Product Review

SMS Passcode 6

November 2011

Introduction

Getting access from any place at any time is already for years one of the key words in many organizations. To arrange that users can get to their data and applications from outside the office, normally two factor authentication is required. In the beginning this was arranged using tokens, but such solutions are pretty expensive and users don't like to carry a physical device like a token with them in their spare time. Also the tokens were lost by the employees causing security risks and the purchase of another expensive token.

In addition to the organizational and budget questions, tokens also have technical disadvantages, because the two factor code is generated based on a time period or "valid-until-used", while you only need a code when the user is logging in to the system.
When using the real-time delivery capability of the SMS service, above challenges are solved. Nowadays a person is always carrying his mobile; a mobile is not lost that easy as a token and using SMS the token is only generated when the service is being used. SMS Passcode created by the company with the same name is the product using SMS token, which will be reviewed in this article.

SMS PASSCODE has via quite a few awards garnered recognition as a leading technology in two-factor authentication solutions via SMS. Essentially, a user first enters username and password and once validated, SMS PASSCODE generates and sends a real-time code that is only valid for that particular login attempt (or session) via SMS, voice call or a secure e-mail such as Blackberry clients. Once the code is entered and validated, the user is granted access. This is a more secure login process than more traditional token solutions and since there is no hardware or software distribution involved, it is at a lower cost. The product is designed for both small and large enterprises, but in a packaging that is very easy to implement including support for the leading login systems such as VPNs, Microsoft, VDIs like Citrix and VMware to name a few, yet enterprise class reliability and scalability.

Installation

SMS Passcode is supported on all regular operating systems (Windows 2003/Windows2008/Windows2008R2) both on 32 bit as 64 bit. The installation files exist of two executables one for the 32bit platform and the other for a 64 bit platform. The product requires .Net Framework 3.5 SP1, which if not installed already will be downloaded an installed by the SMS Passcode installer. For the web based administrator console and the self-service portal also Internet Information Service should be pre-installed.
The administrator console and the self-service portal are part of the so called SMS Passcode core components, which can be seen as the back-end of the product. The other core components are the database service, the transmitter service and the load balancing service.

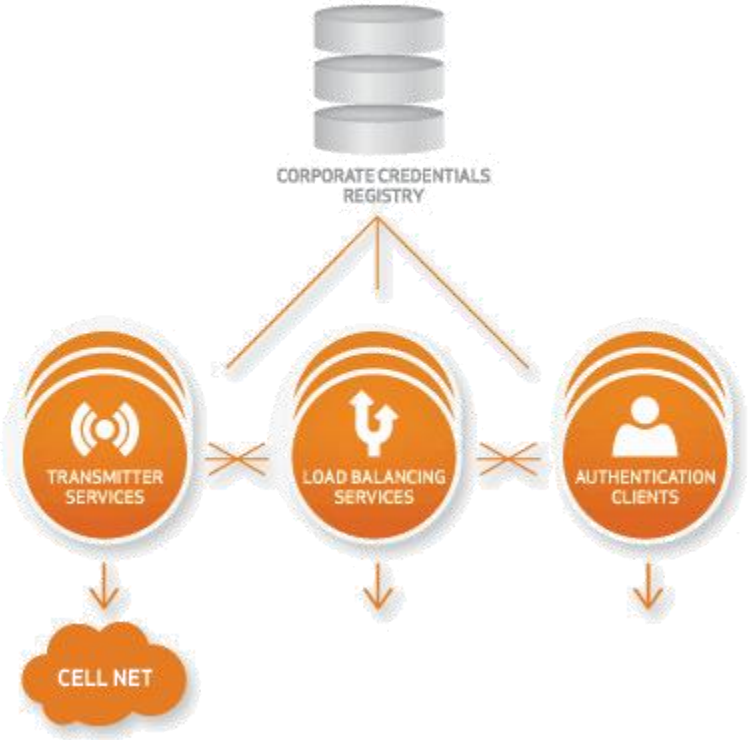

Figure 1: SMS Passcode Components Overview

The transmitter service can be installed on more servers, to arrange fail-over and load balancing over the available GSM modems for the process dispatching messages and validation of the logons. The load balancing service handles failover of load balancing over the transmitter services and even more important arranging the load balance policies described later on. You can install all components on one machine, but can be divided over several servers or as already mentioned deployed more than once for redundancy and load balancing.

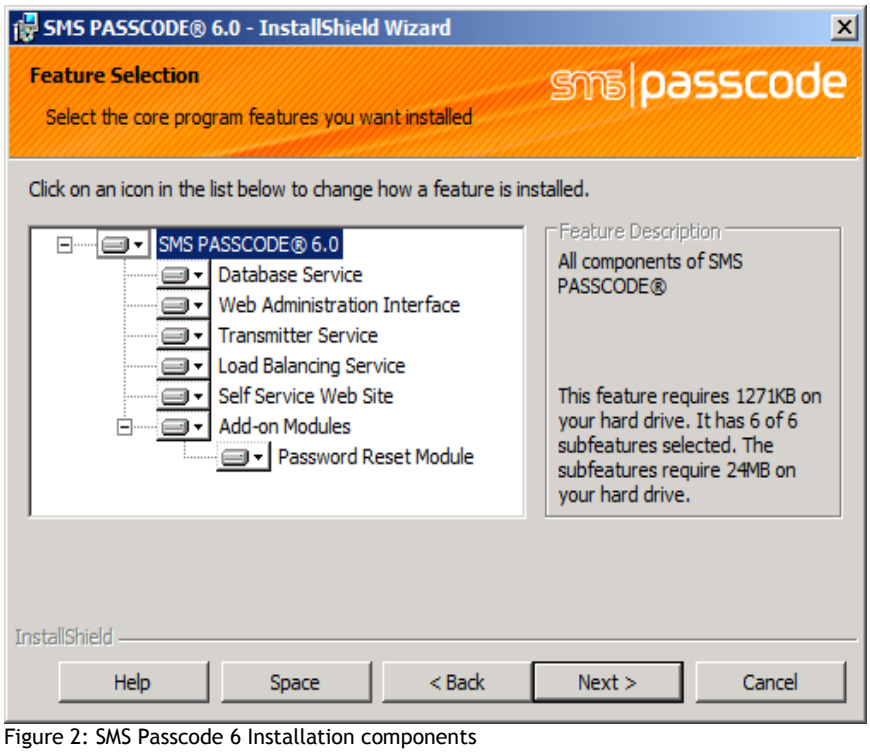

Figure 2: SMS Passcode 6 Installation components

The installation starts really straight forwarded with general questions like the installation location, accepting the license agreement and the choice which components will be installed. Additional questions are the default country prefix (during configuration more can configured, the COM port of the GSM modem, the TCP port for the administration console (default 2000) and if chosen to install the TCP port for the self-service web site (default 3000). As the installation executable included both the core components and the so called authentication clients, you can also select which you would like to install on this server (so you can even combine the core components with the authentication client is wanted). After the installation the configuration tool is started and dependent of your configuration you can configure some settings. Required is the configuration of the shared key, so the components can communicate.

I already just mentioned the authentication clients. This component will be installed on the server hosting the service that you would like to secure with two factor authentication. SMS Passcode provides a lot of authentication clients. For Citrix Web Interface, RADIUS (so it can be used with Juniper, Cisco VPN, Citrix Access Gateway 5, Citrix Cloud Gateway and checkpoint), ISA/TMG (website protection behind a MS ISA/TMG firewall), IIS Web Site Protection (also for OWA, RD Web Access and so on), Windows Logon Protection (2 factor authentication within the Windows XP's GINA logon window or the Windows Vista or 7 Credential Provider), the new Version 6 Cloud Application Protection client for Microsoft Active Directory Federation Services (AD FS) and Citrix Access Gateway Advanced 4.x). On those machines you install using the same executable, deselect the core components (this is a bit confusing the first time and you did not read the installation guide). At the authentication clients you can select the needed client, it's nice that only the clients which were found on the system can be selected.

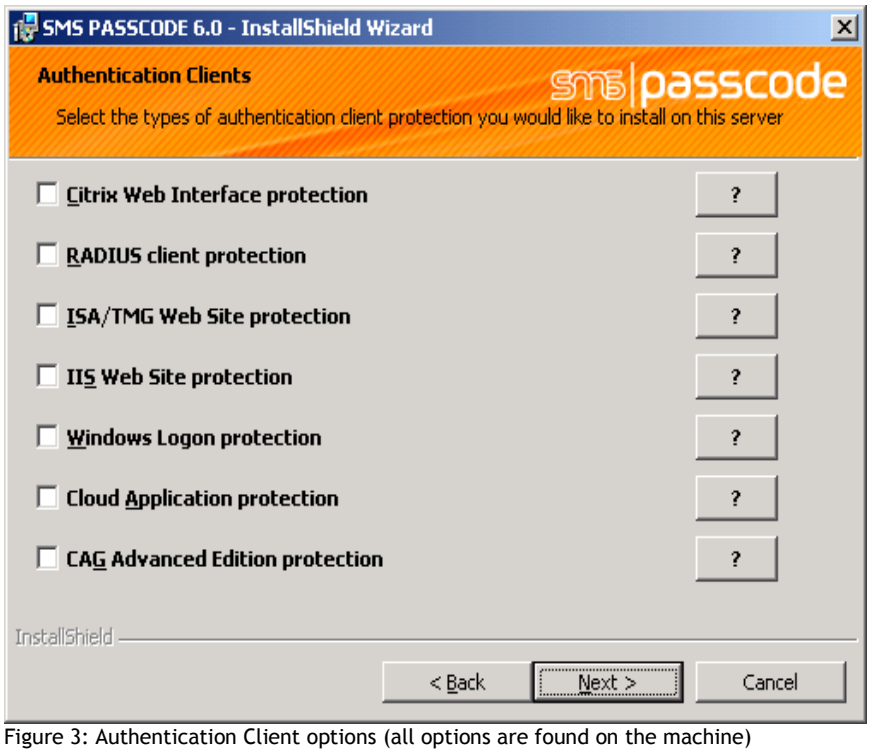

Figure 3: Authentication Client options (all options are found on the machine)

Also on the authentication client, the configuration tool is started. Here you need to configure logically the shared key on the network tab and on the SMS Transmission tab you need to configure the server of servers which provides the transmitter or load balancing service. If you would like the later described enhanced configures rules via Load Balancing Policies you need to choose for load balancing service. Only when using straight SMS on a single server will be possible using only the transmitter service and not the load balancing service. For most installations, it is a good idea to configure the load balancing service, as it is the only wah you can take advantage of the many load balancing policies also benefitial in simple configurations, as you will see described later in the document.

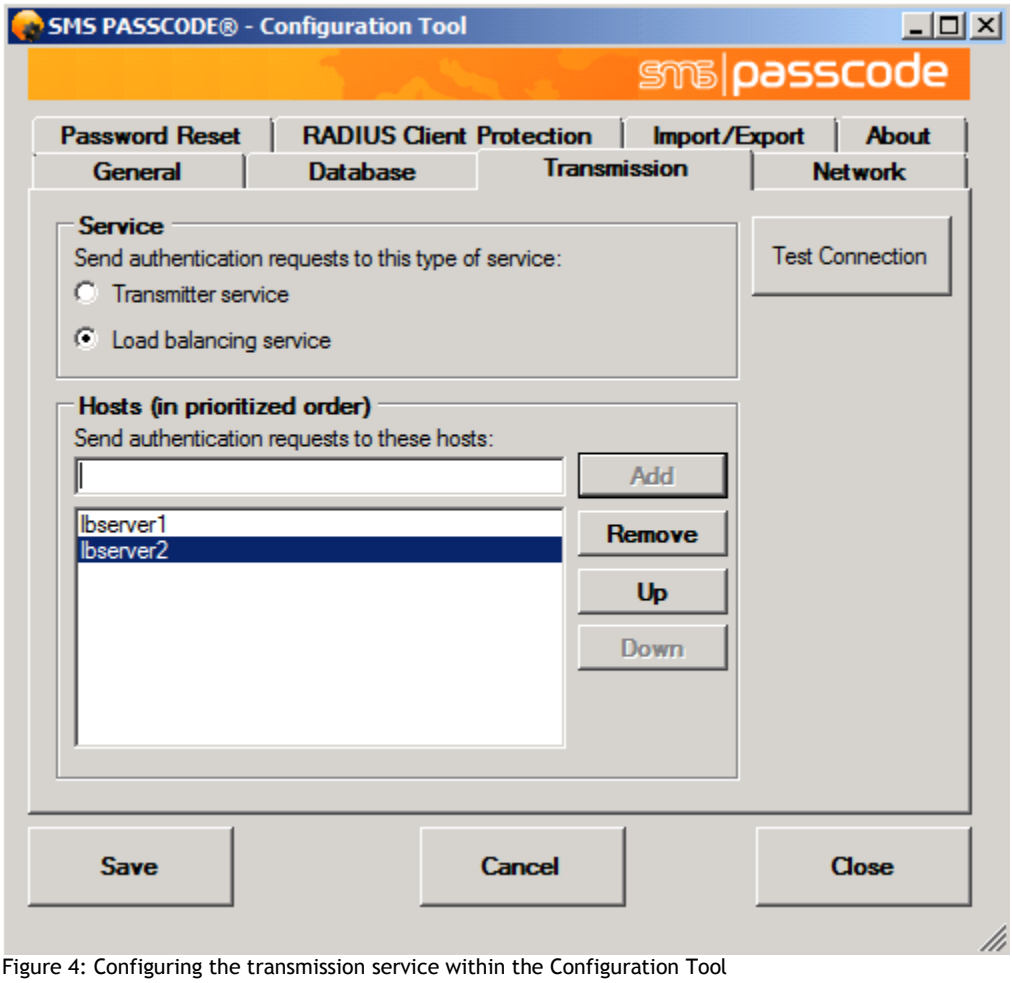

Figure 4: Configuring the transmission service within the Configuration Tool

The last thing I should mention is the GSM modem part. I have already done implementation of previous version of the product and although not actually part of the SMS Passcode this part brings many questions. GSM modems are typically available with a serial connection, so in virtualized infrastructure that won't fit. Happily you can use either a Ethernet enabled modem or a a serial to IP converter (for example a Moxa box) so you can run it on a virtualized server or store the modem separate from the physical server or in many cases have multiple modems connected for configurations such as carrier redundancy. The Moxa serial-to-IP converter as well as the IP modem both comes with support for rack mountable installation (which was one of the complaints of the serial modems in the earlier days). You can add one or more modems to a server or install two or more servers with their own modem(s) attached.

Configuration

From the web-based administrator console you can configure the whole set-up. In most situations you would like to integrate the product with AD, which is fully supported including multiple domains and full nesting of groups. You enable the AD support in the general tab of the Settings component. If the server is member of the domain the integration is automatically set-up. SMS Passcode is using AD groups so you can specify which user can use the service and/or you can configure different configuration based on the groups defined. It is good to know if you only have one domain, but would like to use more than one AD groups (for arranging different configurations) you need to choose Enabled (multi domain mode).
Also on the general tab you can enable several services SMS Passcode is offering. These settings are on global level configured here, but can be configured on group level or user level also. Several are features available from the 5.0 release

- E-mail: send an e-mail with the code instead of sending SMS, usefull for blackberries and especially for the Japanese marked where they often prefer to use email as it supports more characters than SMS and therefore the SMS functionality is not as widely used (as told by SMS Passcode).

- Voice call support: Instead of SMS a voicecall is made telling the code to you (mainly targeted the US market)

- Web Service SMS: Using a provider to send the SMS instead of using your own GSM modem (mainly targeted the US market). It would be nice if this would be available in more countries so if you don't have an ICT infrastructure in that particular country you can send the SMS a bit cheaper (and maybe a bit more reliable). SMSPasscode told me that it's difficult, because most telecom companies are not secure enough for such operations and that SMS services mostly are used for marketing purposes with the limited reliability associated with this kind of service.

- USB Key: In the previous version SMS Passcode already integrated with other third party token products, but only for a few people that don't have a mobile phone (or don't give their phone number) or an area where is no signal. In version 5.0, a cloud-based USB token has been fully integrated within SMS Passcode removing the need for any additional software for those customers that need a few users on other code delivery mechanisms than the SMS or voice call.

You can also configure the of a secondary phone number (you will understand later on, what you do with this).

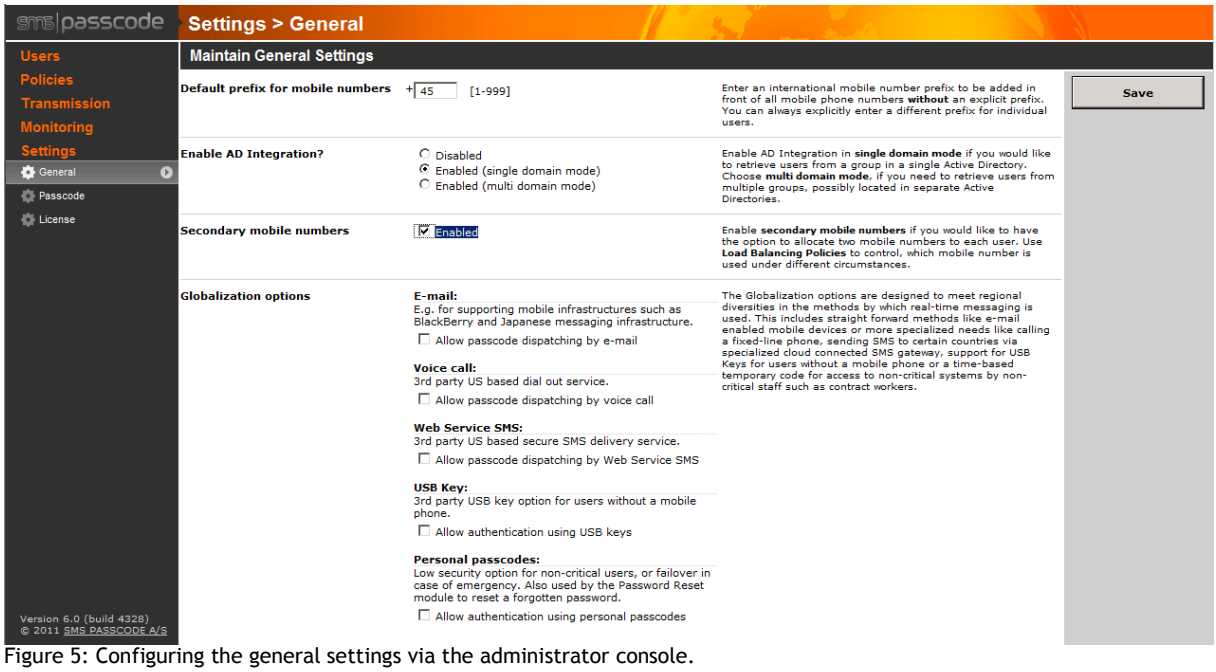

Figure 5: Configuring the general settings via the administrator console.

After enabling the AD integration within the policies component, the User Integration Policies part will become available. Within this part you specify the AD group (by default is SMS PassCode Users). If the group is not available within the AD the sync will not work. If the server is not member of the domain you would like to integrate you can add AD credentials and a server to sync with. For companies that offer the service to other companies, e.g. like hosting or cloud service providers, you can set-up a maximum number of users per company that can be synced using the users sync limit for a truly multi-tenant configuration

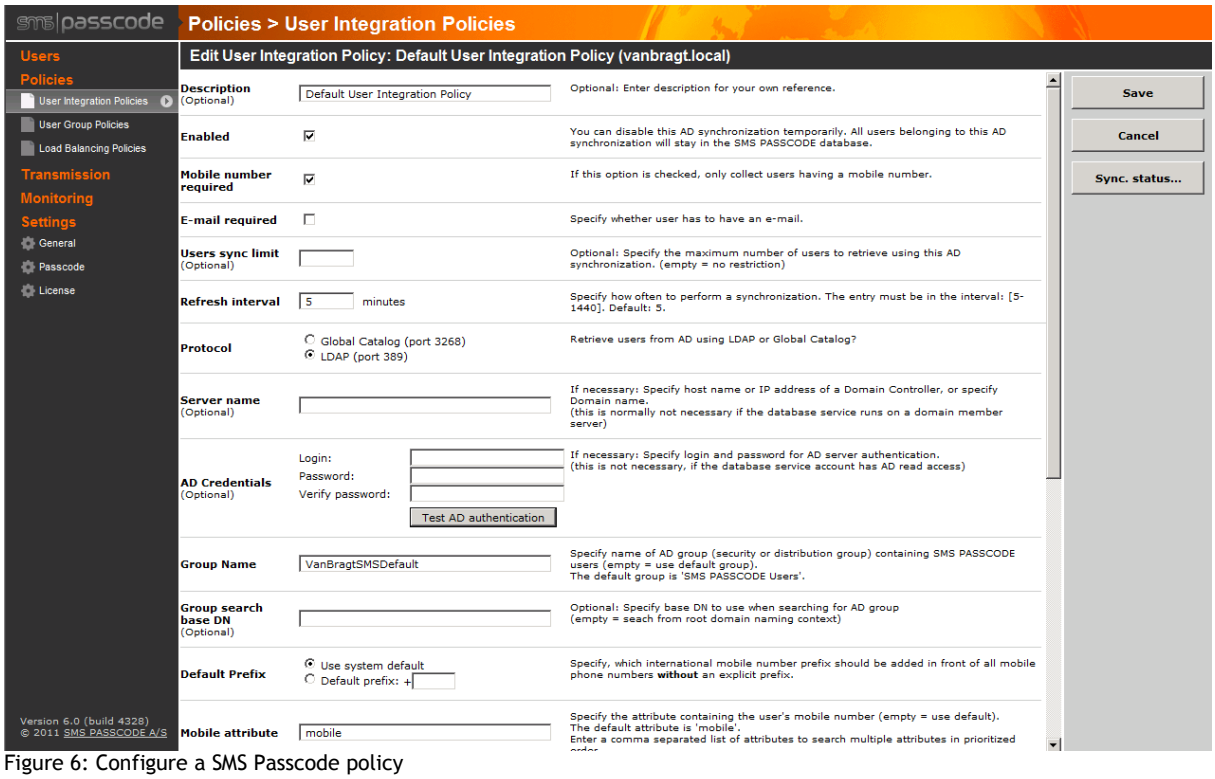

Figure 6: Configure a SMS Passcode policy

In a simple configuration you are pretty much done right now. So if the GSM phone number is specified in AD, the user can now use the access method with the authentication client configured to get access using SMS 2 factor authentication. However SMS Passcode offers much flexibility using the Load Balancing Policies. With these you can use/enable the other authentication methods (like the e-mail, voice mail and secondary phone number) and create rules in case a component is failing for example. A good example is when you are using more modems from different providers in different modem groups, you can create a rule that if the standard modem pool part fails, a new SMS is send to the user via the second provider to create fail-over between providers. Another example is to create two rules again which sends a SMS to the first mobile phone number of the user, if that fails a new SMS is send to the second phone number.

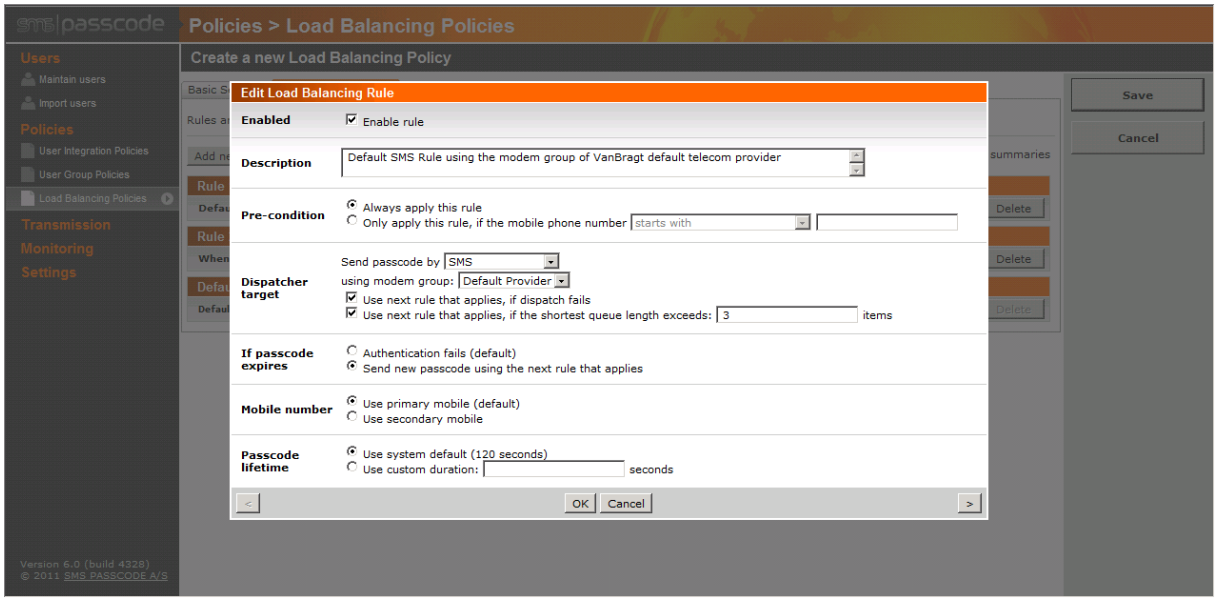

Figure 7: Creating a Load Balancing Rule

You can create several load balancing policies, which can be assigned using the User Group Policies component. At the Dispatch Type you select the Load Balancing Policy you would like to assign. A User Group Policy is assigned again to a User Integration Policy. So all the settings defined in User Group Policy are assigned to AD group at the end. This makes it possible to create different configurations for different groups.

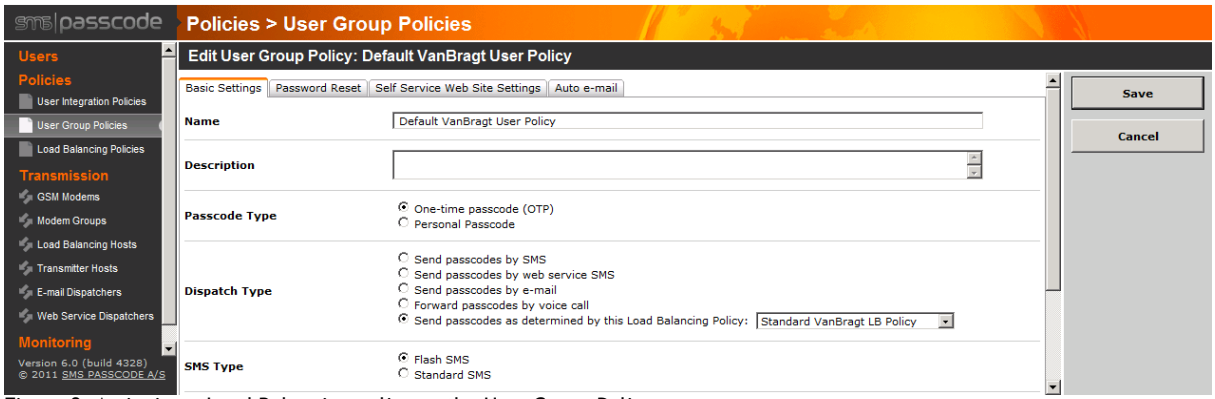

Figure 8: Assigning a Load Balancing policy to the User Group Policy

Also in the User Group Policy, you can enable the self-service web site option including the possibility to configure which settings the user can change (SMS type, mobile number,PIN code and static personal passcode, used for fail-over or password reset described later). The personal passcodes is a kind of last resort option to allow users' access to the system secured with SMS Passcode when the other options are not available. Nice about this last resort option is that you can configure a time period the personal passcode can be used. When you configured an e-mail dispatcher (SMTP) you can also send an e-mail to the user with a link to the self-service site, which will ask the user to fill-in the missing configuration settings.
With these policies configured, the SMS Passcode configuration is ready to send out the passcodes and provide the user with access to the configured authentication clients. On the transmission component in the administrator console you can add additional core components like more GSM modems (this is the only part that requires additional licensing, all other load balancing and redundancy parts are included), configure modem groups (combine modems into a pool also for additional fault tolerancy), add additional transmitter hosts, add load balance services host and set-up e-mail dispatchers.

The last part that can be configured is the passcode itself. You can configure the passcode length, the way it is generated for so called Memopasscode which is a new easy-to-read configuration, and the default time interval the passcode can be used.

SMS Passcode in action

Using SMSPasscode for the end user is pretty easy. The big advantage in comparison with token technologies from a security viewpoint is that the token is generated dynamically on the moment the user is actually logging in. Because of this technology the user will first logon with his username and password and when those are verified a new window will be shown where user can enter the passcode. This is seamlessly integrated into the techniques supported by the product, see the below shown image using Microsoft RDWeb and RDGateway.

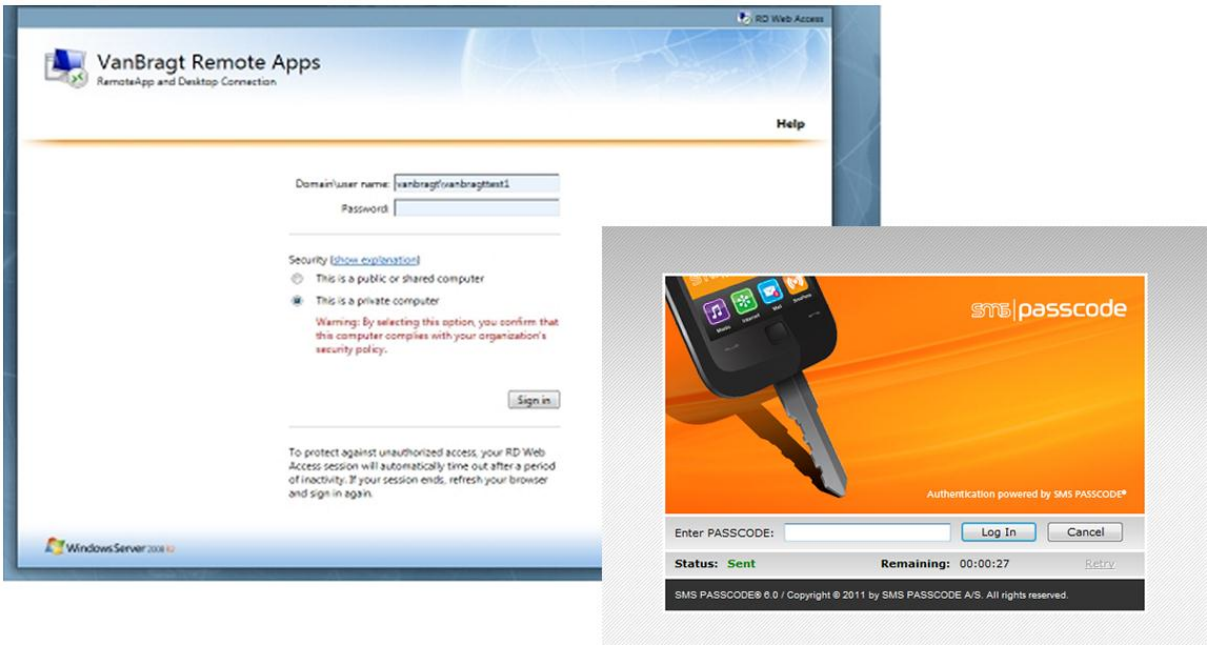

Figure 9: SMS 2 Factor authentication used out of the Microsoft RDWeb and RDGateway

I had the opportunity to test all previous mentioned token delivery methods, like the passcode via SMS, USB Key and the voice dialing system. They all working like a charm (even receiving a voice call out of the US within seconds) also combined with advanced rules of using different techniques after each other.

In version 6 SMS Passcode introduced another nice feature for the end user called Password Reset Module as add-on to the product. This feature makes is possible for the end user to reset or change his password when not already connected to the network infrastructure. It's also usable for those solutions that do not allow connecting to the infrastructure when the password has expired. In these situation to user can go to the specific SMS Passcode Self Password Reset website, where the user need to provide his username and Personal Passcode. After this phase the user will receive a passcode via the normal procedure as configured (normally receiving a SMS on their mobile phone) and after typing the passcode the user will be presented a windows to reset or change their password. In my opinion a nice add-on to the product, especially for non-business hours and the service desk is not available to help the user.
I also implemented previous versions of the product at customers. A big plus of SMS Passcode is the willingness to support you with issues or configurations which are not default. At one customer they helped me out with a difficult NPS configuration, which was actually way out the boundaries of SMS Passcode.

Figure 10: Password Reset Steps within SMS Passcode 6

Also new in the version 6 is Cloud apps protection which introduces support for Microsoft AD FS, a new method for integrating cloud applications like Office365, Salesforce and the likes with the company's internal AD infrastructure. This enables SMS Passcode users to easily integrate these cloud apps in the existing security infrastructure. I don't have any cloud apps available, so I could not test this feature for this review. However SMS Passcode showed me in the demo how they integrate with ADFS and the process is similar for the other solutions SMS Passcode provides.

Monitoring

Although SMS Passcode is an easy program they are providing a nice set of monitoring properties. Within the SMS Passcode console you can view the status of the GSM modems, like the queue, signal strength, retransmissions and other information. SMS Passcode also add three additional event logbooks, where all kind of relevant information is stored like the send messages, status of the service and more.

Conclusion

SMS Passcode is an easy to install and configure, while offering lots of capabilities. With this new release offering other techniques to supplement the SMS code to a mobile phone, they solve the issue in companies where employees don't have a business mobile phone (and don't want to provide their private number) or in the case there is no mobile network available. Also SMS Passcode adds additional security, because the 2 factor authentication code is generated on demand where token based solutions are using a seed file. From a personal experience I know that SMS Passcode is a company that thinks together with the customer for the solution and are more than willing to help you with specific scenarios.

Advantages:

- Easy product to set-up, configure and maintain using on-demand codes (instead of a seed file).
- Offering several ways to provide the code to the users to a lot of available systems.
- Providing several ways to built-in fault tolerance and load balance techniques

Disadvantages:

- The installation of only authentication clients can be bit confusing (while not using the manual)

About the Author
Wilco van Bragt is an independent consultant and author based in the Netherlands. He is the owner of the Server Based Computing and Virtualization website called VanBragt.Net SBC and Virtualization Centre, where he is publishing several articles related to virtualization topics and product reviews. Besides Wilco van Bragt presents on several (independent) conferences and also writes articles for several other websites. Wilco van Bragt is self-employed (VanBragt.Net Consultancy) providing consultancy services in the Netherlands and Belgium. Wilco van Bragt is a MVP on Remote Desktop Services, a RES Valuable Professional and a Citrix Technology Professional.

About SMS PASSCODE®
SMS PASSCODE® is the leading technology in two-factor authentication using your mobile phone. To protect against the rise in internet based identity theft hitting both consumers and corporate employees, SMS PASSCODE offers a stronger authentication via the mobile phone SMS service compared to traditional alternatives. SMS PASSCODE® installs in minutes and is much easier to implement and administer with the added benefit that users find it an intuitively smart way to gain better protection. The solution offers out-of-the-box protection of the standard login systems such as Citrix, Cisco, Microsoft, Juniper and other IPsec and SSL VPN systems as well as websites. Installed at thousands of sites, this is a proven patent pending technology. In the last year, SMS PASSCODE has been awarded twice to the prestigious Red Herring 100 most interesting tech companies list, a Secure Computing Magazine Top 5 Security Innovator, InfoSecurity Guide Best two-factor authentication, a Citrix Solution of the Year Finalist, White Bull top 30 EMEA companies, a Gazelle 2010 and 2011 Fast Growth firm and a ComOn most promising IT company Award. For more information visit: http://www.smspasscode.com or our blog at blog.smspasscode.com.