FortiClient - XML Reference

Version 6.2.7

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

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

FORTINET BLOG
https://blog.fortinet.com

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

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

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

FEEDBACK
Email: techdoc@fortinet.com

October 01, 2020
FortiClient 6.2.7 XML Reference
04-627-546493-20201001

TABLE OF CONTENTS

Introduction

This document provides an overview of FortiClient version 6.2.7 XML configuration.

This document is written for FortiClient (Windows) 6.2.7.

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

XML configuration file

FortiClient supports importing and exporting its configuration via an XML file. The following sections describe the file's structure, sections, and provides descriptions for the elements used 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 8	Basic data controlling the entire configuration file.
System settings on page 8	General settings not specific to any module listed below or that affect more than one module.
Endpoint control on page 22	Endpoint control settings, including: enabling enforcement and off-net updates, skipping confirmation, disabling ability to unregister, and silent registration.
VPN on page 30	Global VPN, IPsec VPN, and SSL VPN settings.
Antivirus on page 50	Antivirus (AV) settings, including: FortiGuard Distribution Network (FDN) analytics, real-time protection (RTP), behavior when a virus is detected, and quarantining.
SSO mobility agent on page 64	Single Sign-On (SSO) mobility agent settings.
Web filter on page 65	Web filter settings, including: logging, white list priority, maximum violations, rate IP addresses, profiles, safe search, and YouTube education filter.
Application firewall on page 72	Application firewall settings.
Vulnerability scan on page 76	Vulnerability scan settings.
Sandboxing on page 79	Sandbox detection settings.
Anti-exploit detection on page 82	Anti-exploit detection settings.

Section	Description
Removable media access on page 82	Removable media access settings.
Apple on page 83	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>Enc9b4e1aae22c65e638aed4e47fbd225256a3b7a24b53f8370d6bc3b9aa90cecd5086c995f0549e94
    4b4acc951e4844529c71d81280de2b951</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>6.2.7.xxx</forticlient_version>	FortiClient version number if the file is exported from FortiClient.
<version>6.2.7</version>	Configuration file version.
<exported_by_version>6.2.7.xxx</exported_by_version>	FortiClient version number when the file was exported from FortiClient.
<date>2019/04/30</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 on page 8
- Log settings on page 12
- Proxy settings on page 14
- Update settings on page 16
- FortiProxy settings on page 19
- Certificate settings on page 20

UI settings

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

```
<forticlient_configuration>
```

```
<system>
   <ui>
      <ads>0</ads>
      <disable_backup>0</disable_backup>
      <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>
      <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
<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. Boolean value: [0 | 1]	0
<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

XML tag	Description	Default value
<password>	Enter an encrypted or non-encrypted password to set the configuration lock upon connecting with a FortiGate.	
<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.	
<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.	

XML tag	Description	Default value
<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

Log-related information is inside the <log_settings> </log_settings> XML tags.

```
<forticlient_configuration>
   <system>
      <log_settings>
         <onnet_local_logging>[0|1]</onnet_local_logging>
         <level>6</level>
         <log_
               events>ipsecvpn,sslvpn,scheduler,update,firewall,av,proxy,shield,webfilter,endpoi
               nt,fssoma,configd,vuln,sandboxing,antiexploit</log_events>
         <remote_logging>
            <log_upload_enabled>0</log_upload_enabled>
            <log_upload_server>0.0.0.0</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>
         </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. • 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.	6
<log_events>	FortiClient events or processes to log. Enter a comma-separated list of one or more of the following: • ipsecvpn: IPsec VPN log events • sslvpn: SSL VPN log events • firewall: Application firewall log events • av: AV log events • webfilter: Web filter log events • vuln: Vulnerability scan log events • fssoma: SSO mobility agent for FortiAuthenticator log events • scheduler: Scheduler log events • update: Update log events • proxy: FortiProxy log events • shield: FortiShield log events • endpoint: Endpoint Control log events • configd: Configuration log events • sandboxing: Sandbox detection events	ipsecvpn, sslvpn, scheduler, update, firewall, av, clientmanager, proxy, shield, webfilter, endpoint, fssoma, configd, vuln (enable all events by default)
<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 to send logs to.	

XML tag	Description	Default value
<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

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`
`<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</fai
               l_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>
      </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. When disabled, the following occurs: • Update tasks use HTTPS to connect to:	1

XML tag	Description	Default value
	• 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.	
<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. You can specify multiple addresses using a semicolon delimited list. For example, 10.10.10.1:80;10.10.10.2:8080;172.16.10.80;www.myfortimanager.net. In this example, FortiClient tries each server specified in order until one works or they all fail.	
<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. Separate multiple servers with a semicolon. IP address or FQDN, followed by a colon and the port number if applicable.	
<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. 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

XML tag	Description	Default value
<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>. Boolean value: [0 | 1]	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
<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 below:

<server>	<fail_over_to_fdn>	Result
"" (empty strings)	0	FortiClient only uses the FDN server.
"" (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 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.	1

XML tag	Description	Default value
	Boolean value: `[0 | 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 />
         <common_name>
            <match_type>
               <![CDATA[simple]]>
            </match_type>
            <pattern>
               <![CDATA[w8.fct.net]]>
            </pattern>
         </common_name>
         <issuer>
```

```
            <match_type>
               <![CDATA[simple]]>
            </match_type>
            <pattern>
               <![CDATA[Subordinate CA]]>
            </pattern>
         </issuer>
      </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]`	
`<server>`	Enter the server IP address.	
`<port>`	Enter the server port number.	
`<common_name>` elements for common name of the certificate automatically selected for VPN logon.		
`<match_type>`	Enter the type of matching to use, for example, `<match_type><![CDATA [simple]]></match_type>`. Choose from: • simple: exact match • wildcard: wildcard • regex: regular expressions	
`<pattern>`	Enter the pattern to use for the type of matching, for example, `<pattern><! [CDATA[w8.fct.net]]></pattern>`.	
`<issuer>` elements about the issuer of the certificate that is automatically selected for VPN logon.		
`<match_type>`	Enter the type of matching to use, for example, `<match_type><![CDATA [simple]]></match_type>`. Choose from: • simple: exact match • wildcard: wildcard	
`<pattern>`	Enter the pattern to use for the type of matching, for example, `<pattern><! [CDATA[subordinate CA]]></pattern>`.	

Following is an example of exact match for `<common_name>`:

```
<certificate>
   <common_name>
      <match_type>
         <![CDATA[simple]]>
      </match_type>
      <pattern>
         <![CDATA[w8.fct.net]]>
      </pattern>
   </common_name>
```

Following is an example of wildcard for <common_name>:

```
<certificate>
   <common_name>
      <match_type>
      <![CDATA[wildcard]]>
      </match_type>
      <pattern>
      <![CDATA[*.fct.net]]>
      </pattern>
   </common_name>
```

Endpoint control

FortiClient usually downloads endpoint control configuration elements from the FortiGate or FortiClient EMS after FortiClient connects to the FortiGate or FortiClient EMS. When FortiClient connects to FortiGate and/or EMS, it is connecting Telemetry to FortiGate and/or EMS. There are two sections:

- Endpoint control general attributes. These are contained in the <endpoint_control></endpoint_control> XML tags.
- Configuration details relating to specific FortiClient services, such as AV, Web Filter, Application Firewall, Vulnerability Scan, and so on. These are found in the respective configuration elements of the services affected.

Endpoint control general attributes are listed below:

```
<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>
      <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>
      <fgt_
           list>Enc256828d1e23febfa0b789324ea1fc9cf45acdc8af3888e7aa26677825bbf8d5d123fcbc28
           84f3cb3f2a03b5414ab01e6a6c22762add0c4f209224f052dec29491e1d15eee4a1a290a81b367c3d
           4a5251258ed14921e231547f52d9e3</fgt_list>
      <send_software_inventory>1</send_software_inventory>
      <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_compliance>1</display_compliance>
            <hide_compliance_warning>0</hide_compliance_warning>
         </ui>
         <alerts>
            <notify_server>1</notify_server>
            <alert_threshold>1</alert_threshold>
         </alerts>
         <fortigates>
            <fortigate>
               <serial_number></serial_number>
               <name></name>
               <registration_password></registration_password>
               <addresses></addresses>
            </fortigate>
         </fortigates>
         <notification_server>
            <address>172.17.60.26:8013</address>
         </notification_server>
         <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 the descriptions and default values where applicable.

XML tag	Description	Default value
<checksum>	Configuration checksum calculated on and enforced by FortiGate and EMS.	
<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.	1:5

XML tag	Description	Default value
	probe_timeout:keep_alive_timeout Changing socket connect time outs may affect performance.	
<ping_server>	Ping server's IP address or FQDN. 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. Boolean value: [0 | 1] 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.	0
<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:	

XML tag	Description	Default value
	• 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
<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]	
<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
<ui> elements		
<display_antivirus>	Display the *Malware Protection* tab in FortiClient. Boolean value: [0 | 1] When this setting is configured as 0, this feature does not display in the FortiClient console.	
<display_sandbox>	Display the *Sandbox Detection* tab in FortiClient. Boolean value: [0 | 1] When this setting is configured as 0, this feature does not display in the FortiClient console.	
<display_webfilter>	Display the *Web Filter* tab in FortiClient. Boolean value: [0 | 1]	

XML tag	Description	Default value
	When this setting is configured as 0, this feature does not display in the FortiClient console.	
<display_firewall>	Display the *Application Firewall* tab in FortiClient. Boolean value: [0 | 1] When this setting is configured as 0, this feature does not display in the FortiClient console.	
<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. Boolean value: [0 | 1] When this setting is configured as 0, this feature does not display in the FortiClient console.	
<display_compliance>	This tag is not used in FortiClient 5.6.0 and newer versions. Display the *Compliance* tab in FortiClient. Boolean value: [0 | 1] When this setting is configured as 0, this feature does not display in FortiClient.	
<hide_compliance_warning>	Hide the compliance enforcement feature message from the *Fabric 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. Boolean value: [0 | 1]. When enabled, FortiClient sends alerts to FortiClient EMS. The priority of alerts sent by FortiClient depends on the <alert_threshold> setting.	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
<fortigates> elements This is a list of FortiGates that immediately appears in the FortiClient console. The client is capable of connecting with them if they are online. If <endpoint_control><silent_registration> is set to 1, the client attempts to silently connect. The list is in priority order.		

XML tag	Description	Default value
<fortigate>	This element (with its child elements) repeats for each FortiGate that should appear in FortiClient's console interface.	
<serial_number>	(Optional] The FortiGate's serial number. Displays to the end user. It may be updated with the real serial number from the FortiGate that the client connects with.	
<name>	(Optional] The FortiGate's name. Displays to the end user. It may be updated with the real name from the FortiGate that the client connects with.	
<registration_password>	When FortiClient registers/connects to FortiGate and *Enable Registration Key for FortiClient* is enabled on the FortiGate, configure the password in the <registration_password> XML setting. The <registration_password> element contains the registration password (encrypted or plain text) required to register to the FortiGate units listed in <endpoint_control><fortigates><fortigate><addresses> When FortiClient registers/connects to EMS and EMS requires a connection key, configure the password in the <registration_password> XML setting. The <registration_password> element contains the connection key required to register to the EMS listed in <endpoint_control><notification_server><addresses>. The element is not needed when FortiGate or EMS does not require a password	
<addresses>	The FortiGate that appears in the console can be a list of FortiGate addresses. FortiClient attempts to connect to the first FortiGate listed here. A "redundancy list" of FortiGate IP:port pairs that represent this FortiGate. The list must have at least one FortiGate IP:port pair. Multiple FortiGate IP:port pairs are delimited with a semicolon. Both IP addresses and FQDN are permitted. The list is in priority order. If *Enable Registration Key for FortiClient* is enabled on the FortiGate, configure the IP address or FQDN of the FortiGate in the FortiClient <addresses> XML setting.	
<local_subnets_only>	Boolean value: [0 | 1]	0
<notification_server>	Enable EMS to manage FortiClient after FortiClient connects to the FortiGate IP address and port numbers specified by EMS. Configure the EMS IP address.	

<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 might 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.

XML tag	Description	Default value
<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.	
<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.

The <fortigate> element is used to define the FortiGates in a roaming (or redundant) FortiGate configuration. One or more <fortigate> elements may be provided within <fortigates>.

Roaming FortiGate example

In the example below, *Research Lab* and *Fortinet* appear in FortiClient. FortiClient attempts to connect silently to one of the IP addresses in *Research Lab* first. If both fail (because the laptop is not in the lab), the client attempts to connect to *Fortinet*.

Because *Fortinet* uses a FQDN, the actual FortiGate that FortiClient attempts to connect to may vary because of DNS settings.

```
<forticlient_configuration>
   <endpoint_control>
      <disable_unregister>1</disable_unregister>
      <silent_registration>1</silent_registration>
      <fortigates>
         <fortigate>
            <name>Research Lab</name>
            <addresses>10.10.10.1:9090;10.10.10.2:9090</addresses>
            <registration_password>33333333</registration_password>
```

```
            </fortigate>
            <fortigate>
               <name>Fortinet</name>
               <addresses>fgt.fortinet.com:8002</addresses>
               <registration_password>22222222</registration_password>
            </fortigate>
         </fortigates>
      </endpoint_control>
   </forticlient_configuration>
```

The FortiGate sets the following elements. FortiClient reads them and imports into its configuration when received from the FortiGate. If modified by the user locally on the Windows system, FortiClient ignores the changes.

```
<disable_unregister>
<ui>
```

For other elements that you can modify locally, if FortiClient receives the same element from the FortiGate, it overwrites the existing value.

The following elements affect Endpoint Control.

Enable AV RTP:

```
<forticlient_configuration>
   <antivirus>
      <real_time_protection>
         <enabled>1</enabled>
      <real_time_protection>
   </antivirus>
</forticlient_configuration>
```

Other services that may be configured from the FortiGate usually use the full set of configuration elements available to them, as described in the various sections of this document. These include the following:

```
<forticlient_configuration>
   <system>
      <update>
      </update>
      <log_settings>
      </log_settings>
   </system>
   <vpn>
   </vpn>
   <firewall>
   </firewall>
   <webfilter>
   </webfilter>
   <vulnerability_scan>
   </vulnerability_scan>
</forticlient_configuration>
```

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>
         <keep_running_max_tries>0</keep_running_max_tries>
         <save_password>0</save_password>
         <minimize_window_on_connect>1</minimize_window_on_connect>
         <allow_personal_vpns>1</allow_personal_vpns>
         <disable_connect_disconnect>0</disable_connect_disconnect>
         <show_vpn_before_logon>0</show_vpn_before_logon>
         <use_windows_credentials>1</use_windows_credentials>
         <use_legacy_vpn_before_logon>0</use_legacy_vpn_before_logon>
         <show_negotiation_wnd>0</show_negotiation_wnd>
         <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>
      </options>
   </vpn>
</forticlient_configuration>
```

The following table provides the 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's name, if any.	
<current_connection_type>	Select the current connection's VPN type: [ipsec | ssl]	

XML tag	Description	Default value
<autoconnect_tunnel>	Name of the configured IPsec VPN or SSL VPN tunnel to automatically connect to when FortiClient starts. Requires that the <save_password> tag be set to 1.	
<autoconnect_only_when_offnet>	Autoconnect only when FortiClient is off-net. Boolean value: [0 | 1]	0
<keep_running_max_tries>	The maximum number of attempts to make when retrying a VPN connection that was lost due to network issues. If this tag is set to 0, it retries indefinitely.	0
<save_password>	Save user-provided connection passwords. Boolean value: [0 | 1]	0
<minimize_window_on_connect>	Minimize FortiClient after successfully establishing a VPN connection. Boolean value: [0 | 1]	1
<allow_personal_vpns>	Enable end users to create, modify, and use personal VPN configurations. Boolean value: [0 | 1] When this setting is configured as 0, FortiClient users are not be able to configure personal VPN connections. Only provisioned VPN connections are available to the user.	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
<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
<show_negotiation_wnd>	Display information in FortiClient while establishing connections. Boolean value: [0 | 1]	0
<disable_dead_gateway_detection>	Notifies the Windows OS to disable the detection of dead gateway. You may set this element to 1 if you observe that FortiClient 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.	

XML tag	Description	Default value
<disable_internet_check>	When this setting is configured as 0, VPN autoconnect only starts when the Internet is accessible. 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.	0

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>
         </options>
         <connections>
            <connection>
               <name>SSLVPN_Name</name>
               <description>Optional_Description</description>
               <server>ssldemo.fortinet.com:10443</server>
               <username>Encrypted/NonEncrypted_UsernameString</username>
               <single_user_mode>0</single_user_mode>
               <disclaimer_msg></disclaimer_msg>
               <ui>
                  <show_remember_password>1</show_remember_password>
                  <show_alwaysup>1</show_alwaysup>
                  <show_autoconnect>1</show_autoconnect>
                  <save_username>0</save_username>
               </ui>
               <password>Encrypted/NonEncrypted_PasswordString</password>
               <certificate/>
               <warn_invalid_server_certificate>1</warn_invalid_server_certificate>
               <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>
               <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>
            </connection>
          </connections>
        </sslvpn>
    </vpn>
</forticlient_configuration>
```

The following table provides the 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 it establishes an SSL VPN tunnel. The DNS cache is restored after the SSL VPN tunnel disconnects. If you observe that FSSO clients function incorrectly when an SSL VPN tunnel is up, use `<prefer_sslvpn_dns>` to control the DNS cache.	`0`
`<prefer_sslvpn_dns>`	When this setting is `0`, the custom DNS server from SSL VPN is not added to the physical interface. When this setting is `1`, the custom DNS server from SSL VPN is prepended to the physical interface. Boolean value: `[0 | 1]`	`0`
`<use_legacy_ssl_adapter>`	When this setting is `0`, FortiClient uses the new SSL driver. When this setting is `1`, FortiClient uses the legacy SSL driver. Boolean value: `[0 | 1]`	`1`
`<preferred_dtls_tunnel>`	DTLS supported only by FortiClient (Windows). When this setting is `0`, FortiClient uses TLS, even if `dtls-tunnel` is enabled on the FortiGate. When this setting is `1`, FortiClient uses DTLS, if it is enabled on the FortiGate, and tunnel establishment is successful. If `dtls-tunnel` is disabled on the FortiGate, or tunnel establishment is not successful, FortiClient uses TLS. DTLS tunnel uses UDP instead of TCP and can increase throughput over VPN. Boolean value: `[0 | 1]`	
`<block_ipv6>`	When this setting is `0`, FortiClient allows IPv6 connection. When this setting is `1`, FortiClient blocks IPv6 connection. FortiClient uses only IPv4 connectivity when the SSL VPN tunnel is up. Boolean value: `[0 | 1]`	`0`
`<no_dhcp_server_route>`	When this setting is `0`, 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`

XML tag	Description	Default value
<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]	

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.	
<description>	Optional description to identify the VPN connection.	
<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.	
<password>	The given user's encrypted or non-encrypted password.	
<certificate> elements		

XML tag	Description	Default value
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.	
`<warn_invalid_server_certificate>`	Display a warning message if the server certificate is invalid. Boolean value: `[0 | 1]`	`0`
`<allow_standard_user_use_system_cert>`	When this setting is `1`, non-administrator users can use local machine certificates to connect SSL VPN. When this setting is `0`, non-administrator users 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. 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. 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]`	
`<ui>` elements The FortiGate sets the elements of the `<ui>` XML tag by following an SSL VPN connection.		

XML tag	Description	Default value
<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]	

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

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>
         </certificate>
         ...
      </connection>
   <connections>
   ...
<sslvpn>
```

This is a balanced but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the SSL VPN configuration are omitted. 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. Wherever you write #username# in your script, it is automatically substituted with the XAuth username of the user that connected the tunnel. Wherever you write #password# in your script, it is automatically substituted with the XAuth password 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

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

```
<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
      </options>
      <connections>
         <connection>
            <name>ipsecdemo</name>
            <single_user_mode>0</single_user_mode>
            <type>manual</type>
            <disclaimer_msg></disclaimer_msg>
            <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>
            </ui>
            <ike_settings>
               <version>1</version>
               <prompt_certificate>0</prompt_certificate>
               <implied_SPDO>0</implied_SPDO>
               <implied_SPDO_timeout>0</implied_SPDO_timeout>
               <server>ipsecdemo.fortinet.com</server>
               <authentication_method>Preshared Key</authentication_method>
               <auth_data>
                  <preshared_
                        key>Encdab907ed117eafaadd92f82b3e768b5414e4402dbd4df4585d4202c65940f1b
                        2e9</preshared_key>
               </auth_key>
               <mode>aggressive</mode>
               <dhgroup>5;</dhgroup>
               <key_life>28800</key_life>
               <localid></localid>
               <nat_traversal>1</nat_traversal>
               <mode_config>1</mode_config>
               <enable_local_lan>0</enable_local_lan>
               <nat_alive_freq>5</nat_alive_freq>
               <dpd>1</dpd>
               <dpd_retry_count>3</dpd_retry_count>
```

```
      <dpd_retry_interval>5</dpd_retry_interval>
      <fgt>1</fgt>
      <enable_ike_fragmentation>0</enable_ike_fragmentation>
      <run_fcauth_system>0</run_fcauth_system>
      <xauth_timeout>120</xauth_timeout>
      <xauth>
         <enabled>1</enabled>
         <prompt_username>1</prompt_username>
         <username>Encrypted/NonEncrypted_UsernameString</username>
         <password />
         <attempts_allowed>1</attempts_allowed>
         <use_otp>0</use_otp>
      </xauth>
      <proposals>
         <proposal>3DES|MD5</proposal>
         <proposal>3DES|SHA1</proposal>
         <proposal>AES128|MD5</proposal>
         <proposal>AES128|SHA1</proposal>
         <proposal>AES256|SHA256</proposal>
      </proposals>
   </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>
   </ipsec_settings>
```

```
            <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>
      </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>`	Supress dialog boxes from displaying in FortiClient when using SmartCard certificates. Boolean value: `[0 | 1]`	`0`
`<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 the 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]`	

XML tag	Description	Default value
<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>	Drop IPv6 traffic when an IPsec VPN connection is established. 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 the VPN tunnel. Set from a minimum of 576 to a maximum of 1500 bytes. The default value is 1300.	1300
<disable_default_route>	Disable the default route to the gateway when the tunnel is up and restore after the tunnel is down. Boolean value: [0 | 1]	0
<check_for_cert_private_key>	Enable checks for the Windows certificate private key. When set to 1, FortiClient 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 <check_for_cert_private_key> is set to 1 and <enhanced_key_usage_manadatory> is set to 1, only the certificates with enhanced key usage are listed. Boolean value: [0 | 1]	

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

- name and type: the 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.	
<ui> elements The elements of the <ui></ui> XML tags are set by the FortiGate following an IPsec VPN connection.		
<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]	

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 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 6.2.7 supports IKE v1 and IKE v2. Enter 1 or 2.	1
<prompt_certificate>	Prompt for certificate on connection. Boolean value: [0 | 1]	

XML tag	Description	Default value
<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]	
<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. 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	
<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 below. The XML sample provided in IPsec VPN on page 38 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 • wildcard: wildcard • regex: regular expressions	

XML tag	Description	Default value
<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.	
<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]	
<mode_config>	Enable mode configuration. Boolean value: [0 | 1]	
<enable_local_lan>	Enable local LAN when using a full tunnel. This setting does not apply to split tunnels. Boolean value: [0 | 1]	0
<nat_alive_freq>	NAT alive frequency.	
<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.	3
<dpd_retry_interval>	Duration of DPD idle periods, in seconds.	5
<enable_ike_fragmentation>	Support fragmented IKE packets.	0
<run_fcauth_system>	When this setting is 1, non-administrator users can use local machine certificates to connect IPsec VPN. When this setting is 0, non-administrator users cannot use machine certificates to connect IPsec VPN.	0

XML tag	Description	Default value
	Boolean value: `[0 | 1]`	
`<xauth_timeout>`	Configure the IKE extended authentication (XAuth) timeout in seconds. Default value is two minutes (120 seconds) if not configured. Enter a value between 120 and 300 seconds.	`120`
`<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.	
`<use_otp>`	Use One Time Password (OTP). When disabled, FortiClient does not respond to DPD during XAuth. When enabled, FortiClient responds to DPD during XAuth, which may be necessary when two-factor authentication and DPD are both involved. Boolean value: `[0 | 1]`	`0`
`<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	

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. All closing tags are included, but some important elements to complete the IPsec VPN configuration are omitted. See IPsec VPN on page 38 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.	
`<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`	

XML tag	Description	Default value
<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 Second setting: Authentication type: MD5, SHA1, SHA256, SHA384, SHA512	

The on_connect and on_disconnect structure and scripting format are similar to those described in SSL VPN on page 33.

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 following XML configuration:

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

DPD example

This section provides an example of a non-default IPsec VPN configuration. You can use this configuration if both of the following symptoms occur:

- 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.

In this case, you can increase the FortiGate DPD wait time and/or enable FortiClient IPsec multithread mode. However, it is recommended not to enable FortiClient IPsec multithread mode if it is not necessary. You must make changes to the FortiGate and FortiClient configurations.

To configure the FortiGate:

Increase the FortiGate DPD wait time using 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
```

To configure FortiClient:

Enable multithread mode on FortiClient using the following XML configuration:

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

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>
      <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>	Enable shell integration. Boolean value: [0 | 1]	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>
         <bypass_java>0</bypass_java>
         <cloud_based_detection>
            <on_virus_found></on_virus_found>
         </cloud_based_detection>
         <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,.B
                     AT,.BIN,.BTM,.CDR,.CFM,.CHM,.CLA,.CLASS,.CMD,.CNN,.COM,.CPL,.CPT,.CPY,.C
                     SC,.CSH,.CSS,.DEV,.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,.V
                     XE,.WBK,.WBT,.WIZ,.WK,.WML,.WPC,.WPD,.WSC,.WSF,.WSH,.XLS,.XML,.XTP</exte
                     nsions>
               <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. • 3: do not scan files when system processes read or write them.	2
<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
<bypass_java>	Enable bypassing digitally signed Java processes. Boolean value: [0 | 1]	0
<cloud_based_detection> elements		

XML tag	Description	Default value
<on_virus_found>	The action FortiClient performs when the Cloud Based Behavior Scan (CBBS) detects a virus. Select 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	
<compressed_files> elements		
<scan>	Scan archive files, including zip, rar, and tar files, for threats. Boolean value: [0 | 1]	1
<maxsize>	Only scan files under the specified size in MB. A number up to 65535. 0 means no limit.	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		
<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: warning • 1: deny access • 3: submit only	
<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		

XML tag	Description	Default value
<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
<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.	

XML tag	Description	Default value
	Boolean value: `[0 | 1]`	
`<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 manually requested by the end user.

```
<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,.CS
                  H,.CSS,.DEV,.DLL,.DOC,.DOT,.DRV,.DVB,.DWG,.EML,.EXE,.FON,.GMS,.GVB,.HLP,.HT
                  A,.HTM,.HTML,.HTT,.HTW,.HTX,.HXS,.INF,.INI,.JPG,.JS,.JTD,.KSE,.LGP,.LIB,.LN
                  K,.MDB,.MHT,.MHTM,.MHTML,.MOD,.MPD,.MPP,.MPT,.MRC,.OCX,.PIF,.PL,.PLG,.PM,.P
                  NF,.PNP,.POT,.PPA,.PPS,.PPT,.PRC,.PWZ,.QLB,.QPW,.REG,.RTF,.SBF,.SCR,.SCT,.S
                  H,.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,.W
                  ML,.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		
<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 that FortiClient performs if it finds a virus. Enter one of the following: • 0: warn the user If a process attempts to access infected files. • 1: deny access to infected files. • 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. • 3: Submit only.	
<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		
<scan>	Scan archive files, including zip, rar, and tar files, for threats. Boolean value: [0 | 1]	1

XML tag	Description	Default value
<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		
<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:

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. 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. Multiple days may be provided, separated by commas. Enter one or more of the following:	

XML tag	Description	Default value
	• 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		
<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, POP3, and Microsoft Outlook.

```
<forticlient_configuration>
   <antivirus>
      <email>
         <smtp>1</smtp>
         <pop3>1</pop3>
         <outlook>1</outlook>
         <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
<outlook>	Scan email files processed through Microsoft Outlook. Boolean value: [0 | 1]	1
<wormdetection> elements		
<enabled>	Scan for worm viruses. Boolean value: [0 | 1]	0
<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

XML tag	Description	Default value
	• 0: log and warn • 1: strip and quarantine	
<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>
      </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

Server

On Windows servers, you may want to exclude system files from being scanned. You can configure these exclusions in the <server></server> XML tags.

```
<forticlient_configuration>
   <antivirus>
      <server>
         <exchange>
            <integrate>0</integrate>
            <action>0</action>
            <excludefilesystemfromscanning>0</excludefilesystemfromscanning>
            <excludefileextensionsfromscanning>0</excludefileextensionsfromscanning>
      </exchange>
      <sqlserver>
            <excludefilesystemfromscanning>0</excludefilesystemfromscanning>
```

```
            <excludefileextensionsfromscanning>0</excludefileextensionsfromscanning>
          </sqlserver>
        </server>
      </antivirus>
    </forticlient_configuration>
```

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

XML tag	Description	Default value
`<exchange>` elements		
`<integrate>`	When enabled, FortiClient integrates into Microsoft Exchange Server. Boolean value: `[0 | 1]`	`0`
`<action>`	Action that FortiClient performs if it finds a virus. Enter one of the following: • `0`: quarantine • `1`: remove attachment only	`0`
`<excludefilesystemfromscanning>`	Exclude the file system from scanning. Boolean value: `[0 | 1]`	`0`
`<excludefileextensionsfromscanning>`	Exclude file extensions from scanning. Boolean value: `[0 | 1]`	`0`
`<sqlserver>` elements		
`<excludefilesystemfromscanning>`	Exclude the file system from scanning. Boolean value: `[0 | 1]`	`0`
`<excludefileextensionsfromscanning>`	Exclude file extensions from scanning. Boolean value: `[0 | 1]`	`0`

SSO mobility agent

the `<fssoma> </fssoma>` XML tags contain FortiClient SSO agent configuration elements.

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

The following table provides the XML tags for SSO mobility agent, 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.	

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.
Profiles	Defines one or more rules that are applied to network traffic.

```
<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>
      <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>
      <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>
            <temp_whitelist_timeout>300</temp_whitelist_timeout>
            <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>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>
   </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>
</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 FDN querying service. Boolean value: `[0 | 1]`	`1`
`<current_profile>`	(Optional) Currently 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>`	A hostname that is a substring of the specified path is treated 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: `[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`
`<block_malicious_websites>`	Configure whether to block web sites with security risk categories (group 5). When this setting is `0`, do not block web sites with security risk categories. When this setting is `1`, block web sites with security risk categories. Boolean: `[0 | 1]`	
`<bypass_private_ip>`	Enable bypassing private IP addresses. This feature is enabled by default. Boolean: `[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, does not calculate the time.	`90`

XML tag	Description	Default value
<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
<fortiguard> elements		
<url>	The FortiGuard server's 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 warning to user with an option to proceed to the website • monitor: Monitor site access	deny
<use_https_rating_server>	By default, Web Filter sends URL rating requests to the FortiGuard rating server via UDP protocol. You can instead enable Web Filter to send the requests via TCP protocol. Boolean value: [0 | 1]	0
<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. 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.	
<temp_whitelist_timeout>	The duration, in seconds, of a bypass that is applied to a page that generated a *warning*, but for which the user selected *continue*.	300
<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><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><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]	
<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. After 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.	0

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

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.	
<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
```

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>
               </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. Boolean value: [0 | 1]	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. 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`

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>
      <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>
   </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]	

XML tag	Description	Default value
<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 below 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, this setting is disabled, and FortiClient 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]	
<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]	
<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]	
<scheduled_scans><schedule> elements Currently there can only be one scheduled item. If <scan_on_maintenance> is enabled, other configured scheduled scans are discarded.		
<enable_schedule>	Enable scheduled vulnerability scans. Boolean value: [0 | 1]	
<repeat>	Configure the frequency of scans: • 0: daily scan • 1: weekly scan	

XML tag	Description	Default value
	• 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 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>	

XML tag	Description	Default value
<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.	

Sandboxing

Sandboxing general attributes are listed below.

```
<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>
    </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.	
<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

XML tag	Description	Default value
<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	
<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.	4

XML tag	Description	Default value
	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]`	

Anti-exploit detection

Anti-exploit detection attributes are listed below.

```
<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

Removable media access attributes are listed below:

```
<forticlient_configuration>
   <removable_media_access>
      <enabled>0</enabled>
      <show_bubble_notifications>1</show_bubble_notifications>
      <use_system_builtin_policy>0</use_system_builtin_policy>
      <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. Available options are: • allow: Allow access to all removable media devices connected to the endpoint. • deny: Deny access to all removable media devices connected to the endpoint. • monitor: Log all removable media device connections to the endpoint.	allow

Apple

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

Apple general attributes are listed below.

```
<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

The FortiClient configuration file is user-editable. The file uses XML format for easy parsing and validation. The configuration file is inclusive of all client configurations and references the client certificates.

Input validation

The import function performs basic validation and writes to log when errors or warnings are found. Default values for omitted items are defined for VPN connections. For other settings omitted values are ignored.

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

It is valid to import a segment of a configuration file. However, the segment should follow the syntax and level defined in this document. For example, this 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 not a valid 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

1. Go to *Settings*.
2. Expand *System*, and click *Backup*.
3. Click the *Browse* button to locate and select the file destination.
4. Choose one of the following options:
   a. Enter a password to save the file in an encrypted format with a password.
   b. Do not enter a password to save the file in an unencrypted format.
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 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.

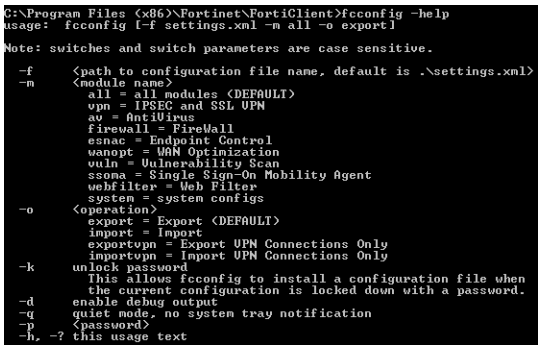
The following commands are available for use:

Command	Description
`FCConfig -m all -f <filename> -o export -i 1`	Back up the configuration file.
`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.

Command	Description
`FCConfig -m all -f <filename> -o import -i 1 -p <encrypted password>`	Restore the configuration file (encrypted).
`FCConfig -m vpn -f <filename> -o exportvpn -i 1`	Export the VPN tunnel configuration.
`FCConfig -m vpn -f <filename> -o exportvpn -i 1 -p <encrypted password>`	Export the VPN tunnel configuration (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 `fccconfig -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 AD/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/redundancy, configure a list of FortiGate IP/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>
                    <redundantsortmethod>1</redundantsortmethod>
                    ...
              </ike_settings>
           </connection>
        </connections>
      </ipsecvpn>
   </vpn>
</forticlient_configuration>
```

This is a balanced but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the IPsec VPN configuration are omitted.

RedundantSortMethod = 1

This XML tag sets the IPsec VPN connection as ping-response based. The VPN connects to the FortiGate that responds the fastest.

RedundantSortMethod = 0

By default, RedundantSortMethod =0, and the IPsec VPN connection is priority-based. Priority-based configuration attempts to connect to FortiGates by starting with the first FortiGate on the configured list.

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. All closing tags are included, but some important elements to complete the SSL VPN configuration are omitted.

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>
         <save_password>1</save_password>
      </options>
   </vpn>
</forticlient_configuration>
```

This is a balanced but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the SSL VPN configuration are omitted.

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. All closing tags are included, but some important elements to complete the SSL VPN configuration are omitted.

Advanced features (macOS)

Creating a redundant IPsec VPN

To use VPN resiliency/redundancy, configure a list of FortiGate IP/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>
                     <redundantsortmethod>1</redundantsortmethod>
                     ...
               </ike_settings>
            </connection>
         </connections>
      </ipsecvpn>
   </vpn>
</forticlient_configuration>
```

This is a balanced but incomplete XML configuration fragment. All closing tags are included, but some important elements to complete the IPsec VPN configuration are omitted.

RedundantSortMethod = 1

This XML tag sets the IPsec VPN connection as ping-response-based. The VPN connects to the FortiGate that responds the fastest.

RedundantSortMethod = 0

By default, RedundantSortMethod =0, and the IPsec VPN connection is priority-based. Priority-based configuration attempts to connect to FortiGates by starting with the first FortiGate on the configured list.

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. All closing tags are included, but some important elements to complete the SSL VPN configuration are omitted.

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>
   </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>
```

Change log

Date	Change Description
2019-04-16	Initial release of 6.2.0.
2019-04-23	Updated <webbrowser_plugin> description in Web filter on page 65.
2019-04-25	Updated <avatar_enabled> description in Endpoint control on page 22.
2019-07-18	Initial release of 6.2.1.
2019-10-15	Initial release of 6.2.2.
2019-10-16	Added <inclusions> to Sandboxing on page 79.
2019-11-06	Updated Web filter on page 65.
2019-12-19	Initial release of 6.2.3.
2020-02-06	Initial release of 6.2.4.
2020-02-27	Initial release of 6.2.5.
2020-03-06	Updated UI settings on page 8.
2020-03-10	Initial release of 6.2.6.
2020-03-18	Updated <no_dns_registration> in SSL VPN on page 33.
2020-06-02	Initial release of 6.2.7.
2020-06-09	Added <ipv4_split_exclude_networks> to IPsec VPN on page 38 and IPsec settings on page 47.
2020-10-01	Updated Update settings on page 16.

Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, 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 General Counsel, 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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.