Release Notes 3.11.5

New Features

- Support for One Touch on RADIUS PAP
- Support for Start TLS on SecureSMTPTransport

Support for OneTouch on RADIUS PAP

This new version allows to the user to authenticate through One Touch in a RADIUS PAP integration.

Configuring NAS to use OneTouch

- On the NAS set the attribute “One Touch enabled” to yes. That will indicate that the authentication method used will be One Touch instead of PAP.
- On Dual Channel Section update the value “In Bound SMS Timeout (ms)” to indicate the amount of time that the RADIUS request will wait for the user response. For example, if that time is set to 30000, the RADIUS call will wait for 30 seconds.
- Reply timeout attribute specified on the VPN RADIUS needs to be set to a value higher than the one specified on Server > Dual Channel > Call/Notification gap (s). That is because if RADIUS tries to authenticate again it will try to send a notification to the user before the time allowed between notification passed and the authentication will be rejected. The best configuration would be to set the reply timeout to be higher than the Dual Channel > In Bound SMS Timeout (ms) to allow to the user to reply before to try to send a new notification.
- Also Reply timeout attribute specified on the VPN RADIUS needs to be higher than the timeout specified in the NAS. Otherwise the timeout on the VPN will occur first, invalidating any RADIUS response given by the Swivel server.

After configuring those attribute the process will be the following:

- User enters username and password
- VPN makes RADIUS request
- Core sends out PUSH and waits for response
- When response is received user is authenticated
- If user does not respond it times out

Support for Start TLS on SecureSMTPTransport

The SecureSMTPTransport class now supports the Start TLS feature of SMTP. This is provided by many SMTP servers, usually on port 587. The connection is initially made using plain text, and then switches to TLS protocol on request.
To use this feature, you need to set the option “Use TLS” on the transport settings.

Additional Notes on Secure SMTP

- Note that secure SMTP is only provided by the SecureSMTPTransport, not the default SMTPTransport class. To use this, you must create a new Transport under Transport -> General, and set the class to com.swiveltechnologies.pinsafe.server.transport.SecureSMTPTransport.
- This transport uses its own settings for SMTP server, not those under Server -> SMTP. The exception to this is the pooling option: if pooling is enabled under Server -> SMTP, it is used for secure SMTP as well.
- A consequence of this is that other features that use SMTP, such as audit logging and scheduled reporting, cannot currently use secure SMTP.
- In addition to support for Start TLS, this release fixes support for “pure” secure SMTP (typically over port 465). In 3.11.4, the option to ignore self-signed certificates did not work, as the wrong SSL class was specified. Therefore, if you select SecureSMTPTransport without the “Use TLS” option, it will now work correctly.