

# AppGate Free Edition

Getting started Manual



# Getting started - AppGate Free Edition

The AppGate Free Edition is a virtual appliance that can be downloaded and run in VMware or Virtual Box virtualization systems.

## Overview of an AppGate Security Server

The AppGate Security Server (AGSS) allows secure and controlled access to resources on protected servers regardless of client location. This is achieved by placing an AGSS between all users and the servers, ideally as close as possible to the servers. Access to the servers is done through the AGSS which encrypts all traffic between the AGSS and the client while only granting access to those who should have it – essentially acting as a gateway or proxy.

All client software is available from the AGSS itself via the built-in web server. The recommended client type is the Java Webstart client. This client requires no installation and can be launched by simply clicking on a launch button on the AGSS web page. For some type of services some additional software may be needed on the client computer. These packages are also available from the AGSS. Clients are available for a very wide range of computing platforms:

- Windows
- Mac OS X
- Linux
- Mobile devices: iPhone, iPad, Android, Nokia smart phones and Windows Mobile devices (CE 5, & 6)

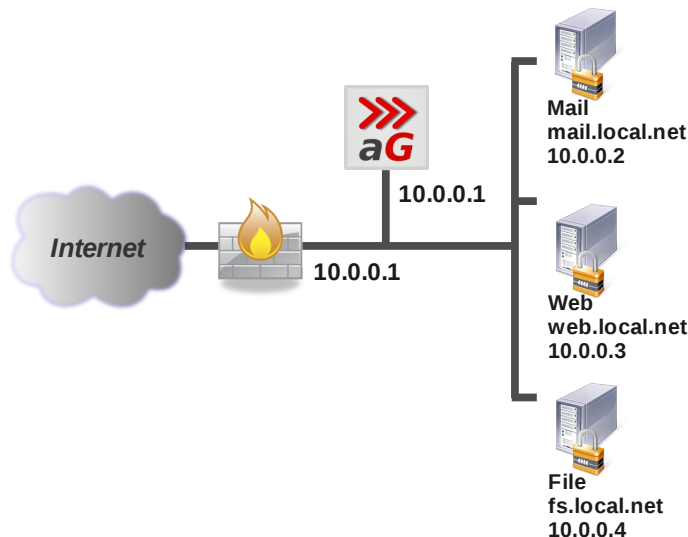
Optionally the AGSS can provide client less access to we and file services through using https and a web browser.

## Before starting the installation

Before starting the installation it's important to know that this guide walks you through how to setup a very common and simple configuration.

This guide will help you setup the following:

- The AGSS will be located behind an existing firewall (aka Internet gateway or NAT-bridge).
- The AGSS will use it's internal database, called Local Accounts, to keep track of the users. External account databases can also be used (eg. Active Directory). Consult the manual for how to do this.
- In our example the AGSS will provide secure access to an email, web and a file server.



## Downloading

The latest version is available after registration at <http://www.cryptzone.com/products/agafe/>.

The AppGate Free Edition can be downloaded as either a .vmx package or a .ovf package. For VMware Player and Workstation the .vmx is recommended. For VMware ESX and VirtualBox the AppGate .ovf package is recommended. A program from VMware called ovftool can be used to upload it to an ESX system.

The AppGate Free Edition packages are compressed with 7zip ([www.7-zip.org](http://www.7-zip.org)). Unpack the AFE file in a suitable position.

## Setting up a VMware Image

If you do not have a VMware player, workstation or ESX you need to install this before continuing see [www.vmware.com](http://www.vmware.com). Follow the instructions from VMware on how to setup it if necessary.

Using the VMware Workstation or VMPlayer open the AFE-vmware.vmx file in the directory where the distribution was unpacked.

If you are using ESX and the ovftool from VMware, load the AFE-vmware.ovf to your ESX from the command line using:

```
ovftool AFE-vmware.ovf vi://username:pass@my_esx_host
```

Start the image.

## Setting up a VirtualBox image

- If you do not have VirtualBox installed you now need to install this before continuing ([www.virtualbox.org](http://www.virtualbox.org)). Virtual Box version 3.0.8 or later is required.
- Open the VirtualBox GUI and select File -> Import Appliance ..., import the AFE-vmware.ovf image.
- Start the image

## Initial configuration

The AppGate Free Edition Image is preconfigured with the IP address 192.168.0.220/24.

In most cases it's necessary to change this IP address to a free IP address available on the internal LAN and in the same subnet as the internal address of the gateway. This is described below. We will also set a password for the AGSS administrative user agadmin.

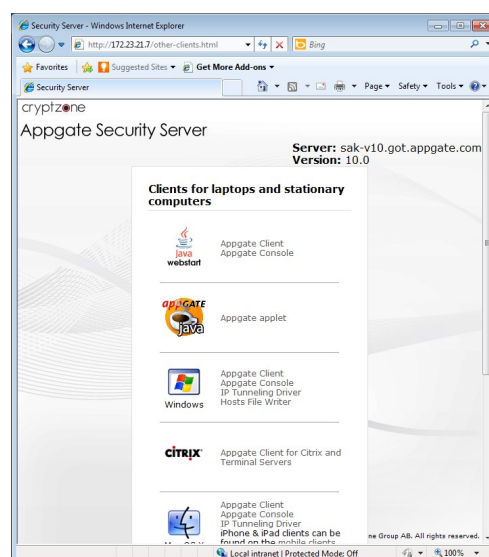
- Using the virtual machine console, login using the account name "root" and the password "changeme".
- Run the following command: "ag\_ipconfig a.b.c.d/m" where a.b.c.d is the new IP address and m is the new netmask. Ex "ag\_ipconfig 10.0.0.42/24". A default gateway can also be provided, ex "ag\_ipconfig 10.0.0.42/8 10.0.0.1".
- Run the command "ag\_passwd\_util agadmin" to set a secure password for the administrative user agadmin.
- Run the command "passwd.rootonly" to set a secure password for the root user.
- All subsequent access will be done through the standard AppGate Console.

## How to start the AppGate administration console

Most of the administrative tasks on AGSS are done using the AppGate Console.

To start the AppGate Console:

1. Start a web browser and enter the IP number of your AGSS (eg. <http://192.168.0.220> if on the internal LAN or the external address of the gateway, see section External access).
2. Select "List Clients for Desktops and Laptops" at the bottom of the page.
3. We recommend the AppGate Console in the [Java Webstart](#) section - it will ensure you are using the correct Console version together with your Appgate.
4. You can also install the AppGate Console, use the [Windows](#) section to install a stand-alone version for Windows.

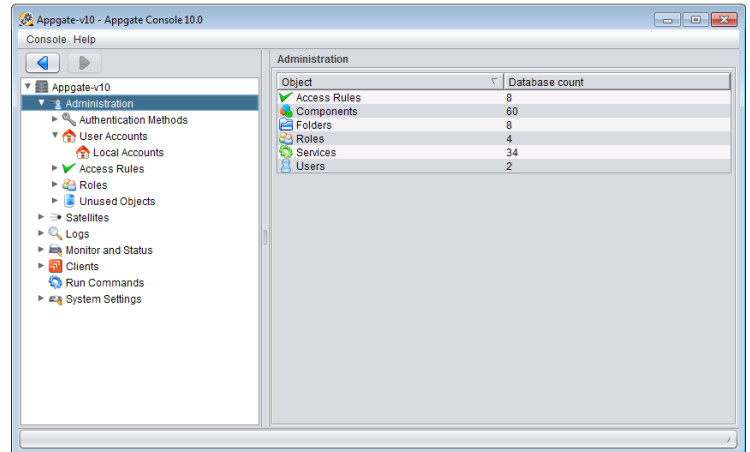


The Console will launch. Click “OK” if any prompts about accepting the program appears. Login with user agadmin using the password that was created earlier.

## Using the AppGate Console

The AppGate Console is used for almost all administration. The principal way of navigating within the console is the tree view on the left side of the console window.

Throughout this guide we will use the following notation to help you find any required settings: **Administration -> User Accounts**. This indicates that the subtree under Administration must be opened where an entry User Accounts is located.



## Add your license

When registering for the AFE download you should have received the free edition license via email.

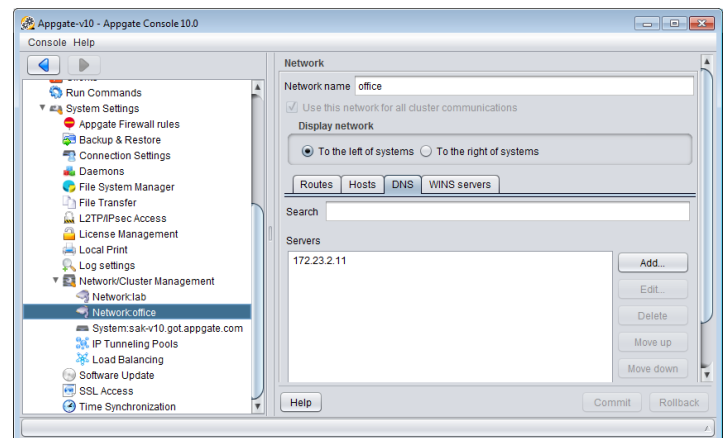
- Copy the entire license blob from the email to the clipboard.
- Go to **System Settings -> License Management -> Add...**
- Click on “Paste from clipboard”

## Setup DNS or hostname mappings

The AGSS must be able to resolve host names to the IP numbers it is providing access to. If a DNS service is available on the internal network this should be used, otherwise static mappings between host names and IP numbers may be used.

- DNS is set under System Settings -> Network/Cluster Management -> Network: *your-network* -> DNS
- If DNS is not available, click on the Hosts tab. Add each servers IP number and IP name. Use the full name, ie mail.local.net instead of mail, e.g:

IP address	Hostname
10.0.0.2	mail.local.net
10.0.0.3	web.local.net
10.0.0.4	fs.local.net



Press **Commit** to apply any changes in Network/Cluster Management to the AGSS.

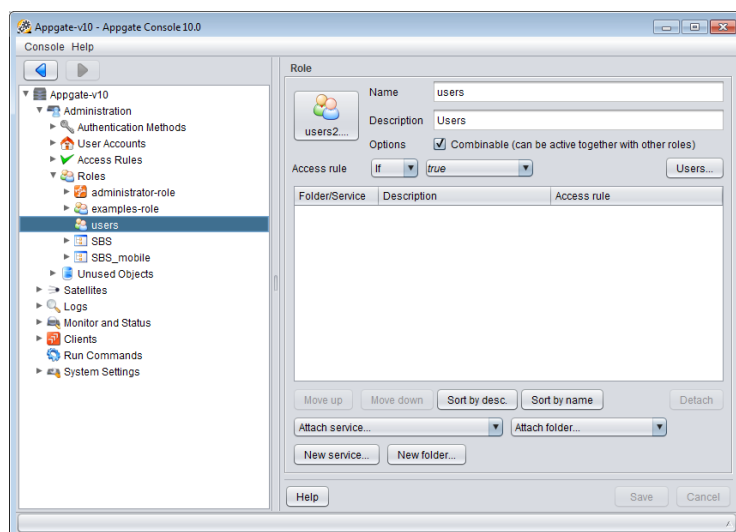
## Create a user Role

The most important concepts when administering an AGSS are the Users and the tree structure of Roles, Services and Components. Users may belong to zero, one or several Roles. A Role provides a number of Services. A Service is some useful entity to the user, for example access to email or access to the internal web or some application or a network. A Service is constructed from Components which we will cover in more detail later on.

Another key concept is that AppGate is *providing access* instead of *blocking access*. This means that the default is to provide no access. Only users with at least one Role assigned to them will be able to login, and access will be granted only to the Services available within that Role.

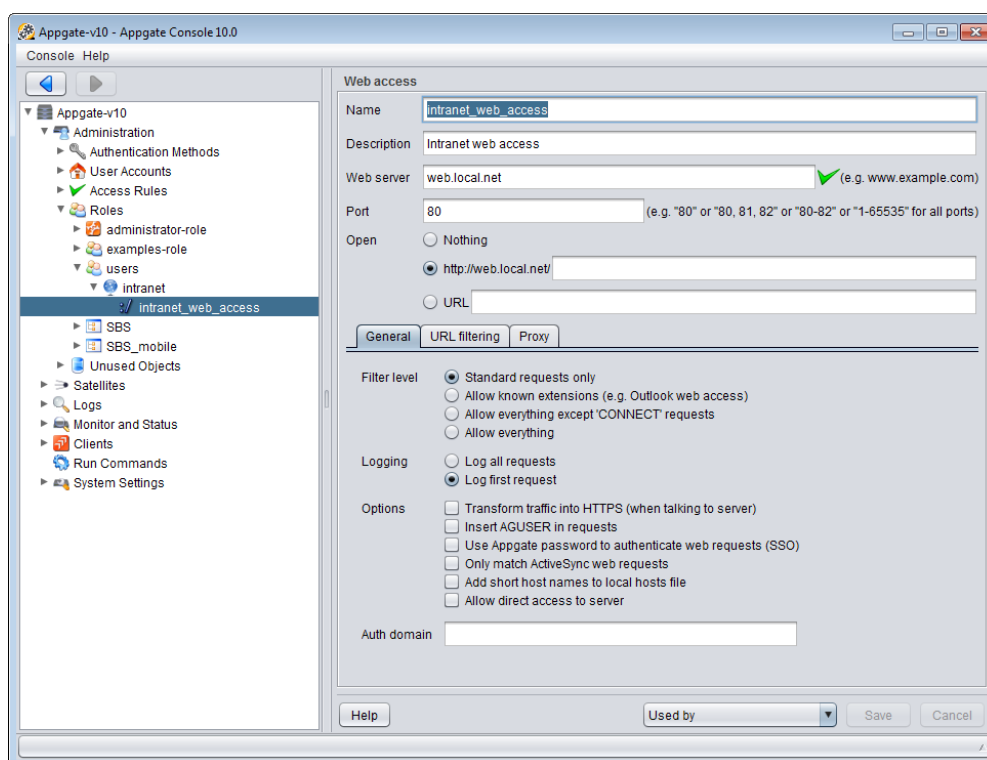
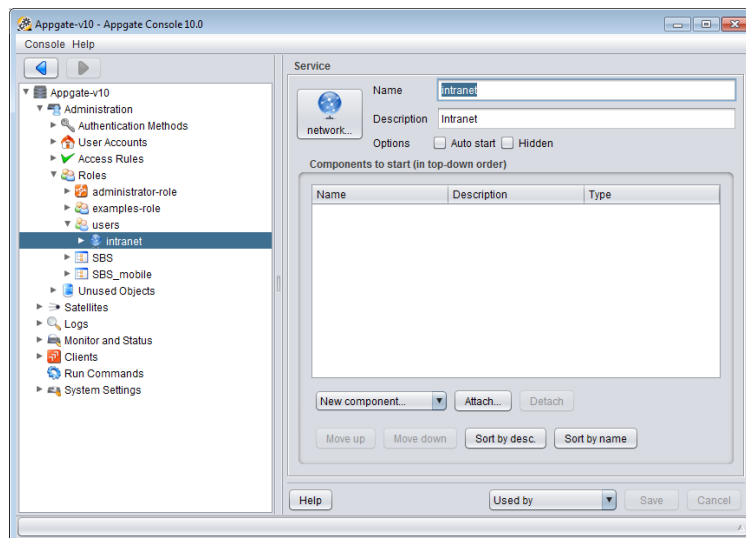
To create a Role for a typical user:

1. Go to **Administration->Roles**, click on "New Role".
2. Change the name to "users".
3. Click on the icon box and select an icon
4. Click on Save.



## Create a service for the internal web

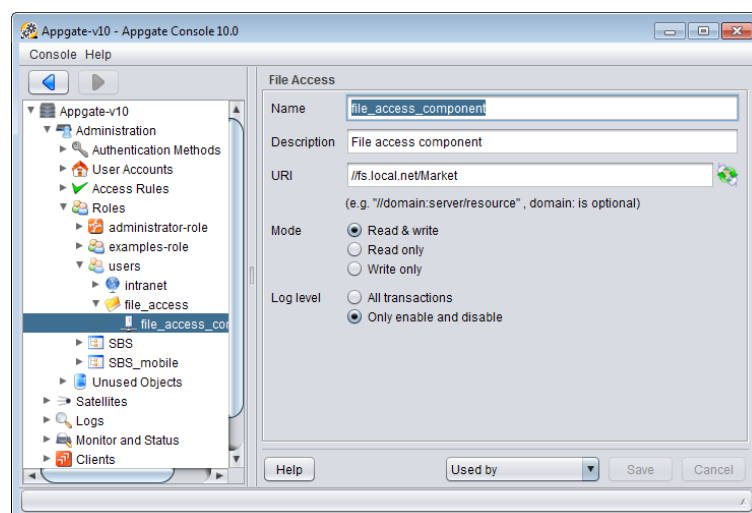
1. Make sure you are in **Administration->Roles->users**
2. Click on “New service”
3. Change name to “intranet”
4. Change the icon to something nice.
5. From the drop-down-menu “New component” select “Web Access”.
6. Change the fields to match the screen shot below. If you use different IP numbers and host names, change accordingly.
7. Click “Save”.



## Create a service for file access

The AppGate File access component provides access to Windows file servers (or Samba servers).

1. Select **Administration->Roles->users** again and click on "New Service".
2. Change the name to "file\_access" and the description to "File Access".
3. Change the icon to something nice.
4. Add a "File Access" component from the "New Component" menu.
5. Name should read "file\_access\_component", description "File Access Component" and the URI "//fs.local.net/Market". If the file server (fs.local.net) has a different name use that. "Market" is the name of the share to be accessed. The share will mount as the user that authenticates in the Appgate Client.
6. Click "Save".



## Create a service for email access

An ordinary email access service will be slightly more complicated (Outlook/Exchange is even a bit more elaborate) This is due to the fact that email typically uses not one but two or three different servers. Imap (or sometimes the older protocol Pop) is used to read emails, Smtplib is used to send emails and in some environments Ldap is used to access the company directory.

1. Select **Administration->Roles->users** again and click on "New Service".
2. Change the name to "email\_access", description to "Email" and the icon to something nice.
3. From the dropdown menu "New Component" add an "IP Access" component. Change the name to "imap\_ip\_access", description to "IMAP IP access", destination host to "mail.local.net" and destination port to "143".
4. Add another "IP Access" component. Change name to "smtp\_ip\_access", description to "SMTP IP access", destination host to "mail.local.net" and destination port to "25".
5. In this example it is important to actually add this second IP Access component, and not just add more ports and servers to the first component. If the system and the clients later on are configured to use IP tunneling (see the manual) it is possible to have multiple ports and servers per IP Access.
6. Click "Save".

## Adding users

1. It's now time to add a user to the Local Accounts database. Please consult the manual if you wish to use LDAP and Active Directory.
2. Go to **Administration -> User Accounts -> Local Accounts**.
3. Click on New and fill in the user name and full name values (eg. "elvis" and "Elvis Presley").
4. Check the Password box to activate plain password authentication for this user. Enter a password. The AGSS is pre-configured with a number of password checks. These can be reconfigured under **Administration -> Authentication Methods -> Password**.
5. Next click on the Role tab. Click on the users role in the right hand column and then on the arrow button to add this role to the list of available roles for this user. Please note that the user must have at least one role assigned to him to be able to login and do anything useful.
6. Click "Save"

## External access

1. If the AGSS is located behind a firewall or NAT gateway you will now have to make the AGSS accessible from the outside through the device. You only need to open two ports in the external firewall:
2. External access to port 80/tcp must be forwarded to 10.0.0.42 80/tcp.
3. External access to port 22/tcp must be forwarded to 10.0.0.42 22/tcp.

## IP tunneling

IP tunneling is a feature of the AGSS that is often very useful, and on Windows 7 clients it may be necessary because of privileges on the local hosts file. We must refer to the manual for more detailed information on configuring IP tunneling, but briefly speaking there are two requirements for IP tunneling to work:

1. The IP tunneling driver should be installed on the client PC
2. An IP tunneling address pool should be configured in: **System Settings -> Network/Cluster Management -> IP tunneling address pools -> Per system pool**

## All done

1. The AGSS is now ready for use. The first time a user connects to the system he should open a web browser to the AGSS external address.
2. The user may first need to install the IP tunneling driver.
3. And then click on the Launch AppGate Client button. Subsequent connections can be done by using the created desktop shortcut.
4. When the AGSS client is started the user needs to enter his username and password. When the connection is established the user will have a portal window with icons for each available service. Starting a service is done the natural way by double clicking on it. For some services this opens a suitable application and connects to the service, other clients must be configured to use the internal name of the server and the port for the protocol. When configuring for example a mailclient the user uses the internal name and default ports, in our example "mail.local.net" port 143 for IMAP and "mail.local.net" port 25 for SMTP.

## Further information

The Cryptzone Support web site contains a lot of public information, notably a number of guides that describes how to setup some of the more advanced features of the AGSS. There is also the AppGate Forum where anybody can ask questions. Should you need more support you will have to purchase a support plan. Available plans are described on our web.

Useful links:

- At <http://mypage.cryptzone.com> you can subscribe to e-mail lists, such as Red Alert, see your licenses and other entitlements. If you have purchased or want to purchase support you can Connect licenses here as well.
- Guides and documentation can be found at <http://tech.cryptzone.com/agsecurityserver/>
- The AppGate Forum at: [forum.appgate.com](http://forum.appgate.com)