



# AppGate Clients

The AppGate client from Cryptzone is the user's interface to the online resources that are protected by the AppGate Security Server. It allows the user to securely access applications and services in a VPN-like manner. The AppGate system will grant each user unique access rights according to a pre-defined security policy. There are different client types available, which are useful in different scenarios and on different types of platforms.

## The AppGate Client

The AppGate Client from Cryptzone is the standard client used on workstations and desktop systems. It displays a set of icons to the user, each icon representing a service available on the secured network. The client is Java based and can therefore run on most types of systems, 32- and 64-bit. It comes in three flavors: one which is pre-installed on the user's system, an applet version, and another which can be downloaded from the AppGate server using a web browser when it is needed.

The downloadable version of the AppGate client is based on Java Web Start technology, which makes it completely self-updating. It is therefore easy to manage in larger organizations and in environments where it is not possible to centrally update the software on client systems, such as for home users. This is the recommended client to use.

The AppGate Client runs on most platforms such as Windows, Mac, Unix and Linux.

## USB Client

There is also a USB Client available, an AppGate client pre-packaged on a USB stick together with its own operating system. The USB client does not rely on, or use, the ordinary operating system on the machine. Instead it executes in a secure and trusted environment making it possible to access remote applications without having to trust the operating system on the user's computer.

The USB client does not use the user's hard disks at all and will leave no traces on the client when it is shut down. For more information, please see the USB Client Datasheet.

## Android and iOS apps

The new clients for Android, Apple iPhone, iPad and iPod Touch devices are now available on the Android and Apple app stores. The AppGate Client requires Android OS 2.1 or later, or iOS 4.2 or later, and requires an AppGate Security Server 10.0 or later.

The client supports several authentication methods including: password, Cryptzone OTP, Radius, and Chained methods.

## Mobile Client

The Mobile client is designed for mobile devices such as smartphones and PDA's. The Mobile client can support "over the air provisioning" enabling installation and configuration of the client with a minimum of user interaction. It is also possible to setup and automatically configure the smartphone's built-in email client with the necessary settings from the AppGate server. This makes the solution extremely easy to use for the end user and virtually no user training is required.

AppGate clients are available for Windows Mobile and Nokia Series 60 (Symbian) devices.

## Client-less access

It is also possible to use standard web browsers and their built-in SSL support to access web based services securely through the AppGate system in a client-less manner without having to download or install any software on the client at all.

The AppGate SSL module enables true client-less access and is an option when only web-based

The flexibility of the AppGate Client enables the system administrator to control the user experience and control network security

applications need to be accessed. It is useful in situations when there is no need for, or when it is not possible to use, a full client eg. when reading email on an airport PC.

## Client check and client commands

The AppGate server can send a command or a set of commands to the clients to be executed. Based on the results of these commands, the server can make decisions about what services should be made available to the user. Typical this is used to check what kind of system the user is using; for example whether it is a corporate workstation, if it has a personal firewall installed, if the anti-virus software is updated, etc. It is also possible to connect to the Windows Security Center to perform tests.

Based on the outcome of these tests, the system can offer suitable services to the user. Similar functionality is often referred to as network access control (NAC/NAP) although here it is used to give individual users access to individual applications.

## User messages

The administrator can create a “message of the day” which is displayed to all users when they log in, or create conditional messages that are displayed if certain access criteria are met: for example to inform users that a particular service is no longer available; to ask users without personal firewalls to contact the help desk before all services can be enabled; and to inform users about various conditions in the system before they request assistance from the help desk.

# AppGate Clients: Key Features and Benefits

---

## Intuitive graphical user interface

The AppGate client is easy to use and its portal-like user interface requires virtually no user training.

## Wide platform support

The AppGate clients run on most systems such as Windows, Unix and Linux systems and also on mobile phones from most vendors, PDA's and tablet computers. The USB client is an option for use with an untrusted computer eg. a home PC or in an Internet café.

## Automatic client updates

The “Java Web Start” functionality of the client ensures that it automatically updates itself if needed so that users always have the latest version of the client installed. This makes deployment of new clients extremely easy.

## Compression

Traffic is encrypted and compressed to increase performance on slower network links. This is particularly useful on mobile devices where users pay for the amount of data transferred. Text messages are typically compressed to less than half their original size.

## Cleaning of web cache

The clients can automatically clean the web cache for Internet Explorer users.

## Proxy traversal

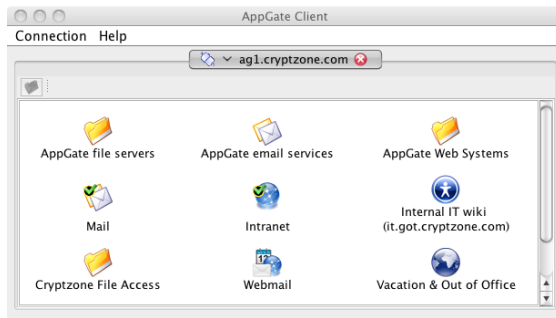
The clients can be configured to traverse both Socks and HTTP proxy servers. This is useful for users working behind firewalls that require a proxy to reach out to the Internet. Both Basic and NTLM authentication are supported for HTTP proxies, which is useful for example to pass through an ISA server. The clients are also insensitive to network address translation, NAT, which may be performed to outgoing traffic by some firewalls.

## User roles

Users can have several roles, for example being members of different projects. When logging in, the user can actively choose which role to take during a session. Roles can be combined to streamline the user's experience if the administrator allows. The administrator can even define access rights based on type of client software and type of system being used; all to enhance the user experience and make it easy and intuitive to use the system. For example, some services such as file sharing may not make sense on a mobile phone.

## Intuitive user interface

The AppGate Client's graphical user interface displays icons showing each user which applications they can use. The available services can vary depending on a wide range of criteria, for example, time of day, authentication method being used, whether a personal firewall is installed on the device or not, etc. The client's icons make it possible for the user to see the applications and services they are currently able to access making the system user-friendly and saving many calls to the help desk.



The portal-like user interface makes the user's interaction with the security system transparent. When a user clicks on an icon, a request is sent to the AppGate Security Server to enable traffic for a particular application. The server logs this request and if it is granted, the client receives an OK and can then start an application for the user, for example a mail reader or a web browser. This mechanism ensures that only traffic to applications that are currently needed are enabled by the server. Access to all other applications is closed until explicitly requested by the user. This is a security-enhancing feature appreciated by many security professionals.

In environments where many services are offered to users, it is possible to group services into folders and to create a "tree view". The user experience is then very similar to a file browser. Multiple connections to other AppGate servers are also supported and are displayed as "tabs" in the main window.

The user experience can be fully customized, and the icon view can even be hidden so that, after successful authentication, the user simply gets a message that he or she is connected. The client hides (iconifies) itself and disappears from the desktop. Pre-configured services can be started automatically without requiring any user interaction via the icons. The AppGate Client can also be configured to exit automatically when the user closes the application, for example a Citrix client.

## Seamless mobility

AppGate clients\* can be allowed to automatically reconnect to the server if the network link is changed or lost, or if transmission changes from 3G to 2G or Wi-Fi. This is a useful feature when using mobile devices where network availability may come and go. Automatic reconnects are even possible when the IP address of the client changes, for example when a laptop switches from a wired network to a wireless connection.

The reconnection to the system is completely transparent to the user and the applications in use, and provides true mobility with the ability to move freely between networks.

*\*Roaming is not available for Apple iPhone, iPad and iPod Touch devices.*

## IP tunneling driver (IPTD)

The standard AppGate Client is able to handle most protocols without help. Occasionally there may be a particularly cumbersome protocol that must be supported or it may be necessary to give a user full access to a remote network, not just to a finite number of applications. This becomes possible by installing the AppGate IP Tunneling Driver (IPTD).

The IPTD module creates one or more virtual network interfaces (the administrator sets the maximum number of interfaces at installation) that announce to the operating system that there is a direct connection to the remote network. There are virtually no limitations to the applications and protocols that it will support. Features include:

- Full UDP, TCP and ICMP support.
- Full connectivity between networks where "wild cards" can be used to specify port, host and network addresses.

The IP tunnelling driver is available for Windows 2000, XP, Server 2003, Server 2008, Vista, Windows 7, Linux and Mac OSX.

## Comparing client features

	AppGate Client	Client for multi-user systems	Client with IPTD	USB Client	Mobile client (smart phones)	Android, iOS devices	Client-less via web browser
True client-less access using web browsers' built-in support for SSL							•
Automatic client updates	•	•	• <sup>2</sup>	•		•	N/A
Portal-like GUI for user interaction	•	•	•	•			•
Client can be used on multi-user systems, Citrix and Terminal Servers		•					•
Automatic and seamless connect and disconnect without re-authentication	•	•	•	•	•		
Native code for encryption <sup>3</sup>	•	•	•	•	•		•
TCP support for most application-level protocols	•	•	•	•	•	•	
Unlimited protocol support			•	•		•	
Application-transparent host-name resolution <sup>4</sup>	•	•	•	•	• <sup>5</sup>	•	•
Windows native file sharing (mount using drive letter)			•				
Remote file access (GUI)	•	•	•	•			•
X-windows support	•	•	•	•			
Client check functionality (similar to NAC and NAP)	•	•	•	•			
Password and token authentication	•	•	•	•	•	•	•
Soft certificate user authentication	•	•	•	•	•		
Smart card support via PKCS#11 and MSCAPI <sup>6</sup>	•	•	•				
Enforcing server-specified firewall policies on clients	•		•				
Secure Local Print support (remote applications can print on user's local printers)	•	•	•				

<sup>1</sup> IP Tunneling Driver supported on Windows, Mac OS X and Linux

<sup>2</sup> IPTD currently not auto-updated

<sup>3</sup> On Windows, Solaris, Linux and some mobile platforms

<sup>4</sup> Windows Vista and later need the AppGate host file writer or IPTD companion installed for this feature

<sup>5</sup> Platform dependent

<sup>6</sup> On Windows platforms

Cryptzone solutions mitigate information security risks identified in four key areas of Policy Compliance, Content Security, Secure Access and Endpoint Security.

The AppGate solution from Cryptzone enables organizations to provide controlled access for all authorized users regardless of their location whilst also ensuring network resources are protected against internal and external threats. This award-winning technology combines an application layer firewall with device security and granular access control system in one easy to use, cost effective system.

Cryptzone Group AB  
 Drakegatan 7,  
 SE-412 50 Gothenburg,  
 Sweden  
 Tel: +46 (0)31 773 86 00

United Kingdom  
 Tel: +44 (0)370 013 1600

United States  
 Tel: +1.949.279.6177

info@cryptzone.com  
 www.cryptzone.com