



# FortiClient - XML Reference

Version 6.0.10

**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](mailto:techdoc@fortinet.com)



October 20, 2020

FortiClient 6.0.10 XML Reference

04-6010-480271-20201020

# TABLE OF CONTENTS

<b>Introduction</b>	<b>5</b>
<b>XML configuration file</b>	<b>6</b>
FortiClient configuration	6
File structure	6
File extensions	6
Configuration file sections	6
Encrypted username and password	7
IP addresses	7
Boolean values	7
Metadata	7
<b>System Settings</b>	<b>9</b>
UI settings	9
Log settings	12
Proxy settings	15
Update settings	16
FortiProxy settings	19
Certificate settings	21
Endpoint Control	23
VPN	31
<b>VPN options</b>	<b>32</b>
SSL VPN	33
IPsec VPN	38
Antivirus	48
General options	48
Real-time protection	49
On-Demand scans	53
Scheduled scans	56
Email	59
Quarantine	60
Server	60
Single sign-on mobility agent	61
Web Filter	62
Application firewall	69
Vulnerability Scan	73
Sandboxing	76
Anti-exploit detection	79
Removable media access	79
Apple	80
<b>FortiClient XML configurations</b>	<b>81</b>
Design considerations	81
Input validation	81
Handling of password fields	81
Segment of configuration file	81

---

Client certificate .....	82
<b>Backing up or restoring the configuration file .....</b>	<b>83</b>
Backing up the full configuration file .....	83
Restoring the full configuration file .....	83
Backing up and restoring command line utility commands and syntax .....	84
Adding XML to advanced profiles in EMS .....	86
<b>Advanced features .....</b>	<b>88</b>
Advanced features (Windows) .....	88
Connecting VPN before logon (AD environments) .....	88
Creating a redundant IPsec VPN .....	88
Priority-based SSL VPN connections .....	89
Enabling VPN autoconnect .....	89
Enabling VPN always up .....	90
Advanced features (macOS) .....	90
Create a redundant IPsec VPN .....	90
Priority-based SSL VPN connections .....	91
Enabling VPN autoconnect .....	91
Enabling VPN always up .....	91
VPN tunnel and script .....	91
Windows .....	92
macOS .....	92
<b>Change log .....</b>	<b>94</b>

# Introduction

This document provides an overview of FortiClient 6.0.10 XML configuration.

---



This document is written for FortiClient (Windows) 6.0.10.

---



For more information on FortiClient installation and configuration, see the [FortiClient 6.0.10 Administration Guide](#).

---

# XML configuration file

## FortiClient configuration

### File structure

FortiClient supports importation and exportation of its configuration via an XML file. This section defines and describes the format of that file.

### 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.

### Configuration file sections

The configuration file contains the following major sections:

Section	Description
<a href="#">Metadata on page 7</a>	Basic data controlling the entire configuration file.
<a href="#">System Settings on page 9</a>	General settings not specific to any module listed below or that affect more than one module.
<a href="#">Endpoint Control on page 23</a>	Endpoint control settings, including: enabling enforcement and off-net updates, skipping confirmation, disabling ability to unregister, and silent registration.
<a href="#">VPN on page 31</a>	Global VPN, IPsec VPN, and SSL VPN settings.
<a href="#">Antivirus on page 48</a>	Antivirus settings, including: FortiGuard Analytics, real-time protection, behavior when a virus is detected, and quarantining.

Section	Description
<a href="#">Single sign-on mobility agent on page 61</a>	Single Sign-On (SSO) mobility agent settings.
<a href="#">Web Filter on page 62</a>	Web Filtering settings, including: logging, white list priority, maximum violations, rate IP addresses, profiles, Safe Search, and YouTube education filter.
<a href="#">Application firewall on page 69</a>	Application Firewall settings.
<a href="#">Vulnerability Scan on page 73</a>	Vulnerability Scan settings.
<a href="#">Sandboxing on page 76</a>	Sandbox Detection settings.
<a href="#">Anti-exploit detection on page 79</a>	Anti-exploit detection settings.
<a href="#">Apple on page 80</a>	Settings that only apply to FortiClient (iOS).

## Encrypted username and password

Several XML tag elements are named `<password>`. All such tags are always encrypted during configuration exports. For modified and imported configurations, FortiClient accepts either 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 a feature is enabled or disabled use Boolean values. The configuration file accepts 0 for false and 1 for true.

## Metadata

The `<forticlient_configuration>` XML tag contains all 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.

The FortiClient configuration file supports the following metadata:

Metadata	Description
<code>&lt;forticlient_version&gt;6.0.10.66&lt;/forticlient_version&gt;</code>	FortiClient version number if the file is exported from FortiClient.
<code>&lt;version&gt;6.0.10&lt;/version&gt;</code>	Configuration file version.
<code>&lt;date&gt;2019/01/31&lt;/date&gt;</code>	Date the file was generated.
<code>&lt;partial_configuration&gt;0&lt;/partial_configuration&gt;</code>	Controls whether the configuration is replaced or added in import/restore. Possible values are 0 or 1.
<code>&lt;os_version&gt;windows&lt;/os_version&gt;</code>	Indicates whether this configuration is generated from Microsoft Windows or macOS. Possible values are windows or MacOSX.
<code>&lt;os_architecture&gt;x64&lt;/os_architecture&gt;</code>	Indicates the OS architecture. Possible values are x64 or x32.



# System Settings

The `<system>` `</system>` XML tags contain system settings. It includes the following subsections:

## UI settings

User interface related information are contained inside the `<ui>` `</ui>` XML tags.

```
<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>
      <password>Encrypted/NonEncrypted_PasswordString</password>
      <culture-code>os-default</culture-code>
      <show_passcode>0</show_passcode>
      <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>
      </providers>
    </avatars>
  </ui>
</system>
</forticlient_configuration>
```

```

        </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 FortiClient do not display, even when set to 1. FortiClient ignores this setting. Boolean value: [0   1]	1
<disable_backup>	Enable or disable configuration backup from the FortiClient console. Boolean value: [0   1]	1
<default_tab>	The tab selected by default in the FortiClient console. Enter one of the following: <ul style="list-style-type: none"> <li>AV: Anti Virus</li> <li>WF: Parental Control/Web Filtering</li> <li>FW: Application Firewall</li> <li>VPN: Remote Access</li> <li>VULN: Vulnerability Scan</li> </ul>	AV
<flashing_system_tray_icon>	Enable or disable the flashing system tray icon. The system tray flashes while FortiClient background processes are running. Boolean value: [0   1]	1

XML tag	Description	Default value
<hide_system_tray_icon>	Hide or display the 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
<password>	Enter an encrypted or non-encrypted password to set the configuration lock upon connecting with a FortiGate.	
<culture-code>	The localized language that FortiClient uses. Enter one of the following: <ul style="list-style-type: none"> <li>os-default: Defaults to the operating system language</li> <li>de-de: German</li> <li>en-us: English (United States)</li> <li>es-es: Spanish (Spain)</li> <li>fr-fr: French (France)</li> <li>ja-jp: Japanese</li> <li>pt-br: Portuguese (Brazil)</li> <li>kr-kr: Korean</li> <li>zh-cn: Simplified Chinese</li> <li>zh-tw: Traditional Chinese</li> </ul>	os-default
<show_passcode>	Display <i>Passcode</i> instead of <i>Password</i> on the VPN tab on the FortiClient console. Boolean value: [0   1]	0
<gpu_rendering>	Enable or disable GPU rendering. Boolean value: [0   1]	0
<replacement_messages>	Displays 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 or disable 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 FortiClient uses to retrieve an avatar picture from Google. Integration with Google requires a <a href="#">Google API Console project</a> .	
<clientid>	Enter your Google API Console project's client ID.	
<clientsecret>	Enter your Google API Console project's client secret.	

XML tag	Description	Default value
<redirecturl>	Enter your Google API Console project's redirect URL.	
<linkedin>	Settings that FortiClient uses to retrieve an avatar picture from LinkedIn. Integration with LinkedIn requires <a href="#">LinkedIn Developers</a> knowledge.	
<clientid>	Enter the LinkedIn client ID.	
<clientsecret>	Enter the LinkedIn client secret.	
<redirecturl>	Enter the LinkedIn redirect URL.	
<salesforce>	Settings that FortiClient uses to retrieve an avatar picture from Salesforce. Integration with Salesforce requires knowledge of <a href="#">Salesforce Developer</a> .	
<clientid>	Enter the Salesforce client ID.	
<clientsecret>	Enter the Salesforce client secret.	
<redirecturl>	Enter the 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, end
        point, 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>
      </remote_logging>
    </log_settings>
  </system>
</forticlient_configuration>
```

```

    <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>
  </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 client-log-when-on-net is enabled on EMS, EMS sends this XML element. Boolean value: [0   1]	
<level>	Select the FortiClient logging level. Enter one of the following: <ul style="list-style-type: none"> <li>0: emergency</li> <li>1: alert</li> <li>2: critical</li> <li>3: error</li> <li>4: warning</li> <li>5: notice</li> <li>6: information</li> <li>7: debug</li> </ul>	6
<log_events>	FortiClient events or processes to log. One or more comma-separated list of: <ul style="list-style-type: none"> <li>ipsecvpn: IPsec VPN log events</li> <li>sslvpn: SSL VPN log events</li> <li>firewall: Application Firewall log events</li> <li>av: Antivirus log events</li> <li>webfilter: Web Filtering log events</li> <li>vuln: Vulnerability Scan log events</li> <li>fssoma: Single Sign-On (SSO) mobility agent for FortiAuthenticator log events</li> <li>scheduler: Scheduler log events</li> <li>update: Update log events</li> <li>proxy: FortiProxy log events</li> <li>shield: FortiShield log events</li> <li>endpoint: Endpoint Control log events</li> <li>configd: Configuration log events</li> <li>sandboxing: Sandbox Detection events</li> </ul>	ipsecvpn, sslvpn, scheduler, update, firewall, av, clientmanager , proxy, shield, webfilter, endpoint, fssoma, configd, vuln (enable all events by default)
<remote_logging>	elements	

XML tag	Description	Default value
All elements for <remote_logging> apply only to remote logs. The elements do not affect the behavior of local logs.		
<log_upload_enabled>	Set the Boolean value to 1 to upload logs to the FortiAnalyzer or FortiManager. Boolean value: [0   1]	0
<log_upload_server>	Enter the IP address of the FortiAnalyzer or FortiManager to send logs to.	
<log_upload_ssl_enabled>	Enable or disable use of SSL protocol during log upload. Boolean value: [0   1]	1
<log_upload_freq_minutes>	The log frequency upload period in minutes.	90
<log_generation_timeout_sec>	How often logs are created in seconds.	900
<log_compressed>	Enable or disable compression of logs. Boolean value: [0   1]	
<log_retention_days>	If the server is not reachable, the number of days to retain the logs in the upload queue before being deleted. Local logs are not deleted.	90
<log_protocol>	Enter the remote server type: <ul style="list-style-type: none"> <li>faz: FortiAnalyzer</li> <li>syslog: Syslog server</li> </ul>	
<netlog_server>	Enter the syslog server's IP address. Used 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 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



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

## Proxy settings

Proxy-related information is contained inside the `<proxy></proxy>` XML tags. 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
<code>&lt;update&gt;</code>	Enable or disable updates. Set the Boolean value to 1 if a proxy server exists between FortiClient and the Internet. Boolean value: [0   1]	0
<code>&lt;fail_over_to_fdn&gt;</code>	Enable or disable failover to FortiGuard servers. Boolean value: [0   1]	0
<code>&lt;online_scep&gt;</code>	Enable or disable Simple Certificate Enrollment Protocol (SCEP). Set the Boolean value to 1 if you are using SCEP server and a proxy server exists between FortiClient and the SCEP server. Boolean value: [0   1]	0
<code>&lt;virus_submission&gt;</code>	Enable or disable virus submission to the FortiGuard Distribution Network (FDN). Set the Boolean value to 1 if a SMTP proxy server exists between FortiClient and Fortinet's virus submission servers. Used when you <i>submit for analysis</i> or <i>submit as false positive</i> . Boolean value: [0   1]	0
<code>&lt;type&gt;</code>	The type of proxy being specified. Enter one of the following: <ul style="list-style-type: none"> <li>HTTP</li> <li>SOCKS4</li> <li>SOCKS5</li> </ul>	HTTP
<code>&lt;address&gt;</code>	The proxy server's IP address or FQDN.	
<code>&lt;port&gt;</code>	The proxy server's port number.	80

XML tag	Description	Default value
	Port range: 1 to 65535	
<username>	If the proxy requires authentication, specify the encrypted or non-encrypted username here.	
<password>	If the proxy requires authentication, specify the encrypted or non-encrypted password here.	

## Update settings

Update-related information is contained inside the <update></update> XML tags. Use this field to specify how FortiClient performs updates from FortiGuard Distribution Network (FDN) servers.

```
<forticlient_configuration>
  <system>
    <update>
      <use_custom_server>0</use_custom_server>
      <restrict_services_to_regions/>
      <server></server>
      <port>80</port>
      <fail_over_servers>server1.fortinet.com:8008;172.81.30.6:80;server2.fortinet.com:80</fail_over_servers>
      <timeout>60</timeout>
      <failoverport>8000</failoverport>
      <fail_over_to_fdn>1</fail_over_to_fdn>
      <use_proxy_when_fail_over_to_fdn>1</use_proxy_when_fail_over_to_fdn>
      <auto_patch>1</auto_patch>
      <update_action>notify_only</update_action>
      <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, use the default FDN server address. When the Boolean value is set to 1, you must specify the address in <update><server>. Typically used when specifying a FortiManager as your update server.	0



XML tag	Description	Default value
	Boolean value: [0   1]	
<code>&lt;restrict_services_to_regions&gt;</code>	<p>Define whether to restrict the FortiGuard server location to U.S.-only, or to use the nearest FortiGuard server.</p> <p>To restrict to U.S.-only FortiGuard server locations, set to <code>USA</code>, as follows:  <code>&lt;restrict_services_to_regions&gt;USA&lt;/restrict_services_to_regions&gt;</code>.</p> <p>Otherwise, leave blank. This is the default configuration.</p>	
<code>&lt;server&gt;</code>	<p>Update server's IP address or FQDN. Use when <code>&lt;use_custom_server&gt;</code> is set to 1.</p> <p>Optionally, you can specify the port number. You can specify multiple addresses using a semicolon delimited list.</p> <p>For example,  <code>10.10.10.1:80;10.10.10.2:8080;172.16.10.80;www.myfortimanager.net</code>. In this example, FortiClient tries each server specified in order until one works or they all fail.</p>	
<code>&lt;port&gt;</code>	<p>Update server's port number. If a port number is not specified in <code>&lt;update&gt;&lt;server&gt;</code>, this port is used.</p> <p>Port range: 1 to 65535</p>	80
<code>&lt;fail_over_servers&gt;</code>	<p>Update servers to try if the primary server cannot be reached. Separate multiple servers with a semicolon. IP address or FQDN, followed by a colon and the port number if applicable.</p>	
<code>&lt;timeout&gt;</code>	<p>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.</p> <p>The timeout specified is applied three times to one <code>&lt;server&gt;: &lt;port&gt;</code> pair before FortiClient gives up on this pair. If <code>&lt;failoverport&gt;</code> is specified, and greater than 0, there are a total of six attempts (three attempts for <code>&lt;server&gt;: &lt;port&gt;</code>, three attempts for <code>&lt;server&gt;: &lt;failoverport&gt;</code>).</p>	60
<code>&lt;failoverport&gt;</code>	<p>Failover port number. If the update server cannot be reached via the port specified in <code>&lt;server&gt;</code> or <code>&lt;port&gt;</code>, FortiClient tries the same address with this port.</p> <p>Port range: 1 to 65535</p>	8000
<code>&lt;fail_over_to_fdn&gt;</code>	<p>Determines whether or not to use FortiGuard servers if communication with custom <code>&lt;server&gt;</code> fails. If the Boolean value is set to 1, <code>&lt;use_custom_server&gt;</code> is set to 1, and the update server specified by <code>&lt;server&gt;</code> 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.</p> <p>Boolean value: [0   1]</p>	1

XML tag	Description	Default value
<code>&lt;use_proxy_when_fail_over_to_fdn&gt;</code>	Supports failover to FortiGuard servers if FortiClient uses a proxy server defined with <code>&lt;forticlient_configuration&gt;&lt;system&gt;&lt;proxy&gt;</code> and <code>&lt;fail_over_to_fdn&gt;</code> is set to 1. Set <code>&lt;use_proxy_when_fail_over_to_fdn&gt;</code> to 1 to fail over to FortiGuard servers. This element is ignored when no proxy server is defined with <code>&lt;forticlient_configuration&gt;&lt;system&gt;&lt;proxy&gt;</code> . Boolean value: [0   1]	1
<code>&lt;auto_patch&gt;</code>	Determines whether to automatically check for software updates. Used with <code>&lt;update_action&gt;</code> . If the Boolean value is set to 1, FortiClient automatically checks for updates and takes the action specified by <code>&lt;update_action&gt;</code> . Boolean value: [0   1]	0
<code>&lt;update_action&gt;</code>	Update action applies to software updates only. FortiClient (macOS) supports only the <code>notify_only</code> and <code>disable</code> options. Select one of the following: <ul style="list-style-type: none"> <li><code>download_and_install</code>: Automatically downloads and installs software updates with no user intervention. It reboots the computer if needed. FortiClient (macOS) does not support this option.</li> <li><code>download_only</code>: Automatically downloads software updates, but does not install them. The user can install by following the message prompt. FortiClient (macOS) does not support this option.</li> <li><code>notify_only</code>: Displays a message when a software update becomes available. The user triggers the update by following the message prompt.</li> <li><code>disable</code>: Disables online software updates. Software updates can only be achieved by manually downloading and installing newer installation packages.</li> </ul>	notify_only
<code>&lt;submit_virus_info_to_fds&gt;</code>	Enable or disable submission of virus information to FortiGuard. Boolean value: [0   1]	1
<code>&lt;submit_vuln_info_to_fds&gt;</code>	Enable or disable submission of vulnerability statistics to FortiGuard Distribution Network. When set to 1, send vulnerability detection statistics from the vulnerability scanner to FortiGuard. When set to 0, do not send vulnerability statistics to FortiGuard. Boolean value: [0   1]	1
<code>&lt;scheduled_update&gt;</code> elements		
Use these elements to define when FortiClient should look for engine, signature and software updates (if enabled).		
<code>&lt;enabled&gt;</code>	Enable or disable scheduled updates. When the Boolean value is set to 1, scheduled update is enabled. When set to 0, scheduled update is disabled. Boolean value: [0   1]	1
<code>&lt;type&gt;</code>	Update frequency: daily or at regular hourly intervals. Select one of the following: <ul style="list-style-type: none"> <li><code>daily</code></li> <li><code>interval</code></li> </ul>	interval

XML tag	Description	Default value
<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 FortiGuard 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	Only FortiGuard server is used.
"" (empty strings)	1	Only FortiGuard server is used.
"xyz" (valid IP address)	0	FortiGuard server is never used.
"xyz" (valid IP address)	1	FortiGuard server is used only as failover.

## FortiProxy settings

FortiProxy information is contained inside the <fortiproxy></fortiproxy> XML tags. FortiProxy is responsible for HTTP/HTTPS filtering and SMTP/POP3 antivirus 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 or disable FortiProxy. When the Boolean value is set to 0, FortiProxy is disabled. HTTP/HTTPS filtering and SMTP/POP3 antivirus scanning are disabled. Boolean value: [0   1]	1
<enable_https_proxy>	Enable or disable 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 types of email clients require continuous response from the server or a connection error may be triggered. Use these settings to enable or disable this feature.		
<pop3_client>	Enable or disable 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 or disable POP3 server comforting. Server comforting helps to prevent POP3 servers from complaining that the client has not responded in time. Example, where FortiClient is installed on a mail server. Boolean value: [0   1]	1
<smtp>	Enable or disable 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 or disable 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

XML tag	Description	Default value
<notify>	When the Boolean value is set to 1, the user sees a bubble notification when self-testing detects that a third party program has blocked HTTP/HTTPS filtering and SMTP/POP3 antivirus scanning. Boolean value: [0   1]	1

## Certificate settings

Certificates are contained in the <certificates></certificates> XML tags. 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		

XML tag	Description	Default value
<enabled>	Use Online Certificate Status Protocol (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: <ul style="list-style-type: none"> <li>• simple: exact match</li> <li>• wildcard: wildcard</li> <li>• regex: regular expressions</li> </ul>	
<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: <ul style="list-style-type: none"> <li>• simple: exact match</li> <li>• wildcard: wildcard</li> </ul>	
<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

Endpoint Control configuration elements are usually downloaded from FortiGate or FortiClient EMS after FortiClient connects to the same 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 Antivirus, Web Filtering, 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>
  </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>
  <onnet_addresses>
    <address>1.1.1.0/255.255.255.0</address>
  </onnet_addresses>
  <onnet_mac_addresses>
    <address>00:00:00:00:00:00</address>
  </onnet_mac_addresses>
  <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 is not intended to be changed.	
<socket_connect_timeouts>	Probe timeout for endpoint control registration and keep-alive message timeout in seconds. probe_timeout:keep_alive_timeout Changing socket connect time outs might affect performance.	1:5
<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.	



XML tag	Description	Default value
<fgt_name>	<p>FortiGate name (FortiGate hostname) or EMS that FortiClient is currently connected to (if any).</p> <p>FortiClient updates this tag when it connects to the FortiGate or EMS.</p> <p>FortiClient overwrites edits to this tag.</p> <p>You can safely delete this field.</p>	
<fgt_sn>	<p>The connected FortiGate or EMS's encrypted serial number (if any). Do not edit this field.</p> <p>You can safely delete this field.</p>	
<offnet_update>	<p>Enable or disable synchronization of configuration updates from the FortiGate or EMS.</p> <p>Boolean value: [0   1]</p>	1
<user>	Encrypted username.	
<skip_confirmation>	<p>Do not prompt user before proceeding to complete connection with FortiGate or EMS.</p> <p>Boolean value: [0   1]</p>	0
<disable_unregister>	<p>Prevent a connected client from being able to disconnect after successfully connecting to FortiGate or EMS.</p> <p>Boolean value: [0   1]</p> <p>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 &lt;silent_registration&gt;. If <i>Enable Registration Key for FortiClient</i> is enabled on FortiGate or EMS, configure this password in the &lt;registration_password&gt; XML tag, and enter the IP address or addresses of the FortiGate or EMS in the &lt;addresses&gt; XML tag.</p>	0
<disable_fgt_switch>	<p>Enable or disable the disabling of the FortiGate switch.</p> <p>Boolean value: [0   1]</p> <p>This XML setting intended for use with &lt;silent_registration&gt; and &lt;disable_unregister&gt;. If <i>Enable Registration Key for FortiClient</i> is enabled on the FortiGate, configure this password in the &lt;registration_password&gt; XML tag and enter the IP address or addresses of the FortiGate in the &lt;addresses&gt; XML tag.</p> <p>When &lt;disable_fgt_switch&gt; is configured as 1, the FortiGate switch is disabled. As a result:</p> <ul style="list-style-type: none"> <li>• FortiClient does not probe default gateway.</li> <li>• FortiClient does not automatically connect to the default gateway.</li> <li>• FortiClient ignores FortiGate broadcasts.</li> <li>• The discovered list displays only predefined FortiGate devices (if discovered).</li> </ul>	

XML tag	Description	Default value
<fgt_logoff_on_fct_shutdown>	Notify FortiGate or EMS when FortiClient is shut down. Boolean value: [0   1]	1
<show_bubble_notifications>	Notify the user when new policies are installed. 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. This field can be safely deleted.	
<ui> elements	These elements only take effect when FortiClient is registered to EMS.	
<display_antivirus>	Display AntiVirus Protection on the Malware Protection tab in the console. Boolean value: [0   1] When this setting is configured as 0, this feature does not display in the FortiClient console.	
<display_sandbox>	Display Sandbox Detection on the Malware Protection tab in the console. 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 Security tab in the console. Boolean value: [0   1] When this setting is configured as 0, this feature does not display in the FortiClient console.	
<display_firewall>	Display the Application Firewall tab in the console. 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_vpn>	Display the Remote Access tab in the console. 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 the console. 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 the console. Boolean value: [0   1] When this setting is configured as 0, this feature does not display in the FortiClient console.	
<hide_compliance_warning>	Enable to hide the compliance enforcement feature message from the Compliance & 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
<onnet_addresses>	Configure the subnet so that FortiClient in this subnet keeps the on-net prefix and subnet mask of the subnet.	
<onnet_mac_addresses>	Configure the default gateway's MAC address so that FortiClient in the subnet specified by <onnet_address> that is using the default gateway configured by <onnet_mac_address> keeps the default gateway's on-net MAC addresss.	
<alerts> element		
<notify_server>	Enable or disable FortiClient to send alerts to EMS. Boolean value: [0   1]. When this setting is configured as 1, FortiClient sends alerts to 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: <ul style="list-style-type: none"> <li>1: High priority alerts</li> <li>3: Medium priority alerts</li> <li>5: Low priority alerts</li> </ul>	1
<fortigates> elements		

XML tag	Description	Default value
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 <code>&lt;endpoint_control&gt;&lt;silent_registration&gt;</code> is set to 1, the client attempts to silently connect. The list is in priority order.		
<code>&lt;fortigate&gt;</code>	This element (with its child elements) should be repeated for each FortiGate that should appear in FortiClient's console interface.	
<code>&lt;serial_number&gt;</code>	[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.	
<code>&lt;name&gt;</code>	[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.	
<code>&lt;registration_password&gt;</code>	<p>When FortiClient registers/connects to FortiGate and <i>Enable Registration Key for FortiClient</i> is enabled on the FortiGate, configure the password in the <code>&lt;registration_password&gt;</code> XML setting. The <code>&lt;registration_password&gt;</code> element contains the registration password (encrypted or plain text) required to register to the FortiGate units listed in <code>&lt;endpoint_control&gt;&lt;fortigates&gt;&lt;fortigate&gt;&lt;addresses&gt;</code></p> <p>When FortiClient registers/connects to EMS and EMS requires a connection key, configure the password in the <code>&lt;registration_password&gt;</code> XML setting. The <code>&lt;registration_password&gt;</code> element contains the connection key required to register to the EMS listed in <code>&lt;endpoint_control&gt;&lt;notification_server&gt;&lt;addresses&gt;</code>.</p> <p>The element is not needed when FortiGate or EMS does not require a password</p>	
<code>&lt;addresses&gt;</code>	<p>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.</p> <p>Both IP addresses and FQDN are permitted. The list is in priority order. If <i>Enable Registration Key for FortiClient</i> is enabled on the FortiGate, configure the IP address or FQDN of the FortiGate in the FortiClient <code>&lt;addresses&gt;</code> XML setting.</p>	
<code>&lt;local_subnets_only&gt;</code>	Boolean value: [0   1]	0
<code>&lt;notification_server&gt;</code>	Enable EMS to manage FortiClient after FortiClient connects to the FortiGate IP address and port numbers specified by EMS. Configure the EMS IP address.	
<code>&lt;nac&gt;</code> elements		

XML tag	Description	Default value
	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 <code>&lt;nac&gt;</code> elements, non-compliance is triggered, and network access might be blocked. For information about how compliance rules work, see the <i>FortiClient Administration Guide</i> . 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.	
<code>&lt;processes&gt;</code>	[Optional] Create a policy for an application and its signature.	
<code>&lt;process&gt;</code>	Identify an application name and its signature. This element should be repeated for each unique application name.	
<code>&lt;process id="" name="" rule=""&gt;</code>	ID of this process entry and name of the application that is associated with the signatures, for example, <code>&lt;process id="1" name="MS Word"&gt;</code> . Also shows whether FortiGate compliance rules require this process to be present or absent on the endpoint.	
<code>&lt;signature name="" /&gt;</code>	Identify the application name and signature. Repeat this element for different versions of the same application.	
<code>&lt;files&gt;</code>	[Optional] Create a policy for a file and path. The policy is compliant when the file can be found.	
<code>&lt;path id="" /&gt;</code>	ID of this path entry. Identify the path of the file for the policy. Repeat this element for each unique file path.	
<code>&lt;registry&gt;</code>	[Optional] Create a policy for a registry key or value.	
<code>&lt;path id="" /&gt;</code>	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 the FortiClient Configurator tool. 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 the FortiClient console. FortiClient attempts to connect silently to one of the IPs 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 the client 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 following elements are set by the FortiGate. 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 the other elements that could be modified locally, If the same element is received from the FortiGate, the existing value is overwritten.

The following elements affect Endpoint Control.

Enable antivirus real-time protection.

```
<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

VPN-related information is contained inside the `<vpn></vpn>` XML tags. 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>
      <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
<code>&lt;current_connection_name&gt;</code>	The current connection's name, if any.	
<code>&lt;current_connection_type&gt;</code>	Select the current connection's VPN type: [ipsec   ssl]	
<code>&lt;autoconnect_tunnel&gt;</code>	Name of the configured IPsec VPN or SSL VPN tunnel to automatically connect to when FortiClient starts. Boolean value: [0   1]	
<code>&lt;autoconnect_only_when_offnet&gt;</code>	Autoconnect only when FortiClient is off-net. Boolean value: [0   1]	0
<code>&lt;keep_running_max_tries&gt;</code>	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
<code>&lt;minimize_window_on_connect&gt;</code>	Minimize FortiClient after successfully establishing a connection. Boolean value: [0   1]	1



XML tag	Description	Default value
<code>&lt;allow_personal_vpns&gt;</code>	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
<code>&lt;use_legacy_vpn_before_logon&gt;</code>	Use the old VPN before logon interface. Boolean value: [0   1]	0
<code>&lt;disable_connect_disconnect&gt;</code>	Enable or disable the <i>Connect/Disconnect</i> button when using <i>Auto Connect</i> with VPN. Boolean value: [0   1]	0
<code>&lt;show_vpn_before_logon&gt;</code>	Allow user to select VPN connection from a list before logging into the system. Boolean value: [0   1]	0
<code>&lt;use_windows_credentials&gt;</code>	Connect with the current username and password. You must enable <code>&lt;show_vpn_before_logon&gt;</code> before enabling <code>&lt;use_windows_credentials&gt;</code> . Boolean value: [0   1]	1
<code>&lt;show_negotiation_wnd&gt;</code>	Display information in FortiClient while establishing connections. Boolean value: [0   1]	0
<code>&lt;disable_dead_gateway_detection&gt;</code>	Notifies Microsoft 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]	
<code>&lt;vendor_id&gt;</code>	The default value is empty, signifying FortiClient should use its hard coded ID during IPsec.	
<code>&lt;disable_internet_check&gt;</code>	When this setting is configured as 0, auto-connect VPN only starts when the Internet is accessible. When this setting is configured as 1, auto-connect VPN starts even if the Internet is not accessible. Boolean value: [0   1]	0
<code>&lt;suppress_vpn_notification&gt;</code>	Block 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>` section(s).

```
<forticlient_configuration>
  <vpn>
    <sslvpn>
      <options>
        <enabled>1</enabled>
```

```

<dnscache_service_control>0</dnscache_service_control>
<!-- 0=disable dnscache, 1=do not touch 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>0</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>
    <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 XML tags for SSL VPN, as well as the descriptions and default values where applicable.

XML tag	Description	Default value
<sslvpn><options> elements		
<enabled>	Enable or disable SSL VPN. Boolean value: [ 0   1 ]	1
<dnscache_service_control>	FortiClient disables Windows OS DNS cache when an SSL VPN tunnel is established. The DNS cache is restored after SSL VPN tunnel is disconnected. If it is observed that FSSO clients do not function correctly when an SSL VPN tunnel is up, use the following XML configuration to control 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 ]	1
<use_legacy_ssl_adapter>	When this setting is 0, the new SSL driver is used. When this setting is 1, the legacy SSL driver is used. Boolean value: [ 0   1 ]	0
<preferred_dtls_tunnel>	When this setting is 0, FortiClient uses TLS, even if dtls-tunnel is enabled on 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 FortiGate, or tunnel establishment is not successful, TLS is used. DTLS tunnel uses UDP instead of TCP and can increase throughput over VPN. Boolean value: [ 0   1 ]	0
<block_ipv6>	When this setting is 0, FortiClient allows IPv6 connection. When this setting is 1, FortiClient blocks IPv6 connection. Only IPv4 connectivity is used 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
<no_dns_registration>	When this setting is 0, FortiClient registers the SSL VPN adapter's address in the AD domain DNS. When this setting is 1, FortiClient does not register the SSL VPN adapter's address in the AD domain DNS. Boolean value: [ 0   1 ]	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.	0

XML tag	Description	Default value
	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 ]	
<keep_connection_alive>	Retry restoring connection of an active VPN session. 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>	Either encrypted or non-encrypted username on SSL server.	
<single_user_mode>	Enable or disable 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
<password>	Either encrypted or non-encrypted password of the given user.	
<certificate>	Encrypted certificate name to connect with.	
<warn_invalid_server_certificate>	Enable or disable displaying of 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 for a certificate during a connection establishment. Boolean value: [ 0   1 ]	0
<prompt_username>	Request for a username.	1

XML Tag	Description	Default Value
	Boolean value: [ 0   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 not 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 ]	
<b>&lt;ui&gt; elements</b> The elements of the <ui> XML tag are set by the FortiGate following an SSL VPN connection.		
<show_remember_password>	Display or hide the <i>Save Password</i> checkbox in the console. Boolean value: [ 0   1 ]	
<show_alwaysup>	Display or hide the <i>Always Up</i> checkbox in the console. Boolean value: [ 0   1 ]	
<show_autoconnect>	Display or hide the <i>Auto Connect</i> 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, its values are overwritten with the new ones.

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. [windows   MacOSX]	
<script>	The MS DOS batch or macOS shell script to run.	
<![CDATA[ ]]>	Wraps the scripts in CDATA elements.	
<p>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.</p> <p>Wherever you write #username# in your script, it is automatically substituted with the XAuth username of the user that connected the tunnel.</p> <p>Wherever you write #password# in your script, it is automatically substituted with the XAuth password of the user that connected the tunnel.</p> <p>Remember to check your XML file before deploying to ensure that carriage returns/line feeds are present.</p>		

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>
    <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>Encdab907ed117eafaadd92f82b3e768b5414e4402dbd4df4585d4202c65940f1b2e9</preshared_key>
      </auth_key>
      <mode>aggressive</mode>
      <dhgroup>5</dhgroup>
      <key_life>28800</key_life>
      <localid></localid>
      <peerid></peerid>
      <nat_traversal>1</nat_traversal>
      <mode_config>1</mode_config>
      <enable_local_lan>0</enable_local_lan>
      <block_outside_dns>0</block_outside_dns>
      <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>
      </proposals>
    </ike_settings>
  </connection>
</connections>

```

```
<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>
  <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>	Suppress 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 or disable IPsec VPN. Boolean value: [0   1]	1
<beep_if_error>	Beep if VPN connection attempt fails. Boolean value: [0   1]	0
<beep_continuously>	Enable or disable 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 Microsoft Windows certificates for connections. Boolean value: [0   1]	
<use_win_current_user_cert>	Use Microsoft Windows current user certificates for connections. Boolean value: [0   1]	1
<use_win_local_computer_cert>	Use Microsoft 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 or disable 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

XML tag	Description	Default value
<code>&lt;disable_default_route&gt;</code>	Disable the default route to the gateway when the tunnel is up and restore after the tunnel is down. Boolean value: [0   1]	0
<code>&lt;check_for_cert_private_key&gt;</code>	Enable or disable checks for the Windows certificate private key. When set to 1, FortiClient checks for the Windows certificate private key. Boolean value: [0   1]	0
<code>&lt;enhanced_key_usage_mandatory&gt;</code>	Enable or disable certificates with enhanced key usage. Used with <code>&lt;check_for_cert_private_key&gt;</code> . When <code>&lt;check_for_cert_private_key&gt;</code> is set to 1 and <code>&lt;enhanced_key_usage_mandatory&gt;</code> 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
- 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
<code>&lt;name&gt;</code>	VPN connection name.	
<code>&lt;single_user_mode&gt;</code>	Enable or disable 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
<code>&lt;type&gt;</code>	IPSec VPN connection type. Select: [manual   auto]	
<b>&lt;ui&gt; elements</b>		
The elements of the <code>&lt;ui&gt;</code> XML tags are set by the FortiGate following an IPsec VPN connection.		
<code>&lt;show_passcode&gt;</code>	Display <i>Passcode</i> instead of <i>Password</i> on the <i>Remote Access</i> tab in the console. Boolean value: [0   1]	
<code>&lt;show_remember_password&gt;</code>	Display the <i>Save Password</i> checkbox in the console. Boolean value: [0   1]	
<code>&lt;show_alwaysup&gt;</code>	Display the <i>Always Up</i> checkbox in the console.	

XML Tag	Description	Default Value
	Boolean value: [0   1]	
<show_ _autoconnect>	Display the <i>Auto Connect</i> 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, its values are overwritten with the new ones.

## IKE settings

Internet Key Exchange (IKE) is performed automatically based on pre-shared 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 IKE version. FortiClient 6.0.10 supports IKE v1 and IKE v2. Enter 1 or 2. If no value is specified, IKE v1 is selected by default.	1
<prompt_certificate>	Prompt for certificate on connect. Boolean value: [0   1]	
<implied_SPDO>	Configure what ports allow traffic. When this setting is 0, only traffic from port 500 and 4500 are allowed. When this setting is 1, other traffic is allowed. 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.	

XML tag	Description	Default value
	When <code>&lt;implied_SPDO&gt;</code> is set to 0, <code>&lt;implied_SPDO_timeout&gt;</code> is ignored.	
<code>&lt;server&gt;</code>	IP address or FQDN.	
<code>&lt;authentication_method&gt;</code>	Authentication method. Select one of the following: <ul style="list-style-type: none"> <li>• Preshared Key</li> <li>• X509 Certificate</li> <li>• Smartcard X509 Certificate</li> <li>• System Store X509 Certificate</li> </ul>	
<code>&lt;auth_data&gt;</code> elements		
<code>&lt;preshared_key&gt;</code>	Encrypted value of the preshared key.	
<code>&lt;certificate&gt;</code>	Use the <code>&lt;common_name&gt;</code> and <code>&lt;issuer&gt;</code> subelements to provide the certificate name and issuer, respectively. FortiClient searches all certificate stores until it finds a match.	
<code>&lt;mode&gt;</code>	Connection mode. [aggressive   main]	
<code>&lt;dhgroup&gt;</code>	A list of possible Diffie-Hellman (DH) protocol groups, separated by semicolons.	
<code>&lt;key_life&gt;</code>	Phase 2 key expiry duration, in seconds.	28800
<code>&lt;localid&gt;</code>	Enter the peer ID configured in the FortiGate Phase 1 configuration. If <i>Accept any peer ID</i> has been configured, leave this field blank.	
<code>&lt;peerid&gt;</code>	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.	
<code>&lt;nat_traversal&gt;</code>	Enable or disable NAT traversal. Boolean value: [0   1]	
<code>&lt;mode_config&gt;</code>	Enable or disable mode configuration. Boolean value: [0   1]	
<code>&lt;enable_local_lan&gt;</code>	Enable or disable local LAN. When the Boolean value is set to 0, local LAN access is disabled when using a full tunnel. When the Boolean value is set to 1, local LAN access is enabled when using a full tunnel. Does not apply to split tunnels. Boolean value: [0   1]	0
<code>&lt;block_outside_dns&gt;</code>	When this setting is 1, Windows uses only the VPN-pushed DNS server when using a full tunnel. When this setting is 0, outside DNS server configuration is retained when the tunnel is up. Boolean value: [0   1]	0

XML tag	Description	Default value
<nat_alive_freq>	NAT alive frequency.	
<dpd>	Enable or disable 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. Boolean value: [0   1]	0
<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>	Select to use IKE Extended Authentication (xAuth). Boolean value: [0   1]	
<prompt_username>	Request a username. Boolean value: [0   1]	
<username>	Enter the encrypted or non-encrypted user name on IPsec server.	
<password>	Enter the encrypted or non-encrypted password.	
<attempts_allowed>	Maximum number of failed login attempts allowed.	
<use_otp>	Use One Time Password (OTP). When this setting is 0, FortiClient does not respond to DPD during XAuth. When this setting is 1, 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	

## 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>.	
<dhgroup>	A list of possible Diffie-Hellman (DH) protocol groups, separated by semicolons.	
<key_life_type>	Phase 2 key re-key duration type. Select one of the following: <ul style="list-style-type: none"> <li>seconds</li> <li>kbytes</li> <li>both</li> </ul>	
<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 or disable Perfect Forward Secrecy (PFS). Boolean value: [0   1]	
<use_vip>	Use virtual IP. Boolean value: [0   1]	
<virtualip> elements		
<type>	Enter the virtual IP address type. [modeconfig   dhcpoveripsec]	
<ip>	IP address.	
<mask>	Network mask.	
<dnsserver>	DNS server IP address.	
<dnsserver_secondary>	The secondary DNS server IP address.	
<winserver>	Microsoft 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.	

XML tag	Description	Default value
	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 that described in the section titled: SSL VPN earlier.

## 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 debug log and the FortiClient debug log, 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 FortiGate:

1. Enable IKE fragmentation on FortiGate using the following FortiOS CLI:

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

### To configure FortiClient:

1. Enable IKE fragmentation on FortiClient using XML:

```
<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 FortiClient fails to connect to IPsec VPN, and you see the following symptom:

- 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 multi-thread mode.

However, it is recommended not to enable FortiClient IPsec multi-thread mode if it is not necessary. You must make changes to the FortiGate configuration and the FortiClient configuration.

**To configure FortiGate:**

1. Increase the FortiGate DPD wait time by using the following FortiOS CLI:

```
config vpn ipsec phase1-interface
edit <your IPsec VPN>
    set dpd-retrycount <give it a bigger number>
    set dpd-retryinterval <give it a bigger number>
```

**To configure FortiClient:**

1. Enable multi-thread mode on FortiClient by using XML:

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

## Antivirus

The Antivirus configuration data are contained in the `<antivirus>` `</antivirus>` XML tags.

## General options

This has options that enable or disable various services in the antivirus 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
<code>&lt;enabled&gt;</code>	Enable or disable antivirus. Boolean value: [ 0   1 ]	1
<code>&lt;signature_expired_notification&gt;</code>	Enable or disable expired signature notification. Boolean value: [ 0   1 ]	0



XML tag	Description	Default value
<scan_on_insertion>	Enable or disable scan on insertion. Boolean value: [0   1]	0
<shell_integration>	Enable or disable shell integration. Boolean value: [0   1]	1
<antirootkit>	Enable or disable 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>	Enable or disable FortiGuard Analytics. Boolean value: [0   1]	1
<multi_process_limit>	The number of antivirus 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 the previous one: <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>
    </real_time_protection>
  </antivirus>
</forticlient_configuration>
```

```

<scan_file_types>
  <all_files>1</all_files>
  <file_types>
    <extensions>.386,.ACE,.ACM,.ACV,.ACX,.ADT,.APP,.ASD,.ASP,.ASX,.AVB,.AX,.AX2,.BAT,.BIN,.BTM,.CDR,.CFM,.CHM,.CLA,.CLASS,.CMD,.CNN,.COM,.CPL,.CPT,.CPY,.CSC,.CSH,.CSS,.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,.VXE,.WBK,.WBT,.WIZ,.WK,.WML,.WPC,.WPD,.WSC,.WSF,.WSH,.XLS,.XML,.XTP</extensions>
    <include_files_with_no_extension>0</include_files_with_no_extension>
  </file_types>
</scan_file_types>
<exclusions>
  <file />
  <folder />
  <file_types>
    <extensions />
  </file_types>
</exclusions>
</real_time_protection>
</antivirus>
</forticlient_configuration>

```

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

XML tag	Description	Default value
<enabled>	Enable or disable real time protection. 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. Select one of the following: <ul style="list-style-type: none"> <li>0: scan files when processes read or write them + enable scan network files</li> <li>1: scan files when processes read them + disable scan network files</li> <li>2: scan files when processes write them + disable scan network files</li> <li>3: scan files when processes read or write them + disable scan network files</li> <li>4: scan files when processes read them + enable scan network files</li> <li>5: scan files when processes write them + enable scan network files</li> </ul>	0
<ignore_system_when>	Select one of the following: <ul style="list-style-type: none"> <li>0: scan files when system processes read or write them</li> <li>1: scan files when system processes read them</li> <li>2: scan files when system processes write them(default)</li> <li>3: do not scan files when system processes read or write them</li> </ul>	2
<on_virus_found>	The action FortiClient performs if a virus is found. Select one of: <ul style="list-style-type: none"> <li>1: ignore</li> <li>4: quarantine</li> </ul>	5

XML tag	Description	Default value
	<ul style="list-style-type: none"> <li>5: deny access</li> </ul>	
<popup_alerts>	Display alerts when a virus is found. Boolean value: [0   1]	1
<popup_registry_alerts>	Enable or disable pop-up registry alerts. This feature displays alerts if a process tries to change registry start items. Boolean value: [0   1]	0
<bypass_java>	Enable or disable bypassing digitally signed Java processes. Boolean value: [0   1]	0
<cloud_based_detection> elements		
<on_virus_found>	The action FortiClient performs when a virus is detected by the Cloud Based Behavior Scan (CBBS). Select one of the following: <ul style="list-style-type: none"> <li>4: Quarantine</li> <li>5: Deny access</li> </ul>	
<compressed_files> elements		
<scan>	Enable or disable scanning of compressed files. Boolean value: [0   1]	1
<maxsize>	Maximum compressed file size to scan in MB. A number up to 65535. 0 means no limit.	2
<riskware> element		
<enabled>	Enable or disable scanning of riskware files. Boolean value: [0   1]	1
<adware> element		
<enabled>	Enable or disable scanning of adware files. Boolean value: [0   1]	1
<heuristic_scanning> elements		
<level>	Level is from 0 to 4. Applied to both real-time and on-demand scans.	
<action>	The action FortiClient performs if a virus is found. Select one of: <ul style="list-style-type: none"> <li>0: warning</li> <li>1: deny access</li> <li>3: submit only</li> </ul>	
<scan_file_types> element		
<all_files>	Enabled or disable 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
<p>&lt;exclusions&gt; elements – FortiClient supports using wildcards and path variables to specify files and folders to exclude from scanning. The following wildcards and variables are supported, among others:</p> <ul style="list-style-type: none"> <li>• Using wildcards to exclude a range of file names with a specified extension, such as Edb*.jrs</li> <li>• Using wildcards to exclude all files with a specified extension, such as *.jrs</li> <li>• Path variable %windir%</li> <li>• Path variable %allusersprofile%</li> <li>• Path variable %systemroot%</li> <li>• Path variable %systemdrive%</li> </ul> <p>Combinations of wildcards and variables are not supported.</p>		
<file>	Full path to a file to exclude from on-demand scanning. 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.	
<sandboxing> element		
<enabled>	Enable or disable 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 or disable the use of FortiSandbox signatures. Boolean value: [0   1]	
<check_for_signatures_every>	Specify how often to check for FortiSandbox signatures when <use_sandbox_signatures> is set to 1. Boolean value: [0   1]	
<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

XML tag	Description	Default value
<scan_usb>	Enable or disable 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 or disable 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 antivirus scanner handles scanning of files manually requested by the end user.

```
<forticlient_configuration>
  <antivirus>
    <on_demand_scanning>
      <use_extreme_db>1</use_extreme_db>
      <on_virus_found>4</on_virus_found>
      <pause_on_battery_power>1</pause_on_battery_power>
      <allow_admin_to_stop>1</allow_admin_to_stop>
      <signature_load_memory_threshold>8</signature_load_memory_threshold>
      <automatic_virus_submission>
        <enabled>0</enabled>
        <smtp_server>fortinetvirussubmit.com</smtp_server>
        <username />
        <password>Encrypted/NonEncrypted_PasswordString</password>
      </automatic_virus_submission>
      <compressed_files>
        <scan>1</scan>
        <maxsize>0</maxsize>
      </compressed_files>
      <riskware>
        <enabled>1</enabled>
      </riskware>
      <adware>
        <enabled>1</enabled>
      </adware>
      <heuristic_scanning>
        <level>3</level>
        <action>2</action>
      </heuristic_scanning>
      <scan_file_types>
        <all_files>1</all_files>
        <file_types>
          <extensions>.386,.ACE,.ACM,.ACV,.ACX,.ADT,.APP,.ASD,.ASP,.ASX,.AVB,.AX,.AX2,.BAT,.BIN,.BTM,.CDR,.CFM,.CHM,.CLA,.CLASS,.CMD,.CNN,.COM,.CPL,.CPT,.CPY,.CSC,.CSH,.CSS,.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></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
<code>&lt;use_extreme_db&gt;</code>	Use the extreme database. Boolean value: [0   1]	1
<code>&lt;on_virus_found&gt;</code>	The action FortiClient performs if a virus is found. Select one of the following: <ul style="list-style-type: none"> <li>4: quarantine</li> <li>5: deny access</li> </ul>	4
<code>&lt;pause_on_battery_power&gt;</code>	Suspend scanning when system is on battery. Boolean value: [0   1]	1
<code>&lt;allow_admin_to_stop&gt;</code>	Control whether the local administrator can stop a scheduled AV scan or an on-demand AV scan initiated by the EMS administrator. Boolean value: [0   1]	1
<code>&lt;signature_load_memory_threshold&gt;</code>	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.	
<code>&lt;heuristic_scanning&gt;</code> elements		
<code>&lt;level&gt;</code>	Level is from 0 to 4. Applied to both real-time and on-demand scans. Select one of the following: <ul style="list-style-type: none"> <li>0: normal</li> </ul>	

XML tag	Description	Default value
	<ul style="list-style-type: none"> <li>1: advanced heuristics on highly infected systems</li> <li>2: Minos engine heuristics on highly infected systems</li> <li>3: both advanced heuristics on highly infected systems and engine heuristics</li> <li>4: both, without waiting to determine if system is highly infected</li> </ul>	
<action>	<p>The action FortiClient performs if a virus is found. Select one of the following:</p> <ul style="list-style-type: none"> <li>0: warning</li> <li>1: deny access</li> <li>2: quarantine</li> <li>3: submit only</li> </ul>	
<automatic_virus_submission> elements		
<enabled>	<p>Send virus files found to FortiGuard servers.</p> <p>Boolean value: [0   1]</p>	0
<smtp_server>	SMTP server IP address or FQDN.	fortinetvirussubmit.com
<username>		
<password>	Enter the encrypted or non-encrypted password.	
<compressed_files> elements		
<scan>	<p>Enable or disable scanning of compressed files.</p> <p>Boolean value: [0   1]</p>	1
<maxsize>	Maximum compressed file size to scan in MB. A number up to 65535. 0 means no limit.	0
<riskware> elements		
<enabled>	<p>Enable or disable scanning of riskware files.</p> <p>Boolean value: [0   1]</p>	1
<adware> element		
<enabled>	<p>Enable or disable scanning of adware files.</p> <p>Boolean value: [0   1]</p>	1
<scan_file_types> element		
<all_files>	<p>Enabled or disable scanning of all file types. If enabled, ignore the &lt;file_types&gt; element.</p> <p>Boolean value: [0   1]</p>	1
<scan_file_types> <file_types> elements		
<extensions>	Comma separated list of extensions to scan.	

XML tag	Description	Default value
<code>&lt;include_files_with_no_extension&gt;</code>	Determines whether to scan files with no extension. Boolean value: [0   1]	0
<code>&lt;exclusions&gt;</code> elements		
<code>&lt;file&gt;</code>	Full path to a file to exclude from on-demand scanning. Wildcards are not accepted. Element may be repeated to list more files.	
<code>&lt;folder&gt;</code>	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, <code>&lt;folder&gt;\Device\HarddiskVolumeShadowCopy*&lt;/folder&gt;</code> . Shadow Copy is also known as Volume Snapshot Service, Volume Shadow Copy Service, or VSS. Wildcards are not accepted.	
<code>&lt;exclusions&gt;</code> <code>&lt;file_types&gt;</code> element		
<code>&lt;extensions&gt;</code>	Comma separated list of extensions to exclude from on-demand scanning.	

## Scheduled scans

User may schedule scanning for viruses in one of three ways:

- Full scan  
Scan the entire system.
- Quick scan  
Scan only none-system files.
- Custom scan  
Scan a selection of files, as specified by user.

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 hours.

```
<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>
  </antivirus>
</forticlient_configuration>
```



```
</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.

XML tag	Description	Default value
common elements		
<enabled>	Enable or disable scheduled scan. You can enable only one of the following scan types at a time: quick scan, full scan, or custom scan. 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: <ul style="list-style-type: none"> <li>0: daily</li> <li>1: weekly</li> <li>2: monthly</li> </ul>	
<days>	Day of the week to run scan. Used when <repeat> is set to 1 for weekly scans. Multiple days may be provided, separated by comma. Select one or more of the following: <ul style="list-style-type: none"> <li>1: Sunday</li> <li>2: Monday</li> <li>3: Tuesday</li> <li>4: Wednesday</li> <li>5: Thursday</li> <li>6: Friday</li> <li>7: Saturday</li> </ul>	
<day_of_month>	The day of the month to run a scan. Used when <repeat> is set to 2 for weekly scans. A number from 1 to 31.	
<time>	Time value in 24 hour clock.	

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

XML Tag	Description	Default Value
<full> elements		
<removable_media>	Enable or disable scanning files on removable media. Boolean value: [0   1]	1
<network_drives>	Enable or disable scanning files on network drives. Boolean value: [0   1]	0
<priority>	Scan priority. Select one of the following: <ul style="list-style-type: none"> <li>0: normal</li> <li>1: low</li> <li>2: high</li> </ul>	0

XML Tag	Description	Default Value
<directory> elements		
<directory>	The full path to the directory to scan.	
<priority>	Scan priority. Select one of the following: <ul style="list-style-type: none"> <li>0: normal</li> <li>1: low</li> <li>2: high</li> </ul>	

## Email

Emails are scanned 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>	When enabled, scan email messages sent through SMTP protocol. Boolean value: [0   1]	1
<pop3>	Determines whether to scan email messages received through POP3 protocol. Boolean value: [0   1]	1
<outlook>	Scan email files processed through Microsoft Outlook. Boolean value: [0   1]	1

XML tag	Description	Default value
<wormdetection> elements		
<enabled>	Scan for worm viruses. Boolean value: [0   1]	0
<action>	The action FortiClient performs if a virus is found. Select either: <ul style="list-style-type: none"> <li>0: warn</li> <li>1: terminate process</li> </ul>	0
<heuristic_scanning> elements		
<enabled>	Enable or disable heuristics signatures. Boolean value: [0   1]	0
<action>	The action FortiClient performs if a virus is found. Select either: <ul style="list-style-type: none"> <li>0: log and warn</li> <li>1: strip and quarantine</li> </ul>	0
<mime_scanning>	Enable or disable scanning for Multipurpose Internet Mail Extensions (MIME) files. Boolean value: [0   1]	

## Quarantine

The maximum age for quarantined files is specified 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>	How long to hold quarantined files, in days, before deleting them. A number from 1 to 365.	100

## Server

On Microsoft Windows servers, it may be desired to exclude system files from being scanned. These are configured 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 the Boolean value is set to 1 FortiClient integrates into Exchange Server. Boolean value: [0   1]	0
<action>	The action FortiClient performs if a virus is found. Select either: <ul style="list-style-type: none"> <li>0: Quarantine</li> <li>1: Remove Attachment Only</li> </ul>	0
<excludefilesystemfromscanning>	Enable to exclude file system from scanning. Boolean value: [0   1]	0
<excludefileextensionsfromscanning>	Enable to exclude file extensions from scanning. Boolean value: [0   1]	0
<sqlserver> elements		
<excludefilesystemfromscanning>	Enable to exclude file system from scanning. Boolean value: [0   1]	0
<excludefileextensionsfromscanning>	Enable to exclude file extensions from scanning. Boolean value: [0   1]	0

## Single sign-on mobility agent

Configuration elements for FortiClient single sign-on mobility agent are contained in the <fssoma> </fssoma> XML tags.

```

<forticlient_configuration>
  <fssoma>
    <enabled>0</enabled>
  </fssoma>
</forticlient_configuration>

```

```

    <serveraddress>IP_or_FQDN</serveraddress>
    <presharesharedkey>Encrypted_Preshared_Key</presharesharedkey>
  </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 or disable Single Sign On (SSO). Boolean value: [0   1]	0
<serveraddress>	FortiAuthenticator IP address or FQDN.	
<presharesharedkey>	Encrypted or unencrypted pre-shared key.	



To enable the FortiClient SSO Mobility agent service on the FortiAuthenticator, you must first apply the applicable FortiClient license for FortiAuthenticator. For more information, see the [FortiAuthenticator Administration Guide](#). For information on purchasing a FortiClient license, please contact your authorized Fortinet reseller.

## Web Filter

Web Filter XML configurations are contained in the <webfilter></webfilter> tags.

There are two main sections:

- **General options**  
Configuration elements that affect the whole of the web filtering 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>
    </profiles>
  </webfilter>
</forticlient_configuration>

```

```
<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>
  </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>
<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 or disable Web Filtering. Boolean value: [0   1]	1
<enabled>	Enable or disable FortiGuard querying service. Boolean value: [0   1]	1
<current_profile>	Currently selected profile ID (optional). The default is 0 when FortiClient is standalone. 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 set to 1 (true), Web Filtering is disabled when FortiClient is connected to a FortiGate using Endpoint Control. Boolean: [0   1]	
<max_violations>	Maximum number of violations stored at any one. 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 or disable bypassing private IP addresses. This feature is enabled by default. Boolean: [0   1]	1



XML tag	Description	Default value
<code>&lt;browser_read_time_threshold&gt;</code>	Configure the threshold in seconds for web browser to be considered idle. When a web browser is idle more than the threshold, the web browser is considered idle, and time is not calculated.	90
<code>&lt;https_block_method&gt;</code>	Control how FortiClient behaves when Web Filtering blocks an HTTPS site: <ul style="list-style-type: none"> <li>• If set to 0, displays in-browser as not reachable/unable to reach, that your connection is not private, or that the site is not secure.</li> <li>• If set to 1, shows a bubble notification to the user. The connection fails/times out.</li> <li>• If set to 2, the connection fails/times out with no notification to the user.</li> </ul>	0
<code>&lt;fortiguard&gt;</code> elements		
<code>&lt;url&gt;</code>	IP address or FQDN of the FortiGuard server.	fgdl.fortigate.com
<code>&lt;enabled&gt;</code>	Enable or disable use of FortiGuard servers. Boolean value: [0   1]	1
<code>&lt;rate_ip_addresses&gt;</code>	Rate IP addresses. Boolean value: [0   1]	1
<code>&lt;action_when_unavailable&gt;</code>	Configure the action to take with all websites when FortiGuard is temporarily unavailable. FortiClient takes the configured action until contact is reestablished with FortiGuard. Available options are: <ul style="list-style-type: none"> <li>• allow: Allow full, unfiltered access to all websites</li> <li>• deny: Deny access to any website</li> <li>• warn: Display in-browser warning to user, with an option to proceed to the website</li> <li>• monitor: Monitor site access</li> </ul>	deny
<code>&lt;profiles&gt;&lt;profile&gt;&lt;safe_search&gt;</code> element		
<code>&lt;enabled&gt;</code>	Enable or disable SafeSearch. Boolean value: [0   1]	
<code>&lt;profiles&gt;&lt;profile&gt;&lt;safe_search&gt;&lt;search_engines&gt;&lt;engine&gt;</code> element		
<code>&lt;enabled&gt;</code>	Enable or disable SafeSearch 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 <i>warning</i> , but for which the user selected <i>continue</i> .	300
<log_all_urls>	Configure whether to log all URLs. When this setting is 0, only URLs are logged as specified by per-category or per-URL settings. When this setting is 1, all URLs are logged. Boolean value: [0   1]	
<log_user_initiated_traffic>	Configure what traffic to record. When this setting is 0, record all traffic. When this setting is 1, record only traffic initiated by the user. 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. Select one of the following: <ul style="list-style-type: none"> <li>allow</li> <li>deny</li> <li>warn</li> <li>monitor</li> </ul>	
<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. Select either: [allow   deny]	

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 SafeSearch 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
<code>&lt;profiles&gt;&lt;profile&gt;&lt;safe_search&gt;&lt;search_engines&gt;&lt;engine&gt;</code> elements		
<code>&lt;name&gt;</code>	Name of the SafeSearch profile.	
<code>&lt;host&gt;</code>	The FQDN of the search engine. FortiClient monitors attempts to visit this address.	
<code>&lt;url&gt;</code>	The URL substring to match or monitor, along with the FQDN.	
<code>&lt;query&gt;</code>	The query string appended to the URL.	
<code>&lt;safe_search_string&gt;</code>	The correct safe search string appended to the URL for the specified engine.	
<code>&lt;cookie_name&gt;</code>	The name of the cookie to send the search engine.	
<code>&lt;cookie_value&gt;</code>	The cookie value to send the search engine.	
<code>&lt;profiles&gt;&lt;profile&gt;&lt;safe_search&gt;&lt;youtube_education_filter&gt;</code> elements		
<code>&lt;enabled&gt;</code>	Enable YouTube education filter. Boolean value: [0   1]	
<code>&lt;filter_id&gt;</code>	The institutions 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

Application Firewall configuration data is contained in `<firewall>` `</firewall>` XML tags.

The set of elements may be grouped into two:

- General options  
Options that apply to the entire firewall activities.
- Profiles  
Defines the 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 or disable Application Firewall. This setting allows FortiClient 5.4 to be compatible with FortiGate 5.2. Boolean value: [0   1]	1
<app_enabled>	Enable or disable Application Firewall. Boolean value: [0   1]	
<enable_exploit_signatures>	Enable or disable detection of evasive exploits. When set to 1, evasive exploits are detected. When set to 0, evasive exploits are not detected. Boolean value: [0   1]	0
<candc_enabled>	Enable or disable detection of a connection to a botnet command and control server. Set to 0 to disable detection of a connection. Set to 1 to enable detection of a connection. Boolean value: [0   1]	

XML tag	Description	Default value
<code>&lt;current_profile&gt;</code>	Currently selected profile ID.	
<code>&lt;default_action&gt;</code>	Action to enforce on traffic that does not match any of the profiles defined. Select one of the following: <ul style="list-style-type: none"> <li>• block</li> <li>• reset</li> <li>• pass</li> </ul>	pass
<code>&lt;show_bubble_notifications&gt;</code>	Display a bubble message each time an application is blocked for matching a profile. Boolean value: [0   1]	
<code>&lt;max_violations&gt;</code>	Maximum number of violations stored at any one. A number from 250 to 5000	5000
<code>&lt;max_violation_age&gt;</code>	Maximum age in days of a violation record before it is culled. A number from 1 to 90.	90
<code>&lt;bypass_3rd_party_packets&gt;</code>	If set to 1, Application Firewall bypasses packets generated by third party applications. If set to 0, Application Firewall does not bypass packets generated by third party applications. 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
<code>&lt;profile&gt;</code> element		
<code>&lt;id&gt;</code>	Unique ID. A unique ID number.	

XML Tag	Description	Default Value
<profile><rules><rule> elements		
<action>	Action to enforce on traffic that matches this rule. Select one of the following: <ul style="list-style-type: none"> <li>• block</li> <li>• reset</li> <li>• pass</li> </ul>	
<compliance>	Specifies whether the rule is a compliance rule or a regular rule. When set to 1, this is a compliance rule. When set to 0 or the tag doesn't exist, this is a regular rule for FortiClient profile. For more information, see the <i>FortiClient Administration Guide</i> . Boolean value: [0   1]	
<enabled>	Enable or disable this rule. Boolean value: [0   1]	1
<category>	Categories of the applications to apply <action> on.	csv list
<vendor>	Vendors of the applications to apply <action> on.	csv list
<behavior>	Behavior of the applications 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, the first rule is used for compliance. The second rule is a regular rule and not used for compliance.

```
<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>
```



```

    </filter>
  </rule>
</rules>

```

## Vulnerability Scan

Configurations for Vulnerability Scan are contained in the `<vulnerability_scan></vulnerability_scan>` XML tags.

```

<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
<code>&lt;enabled&gt;</code>	Vulnerability Scan is enabled.	
<code>&lt;scan_on_registration&gt;</code>	Specifies whether to start a vulnerability scan when FortiClient registers to FortiGate. When set to 1, start vulnerability scan on registration. When set to 0, do not start a vulnerability scan on registration.	

XML tag	Description	Default value
	In older versions of FortiClient, this tag was named <code>&lt;scan_on_fgt_registration&gt;</code> . Boolean value: [0   1]	
<code>&lt;scan_on_signature_update&gt;</code>	Specifies whether to start a vulnerability scan when signatures are updated. When set to 1, start vulnerability scan when signatures updated. When set to 0, do not start a vulnerability scan when signatures updated. Boolean value: [0   1]	
<code>&lt;auto_patch&gt;</code>	Specifies whether to automatically install patches. Use <code>&lt;level&gt;</code> to enable and disable automatic patch installation.	
<code>&lt;level&gt;</code>	Specify whether to patch vulnerabilities with a severity higher than the defined level. Disabled when set to 0, and patches are not automatically installed when vulnerabilities are detected. When set to <code>info</code> , all patches are automatically installed when vulnerabilities are detected. Select one of the following: <ul style="list-style-type: none"> <li>0</li> <li>critical</li> <li>high</li> <li>medium</li> <li>low</li> <li>info</li> </ul>	
<code>&lt;windows_update&gt;</code>	Specifies whether to scan both Windows updates and third-party application updates. When set to 1, scan both Windows updates and third-party application updates. When set to 0, scan only third-party application updates. Boolean value: [0   1]	
<code>&lt;proxy_enabled&gt;</code>	Enable or disable using proxy settings configured in FortiClient when downloading updates for vulnerability patches. Boolean value: [0   1]	0
<code>&lt;exempt_manual&gt;</code>	Specifies whether to exempt from vulnerability scanning any applications that require the endpoint user to manually install patches. Boolean value: [0   1]	
<code>&lt;exemptions&gt;</code>	Identifies the names of applications that are exempted.	
<code>&lt;exempt_no_auto_patch&gt;</code>	Specifies whether to exempt any applications that FortiClient can automatically patch from vulnerability scanning. Boolean value: [0   1]	
<code>&lt;scheduled_scans&gt;</code>	<code>&lt;schedule&gt;</code> elements Currently there can only be one scheduled item. If <code>&lt;scan_on_maintenance&gt;</code> is enabled, other configured scheduled scans are discarded.	
<code>&lt;enable_schedule&gt;</code>	Enable or disable scheduled vulnerability scans.	

XML tag	Description	Default value
	Boolean value: [ 0   1 ]	
<repeat>	Frequency of scans. Select one of the following: <ul style="list-style-type: none"> <li>0: daily scan</li> <li>1: weekly scan</li> <li>2: monthly scan</li> </ul>	
<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: <ul style="list-style-type: none"> <li>1: Sunday</li> <li>2: Monday</li> <li>3: Tuesday</li> <li>4: Wednesday</li> <li>5: Thursday</li> <li>6: Friday</li> <li>7: Saturday</li> </ul> If the <repeat> tag is set to 2 (monthly), <day> is the date of each month to run a scan. A number from 1 to 31.	The default is the date the policy was installed from FortiGate.
<time>	The time when to run the scan. Specify a time value in 24 hour clock.	The default is the time the policy was installed from FortiGate.
<scheduled_scans><automatic_maintenance> elements		
This configures Vulnerability Scan 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 will have minimal impact to the user, PC performance, and energy efficiency. See <a href="#">Automatic Maintenance</a> .		
<scan_on_maintenance>	Enable or disable running vulnerability scan as part of Windows automatic maintenance. Boolean value: [ 0   1 ]	0
<maintenance_period>	Specify how often Vulnerability Scan needs to 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:	

XML tag	Description	Default value
	<maintenance_period>P1M4DT2H5M</maintenance_period>	
<maintenance_deadline>	Specify when Windows must start Vulnerability Scan during emergency automatic maintenance, if Vulnerability Scan 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.	

## Daily scan example

```
<schedule>
  <repeat>0</repeat>
  <time>19:30</time>
</schedule>
```

## 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</custom_extensions>
    </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>
    <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 or disable 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>	Enable or disable Sandbox Detection for executable files on removable media. Boolean value: [0   1]	
<executables_on_mapped_nw_drives>	Enable or disable Sandbox Detection for executable files on mapped drives. Boolean value: [0   1].	
<web_downloads>	Enable or disable Sandbox Detection for files downloaded from the Internet. Boolean value: [0   1].	
<email_downloads>	Enable or disable Sandbox Detection for files downloaded from email. Boolean value: [0   1].	
<submit_by_extension> elements		
<enabled>	Enable or disable submitting specified file extensions to FortiSandbox for analysis. When disabled, no file extensions are submitted to FortiSandbox, but FortiClient can still retrieve signatures from FortiSandbox. Boolean value: [0   1].	1
<use_custom_extensions>	Enable or disable 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, xls, xlsb, xlt, 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>	Enable or disable an exclusion list of trusted sources. When enabled, the list of trusted sources is excluded from Sandbox Detection. Boolean value: [0   1].	
<exclude_files_and_folders>	Enable or disable an exclusion list of files and folders. When enabled, the list of files and folders are excluded from Sandbox Detection. 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\	
<remediation> elements		
<action>	Specify how to handle infected files. Infected files can be quarantined. Alternately you can allow alert endpoint users about infected files, but allow access to infected files. Options: <ul style="list-style-type: none"> <li>quarantine</li> <li>alert</li> </ul>	
<on_error>	Specify how to handle files when FortiSandbox cannot be reached. You can block or allow access to files. Options: <ul style="list-style-type: none"> <li>block</li> <li>allow</li> </ul>	
<detect_level>	When 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 value is 3: If FortiSandbox returns score 1/2/3, FortiClient takes the configured remediation action (quarantine or alert & notify). If FortiSandbox returns score 0/4, FortiClient releases the file. When 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 value is 1: If FortiSandbox returns score 1, FortiClient takes the configured remediation action (quarantine or alert & notify). If FortiSandbox returns score 0/2/3/4, FortiClient releases the file. Possible values: [4   3   2   1]	4

## 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 or disable anti-exploit detection. Boolean value: [0   1]	
<show_bubble_notifications>	Enable or disable bubble notifications of blocked exploit attempts. Boolean value: [0   1]	
<exclusion_applications>	Specify the executable names to exclude from anti-exploit detection, for example, <code>acrobat.exe</code> .	

## 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_built_in_policy>0</use_system_built_in_policy>
    <action>allow</action>
  </removable_media_access>
</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 or disable removable media access. Boolean value: [0   1]	0
<show_bubble_notifications>	Enable or disable bubble notifications when removable media access is blocked.	1

XML tag	Description	Default value
	Boolean value: [0   1]	
<code>&lt;use_system_builtin_policy&gt;</code>	Configure whether FortiClient uses the system's built-in policy regarding removable media devices. Boolean value: [0   1]	0
<code>&lt;action&gt;</code>	Configure the action to take with removable media devices. Available options are: <ul style="list-style-type: none"> <li><code>allow</code>: Allow access to all removable media devices connected to the endpoint.</li> <li><code>deny</code>: Deny access to all removable media devices connected to the endpoint.</li> <li><code>monitor</code>: Log all removable media device connections to the endpoint.</li> </ul>	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
<code>&lt;ios&gt;</code> elements		
<code>&lt;mobileconfiguration&gt;</code>	Configuration for iOS on mobile devices.	
<code>&lt;mobileconfig_name&gt;</code>	Name of the mobile configuration for iOS.	



# FortiClient XML configurations

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.

## Design considerations

### 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 of password fields

When exporting, the password and username fields are encrypted (prefixed with “Enc”). However, the import function is able to take the clear text or encrypted format.

### Segment of configuration file

It is valid to import the 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>
```

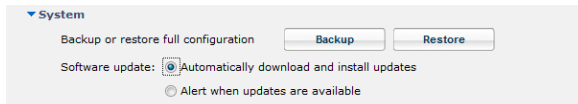
## Client certificate

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

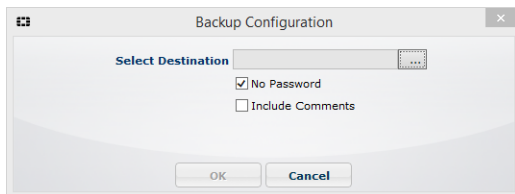
# Backing up or restoring the configuration file

## Backing up the full configuration file

1. Go to *File > Settings*.
2. Expand *System*, and click *Backup*.



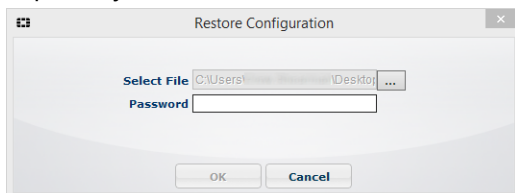
3. Click the *Browse* button to locate and select the file destination.
4. Choose one of the following options:
  - Select the *No Password* checkbox to save the file in an unencrypted format. You can also include comments in the configuration file.
  - Clear the *No Password* checkbox to save the file in an encrypted format with a password.



5. Click *OK*.

## Restoring the full configuration file

1. Go to *File > 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 is displayed. Enter the password used to encrypt the backup configuration file.
5. Click *OK*.

## Backing up and restoring command line utility commands and syntax

Fortinet provides administrators the ability to import and export configurations via the CLI. The `fcconfig` utility can be run locally or remotely as the system user (or admin user) to import or export the configuration file. In Microsoft 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:

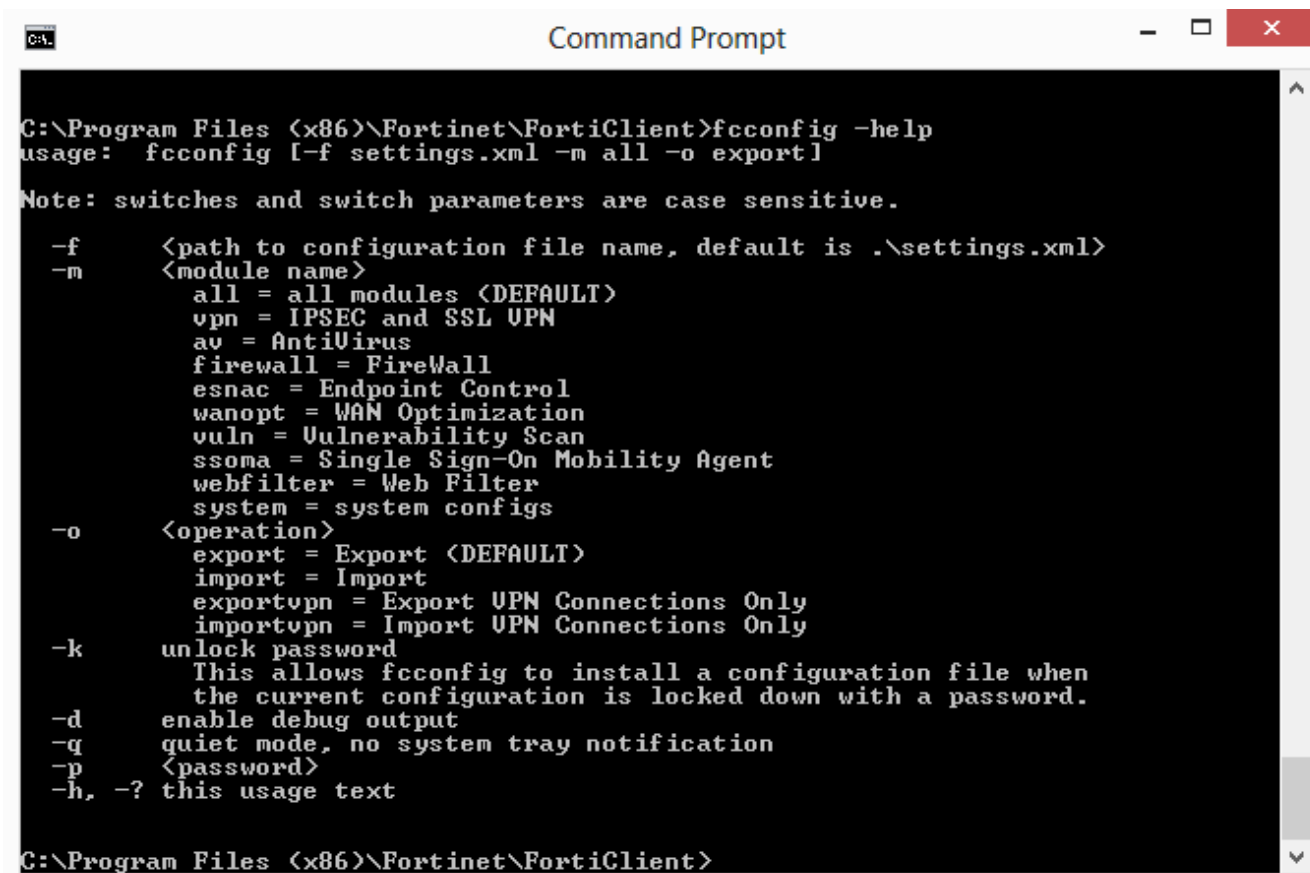
Command	Description
<code>FCConfig -m all -f &lt;filename&gt; -o export -i 1</code>	Back up the configuration file.
<code>FCConfig -m all -f &lt;filename&gt; -o export -i 1 -p &lt;encrypted password&gt;</code>	Back up the configuration file (encrypted).
<code>FCConfig -m all -f &lt;filename&gt; -o import -i 1</code>	Restore the configuration file.
<code>FCConfig -m all -f &lt;filename&gt; -o import -i 1 -p &lt;encrypted password&gt;</code>	Restore the configuration file (encrypted).
<code>FCConfig -m vpn -f &lt;filename&gt; -o exportvpn -i 1</code>	Export the VPN tunnel configuration.
<code>FCConfig -m vpn -f &lt;filename&gt; -o exportvpn -i 1 -p &lt;encrypted password&gt;</code>	Export the VPN tunnel configuration (encrypted).
<code>FCConfig -m vpn -f &lt;filename&gt; -o importvpn -i 1</code>	Import the VPN tunnel configuration.
<code>FCConfig -m vpn -f &lt;filename&gt; -o importvpn -i 1 -p &lt;encrypted password&gt;</code>	Import the VPN tunnel configuration (encrypted).



Switches and switch parameters are case sensitive.



Backup and restore CLI commands are an advanced configuration option.



```
C:\Program Files (x86)\Fortinet\FortiClient>fcconfig -help
usage: fcconfig [-f settings.xml -m all -o export]

Note: switches and switch parameters are case sensitive.

-f      <path to configuration file name, default is .\settings.xml>
-m      <module name>
        all = all modules (DEFAULT)
        vpn = IPSEC and SSL VPN
        av = AntiVirus
        firewall = FireWall
        esnac = Endpoint Control
        wanopt = WAN Optimization
        vuln = Vulnerability Scan
        ssoma = Single Sign-On Mobility Agent
        webfilter = Web Filter
        system = system configs
-o      <operation>
        export = Export (DEFAULT)
        import = Import
        exportvpn = Export VPN Connections Only
        importvpn = Import VPN Connections Only
-k      unlock password
        This allows fcconfig to install a configuration file when
        the current configuration is locked down with a password.
-d      enable debug output
-q      quiet mode, no system tray notification
-p      <password>
-h, -?  this usage text

C:\Program Files (x86)\Fortinet\FortiClient>
```

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

```
<?xml version="1.0" encoding="UTF-8"?>
- <forticlient_configuration>
  <forticlient_version>5.0.1.194</forticlient_version>
  <version>5.0</version>
  <date>2013/01/04</date>
  <partial_configuration>0</partial_configuration>
  <os_version>windows</os_version>
- <system>
  - <ui>
    <ads>1</ads>
    <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>
    <password/>
    <culture_code>en-us</culture_code>
    <gpu_rendering>0</gpu_rendering>
  </ui>
  - <log_settings>
    <level>6</level>
    <!--0=emergency, 1=alert, 2=critical, 3=error, 4=warning, 5=notice, 6=info, 7=debug, -->
    <log_events>ipsecvpn,sslvpn,scheduler,update,firewall,av,proxy,shield,webfilter,endpoint,fssoma,wanacc,configd,vuln</log_events>
    <!--ipsecvpn=ipsec vpn, sslvpn=ssl vpn, firewall=firewall, av=antivirus, webfilter=webfilter, vuln=vulnerability scan, wanacc=wan acceleration,
    fssoma=single sign-on mobility for fortiauthenticator, scheduler=scheduler, update=update, proxy=fortiproxy, shield=fortishield,
    endpoint=endpoint control, configd=configuration, -->
  - <remote_logging>
    <log_upload_enabled>0</log_upload_enabled>
    <log_upload_server/>
    <log_upload_freq_hours>1</log_upload_freq_hours>
    <log_last_upload_date>0</log_last_upload_date>
  </remote_logging>
</log_settings>
- <proxy>
  <update>0</update>
  <online_scep>0</online_scep>
  <virus_submission>0</virus_submission>
  <type>http</type>
  <address/>
  <port>0</port>
  <username>Enc 7aac3f27116b54f493ddeec98f010ee1bb2f9c8d4db3e884</username>
  <password>Enc 42f61986b5bc5d5882f716fd1f6b648fb91ead48a102dd31</password>
</proxy>
- <update>
```

## 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 > Add a new profile*.
2. Click *Advanced*.
3. On the *XML Configuration* tab, click *Edit*.  
Two panes are displayed. Use the pane on the right-hand side to edit XML.
4. On the *XML Configuration* tab, overwrite the XML 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 *XML Configuration* tab.
5. Click *Test XML*.

When valid, an *XML is valid* message is displayed. When invalid, an *XML is invalid* message is displayed. The XML must be valid before you can save the profile.

6. When the XML is valid, click *Save Profile*.

# 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 committed.



## RedundantSortMethod = 1

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

## RedundantSortMethod = 0

By default, RedundantSortMethod=0, and the IPsec VPN connection is priority based. Priority based configurations tries to connect to the FortiGate starting with the first on the 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 committed.

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

## Enabling VPN autoconnect

VPN autoconnect uses the following XML tag:

```
<autoconnect_tunnel>ipsecdemo.fortinet.com</autoconnect_tunnel>
```

Inside:

```
<vpn>
  <options>
```

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 tag:

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

Inside:

```
<vpn>
  <connection>
```

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)

### Create 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 committed.

### RedundantSortMethod = 1

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

## RedundantSortMethod = 0

By default, RedundantSortMethod = 0, and the IPsec VPN connection is priority based. Priority based configurations tries to connect to the FortiGate starting with the first on the 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 committed.

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

### Mapping a network drive after tunnel connection

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

```
<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 is disconnected

The script deletes the network drive after the tunnel is disconnected.

```
<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 is connected.

```
<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 is disconnected.

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

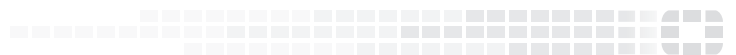
# Change log

Date	Change Description
2018-05-31	Initial release of 6.0.0.
2018-07-10	Updated description of <disable_connect_disconnect> in <a href="#">VPN options on page 32</a> .
2018-07-23	Initial release of 6.0.1.
2018-08-09	Updated description of <action_when_unavailable> in <a href="#">Web Filter on page 62</a> .
2018-08-30	Updated description of <action_when_unavailable> in <a href="#">Web Filter on page 62</a> .
2018-09-07	Initial release of 6.0.2.
2018-09-19	Updated description of <https_block_method> in <a href="#">Web Filter on page 62</a> .
2018-10-18	Initial release of 6.0.3.
2018-10-22	Updated description of <xauth_timeout> in <a href="#">IKE settings on page 43</a> .
2018-11-08	Updated <preferred_dtls_tunnel> in <a href="#">SSL VPN on page 33</a> .
2018-11-28	Updated description of <https_block_method> in <a href="#">Web Filter on page 62</a> .
2018-12-10	Initial release of 6.0.4.
2018-12-18	Removed <save_password> from <a href="#">VPN options on page 32</a> . Updated description of <ui> in <a href="#">Endpoint Control on page 23</a> .
2019-01-04	Added <a href="#">Removable media access on page 79</a> .
2019-01-31	Initial release of 6.0.5.
2019-02-06	Added <block_ipv6> to <a href="#">SSL VPN on page 33</a> and <peerid> to <a href="#">IKE settings on page 43</a> .
2019-02-14	Updated description of <use_windows_credentials> in <a href="#">VPN options on page 32</a> .
2019-02-20	Added <allow_admin_to_stop> to <a href="#">On-Demand scans on page 53</a> .
2019-03-26	Updated <a href="#">Certificate settings on page 21</a> and <a href="#">Real-time protection on page 49</a> .
2019-04-25	Updated description of <avatar_enabled> in <a href="#">Endpoint Control on page 23</a> .
2019-05-15	Initial release of 6.0.6.
2019-05-22	Added <suppress_vpn_notification> to <a href="#">VPN options on page 32</a> .
2019-06-19	Initial release of 6.0.7.
2019-08-08	Initial release of 6.0.8.
2019-11-13	Initial release of 6.0.9.
2020-04-28	Updated <a href="#">VPN options on page 32</a> and <a href="#">SSL VPN on page 33</a> .
2020-09-08	Initial release of 6.0.10.

Date	Change Description
2020-10-20	Added <code>&lt;block_outside_dns&gt;</code> to <a href="#">IPsec VPN on page 38</a> and <a href="#">IKE settings on page 43</a> .



**FORTINET®**



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.