SSL Internal Certificate Authority

Contents

Overview

This document covers using an Internal Certificate Authority (CA) in Swivel deployments. See also SSL Certificate PINsafe Appliance How to Guide and SSL Solutions.

Prerequisites

Swivel 3.x

Using an Internal CA

Q). Can use certificates issued by our internal CA

A). In order for the certificates to be recognized without certificate problems arising, the CA certificate must be installed in the trusted root certificates store of any client machine.

- The host name by which the server is referenced must match the host name in the certificate, or an alternate name stored in the certificate.
- The certificate must be within its validity period.
- The certificate must be trusted by the client machine, either directly, or more commonly, by trusting the root CA certificate.

Where the request is proxied such as OWA, ADFS Proxy then this server is the client and needs to have the CA certificate which must be installed in the trusted root certificates store on that server, but users connecting in do not need to.

Where the request is made directly to the Swivel server or through a NAT then the user's PC is the client, and would need to have the certificate installed. In such situations a valid public certificate assigned to the public hostname of the Swivel server NAT is usually more appropriate.

Some browsers and access devices permit certificate errors to be ignored, but creating such a scenario may not be the most secure option.

Testing

Known Issues

Troubleshooting