled_update> elements Use these elements to define when FortiClient should look for engine, signature, and software updates, if enabled.		
<enabled>	Enable scheduled updates. Boolean value: [0 | 1]	1
<type>	Update frequency: daily or at regular hourly intervals. Enter one of the following: • daily • interval	interval
<daily_at>	Time of the day, in the format HH:MM (24-hour clock), this field is mandatory if the <type> tag is set to daily. This field specifies the time that FortiClient should check for updates.	
<update_interval_in_hours>	Update interval in hours if the <type> tag is set to interval. This field specifies the frequency that FortiClient should check for updates. The minimum value is 1, the maximum value is 24.	3

When <use_custom_server> is 0 or both <server> and <fail_over_servers> are each an empty (null) string, FortiClient only uses the default FDN server for software updates. If a string is specified in <server> and communication fails with that server, each of the servers specified in <fail_over_servers> are tried until one succeeds. If that also fails, then software updates are not possible unless <fail_over_to_fdn> is set to 1.

If communication fails with the server(s) specified in both <server> and <fail_over_servers>, <fail_over_to_fdn> determines the next course of action as listed:

<server>	<fail_over_to_fdn>	Result
"" (empty strings)	0	FortiClient only uses the FDN server.

<server>	<fail_over_to_fdn>	Result
“” (empty strings)	1	FortiClient only uses the FDN server.
“xyz” (valid IP address)	0	FortiClient never uses the FDN server.
“xyz” (valid IP address)	1	FortiClient only uses the FDN server as failover.

FortiProxy settings

The <fortiproxy></fortiproxy> XML tags contain FortiProxy information. FortiProxy is responsible for HTTP/HTTPS filtering and SMTP/POP3 AV scanning. Use these settings to configure FortiProxy's behavior.

```
<forticlient_configuration>
   <system>
      <fortiproxy>
         <enabled>1</enabled>
         <enable_https_proxy>1</enable_https_proxy>
         <http_timeout>60</http_timeout>
         <client_comforting>
            <pop3_client>1</pop3_client>
            <pop3_server>1</pop3_server>
            <smtp>1</smtp>
         </client_comforting>
         <selftest>
            <enabled>0</enabled>
            <last_port>-172</last_port>
            <notify>0</notify>
         </selftest>
      </fortiproxy>
   </system>
</forticlient_configuration>
```

The following table provides the XML tags for FortiProxy settings, as well as the descriptions and default values where applicable.

XML tag	Description	Default value
<enabled>	Enable FortiProxy. When set to 0, FortiProxy is disabled. HTTP/HTTPS filtering and SMTP/POP3 AV scanning are disabled. Boolean value: [0 | 1]	1
<enable_https_proxy>	Enable HTTPS proxy. When the Boolean value is set to 0, FortiProxy is unable to perform filtering on HTTPS traffic. Boolean value: [0 | 1]	1
<http_timeout>	Connection timeout in seconds. FortiProxy determines if the remote server is available based on this timeout value. Lower this timeout value if your client requires a faster fail response.	60
<client_comforting> elements		

XML tag	Description	Default value
Some email clients require continuous response from the server or a connection error may be triggered. Use these settings to enable this feature.		
<pop3_client>	Enable POP3 client comforting. Client comforting helps to prevent POP3 clients from complaining that the server has not responded in time. Boolean value: [0 | 1]	1
<pop3_server>	Enable POP3 server comforting. Server comforting helps to prevent POP3 servers from complaining that the client has not responded in time. This may be used in a situation where FortiClient is installed on a mail server. Boolean value: [0 | 1]	1
<smtp>	Enable SMTP client comforting. SMTP comforting helps to prevent SMTP clients from complaining that the server has not responded in time. Boolean value: [0 | 1]	1
<selftest> elements FortiProxy can detect if other software is disrupting internal traffic between FortiProxy's internal modules. It does this by sending packets periodically to 1.1.1.1, which are intercepted by FortiClient and dropped (they never leave the computer). If the packets are not detected, then it is deemed highly likely that third party software is intercepting the packets, signaling that FortiProxy is not able to perform regular traffic filtering.		
<enabled>	Enable self tests. FortiProxy periodically checks its own connectivity to determine if it is able to proxy other applications' traffic. Boolean value: [0 | 1]	1
<last_port>	Last port number used. This is the highest port number you want to allow FortiProxy to listen on. Use to prevent FortiProxy from binding to another port that another service normally uses. Port range: 65535 to 10000	65535
<notify>	When enabled, the user sees a bubble notification when self-testing detects that a third party program has blocked HTTP/HTTPS filtering and SMTP/POP3 AV scanning. Boolean value: [0 | 1]	1

Certificate settings

The <certificates></certificates> XML tags contain certificate settings. Following are the subsections:

- CRL: uses Online Certificate Status Protocol (OCSP).
- HDD

- CA certificate: base 64 encoded CA certificate.

```
<forticlient_configuration>
   <system>
      <certificates>
         <crl>
            <ocsp />
         </crl>
         <hdd />
         <ca>
            <certificate> <![CDATA[-----BEGIN CERTIFICATE-----
                  MIID8zCCAtugAwIBAgIIL8XAg5HYn7owDQYJKoZIhvcNAQELBQAwgakxCzAJBgNV
                  ..............................................................
                  1/LXOCM24niwVTn2pnik9mspwxygAwExE9gQPfbXaV14BrZcp5yzaorHLXKFNQmA
                  NdVcSlvoMqsDpeKU2Ohz+MXj1GsowHor96x88wbLe0CpeJLkwgmmH5TO37ke2Awp H9idHn5MdQ==
                  -----END CERTIFICATE----- ]]>
            </certificate>
         </ca>
      </certificates>
   </system>
</forticlient_configuration>
```

The following table provides the XML tags for certificate settings, as well as the descriptions and default values where applicable.

XML tag	Description	Default value
`<crl><OCSP>` elements		
`<enabled>`	Use OCSP. Boolean value: `[0 | 1]`	`0`
`<server>`	Enter the server IP address.	
`<port>`	Enter the server port number.	
`<ca><certificate>`	Contains a certificate in PEM format. FortiClient installs this certificate if it is embedded in the configuration.	

User identity settings

The `<user_identity></user_identity>` XML tags contain user identity settings:

```
<forticlient_configuration>
   <system>
      <user_identity>
         <enable_manually_entering>1</enable_manually_entering>
         <enable_linkedin>1</enable_linkedin>
         <enable_google>1</enable_google>
         <enable_salesforce>1</enable_salesforce>
         <notify_user>1</notify_user>
      </user_identity>
   </system>
</forticlient_configuration>
```

The following table provides the XML tags for user identity settings, as well as the descriptions and default values where applicable.

XML tag	Description	Default value
`<enable_manually_entering>`	Enable users to specify their identity in FortiClient by manually entering their details in FortiClient. Boolean value: `[0 | 1]`	
`<enable_linkedin>`	Enable users to specify their identity in FortiClient by logging in to their LinkedIn account. Boolean value: `[0 | 1]`	
`<enable_google>`	Enable users to specify their identity in FortiClient by logging in to their Google account. Boolean value: `[0 | 1]`	
`<enable_salesforce>`	Enable users to specify their identity in FortiClient by logging in to their Salesforce account. Boolean value: `[0 | 1]`	
`<notify_user>`	Displays a notification on the endpoint for the user to specify their identity. If the user closes the notification without specifying their identity, the notification displays every ten minutes until the user submits their identity information. Boolean value: `[0 | 1]`	

If you have not configured the above options or the user does not provide their identity information, EMS obtains and displays user details from the endpoint OS.

Installer settings

The `<installer></installer>` XML tags contain installer-related information.

```
<forticlient_configuration>
   <system>
      <installer>
         <allow_admin_uninstall_when_locked>1</allow_admin_uninstall_when_locked>
         <remove_user_data>0</remove_user_data>
      <installer>
   <system>
<forticlient_configuration>
```

The following table provides the XML tags for installer settings, as well as the descriptions and default values where applicable:

XML tag	Description	Default value
<allow_admin_ uninstall_ when_locked>	This setting allows the FortiClient endpoint administrator to uninstall FortiClient using the msiexec command line without needing to use the configured EMS disconnection password. This feature is especially useful if you are using a mobile device management solution to deploy FortiClient. Because FortiClient endpoint users have no administrative privileges, so there is no risk that an endpoint user could intentionally or accidentally uninstall FortiClient. For this element to take effect, <system><ui><password> must be configured. See UI settings on page 12. Boolean value: [0 | 1]	
<remove_user_ data>	Enable to remove FortiClient HKCU registry entries (which stores personal tunnel data and other data) for all logged-in users during uninstallation. Boolean value: [0 | 1]	0

Endpoint control

FortiClient usually downloads endpoint control configuration elements from FortiClient EMS after FortiClient connects to FortiClient EMS. There are two sections:

- The <endpoint_control></endpoint_control> XML tags contain general endpoint control attributes.
- Configuration details relating to specific FortiClient services, such as antivirus, Web Filter, Application Firewall, Vulnerability Scan, and so on. You can find these in the respective configuration elements of the services affected.

The following lists general endpoint control attributes:

```
<forticlient_configuration>
   <endpoint_control>
      <checksum></checksum>
      <enabled>1</enabled>
      <socket_connect_timeouts>1:5</socket_connect_timeouts>
      <system_data>Encrypted_String</system_data>
      <disable_unregister>0</disable_unregister>
      <invalid_cert_action>warn</invalid_cert_action>
      <edr_collector>1</edr_collector>
      <disable_fgt_switch>1</disable_fgt_switch>
      <ping_server>172.17.61.178:8010</ping_server>
      <fgt_name>FG_Hostname</fgt_name>
      <fgt_sn>Encrypted_Serial_Number_String</fgt_sn>
      <offnet_update>1</offnet_update>
      <user>Encrypted_UsernameString</user>
      <skip_confirmation>0</skip_confirmation>
      <fgt_logoff_on_fct_shutdown>1</fgt_logoff_on_fct_shutdown>
      <show_bubble_notifications>1</show_bubble_notifications>
      <avatar_enabled>1</avatar_enabled>
      <silent_registration>0</silent_registration>
```

```
<notify_fgt_on_logoff>1</notify_fgt_on_logoff>
<forensics_license>1</forensics_license>
<auto_start>0</auto_start>
<fgt_
      list>Enc256828d1e23febfa0b789324ea1fc9cf45acdc8af3888e7aa26677825bbf8d5d123fcbc2884f3
      cb3f2a03b5414ab01e6a6c22762add0c4f209224f052dec29491e1d15eee4a1a290a81b367c3d4a525125
      8ed14921e231547f52d9e3</fgt_list>
<send_software_inventory>1</send_software_inventory>
<onnet_addresses></onnet_addresses>
<onnet_mac_addresses></onnet_mac_addresses>
<override_invitation_code>1</override_invitation_code>
<confirm_migration>1</confirm_migration>
<onnet_rules>
   <rule_set>
      <dhcp_server>
         <dhcp_code>
            <criterion id="0">123456</criterion>
            <criterion id="1">abcdef</criterion>
         </dhcp_code>
      </dhcp_server>
      <local_ip>
         <ip_address>
            <criterion id="2">1234:abc:abcd:0012::0/64</criterion>
            <criterion id="3">2.2.2.2/3</criterion>
         </ip_address>
         <mac_address>
            <criterion id="4">11-11-11-11-11-11</criterion>
            <criterion id="5">22-22-22-22-22-22</criterion>
         </mac_address>
      </local_ip>
   </rule_set>
   <rule_set>
      <connection_media>
         <wifi_ssid>
            <criterion id="6">STAFF-NETWORK, WPA3</criterion>
         </wifi_ssid>
         <ethernet>
            <criterion id="10">Connected</criterion>
         </ethernet>
      </connection_media>
      <local_ip>
         <ip_address>
            <criterion id="7">1.1.1.1-2.2.2.2</criterion>
         </ip_address>
         <mac_address>
            <criterion id="8">33-33-33-33-33-33</criterion>
         </mac_address>
      </local_ip>
      <vpn>
         <tunnel_name>
            <criterion id="9">SSLVPN_VAN</criterion>
         </tunnel_name>
      </vpn>
   </rule_set>
</onnet_rules>
<ui>
   <display_antivirus>1</display_antivirus>
```

```
            <display_sandbox>1</display_sandbox>
            <display_webfilter>1</display_webfilter>
            <display_firewall>1</display_firewall>
            <display_vpn>1</display_vpn>
            <display_vulnerability_scan>1</display_vulnerability_scan>
            <display_ztna>1</display_ztna>
            <display_compliance>1</display_compliance>
            <hide_compliance_warning>0</hide_compliance_warning>
         </ui>
         <alerts>
            <notify_server>1</notify_server>
            <alert_threshold>1</alert_threshold>
         </alerts>
         <nac>
            <processes>
               <process id="1" name="MS Word" rule="present">
                  <signature name="processname.exe">SHA256 of file</signature>
                  <signature name="processname.exe">SHA256 of file</signature>
               </process>
               <process id="2" name="FortiToken" rule="absent">
                  <signature name="processname2.exe"/>
               </process>
            </processes>
            <files>
               <path id="1">Path to folder/file</path>
               <path id="2">Path to folder/file</path>
            </files>
            <registry>
               <path id="1">path to 32bit or 64bit registry key or value</path>
               <path id="2">path to 32bit or 64bit registry key or value</path>
            </registry>
         </nac>
      </endpoint_control>
   </forticlient_configuration>
```

The following table provides the XML tags for endpoint control, as well as descriptions and default values where applicable:

XML tag	Description	Default value
<checksum>	Configuration checksum that FortiGate and EMS calculate and enforce.	
<enabled>	Enable endpoint control.	
<system_data>	Endpoint control system information. This element is protected and not intended to be changed.	
<socket_connect_timeouts>	Probe timeout for endpoint control registration and keep-alive message timeout in seconds. probe_timeout:keep_alive_timeout Changing socket connect time outs may affect performance.	1:5
<ping_server>	Ping server's IP address or FQDN.	

XML tag	Description	Default value
	FortiClient updates this tag when it connects to FortiGate or EMS. FortiClient overwrites edits to this tag. You can safely delete this field.	
<fgt_name>	The FortiGate hostname or EMS that FortiClient is currently connected to, if any. FortiClient updates this tag when it connects to the FortiGate or EMS. FortiClient overwrites edits to this tag. You can safely delete this field.	
<fgt_sn>	The connected FortiGate or EMS's encrypted serial number, if any. Do not edit this field. You can safely delete this field.	
<offnet_update>	Enable synchronization of configuration updates from the FortiGate or EMS. Boolean value: [0 | 1]	1
<user>	Encrypted username.	
<skip_confirmation>	Skip prompting the user before proceeding to complete connection with FortiGate or EMS. Boolean value: [0 | 1]	0
<disable_unregister>	Prevent a connected client from being able to disconnect after successfully connecting to FortiGate or EMS. When this setting is configured as 1, the FortiClient user is unable to disconnect from the FortiGate or EMS after initial registration. This XML setting is intended to be used with <silent_registration>. If *Enable Registration Key for FortiClient* is enabled on FortiGate or EMS, configure this password in the <registration_password> XML tag, and enter the IP address or addresses of the FortiGate or EMS in the <addresses> XML tag. Boolean value: [0 | 1]	0
<invalid_cert_action>	Configure the action to take when FortiClient attempts to connect to EMS with an invalid certificate: • allow: allows FortiClient to connect to EMS with an invalid certificate. • warn: warn the user about the invalid server certificate. Ask the user whether to proceed with connecting to EMS, or terminate the connection attempt. FortiClient remembers the user's decision for this EMS, but displays the warning prompt if FortiClient attempts to connect to another EMS (using a different EMS FQDN/IP address and certificate) with an invalid certificate. • deny: block FortiClient from connecting to EMS with an invalid	

XML tag	Description	Default value
	certificate. When creating a new FortiClient installer on EMS, if EMS considers the certificate used for endpoint control invalid, the default action in the new installer is `allow`. The EMS administrator can modify this setting as desired. Boolean value: `[0 | 1]`	
`<edr_collector>`	Enable the Endpoint Detection & Response (EDR) feature. This feature is only available for endpoints connected to FortiClient Cloud with an EDR or extended detection & response license. See Creating a unified installer with EDR feature. Boolean value: `[0 | 1]`	
`<disable_fgt_switch>`	Disable the FortiGate switch. Boolean value: `[0 | 1]` This XML setting is intended for use with `<silent_registration>` and `<disable_unregister>`. If *Enable Registration Key for FortiClient* is enabled on the FortiGate, configure this password in the `<registration_password>` XML tag and enter the IP address or addresses of the FortiGate in the `<addresses>` XML tag. When `<disable_fgt_switch>` is configured as `1`, the FortiGate switch is disabled. As a result: • FortiClient does not probe the default gateway. • FortiClient does not automatically connect to the default gateway. • FortiClient ignores FortiGate broadcasts. • The discovered list displays only predefined FortiGate devices, if discovered.	
`<fgt_logoff_on_fct_shutdown>`	Notify FortiGate or EMS when FortiClient is shut down. Boolean value: `[0 | 1]`	`1`
`<show_bubble_notification>`	Show notifications in the system tray when a configuration update is received from the FortiGate or EMS. Boolean value: `[0 | 1]`	`1`
`<avatar_enabled>`	Control whether FortiClient sends the user avatar to EMS and the FortiGate. Boolean value: `[0 | 1]`	`1`
`<silent_registration>`	Connect to the FortiGate or EMS without prompting the user to accept connection. When enabled, no end user interaction is required to get the client to connect to FortiGate or EMS. Boolean value: `[0 | 1]` This XML setting is intended to be used with `<disable_unregister>`.	`0`

XML tag	Description	Default value
<notify_fgt_on_logoff>	Notify FortiGate or EMS when the FortiClient endpoint detects that a user logs off. When this setting is configured as 0, no message is sent to FortiGate or EMS. When this setting is configured as 1, a message is sent to FortiGate or EMS. Boolean value: [0 | 1]	
<forensics_license>	Enable the forensic analysis feature. You can request forensic analysis on a suspected device from on-premise EMS. The Fortinet forensics team investigates the logs and provides a detailed report with their verdict. You can download the report from EMS. Boolean value: [0 | 1]	
(Android only) <auto_start>	Enable <auto_start> to gray out the *Auto restart* configuration option in FortiClient Android so that FortiClient Android application always automatically starts. When disabled (default), FortiClient Android users will be able to configure the *Auto restart* option. Boolean value: [0 | 1]	0
<fgt_list>	Encrypted list of remembered FortiGate or EMS units. Do not edit this field. You can safely delete this field.	
<send_software_inventory>	Enable sending software inventory reports to EMS. Boolean value: [0 | 1]	1
<onnet_addresses>	Use the <address> subelement to configure IP addresses. If the endpoint's IP address matches the specified IP address, it is considered on-fabric.	
<onnet_mac_addresses>	Use the <address> subelement to configure IP addresses. If the endpoint's MAC address matches the specified MAC address, it is considered on-fabric.	
<override_invitation_code>	FortiClient installer/ESNAC uses the <standalone_invitation_code> value bundled in the deployment package to connect to EMS. Boolean value: [0 | 1]	
<confirm_migration>	FortiClient prompts user for confirmation when the EMS administrator has initiated migration to another EMS instance for the endpoint. • If the user confirms the migration, the endpoint attempts to migrate to the new EMS. If migration fails, the endpoint rolls back to connect to the previous EMS. • If the user does not confirm the migration, FortiClient attempts to retain connection to the original EMS instance.	

XML tag	Description	Default value
	Boolean value: `[0 | 1]`	
`<onnet_rules>` elements	Configure rule sets to determine endpoint on-/off-fabric status. The endpoint must satisfy all rules within a rule set for EMS to consider it as on-fabric. An endpoint only needs to satisfy one rule set to be considered on-fabric. See On-fabric Detection Rules. Use the `<criterion id>` element as shown in the sample code to configure multiple criteria for each rule type.	
`<dhcp_server>`	EMS considers the endpoint as satisfying the rule if it is connected to a DHCP server that matches the specified configuration. Use the following subelements: • `<dhcp_code>` • `<ip_address>` • `<mac_address>`	
`<dns_server>`	EMS considers the endpoint as satisfying the rule if it is connected to a DNS server that matches the specified configuration. Use the following subelements: • `<ip_address>` • `<mac_address>`	

`<ems_connection>`	EMS considers the endpoint as satisfying the rule if it is online with EMS. Configure this element as follows:
	`<ems_connection>`
	`  <online_status>Online with EMS</online_status>`
	`</ems_connection>`	

`<local_ip>`	EMS considers the endpoint as satisfying the rule if its Ethernet or wireless IP address is within the range specified and if its default gateway MAC address matches the one specified, if configured. Configuring the MAC address is optional. Use the following subelements: • `<ip_address>` • `<mac_address>`	
`<gateway>`	EMS considers the endpoint as satisfying the rule if its default gateway configuration matches the IP address specified and MAC address, if configured. Configuring the MAC address is optional. Use the following subelements: • `<ip_address>` • `<mac_address>`	
`<ping_server>`	EMS considers the endpoint as satisfying the rule if it can access the server at the specified IP address. Use the `<ip_address>` subelement.	

XML tag	Description	Default value
<public_ip>	EMS considers the endpoint as satisfying the rule if its public (WAN) IP address matches the one specified. Use the <ip_address> subelement.	
<connection_media>	EMS considers the endpoint as satisfying the rule if its network settings match all configured fields. Use the <wifi_ssid> and <ethernet> subelements as the sample code shows. When using the Ethernet rule, you must add at least one network identification rule.	
<vpn>	EMS considers the endpoint as satisfying the rule if its VPN settings match all configured fields. Use the <tunnel_name> subelement as the sample code shows.	
<ui> elements		
<display_antivirus>	Display the *Malware Protection* tab in FortiClient. When this setting is configured as 0, this feature does not display in the FortiClient console. Boolean value: [0 | 1]	
<display_sandbox>	Display the *Sandbox Detection* tab in FortiClient. When this setting is configured as 0, this feature does not display in the FortiClient console. Boolean value: [0 | 1]	
<display_webfilter>	Display the *Web Filter* tab in FortiClient. When this setting is configured as 0, this feature does not display in the FortiClient console. Boolean value: [0 | 1]	
<display_firewall>	Display the *Application Firewall* tab in FortiClient. When this setting is configured as 0, this feature does not display in the FortiClient console. Boolean value: [0 | 1]	
<display_vpn>	Display the *Remote Access* tab in FortiClient. Boolean value: [0 | 1] When this setting is configured as 0, this feature does not display in the FortiClient console.	
<display_vulnerability_scan>	Display the *Vulnerability Scan* tab in FortiClient. When this setting is configured as 0, this feature does not display in the FortiClient console. Boolean value: [0 | 1]	
<display_ztna>	Display the *ZTNA Connection Rules* tab in FortiClient.	

XML tag	Description	Default value
	When this setting is configured as 0, this feature does not display in the FortiClient console. Boolean value: [0 | 1]	
<hide_compliance_warning>	Hide the compliance enforcement feature message from the *Zero Trust Telemetry* tab. This option is only enforced on FortiClient endpoints connected to EMS. This option does not apply to monitored clients. Boolean value: [0 | 1]	1
<alerts> elements		
<notify_server>	Enable FortiClient to send alerts to FortiClient EMS. The priority of alerts that FortiClient sends depends on <alert_threshold>. Boolean value: [0 | 1]	1
<alert_threshold>	Configures the threshold of alerts FortiClient sends to EMS. Enter one of the following: • 1: High priority alerts • 3: Medium priority alerts • 5: Low priority alerts	1
<nac> elements This element (with its child elements) specifies up to three compliance rules for network access control (NAC). When an endpoint configuration does not comply with all compliance rules configured in the <nac> elements, non-compliance is triggered, and network access may be blocked. For information about how compliance rules work, see the *FortiClient Administration Guide*. Compliance rules apply only when FortiClient is connected to FortiGate. When FortiClient is not connected to FortiGate, compliance rules are not used. You can configure none, one, or all three compliance rules.		
<processes>	(Optional) Create a policy for an application and its signature.	
<process>	Identify an application name and its signature. This element should be repeated for each unique application name.	
<process id="" name="" rule="">	ID of this process entry and name of the application that is associated with the signatures, for example, <process id="1" name="MS Word">. Also shows whether FortiGate compliance rules require this process to be present or absent on the endpoint.	
<signature name="" />	Identify the application name and signature. Repeat this element for different versions of the same application.	
<files>	(Optional) Create a policy for a file and path. The policy is compliant when the file can be found.	
<path id=""/>	ID of this path entry. Identify the path of the file for the policy. Repeat this element for each unique file path.	
<registry>	(Optional) Create a policy for a registry key or value.	

XML tag	Description	Default value
`<path id=""/>`	ID of this path entry. Identify the registry key or value. When the path ends with a forward slash (/), it identifies a key. When the path ends without a forward slash, it identifies a registry value.	

When you disable `<ui>` elements from displaying in the FortiClient console, the modules are still installed as part of the FortiClient installation. To configure a VPN-only installation, you can use FortiClient EMS. When selecting VPN only, all other modules are not part of the FortiClient installation.

VPN

The <VPN></VPN> XML tags contain VPN-related information. The VPN configuration includes the following subsections. The VPN options section describes global options that apply to both SSL VPN and IPsec VPN. Options specific to SSL VPN or IPsec VPN are described in their respective sections:

VPN options

The VPN <options> XML tag contains global information controlling VPN states:

```
<forticlient_configuration>
   <vpn>
      <options>
         <current_connection_name>ssldemo</current_connection_name>
         <current_connection_type>ssl</current_connection_type>
         <autoconnect_tunnel></autoconnect_tunnel>
         <autoconnect_only_when_offnet>0</autoconnect_only_when_offnet>
         <autoconnect_only_when_epc_state_determined>0</autoconnect_only_when_epc_state_determined>
         <autoconnect_on_install>1</autoconnect_on_install>
         <keep_running_max_tries>0</keep_running_max_tries>
         <secure_remote_access>0</secure_remote_access>
         <minimize_window_on_connect>1</minimize_window_on_connect>
         <allow_personal_vpns>1</allow_personal_vpns>
         <disable_connect_disconnect>0</disable_connect_disconnect>
         <on_os_start_connect>SSLVPN_Name</on_os_start_connect>
         <on_os_start_connect_has_priority>0</on_os_start_connect_has_priority>
         <show_vpn_before_logon>1</show_vpn_before_logon>
         <use_windows_credentials>1</use_windows_credentials>
         <use_legacy_vpn_before_logon>0</use_legacy_vpn_before_logon>
         <disable_dead_gateway_detection>0</disable_dead_gateway_detection>
         <vendor_id></vendor_id>
         <disable_internet_check>0</disable_internet_check>
         <suppress_vpn_notification>0</suppress_vpn_notification>
         <before_logon_saml_auth>1</before_logon_saml_auth>
         <after_logon_saml_auth>0</after_logon_saml_auth>
         <certs_require_keyspec>0</certs_require_keyspec>
         <vpn_before_logon_style>1</vpn_before_logon_style>
         <keep_running_delay>0</keep_running_delay>
         <failover_delay>0</failover_delay>
         <power_resume_autoconnect_delay>5</power_resume_autoconnect_delay>
         <user_login_autoconnect_delay>0</user_login_autoconnect_delay>
         <enable_multi_vpn>1</enable_multi_vpn>
         <enable_view_selected_vpns>0</enable_view_selected_vpns>
         <disconnect_password>1</disconnect_password>
         <refresh_btn>1</refresh_btn>
         <sase_location_selection>1</sase_location_selection>
         <enforce_disabling_smartdns>0</enforce_disabling_smartdns>
         <saml_auth_enable_proxy_server>1</saml_auth_enable_proxy_server>
         <lockdown>
            <enabled>1</enabled>
```

```
            <grace_period>120</grace_period>
            <max_attempts>3</max_attempts>
            <exceptions>
               <apps>
                  <app>C:\Program Files\Google\Chrome\Application\chrome.exe</app>
               </apps>
               <ips>
                  <ip>172.17.81.15/32</ip>
               </ips>
               <icdb_domains>
                  <name>adobe</name>
               </icdb_domains>
               <domains>
                  <domain>google.com</domain>
               </domain>
            </exceptions>
            <detect_captive_portal>
                           <enabled>1</enabled>
               <login_method>1</login_method>
                        <os_active_probing>0</os_active_probing>
            </detect_captive_portal>
         </lockdown>
      </options>
   </vpn>
</forticlient_configuration>
```

The following table provides XML tags for VPN options, as well as the descriptions and default values where applicable:

XML tag	Description	Default value
`<current_connection_name>`	Enter the current connection name, if any.	
`<current_connection_type>`	Select the current connection's VPN type: `[ipsec | ssl]`	
`<autoconnect_tunnel>`	Name of the configured IPsec or SSL VPN tunnel to automatically connect to when FortiClient starts.	
`<autoconnect_only_when_offnet>`	Autoconnect only when FortiClient is off-fabric. Boolean value: `[0 | 1]`	`0`
`<autoconnect_only_when_epc_state_determined>`	When FortiClient cannot determine the endpoint's on-/off-Fabric status, it does not autoconnect to VPN. If the autoconnect process was in progress, FortiClient halts the process and waits for the on-/off-Fabric status to be determined. This tag does not apply to when the user manually attempts connection to VPN via the GUI or FortiTray. It only applies to VPN autoconnect and related reconnection attempts. Boolean value: `[0 | 1]`	

XML tag	Description	Default value
<autoconnect_on_install>	When enabled, the endpoint automatically connects to the VPN tunnel specified in <autoconnect_tunnel> after FortiClient receives an endpoint profile update. Boolean value: [0 | 1]	
<keep_running_max_tries>	Maximum number of attempts to make when retrying a VPN connection that FortiClient lost due to network issues. If you disable this option, FortiClient retries the connection indefinitely.	0
<secure_remote_access>	When enabled, FortiClient allows or denies the endpoint from connecting to a VPN tunnel based on the tags applied to the endpoint and whether those tags are configured as <allowed> or <prohibited> in the specified VPN tunnel configuration. If configured, FortiClient displays a custom warning message to the end user. Boolean value: [0 | 1]	
<minimize_window_on_connect>	If FortiClient is connected to one VPN tunnel, the FortiClient console minimizes after successfully establishing the tunnel connection. If FortiClient is connected to multiple concurrent VPN tunnels, the FortiClient console does not automatically minimize regardless of this setting. Boolean value: [0 | 1]	1
<allow_personal_vpns>	Enable end users to create, modify, and use personal VPN configurations. When you disable this setting, FortiClient users cannot configure personal VPN connections. Only provisioned VPN connections are available to the user. Boolean value: [0 | 1]	1
<use_legacy_vpn_before_logon>	Use the old VPN before logon interface. Boolean value: [0 | 1]	1
<disable_connect_disconnect>	Enable the *Connect/Disconnect* button when using *Auto Connect* with VPN. Boolean value: [0 | 1]	0
<on_os_start_connect>	Enter the name of the VPN tunnel that FortiClient starts when the OS boots up. You must configure this tunnel with <machine> enabled, with its credentials provided in the XML configuration and stored in HKLM as opposed to HKCU. If using a certificate, the certificate must exist in the computer certificate store.	

XML tag	Description	Default value
	If the stored tunnel credentials are incorrect, FortiClient prompts the user for credentials to establish the tunnel connection. This feature may not work for IPsec VPN tunnels using certificates when per-user autoconnect is configured.	
<on_os_start_connect_has_priority>	When you disable this setting, FortiClient connects to a per-user VPN tunnel after user logon. If FortiClient was previously connected to a VPN tunnel configured with the <machine> element, it disconnects from that tunnel to connect to the per-user tunnel. When this element is enabled, the tunnel configured with the <machine> element takes priority over any per-user tunnel configured. The machine tunnel remains connected after user logon. Boolean value: [0 | 1]	0
<show_vpn_before_logon>	Allow user to select a VPN connection before logging into the system. Boolean value: [0 | 1]	0
<use_windows_credentials>	Connect with the current username and password. You must enable <show_vpn_before_logon> before enabling <use_windows_credentials>. Boolean value: [0 | 1]	1
<disable_dead_gateway_detection>	Notifies the Windows OS to disable the detection of dead gateway. You may enable this element if you observe that IPsec VPN sends packets using an IP address other than those in the IP address pool assigned by the IPsec VPN server. Boolean value: [0 | 1]	
<vendor_id>	The default value is empty, signifying that FortiClient should use its hard-coded ID during IPsec VPN connection.	
<disable_internet_check>	When this setting is disabled, VPN autoconnect only starts FortiClient can access the internet. When enabled, VPN autoconnect starts even if FortiClient cannot access the internet. Boolean value: [0 | 1]	0
<suppress_vpn_notification>	Block FortiClient from displaying any VPN connection or error notifications. Boolean value: [0 | 1]	0
<before_logon_saml_auth>	Depending on the SAML authentication use case, you may need to use a specific authentication framework. Configure the desired framework to use if connecting to VPN before logon:	1

XML tag	Description	Default value
	1 - Electron (Chromium)—Recommended as it provides enhanced security and aligns with modern web standards. 2 - WebBrowser (Internet Explorer) Microsoft Edge WebView2 is unsupported.	
<after_logon_saml_auth>	Depending on the SAML authentication use case, you may need to use a specific authentication framework. Configure the desired framework to use if connecting to VPN after logon: 0 - Microsoft Edge WebView2 1 - Electron (Chromium) 2 - WebBrowser (Internet Explorer) —If Microsoft Entra ID is used as an identity provider and the endpoint is Azure-joined or added to an Azure account, the VPN connection establishes seamlessly without prompting for Azure credentials, regardless of the *Save Password* configuration. *Microsoft Edge WebView2* or *Electron* is recommended as they provide enhanced security and align with modern web standards.	0
<certs_require_keyspec>	If this element is disabled, FortiClient includes all certificates that have a NULL key specification when prompting the user to select a certificate. If this element is enabled, FortiClient only lists certificates that include AT_KEYEXCHANGE/AT_SIGNATURE/CERT_NCRYPT_KEY_SPEC when prompting the user to select a certificate. The state of the key spec is only accessible by querying the certificate for its private key. If the certificate is on a smartcard or if the private key is password-protected, Windows requests a PIN or password. This can result in unwanted PIN or password prompts when the user opens the FortiClient GUI. For example, it can result in PIN or password prompts when viewing the *Remote Access* tab in the FortiClient GUI, potentially one prompt for each certificate on the smartcard. Boolean value: [0 | 1]	0
<vpn_before_logon_style>	If this element is disabled, FortiClient displays the VPN tunnel list below the Windows username and password fields for VPN before logon.	1

XML tag	Description	Default value
	If this element is enabled, FortiClient displays the VPN tunnel list above the Windows username and password fields for VPN before logon. Boolean value: `[0 | 1]`	
`<keep_running_delay>`	Delay in seconds between a tunnel being detected as unexpectedly disconnected and the VPN controller attempting to reconnect the tunnel.	
`<failover_delay>`	Used when `<failover_sslvpn_connection>` is defined in an IPsec VPN tunnel. Delay in seconds between failing to connect the IPsec VPN tunnel and attempting to connect the failover SSL VPN connection tunnel.	
`<power_resume_autoconnect_delay>`	Requires an autoconnect tunnel to be defined (user or machine). Delay in seconds between the OS signaling power resume, such as waking up, and the VPN controller attempting to connect the autoconnect tunnel.	
`<user_login_autoconnect_delay>`	Requires an autoconnect tunnel to be defined (per-user autoconnect, not machine autoconnect). Delay in seconds between the OS signaling a user has logged into the OS and the VPN controller attempting to connect the user's autoconnect tunnel.	
`<enable_multi_vpn>`	Enable FortiClient to connect to multiple tunnels concurrently. This feature is in beta and only supports IPsec VPN IKEv2 tunnels. Boolean value: `[0 | 1]`	`0`
`<enable_view_selected_vpns>`	Enable for FortiClient to display pinned tunnels by default. If disabled, the FortiClient GUI displays all configured VPN tunnels. The user can select *View* > *Selected VPNs* to only display pinned tunnels. FortiClient remembers this setting and only shows pinned tunnels for that user when they open the FortiClient console in the future. FortiClient respects the local setting over the EMS setting in this case. Boolean value: `[0 | 1]`	`0`
`<disconnect_password>`	Configure the password for users to disconnect FortiClient from FortiOS. The password will be encrypted using the PBKDF2 method. The default is no password. When a disconnect password is set, the *Disconnect* option will remain visible to end users using autoconnect VPN even if `<disable_connect_disconnect>` is set to 1.	

XML tag	Description	Default value
`<enforce_disabling_smartdns>`	This element changes the status of the following registry key: *Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient\DisableSmartNameResolution* or in a group policy, *Computer Configuration > Administrative Templates > Network > DNS Client > Turn off smart multi-homed name resolution*. When using IPsec or SSL VPN split DNS, if this element is enabled, it may prevent the client from sending simultaneous DNS queries on multiple network interfaces. However, in cases where DNS queries via the FortiClient VPN virtual network interface are slow or fail, Windows may still attempt to resolve DNS queries through the physical network adapter. If you want to route DNS queries primarily through the FortiClient VPN interface, enabling the element helps ensure that queries are typically restricted to a single interface, though this behavior cannot be fully guaranteed. Boolean value: `[0 | 1]`	`0`
`<saml_auth_enable_proxy_server>`	Enable proxy automatic detection for WebView2 SAML authentication. When disabled, the SAML authentication window can load faster. Boolean value: `[0 | 1]`	`1`
`<lockdown>` elements		
`<enabled>`	Configure network lockdown for off-Fabric endpoints when they are not connected to VPN. When network lockdown is configured, when an endpoint goes off-fabric, a grace period that the EMS administrator configured comes into effect. During the grace period, an endpoint can continue to access LAN and the internet without restrictions. If the endpoint does not connect to VPN by the end of the grace period, the endpoint cannot access LAN and the internet. It can still access IP addresses and applications that the EMS administrator has configured as exceptions, as well as connect to VPN to regain internet access. For a full tunnel VPN, LAN is only accessible if exclusive routing is disabled. The administrator configures a limited number of attempts for the end user to enter valid VPN credentials. Once the user reaches the limit, the endpoint is in network lockdown. Boolean value: `[0 | 1]`	

XML tag	Description	Default value
<grace_period>	Configure a grace period in seconds during which an off-fabric endpoint that is not connected to VPN can continue to access LAN and the internet without restrictions. Enter a value between 20 and 3600.	120
<max_attempts>	Configure the maximum number of attempts for the end user of an off-Fabric endpoint to enter valid VPN credentials.	3
<lockdown><exceptions> elements		
<apps><app>	Enter the path to applications that an off-Fabric endpoint that is not connected to VPN can still access.	
<ips><ip>	Enter IP addresses that an off-Fabric endpoint that is not connected to VPN can still access. This element supports entering an IP address or subnet. You can specify a port or port range to access the IP address or subnet on. TCP, UDP, and ICMP are supported.	
<icdb_domains><name>	Enter a SaaS application name that an off-Fabric endpoint that is not connected to VPN can still access.	
<domains><domain>	Enter domains or fully qualified domain names that an off-Fabric endpoint that is not connected to VPN can still access.	
<lockdown><detect_captive_portal> elements		
<enabled>	Enable captive portal detection. Boolean value: [0 | 1]	
<login_method>	Specify the method used to handle captive portal login. This element only supports the FortiClient embedded browser. Boolean value: [0 | 1]	
<os_active_probing>	Enable or disable active probing by the operating system. Active probing involves sending network requests to determine if a captive portal is present. Boolean value: [0 | 1]	

SSL VPN

SSL VPN configurations consist of one <options> section, followed by one or more VPN <connection> sections:

```
<forticlient_configuration>
   <vpn>
      <sslvpn>
         <options>
            <enabled>1</enabled>
            <dnscache_service_control>0</dnscache_service_control>
            <!-- 0=disable dnscache, 1=do not tounch dnscache service, 2=restart dnscache service,
                  3=sc control dnscache paramchange -->
            <prefer_sslvpn_dns>1</prefer_sslvpn_dns>
            <use_legacy_ssl_adapter>1</use_legacy_ssl_adapter>
            <preferred_dtls_tunnel>1</preferred_dtls_tunnel>
            <block_ipv6>0</block_ipv6>
            <no_dhcp_server_route>0</no_dhcp_server_route>
            <no_dns_registration>0</no_dns_registration>
            <disallow_invalid_server_certificate>0</disallow_invalid_server_certificate>
            <keep_connection_alive>1</keep_connection_alive>
            <show_auth_cert_only>1</show_auth_cert_only>
            <negative_split_tunnel_metric>10</negative_split_tunnel_metric>
            <dtls_mtu>1100</dtls_mtu>
            <mtu_size>1300</mtu_size>
         </options>
         <connections>
            <connection>
               <name>SSLVPN_Name</name>
               <description>Optional_Description</description>
               <no_vnic_dns_server>0</no_vnic_dns_server>
               <server>ssldemo.fortinet.com:10443</server>
               <username>Encrypted/NonEncrypted_UsernameString</username>
               <single_user_mode>0</single_user_mode>
               <disclaimer_msg></disclaimer_msg>
               <redundant_sort_method>0</redundant_sort_method>
               <sso_enabled>1</sso_enabled>
               <keep_fqdn_resolution_consistency>1</keep_fqdn_resolution_consistency>
               <use_external_browser>1</use_external_browser>
               <warn_invalid_server_certificate>1</warn_invalid_server_certificate>
               <machine>1</machine>
               <pinned>1</pinned>
               <dual_stack>0</dual_stack>
               <keep_running>0</keep_running>
               <resolve_to_ipv4_only>1</resolve_to_ipv4_only>
               <android_cert_path>certdir/</android_cert_path>
               <pkcs11_lib>/usr/lib/sample.so</pkcs11_lib>
               <traffic_keep_strategy>0</traffic_keep_strategy>
               <traffic_keep_timer>5000</traffic_keep_timer>
               <saml_cert_selection>1</saml_cert_selection>
               <ssl_vpn_method>1</ssl_vpn_method>
               <fido_auth>1</fido_auth>
               <splitdns_tcp_enabled>1</splitdns_tcp_enabled>
               <ui>
```

```
      <show_remember_password>1</show_remember_password>
      <show_alwaysup>1</show_alwaysup>
      <show_autoconnect>1</show_autoconnect>
      <save_username>0</save_username>
      <save_password>0</save_password>
   </ui>
   <password>Encrypted/NonEncrypted_PasswordString</password>
   <allow_standard_user_use_system_cert>0</allow_standard_user_use_system_cert>
   <prompt_certificate>0</prompt_certificate>
   <prompt_username>0</prompt_username>
   <fgt>1</fgt>
   <certificate/>
   <on_connect>
      <script>
         <os>windows</os>
         <script>
            <![CDATA[test]]>
         </script>
      </script>
   </on_connect>
   <on_disconnect>
      <script>
         <os>windows</os>
      <script>
         <![CDATA]]>
      </script>
      </script>
   </on_disconnect>
   <traffic_control>
      <enabled>1</enabled>
      <mode>2</mode>
      <enable_local_lan>1</enable_local_lan>
      <apps>
         <app>%LOCALAPPDATA%\Microsoft\Teams\Current\Teams.exe</app>
         <app>%appdata%\Zoom\bin\Zoom.exe</app>
         <app>C:\Program Files (x86)\Microsoft\Skype for Desktop\skype.exe</app>
         <app>%LOCALAPPDATA%\GoToMeeting\18068\g2mcomm.exe</app>
         <app>%LOCALAPPDATA%\GoToMeeting\18068\g2mlauncher.exe</app>
         <app>%LOCALAPPDATA%\GoToMeeting\18068\g2mstart.exe</app>
      </apps>
      <fqdns>
         <fqdn>webex.com</fqdn>
         <fqdn>gotomeeting.com</fqdn>
         <fqdn>youtube.com</fqdn>
      </fqdns>
   </traffic_control>
   <tags>
      <allowed>NoVuln</allowed>
      <prohibited>CriticalVuln</prohibited>
   </tags>
   <azure_auto_login>
      <enabled></enabled>
      <azure_app>
         <tenant_name></tenant_name>
         <client_id></client_id>
      </azure_app>
   </azure_auto_login>
```

```
            <vpn_before_logon>
               <username_format>username</username_format>
            <vpn_before_logon/>
            <android_app_control>
               <enabled>0</enabled>
               <mode>1</mode>
               <apps>
                  <app>com.google.android.youtube</app>
               </apps>
            </android_app_control>
         </connection>
      </connections>
   </sslvpn>
 </vpn>
</forticlient_configuration>
```

The following table provides SSL VPN XML tags, as well as the descriptions and default values where applicable:

XML tag	Description	Default value
`<sslvpn><options>` elements		
`<enabled>`	Enable SSL VPN. Boolean value: `[0 | 1]`	`1`
`<dnscache_service_control>`	FortiClient disables Windows OS DNS cache when FortiClient establishes an SSL VPN tunnel. The DNS cache is restored after FortiClient disconnects from the SSL VPN tunnel. If you observe that FSSO clients do not function correctly when an SSL VPN tunnel is up, use `<prefer_sslvpn_dns>` to control the DNS cache. Boolean value: `[0 | 1]`	`0`
`<prefer_sslvpn_dns>`	When disabled, the custom DNS server from SSL VPN is not added to the physical interface. When enabled, the custom DNS server from SSL VPN is prepended to the physical interface. Boolean value: `[0 | 1]`	`0`
`<use_legacy_ssl_adapter>`	When disabled, FortiClient uses the new SSL driver. When enabled, FortiClient uses the legacy SSL driver. Boolean value: `[0 | 1]`	`1`
`<preferred_dtls_tunnel>`	Only FortiClient (Windows) supports DTLS. When disabled, FortiClient uses TLS, even if `dtls-tunnel` is enabled on the FortiGate. When enabled, FortiClient uses DTLS, if it is enabled on the FortiGate, and tunnel establishment succeeds. If `dtls-tunnel` is disabled on the FortiGate, or tunnel establishment does not succeed, FortiClient uses TLS. DTLS tunnel uses UDP instead of TCP and can increase throughput over VPN.	

XML tag	Description	Default value
	Boolean value: [0 | 1]	
<block_ipv6>	When disabled, FortiClient allows IPv6 traffic. When enabled, FortiClient blocks IPv6 traffic sent outside of VPN interface when it establishes the VPN connection. This option is unsupported on FortiClient (Linux). Boolean value: [0 | 1]	0
<no_dhcp_server_route>	When disabled, FortiClient creates the DHCP public server route upon tunnel establishment. When this setting is 1, FortiClient does not create the DHCP public server route upon tunnel establishment. Boolean value: [0 | 1]	0
<no_dns_registration>	When this setting is 0, FortiClient registers the SSL VPN adapter's address in the Active Directory (AD) DNS server. When this setting is 1, FortiClient does not register the SSL VPN adapter's address in the AD DNS server. When this setting is 2, FortiClient registers only its own tunnel interface IP address in the AD DNS server.	0
<disallow_invalid_server_certificate>	When this setting is 0 and an invalid server certificate is used, FortiClient displays a popup that allows the user to continue with the invalid certificate. When this setting is 1 and an invalid server certificate is used, FortiClient does not display a popup and stops the connection. Boolean value: [0 | 1]	0
<keep_connection_alive>	Retry restoring an active VPN session connection. Boolean value: [0 | 1]	
<show_auth_cert_only>	Suppress dialogs from displaying certificates that do not bear OID "1.3.6.1.5.5.7.3.2" (client authentication). Boolean value: [0 | 1]	0
<negative_split_tunnel_metric>	Set route metric for certain subnet as needed. For example, you may want to set negative split routes with a higher metric, so these routes can be deactivated when another VPN product is being used and sets the same routes as FortiClient negatives split routes but with a lower metric. This configuration is not recommended for most use cases. This element only takes effect when you enable negative split tunnel.	
<dtls_mtu>	Maximum transmit unit (MTU) size for packets on SSL VPN tunnels when using DTLS. Set from a minimum of 576 to a maximum of 1500 bytes.	1100

XML tag	Description	Default value
<mtu_size>	Maximum transmit unit (MTU) size for packets on SSL VPN tunnels when not using DTLS. Set from a minimum of 576 to a maximum of 1392 bytes.	1300

The <connections> XML tag may contain one or more <connection> elements. Each <connection> has the following:

- Information used to establish an SSL VPN connection
- on_connect: a script to run right after a successful connection
- on_disconnect: a script to run just after a disconnection

The following table provides VPN connection XML tags, the description, and the default value (where applicable).

XML tag	Description	Default value
<name>	VPN connection name. The VPN connection name is mandatory. If a connection of this type and this name exists, FortiClient overwrites its values with the new ones.	
<description>	Optional description to identify the VPN connection.	
<no_vnic_dns_server>	If enabled, FortiClient does not send DNS requests to the SSL VPN virtual adapter and only to the local adapters. If disabled, FortiClient may send DNS requests to both the SSL VPN virtual and local adapters depending on other DNS configuration settings. Boolean value: [0 | 1]	0
<server>	SSL server IP address or FQDN, along with the port number as applicable.	Default port number: 443
<username>	Encrypted or non-encrypted username on SSL server.	
<single_user_mode>	Enable single user mode. If enabled, new and existing VPN connections cannot be established or are disconnected if more than one user is logged on the computer. Boolean value: [0 | 1]	0
<disclaimer_msg>	Enter a disclaimer message that appears when the user attempts VPN connection. The user must accept the message to allow connection.	

XML tag	Description	Default value
<redundant_sort_method>	How FortiClient determines the order in which to try connection to the SSL VPN servers when more than one is defined. FortiClient calculates the order before each SSL VPN connection attempt. • When the value is 0, FortiClient tries the order explicitly defined in the <server> tag. • When the value is 1, FortiClient determines the order by the ping response speed. • When the value is 2, FortiClient determines the order by the TCP round trip time.	0
<sso_enabled>	Enable SAML SSO for the VPN tunnel. For this feature to function, the administrator must have configured the necessary options on the Service Provider and Identity Provider. See SAML support for SSL VPN.	
<keep_fqdn_resolution_consistency>	Enable FortiClient to remember the IP address with which it contacts the FortiGate and reuse it throughout the connection phase. This feature helps support load balancing SSL VPN gateways with one FQDN. This feature is only available for FortiClient (Windows). See Load balancing SSL VPN gateways with one FQDN.	
<use_external_browser>	Display the SAML authentication prompt in an external browser instead of in the FortiClient GUI. See Using a browser as an external user-agent for SAML authentication in an SSL VPN connection.	
<warn_invalid_server_certificate>	Display a warning message if the server certificate is invalid. EMS automatically copies this setting to each SSL VPN tunnel. Boolean value: [0 | 1]	0
<machine>	When this setting is 1, FortiClient can connect to the tunnel without user interaction. See <on_os_start_connect> in VPN options on page 38. Boolean value: [0 | 1]	
<pinned>	Indicates that a tunnel has been selected by the EMS configuration. When a tunnel is pinned, you cannot manually unpin it from the FortiClient GUI. If a tunnel is not pinned, you can select or deselect it. All pinned tunnels display in the *Remote Access* tab in FortiClient. Boolean value: [0 | 1]	
<dual_stack>	Enable or disable FortiClient to establish a dual stack SSL VPN tunnel to allow both IPv4 and IPv6 traffic to pass through. See Dual stack IPv4 and IPv6 support for SSL VPN. The following summarizes what occurs when dual stack settings differ between FortiClient and FortiOS:	

XML tag	Description	Default value
	• If FortiClient XML is set to `<dual_stack>1</dual_stack>` and FortiOS CLI has set `dual-stack-mode enable`, the tunnel allows IPv4 and IPv6 traffic. • If FortiClient XML is set to `<dual_stack>1</dual_stack>` and FortiOS CLI has set `dual-stack-mode disable`, FortiClient cannot connect to the SSL VPN tunnel. • If FortiClient XML is set to `<dual_stack>0</dual_stack>` and FortiOS CLI has set `dual-stack-mode enable` or `disable`, FortiClient can connect to the SSL VPN tunnel, but IPv4 traffic can only go through the IPv4 tunnel, and IPv6 traffic can only go through the IPv6 tunnel. In summary, for dual stack to function, you must enable the respective `dual_stack` settings for both FortiClient and FortiGate. In addition, the FortiGate firewall policy must allow both IPv4 and IPv6 traffic to go through VPN tunnel. Only FortiClient (Windows) supports this feature. Boolean value: `[0 | 1]`	
`<keep_running>`	Ensures that the VPN tunnel remains connected if it is already connected. This is useful when there is a temporary network disconnection that causes the tunnel to drop the connection. An EMS-pushed tunnel with `<keep_running>` enabled displays with *Save Password* and *Always Up* enabled and grayed out in the FortiClient GUI. Boolean value: `[0 | 1]`	0
`<resolve_to_ipv4_only>`	If the SSL VPN gateway FQDN resolves to both IPv4 and IPv6 addresses, this option forces FortiClient to use the IPv4 address to access the SSL VPN gateway. When you disable this option, FortiClient may use the IPv4 or IPv6 address to access the SSL VPN gateway. Boolean value: `[0 | 1]`	
`<android_cert_path>`	Configure a certificate location for FortiClient (Android) to automatically go to when doing the following: • When selecting a certificate • When the user clicks *Connect* to connect to this tunnel See Certificate path configuration for automated certificate selection.	
`<pkcs11_lib>`	Enter the name or path of a shared library on a Linux machine where FortiClient can find a smart card certificate to authenticate the connection. For example, you could enter `/usr/lib/sample.so`.	
`<traffic_keep_strategy>`	Configure the traffic strategy: • **0**—Keep traffic in tunnel with route change to preserve the route's metric.	`0`

XML tag	Description	Default value
	• **1**—Flush DNS, which may help resolve issues with accessing local services via DNS. • **2**—No change to the traffic.	
<traffic_keep_timer>	Configure the interval (in milliseconds) for route change or DNS flush. The minimum is 3000. If you specify a value below 3000, FortiClient will use 3000 instead. No maximum is enforced.	5000
<saml_cert_selection>	Enable to allow certificate selection for identity provider client certificate challenge. If you disable this setting, the FortiClient internal browser allows the system to select the default option for the client certificate challenge. This setting only applies to FortiClient (macOS). Boolean value: [0 | 1]	0
<ssl_vpn_method>	This option only applies for FortiClient (macOS). Enable to use alternative OpenSSL code, which can be used when using DTLS fallback to TLS. Otherwise, FortiClient uses the default existing SSL VPN logic. Boolean value: [0 | 1]	0
<fido_auth>	Enable to allow Yubikey (FIDO2) authentication for SAML SSO VPN connections in the FortiClient embedded (internal) browser for macOS. Boolean value: [0 | 1]	
<password>	Given user's encrypted or non-encrypted password.	
<allow_standard_user_use_system_cert>	When you enable this setting, non-administrators can use local machine certificates to connect SSL VPN. When you disable this setting, non-administrators cannot use machine certificates to connect SSL VPN. Boolean value: [0 | 1]	0
<prompt_certificate>	Request a certificate during connection establishment. Boolean value: [0 | 1]	0
<prompt_username>	Request a username during connection establishment. Boolean value: [0 | 1]	1
<fgt>	Indicates whether FortiClient received a VPN configuration from FortiGate or EMS. When this setting is 1, FortiClient received a VPN configuration from FortiGate or EMS, and the user can view the VPN configuration when connected to FortiGate or EMS. If FortiClient is disconnected from FortiGate or EMS after connecting and receiving the VPN configuration, the user can view and delete the VPN configuration but cannot edit it.	

XML tag	Description	Default value
	When this setting is `0`, FortiClient did not receive a VPN configuration from FortiGate or EMS, and the user can view or delete VPN configurations. It is not recommended to manually change the `<fgt>` setting. Boolean value: `[0 | 1]`	
`<splitdns_tcp_enabled>`	 This tag takes effect only when ZTNA is not running. It is ignored when ZTNA is running. • When enabled, DNS over TCP works well in split-tunnel split-dns configuration. • When disabled, DNS requests and responses use UDP. Boolean value: `[0 | 1]`	`1`
`<certificate>` elements The XML sample provided above only shows XML configuration when using a username and password. See Sample XML using certificate authentication for example of XML configuration for certificate authentication.		
`<certificate><common_name>` elements Elements for common name of the certificate for VPN logon.		
`<match_type>`	Enter the type of matching to use: • simple: exact match • wildcard: wildcard • regex: regular expressions	
`<pattern>`	Enter the pattern to use for the type of matching.	
`<certificate><issuer>` elements Elements about the issuer of the certificate for VPN logon.		
`<match_type>`	Enter the type of matching to use: • simple: exact match • wildcard: wildcard	
`<pattern>`	Enter the pattern to use for the type of matching.	
`<oid>` elements Elements about the certificate object identifier (OID). This feature filters based on all certificate OIDs at the first level of the X.509 ASN.1 structure. Nested, or second level OIDs are not supported, other than the EKU (extendedKeyUsage) OIDs.		
`<match_type>`	Enter the type of matching to use. Choose from: • simple: exact match • wildcard: wildcard • regex: regular expressions	

XML tag	Description	Default value
<pattern>	Enter the pattern to use for the type of matching.	
<ui> elements The FortiGate sets the elements of the <ui> XML tag by following an SSL VPN connection.		
<show_remember_password>	Display the *Save Password* checkbox in the console. Boolean value: [0 | 1]	
<show_alwaysup>	Display the *Always Up* checkbox in the console. Boolean value: [0 | 1]	
<show_autoconnect>	Display the *Auto Connect* checkbox in the console. Boolean value: [0 | 1]	
<save_username>	Save and display the last username used for VPN connection. Boolean value: [0 | 1]	
<save_password>	When enabled, *Save Password* is enabled for the VPN tunnel in the FortiClient GUI. An EMS-pushed tunnel with <save_password> enabled displays with *Save Password* enabled and grayed out in the FortiClient GUI. Boolean value: [0 | 1]	0
<traffic_control> elements		
<enabled>	To enable the feature, enter 1. To disable the feature, enter 0. Boolean value: [0 | 1]	
<mode>	Enter 2 so that network traffic for all defined applications and FQDNs do not go through the VPN tunnel. You must configure this value as 2 for the feature to function.	
<app>	Specify which application traffic to exclude from the VPN tunnel and redirect to the endpoint physical interface. You can specify an application using its process name, full path, or the directory where it is installed. You can enter file and directory paths using environment variables, such as %LOCALAPPDATA%,%programfiles%, and %appdata%. Do not use spaces in the tail or head, or add double quotes to full paths with spaces. To find a running application's full path, on the *Details* tab in Task Manager, add the *Image path name* column. Once the VPN tunnel is up, FortiClient binds the specified applications to the physical interface. In the example, for the GoToMeeting path, 18068 refers to the current installed version of the GoToMeeting application.	

XML tag	Description	Default value
<enable_local_lan>	Enable access to local resources while an application-based split tunnel with an exclusion rule configured is up. If this option is disabled, access to local resources may be denied when an application-based split tunnel with an exclusion rule configured is up. Boolean value: [0 | 1]	1
<fqdn>	Specify which FQDN traffic to exclude from the VPN tunnel and redirect to the endpoint physical interface. The FQDN resolved IP address is dynamically added to the route table when in use, and is removed after disconnection. In the example, youtube.com equals youtube.com and *.youtube.com. After defining an FQDN, such as youtube.com in the example, if you use any popular browser such as Chrome, Edge, or Firefox to access youtube.com, this traffic does not go through the VPN tunnel.	
<tags> elements		
<allowed>	Enter the desired Zero Trust tags. If EMS has tagged this endpoint with any of the entered tags, FortiClient allows the endpoint to connect to the VPN tunnel.	
<prohibited>	Enter the desired Zero Trust tags. If EMS has tagged this endpoint with any of the entered tags, FortiClient denies the endpoint from connecting to the VPN tunnel.	
<azure_auto_login> elements		
<enabled>	Enable Azure auto login. When the user logs in to the endpoint using an Azure Active Directory (AD) account, FortiClient silently automatically connects to the VPN tunnel configured in <vpn><options><autoconnect_tunnel>. <sso_enabled> must be enabled for this feature to function correctly. See the EMS Administration Guide for details on configuring this feature. Boolean value: [0 | 1]	
<azure_auto_login><azure_app> elements		
<tenant_name>	Enter the Azure domain name as obtained from the Azure portal.	
<client_id>	Enter the FortiClient application ID as obtained from the Azure portal.	

XML tag	Description	Default value
`<vpn_before_logon><username_format>`	Configure the required username format for the VPN before logon connection to successfully authenticate. This configuration takes effect if the user selects their username from the left panel when logging into Windows instead of typing in their name. Configure one of the following: • `username` • `upn` or `user principal name`. Configure this if the username must be in the format username@domain, such as rpark@fortinet.com. • `dlln` or `down-level logon name`. Configure this if the username must be in the format domain\username, such as fortinet.com/rpark.	username
`<android_app_control>` elements		
`<enabled>`	Enable per-application SSL VPN on FortiClient Android to allow only traffic from specific applications to pass through the SSL VPN tunnel or to prevent traffic from specific applications from passing through the SSL VPN tunnel. Unlike personal per-application VPN tunnels (see Configuring per-application SSL VPN on FortiClient Android) that are listed in a dedicated *PER APP VPN TUNNELS* section in the VPN list, EMS-pushed per-application VPN tunnels are listed under the *CORPORATE VPN TUNNELS* section. For each per-application VPN, the associated allowed apps are displayed under the VPN name. Boolean value: `[0 | 1]`	
`<mode>`	Configure the mode for per-application SSL VPN on FortiClient Android: • 1 - **include**: Only allow traffic from the specified applications to pass through the SSL VPN tunnel. • 2 - **exclude**: All traffic except for the specified applications is able to pass through the VPN tunnel.	

`<apps>`	List the applications to allow or exclude from the SSL VPN tunnel. The following is an example configuration for YouTube application:
	
	`<apps>`
	`<app>com.google.android.youtube</app>`
	`</apps>`	

Sample XML using certificate authentication

```
<sslvpn>
   ...
   <connections>
```

```
        <connection>
           ...
           <certificate>
              <common_name>
                 <match_type>
                    <![CDATA[wildcard]]>
                 </match_type>
                 <pattern>
                    <![CDATA[*]]>
                 </pattern>
              </common_name>
              <issuer>
                 <match_type>
                    <![CDATA[simple]]>
                 </match_type>
                 <pattern>
                    <![CDATA[Certificate Authority]]>
                 </pattern>
              </issuer>
              <oids>
                 <oid>
                    <match_type>simple</match_type>
                    <pattern>
                       <![CDATA[1.3.6.1.5.5.7.3.1]]>
                    </pattern>
                 </oid>
              </oids>
              ...
           </certificate>
        </connection>
     </connections>
     ...
<sslvpn>
```

This is a balanced but incomplete XML configuration fragment. It includes all closing tags, but omits some important elements to complete the configuration.

See the first XML sample in this topic for a more complete XML configuration example using a username and password for authentication.

The <on_connect> and <on_disconnect> tags both have very similar tag structure:

```
   <on_connect>
      <script>
         <os>windows</os>
         <script>
            <script>
               <![CDATA[
               ]]>
            </script>
         </script>
      </script>
   </on_connect>
   <on_disconnect>
      <script>
         <os>windows</os>
         <script>
            <script>
```

```
            <![CDATA[
            ]]>
          </script>
        </script>
      </script>
    </on_disconnect>
```

The following table provides CDATA XML tags, the description, and the default value (where applicable):

XML tag	Description	Default value
<os>	The OS for which the script is written. Enter one of the following: [windows | MacOSX]	
<script>	The MS DOS batch or macOS shell script to run.	
<![CDATA[ ]]>	Wraps the scripts in CDATA elements.	
Write the MS DOS batch or macOS shell script inside the CDATA tag. Write one line per command like a regular batch script file. The script is executed in the context of the user that connected the tunnel. Remember to check your XML file before deploying to ensure that carriage returns/line feeds are present.		

The example scripts above show a script that mounts several network drives after an SSL connection is established. The drives are unmounted with the corresponding scripts in the <on_disconnect> XML tag.

The <on_connect> and <on_disconnect> scripts are optional.

IPsec VPN

FortiClient 7.4.6 does not support IPsec VPN IKEv1. Configure IPsec VPN IKEv2 if using FortiClient 7.4.6.

IPsec VPN configurations have one <options> section and one or more <connection> sections:

```
<forticlient_configuration>
   <vpn>
      <ipsecvpn>
         <options>
            <show_auth_cert_only>1</show_auth_cert_only>
            <disconnect_on_log_off>1</disconnect_on_log_off>
            <enabled>1</enabled>
            <beep_if_error>0</beep_if_error>
            <beep_continuously>0</beep_continuously>
            <beep_seconds>0</beep_seconds>
            <usewincert>1</usewincert>
            <use_win_current_user_cert>1</use_win_current_user_cert>
            <use_win_local_computer_cert>1</use_win_local_computer_cert>
            <block_ipv6>1</block_ipv6>
            <uselocalcert>0</uselocalcert>
            <usesmcardcert>1</usesmcardcert>
            <enable_udp_checksum>0</enable_udp_checksum>
            <mtu_size>1300</mtu_size>
            <disable_default_route>0</disable_default_route>
            <check_for_cert_private_key>1</check_for_cert_private_key>
            <enhanced_key_usage_mandatory>1</enhanced_key_usage_mandatory
            <no_dns_registration>0</no_dns_registration>
            <prefer_ipsecvpn_dns>1</prefer_ipsecvpn_dns>
            <disallow_invalid_server_certificate>1</disallow_invalid_server_certificate>
         </options>
         <connections>
            <connection>
               <name>ipsecdemo</name>
               <single_user_mode>0</single_user_mode>
               <type>manual</type>
               <disclaimer_msg></disclaimer_msg>
               <redundant_sort_method>0</redundant_sort_method>
               <failover_sslvpn_connection>SSLVPN_Name</failover_sslvpn_connection>
               <machine>0</machine>
               <keep_running>0</keep_running>
               <android_cert_path>certdir/</android_cert_path>
               <pinned>1</pinned>
               <allow_concurrent>1</allow_concurrent>
               <dns_priority>3</dns_priority>
               <traffic_keep_strategy>0</traffic_keep_strategy>
               <traffic_keep_timer>5000</traffic_keep_timer>
               <resolve_to_ipv4_only>0</resolve_to_ipv4_only>
               <ui>
                  <show_passcode>0</show_passcode>
                  <show_remember_password>1</show_remember_password>
```

```
      <show_alwaysup>1</show_alwaysup>
      <show_autoconnect>1</show_autoconnect>
      <save_username>0</save_username>
      <save_password>0</save_password>
   </ui>
   <ike_settings>
      <version>1</version>
      <prompt_certificate>0</prompt_certificate>
      <implied_SPDO>0</implied_SPDO>
      <implied_SPDO_timeout>60</implied_SPDO_timeout>
      <server>ipsecdemo.fortinet.com</server>
      <authentication_method>Preshared Key</authentication_method>
      <cert_subjectcheck>0</cert_subjectcheck>
      <auth_data>
         <preshared_
               key>Encdab907ed117eafaadd92f82b3e768b5414e4402dbd4df4585d4202c65940f1b2e9<
               /preshared_key>
      </auth_key>
      <mode>aggressive</mode>
      <dhgroup>5;</dhgroup>
      <key_life>28800</key_life>
      <localid></localid>
      <nat_traversal>1</nat_traversal>
      <sase_mode>1</sase_mode>
      <mode_config>1</mode_config>
         <modeconfig_type>0<modeconfig_type>
      <enable_local_lan>0</enable_local_lan>
      <block_outside_dns>0</block_outside_dns>
      <nat_alive_freq>10</nat_alive_freq>
      <dpd>1</dpd>
      <dpd_retry_count>3</dpd_retry_count>
      <dpd_retry_interval>20</dpd_retry_interval>
      <fgt>1</fgt>
      <enable_ike_fragmentation>1</enable_ike_fragmentation>
      <run_fcauth_system>0</run_fcauth_system>
      <sso_enabled>1</sso_enabled>
      <use_external_browser>0</use_external_browser>
      <ike_saml_port>10428</ike_saml_port>
      <failover_sslvpn_connection>SSLVPN HQ</failover_sslvpn_connection>
      <xauth_timeout>120</xauth_timeout>
      <session_resume>0</session_resume>
      <networkid>0</networkid>
      <eap_method>1</eap_method>
      <remove_password_for_unexpected_eap_failure>0</remove_password_for_unexpected_eap_
            failure>
      <fido_auth>1</fido_auth>
      <saml_cert_selection>1</saml_cert_selection>
      <transport_mode>0</transport_mode>
      <udp_port>5000</udp_port>
      <keep_fqdn_resolution_consistency>1</keep_fqdn_resolution_consistency>
      <no_vnic_dns_server>0</no_vnic_dns_server>
      <xauth>
         <enabled>1</enabled>
         <prsompt_username>1</prompt_username>
         <username>Encrypted/NonEncrypted_UsernameString</username>
         <password />
         <attempts_allowed>1</attempts_allowed>
```

```
            </xauth>
            <proposals>
               <proposal>3DES|MD5</proposal>
               <proposal>3DES|SHA1</proposal>
               <proposal>AES128|MD5</proposal>
               <proposal>AES128|SHA1</proposal>
               <proposal>AES256|SHA256</proposal>
            </proposals>
            <azure_auto_login>
               <enabled>1</enabled>
               <azure_app>
                  <client_id>...</client_id>
                  <tenant_name>...</tenant_name>
               </azure_app>
            </azure_auto_login>
         </ike_settings>
         <ipsec_settings>
            <remote_networks>
               <network>
                  <addr>0.0.0.0</addr>
                  <mask>0.0.0.0</mask>
               </network>
            </remote_networks>
            <ipv4_split_exclude_networks>
               <subnetwork>10.10.10.0/255.255.255.0</subnetwork>
               <subnetwork>13.106.56.0/25</subnetwork>
               <subnetwork>teams.microsoft.com</subnetwork>
            </ipv4_split_exclude_networks>
            <dhgroup>5</dhgroup>
            <key_life_type>seconds</key_life_type>
            <key_life_seconds>1800</key_life_seconds>
            <key_life_Kbytes>5120</key_life_Kbytes>
            <replay_detection>1</replay_detection>
            <pfs>1</pfs>
            <use_vip>1</use_vip>
            <virtualip>
               <dnsserver_secondary></dnsserver_secondary>
               <!-- server IP address -->
               <type>modeconfig</type>
               <ip>0.0.0.0</ip>
               <mask>0.0.0.0</mask>
               <dnsserver>0.0.0.0</dnsserver>
               <winserver>0.0.0.0</winserver>
            </virtualip>
            <proposals>
               <proposal>3DES|MD5</proposal>
               <proposal>3DES|SHA1</proposal>
               <proposal>AES128|MD5</proposal>
               <proposal>AES128|SHA1</proposal>
               <proposal>AES256|SHA256</proposal>
            </proposals>
            <dns_suffix_list>vpn.example.com,sub.vpn.example.com,vp2.example.com</dns_suffix_
                  list>
         </ipsec_settings>
         <on_connect>
            <script>
               <os>windows</os>
```

```
                  <script>
                     <![CDATA[]]>
                  </script>
               </script>
            </on_connect>
            <on_disconnect>
            <script>
               <os>windows</os>
               <script>
                  <script>
                     <![CDATA[]]>
                  </script>
               </script>
            </script>
            </on_disconnect>
            <traffic_control>
               <enabled>1</enabled>
               <mode>2</mode>
               <apps>
                  <app>%LOCALAPPDATA%\Microsoft\Teams\Current\Teams.exe</app>
                  <app>%appdata%\Zoom\bin\Zoom.exe</app>
                  <app>C:\Program Files (x86)\Microsoft\Skype for Desktop\skype.exe</app>
                  <app>%LOCALAPPDATA%\GoToMeeting\18068\g2mcomm.exe</app>
                  <app>%LOCALAPPDATA%\GoToMeeting\18068\g2mlauncher.exe</app>
                  <app>%LOCALAPPDATA%\GoToMeeting\18068\g2mstart.exe</app>
               </apps>
               <fqdns>
                  <fqdn>webex.com</fqdn>
                  <fqdn>gotomeeting.com</fqdn>
                  <fqdn>youtube.com</fqdn>
               </fqdns>
            </traffic_control>
            <tags>
               <allowed>NoVuln</allowed>
               <prohibited>CriticalVuln</prohibited>
            </tags>
            <vpn_before_logon>
               <username_format>username</username_format>
            <vpn_before_logon/>
         </connection>
      </connections>
   </ipsecvpn>
</vpn>
</forticlient_configuration>
```

The following table provides the XML tags for IPsec VPN, as well as the descriptions and default values where applicable:

XML tag	Description	Default value
`<ipsecvpn> <options>` elements		
`<show_auth_cert_only>`	Suppress dialogs from displaying in FortiClient when using SmartCard certificates. Boolean value: `[0 | 1]`	`0`

XML tag	Description	Default value
<disconnect_on_log_off>	Drop the established VPN connection when the user logs off. Boolean value: [0 | 1]	1
<enabled>	Enable IPsec VPN. Boolean value: [0 | 1]	1
<beep_if_error>	Beep if VPN connection attempt fails. Boolean value: [0 | 1]	0
<beep_continuously>	Enable continuous beep. Boolean value: [0 | 1]	1
<beep_seconds>	Enter a value for the number of seconds after which to beep if an error occurs.	60
<usewincert>	Use Windows certificates for connections. Boolean value: [0 | 1]	
<use_win_current_user_cert>	Use Windows current user certificates for connections. Boolean value: [0 | 1]	1
<use_win_local_computer_cert>	Use Windows local computer certificates for connections. Boolean value: [0 | 1]	1
<block_ipv6>	Block IPv6 traffic sent outside of VPN interface when connected to an IPv4 full tunnel. This option does not support the following: • FortiClient (Linux) • FortiClient 7.4.4 and 7.4.6 (due to lack of IPv6 support for IPsec VPN) Boolean value: [0 | 1]	0
<uselocalcert>	Use local certificates for connections. Boolean value: [0 | 1]	
<usesmcardcert>	Use certificates on smart cards. Boolean value: [0 | 1]	
<enable_udp_checksums>	Enable UDP checksums. This setting stops FortiClient from calculating and inserting checksums into the UDP packets that it creates. Boolean value: [0 | 1]	0
<mtu_size>	Maximum transmit unit (MTU) size for packets on IPsec VPN tunnels. Set from a minimum of 576 to a maximum of 1500 bytes.	1280
<disable_default_route>	Disable the default route to the gateway when the tunnel is up and restore after the tunnel is down.	0

XML tag	Description	Default value
	Boolean value: `[0 | 1]`	
`<check_for_cert_private_key>`	Enable checks for the Windows certificate private key. Boolean value: `[0 | 1]`	`0`
`<enhanced_key_usage_mandatory>`	Enable certificates with enhanced key usage. Used with `<check_for_cert_private_key>`. When you enable `<check_for_cert_private_key>` and `<enhanced_key_usage_manadatory>`, FortiClient only lists certificates with enhanced key usage. Boolean value: `[0 | 1]`	
`<no_dns_registration>`	When this setting is `0`, FortiClient registers the IPsec VPN adapter's address in the Active Directory (AD) DNS server. When this setting is `1`, FortiClient does not register the IPsec VPN adapter's address in the AD DNS server. When this setting is `2`, FortiClient registers only its own tunnel interface IP address in the AD DNS server.	`0`
`<prefer_ipsecvpn_dns>`	When enabled (default), FortiClient pushes the DNS server entries configured on the FortiOS side onto the physical adapter of the endpoint. When disabled, FortiClient does not apply the DNS servers from the IPsec tunnel to the physical adapter. Boolean value: `[0 | 1]`	`1`

`<disallow_invalid_server_certificate>`	When you disable this setting and an invalid server certificate is used, FortiClient displays a popup that allows the user to continue with the invalid certificate.
	When you enable this setting and an invalid server certificate is used, FortiClient does not display a popup and stops the connection.
	This setting checks the certificate used for SAML authentication that FortiOS, in the role of the SAML service provider, presents to FortiClient. On FortiOS, this certificate is configured under the following command:
	`config user setting`
	`set auth-cert "<certificate>"`
	`end`
	Boolean value: `[0 | 1]`	

The `<connections>` XML tag may contain one or more `<connection>` element. Each `<connection>` has the following:

- name and type: name and type of connection
- Internet Key Exchange (IKE) settings: information used to establish an IPsec VPN connection

- IPsec settings:
  - on_connect: a script to run right after a successful connection
  - on_disconnect: a script to run just after a disconnection

The following table provides VPN connection XML tags, the description, and the default value (where applicable):

XML tag	Description	Default Value
`<name>`	VPN connection name.	
`<single_user_mode>`	Enable single user mode. If enabled, new and existing VPN connections cannot be established or are disconnected if more than one user is logged in. Boolean value: `[0 | 1]`	`0`
`<type>`	IPsec VPN connection type. Enter one of the following: `[manual | auto]`	
`<disclaimer_msg>`	Enable and enter a disclaimer message that appears when the user attempts VPN connection. The user must accept the message to allow connection.	
`<redundant_sort_method>`	How FortiClient determines the order in which to try connection to the IPsec VPN servers when more than one is defined. FortiClient calculates the order before each IPsec VPN connection attempt. • When the value is `0`, FortiClient tries the order explicitly defined in the `<server>` tag. • When the value is `1`, FortiClient determines the order by the ping response speed. • When the value is `2`, FortiClient determines the order by the TCP round trip time.	`0`
`<failover_sslvpn_connection>`	If the IPsec VPN connection fails, FortiClient attempts to connect to the specified SSL VPN tunnel.	
`<machine>`	When this setting is 1, FortiClient can connect to the tunnel without user interaction. See `<on_os_start_connect>` in VPN options on page 38. Boolean value: `[0 | 1]`	
`<keep_running>`	Ensures that the VPN tunnel remains connected if it is already connected. This is useful when there is a temporary network disconnection that causes the tunnel to drop the connection. An EMS-pushed tunnel with `<keep_running>` enabled displays with *Save Password* and *Always Up* enabled and grayed out in the FortiClient GUI. Boolean value: `[0 | 1]`	0
`<android_cert_path>`	Configure a certificate location for FortiClient (Android) to automatically go to when doing the following:	

XML tag	Description	Default Value
	• When selecting a certificate • When the user clicks *Connect* to connect to this tunnel See Certificate path configuration for automated certificate selection.	
`<pinned>`	Indicates that a tunnel has been selected by the EMS configuration. When a tunnel is pinned, you cannot manually unpin it from the FortiClient GUI. If a tunnel is not pinned, you can select or deselect it. All pinned tunnels display in the *Remote Access* tab in FortiClient. The EMS administrator can pin a maximum of three tunnels per profile. The end user may pin an additional tunnel in FortiClient. FortiClient therefore supports pinning a maximum of four tunnels. Boolean value: `[0 | 1]`	
`<allow_concurrent>`	Specify whether the IPsec VPN IKEv2 tunnel supports concurrent connections. This setting is relevant only when `<enable_multi_vpn>` is enabled. Boolean value: `[0 | 1]`	
`<dns_priority>`	Enter an integer between 1 to 255. When FortiClient is connected to concurrent IPsec VPN IKEv2 tunnels, it connects to the DNS server for the IPsec VPN IKEv2 tunnel with the lowest `<dns_priority>` value. This setting is relevant only when `<enable_multi_vpn>` is enabled.	
`<traffic_keep_strategy>`	Configure the traffic strategy: • **0**—Keep traffic in tunnel with route change to preserve the route's metric. • **1**—Flush DNS, which may help resolve issues with accessing local services via DNS. • **2**—No change to the traffic.	`0`
`<traffic_keep_timer>`	Configure the interval (in milliseconds) for route change or DNS flush. The minimum is 3000. If you specify a value below 3000, FortiClient will use 3000 instead. No maximum is enforced.	`5000`
`<resolve_to_ipv4_only>`	Enable this option to disable the use of IPv6 on the FortiClient. Boolean value: `[0 | 1]`	`0`
`<ui>` elements The elements of the `<ui></ui>` XML tags are set by the FortiGate following an IPsec VPN connection.		

XML tag	Description	Default Value
<show_passcode>	Display *Passcode* instead of *Password* on the *Remote Access* tab in the console. Boolean value: [0 | 1]	
<show_remember_password>	Display the *Save Password* checkbox in the console. Boolean value: [0 | 1]	
<show_alwaysup>	Display the *Always Up* checkbox in the console. Boolean value: [0 | 1]	
<show_autoconnect>	Display the *Auto Connect* checkbox in the console. Boolean value: [0 | 1]	
<save_username>	Save and display the last username used for VPN connection. Boolean value: [0 | 1]	
<save_password>	When enabled, *Save Password* is enabled for the VPN tunnel in the FortiClient GUI. An EMS-pushed tunnel with <save_password> enabled displays with *Save Password* enabled and grayed out in the FortiClient GUI. Boolean value: [0 | 1]	0
<ipsec_settings> elements		
(Windows only) <dns_suffix_list>	This tag depends on <prefer_ipsecvpn_dns>. • When <prefer_ipsecvpn_dns> = 1 (enabled), all entries in <dns_suffix_list> are appended to the global DNS suffix search list. Windows will try the suffixes in the configured order until one resolves. If both FortiOS and EMS provide suffix lists, the FortiOS list takes precedence. For example, if FortiOS is configured as `set dns-suffix-search "fortinet.com" "google.com"` and EMS is configured as <dns_suffix_list>google.com,fortinet.com</dns_suffix_list>, an unqualified query like mail resolves first as `mail.fortinet.com` because the FortiOS order takes precedence. Windows appends suffixes in order until a reply is received. For example, for drive, Windows first tries `drive.fortinet.com`, then `drive.google.com`, stopping at the first success. • When <prefer_ipsecvpn_dns> = 0 (disabled), only one suffix is supported. That single entry is applied as the connection-specific DNS suffix on the IKEv2 virtual adapter. Additional entries, if present, are ignored.	1
<traffic_control> elements		
<enabled>	To enable the feature, enter 1. To disable the feature, enter 0.	

XML tag	Description	Default Value
	Boolean value: `[0 | 1]`	
`<mode>`	Enter `2` so that network traffic for all defined applications and FQDNs do not go through the VPN tunnel. You must configure this value as `2` for the feature to function.	
`<app>`	Specify which application traffic to exclude from the VPN tunnel and redirect to the endpoint physical interface. You can specify an application using its process name, full path, or the directory where it is installed. You can enter file and directory paths using environment variables, such as %LOCALAPPDATA%,%programfiles%, and %appdata%. Do not use spaces in the tail or head, or add double quotes to full paths with spaces. To find a running application's full path, on the *Details* tab in Task Manager, add the *Image path name* column. Once the VPN tunnel is up, FortiClient binds the specified applications to the physical interface. In the example, for the GoToMeeting path, 18068 refers to the current installed version of the GoToMeeting application.	
`<fqdn>`	Specify which FQDN traffic to exclude from the VPN tunnel and redirect to the endpoint physical interface. The FQDN resolved IP address is dynamically added to the route table when in use, and is removed after disconnection. In the example, youtube.com equals youtube.com and *.youtube.com. After defining an FQDN, such as youtube.com in the example, if you use any popular browser such as Chrome, Edge, or Firefox to access youtube.com, this traffic does not go through the VPN tunnel.	
`<tags>` elements		
`<allowed>`	Enter the desired security posture tags. If EMS has tagged this endpoint with any of the entered tags, FortiClient allows the endpoint to connect to the VPN tunnel.	
`<prohibited>`	Enter the desired security posture tags. If EMS has tagged this endpoint with any of the entered tags, FortiClient denies the endpoint from connecting to the VPN tunnel.	
`<vpn_before_logon><username_format>`	Configure the required username format for the VPN before logon connection to successfully authenticate. This configuration takes effect if the user selects their username from the left panel when logging into Windows instead of typing in their name. Configure one of the following: • `username` • `upn` or `user principal name`. Configure this if the	username

XML tag	Description	Default Value
	username must be in the format username@domain, such as rpark@fortinet.com. • `dlln` or `down-level logon name`. Configure this if the username must be in the format domain\username, such as fortinet.com/rpark.	

The VPN connection name is mandatory. If a connection of this type and this name exists, FortiClient overwrites its values with the new ones.

IKE settings

FortiClient 7.4.6 does not support IPsec VPN IKEv1. Configure IPsec VPN IKEv2 if using FortiClient 7.4.6.

FortiClient automatically performs IKE based on preshared keys or X.509 digital certificates.

The following table provides the XML tags for IKE settings, as well as the descriptions and default values where applicable:

XML tag	Description	Default value
`<version>`	Determine the IKE version. FortiClient supports IKE v1 and IKE v2. Enter `1` or `2`.	`1`
`<prompt_certificate>`	Prompt for certificate on connection. Boolean value: `[0 | 1]`	`1`
`<implied_SPDO>`	Specify which ports allow traffic. When this setting is `0`, FortiClient only allows traffic from ports 500 and 4500. When this setting is `1`, FortiClient allows other traffic during the connection phase, including Internet traffic. Boolean value: `[0 | 1]`	`0`
`<implied_SPDO_timeout>`	When `<implied_SPDO>` is set to `1`, `<implied_SPDO_timeout>` is the timeout in seconds. FortiClient blocks all outbound non-IKE packets when `<implied_SPDO>` is set to `1`. This is a security feature in the IPsec protocol. If the network traffic goes through a captive portal, the intended IPsec VPN server may be unreachable, until the user provides some credentials on a web page. Thus, setting `<implied_SPDO>` to `1` may have the side effect of blocking access to the captive portal, which in turn blocks access to the IPsec VPN server.	`60`

XML tag	Description	Default value
	To avoid this deadlock, set <implied_SPDO_timeout> to a value greater than 0. FortiClient allows all outbound traffic (including non-IKE traffic) for the duration configured. Some users find that a value of 30 or 60 seconds suffices. If <implied_SPDO_timeout> is set to 0, the <implied_SPDO> element behaves as if set to 0. When <implied_SPDO> is set to 0, <implied_SPDO_timeout> is ignored.	
<server>	IP address or FQDN.	
<authentication_method>	Authentication method. Enter one of the following: • Preshared Key • X509 Certificate • Smartcard X509 Certificate • System Store X509 Certificate	

<cert_subjectcheck>	When enabled, if the CN type of the server certificate is FQDN (see FortiOS documentation), FortiClient validates the remote gateway hostname to match the CN in the subject field of the server certificate of the IPsec phase1 interface, which is configured on the FortiGate under the following command:
	`config vpn ipsec phase1-interface`
	`edit "<interface>"`
	`set authmethod signature`
	`set certificate "<certificate>"`
	`next`
	`end`
	If there is no match, the VPN connection does not succeed.
	Boolean value: [0 | 1]
		0

<auth_data> elements		
<preshared_key>	Encrypted value of the preshared key.	
<auth_data><certificate> elements FortiClient searches all certificate stores until it finds a match for the certificate name and issuer supplied. The XML sample provided in IPsec VPN on page 60 only shows XML configuration when using a preshared key. See Sample XML using certificate authentication for example of XML configuration for a System Store X509 certificate.		
<auth_data><certificate><common_name> elements Elements for common name of the certificate for VPN logon.		
<match_type>	Enter the type of matching to use: • simple: exact match	

XML tag	Description	Default value
	• wildcard: wildcard • regex: regular expressions	
`<pattern>`	Enter the pattern to use for the type of matching.	
`<auth_data><certificate><issuer>` elements		
`<match_type>`	Enter the type of matching to use: • simple: exact match • wildcard: wildcard	
`<pattern>`	Enter the pattern to use for the type of matching.	
`<auth_data><certificate><oids><oid>` elements Elements about the certificate object identifier (OID). This feature filters based on all certificate OIDs at the first level of the X.509 ASN.1 structure. Nested, or second level OIDs are not supported, other than the EKU (extendedKeyUsage) OIDs.		
`<match_type>`	Enter the type of matching to use. Choose from: • simple: exact match • wildcard: wildcard • regex: regular expressions	
`<pattern>`	Enter the pattern to use for the type of matching.	
`<mode>`	Connection mode. Enter one of the following: `[aggressive | main]`	
`<dhgroup>`	A list of possible Diffie-Hellman (DH) protocol groups, separated by semicolons.	
`<key_life>`	Phase 2 key expiry duration, in seconds.	`28800`
`<localid>`	Enter the peer ID configured in the FortiGate phase 1 configuration. If *Accept any peer ID* has been configured, leave this field blank.	
`<peerid>`	Enter the FortiGate certificate subject name or FQDN. The peer ID must match the certificate local ID on the FortiGate for a successful IPsec VPN connection.	
`<nat_traversal>`	Enable NAT traversal. Boolean value: `[0 | 1]`	
`<sase_mode>`	When enabled, the IPsec VPN forces the new connection port (including the first message) to use port 4500. All traffic that goes through this IPsec VPN tunnel is seen on port 4500. IKE_SA_INIT also has the EMS serial number as its payload. You must enable this feature to provide IPsec VPN-based SASE. For this feature to function correctly, you must configure the following on the FortiGate:	`0`

XML tag	Description	Default value

	`config system settings`
	`set ike-port 4500`
	`end`
	This feature only supports IKEv2 and requires NAT traversal to be enabled.
	Boolean value: `[0 | 1]`	

`<mode_config>`	Enable mode configuration. Boolean value: `[0 | 1]`	
`<modeconfig_type>`	Select the mode configuration type: • 0 - IPv4 only (default) • 1 - IPv6 only • 2 - IPv4 & IPv6 dual stack This setting must match the FortiOS *Mode config* setting.	
`<enable_local_lan>`	Enable local LAN when using a full tunnel. This setting does not apply to split tunnels. Boolean value: `[0 | 1]`	`0`
`<block_outside_dns>`	When you enable this setting, Windows uses only the VPN-pushed DNS server when using a full tunnel. When you disable this setting, FortiClient retains the outside DNS server configuration when the tunnel is up. Boolean value: `[0 | 1]`	`0`
`<nat_alive_freq>`	NAT alive frequency. The minimum (and default) is 10.	`10`
`<dpd>`	Enable dead peer detection (DPD). Boolean value: `[0 | 1]`	`1`
`<dpd_retry_count>`	Number of times to send unacknowledged DPD messages before declaring peer as dead. Maximum value is 10. If the specified value is greater than the maximum (10), FortiClient uses the maximum value (10) instead.	`3`
`<dpd_retry_interval>`	Duration of DPD idle periods, in seconds. Maximum value is 3600. If the specified value is greater than the maximum (3600), FortiClient uses the maximum value (3600) instead.	`20`
`<enable_ike_fragmentation>`	Enable support of fragmented IKE packets to avoid packet loss and ensure reliable IPsec VPN tunnel establishment. See the following for more details: • IKE fragmentation example on page 81 • *IKEv1 fragmentation* and *IKEv2 fragmentation* sections in FortiOS documentation for more details. Boolean value: `[0 | 1]`	`1`

XML tag	Description	Default value
<run_fcauth_system>	When you enable this setting, non-administrators can use local machine certificates to connect IPsec VPN. When you disable this setting, non-administrators cannot use machine certificates to connect IPsec VPN. Boolean value: [0 | 1]	0
<sso_enabled>	Enable SAML single sign on (SSO) login for the VPN tunnel. For this feature to function, the administrator must configure the necessary options on the service and identity providers. See IPsec VPN SAML-based authentication. Boolean value: [0 | 1]	
<use_external_browser>	Display the SAML authentication prompt in an external browser instead of in the FortiClient GUI. If you configure <version> as 2 and <sso_enabled> as 1, FortiClient automatically enables this field. Only IKEv2 tunnels support using an external browser for IPsec VPN. Boolean value: [0 | 1]	1
<ike_saml_port>	Enter the port number that FortiClient uses to communicate with the FortiGate, which acts as the SAML service provider.	
<failover_sslvpn_connection>	If the IPsec VPN connection fails, FortiClient attempts to connect to the specified SSL VPN tunnel. In the example, the SSL VPN tunnel name is "SSL VPN HQ".	
<xauth_timeout>	Configure the IKE extended authentication (XAuth) timeout in seconds. Enter a value between 120 and 300 seconds.	120
<session_resume>	Enable session resumption. If FortiClient loses the network connection or the client device goes to sleep, the FortiGate starts a client-resume sleep period. When the network connectivity is restored or the device wakes, FortiClient attempts to resume the session. If FortiClient resumes the session within the set interval, the FortiGate detects that the client has resumed and maintains the existing session. The FortiOS administrator configures the interval using set client-resume-interval. If FortiClient does not resume the session within the set interval, the session expires on the FortiGate and the tunnel is deleted. FortiClient must initiate a new full IKEv2 negotiation for reconnection. Boolean value: [0 | 1]	0
<networkid>	Configure a network ID value between 0 to 255 to differentiate between multiple IKEv2 certificate-based phase 1 tunnels. See FortiOS documentation for more details.	

XML tag	Description	Default value
	The network ID is a Fortinet proprietary attribute used to select the correct phase 1 between IPsec peers, so that multiple IKEv2 tunnels can be established between the same local and remote gateway pairs. In a dialup VPN, network-id is in the first initiator message of an IKEv2 phase 1 negotiation. The responder (hub) uses the network-id to match a phase 1 configuration with a matching network-id. The hub can then differentiate multiple dialup phase 1s that are bound to the same underlay interface and IP address. Without a network-id, the hub cannot have multiple phase 1 dialup tunnels on the same interface. In static phase 1 configurations, network-id is used with the pair of gateway IP addresses to negotiate the correct tunnel with a matching network-id. This allows IPsec VPN peers to use the same pair of underlay IP addresses to establish multiple IPsec VPN tunnels. Without it, only a single tunnel can be established over the same pair of underlay IP addresses. The `<networkid>` option is not supported on FortiClient iOS or Android.	
`<eap_method>`	Configure one of the following for the EAP method: • `1`: requires EAP-MSCHAPv2 authentication • `2`: requires EAP-TTLS/PAP authentication For LDAP-based user authentication using IKEv2, the EAP-TTLS authentication method allows credentials to be securely transmitted to FortiGate over a TLS tunnel and ensures secure user authentication. FortiClient (iOS) and (Android) do not support EAP-TTLS/PAP authentication.	`1`
`<remove_password_for_unexpected_eap_failure>`	Configure whether to remove the old saved password when FortiClient does not receive the expected “expiring due to EAP failure” message. Boolean value: `[0 | 1]`	`0`
`<fido_auth>`	Enable to allow Yubikey (FIDO2) authentication for SAML SSO VPN connections in the FortiClient embedded (internal) browser for macOS. Boolean value: `[0 | 1]`	`<fido_auth>`
`<saml_cert_selection>`	Enable to allow certificate selection for identity provider client certificate challenge. If you disable this setting, the FortiClient internal browser allows the system to select the default option for the client certificate challenge.	`0`

XML tag	Description	Default value
	This setting only applies to FortiClient (macOS). Boolean value: `[0 | 1]`	

`<transport_mode>`	Configure the desired transport mode for this connection. Possible values are:
	• `0`: UDP transport mode. This is the default and used for most VPN connections. Configure a custom port number if desired. If you select this option, you only need to configure `<udp_port>` and do not need to configure `<tcp_port>`. The value for `<udp_port>` should match the port number configured on FortiOS via the following command:
	`config system settings`
	`set ike-port 500`
	`end`
	After IKE packets are negotiated over UDP on the configured port, if no NAT is detected and ESP packets are allowed to pass through the internet, ESP packets do not need to be encapsulated inside UDP headers. In this scenario, the recommended setting on FortiOS is `set nattraversal disable`, as disabling NAT-T avoids the additional overhead of encapsulating and decapsulating ESP packets. This typically provides optimal VPN performance on the endpoint and FortiGate when NAT-T is unneeded.
	If NAT is detected and you prefer NAT-T with ESP encapsulation over UDP, consider using auto mode, `<transport_mode>2</transport_mode>` as the following describes. In auto mode, once the IKE negotiation completes, ESP packets are transferred over UDP on the default port (UDP/4500).
	• `1`: TCP transport mode. This is recommended for use in restrictive networks. Configure a custom port number if desired. If you select this mode, you only need to configure `<tcp_port>` and do not need to configure `udp_port`. The value for `<tcp_port>` should match the port number configured on FortiOS via the following command:
	`config system settings`
	`set ike-tcp-port 443`
	`end`
	Use this mode when NAT is detected or if both UDP and ESP are blocked. In this scenario, IKE and ESP packets are encapsulated inside TCP, typically on port 443, to ensure the traffic can pass through strict network environments.
	• `2`: Auto mode. FortiOS dynamically selects the transport mode. If you configure auto mode, you must configure
		`0`

XML tag	Description	Default value

	both the udp_port and <tcp_port> fields. The values must match those set on FortiOS using the following commands:
	`config system settings`
	`set ike-port 500`
	`set ike-tcp-port 443`
	`end`
	You must also configure the following phase 1 settings on FortiOS 7.4.2 and later versions:
	`config vpn ipsec phase1`
	`edit`
	`set nattraversal forced`
	`set transport udp-fallback-tcp`
	`next`
	`end`
	On FortiOS 7.6, you can configure the following phase 1 settings:
	`config vpn ipsec phase1`
	`edit`
	`set nattraversal forced`
	`set transport auto`
	`next`
	`end`
	If using FortiOS 7.4.1 or an earlier version, FortiClient will connect to IPsec VPN using UDP mode as udp-fallback-tcp and auto are unavailable.
	This mode dynamically uses UDP or TCP based on network conditions and NAT detection, automatically falling back to TCP/443 if UDP or ESP traffic is blocked.	

<udp_port>	If <transport_mode> is configured as 0 or 2, configure a custom port for UDP. If <udp_port> is not configured, the default port is used.	
<tcp_port>	If <transport_mode> is configured as 1 or 2, configure a custom port for UDP. If this element is not configured, the default port is used.	
<keep_fqdn_resolution_consistency>	Keep IPsec VPN connection gateway IP address consistent by keeping resolved FQDN in hosts file before FortiClient establishes IPsec VPN connection. Boolean value: [0 | 1]	0

XML tag	Description	Default value
<no_vnic_dns_server>	When enabled, FortiClient does not apply a DNS server to the IKEv2 full-tunnel VPN's virtual adapter. Instead, it sets the VPN adapter's DNS to 0.0.0.0, forcing Windows to immediately fall back to the DNS server on the physical interface. This avoids cases where the VPN-assigned DNS matches the physical adapter's DNS, causing Windows to route queries into the tunnel and wait for timeouts when that server is unreachable through the VPN. It also ensures DNS lookups resolve normally without delay, providing faster and more reliable name resolution while connected to the VPN. Boolean value: [0 | 1]	0
<xauth> elements		
<enabled>	Enable IKE XAuth. Boolean value: [0 | 1]	
<prompt_username>	Request a username. Boolean value: [0 | 1]	
<username>	Encrypted or non-encrypted username on the IPsec server.	
<password>	Encrypted or non-encrypted password.	
<attempts_allowed>	Maximum number of failed login attempts allowed.	
<proposals> elements		
<proposal>	Encryption and authentication types to use, separated by a pipe. Example: <proposal>3DES|MD5<proposal> Multiple elements accepted. First setting: Encryption type: DES, 3DES, AES128, AES192, AES256 Second setting: Authentication type: MD5, SHA1, SHA256, SHA384, SHA512	
<azure_auto_login> elements		
<enabled>	Enable FortiClient to autoconnect to this IPsec VPN tunnel on a Microsoft Entra ID domain-joined endpoint using the Entra ID credentials. See Autoconnect to IPsec VPN using Entra ID logon session information. Boolean value: [0 | 1]	
<azure_app><client_id>	Enter the Entra ID enterprise application client ID. You can find this information on the Entra ID portal.	
<azure_app><tenant_name>	Enter the Azure tenant ID. You can find this information on the Entra ID portal.	

Sample XML using certificate authentication

```
<ipsecvpn>
   ...
   <connections>
      <connection>
         ...
         <ike_settings>
            <auth_data>
               <certificate>
                  <common_name>
                     <match_type>
                        <![CDATA[wildcard]]>
                     </match_type>
                     <pattern>
                        <![CDATA[*]]>
                     </pattern>
                  </common_name>
                  <issuer>
                     <match_type>
                        <![CDATA[simple]]>
                     </match_type>
                     <pattern>
                        <![CDATA[Certificate Authority]]>
                     </pattern>
                  </issuer>
               </certificate>
            </auth_data>
         </ike_settings>
         ...
      </connection>
   </connections>
   ...
</ipsecvpn>
```

This is a balanced but incomplete XML configuration fragment. It includes all closing tags, but omits some important elements to complete the configuration.

See IPsec VPN on page 60 for a more complete XML configuration example using a preshared key for authentication.

IPsec settings

The following table provides the XML tags for IPsec settings, as well as the descriptions and default values where applicable.

XML tag	Description	Default value
`<remote_networks>` elements		
`<network>`	Specifies a network address `<addr>` with subnet mask `<mask>`.	
`<addr>`	Network IP address.	

XML tag	Description	Default value
<mask>	Subnet mask to apply to network address <addr>.	
<ipv4_split_exclude_networks>	Configure negative split tunnel or network exclusion for IPsec VPN using the <subnetwork> subelement. This feature supports FQDN, resolved from the client and expanded into a list of networks. If negative split tunnel configuration is also received from FortiOS, FortiClient uses the settings from FortiOS and ignores the <ipv4_split_exclude_networks> settings. See Configure VPN remote gateway.	
<dhgroup>	A list of possible DH protocol groups, separated by semicolons.	
<key_life_type>	Phase 2 key re-key duration type. Select one of the following: • seconds • kbytes • both	
<key_life_seconds>	Phase 2 key maximum life in seconds.	1800
<key_life_Kbytes>	Phase 2 key maximum life in KB.	5120
<replay_detection>	Detect an attempt to replay a previous VPN session.	
<pfs>	Enable perfect forward secrecy (PFS). Boolean value: [0 | 1]	
<use_vip>	Use a virtual IP address. Boolean value: [0 | 1]	
<virtualip> elements		
<type>	Enter the virtual IP address type: [modeconfig | dhcpoveripsec]	
<ip>	Enter the IP address.	
<mask>	Enter the Network mask.	
<dnsserver>	Enter the DNS server IP address.	
<dnsserver_secondary>	Enter the secondary DNS server IP address.	
<winserver>	Enter the Windows server IP address.	
<proposals> elements		
<proposal>	Encryption and authentication types to use, separated by a pipe. Example: <proposal>3DES|MD5<proposal> Multiple elements accepted. First setting: Encryption type: DES, 3DES, AES128, AES192, AES256, AES128GCM, AES 256GCM Second setting: Authentication type: MD5, SHA1, SHA256, SHA384, SHA512, PRF SHA1, PRF SHA256, PRF SHA384, PRF SHA512	

The `on_connect` and `on_disconnect` structure and scripting format are similar to those described in SSL VPN on page 46.

IKE fragmentation example

This section provides an example of a non-default IPsec VPN configuration. You can use this configuration if FortiClient fails to connect to IPsec VPN and you see the following symptoms:

- When you view the FortiGate IKE and FortiClient debug logs, they show that FortiClient fails at phase-1.
- Packet capture shows that FortiGate sends some IKE packets with a packet length that is longer than the usual Ethernet packet with regards to MTU, but FortiClient does not receive those packets.

In this case, you can try IKE fragmentation. You must make changes to the FortiGate and FortiClient configurations.

To configure the FortiGate:

Enable IKE fragmentation on the FortiGate using the following FortiOS CLI commands:

```
config vpn ipsec phase1-interface
   edit <your IPsec VPN>
      set fragmentation enable
   next
end
```

To configure FortiClient:

Enable IKE fragmentation on FortiClient using the *Enable IKE Fragmentation* GUI option (under *Endpoint Profiles > Remote Access > IPsec VPN tunnel > Phase 1*) or the following XML configuration:

```
<ipsecvpn>
      <connections>
         <connection>
            <name>your IPsec VPN</name>
            <ike_settings>
                  <enable_ike_fragmentation>1</enable_ike_fragmentation>
```

See the *IKEv1 fragmentation* and *IKEv2 fragmentation* sections in FortiOS documentation for more details.

DPD example

In unstable or unreliable network access conditions with high packet loss and jitter, look for the following signs for high DPD sensitivity:

- FortiClient fails to connect to IPsec VPN.
- When you view the FortiGate IKE debug log, you see that FortiOS sends `R_U_THERE` to FortiClient, but there is no reply, and it times out.
- You see keywords similar to the following in the log:

```
[2025-10-29 16:17:02.3689080 UTC-07:00] [13412:856] [iked  2364    info] ikev2 create server
success
...
```

```
[2025-10-29 16:17:02.3939415 UTC-07:00] [13412:856] [iked  1155   debug] config_getstatic:
dpd_enabled 1
[2025-10-29 16:17:02.3939430 UTC-07:00] [13412:856] [iked  1157   debug] config_getstatic:
dpd_check_interval 5
[2025-10-29 16:17:02.3939449 UTC-07:00] [13412:856] [iked  1158   debug] config_getstatic:
dpd_retry_count 10
...

[2025-10-29 16:17:40.1481546 UTC-07:00] [13412:856] [iked  446    info] Informational(1)
spi=0xc83fcd30b5ed3339:  send INFORMATIONAL req 9 peer 192.168.100.1:4500 local
192.168.100.111:50412, 80 bytes , NAT-T
[2025-10-29 16:17:40.1481628 UTC-07:00] [13412:856] [iked  504   debug] sendtofrom: send from
192.168.100.111 to 192.168.100.1
[2025-10-29 16:17:40.1488877 UTC-07:00] [13412:856] [iked  1466    info] ikev2_msg_dispose:
dequeue retransmit msg, msg_id: 9
[2025-10-29 16:17:40.1488999 UTC-07:00] [13412:856] [iked  1237   debug] ikev2_negotiation_
recv: updated SA to peer 192.168.100.1:4500 local 192.168.100.111:50412
[2025-10-29 16:17:40.1489020 UTC-07:00] [13412:856] [iked  2358    info] ikev2_init_recv:
Receive message with id: 9
[2025-10-29 16:17:40.1489042 UTC-07:00] [13412:856] [iked  2391    info] <== INFORMATIONAL
reply

[2025-10-29 16:17:50.1398645 UTC-07:00] [13412:856] [iked  446    info] Informational(1)
spi=0xc83fcd30b5ed3339:  send INFORMATIONAL req 10 peer 192.168.100.1:4500 local
192.168.100.111:50412, 80 bytes , NAT-T
[2025-10-29 16:17:50.1398746 UTC-07:00] [13412:856] [iked  504   debug] sendtofrom: send from
192.168.100.111 to 192.168.100.1
[2025-10-29 16:17:50.1407480 UTC-07:00] [13412:856] [iked  1466    info] ikev2_msg_dispose:
dequeue retransmit msg, msg_id: 10
[2025-10-29 16:17:50.1407641 UTC-07:00] [13412:856] [iked  1237   debug] ikev2_negotiation_
recv: updated SA to peer 192.168.100.1:4500 local 192.168.100.111:50412
[2025-10-29 16:17:50.1407671 UTC-07:00] [13412:856] [iked  2358    info] ikev2_init_recv:
Receive message with id: 10
[2025-10-29 16:17:50.1407700 UTC-07:00] [13412:856] [iked  2391    info] <== INFORMATIONAL
reply

[2025-10-29 16:18:00.1448143 UTC-07:00] [13412:856] [iked  446    info] Informational(1)
spi=0xc83fcd30b5ed3339:  send INFORMATIONAL req 11 peer 192.168.100.1:4500 local
192.168.100.111:50412, 80 bytes , NAT-T
[2025-10-29 16:18:00.1448246 UTC-07:00] [13412:856] [iked  504   debug] sendtofrom: send from
192.168.100.111 to 192.168.100.1

[2025-10-29 16:18:00.1449108 UTC-07:00] [13412:856] [iked  520    info] ikev2_msg_send:
enqueue request, msg_id: 11

[2025-10-29 16:18:02.1503937 UTC-07:00] [13412:856] [iked  1633    info]
spi=0xc83fcd30b5ed3339:  retransmit 1 INFORMATIONAL req 11 peer 192.168.100.1:4500 local
192.168.100.111:50412
[2025-10-29 16:18:07.1518140 UTC-07:00] [13412:856] [iked  1633    info]
spi=0xc83fcd30b5ed3339:  retransmit 2 INFORMATIONAL req 11 peer 192.168.100.1:4500 local
192.168.100.111:50412
```

```
[2025-10-29 16:18:12.1418452 UTC-07:00] [13412:856] [iked  1633    info]
spi=0xc83fcd30b5ed3339:  retransmit 3 INFORMATIONAL req 11 peer 192.168.100.1:4500 local
192.168.100.111:50412
[2025-10-29 16:18:17.1487448 UTC-07:00] [13412:856] [iked  1633    info]
spi=0xc83fcd30b5ed3339:  retransmit 4 INFORMATIONAL req 11 peer 192.168.100.1:4500 local
192.168.100.111:50412
[2025-10-29 16:18:22.1560107 UTC-07:00] [13412:856] [iked  1633    info]
spi=0xc83fcd30b5ed3339:  retransmit 5 INFORMATIONAL req 11 peer 192.168.100.1:4500 local
192.168.100.111:50412
[2025-10-29 16:18:27.1754173 UTC-07:00] [13412:856] [iked  1633    info]
spi=0xc83fcd30b5ed3339:  retransmit 6 INFORMATIONAL req 11 peer 192.168.100.1:4500 local
192.168.100.111:50412
[2025-10-29 16:18:32.1770519 UTC-07:00] [13412:856] [iked  1633    info]
spi=0xc83fcd30b5ed3339:  retransmit 7 INFORMATIONAL req 11 peer 192.168.100.1:4500 local
192.168.100.111:50412
[2025-10-29 16:18:37.1788013 UTC-07:00] [13412:856] [iked  1633    info]
spi=0xc83fcd30b5ed3339:  retransmit 8 INFORMATIONAL req 11 peer 192.168.100.1:4500 local
192.168.100.111:50412
[2025-10-29 16:18:42.2001021 UTC-07:00] [13412:856] [iked  1633    info]
spi=0xc83fcd30b5ed3339:  retransmit 9 INFORMATIONAL req 11 peer 192.168.100.1:4500 local
192.168.100.111:50412
[2025-10-29 16:18:47.2002767 UTC-07:00] [13412:856] [iked  1633    info]
spi=0xc83fcd30b5ed3339:  retransmit 10 INFORMATIONAL req 11 peer 192.168.100.1:4500 local
192.168.100.111:50412

[2025-10-29 16:18:52.1920136 UTC-07:00] [13412:856] [iked  1659   debug] ikev2_msg_retransmit_
timeout: retransmit limit reached for req 11
[2025-10-29 16:18:52.1921247 UTC-07:00] [13412:856] [iked  646    info]
spi=0xc83fcd30b5ed3339: sa_free: retransmit limit reached
[2025-10-29 16:18:52.1921420 UTC-07:00] [13412:856] [iked  194   debug] SA deleted: SPI
0x261d20fa
[2025-10-29 16:18:52.1921652 UTC-07:00] [13412:856] [iked  1466    info] ikev2_msg_dispose:
dequeue retransmit msg, msg_id: 11

[2025-10-29 16:18:52.7939176 UTC-07:00] [13412:856] [iked  605   debug] config_doreset:
flushing policies
[2025-10-29 16:18:52.7939327 UTC-07:00] [13412:856] [iked  315   debug] config_free_proposals:
free 0x000001FC7768FE70
[2025-10-29 16:18:52.7939371 UTC-07:00] [13412:856] [iked  315   debug] config_free_proposals:
free 0x000001FC7768FEC0
[2025-10-29 16:18:52.7939392 UTC-07:00] [13412:856] [iked  315   debug] config_free_proposals:
free 0x000001FC77690EB0
[2025-10-29 16:18:52.7939508 UTC-07:00] [13412:856] [iked  315   debug] config_free_proposals:
free 0x000001FC77690FA0
[2025-10-29 16:18:52.7939535 UTC-07:00] [13412:856] [iked  327   debug] config_free_flows:
free 0x000001FC77F41930
[2025-10-29 16:18:52.7939572 UTC-07:00] [13412:856] [iked  612   debug] config_doreset:
flushing SAs
[2025-10-29 16:18:52.7939588 UTC-07:00] [13412:856] [iked  665   debug] config_doreset:
flushing users
[2025-10-29 16:18:52.8026337 UTC-07:00] [13412:856] [iked  712    info] ikev2 exiting, pid
```

```
13412
[2025-10-29 16:18:52.8026476 UTC-07:00] [13412:856] [iked  1418    info] trace stopped
```

You can reduce the DPD sensitivity by increasing the values for counter and interval on both FortiClient and FortiGate. These values are not negotiated and are independent of each other.

FortiGate	Use the following FortiOS CLI commands:
	`config vpn ipsec phase1-interface`
	`edit <your IPsec VPN>`
	`set dpd-retrycount <configure a higher number>`
	`set dpd-retryinterval <configure a higher number>`
	`next`
	`end`

FortiClient	Using the following XML configuration:
	`<ipsecvpn>`
	`<connections>`
	`<connection>`
	`<ike_settings>`
	`<dpd>1</dpd>`
	`<dpd_retry_count>configure a higher number</dpd_retry_count>`
	`<dpd_retry_interval>configure a higher number</dpd_retry_interval>`

Antivirus

The <antivirus> </antivirus> XML tags contain AV configuration data. The following are subsections of the AV configuration.

General options

This section has options that enable various services in the AV feature:

```
<forticlient_configuration>
   <antivirus>
      <enabled>1</enabled>
      <signature_expired_notification>0</signature_expired_notification>
      <scan_on_insertion>0</scan_on_insertion>
      <shell_integration>1</shell_integration>
      <advanced_shell_integration>
         <hide_av_scan>0</hide_av_scan>
         <hide_av_analyse>0</hide_av_analyse>
      </advanced_shell_integration>
      <antirootkit>4294967295</antirootkit>
      <fortiguard_analytics>0</fortiguard_analytics>
      <multi_process_limit>1</multi_process_limit>
   </antivirus>
</forticlient_configuration>
```

The following table provides the XML tags for general AV options, as well as the descriptions and default values where applicable.

XML tag	Description	Default value
<enabled>	Enable AV. Boolean value: [0 | 1]	1
<signature_expired_notification>	Notify logged in users if their AV signatures expired. Boolean value: [0 | 1]	0
<scan_on_insertion>	Scan removable media (CDs, DVDs, Blu-ray disks, USB keys, etc.) on insertion. Boolean value: [0 | 1]	0
<shell_integration>	Integrate FortiClient into Windows Explorer's context menu. Boolean value: [0 | 1]	1
<hide_av_scan>	Hide AV scan option from Windows Explorer's context menu. Boolean value: [0 | 1]	

XML tag	Description	Default value
<hide_av_analysis>	Hide option to submit file for AV analysis from Windows Explorer's context menu. Boolean value: [0 | 1]	
<antirootkit>	Enable antirootkit. This field is a bit mask. When set to 0, all antirootkit features are disabled. 4294947295 (=0xffffffff) means all antirootkit features are enabled.	
<fortiguard_analytics>	Automatically send suspicious files to FortiGuard for analysis. Boolean value: [0 | 1]	1
<multi_process_limit>	The number of AV scanning processes to use for scheduled or on-demand scans. The maximum is the number of CPU processors and cores. When set to 0, FortiClient determines the optimal value.	0

Real-time protection

The <real_time_protection> element configures how the scanner processes files used by programs running on the system.

Several tags are similar between this section and <on_demand_scanning>.

```
<forticlient_configuration>
   <antivirus>
      <real_time_protection>
         <enabled>1</enabled>
         <use_extreme_db>0</use_extreme_db>
         <when>0</when>
         <ignore_system_when>0</ignore_system_when>
         <on_virus_found>0</on_virus_found>
         <popup_alerts>0</popup_alerts>
         <popup_registry_alerts>0</popup_registry_alerts>
         <amsi_enabled>0</amsi_enabled>
         <conflicting_rtp_action>disable</conflicting_rtp_action>
         <compressed_files>
            <scan>1</scan>
            <maxsize>2</maxsize>
         </compressed_files>
         <riskware>
            <enabled>1</enabled>
         </riskware>
         <adware>
            <enabled>1</enabled>
         </adware>
         <heuristic_scanning>
            <level>3</level>
            <action>0</action>
         </heuristic_scanning>
         <scan_file_types>
            <all_files>1</all_files>
```

```
            <file_types>
               <extensions>.386,.ACE,.ACM,.ACV,.ACX,.ADT,.APP,.ASD,.ASP,.ASX,.AVB,.AX,.AX2,.BAT,.BIN
                     ,.BTM,.CDR,.CFM,.CHM,.CLA,.CLASS,.CMD,.CNN,.COM,.CPL,.CPT,.CPY,.CSC,.CSH,.CSS,.D
                     EV,.DLL,.DOC,.DOT,.DRV,.DVB,.DWG,.EML,.EXE,.FON,.GMS,.GVB,.HLP,.HTA,.HTM,.HTML,.
                     HTT,.HTW,.HTX,.HXS,.INF,.INI,.JPG,.JS,.JTD,.KSE,.LGP,.LIB,.LNK,.MDB,.MHT,.MHTM,.
                     MHTML,.MOD,.MPD,.MPP,.MPT,.MRC,.OCX,.PIF,.PL,.PLG,.PM,.PNF,.PNP,.POT,.PPA,.PPS,.
                     PPT,.PRC,.PWZ,.QLB,.QPW,.REG,.RTF,.SBF,.SCR,.SCT,.SH,.SHB,.SHS,.SHT,.SHTML,.SHW,
                     .SIS,.SMM,.SWF,.SYS,.TD0,.TLB,.TSK,.TSP,.TT6,.VBA,.VBE,.VBS,.VBX,.VOM,.VSD,.VSS,
                     .VST,.VWP,.VXD,.VXE,.WBK,.WBT,.WIZ,.WK,.WML,.WPC,.WPD,.WSC,.WSF,.WSH,.XLS,.XML,.
                     XTP</extensions>
               <include_files_with_no_extension>0</include_files_with_no_extension>
            </file_types>
         </scan_file_types>
         <exclusions>
            <file />
            <folder />
            <file_types>
               <extensions />
            </file_types>
         </exclusions>
         </real_time_protection>
      </antivirus>
</forticlient_configuration>
```

The following table provides the XML tags for RTP, as well as the descriptions and default values where applicable.

XML tag	Description	Default value
`<enabled>`	Enable RTP. Boolean value: [`0` | `1`]	`1`
`<use_extreme_db>`	Use extreme database. Boolean value: [`0` | `1`]	
`<when>`	File I/O activities that result in a scan. Configure one of the following: • `0`: scan files when processes read or write them and enable scanning network files. • `1`: scan files when processes read them and disable scanning network files. • `2`: scan files when processes write them and disable scanning network files. • `3`: scan files when processes read or write them and disable scanning network files. • `4`: scan files when processes read them and enable scanning network files. • `5`: scan files when processes write them and enable scanning network files.	`0`
`<ignore_system_when>`	Configure one of the following: • `0`: scan files when system processes read or write them. • `1`: scan files when system processes read them. • `2`: scan files when system processes write them.	`2`

XML tag	Description	Default value
	• 3: do not scan files when system processes read or write them.	
<on_virus_found>	Configure the action FortiClient performs if it finds a virus: • 1: ignore infected files. • 4: quarantine infected files. You can use FortiClient to view, restore, or delete the quarantined file, as well as view the virus name, submit the file to FortiGuard, and view logs. • 5: deny access to infected files.	5
<popup_alerts>	If enabled, displays the *Virus Alert* dialog when a virus is detected while attempting to download a file via a web browser. The dialog allows you to view recently detected viruses, their locations, and statuses. Boolean value: [0 | 1]	1
<popup_registry_alerts>	Enable popup registry alerts. This feature displays alerts if a process tries to change registry start items. Boolean value: [0 | 1]	0
<amsi_enabled>	Enable Microsoft Anti-Malware Interface Scan (AMSI). This feature is only available for Windows 10 endpoints. AMSI scans memory for the following malicious behavior: • User Account Control (elevation of EXE, COM, MSI, or ActiveX installation) • PowerShell (scripts, interactive use, and dynamic code evaluation) • Windows Script Host (wscript.exe and script.exe) • JavaScript and VBScript • Office VBA macros Boolean value: [0 | 1]	0
<conflicting_rtp_action>	FortiClient RTP may have conflicts with other AV products. Configure one of the following for RTP: • disable: disable FortiClient RTP. You may want to configure this option if you have another similar AV product installed on the endpoint. • enable: enable FortiClient RTP if another Fortinet AV product is installed on the endpoint. • always_enable: FortiClient RTP is always enabled. Selecting this option allows multiple AV products to run concurrently on the endpoint and may cause system instability.	disable
<compressed_files> elements		
<scan>	Scan archive files, including zip, rar, and tar files, for threats. Boolean value: [0 | 1]	1

XML tag	Description	Default value
<maxsize>	Only scan files under the specified size in MB. A number up to 65535. 0 means no limit. For compressed files, FortiClient supports a maximum file size of 1 GB for antivirus scanning. For a compressed file with a size larger than 1 GB, FortiClient scans it after decompression.	2
<riskware> element		
<enabled>	Scan for riskware. Riskware refers to legitimate programs which, when installed and executed, presents a possible but not definite risk to the computer. Boolean value: [0 | 1]	1
<adware> element		
<enabled>	Scan for adware. Adware is a form of software that downloads or displays unwanted ads when a user is online. Boolean value: [0 | 1]	1
<heuristic_scanning> elements The new FortiClient AV engine incorporates a smarter signature-less machine learning (ML)-based advanced threat detection. The antimalware solution includes ML models static and dynamic analysis of threats.		
<level>	This setting applies to real-time and on-demand scans. Enter one of the following: • 0: normal • 1: advanced heuristics on highly infected systems • 2: Minos engine heuristics on highly infected systems • 3: both advanced heuristics on highly infected systems and engine heuristics • 4: both, without waiting to determine if system is highly infected	
<action>	The action FortiClient performs if it finds a virus. Enter one of the following: • 0: detect and notify only (with log entries, no other action) • 2: quarantine the file	
<scan_file_types> element		
<all_files>	Enabled scanning of all file types. If enabled, ignore the <file_types> element. Boolean value: [0 | 1]	1
<scan_file_types><file_types> elements		
<extensions>	Comma separated list of extensions to scan.	
<include_files_with_no_extension>	Determines whether to scan files with no extension. Boolean value: [0 | 1]	0

XML tag	Description	Default value
<exclusions> elements FortiClient supports using wildcards and path variables to specify files and folders to exclude from scanning. FortiClient supports the following wildcards and variables, among others: • Using wildcards to exclude a range of file names with a specified extension, such as Edb*.jrs • Using wildcards to exclude all files with a specified extension, such as *.jrs • Path variable %allusersprofile% • Path variable %appdata% • Path variable %localappdata% • Path variable %systemroot% • Path variable %systemdrive% • Path variable %userprofile% • Path variable %windir% FortiClient does not support combinations of wildcards and variables.		
<file>	Full path to a file to exclude from RTP scanning. Element may be repeated to list more files.	
<folder>	Full path to a directory to exclude from RTP scanning. Element may be repeated to list more directories. Shadow Copy format is supported, for example, <folder>\Device\HarddiskVolumeShadowCopy*</folder>. Shadow Copy is also known as Volume Snapshot Service, Volume Shadow Copy Service, or VSS. Wildcards are not accepted.	
<exclusions> <file_types> element		
<extensions>	Comma separated list of extensions to exclude from RTP scanning.	
<sandboxing> element		
<enabled>	Enable FortiSandbox configuration. Boolean value: [0 | 1]	
<sandbox_address>	Specify the IP address for FortiSandbox.	
<timeout>	Specify how long to wait in seconds for FortiSandbox results before allowing file access. When set to 0 seconds, file access is granted without waiting for FortiSandbox results. Range: 0-4294967295 in seconds	
<use_sandbox_signatures>	Enable using FortiSandbox signatures. Boolean value: [0 | 1]	
<check_for_signatures_every>	Specify how often to check for FortiSandbox signatures when <use_sandbox_signatures> is set to 1. Boolean value: [0 | 1]	

XML tag	Description	Default value
<action_on_error>	Specify whether to block traffic when FortiSandbox finds errors. When this setting is 0, traffic is passed. When this setting is 1, traffic is blocked. Boolean value: [0 | 1]	0
<scan_usb>	Enable sending files from USB drives to FortiSandbox for scanning. When this setting is 0, files are not scanned. When this setting is 1, files are scanned. Boolean value: [0 | 1]	0
<scan_mapped_drives>	Enable sending files from mapped drives to FortiSandbox for scanning. When this setting is 0, files are not scanned. When this setting is 1, files are scanned. Boolean value: [0 | 1]	0

On-demand scans

The <on_demand_scanning> element defines how the AV scanner handles scanning of files that the end user manually requested.

```
<forticlient_configuration>
   <antivirus>
      <on_demand_scanning>
      <use_extreme_db>0</use_extreme_db>
      <on_virus_found>4</on_virus_found>
      <pause_on_battery_power>1</pause_on_battery_power>
      <allow_admin_to_stop>1</allow_admin_to_stop>
      <signature_load_memory_threshold>8</signature_load_memory_threshold>
      <automatic_virus_submission>
         <enabled>0</enabled>
         <smtp_server>fortinetvirussubmit.com</smtp_server>
         <username />
         <password>Encrypted/NonEncrypted_PasswordString</password>
      </automatic_virus_submission>
      <compressed_files>
         <scan>1</scan>
         <maxsize>0</maxsize>
      </compressed_files>
      <riskware>
         <enabled>1</enabled>
      </riskware>
      <adware>
         <enabled>1</enabled>
      </adware>
      <heuristic_scanning>
         <level>3</level>
         <action>2</action>
      </heuristic_scanning>
      <scan_file_types>
         <all_files>1</all_files>
         <file_types>
```

```
            <extensions>.386,.ACE,.ACM,.ACV,.ACX,.ADT,.APP,.ASD,.ASP,.ASX,.AVB,.AX,.AX2,.BAT,.BIN
                  ,.BTM,.CDR,.CFM,.CHM,.CLA,.CLASS,.CMD,.CNN,.COM,.CPL,.CPT,.CPY,.CSC,.CSH,.CSS,.D
                  EV,.DLL,.DOC,.DOT,.DRV,.DVB,.DWG,.EML,.EXE,.FON,.GMS,.GVB,.HLP,.HTA,.HTM,.HTML,.
                  HTT,.HTW,.HTX,.HXS,.INF,.INI,.JPG,.JS,.JTD,.KSE,.LGP,.LIB,.LNK,.MDB,.MHT,.MHTM,.
                  MHTML,.MOD,.MPD,.MPP,.MPT,.MRC,.OCX,.PIF,.PL,.PLG,.PM,.PNF,.PNP,.POT,.PPA,.PPS,.
                  PPT,.PRC,.PWZ,.QLB,.QPW,.REG,.RTF,.SBF,.SCR,.SCT,.SH,.SHB,.SHS,.SHT,.SHTML,.SHW,
                  .SIS,.SMM,.SWF,.SYS,.TD0,.TLB,.TSK,.TSP,.TT6,.VBA,.VBE,.VBS,.VBX,.VOM,.VSD,.VSS,
                  .VST,.VWP,.VXD,.VXE,.WBK,.WBT,.WIZ,.WK,.WML,.WPC,.WPD,.WSC,.WSF,.WSH,.XLS,.XML,.
                  XTP</extensions>
               <include_files_with_no_extension>0</include_files_with_no_extension>
         </file_types>
         </scan_file_types>
         <exclusions>
            <file></file>
            <folder></folder>
            <file_types>
               <extensions></extensions>
            </file_types>
         </exclusions>
      </on_demand_scanning>
   </antivirus>
</forticlient_configuration>
```

The following table provides the XML tags for on-demand scans, as well as the descriptions and default values where applicable.

XML tag	Description	Default value
`<use_extreme_db>`	Use the extreme database. Boolean value: `[0 | 1]`	`0`
`<on_virus_found>`	The action FortiClient performs if it finds a virus. Configure one of the following: • `4`: quarantine infected files. You can use FortiClient to view, restore, or delete the quarantined file, as well as view the virus name, submit the file to FortiGuard, and view logs. • `5`: deny access to infected files.	`4`
`<pause_on_ battery_ power>`	Pause scanning when the computer is running on battery power. Boolean value: `[0 | 1]`	`1`
`<allow_admin_to_ stop>`	Control whether the local administrator can stop a scheduled or on-demand AV scan that the EMS administrator initiated. Boolean value: `[0 | 1]`	`1`

XML tag	Description	Default value
<signature_load_memory_threshold>	Configure the threshold used to control memory allocation mechanism for signature loading. When the physical machine has more memory than the threshold, it uses the static memory mechanism to load signatures one time, which ensures that the scan is efficient. When the physical machine has less memory than the threshold, it uses the dynamic memory mechanism to load the signatures, which ensures that the scan process does not use too much memory.	
<heuristic_scanning> elements The new FortiClient AV engine incorporates a smarter signature-less machine learning (ML)-based advanced threat detection. The antimalware solution includes ML models static and dynamic analysis of threats.		
<level>	This setting applies to real-time and on-demand scans. Enable or disable ML: • 0: disable ML. • 2: enable ML. If you enter a value higher than 2, the value defaults to 2.	
<action>	The action that FortiClient performs if it finds a virus. Enter one of the following: • 0: detect the sample, display a warning message, and log the activity. • 2: quarantine infected files. You can use FortiClient to view, restore, or delete the quarantined file, as well as view the virus name, submit the file to FortiGuard, and view logs. If you enter a value higher than 2, the value defaults to 2.	
<automatic_virus_submission> elements		
<enabled>	Automatically submit suspicious files to FortiGuard for analysis. You do not receive feedback for files submitted for analysis. The FortiGuard team is able to create signatures for any files that are submitted for analysis and determined to be malicious. Boolean value: [0 | 1]	0
<smtp_server>	SMTP server IP address or FQDN.	fortinetvirussubmit.com
<username>	SMTP server username.	
<password>	SMTP server encrypted or non-encrypted password.	
<compressed_files> elements		

XML tag	Description	Default value
<scan>	Scan archive files, including zip, rar, and tar files, for threats. Boolean value: [0 | 1]	1
<maxsize>	Maximum compressed file size to scan in MB. A number up to 65535. 0 means no limit.	0
<riskware> elements		
<enabled>	Scan for riskware. Riskware refers to legitimate programs which, when installed and executed, presents a possible but not definite risk to the computer. Boolean value: [0 | 1]	1
<adware> element		
<enabled>	Scan for adware. Adware is a form of software that downloads or displays unwanted ads when a user is online. Boolean value: [0 | 1]	1
<scan_file_types> element		
<all_files>	Scan all file types. If enabled, ignore the <file_types> element. Boolean value: [0 | 1]	1
<scan_file_types> <file_types> elements		
<extensions>	Enter a comma separated list of extensions to scan.	
<include_files_with_no_extension>	Determines whether to scan files with no extension. Boolean value: [0 | 1]	0
<exclusions> elements		
<file>	Full path to a file to exclude from on-demand scanning. Wildcards are not accepted. Element may be repeated to list more files.	
<folder>	Full path to a directory to exclude from on-demand scanning. Element may be repeated to list more directories. Shadow Copy format is supported, for example, <folder>\Device\HarddiskVolumeShadowCopy*</folder>. Shadow Copy is also known as Volume Snapshot Service, Volume Shadow Copy Service, or VSS. Wildcards are not accepted.	
<exclusions> <file_types> element		

XML tag	Description	Default value
<extensions>	Comma separated list of extensions to exclude from on-demand scanning.	

Scheduled scans

You may schedule scanning for viruses in one of three ways. FortiClient does not support multiple instances of the <scheduled_scans> element.

Scan type	Description
Quick scan	Runs the rootkit detection engine to detect and remove rootkits. The quick scan only scans the following items for threats: executable files, DLLs, and drivers that are currently running.
Full scan	Runs the rootkit detection engine to detect and remove rootkits, then performs a full system scan of all files, executable files, DLLs, and drivers. If *Full* is selected, you have the following options: • Scan removable media, if present • Scan network drives
Custom scan	Runs the rootkit detection engine to detect and remove rootkits. Use the <directory> element to enter the full path of the folder on your local hard disk drive that will be scanned.

You can enable only one scheduled scan at a time. For example, you can enable a full scan and disable quick scans and custom scans.

Each of three scheduling options require specific combinations of several common elements, which define when scanning should occur. The common elements are described first. Other elements specific to the full and custom scans are described later.

The factory default at the time of installation is to run a full scan on the first day of the month at 19:30.

```
<forticlient_configuration>
   <antivirus>
      <scheduled_scans>
      <ignore_3rd_party_av_conflicts>1</ignore_3rd_party_av_conflicts>
         <quick>
            <enabled>1</enabled>
            <repeat>0</repeat>
            <time>19:30</time>
         </quick>
      </scheduled_scans>
      <scheduled_scans>
      <ignore_3rd_party_av_conflicts>1</ignore_3rd_party_av_conflicts>
         <full>
            <enabled>0</enabled>
            <repeat>0</repeat>
            <time>19:30</time>
            <removable_media>1</removable_media>
            <network_drives>1</network_drives>
            <priority>2</priority>
```

```
            </full>
         </scheduled_scans>
         <scheduled_scans>
         <ignore_3rd_party_av_conflicts>1</ignore_3rd_party_av_conflicts>
               <enabled>1</enabled>
               <repeat>0</repeat>
               <days>2</days>
               <time>19:30</time>
               <directory>c:\</directory>
               <priority>0</priority>
            </directory>
         </scheduled_scans>
      </antivirus>
   </forticlient_configuration>
```

Following is an example of the elements for a quick monthly scan:

```
         <scheduled_scans>
         <ignore_3rd_party_av_conflicts>1</ignore_3rd_party_av_conflicts>
            <quick>
               <enabled>1</enabled>
               <repeat>2</repeat>
               <day_of_month>1</day_of_month>
               <time>19:30</time>
            </quick>
         </scheduled_scans>
```

Following is an example of the elements for a quick weekly scan:

```
         <scheduled_scans>
         <ignore_3rd_party_av_conflicts>1</ignore_3rd_party_av_conflicts>
            <quick>
               <enabled>1</enabled>
               <repeat>1</repeat>
               <days>1</days>
               <time>19:30</time>
            </quick>
         </scheduled_scans>
```

Following is an example of the elements for a quick daily scan:

```
         <scheduled_scans>
         <ignore_3rd_party_av_conflicts>1</ignore_3rd_party_av_conflicts>
            <quick>
               <enabled>1</enabled>
               <repeat>0</repeat>
               <time>19:30</time>
            </quick>
         </scheduled_scans>
```

The following table provides the XML tags for scheduled scans, as well as the descriptions and default values where applicable. These elements are common to all scheduled scan types:

XML tag	Description	Default value
<enabled>	Enable scheduled scans. You can enable only one of the following scan types at a time: quick, full, or custom.	

XML tag	Description	Default value
	Boolean value: [0 | 1]	
<repeat>	Frequency of scans. The selected frequency affects the elements required to correctly configure the scan. Examples are provided before the table. Select one of the following: • 0: daily • 1: weekly • 2: monthly	
<days>	Day of the week to run the scan. Used when <repeat> is set to 1 for weekly scans. Enter one of the following: • 1: Sunday • 2: Monday • 3: Tuesday • 4: Wednesday • 5: Thursday • 6: Friday • 7: Saturday	
<day_of_month>	The day of the month to run a scan. Used when <repeat> is set to 2 for monthly scans. Enter a number from 1 to 31. If you configure monthly scans to occur on the 31st of each month, the scan occurs on the first day of the month for months with fewer than 31 days.	
<time>	Configure the start time for the scheduled scan, using a 24-hour clock.	

The following table provides full scan and custom scan element XML tags, the description, and the default value (where applicable).

XML tag	Description	Default value
<full> elements		
<removable_media>	Scan connected removable media, such as USB drives, for threats, if present. Boolean value: [0 | 1]	1
<network_drives>	Scan attached or mounted network drives for threats. Boolean value: [0 | 1]	0
<priority>	Scan priority. This refers to the amount of processing power the scan uses and its impact on other processes. Enter one of the following: • 0: normal • 1: low • 2: high	0
<directory> elements		

XML tag	Description	Default value
<directory>	The full path to the directory to scan when using a custom scan.	
<priority>	Scan priority. This refers to the amount of processing power the scan uses and its impact on other processes. Select one of the following: • 0: normal • 1: low • 2: high	

Email

FortiClient scans emails for viruses based on the settings in the <email> </email> XML tags. You can configure virus scanning for SMTP and POP3.

```
<forticlient_configuration>
   <antivirus>
      <email>
         <smtp>1</smtp>
         <pop3>1</pop3>
         <wormdetection>
            <enabled>0</enabled>
            <action>0</action>
         </wormdetection>
         <heuristic_scanning>
            <enabled>0</enabled>
            <action>0</action>
         </heuristic_scanning>
         <mime_scanning>
            <enabled>1</enabled>
         </mime_scanning>
      </email>
   </antivirus>
</forticlient_configuration>
```

The following table provides the XML tags for email scans, as well as the descriptions and default values where applicable.

XML tag	Description	Default value
<smtp>	Scan email messages sent through the SMTP protocol. Boolean value: [0 | 1]	1
<pop3>	Scan email messages received through the POP3 protocol. Boolean value: [0 | 1]	1
<wormdetection> elements		
<enabled>	Scan for worm viruses. Boolean value: [0 | 1]	0

XML tag	Description	Default value
<action>	Action that FortiClient performs if it finds a virus. Enter one of the following: • 0: warn • 1: terminate process	0
<heuristic_scanning> elements		
<enabled>	Scan with heuristics signature. Boolean value: [0 | 1]	0
<action>	Action FortiClient performs if it finds a virus. Enter one of the following: • 0: log and warn • 1: strip and quarantine	0
<mime_scanning>	Scan inbox email content with Multipurpose Internet Mail Extensions (MIME) file types. MIME is an Internet standard that extends the format of the email to support the following: • Text in character sets other than ASCII • Non text attachments (audio, video, images, applications) • Message bodies with multiple parts Boolean value: [0 | 1]	

Quarantine

You can specify the maximum age for quarantined files in the <quarantine></quarantine> XML tags.

```
<forticlient_configuration>
   <antivirus>
      <quarantine>
         <cullage>100</cullage>
         <force_delete>1</force_delete>
      </quarantine>
   </antivirus>
</forticlient_configuration>
```

The following table provides the XML tags for quarantining files, as well as the descriptions and default values where applicable.

XML tag	Description	Default value
<cullage>	Specify the number of days to hold quarantined files before deleting them. Enter a number from 1 and 365.	100
<force_delete>	If enabled, FortiClient terminates programs that are using a file that it detected as malware, then quarantines the file. Boolean: [0 | 1]	

Antiransomware

The following lists antiransomware attributes:

```
<forticlient_configuration>
  <rs_protection>
     <enabled>1</enabled>
     <default_action>1</default_action>
     <bypass_valid_signer>1<\bypass_valid_signer>
     <default_action_timeout>5</default_action_timeout>
     <enable_backup>1</enable_backup>
     <backup_interval>1</backup_interval>
     <backup_file_size_limit>1</backup_file_size_limit>
     <backup_disk_quota>10</backup_disk_quota>
     <use_custom_file_extensions>1</use_custom_file_extensions>
     <custom_
           extensions>cmd,csv,dll,dmg,docm,docx,dot,dotm,dotx,elf,eml,exe,gz,iqy,iso,jar,jse,msi,pd
           f,pot,potm,potx,ppam,pps,ppsm,ppsx,ppt,pptm,pptx,ps1,rar,rtf,tar,thmx,xlam,xls,xlsb,xlsm
           ,xlsx,xlt,xltm,xltx,xz,z,zip</custom_extensions>
     <protections>
        <folders>
           <folder>C:\Users\%USERNAME%\Documents\</folder>
           <folder>C:\Users\%USERNAME%\Pictures\</folder>
           <folder>C:\Users\%USERNAME%\Videos\</folder>
           <folder>C:\Users\%USERNAME%\Music\</folder>
           <folder>C:\Users\%USERNAME%\Desktop\</folder>
           <folder>C:\Users\%USERNAME%\Favorites\</folder>
           <folder>C:\ransome</folder>
        </folders>
     </protections>
     <exclusions>
        <folders>
           <folder>C:\Users\%USERNAME%\Documents\folder 1</folder>
           <folder>C:\Users\%USERNAME%\Desktop\folder 2</folder>
        </folders>
        <files>
           <file>C:\Users\%USERNAME%\Pictures\image.png</file>
           <file>C:\Users\%USERNAME%\Videos\video.mp4</file>
        </files>
     </exclusions>
  </rs_protection>
</forticlient_configuration>
```

The following table provides the XML tags for antiransomware detection, as well as the descriptions and default values where applicable:

XML tag	Description	Default value
`<enabled>`	Enable antiransomware detection to protect specific files, folders, or file types on your endpoints from unauthorized changes. Boolean value: `[0 | 1]`	

XML tag	Description	Default value

<default_action>	When antiransomware detects suspicious activity, it displays a popup asking the user if they want to terminate the process:
	• If the user selects *Yes*, FortiClient terminates the suspicious process.
	• If the user selects *No*, FortiClient allows the process to continue.
	• If the user does not select an option, FortiClient waits for the configured action timeout, then does one of the following, as configured:
	  • 1: terminate ransomware behavior
	  • 2: FortiClient allows the process to continue and monitors it.	

<bypass_valid_signer>	Exclude a process from the selected antiransomware action if it has a valid signer. Boolean value: [0 | 1]	
<default_action_timeout>	Enter the desired timeout value in seconds.	120
<enable_backup>	Enable FortiClient to restore files that the detected ransomware encrypted after detecting ransomware behavior on the endpoint Boolean value: [0 | 1]	0
<backup_interval>	Enter the desired backup interval value in hours. FortiClient backs up files in protected folders that were last modified at a time that is longer ago than the backup interval value. The backup only occurs when the files will be modified.	
<backup_file_size_limit>	Enter the desired size limit in MB for ransomware-encrypted files for FortiClient to back up. The size limit refers to the original file size, not the size limit after encryption.	
<backup_disk_quota>	Enter the desired backup disk quota value as a percentage of free disk space.	
<use_custom_file_extensions>	Enable FortiClient to protect a customized list of file extension types. Boolean value: [0 | 1]	

XML tag	Description	Default value
<custom_extensions>	Enter the desired file types to protect from suspicious activity, separating each file type with a comma. Do not include the leading dot when entering a file type. For example, to include text files, you would enter txt, as opposed to .txt.	
<protections><folders><folder>	Enter the desired file directories for FortiClient antiransomware to protect. FortiClient anti-ransomware protects all content in the selected folders against unauthorized changes. Everything else is excluded from anti-ransomware protection.	
<exclusions>	Add specific file directories or paths within the protected folders to exclude from FortiClient antiransomware protection.	
<folders><folder>	Enter the desired file directories within the protected folders for FortiClient antiransomware to exclude. FortiClient anti-ransomware then skips all content in the selected folders.	
<files><file>	Enter the desired file paths within the protected folders for FortiClient antiransomware to exclude. FortiClient anti-ransomware then skips all specified files.	

SSOMA

The <fssoma></fssoma> XML tags contain FortiClient single sign on mobility agent (SSOMA) configuration elements:

```
<forticlient_configuration>
   <fssoma>
      <enabled>0</enabled>
      <serveraddress>IP_or_FQDN</serveraddress>
      <presharedkey>Encypted_Preshared_Key</presharedkey>
      <address_category>0</address_category>
      <prefer_azure>1</prefer_azure>
   </fssoma>
</forticlient_configuration>
```

The following table provides the XML tags for SSOMA, as well as the descriptions and default values where applicable:

XML tag	Description	Default value
<enabled>	Enable SSO. Boolean value: [0 | 1]	0
<serveraddress>	FortiAuthenticator IP address or FQDN. Separate multiple IP addresses with a colon, for example, 10.5.0.150; 10.5.0.155.	
<presharedkey>	Encrypted or unencrypted preshared key.	
<address_category>	If you enable this option, SSOMA sends the physical adapter IP address to FortiAuthenticator when FortiClient is not connected to VPN. When connected to VPN, SSOMA only sends the virtual adapter IP address to FortiAuthenticator. If you disable this option, SSOMA sends the physical adapter IP address to FortiAuthenticator when FortiClient is not connected to VPN. When connected to VPN, SSOMA sends the virtual and physical adapter's IP addresses to FortiAuthenticator. Boolean value: [0 | 1]	

<prefer_azure>	Configure whether FortiClient detects Azure user information and sends it to FortiAuthenticator.
	• If the endpoint is in a hybrid join (on-premise Active Directory (AD) and Microsoft Entra ID) environment, the following occurs:
	  • If <prefer_azure> is disabled, FortiClient sends the on-premise AD information to FortiAuthenticator.
	  • If <prefer_azure> is set to 1, FortiClient sends Entra ID information to FortiAuthenticator.
	• If the endpoint is in an only on-premise local AD environment, FortiClient sends the on-premise local AD information to FortiAuthenticator regardless of the <prefer_azure> configuration.
	• If the endpoint is in an Entra ID environment, FortiClient sends the Entra ID information to FortiAuthenticator regardless of the <prefer_azure> configuration.
	Boolean value: [0 | 1]	

To enable the FortiClient SSO mobility agent service on FortiAuthenticator, you must first apply the applicable FortiClient license for FortiAuthenticator. See the *FortiAuthenticator Administration Guide*. For information on purchasing a FortiClient license, contact your authorized Fortinet reseller.

Web filter

The <webfilter></webfilter> tags contain web filter XML configurations. There are two main sections:

Section	Description
General options	Configuration elements that affect the whole of the web filter service.
Scheduling information	Defines a schedule for when Web Filter settings are in effect.
Profiles	Defines one or more rules that FortiClient applies to network traffic.

You cannot configure Web Filter to block the Chrome web store URL, as it is a critical resource to download the FortiClient Web Filter extension. FortiClient can access the Chrome web store URL regardless of the Web Filter configuration.

```
<forticlient_configuration>
   <webfilter>
      <enable_filter>1</enable_filter>
      <enabled>1</enabled>
      <current_profile>0</current_profile>
      <partial_match_host>0</partial_match_host>
      <disable_when_managed>0</disable_when_managed>
      <keep_extension_when_managed>1</keep_extension_when_managed>
      <max_violations>250</max_violations>
      <max_violations_age>7</max_violations_age>
      <block_malicious_websites>1</block_malicious_websites>
      <bypass_private_ip>1</bypass_private_ip>
      <browser_read_time_threshold>180</browser_read_time_threshold>
      <https_block_method>0</https_block_method>
      <use_transparent_proxy>1</use_transparent_proxy>
      <request_timeout>3</request_timeout>
      <wildcard_match_root_domain>0</wildcard_match_root_domain>
      <enable_https_deep_inspection>1</enable_https_deep_inspection>
      <interception_mode>1</interception_mode>
      <fgd_down_retry_interval_s>1</fgd_down_retry_interval_s>
      <modify_hosts>1</modify_hosts>
      <scheduling_info>
         <enabled>1</enabled>
         <fallback_action>deny</fallback_action>
         <schedule_item>
            <days_of_week>2,4</days_of_week>
            <start_time>06:00</start_time>
            <end_time>18:00</end_time>
         </schedule_item>
      </scheduling_info>
      <profiles>
         <profile>
            <id>999</id>
            <use_exclusion_list>1</use_exclusion_list>
         </profile>
         <profile>
            <id>0</id>
            <cate_ver>6</cate_ver>
            <description>deny</description>
            <name>deny</name>
            <log_all_urls>1</log_all_urls>
            <log_user_initiated_traffic>1</log_user_initiated_traffic>
            <categories>
               <fortiguard>
```

```
            <enabled>1</enabled>
            <url>fgd1.fortigate.com</url>
            <rate_ip_addresses>1</rate_ip_addresses>
            <action_when_unavailable>deny</action_when_unavailable>
            <use_https_rating_server>0</use_https_rating_server>
         </fortiguard>
         <category>
            <id>0</id>
            <action>deny</action>
            <isdb_objects>
               <object>
                  <owner>30</owner>
                  <app>103</app>
                  <action>allow</action>
               </object>
            </isdb_objects>
         </category>
         <category>
            <id>1</id>
            <action>deny</action>
         </category>
         <category>
            <id>2</id>
            <action>deny</action>
         </category>
         <category>
            <id>3</id>
            <action>deny</action>
         </category>
         <category>
            <id>4</id>
            <action>deny</action>
         </category>
         <category>
            <id>5</id>
            <action>deny</action>
         </category>
      </categories>
      <urls>
         <url>
            <address>
            <![CDATA[www.777.com]]>
            </address>
            <type>simple</type>
            <action>deny</action>
            <referrer>google.com</referrer>
         </url>
         <url>
            <address>
            <![CDATA[www.fortinet.com]]>
            </address>
            <type>simple</type>
            <action>allow</action>
         </url>
      </urls>
      <webbrowser_plugin>
         <enabled>0</enabled>
```

```
            <sync_mode>0</sync_mode>
            <addressbar_only>0</addressbar_only>
            <ignore_data_url>1</ignore_data_url>
            <force_enable_in_private_mode>1</force_enable_in_private_mode>
         </webbrowser_plugin>
         <safe_search>
            <enabled>0</enabled>
            <search_engines>
               <enabled>0</enabled>
            </search_engines>
            <youtube_education_filter>
               <enabled>0</enabled>
               <filter_id>
                  <![CDATA[]]>
                  </filter_id>
               </youtube_education_filter>
         </safe_search>
      </profile>
   </profiles>
</webfilter>
</forticlient_configuration>
```

The following table provides the XML tags for web filter, as well as the descriptions and default values where applicable.

XML tag	Description	Default value
`<enable_filter>`	Enable web filter. Boolean value: `[0 | 1]`	`1`
`<enabled>`	Enable FortiGuard distribution network querying service. Boolean value: `[0 | 1]`	`1`
`<current_profile>`	(Optional) Selected profile ID. If using the advanced configuration on the FortiGate for endpoint control, set this to `1000`. The value should always match the `<profile><id>` selected.	
`<partial_match_host>`	FortiClient treats a hostname that is a substring of the specified path as a full match. Boolean value: `[0 | 1]`	`0`
`<disable_when_managed>`	If enabled, FortiClient disables web filter when connected to a FortiGate using Endpoint Control. Boolean value: `[0 | 1]`	
`<keep_extension_when_managed>`	If disabled, the FortiClient Web Filter extension is uninstalled when the endpoint goes from being on- to off-net. For Firefox, the Web Filter extension is not automatically uninstalled, due to the Firefox default behavior. Instead, you can manually remove the extension. This is a Firefox limitation. Boolean value: `[0 | 1]`	`1`

XML tag	Description	Default value
<max_violations>	Maximum number of violations stored at any one time. Enter a number from 250 to 5000.	5000
<max_violation_age>	Maximum age in days of a violation record before FortiClient culls it. Enter a number from 1 to 90.	90
<block_malicious_websites>	Configure whether to block websites with security risk categories (group 5). Boolean value: [0 | 1]	0
<bypass_private_ip>	Enable bypassing private IP addresses. Boolean value: [0 | 1]	1
<browser_read_time_threshold>	Configure the threshold in seconds for web browser to be considered idle. When a web browser is idle for longer than the threshold, FortiClient considers the web browser idle and does not calculate the time.	90
<https_block_method>	Control how FortiClient behaves when Web Filter blocks an HTTPS site: • If set to 0, FortiClient displays an in-browser message that the site is not reachable or that it is unable to reach the site, that your connection is not private, or that the site is not secure. • If set to 1, FortiClient shows a bubble notification to the user. The connection fails/times out. • If set to 2, the connection fails/times out with no notification to the user.	0
<use_transparent_proxy>	Enable the com.fortinet.forticlient.macos.proxy system extension, which works as a proxy server to proxy a TCP connection. macOS manages the extension's connection status and other statistics. This resolves the issue that Web Filter fails to work when SSL and IPsec VPN are connected. FortiClient (macOS) automatically installs the extension on an M1 Pro or newer macOS device. You only need to enable this option on a macOS device with an Intel or M1 chip. See Special notices. This element does not affect Windows endpoints.	
<request_timeout>	Configure the desired timeout value in seconds for a Web Filter site rating request to FortiGuard times out. You can configure a value between 1 to 30 seconds.	7
<wildcard_match_root_domain>	FortiClient applies wildcard matching to the sites in the exclusion list, even if they are not configured with wildcard characters.	0

XML tag	Description	Default value
	For example, if you configured office365.com in the exclusion list and enable <wildcard_match_root_domain>, FortiClient excludes (.*\.)?office365\.com. Enabling <wildcard_match_root_domain> causes the exclusion list to include subdomains such as outlook.office365.com. Boolean value: [0 | 1]	
<enable_https_deep_inspection>	Enable HTTPS deep inspection on FortiClient (macOS) and (Linux) endpoints. When HTTPS deep inspection is enabled, FortiClient can proxy HTTPS requests and rate whole HTTPS URL requests. Otherwise, FortiClient can only rate domain URLs for HTTPS requests. Boolean value: [0 | 1]	1
<interception_mode>	Only modify this element if you are experiencing recurrent blue screen of death (BSOD) issues. When enabled, the system is in interception mode. In this mode, all HTTPS and HTTP-related packets are intercepted and sent to the Web Filter daemon for processing. After processing, the packets are forwarded to the driver for injection, operating in a synchronous manner. If Web Filter blocks access to a webpage, the browser displays a block page. When disabled, the system operates in non-interception mode. In this case, all HTTPS and HTTP packets are duplicated and sent to the Web Filter Daemon for processing, while the original packets continue to pass through the network stack. The daemon processes the duplicate packets and instructs the driver to terminate connections if it detects any suspicious packets. If Web Filter blocks access to a webpage, the browser does not display a block page. Boolean value: [0 | 1]	1
<fgd_down_retry_interval_s>	Configure the number of seconds that FortiClient blocks all sites once it determines that the FortiGuard rating server is down. The minimum interval is one second.	
<modify_hosts>	If the Web Filter extension is enabled and <modify_hosts> is disabled, entries for YouTube safe search are not added to the hosts file. Instead, the extension handles safe search using HTTP header replacement. Boolean value: [0 | 1]	
<scheduling_info> elements		
<enabled>	Enable to have Web Filter settings only take effect during the configured schedule.	0

XML tag	Description	Default value
<fallback_action>	Configure the desired action for Web Filter to take for web traffic outside of the scheduled times: • allow: allow full, unfiltered access to all websites • deny: deny access to any website	deny
<scheduling_info><schedule_item> elements		
<days_of_week>	Configure the days of the week for the schedule: • 1: Sunday • 2: Monday • 3: Tuesday • 4: Wednesday • 5: Thursday • 6: Friday • 7: Saturday Enter multiple days by separating the numbers with a comma. For example, to enable the schedule on Monday and Wednesday, enter <days_of_week>2,4</days_of_week>.	1
<start_time>	Configure the desired time in 24-hour clock format for the Web Filter settings to start on the selected days of the week.	06:00
<end_time>	Configure the desired time in 24-hour clock format for the Web Filter settings to end on the selected days of the week.	18:00
<profiles><profile><safe_search> element		
<enabled>	Enable safe search. When you enable safe search, the endpoint's Google search is set to restricted mode, and YouTube access is set to strict restricted access. To set YouTube access to moderate restricted or unrestricted YouTube access, you can disable safe search and configure Google search and YouTube access with the Google Admin Console instead of with EMS. You can enable Safe Search on the Video Filter and Web Filter profiles. When Safe Search is enabled on both profiles, the more restrictive settings are applied to YouTube. Boolean value: [0 | 1]	
<profiles><profile><safe_search><search_engines><engine> element		
<enabled>	Enable safe search for the predefined search engines. Boolean value: [0 | 1]	

The <profiles> XML element may have one or more profiles, defined in the <profile> tag. Each <profile>, in turn, has one or more <category>, <url> and <safe_search> tags, along with other elements.

The following table provides profile XML tags, the description, and the default value (where applicable).

XML tag	Description	Default value
`<profile>` elements		
`<id>`	Unique ID. A number to define the profile.	
`<cate_ver>`	FortiGuard category version used in this profile. A number.	`6`
`<description>`	Summary describing this profile.	
`<name>`	A descriptive name for the profile.	
`<log_all_urls>`	Configure whether to log all URLs. When this setting is `0`, FortiClient only logs URLs as specified by per-category or per-URL settings. When this setting is `1`, FortiClient logs all URLs. Boolean value: `[0 | 1]`	
`<log_user_initiated_traffic>`	Configure what traffic to record. When this setting is `0`, FortiClient records all traffic. When this setting is `1`, FortiClient records only traffic that the user initiates. Boolean value: `[0 | 1]`	
`<profile><categories><fortiguard>` elements		
`<url>`	FortiGuard server IP address or FQDN.	`fgd1.fortigate.com`
`<enabled>`	Enable using FortiGuard servers. Boolean value: `[0 | 1]`	`1`
`<rate_ip_addresses>`	Rate IP addresses. Boolean value: `[0 | 1]`	`1`
`<action_when_unavailable>`	Configure the action to take with all websites when FortiGuard is temporarily unavailable. FortiClient takes the configured action until it reestablishes contact with FortiGuard. Available options are: • `allow`: Allow full, unfiltered access to all websites • `deny`: Deny access to any website • `warn`: Display an in-browser	`deny`

XML tag	Description	Default value
	warning to user with an option to proceed to the website • `monitor`: Monitor site access	
`<use_https_rating_server>`	By default, Web Filter sends URL rating requests to the FortiGuard Anycast rating server via TCP protocol. You can instead enable Web Filter to send the requests to the FortiGuard legacy server via UDP protocol. Boolean value: `[0 | 1]`	`0`
`<profile><categories><category>` elements		
`<id>`	Unique ID. A number. The valid set of category IDs is predefined, and is listed in exported configuration files.	
`<action>`	Action to perform on matching network traffic. Enter one of the following: • `allow` • `deny` • `warn` • `monitor`	
`<profile><categories><category><isdb_objects><object>` elements	These elements only apply to the unrated category, which has an id of 0. This feature allows you to configure actions for specific cloud applications that FortiGuard categorizes as unrated using the Internet Services Database (ISDB).	
`<owner>`	Owner ID of the cloud application in ISDB.	
`<app>`	Application ID of the cloud application in ISDB.	
`<action>`	Action to perform on matching network traffic. Enter one of the following: • `allow` • `deny` • `warn`	

XML tag	Description	Default value
	• monitor	
<profile><urls><url> elements		
<address>	The web address in which <action> (allow or deny) is performed. This should be wrapped in a CDATA tag. For example: <![CDATA[www.777.com]]>	
<action>	Action to perform on matching network traffic. Enter one of the following: [allow | deny]	
<referrer>	Enter a specific referrer or host to allow, block, or monitor. You can provide the full URL or only the domain name. If the end user visits the URL through the referrer provided, EMS considers the rule a match and applies the specified action. If the end user visits the URL directly or through a different referrer, EMS does not consider the rule a match and does not apply the specified action. This option is only available for FortiClient Windows, macOS, Linux, and Chromebooks.	
<profile><webbrowser_plugin> elements		
<enabled>	Enable a web browser plugin for HTTPS web filtering. This improves detection and enforcement of Web Filter rules on HTTPS sites. When this option is enabled, the user must open the browser to approve installing the new plugin. Currently this feature is only supported when using the Chrome browser on a Windows machine.	1

XML tag	Description	Default value
<sync_mode>	When this option is enabled, the web browser waits for a response from an HTTPS request before sending another HTTPS request.	0
<addressbar_only>	Enable the plugin to only check domains, even if the full URL is provided. This allows for faster processing. When this option is disabled, the plugin checks full URLs.	0
<ignore_data_url>	If this tag does not exist, by default, FortiClient treats it as false. When this option is enabled, the plugin bypasses Base64 data URLs. The format for data URLs is as follows: data:application/text(or other MIME type); base64,XXXXXXX... The plugin does not bypass the following data formats since they have valid URLs within the data protocol: • data:https://xxxxx • blob:http://xxxx Instead, the plugin uses the https://xxxx inside to rate the download.	
<force_enable_in_private_mode>	Configure whether to force run the FortiClient Web Filter extension in incognito or private mode:	1

XML tag	Description	Default value
	As Chrome and Edge explicitly prevent extensions from silently enabling extension access in Incognito for user privacy and security, when this option is enabled, Chrome and Edge users must manually enable an option in the browser to allow running the FortiClient Web Filter extension for Incognito (private browsing). FortiClient cannot force enable the FortiClient Web Filter extension for Incognito in Chrome and Edge.	
	Enabled • **(Firefox)** The FortiClient Web Filter extension will be active in incognito or private mode. • **(Chrome or Edge)** Users will be prompted to enable the option in the browser to allow running the FortiClient Web Filter extension for Incognito. If the user does not	

XML tag	Description	Default value
	enable the option in the browser as requested, Internet access will be disabled completely for both regular and private browsing. **Disabled** The FortiClient Web Filter extension will not run in Incognito. Web Filter will not apply to websites accessed in Incognito. Boolean value: `[0 | 1]`	

The `<safe_search>` element has two main components:

- Search engines `<search_engines>`
  Users may define safe search parameters for each of the popular search engines: Bing and Yandex. Subsequent use of the engines for web searches have Safe Search enabled.
- YouTube education filter `<youtube_education_filter>`
  Educational institutions with valid YouTube education ID can provide this in the `<youtube_education_filter>` element to restrict YouTube contents appropriately.

The following table provides profile XML tags and the description. See the `<safe_search>` listing in the previous pages for examples of each tag.

XML tag	Description	Default value
`<profiles><profile><safe_search><search_engines><engine>` elements		
`<name>`	Name of the Safe Search profile.	
`<host>`	The search engine's FQDN. FortiClient monitors attempts to visit this address.	
`<url>`	The URL substring to match or monitor, along with the FQDN.	
`<query>`	The query string appended to the URL.	

XML tag	Description	Default value
<safe_search_string>	The correct safe search string appended to the URL for the specified engine.	
<cookie_name>	The name of the cookie to send the search engine.	
<cookie_value>	The cookie value to send the search engine.	
<profiles><profile><safe_search><youtube_education_filter> elements		
<enabled>	Enable YouTube education filter. Boolean value: [0 | 1]	
<filter_id>	The institution's education identifier.	

Other than the <name> and <enabled> elements, the values for each of the elements in the previous table should be wrapped in <![CDATA[]]> XML tags. Here is an example for a <host> element taken from the <safe_search> listing.

```
<host><![CDATA[yandex\..*]]></host>
```

See Manage your YouTube settings for more information on YouTube for schools and the education filter.

The following is a list of all Web Filter categories including the category <id> and category name:

```
0 ==> Unrated
1 ==> Drug Abuse
2 ==> Alternative Beliefs
3 ==> Hacking
4 ==> Illegal or Unethical
5 ==> Discrimination
6 ==> Explicit Violence
7 ==> Abortion
8 ==> Other Adult Materials
9 ==> Advocacy Organizations
11 ==> Gambling
12 ==> Extremist Groups
13 ==> Nudity and Risque
14 ==> Pornography
15 ==> Dating
16 ==> Weapons (Sales)
17 ==> Advertising
18 ==> Brokerage and Trading
19 ==> Freeware and Software Downloads
20 ==> Games
23 ==> Web-based Email
24 ==> File Sharing and Storage
25 ==> Streaming Media and Download
26 ==> Malicious Websites
28 ==> Entertainment
29 ==> Arts and Culture
30 ==> Education
31 ==> Finance and Banking
33 ==> Health and Wellness
34 ==> Job Search
35 ==> Medicine
36 ==> News and Media
```

```
37 ==> Social Networking
38 ==> Political Organizations
39 ==> Reference
40 ==> Global Religion
41 ==> Search Engines and Portals
42 ==> Shopping
43 ==> General Organizations
44 ==> Society and Lifestyles
46 ==> Sports
47 ==> Travel
48 ==> Personal Vehicles
49 ==> Business
50 ==> Information and Computer Security
51 ==> Government and Legal Organizations
52 ==> Information Technology
53 ==> Armed Forces
54 ==> Dynamic Content
55 ==> Meaningless Content
56 ==> Web Hosting
57 ==> Marijuana
58 ==> Folklore
59 ==> Proxy Avoidance
61 ==> Phishing
62 ==> Plagiarism
63 ==> Sex Education
64 ==> Alcohol
65 ==> Tobacco
66 ==> Lingerie and Swimsuit
67 ==> Sports Hunting and War Games
68 ==> Web Chat
69 ==> Instant Messaging
70 ==> Newsgroups and Message Boards
71 ==> Digital Postcards
72 ==> Peer-to-peer File Sharing
75 ==> Internet Radio and TV
76 ==> Internet Telephony
77 ==> Child Education
78 ==> Real Estate
79 ==> Restaurant and Dining
80 ==> Personal Websites and Blogs
81 ==> Secure Websites
82 ==> Content Servers
83 ==> Child Abuse
84 ==> Web-based Applications
85 ==> Domain Parking
86 ==> Spam URLs
88 ==> Dynamic DNS
89 ==> Auction
90 ==> Newly Observed Domain
91 ==> Newly Registered Domain
92 ==> Charitable Organizations
93 ==> Remote Access
94 ==> Web Analytics
95 ==> Online Meeting
```

Video Filter

Video filter XML configurations are contained in the <videofilter></videofilter> tags:

```
<forticlient_configuration>
	<videofilter>
		<youtube>
			<advanced>
				<safe_search>
					<enabled>0</enabled>
					<restriction_level>moderate</restriction_level>
				</safe_search>
				<channels>
					<channel>
						<id>BTSport</id>
						<comments/>
						<action>deny</action>
					</channel>
				</channels>
				<enabled>1</enabled>
				<videos>
					<video>
						<name>blocked_video</name>
						<link>youtube.com/watch?v=m2YJ7aR25P0</link>
						<comments/>
						<action>deny</action>
					</video>
				</videos>
				<hide_comments>0</hide_comments>
			</advanced>
			<category>
				<enabled>1</enabled>
			</category>
		</youtube>
		<fortiguard>
			<action_when_unavailable>allow</action_when_unavailable>
			<restrict_services_to_regions>USA<restrict_services_to_regions>
		</fortiguard>
		<categories>
			<category>
				<id>0</id>
				<action>allow</action>
			</category>
			<category>
				<id>1</id>
				<action>allow</action>
			</category>
			<category>
				<id>2</id>
				<action>allow</action>
```

```
                        </category>
                        <category>
                                <id>3</id>
                                <action>allow</action>
                        </category>
                        <category>
                                <id>4</id>
                                <action>allow</action>
                        </category>
                        <category>
                                <id>5</id>
                                <action>allow</action>
                        </category>
                        <category>
                                <id>6</id>
                                <action>allow</action>
                        </category>
                        <category>
                                <id>7</id>
                                <action>allow</action>
                        </category>
                        <category>
                                <id>8</id>
                                <action>allow</action>
                        </category>
                        <category>
                                <id>9</id>
                                <action>allow</action>
                        </category>
                        <category>
                                <id>10</id>
                                <action>allow</action>
                        </category>
                </categories>
                <enabled>0</enabled>
        </videofilter>
```

```
<forticlient_configuration>
```

The following table provides the XML tags for web filter, as well as the descriptions and default values where applicable.

XML tag	Description	Default value
`<enabled>`	Enable video filter. This feature is only available for Windows endpoints. This feature requires web filtering and`<webfilter><profiles><profile><webbrowser_plugin>` to be enabled. This feature is only available for FortiClient (Windows) endpoints. Boolean value: `[0 | 1]`	

XML tag	Description	Default value
<youtube><advanced> elements		
<enabled>	Enable advanced settings for YouTube filtering. Boolean value: [0 | 1]	
<safe_search>	When enabling Safe Search, you can configure the restriction level to strict or moderate. This setting affects the content that endpoint users can access via YouTube. You can enable Safe Search on the Video Filter and Web Filter profiles. When Safe Search is enabled on both profiles, the more restrictive settings are applied to YouTube.	
<channels>	Configure access for a specific YouTube channel. In the <id> element, enter the YouTube channel ID. In the <action> field, enter the desired action for the channel. If you block access to a channel and allow access to a specific video that belongs to the blocked channel, FortiClient blocks access to the video. The action configured for the channel overrides the action configured for the specific video.	
<videos>	Configure access for a specific YouTube video. In the <link> element,enter the video URL in the format: youtube.com/watch?v=<video ID>. In the <action> field, enter the desired action for the video.	
<hide_comments>	Hide YouTube comments from end users. Boolean value: [0 | 1]	
<youtube><category>	?	
<fortiguard> elements		
<action_when_unavailable>	Configure an action for FortiClient to take for YouTube videos when it cannot reach the FortiGuard server.	
<restrict_services_to_regions>	Configure the FortiGuard server location. FortiClient connects to FortiGuard to query for URL ratings. You can enter USA to configure the FortiGuard U.S. server. Otherwise, FortiClient uses the global FortiGuard server. The URLs connected to for each server location are as follows: • Global: fctguard.fortinet.net • U.S.: fctusguard.fortinet.net	0
<categories>	For each category, configure the desired action. The following lists available categories and their IDs: • Not Rated: 0 • Business: 1 • Entertainment: 2	

XML tag	Description	Default value
	• Games: 3 • Knowledge: 4 • Lifestyle: 5 • Music: 6 • News: 7 • People: 8 • Society: 9 • Sports: 10	

Application firewall

The <firewall> </firewall> XML tags contain application firewall configuration data. The set of elements consists of two sections:

Section	Description
General options	Options that apply to all application firewall activities.
Profiles	Defines applications and the actions to apply to them.

```
<forticlient_configuration>
   <firewall>
      <enabled>1</enabled>
      <app_enabled>1</app_enabled>
      <enable_exploit_signatures>0</enable_exploit_signatures>
      <candc_enabled>1</candc_enabled>
      <current_profile>0</current_profile>
      <default_action>Pass</default_action>
      <show_bubble_notifications>0</show_bubble_notifications>
      <max_violations>250</max_violations>
      <max_violations_age>7</max_violations_age>
      <bypass_3rd_party_packets>0</bypass_3rd_party_packets>
      <profiles>
         <profile>
            <id>1000</id>
            <rules>
               <rule>
                  <enabled>1</enabled>
                  <action>Block</action>
                  <compliance>1</compliance>
                  <application>
                     <id>34038,34039</id>
                  </application>
               </rule>
               <rule>
                  <action>Block</action>
                  <compliance>1</compliance>
                  <enabled>1</enabled>
```

```
                  <category>
                     <id>8</id>
                  </category>
               </rule>
               <rule>
                  <action>Pass</action>
                  <compliance>1</compliance>
                  <enabled>1</enabled>
                  <category>
                     <id>7,19,29</id>
                  </category>
               </rule>
               <rule>
                  <action>Block</action>
                  <compliance>0</compliance>
                  <enabled>1</enabled>
                  <category>
                     <id>1,2,3</id>
                  </category>
               </rule>
               <rule>
                  <action>Pass</action>
                  <compliance>0</compliance>
                  <enabled>1</enabled>
                  <category>
                     <id>All</id>
                  </category>
               </rule>
               <rule>
                  <action>Pass</action>
                  <compliance>0</compliance>
                  <enabled>1</enabled>
                  <application>
                     <id>0</id>
                  </application>
               </rule>
               <rule>
                  <enabled>1</enabled>
                  <action>pass</action>
                  <ips>
                     <id>12449</id>
                  </ips>
               </rule>
               </rules>
            </profile>
      </profiles>
   </firewall>
</forticlient_configuration>
```

The following table provides the XML tags for application firewall, as well as the descriptions and default values where applicable.

XML tag	Description	Default value
<enabled>	Enable application firewall.	1

XML tag	Description	Default value
	Boolean value: [0 | 1]	
<app_enabled>	Enable application firewall. Boolean value: [0 | 1]	
<enable_exploit_signatures>	Enable detection of evasive exploits. Boolean value: [0 | 1]	0
<candc_enabled>	Enable detection of a connection to a botnet command and control server. If *Block Known Communication Channels Used by Attackers* is enabled on the Malware Protection profile and this option is disabled, *Block Known Communication Channels Used by Attackers* takes precedence and FortiClient enables Command and Control detection. Boolean value: [0 | 1]	
<current_profile>	Currently selected profile ID.	
<default_action>	Action to enforce on traffic that does not match any of the profiles defined. Enter one of the following: • block • reset • pass	pass
<show_bubble_notifications>	Display a bubble message each time FortiClient blocks an application for matching a profile. Boolean value: [0 | 1]	
<max_violations>	Maximum number of violations stored at any one time. A number from 250 to 5000	5000
<max_violation_age>	Maximum age in days of a violation record before it is culled. A number from 1 to 90.	90
<bypass_3rd_party_packets>	Enable bypassing packets that third party applications generate. Boolean value: [0 | 1]	0

The <profiles> tag may contain one or more <profile> tags, each of which has a <rules> element. The <rules> element may, itself, have zero or more <rule> tags.

The following filter elements may be used to define applications in a <rule> tag:

```
<category>
<vendor>
<behavior>
<technology>
<protocol>
<application>
<popularity>
```

If the <application> element is present, all other sibling elements (listed above) are ignored. If it is not, a given application must match all of the provided filters to trigger the rule.

Each of these seven elements is a container for the tag: <ids>, which is a list of the identifiers (numbers) selected for that particular filter. The full <firewall> profile listed at the beginning of this section shows several examples of the use of filters within the <rule> element. Using an <ids> value all selects all matching applications.

The following table provides profile element XML tags, the description, and the default value (where applicable).

XML tag	Description	Default value
<profile> element		
<id>	Unique ID. A unique ID number.	
<profile><rules><rule> elements		
<action>	Action to enforce on traffic that matches this rule. Select one of the following: • block • reset • pass	
<compliance>	Specifies whether the rule is a compliance or regular rule. When set to 1, this is a compliance rule. When set to 0 or the tag does not exist, this is a FortiClient profile rule. For more information, see the *FortiClient Administration Guide*. Boolean value: [0 | 1]	
<enabled>	Enable this rule. Boolean value: [0 | 1]	1
<category>	Application categories to apply <action> on.	csv list
<vendor>	Application vendors to apply <action> on.	csv list
<behavior>	Application behavior to apply <action> on.	csv list
<technology>	Technologies used by the applications to apply <action> on.	csv list
<protocol>	Protocols used by the applications to apply <action> on.	csv list
<application>	Identifiers (IDs) of the applications to apply <action> on.	csv list
<popularity>	Popularity of the applications to apply <action> on.	csv list
<ips><id>	IPS signature version to apply <action> on.	

Rule example

In the following example, FortiClient uses the first rule and the second rule as a FortiClient profile rule:

```
<rules>
   <rule>
      <enabled>1</enabled>
      <action>block | warn | monitor</action>
      <compliance>1</compliance>
      <filter>
```

```
            <application>
               <ids>36373</ids>
            </application>
         </filter>
      </rule>
      <rule>
         <enabled>1</enabled>
         <action>block | warn | monitor</action>
         <filter>
            <category>
               <ids>1</ids>
            </category>
         </filter>
      </rule>
   </rules>
```

Vulnerability scan

The <vulnerability_scan></vulnerability_scan> XML tags contain vulnerability scan configurations.

```
<forticlient_configuration>
   <vulnerability_scan>
      <enabled>1</enabled>
      <scan_on_registration>1</scan_on_registration>
      <scan_on_signature_update>1</scan_on_signature_update>
      <auto_patch>
         <level>critical</level>
      </auto_patch>
      <windows_update>1</windows_update>
      <proxy_enabled>0</proxy_enabled>
      <exempt_manual>1</exempt_manual>
      <send_exempted_apps_to_ems>1</send_exempted_apps_to_ems>
      <show_fct_vuln_popup>1</show_fct_vuln_popup>
      <exemptions>
         <exemption>Google Chrome</exemption>
         <exemption>Java JDK</exemption>
      </exemptions>
      <exempt_no_auto_patch>1</exempt_no_auto_patch>
      <scheduled_scans>
         <schedule>
            <enable_schedule>1</enable_schedule>
            <repeat>1</repeat>
            <day>1</day>
            <time>19:30</time>
         </schedule>
         <automatic_maintenance>
            <scan_on_maintenance>0</scan_on_maintenance>
            <maintenance_period></maintenance_period>
            <maintenance_deadline></maintenance_deadline>
         </automatic_maintenance>
      </scheduled_scans>
      <vcm_expire_days>10</vcm_expire_days>
   </vulnerability_scan>
```

```
</forticlient_configuration>
```

The following table provides the XML tags for Vulnerability Scan, as well as the descriptions and default values where applicable.

XML tag	Description	Default value
<enabled>	Enable vulnerability scan.	
<scan_on_ registration>	Specifies whether to start a vulnerability scan when FortiClient registers to a FortiGate. Boolean value: [0 | 1]	
<scan_on_signature_ update>	Specifies whether to start a vulnerability scan when FortiClient updates its signatures. Boolean value: [0 | 1]	
<auto_patch>	Specifies whether to automatically install patches. Use the <level> element to enable and disable automatic patch installation.	
<level>	Specify whether to patch vulnerabilities with a severity higher than the defined level. When set to 0, FortiClient disables this setting and does not automatically install patches when it detects vulnerabilities. When set to info, FortiClient automatically installs all patches when it detects vulnerabilities. Configure one of the following: • 0 • critical • high • medium • low • info	
<windows_update>	Specifies whether to scan Windows updates and third party application updates. When set to 1, FortiClient scans Windows updates and third party application updates. When set to 0, FortiClient scans only third party application updates. Boolean value: [0 | 1]	1
<proxy_enabled>	Enable using proxy settings configured in FortiClient when downloading updates for vulnerability patches. Boolean value: [0 | 1]	0
<exempt_manual>	Specifies whether to exempt from vulnerability scanning any applications that require the endpoint user to manually install patches. Boolean value: [0 | 1]	0
<send_exempted_apps_ to_ems>	Specifies whether to send vulnerability information from applications that are exempt from Vulnerability Scan to EMS. Boolean value: [0 | 1]	0

XML tag	Description	Default value
<show_fct_vuln_popup>	FortiClient displays a *Vulnerabilities Scan Summary* popup after it completes a scan. The user can click the *View All Vulnerabilities* button in the popup to go to the *Vulnerability Scan* tab in FortiClient. Boolean value: [0 | 1]	1
<exemptions>	Identifies the names of applications that are exempted.	
<exempt_no_auto_patch>	Specifies whether to exempt any applications that FortiClient can automatically patch from vulnerability scanning. Boolean value: [0 | 1]	0
<scheduled_scans><schedule> elements		
<enable_schedule>	Enable scheduled vulnerability scans. Boolean value: [0 | 1]	
<repeat>	Configure the frequency of scans: • 0: daily scan • 1: weekly scan • 2: monthly scan	
<day>	Used only for weekly scan and monthly scan. If the <repeat> tag is set to 0 (daily), the <day> tag is ignored. If the <repeat> tag is set to 1 (weekly), <day> is the day of the week to run scan. Select one of the following: • 1: Sunday • 2: Monday • 3: Tuesday • 4: Wednesday • 5: Thursday • 6: Friday • 7: Saturday If the <repeat> tag is set to 2 (monthly), <day> is the date of each month to run a scan. Enter a number from 1 to 31.	The default is the date that the policy was installed from FortiGate.
<time>	Configure the time to run the scan. Specify a time value in 24-hour clock. The following shows an example configuration for a scan that runs at 7:30 PM (19:30 on a 24-hour clock) daily: <schedule> <repeat>0</repeat> <time>19:30</time> </schedule>	The default is the time that the policy was installed from FortiGate.
<scheduled_scans><automatic_maintenance> elements		

XML tag	Description	Default value
This configures vulnerability scans to run as part of Windows automatic maintenance. Adding FortiClient vulnerability scans to the Windows automatic maintenance queue allows the system to choose an appropriate time for the scan that minimally impact the user, PC performance, and energy efficiency. See Automatic Maintenance.		
<scan_on_maintenance>	Enable running vulnerability scan as part of Windows automatic maintenance. Boolean value: [0 | 1]	0
<maintenance_period>	Specify how often vulnerability scanning must be started during automatic maintenance. Enter the desired period in the format PnYnMnDTnHnMnS, where nY is the number of years, nM is the number of months, nD is the number of days, T is the date/time separator, nH is the number of hours, nM is the number of minutes, and nS is the number of seconds. For example, to configure a period of five minutes, you would enter the following: <maintenance_period>PT5M</maintenance_period> To configure a period of one month, four days, two hours, and five minutes, you would enter the following: <maintenance_period>P1M4DT2H5M</maintenance_period>	
<maintenance_deadline>	Specify when Windows must start vulnerability scanning during emergency automatic maintenance, if vulnerability scanning did not complete during regular automatic maintenance. This value must be greater than the <maintenance_period> value. Enter the desired deadline in the format PnYnMnDTnHnMnS. For details on this format, see <maintenance_period> above.	
<vcm_expire_days>	Configure the number of days after which FortiClient deletes Vulnerability Scan logs. If this element is not configured, by default, FortiClient deletes Vulnerability Scan logs after 30 days.	

Sandboxing

The following lists sandboxing general attributes:

```
<forticlient_configuration>
   <sandboxing>
      <enabled>1</enabled>
      <type>appliance</type>
      <address>n.n.n.n</address>
      <response_timeout>30</response_timeout>
      <when>
         <executables_on_removable_media>1</executables_on_removable_media>
         <executables_on_mapped_nw_drives>1</executables_on_mapped_nw_drives>
```

```
            <web_downloads>1</web_downloads>
            <email_downloads>1</email_downloads>
         </when>
         <submit_by_extensions>
            <enabled>1</enabled>
            <use_custom_extensions>1</use_custom_extensions>
            <custom_extensions>.exe,.dll,.com</customextensions>
         </submit_by_extensions>
         <exceptions>
            <exclude_files_from_trusted_sources>1</exclude_files_from_trusted_sources>
            <exclude_files_and_folders>0</exclude_files_and_folders>
            <folders>
               <folder>C:\path1\to\folder\,C:\path2\to\folder\</folder>
            </folders>
            <files>
               <file>C:\path\to\file1.txt, C:\path\to\file2.txt</file>
            </files>
         </exceptions>
         <inclusions>
            <include_files_and_folders>1</include_files_and_folders>
            <folders>
               <folder>C:\folder1,C:\path2\to\folder2\</folder>
            </folders>
            <files>
               <file>C:\path\to\file3.txt, C:\path\to\file4.txt</file>
            </files>
         </inclusions>
         <remediation>
            <action>quarantine</action>
            <on_error>block</on_error>
         </remediation>
         <detect_level>4</detect_level>
         <shell_integration>
            <hide_sandbox_scan>0</hide_sandbox_scan>
         </shell_integration>
         <notification_type>0</notification_type>
         <max_size>200</max_size>
      </sandboxing>
   </forticlient_configuration>
```

The following table provides the XML tags for Sandbox, as well as the descriptions and default values where applicable.

XML tag	Description	Default value
`<enabled>`	Enable Sandbox Detection. Boolean value: `[0 | 1]`	
`<type>`	Specify the type of FortiSandbox unit.	
`<address>`	Specify the IP address or FQDN of the FortiSandbox unit.	
`<response_timeout>`	Specify the response timeout value in seconds. File access is allowed if FortiSandbox results are not received when the timeout expires. Set to `-1` to infinitely restrict access to the file.	

XML tag	Description	Default value
<when> elements		
<executables_on_removable_media>	Submit all files executed on removable media, such as USB drives, to FortiSandbox for analysis. Boolean value: [0 | 1]	
<executables_on_mapped_nw_drives>	Submit all files executed from mapped network drives. Boolean value: [0 | 1].	
<web_downloads>	Submit all web downloads. Boolean value: [0 | 1].	
<email_downloads>	Submit all email downloads. Boolean value: [0 | 1].	
<submit_by_extension> elements		
<enabled>	Submit specified file extensions to FortiSandbox for analysis. When disabled, FortiClient does not submit any file extensions to FortiSandbox, but can still retrieve signatures from FortiSandbox. Boolean value: [0 | 1].	1
<use_custom_extensions>	Enable using a custom list of file extensions. If enabled, configure the custom list of file extensions using the <custom_extensions> element below. If disabled, the default list of file extensions is used: exe, dll, msi, cpl, ocx, ps1, swf, swz, jsfl, flv, swc, fla, xfl, jsfl, 7z, xz, bz2, gz, tar, zip, rar, arj, z, pdf, doc, docx, docm, dotx, dotm, dot, rtf, mht, mhtml, odt, xlsx, xl, xlsm, xlsb, xltx, xltm, xls, xlt, xlam, xlw, pptx, pptm, ppt, xps, potx, potm, pot, thmx, pps, ppsx, ppsm, ppt, ppam, odp Boolean value: [0 | 1].	0
<custom_extensions>	If using a custom list of file extensions, enter the list of desired file extensions, separated only by commas. The example submits .exe, .dll, and .com files to FortiSandbox for analysis.	
<exceptions> elements		
<exclude_files_from_trusted_sources>	Exclude files signed by trusted sources from FortiSandbox submission. Boolean value: [0 | 1].	
<exclude files_and_folders>	Exclude specified folders/files from FortiSandbox submission. You must also create the exclusion list. Boolean value: [0 | 1].	
<files>	Specify a list of files to exclude. Separate multiple files with a comma. Example: C:\path\to\file1.txt, C:\path\to\file2.txt	

XML tag	Description	Default value
<folders>	Specify a list of folders to exclude. Separate multiple folders with a comma. Example: C:\path1\to\folder\,C:\path2\to\folder\	
<inclusions> elements		
<include files_and_ folders>	Include specified folders/files in FortiSandbox submission. You must also create the inclusion list. Boolean value: [0 | 1].	
<files>	Specify a list of files to include. Separate multiple files with a comma. Example: C:\path\to\file3.txt, C:\path\to\file4.txt	
<folders>	Specify a list of folders to include. Separate multiple folders with a comma. Example: C:\folder1,C:\path2\to\folder2\.	
<remediation> elements		
<action>	Specify how to handle infected files. FortiClient can quarantine infected files. Enter one of the following: • quarantine: quarantine infected files • alert: alert the user about infected files but allow access to infected files	
<on_error>	Specify how to handle files when FortiClient cannot reach FortiSandbox. You can block or allow access to files. Enter one of the following: • block • allow	
<detect_level>	When the value is 4: If FortiSandbox returns score 1/2/3/4, FortiClient takes the configured remediation action (quarantine or alert & notify). If FortiSandbox returns score 0, FortiClient releases the file. When the value is 3: If FortiSandbox returns score 1/2/3, FortiClient takes the configured remediation action (quarantine or alert & notify). If FortiSandbox returns score 0/4, FortiClient releases the file. When the value is 2: If FortiSandbox returns score 1/2, FortiClient takes the configured remediation action (quarantine or alert & notify). If FortiSandbox returns score 0/3/4, FortiClient releases the file. When the value is 1: If FortiSandbox returns score 1, FortiClient takes the configured remediation action (quarantine or alert & notify). If FortiSandbox returns score 0/2/3/4, FortiClient releases the file. Possible values: [4 | 3 | 2 |1]	4
<hide_sandbox_scan>	Hide Sandbox scan option from Windows Explorer's context menu.	

XML tag	Description	Default value
	Boolean value: [0 | 1]	
<notification_type>	Specify the notification configuration for FortiSandbox file submission: • 0: Displays notification balloon when FortiSandbox detects malware in a submission. • 1: Displays a popup for all FortiSandbox file submissions. • 2: Does not display any notification for FortiSandbox file submissions, malware detection, or quarantine.	0
<max_size>	Specify the file size limit in MB for FortiSandbox file submission. 500 MB is the maximum allowed file size.	200

Anti-exploit detection

The following lists anti-exploit detection attributes:

```
<forticlient_configuration>
   <antiexploit>
      <enabled>1</enabled>
      <show_bubble_notifications>0</show_bubble_notifications>
      <exclusion_applications>acrobat.exe;chrome.exe</exclusion_applications>
   </antiexploit>
</forticlient_configuration>
```

The following table provides the XML tags for anti-exploit detection, as well as the descriptions and default values where applicable.

XML tag	Description	Default value
<enabled>	Enable anti-exploit detection to monitor commonly used applications for attempts to exploit known vulnerabilities. Boolean value: [0 | 1]	
<show_bubble_ notifications>	Show system tray notifications when anti-exploit engine detects an exploit. Boolean value: [0 | 1]	
<exclusion_ applications>	Exclude applications from anti-exploit detection. For example, to exclude Adobe Acrobat from anti-exploit detection, enter acrobat.exe.	

Removable media access

The following lists removable media access attributes:

```
<forticlient_configuration>
   <removable_media_access>
      <enabled>0</enabled>
      <show_bubble_notifications>1</show_bubble_notifications>
      <use_system_builtin_policy>0</use_system_builtin_policy>
      <rules>
         <rule uid="<UID>">
            <description>Mouse23</description>
            <type>simple</type>
            <class>Mouse</class>
            <manufacturer>Microsoft</manufacturer>
            <vid>1B36</vid>
            <pid>000D</pid>
            <rev>0001</rev>
            <action>block</action>
         </rule>
      </rules>
      <action>allow</action>
   </removable_media_access>
</forticlient_configuration>
```

The following table provides the XML tags for removable media access, as well as the descriptions and default values where applicable.

XML tag	Description	Default value
`<enabled>`	Control access to removable media devices, such as USB drives. Boolean value: `[0 | 1]`	`0`
`<show_bubble_notifications>`	Display bubble notifications when FortiClient blocks removable media access. Boolean value: `[0 | 1]`	`1`
`<use_system_builtin_policy>`	Configure whether FortiClient uses the system's built-in policy regarding removable media devices. Boolean value: `[0 | 1]`	`0`
`<action>`	Configure the action to take with removable media devices that do not match any configured rules. Available options are: • `allow`: Allow access to removable media devices connected to the endpoint that do not match any configured rules. • `deny`: Deny access to removable media devices connected to the endpoint that do not match any configured rules. • `monitor`: Log removable media device connections to the endpoint that do not match any configured rules.	`allow`

XML tag	Description	Default value
<rules><rule> elements	You can configure rules to allow or block specific removable devices. For a removable device that does not match any defined rule, FortiClient applies the <action> outside the <rules> element. For the <class>, <manufacturer>, <vid>, <pid>, and <rev> elements, you can find the desired values for the device in one of the following ways: • Microsoft Windows Device Manager: select the device and view its properties. • USBDeview	
<description>	Enter the desired rule description.	
<type>	Enter simple or regex for the rule type. When regex is entered, FortiClient accepts regular expressions for the <manufacturer> element. This supports Perl Compatible Regular Expressions.	
<class>	Enter the device class.	
<manufacturer>	Enter the device manufacturer.	
<vid>	Enter the device version ID.	
<pid>	Enter the device product ID.	
<rev>	Enter the device revision number.	
<action>	Configure the action to take with removable media devices connected to the endpoint that match this rule. Available options are: • allow: Allow access to removable media devices connected to the endpoint that match this rule. • deny: Deny access to removable media devices connected to the endpoint that match this rule. • monitor: Log removable media device connections to the endpoint that match this rule.	

Cloud-based malware protection

Cloud-based malware protection attributes are as follows:

```
<forticlient_configuration>
   <cloudscan>
      <enabled>1</enabled>
      <notification_type>0</notification_type>
      <response_timeout>0</response_timeout>
      <when>
```

```
            <executables_on_removable_media>1</executables_on_removable_media>
            <executables_on_mapped_nw_drives>1</executables_on_mapped_nw_drives>
            <web_downloads>1</web_downloads>
            <email_downloads>1</email_downloads>
         </when>
         <remediation>
            <action>quarantine</action>
            <on_error>allow</on_error>
         </remediation>
         <exceptions>
            <exclude_files_from_trusted_sources>1</exclude_files_from_trusted_sources>
            <exclude_files_and_folders>1</exclude_files_and_folders>
            <folders></folders>
            <files></files>
         </exceptions>
         <submit_by_extensions>
            <enabled>1</enabled>
            <use_custom_extensions>1</use_custom_extensions>
            <custom_
                  extensions>7z,arj,bz2,cpl,dll,doc,docm,docx,dot,dotm,dotx,exe,fla,flv,gz,jsfl</cust
                  om_extensions>
         </submit_by_extensions>
      </cloudscan>
   </forticlient_configuration>
```

The following table provides the XML tags for cloud-based malware protection, as well as the descriptions and default values where applicable.

XML tag	Description	Default value
`<enabled>`	Enable cloud-based malware protection. The cloud-based malware protection feature helps protect endpoints from high risk file types from external sources such as the Internet or network drives by querying FortiGuard to determine whether files are malicious. The following describes the process for cloud-based malware protection: **1.** A high risk file is downloaded or executed on the endpoint. **2.** FortiClient generates a SHA1 checksum for the file. **3.** FortiClient sends the checksum to FortiGuard to determine if it is malicious against the FortiGuard checksum library. **4.** If the checksum is found in the library, FortiGuard communicates to FortiClient that the file is deemed malware. By default, FortiClient quarantines the file. Boolean value: `[0 | 1]`	
`<notification_type>`	Configure the notification type for malicious activity from cloud-based malware protection: • **0** - Lite: Only display a balloon for malicious activity. No dialog box will be shown. • **1** - Full: Display a dialog box and a balloon notification. • **2** - None: Do not display any notification.	0

XML tag	Description	Default value
<response_timeout>	Enter the number of seconds to wait for cloud-based malware protection results before allowing file access. If FortiClient does not receive the results before the timeout expires, file access is allowed.	
<when> elements		
<executables_on_removable_media>	Enable submitting files executed from removable media for cloud-based malware protection. Boolean value: [0 | 1]	
<executables_on_mapped_nw_drives>	Enable submitting files executed from mapped network drives for cloud-based malware protection. Boolean value: [0 | 1]	
<web_downloads>	Enable submitting web downloads for cloud-based malware protection. Boolean value: [0 | 1]	
<email_downloads>	Enable submitting email downloads for cloud-based malware protection. Boolean value: [0 | 1]	
<remediation> elements		
<action>	Specify how to handle malicious files. FortiClient can quarantine malicious files. Enter one of the following: • quarantine: quarantine malicious files • alert: alert the user about malicious files but allow access to malicious files	
<on_error>	Specify how to handle files when FortiClient cannot reach the cloud-based malware protection service. You can block or allow access to files. Enter one of the following: • block • allow	
<exceptions> elements		
<exclude_files_from_trusted_sources>	Exclude files signed by trusted sources from cloud-based malware protection submission. Boolean value: [0 | 1]	
<exclude_files_and_folders>	Exclude specified folders/files from cloud-based malware protection submission. You must also create the exclusion list. Boolean value: [0 | 1]	
<folders>	Specify a list of folders to exclude. Separate multiple files with a comma. Example: C:\path\to\file1.txt, C:\path\to\file2.txt	

XML tag	Description	Default value
<files>	Specify a list of files to exclude. Separate multiple folders with a comma. Example: C:\path1\to\folder\,C:\path2\to\folder\	
<submit_by_extensions>	elements	
<enabled>	Submit specified file extensions to cloud-based malware protection for analysis. When disabled, FortiClient does not submit any file extensions to cloud-based malware protection. Boolean value: [0 | 1]	
<use_custom_ extensions>	Enable using a custom list of file extensions. If enabled, configure the custom list of file extensions using the <custom_extensions> element. If disabled, this feature only submits high risk file types such as .exe, .doc, .pdf, and .dll to cloud-based malware protection. Boolean value: [0 | 1]	
<custom_extensions>	If using a custom list of file extensions, enter the list of desired file extensions, separated only by commas.	

ZTNA

The following lists zero trust network access (ZTNA) general attributes:

```
<forticlient_configuration>
   <ztna>
      <enabled>1</enabled>
      <allow_personal_rules>1</allow_personal_rules>
      <gateways_enabled>1</gateways_enabled>
      <notify_on_error>1</notify_on_error>
      <disallow_invalid_server_certificate>1</disallow_invalid_server_certificate>
      <warn_invalid_server_certificate>1</warn_invalid_server_certificate>
      <save_password>1</save_password>
      <proxy_mode>4<proxy_mode/>
      <fqdn_exceptions>www.example.com</fqdn_exceptions>
      <azure_auto_login>
         <enabled>1</enabled>
         <azure_app>
            <client_id>997e.....400b5ca</client_id>
            <tenant_name>f794ab...3866d1</tenant_name>
         </azure_app>
      </azure_auto_login>
      <rules>
         <rule>
            <name>ssh</name>
            <destination>10.100.77.8:22</destination>
            <gateway>172.17.80.79:443</gateway>
            <mode>transparent</mode>
            <local_port>7788</local_port>
```

```
            <encryption>1</encryption>
            <enable_udp>1</enable_udp>
            <redirect>0</redirect>
         </rule>
      </rules>
      <web_proxy_rules>
         <web_proxy_rule>
            <gateway>example.com:80</gateway>
            <gateway_ip>192.158.1.38</gateway_ip>
         </web_proxy_rule>
      </web_proxy_rules>
   </ztna>
</forticlient_configuration>
```

The following table provides the XML tags for ZTNA, as well as the descriptions and default values where applicable:

XML tag	Description	Default value
`<enabled>`	Enable ZTNA. You can use FortiClient to create a secure encrypted connection to protected applications without using VPN. Acting as a local proxy gateway, FortiClient works with the FortiGate application proxy feature to create a secure connection via HTTPS using a certificate received from EMS that includes the FortiClient UID. The FortiGate retrieves the UID to identify the device and check other endpoint information that EMS provides to the FortiGate, which can include other identity and posture information. The FortiGate allows or denies the access as applicable. For TCP forwarding to non-web-based applications, you must define ZTNA connection rules using the following elements. Boolean value: `[0 | 1]`	1
`<allow_personal_ rules>`	Allow end users to configure personal ZTNA destinations. Boolean value: `[0 | 1]`	1
`<gateways_enabled>`	Allow EMS-pushed ZTNA rules. When disabled, user can only configure local ZTNA rules. Boolean value: `[0 | 1]`	1
`<notify_on_error>`	Enable or disable browser error message for ZTNA TCP forwarding failures. Boolean value: `[0 | 1]`	1
`<disallow_invalid_ server_ certificate>`	When this setting is disabled and an invalid server certificate is used, FortiClient allows the user to continue with the invalid certificate. When this setting is enabled and an invalid server certificate is used, FortiClient rejects the invalid certificate and stops the connection. Boolean value: `[0 | 1]`	0

XML tag	Description	Default value
<warn_invalid_server_certificate>	When <disallow_invalid_server_certificate> is disabled: • If <warn_invalid_server_certificate> is enabled, an invalid server certificate is used, and FortiClient uses the built-in browser for SAML authentication, FortiClient displays a security warning to the user that installing the certificate may result in a security risk. • If <warn_invalid_server_certificate> is disabled, FortiClient does not display a security warning to the user that installing the certificate may result in a security risk. When <disallow_invalid_server_certificate> is enabled and an invalid server certificate is used, FortiClient does not display a popup and stops the connection. Boolean value: [0 | 1]	
<save_password>	Enable or disable ZTNA SAML authentication browser to save SAML identity provider cookies. Boolean value: [0 | 1]	0
<proxy_mode>	Configure one of the following for ZTNA on FortiClient (macOS) to use for network traffic interception and redirection: • 4: use the FortiClient (macOS) proxy extension. Otherwise, ZTNA uses macOS packet filter (pf). This is the solution that Apple officially recommends. • 0: use the macOS pf.	0
<fqdn_exceptions>	Define exceptions for wildcard domains in ZTNA destinations. Separate multiple domains with a semicolon. For example, <fqdn_exceptions>www.example.com;www.test.com</fqdn_exceptions>.	
<azure_auto_login> elements	Enable ZTNA automatic login using Microsoft Entra ID by specifying the tenant name and client ID. When configured, users logged in to an Entra ID domain on an endpoint are automatically authenticated with the FortiGate (7.6.1 or later) using Entra ID credentials when they attempt to access zero trust network access (ZTNA) TCP-forwarding traffic. See ZTNA automatic login using Microsoft Entra ID for more details about FortiOS configuration.	
<enabled>	Enable or disable ZTNA automatic login using Microsoft Entra ID. Boolean value: [0 | 1]	
<azure_app> elements		
<client_id>	Enter the client ID of the application used to connect with EMS that you collected from the Azure management console.	
<tenant_name>	Enter the tenant name of the application used to connect with EMS that you collected from the Azure management console.	

XML tag	Description	Default value
<rules><rule> elements		
<name>	Enter the desired rule name.	
<destination>	Enter the IP address or FQDN and port of the destination host in the format <IP address or FQDN>:<port>. This field does not support entering only a hostname.	
<gateway>	Enter the FortiGate access IP address and port in the format <IP address or FQDN>:<port>.	
<mode>	Enter transparent. This element only supports transparent mode.	
<encryption>	Enable encryption. When encryption is enabled, traffic between FortiClient and the FortiGate is always encrypted, even if the original traffic has already been encrypted. When encryption is disabled, traffic between FortiClient and the FortiGate is not encrypted. Boolean value: [0 | 1]	
<enable_udp>	Enable ZTNA for UDP traffic. FortiClient applies ZTNA is for UDP and TCP traffic. Boolean value: [0 | 1]	
<redirect>	Enable to use the default external browser for ZTNA SAML authentication. Disable to use the FortiClient embedded browser for ZTNA SAML authentication. Boolean value: [0 | 1]	0
<web_proxy_rules><web_proxy_rule> elements	Configure ZTNA rule for web applications.	
<gateway>	Enter the web application IP address and port in the format <IP address or FQDN>:<port>. You must enter a port value.	
<gateway_ip>	If you enter an FQDN in <gateway>, FortiClient populates <gateway_ip>with the IP address. This element mainly ensures that FortiClient retains data during profile import and export.	

PAM

The following lists privilege access management (PAM) general attributes:

```
<forticlient_configuration>
   <pam>
      <enabled>1</enabled>
      <default_port>9191</default_port>
```

```
      <remove_web_extension_when_disabled>0</remove_web_extension_when_disabled>
   </pam>
```

</forticlient_configuration>

The following table provides the XML tags for PAM, as well as the descriptions and default values where applicable:

XML tag	Description	Default value
<enabled>	Enable PAM. This feature requires a FortiPAM instance. Boolean value: [0 | 1]	
<default_port>	Configure the port for communication between FortiPAM and EMS. The default port for this communication is 9191. If you change this value, ensure that you also change it in FortiPAM.	
<remove_web_extension_when_disabled>	If this option is enabled and the PAM feature is disabled in EMS, the PAM web extension is uninstalled. If the PAM feature is enabled in EMS, this option has no effect. Boolean value: [0 | 1]	

Apple

The following mobile configuration elements only apply to FortiClient (iOS).

The following lists Apple general attributes.

```
<forticlient_configuration>
   <apple>
      <ios>
         <mobileconfig></mobileconfig>
         <mobileconfig_name>ios_anyconnect.mobileconfig</mobileconfig_name>
      </ios>
   </apple>
</forticlient_configuration>
```

The following table provides the XML tags for FortiClient (iOS), as well as the descriptions and default values where applicable.

XML tag	Description	Default value
<mobileconfiguration>	Configuration for iOS on mobile devices.	
<mobileconfig_name>	Name of the mobile configuration for iOS.	

Design considerations

You can edit the FortiClient configuration file. The file uses XML format for easy parsing and validation. The configuration file includes all client configurations and references the client certificates.

Input validation

The import function performs basic validation and writes to log when it finds errors or warnings. The function defines default values for omitted items for VPN connections. For other settings, the function ignores omitted values.

Handling password fields

When exporting, FortiClient encrypts password and username fields (prefixed with `Enc`). However, the import function can take the clear text or encrypted format.

Importing configuration file segments

Importing a segment of a configuration file is valid. However, the segment should follow the syntax and level that this document defines. For example, the following is a valid segment:

```
<?xml version=”1.0” encoding=”utf-8”?>
<forticlient_configuration>
   <VPN>
      <SSLVPN>
         <connections>
            <connection>
               // connection 1
            </connection>
         </connections>
      </SSLVPN>
   </VPN>
</forticlient_configuration>
```

This is an invalid segment:

```
<?xml version=”1.0” encoding=”utf-8”?>
   <connections>
      <connection>
         // connection 1
      </connection>
```

```
    </connections>
```

Client certificate

The configuration file includes the client certificate(s) when exported in an encrypted format.

Backing up or restoring the configuration file

Backing up the full configuration file

To back up the full configuration file:

1. Go to *Settings*.
2. Under *System*, click *Backup*.
3. Select the file destination.
4. Enter a password to save the file in an encrypted format with a password.
5. Click *OK*.

Restoring the full configuration file

1. Go to *Settings*.
2. Expand *System*, and click *Restore*.
3. Locate and select the file.
4. If the configuration was protected with a password, a password text box displays. Enter the password used to encrypt the backup configuration file.
5. Click *OK*.

Backing up and restoring CLI utility commands and syntax

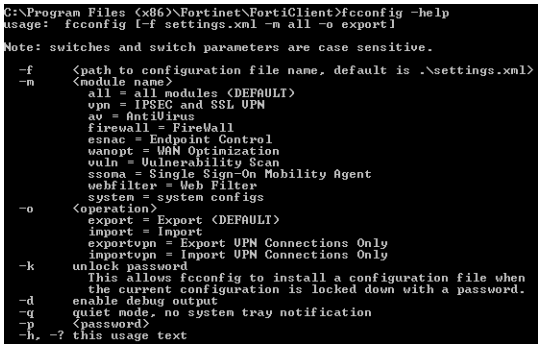
Fortinet provides administrators the ability to import and export configurations via the CLI. The system or admin user can run the FCConfig utility for Windows or the fcconfig utility for macOS locally or remotely to import or export the configuration file. In Windows, the FCConfig utility is located in the C:\Program Files (x86)\Fortinet\FortiClient> directory. In macOS, the fccconfig utility is located in the /Library/Application Support/Fortinet/FortiClient/bin directory.

The following commands are available for use. Note that `-i 1` is not available on macOS:

Command	Description
`FCConfig -m all -f <filename> -o export -i 1 -p <encrypted password>`	Back up the configuration file (encrypted).
`FCConfig -m all -f <filename> -o import -i 1`	Restore the configuration file.
`FCConfig -m all -f <filename> -o import -i 1 -p <encrypted password>`	Restore the configuration file (encrypted).
`FCConfig -m vpn -f <filename> -o importvpn -i 1`	Import the VPN tunnel configuration.
`FCConfig -m vpn -f <filename> -o importvpn -i 1 -p <encrypted password>`	Import the VPN tunnel configuration (encrypted).

Switches and switch parameters are case-sensitive.

Backing up and restoring CLI commands are advanced configuration options.



The command `fcconfig -f settings.xml -m all -o export` exports the configuration as an XML file in the FortiClient directory.

Adding XML to advanced profiles in EMS

You can add custom XML to a profile in EMS by using an advanced profile.

To reduce the size of the FortiClient XML configuration file, you can delete all help text found within the `<!-- .... -->` comment tags.

1. In EMS, go to *Endpoint Profiles* > *Manage Profiles* > *Add*.
2. Click *Advanced*.
3. On the *XML Configuration* tab, click *Edit*. EMS displays two panes. Use the pane on the right to edit the XML configuration.
4. Overwrite the existing XML configuration by pasting the XML from your custom XML configuration file into the right-hand pane:
   a. Open the FortiClient XML configuration file in a source code editor.
   b. Copy the FortiClient XML.
   c. Paste the FortiClient XML into the right pane on the *XML Configuration* tab.

5. Click *Test XML*. When valid, an *XML is valid* message displays. When invalid, an *XML is invalid* message displays. The XML must be valid before you can save the profile.
6. When the XML is valid, click *Save*.

Advanced features

Advanced features (Windows)

Connecting VPN before logon (AD environments)

The VPN <options> XML tag holds global information controlling VPN states. The VPN connects first, then logs into the Active Directory server or domain.

```
<forticlient_configuration>
   <vpn>
      <options>
         <show_vpn_before_logon>1</show_vpn_before_logon>
         <use_windows_credentials>1</use_windows_credentials>
      </options>
   </vpn>
</forticlient_configuration>
```

Creating a redundant IPsec VPN

To use VPN resiliency or redundancy, configure a list of FortiGate IP address or FQDN servers, instead of just one:

```
<forticlient_configuration>
   <vpn>
      <ipsecvpn>
         <connections>
            <connection>
               <name>psk_90_1</name>
               <type>manual</type>
               <ike_settings>
                  <prompt_certificate>0</prompt_certificate>
                  <server>10.10.90.1;ipsecdemo.fortinet.com;172.17.61.143</server>
                  <redundant_sort_method>1</redundant_sort_method>
               </ike_settings>
            </connection>
         </connections>
      </ipsecvpn>
   </vpn>
</forticlient_configuration>
```

This is a balanced but incomplete XML configuration fragment. It includes all closing tags, but omits some important elements to complete the configuration.

<redundant_sort_method> value	Description
1	IPsec VPN connection is ping response-based. The VPN connects to the FortiGate that responds the most quickly.
0	IPsec VPN connection is priority-based. Priority-based configuration attempts to connect to FortiGates by starting with the first FortiGate on the configured list. Default method.

Priority-based SSL VPN connections

SSL VPN supports priority-based configurations for redundancy.

```
<forticlient_configuration>
   <vpn>
      <sslvpn>
         <options>
            <enabled>1</enabled>
         </options>
         <connections>
            <connection>
               <name>ssl_90_1</name>
               <server>10.10.90.1;ssldemo.fortinet.com;172.17.61.143:443</server>
            </connection>
         </connections>
      </sslvpn>
   </vpn>
</forticlient_configuration>
```

This is a balanced but incomplete XML configuration fragment. It includes all closing tags, but omits some important elements to complete the configuration.

For SSL VPN, all FortiGates must use the same TCP port.

Enabling VPN autoconnect

VPN autoconnect uses the following XML tags:

```
<forticlient_configuration>
   <vpn>
      <options>
         <autoconnect_tunnel>ipsecdemo.fortinet.com</autoconnect_tunnel>
      </options>
   </vpn>
</forticlient_configuration>
```

This is a balanced but incomplete XML configuration fragment. It includes all closing tags, but omits some important elements to complete the configuration.

Enabling VPN always up

VPN always up uses the following XML tags:

```
<forticlient_configuration>
   <vpn>
      <connection>
         <keep_running>1</keep_running>
      </connection>
   </vpn>
</forticlient_configuration>
```

This is a balanced but incomplete XML configuration fragment. It includes all closing tags, but omits some important elements to complete the configuration.

Advanced features (macOS)

Creating a redundant IPsec VPN

To use VPN resiliency or redundancy, configure a list of FortiGate IP or FQDN servers, instead of just one:

```
<forticlient_configuration>
   <vpn>
      <ipsecvpn>
            <options>
            ...
            </options>
               <connections>
                  <connection>
                     <name>psk_90_1</name>
                     <type>manual</type>
                     <ike_settings>
                     <prompt_certificate>0</prompt_certificate>
                     <server>10.10.90.1;ipsecdemo.fortinet.com;172.17.61.143</server>
                     <redundant_sort_method>1</redundant_sort_method>
                     ...
               </ike_settings>
            </connection>
         </connections>
      </ipsecvpn>
   </vpn>
</forticlient_configuration>
```

This is a balanced but incomplete XML configuration fragment. It includes all closing tags, but omits some important elements to complete the configuration.

<redundant_sort_method> value	Description
1	IPsec VPN connection is ping response-based. The VPN connects to the FortiGate that responds the most quickly.
0	IPsec VPN connection is priority-based. Priority-based configuration attempts to connect to FortiGates by starting with the first FortiGate on the configured list. Default method.

Priority-based SSL VPN connections

SSL VPN supports priority-based configurations for redundancy.

```
<forticlient_configuration>
   <vpn>
      <sslvpn>
         <options>
            <enabled>1</enabled>
            ...
         </options>
         <connections>
            <connection>
               <name>ssl_90_1</name>
               <server>10.10.90.1;ssldemo.fortinet.com;172.17.61.143:443</server>
               ...
            </connection>
         </connections>
      </sslvpn>
   </vpn>
</forticlient_configuration>
```

This is a balanced but incomplete XML configuration fragment. It includes all closing tags, but omits some important elements to complete the configuration.

For SSL VPN, all FortiGates must use the same TCP port.

Enabling VPN autoconnect

VPN autoconnect uses the following XML tag:

```
<autoconnect_tunnel>ssl 198 no cert</autoconnect_tunnel>
```

Enabling VPN always up

VPN always up uses the following XML tag:

```
<keep_running>1</keep_running>
```

VPN tunnel and script

This feature supports auto-running a user-defined script after the configured VPN tunnel is connected or disconnected. The scripts are batch scripts in Windows and shell scripts in macOS. They are defined as part of a VPN tunnel configuration on FortiGate's XML format endpoint profile. The profile is pushed to FortiClient from FortiGate. When FortiClient's VPN tunnel is connected or disconnected, the respective script defined under that tunnel is executed. These scripts can also be configured directly on FortiClient by importing the XML configuration file.

Windows

This feature supports auto-running a user-defined script after the configured VPN tunnel is connected or disconnected. The scripts are batch scripts in Windows and shell scripts in macOS. They are defined as part of a VPN tunnel configuration on FortiGate's XML format endpoint profile. The profile is pushed to FortiClient from FortiGate. When FortiClient's VPN tunnel is connected or disconnected, the respective script defined under that tunnel is executed. These scripts can also be configured directly on FortiClient by importing the XML configuration file.

Mapping a network drive after tunnel connection

The script maps a network drive and copies some files after the tunnel connects.

```
<on_connect>
   <script>
      <os>windows</os>
      <script>
         <script>
            <![CDATA[
               net use x: \\192.168.10.3\ftpshare /user:Honey Boo Boo
               md c:\test
               copy x:\PDF\*.* c:\test
            ]]>
         </script>
      </script>
   </script>
</on_connect>
```

Deleting a network drive after the tunnel disconnects

The script deletes the network drive after the tunnel disconnects.

```
<on_disconnect>
   <script>
      <os>windows</os>
      <script>
         <script>
            <![CDATA[
               net use x: /DELETE
```

```
            ]]>
          </script>
        </script>
      </on_disconnect>
```

macOS

Mapping a network drive after tunnel connection

The script maps a network drive and copies some files after the tunnel connects.

```
<on_connect>
   <script>
      <os>mac</os>
      <script>
         /bin/mkdir /Volumes/installers
         /sbin/ping -c 4 192.168.1.147 > /Users/admin/Desktop/dropbox/p.txt
         /sbin/mount -t smbfs //kimberly:RigUpTown@ssldemo.fortinet.com/installers
               /Volumes/installers/ > /Users/admin/Desktop/dropbox/m.txt
         /bin/mkdir /Users/admin/Desktop/dropbox/dir
         /bin/cp /Volumes/installers/*.log /Users/admin/Desktop/dropbox/dir/.
      </script>
   </script>
</on_connect>
```

Deleting a network drive after tunnel disconnection

The script deletes the network drive after the tunnel disconnects.

```
<on_disconnect>
   <script>
      <os>mac</os>
      <script>
         /sbin/umount /Volumes/installers
         /bin/rm -fr /Users/admin/Desktop/dropbox/*
      </script>
   </script>
</on_disconnect>
```

www.fortinet.com

Copyright© 2026 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.