

In a world with fewer borders, the demand for network security changes from security at the gate to security at the source. AppGate is the leader in this space with a solution that protects applications, communication and secures end-point devices. The AppGate solution supports all types of networks, fixed, wireless and mobile and is easily integrated into existing customer environments.

Clients for all kinds of systems

The client software is Java based which makes it possible to install and run it on almost all types of systems and platforms. There is a choice of client software for different types of systems:

- **AppGate Client** is the client used on workstations and desktop systems. It displays all available services to the users as a set of icons, each representing a service available on the secured remote network. The client can either be pre-installed or be downloaded from the AppGate server through a web browser when it is needed. It is automatically updated if a new version becomes available on the AppGate server.
- The **Applet** has similar functionality although it is designed to be as little intrusive as possible on the target system. It therefore fits in environments with limited hardware capabilities or where very old or limited versions of Java is installed. This client requires very little from the host system but has a limited user interface. The applet can be downloaded from the AppGate server in almost any web browser and is primarily targeted for users on public workstations for example on airports and Internet kiosks.
- The **Mobile client** is a client designed for mobile devices such as PDAs and Java-enabled telephones.



Key features and benefits

Wide platform support: The client runs on most systems including all (32-bit) Windows versions, Unix and Linux systems, PDAs and mobile phones from Sony Ericsson, Nokia, Qtek, and many more. The applet client can be used in public access areas such as in airports and Internet kiosks.

Minimal System modifications: The AppGate client executes as an ordinary application and requires no reconfiguration of the underlying operating system. This makes it possible to run the client on almost any type of system including systems owned by partners and by home users.

Automatic client updates: The AppGate client supports the “Java Web Start” feature which ensures that all users always have the latest version of the client installed, and it automatically updates the clients if needed. This makes deployment of new clients extremely easy.

Compression: Traffic compression can increase performance on slower network links. It is also useful on mobile devices where the users pay per byte being sent. Plain text messages are typically compressed to half the original size.

Flexible authentication: The client supports a very wide range of authentications methods such as passwords, token cards, certificates, Smart Cards and biometric authentication.

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

Intuitive graphical user interface. The AppGate client is easy to use, requiring virtually no user training. The user interface can be changed to suit different users and environments, for example the login dialog can be told to only display available authentication mechanisms and to only display a few options to the user.



The login dialog

Proxy traversal: The client can be configured to traverse both Socks and HTTP proxy servers. This is useful for users located behind firewalls that require a proxy to be used to reach the Internet. The clients are also insensitive to NAT (network address translation), which may be performed by some firewalls.

Highly configurable: It is possible to configure the look and feel of the clients, menus and options can be pre-configured or removed from the user interface if desired. Central configuration by systems administrators is supported.

Roaming: The roaming functionality in the clients allows automatic reconnects if the network link goes down. It can be done without any user interaction with the system. This is useful in environments where network connections come and go, for example when moving between different base stations or carrier networks. Roaming is even possible when the IP address of the client changes and it is transparent to running applications.

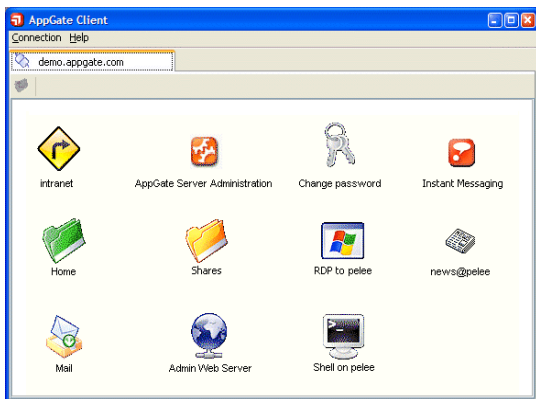
Client check and client command: The clients can execute a server-defined command that checks client configuration before access to certain services are granted. This command can also instruct the client to do some actions, for example to update some software or to reconfigure the client.

User roles: Users can have several roles, for example being members of different projects. When logging in, the user can actively choose what role to take during a session. The AppGate server can offer users tailored services based on the client software and type of system being used; all to enhance the user experience and make it easy and intuitive to use the system.

AppGate Client user interface

The AppGate Client allows users to see what applications are available from the AppGate server. Since available services can vary depending on, for example, time of day, whether a personal firewall is installed or not and the authentication method being used, the icons makes it possible for the user to see what applications and services it is currently possible to access. This feature is not just user-friendly; it can also save many calls to the customer help desk.

The portal-like user interface makes users unknowingly interact with the security system. When a user clicks on an icon, a message is (invisibly) sent to the AppGate server to request traffic for an application. The request is logged by the server and if it is granted, the client receives an OK and can then start the 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 in the security server.



Client view when logged in

In environments where many services are offered to users, it is possible to group services into folders (to have a “tree view”). The user experience is 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 customised, and the icon view can even be hidden so that a user, after successful authentication, only gets a message that he/she is connected and then the client iconifies itself and disappears from the desktop. The flexibility of the client makes it possible to fully control the user interface and appearance by the system administrator.

When the user iconifies the client, it will hide in the system tray indicating that a secure connection exists. The window can be restored anytime simply by clicking the icon in the system tray.



AppGate Client visible in system tray

Client check and client command feature

The AppGate server has the possibility to send a command or a set of commands to the clients to be executed. Based on the result of these commands, the server can make decisions about what services should be available to the user. Typical use is to check what kind of system the user is using; for example whether it is a corporate PC, if it has a personal firewall installed, if it has anti-virus software, etc., and based on that offer suitable services to the user.

Roaming

The roaming functionality in the clients can be configured to do automatic reconnects to the AppGate server (invisibly to the users), if the network link is changed or goes down. This is useful, for example, when using mobile devices where network connections may come and go. Automatic reconnects are even possible when the IP address of the client changes without affecting running applications, for example when a laptop switches from a wired network into a wireless connection. This gives user true mobility and the freedom to move arbitrarily between networks.

AppGate IP tunnelling driver (IPTD)

An AppGate system is normally configured to give access just to a number of pre-defined applications. However, 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. This is possible by installing the AppGate IP Tunnelling Driver (IPTD).

The IPTD module creates a virtual network interface that announces to the operating system that it has a direct connection to the protected network. Thus it has virtually no limitations of what applications and protocols it supports. Features include:

- Full UDP, TCP and ICMP support, full connectivity between networks and wild-cards can be used to specify port, host and network addresses.
- It is available for Windows 2000, XP and 2003 server, Linux and Mac OS X. Future releases will support even more platforms.

The possibility to use the IPTD module makes the AppGate system a safe investment, since system owners now know that all protocols can always be supported by the system.

User messages

The administrator has the possibility to define a “message of the day” which is displayed to all users when they log in. In addition, it is possible to display conditional messages to users based on the same parameters as services are decided upon, for example to inform external users of smart cards that a particular service may no longer be available; to ask users without personal firewalls to contact the help desk before all services can be enabled; etc. This makes the AppGate server an ideal message system to inform and help users and to tell them about various conditions in the system.

Comparing the clients

	AppGate Client	Applet	Mobile Client
Automatic client updates using Java WebStart	✓		
Portal-like GUI for user interaction	✓		
Simultaneous connections to multiple AppGate servers	✓		
Clients can securely be used on multi-user systems such as Citrix and Microsoft Terminal Servers	✓		
Roaming, seamless connect and disconnect from networks	✓	✓	✓
Native code for encryption ¹	✓	✓	
TCP support	✓	✓	✓
UDP and ICMP support ⁴	✓	✓	
Full IP traffic support ⁴	✓	✓	
NetBIOS network file sharing	✓	✓	
X-Windows support	✓	✓	
Client can run server-provided commands at startup ("client check")	✓	✓	
Passwords and token card authentication	✓	✓	✓
Certificate support for user authentication	✓	✓	
Smart card support ²	✓	✓	
Enforce Server-specified Personal Firewall policy ²	✓	✓	
Application-transparent host name resolution ³	✓	✓	✓ (5)
Secure Local Print support	✓	✓	

(1) On Windows, Solaris, HP-UX and Linux platforms

(2) On Windows platforms

(3) With proper write permission on hosts file

(4) With IP tunnelling Driver installed which is supported on Windows-2k and later, Mac OS X and Linux

(5) Depends on platform