SecureAuth IdP SHA256 Cloud Web Service

Issue

SecureAuth IdP now supports SHA256 hashed certificates to improve security, reliability, and performance of the SecureAuth Cloud Services. Microsoft issued a Security Advisory recommending that Certificate Authorities (CAs) stop using SHA-1 SSL certificates by January 1, 2017, and that customers migrate any SHA-1 SSL and Code Signing certificates to the SHA256 (SHA-2) hashing algorithm at the earliest opportunity.

How / Why SSL Certificates are Used with SecureAuth IdP

1. **SecureAuth IdP – SecureAuth Cloud Communication**

   Communicating through *mutual authentication*, where the client (SecureAuth IdP) is uniquely identified by the service (SecureAuth Cloud), and the service is uniquely identified by the client

   Communications include:

   - SMS
   - Telephony
   - Push
   - User Certificate Signing

2. **Browser to IdP Appliance Communication**

   Utilize secure (HTTPS) browser to web server communications for third-party certificates

3. **Profile Data Encryption**

   Encrypt the user profile data before writing it to a user profile field in the on-premises directory

4. **SAML, WS-Federation, and other Assertion Languages Signing and Encryption**

   Use SSL certificates to sign and encrypt SecureAuth IdP – SaaS communication

Impact to SecureAuth Customers

1. **Certificate Renewal**

   Third-party, publicly-trusted SHA-1 hashed certificates installed on the SecureAuth IdP appliances require renewal or replacement with a SHA-2 SSL certificate

2. **Upgrade / Migrate SecureAuth IdP Appliance**

   Pre-8.1 SecureAuth IdP appliances must be upgraded or migrated to the new cloud services environment

   Schedule a maintenance window with **SecureAuth Support** to upgrade the appliance using the automated tools

3. **Root and Intermediate Certificate Authority Certificate Renewal**

   SSL VPNs or other Gateway devices that utilize SecureAuth-issued native certificates must be updated with the SHA-2 Root and Intermediate CA Certificates

It is recommended that all customers review their environments for the existence of SHA-1 hashed certificates, and replace / renew them as soon as possible

The existing certificates will still be valid through their expiration date, but will need to be replaced with SHA-2 hashed certificates once expired

Most certificate vendors offer renewal services in an effort to address the changes

Key Benefits for SecureAuth Customers

- Increased security of all encrypted communication
- Increased support (4x the current capacity) for Certificate Authority (CA) infrastructure
- Longer certificate validity periods
- Web Services' support of Windows Communication Foundation (WCF), and additional transports, security scenarios, and WS-* specifications
- Improved performance
  - Microsoft states that a service migrated from WSE3 to WCF can experience a 200-400% performance improvement
- No re-enrollment required

More Information

SecureAuth Appliance Certificate Renewal Utility (ACRU)