

# Cryptzone OTP module for the Appgate Security Server

One Time Passwords (OTP) generated by a mobile phone

Authors: Jamie Bodley-Scott and Martin Forssen  
February 14th, 2011

## Content

Two factor authentication.....	3
The One Time Password.....	3
What is OATH? .....	3
Appgate authentication methods .....	3
Use of Chained Authentication.....	4
Cryptzone OTP .....	4
Easy to enable.....	4
Easy to provision .....	5
Easy to use .....	6
Token Support .....	6
Technical Data .....	6

## Two factor authentication

Many businesses are opening up their systems more than they have in past. At the same time there are many scare stories relating to data leakage – and the fines imposed on some businesses as a result of those leaks. Two factor authentication is a key ingredient for businesses which are trying to maintain the right balance between openness and data leak prevention.

Interestingly two factor authentication does not actually help the user to be more productive (as might be the case with a VPN solution) and neither does it help them work more securely (as might be the case with USB encryption). Two factor authentication is purely there to make it much harder for the bad guys to gain access to data or resources which they are not entitled to access.

Ordinary passwords are vulnerable to keyboard sniffers, password guessing bots and shoulder surfing. Users also share their password or write them down. This sometimes extends to usernames as well which leads to issues with accountability and reporting when it becomes harder to verify who the actual user was at some point of interest in the past.

## The One Time Password

A one-time password (OTP) is a password that is valid for only one authentication attempt. OTPs avoid most of shortcomings that are associated with password only authentication. The most significant shortcoming with passwords is that they are vulnerable to replay attacks. By contrast, if a bad guy manages to record an OTP that was already used and replays it, it won't work because it is no longer valid.

The problem with OTPs are that it is difficult for human beings to memorize or generate OTPs unaided so some additional technology must be used in order for it to work well. There are two main ways of helping the user out, either the OTP is **sent** to the user at (or before) an authorisation attempt (often done by SMS) or **self generated** when needed (often using a token).

Two issues which need to be considered when using any OTP solution is Set-up and usability. Set-up encompasses 'on-boarding' a new user; configuring software/accounts and ensuring that any shared secrets required are correctly configured at both ends. Usability is critical because users hate added complexity and help desks hate lots of unnecessary support tickets.

### What is OATH?

The Initiative for Open Authentication (OATH) is an industry wide collaboration to develop a reference architecture for two factor authentication. One of the areas covered by OATH is the use of one time passwords. The architecture includes algorithms for the generation of one time passwords, the means of distributing the shared secrets in a secure way and is built around well-established infrastructure components such as directory and RADIUS servers. The idea is to have a standard approach, open to all delivering solutions that allow for strong authentication of all users on all devices, across all networks.

## Appgate authentication methods

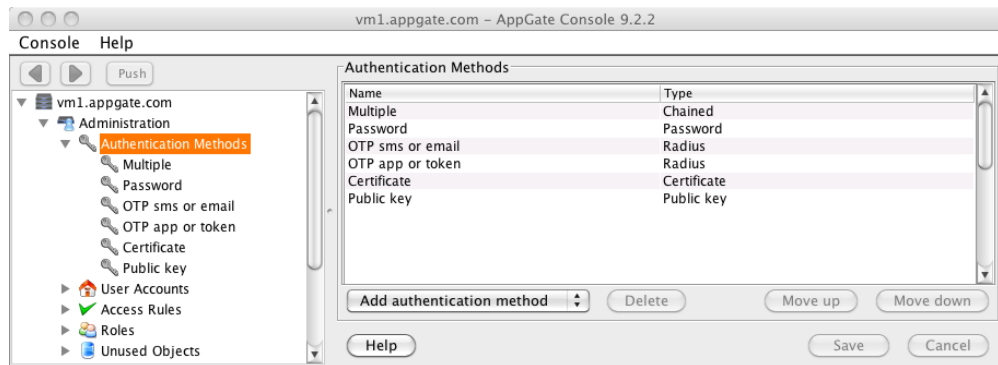
The Appgate Security Server has always supported many different authentication methods as well as being linked to directory servers such as AD. The new OTP method is now being added and will be available from version 10.0 of the Appgate Security Server. The methods available are:

- Directory server authentication (Password)
- Local Password
- Radius
- Certificate
- Public/Private key pair
- SecurID
- **Cryptzone OTP**

The Cryptzone OTP method uses OATH under the covers.

For more information about OATH see:

<http://www.openauthentication.org/>



One key design element is the ability to support multiple methods concurrently. You can have two different groups of users one who only require password whilst a second require the new OTP method of two factor authentication. Or maybe you want the same group to have two different levels of access depending on the level of authentication they have used – that is possible too.

It should also be remembered that it is possible to configure some types of authentication multiple times, so it is quite possible to interface the Appgate server to two Radius servers at the same time as is shown in the example above.

## Use of Chained Authentication

This is a mechanism that Appgate supports for allowing two different authentication methods to be used at once and the results ANDed together. This would make it possible for a network user to have say Kerberos authentication specified as one of the links in the chain and an OTP as the other. This makes it possible for users to 'upgrade' their privileges beyond standard network logon as might be the case if a user needed to access some controlled resources such PCI related data.

## Cryptzone OTP

The new authentication method is a fully integrated OTP solution that will provide an easy to initialise and use authentication method where a user does not want to deploy any additional hardware/servers.

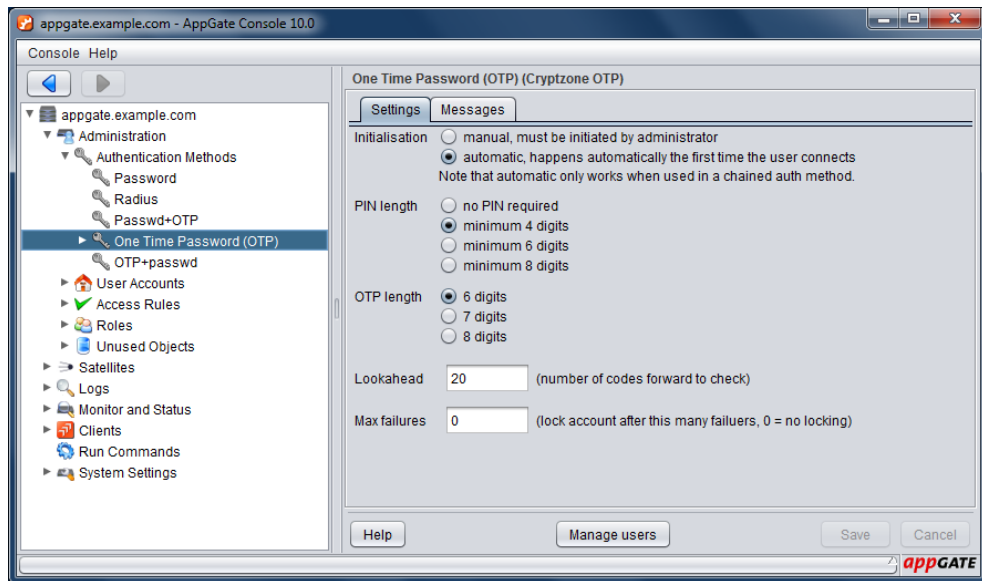
The integrated OTP method relies on self generated OTPs done using a mobile phone as the platform for the app that generates the OTPs. These OTPs are sequence based so both the phone app and the Appgate Security Server need to be seeded with a common start value. After that, each time the user wants to authenticate they simply generate the next OTP in the sequence and enter it into the Appgate login dialogue.

When this new OTP method is combined with ordinary passwords, it gives you true two factor authentication. This builds on the concepts of something you know and something you have. The thing you know is your password and the thing to have is the mobile phone with the software that generates the OTP installed and seeded correctly.

## Easy to enable

The Cryptzone OTP module is an integrated part of the Appgate security server. It only requires a license key to be added using the console. Once added then a new authentication method can be added and configured, all without disturbing the existing configurations or running of the Appgate server.

There are just a few simple settings which can be configured as shown in the dialogue blow.



## Easy to initialise

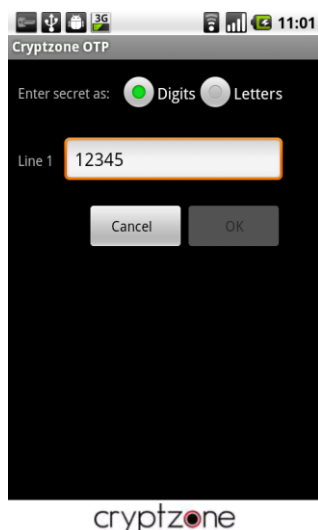
Once the Appgate administrator has added the new authentication method (the integrated OTP in this case) this will appear on the user pick list when a user next logs in. If the user chooses this option then they will either be directed to the usual dialogue where they enter the OTP or if they are a new user of the OTP method then they will be directed to a initialisation dialogue.

The provisioning dialogue tells them where to download the app to their phones. Once this is done the app can be used but it has not been initialised (it does not contain any secret) so it cannot really be used to prove who the user is.

Initialisation happens automatically the first time the phone app is used to authenticate. There are no settings or configuration options to specify during installation. The user will be presented with a string of digits or letters provided over an encrypted link from the Appgate server. These have to be entered manually by the user but every sixth digit or letter is a check-digit and any errors are indicated at once. This makes it robust and not prone to mistakes.

The Cryptzone OTP client is easy to install and use.

Initialisation happens automatically the first time the software is used to authenticate.



With new user provisioning there is always a chicken and egg type problem where the administrator must decide on the trust level required for this first connection. The choices are:

1. The OTP method can be **Chained** with another authentication method like password. In this case the password is deemed sufficient for the first connection.
2. The administrator can manually setup the user in the Appgate administration console. This will generate a code that has to be communicated to the user. The user must then use this code to authenticate before the client can be initialised. This alternative may provide better security than the first two with a cost of increased administration.

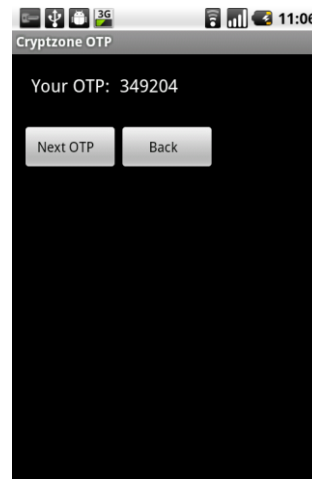
## Easy to use

Once initialised all the user needs to do is enter the pin (optional) and press a button to generate the next OTP. Each generated OTP is 6-8 digits long.

The system does not require any network connectivity on the phone. There are also no SMSs sent. This makes Cryptzone OTP a robust solution.



cryptzone



cryptzone

## Token Support

Tokens as well as the mobile phone app can be used to generate the OTPs.

Because the implementation of this new OTP authentication method has been done using the HOTP standard it is possible to use 3<sup>rd</sup> party tokens as well as the 'soft tokens' that come as part of the solution. Many manufacturers produce variants of their tokens that run the OATH algorithms. These are usually much less expensive than the ones running proprietary algorithms.



Set up in this case has to be done at the server end not the user end. A new command allows you to enter each token's seed value and counter value and associate it with a specific user.

## Technical Data

OTP algorithm:	HOTP (as per RFC4226)
Secret size:	160bits
PIN length:	Minimum of 0, 4, 6 or 8 digits
OTP length:	6, 7 or 8 digits

Supported phones:	MIDP Java (almost any Symbian based phone and Blackberrys), iPhone, Android, Windows mobile 6.5
-------------------	--