Login for Windows SSL configuration requirements

Introduction

Login for Windows (available in SecureAuth IdP version 9.2+) adds SecureAuth's Multi-Factor Authentication to the Windows desktop and remote server login experience.

When implemented in a PCI (Payment Card Industry) environment, Login for Windows will not install on a machine since it is unable to validate SecureAuth IdP's SSL certificate.

Applies to

- Login for Windows (see also Login for Endpoints Configuration Guide v1.0.2) used in a PCI environment

---

Cause

In a high security environment, port 80 is configured to block outbound connections on both the endpoint and SecureAuth IdP. This setup prevents Login for Windows from verifying if SecureAuth IdP's SSL certificate has been revoked.

Resolution

Use one of these solutions to grant either clients or the SecureAuth IdP server lookup access to verify whether SecureAuth IdP's SSL certificate has been revoked. Each solution uses port 80 (HTTP) because port 443 (HTTPS) requires a certificate validation and subsequent lookup retrieval, potentially resulting in an infinite certificate validation loop.

Grant clients port 80 access to the CRL / OCSP address

Use either solution to grant clients port 80 access to verify the SecureAuth IdP web server certificate:

> **Certificate Revocation List (CRL)**: When the client starts to connect to a web server via HTTPS, the web server certificate includes the URL of the CRL, typically hosted by the Certificate Authority which issued the certificate. The client connects to the CA to download the CRL list and checks to make sure the web server's certificate doesn't appear on the list.
>
> **Online Certificate Status Protocol (OCSP)**: The client connects to the OCSP address specified in the web server's certificate and checks the validity of the certificate.

Grant the SecureAuth IdP web server port 80 access to the OCSP address

Use this solution to grant the SecureAuth IdP web server port 80 access to verify its certificate:

> **OCSP stapling**: The web server regularly visits the OCSP address, obtains a timestamped OCSP validation of its own certificate, then presents this information to the client during the HTTPS transaction. This process eliminates the need for endpoints to connect directly to the CA.
>
> NOTE: OCSP stapling should be enabled by default on any SecureAuth IdP server running Windows 2008 and later. To verify OCSP stapling is functioning, see https://www.ssllabs.com/ssltest/.

Limit access to CRL / OCSP addresses

If opening port 80 to any site is not advised in your environment, you can limit access to the CRL / OCSP address. However, be sure the appropriate address is updated when certificates are renewed in case the URL changes.