Penetration Test Solutions Guide

Contents

Overview

From time to time we receive requests from customers who have had an automated Pen Test to inspect the vulnerability of their solution. Common questions arise around the subject of SSL. This article points to some common articles which you can use to alleviate your Pen Test concerns.

Solutions

- Perhaps you've not installed an SSL certificate? See: SSL Certificate PINsafe Appliance How to Guide

- If you have installed an SSL certificate, perhaps you need to restrict the ciphers. See: 128-bit encryption enforcement How to Guide

If the ciphers you see are out of date or do not meet your customers requirements it might be that you need to upgrade your Java version (and so PINsafe too) to take advantage of newer ciphers. Note that restricting the ciphers available can reduce the compatibility for older browsers, so be aware of the potential effects and check compatibility with your customer's browser base.

To upgrade the Swivel authentication platform and underlying appliance OS see the following articles:

- Upgrade Appliance
- Upgrade PINsafe
- JAVA upgrade

Further Reading

The following articles show the ciphers available in Java 1.5 and Java 1.6 respectively:

http://fusesource.com/docs/esb/4.4/cxf_security/i343418.html

http://docs.oracle.com/javase/6/docs/technotes/guides/security/SunProviders.html#SunJSSEProvider

Upgrading Tomcat

It's possible to upgrade on custom installations, but not necessarily recommended to do so on Swivel appliances. For appliances, the advise is to wait for the next release.