

*“Tips & Tricks” is our regular technical bulletin designed to help you get the most out your AppGate system. This issue looks at **secure access for smart-phones**. In the next edition we’ll focus on Virtualisation. Please send us your comments via the [AppGate Forum](#), or drop us an email to: feedback@appgate.com.*

Focus on ... Secure Access for Smart-Phones

SMS Provisioning – A Built-In Feature

As mobiles have become more intelligent and versatile, users increasingly expect to use them to access applications and data when they are on the move. How do you provision secure access to users’ mobiles quickly and cheaply? With your AppGate solution, deploying solutions to mobile phones is as easy as it is for pc’s, and the required functionality is built-in to your AppGate Security Server.

Step 1: Setup a Mobile Access Rule

The AppGate system harvests information about the platform OS automatically, so you can create an access rule to check whether a mobile device is being used. Below is typical syntax for checking whether the user is using a Windows CE or Symbian phone:

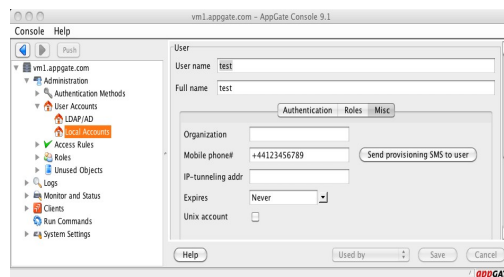
```
attribute{client.platform="^windowsce.*.*"} or
attribute{client.platform="^symbian.[^]*.*"}
```

Step 2: Set up a Mobile role

With AppGate you can treat access from mobile phones in the same way as access from computers, and control which services a mobile user can access. Create a new Mobile role and apply the Mobile Access Rule to the relevant services: email, IM, web browser etc. This role could easily be linked to a group in Active Directory.

Step 3: Setting up the user’s phone

On the AppGate Console, under User Accounts, you will see a ‘Misc’ tab on the User Details page. Simply type in the user’s mobile phone number and press ‘Send provisioning SMS to user’. The user will receive two SMS messages.



The first SMS provides a link that will download and install the mobile client. The second SMS provides the personal settings information. The user simply connects to the AppGate server using their normal network username and password, and the client automatically grabs the second SMS message, extracts the configuration information and sets up the phone for the relevant services eg. setting up the email account, putting a bookmark into the browser for the Intranet, etc.

Your AppGate server is preconfigured to support SMS provisioning but you may need to configure a firewall rule to allow the AG server to connect to this SMS gateway service. Free SMS messages are automatically included for customers who have purchased the AppGate support package. This includes customers using the AppGate Free Edition.

Bits & Bytes

Web Filter For Windows Mobile

One of the challenges of providing remote access from mobile phones is how to implement corporate security policies. We have a number of customers using AppGate’s mobile web filter, enabling them to control mobile users’ direct access to the internet without having to pay for a private APN.

Designed for Windows Mobile devices, the AppGate Mobile Filter includes a Winsock Layered Service Provider that filters all attempts to initiate TCP connections based on a set of rules. Default rules only allow connections to localhost and SSH servers. So the user is only able to surf the web if there is an AppGate client/server connection and the browser is configured to use the AppGate web proxy tunnel.

The AppGate Mobile Filter is easy to install and rules can be defined to set different policies to the default.

Improved check.exe available

We have added more tests to our client check tool: check.exe. So you can now check on things like the status of the anti-virus and the firewall, and whether Windows is up to date.

For more information and a link to download the new check.exe, go to the AppGate Forum: <http://forum.appgate.com/index.php?topic=202.0>

Two Factor Authentication using Soft Certificates

The AppGate mobile client now supports X.509 certificate authentication using soft certificates that are stored in encrypted format on the device. Users only have to enter a password to unlock the certificate, which will be used to authenticate the user on remote servers.

Using certificate authentication to log on to AppGate effectively implements certificate authentication for applications that don't support it natively. Certificate authentication can be set up in the AppGate server by creating a new certificate authentication method. Enable certificate authentication and upload the CA certificate. The client must have access to both a valid certificate and the corresponding private key. For a mobile phone client, copy the certificate and private key onto the phone in PKCS#12 format, which stores the private key in encrypted form and requires a password to unlock. When the user chooses Certificate Authentication, a file chooser will appear to allow the user to specify where the PKCS#12 file is located. This only needs to be done once, when the PKCS#12 file is copied onto the phone.

An important feature of the AppGate solution is central logging of failed password guessing attempts for certificates. When the user enters the wrong password for the certificate, the client will send a log message to the server. This information can be used in access rules to disable the certificate after a specified number of incorrect password guessing attempts. The server can also check the expiration date on certificates and trigger warning messages to the user that it is time to get a new one.

You can find more information about how to configure AppGate for certificate authentication on our website: <http://www.appgate.com/index/support/guides/ag-cert.pdf>

Automatic SMS authentication takes the complexity out of 2-factor authentication

Two factor authentication adds another layer of security to your system, reducing the risk of unauthorised access to network resources. But it also adds another layer of complexity for users, requiring them to jump through yet another hoop before they are granted access. With AppGate, the authentication process can be simplified for users with automatic SMS authentication.

When connecting to the AppGate server using the Mobile Client, the user chooses the OTP authentication method, and logs in using their normal username and password. An SMS is sent to their mobile phone and is automatically read by the Mobile Client. Effectively the one-time-password is automatically entered into the dialog box – the user doesn't have to do anything.

The AppGate security server supports a wide variety of two-factor authentication methods. Automatic SMS authentication using one-time-passwords ensures you have the same level of security for mobile users without adding complexity, getting round the issue of user resistance. All you need is a Radius server that can send out one-time-passwords

For more information:

www.appgate.com

+46 31 774 43 50

info@appgate.com