

# How the Appgate Security Server works

For authorized users, the Appgate system provides fast, easy access to multiple applications through a single logon procedure - while protecting user traffic through encryption and tunneling, and enforcing highly granular security policies.

## Easy to use, easy to implement

The application solution is a plug-and-play, appliance-based, turnkey offering based on:

- Appgate Server protects the hosting site and controls all accesses to application servers
- Appgate Client software for end-user access
- Optional Personal Firewall to protect user workstations
- Optional client check functionality for social media control
- Optional SMS authentication software
- A Secure local print module to allow remote applications to print to printers at the user's local network

The Appgate system ties together all the pieces of security technology required for premium security - authentication, authorization, tunnelling, encryption, policy management, activity logging and reporting in one easy-to-administer solution.

## Easy access for authorized users

Authorized users - employees, partners or customers - identify themselves to the network through the enterprise's preferred authentication methods, and then can access the specific resources for which they have access privileges, based on who they are and their role with respect to the enterprise. Users can access their approved resources from any wired or wireless network using Macintosh, Windows and Unix-based workstations and other hand-held devices such as Smartphones. This enables users to become truly mobile in a fully secure way.

Fine-grained access control restricts or allows access based on the user's identity, user's location, authentication method, day of week and time of day. Powerful encryption prevents eavesdropping and detailed audit trails register every log-in, attempted log-in, application use and suspicious activity.

## Key features and benefits

**No client system modification.** The Appgate clients execute as normal applications on the user's workstation and require no modification of the underlying operating system. There is no requirement for the IT department to have to "enable" the access software. If needed, the client software can even be user downloaded from the Appgate server.

*"Users can access their approved resources from any wired or wireless access point"*

**Intuitive graphical user interface.** Appgate clients are easy to use requiring virtually no training. The user starts the client just as any other windows application. A dialog box asks the user to sign on and the server either automatically opens up traffic to the approved applications or displays a window of icons showing the available applications and from which the user can select an application.

**Central administration.** All Appgate servers including server clusters can be centrally administered through a intuitive easy-to-use GUI.

**Easy to integrate.** Appgate servers are easy to integrate into the existing IT infrastructure. Flexible hardware and software makes it possible to protect network segments, application servers, or even the whole network with the Appgate server acting as a policy server.

**Mobility.** The Appgate clients run on a variety of systems and devices to make the users truly mobile. Anything from workstations to Smartphones can be used to access resources protected by an Appgate server.

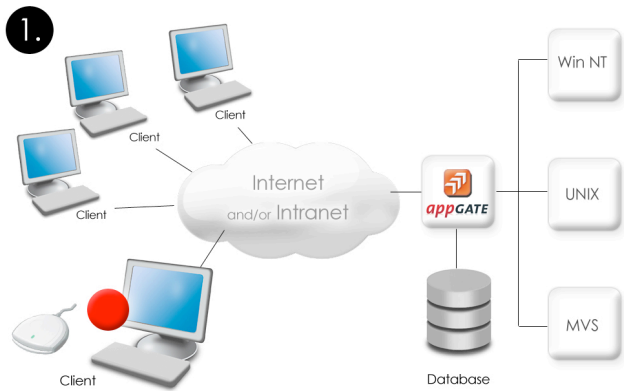
*"Easy access to multiple applications through a single logon procedure"*

## Step-by-step a typical Appgate session

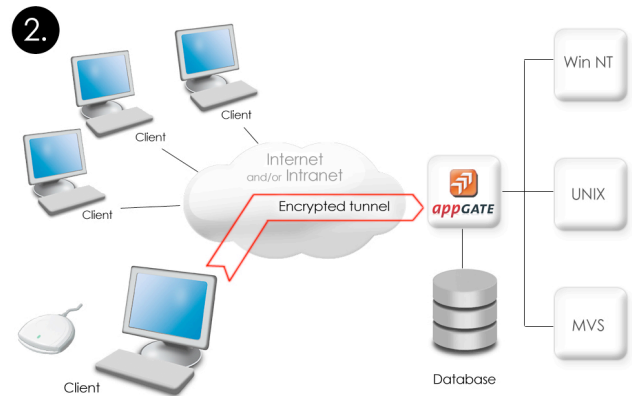
The Appgate system is intuitive for users, using these steps to initiate a user session:

1. When the user starts a session, the Appgate client sets up an encrypted tunnel to the Appgate server. The traffic is encrypted by the SSL or SSH protocol and the client software begins with verifying the servers identity.
2. The Appgate server authenticates the user, for example through a pass-word, a certificate, SMS or a token device such as SecurID. User identities can reside on the Appgate server or on an external AD or LDAP database server.
3. The Appgate server checks the user's identity against a database of authorized users and access privileges.
4. The AppGate server can check the user's computer and its configuration. The results of this check can be used in the next step when the server decides what services should be available.
5. The system checks what services and applications should be available to the user. Each service has a set of rules defining under what circumstances it should be available. For example, access to a network disk could be allowed after password authentication when the user is connecting from the local LAN, but may require SecurIDTM authentication when connecting from elsewhere.
6. Available services are displayed to the user in a window. By clicking an icon in the window, the service is enabled and an application can be started. For example, clicking the mailbox icon enables traffic to the mail server and launches the user's mail program.

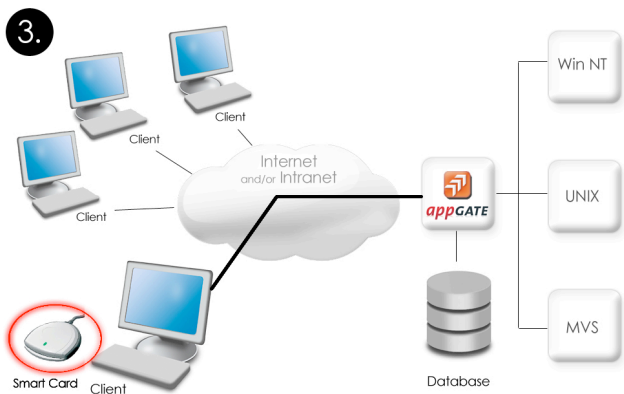
# Step-by-step guide



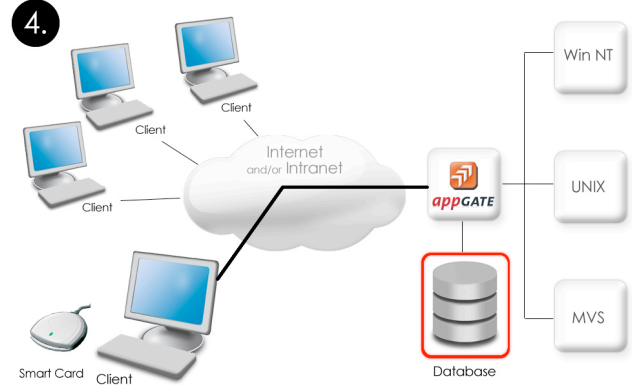
The user starts the AppGate Client. It is either a pre-installed client or a java webstart application downloaded from a web server. Almost all Java-enabled platforms are supported, from workstations to hand-held devices such as Smartphones



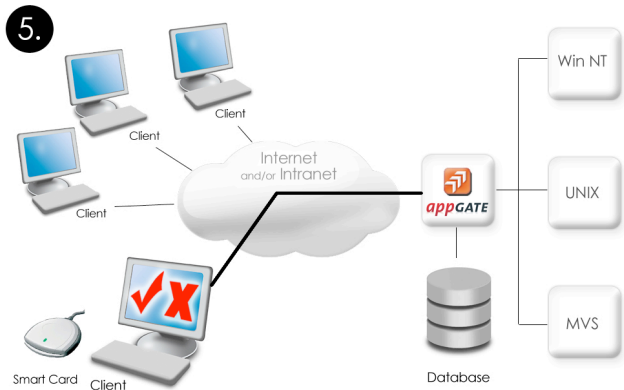
A secure encrypted connection, a tunnel, is set up between the user and the AppGate server. Strong ciphers such as AES with up to 256-bit keys are supported. All traffic is sent inside this tunnel.



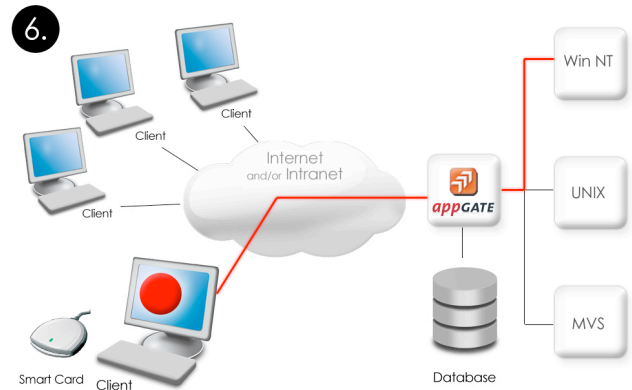
The AppGate Server requires the users to authenticate themselves. Most authentication methods on the market are supported.



The AppGate server grants access only to selected applications based on rules and parameters stored in its authorization database. Each user or category of users can have their own rulesets defined.



The client has a portal-like user interface that shows each user what applications currently are available. Starting an application is just a mouse-click away.



Traffic is encrypted and user actions are logged in detail to enable security audits or to support accounting. Many applications can benefit from the single sign-on functionality offered by the AppGate server.