Trend Micro™

Deep Security for Web Apps

In 2013, Microsoft announced that it would deprecate SHA-1 certificates in January 2017, and most certificate authorities like Trend Micro began implementing a program to move customers from SHA-1 certificates to SHA-256 certificates by the end of 2016.

However, this timeline was recently greatly accelerated with an announcement from Google that it would stop supporting SHA-1 certificates a year earlier – January 1, 2016. This move is intended to force certificate users to start moving to SHA-256 certificates as soon as possible. No other independent browser or application is following Google's example at the present time (Mozilla has announced it will follow the Microsoft timeline).

Google has announced the following timeline (Chromium release calendar is available at http://www.chromium.org/developers/calendar):

Chrome release 39, September 26, 2014 – Will NOT affect Trend Micro Customers

- All SHA-1 certificates expiring after December 31, 2016 will display degraded HTTPS feedback in the address bar.

Chrome release 40, November 7, 2014 – Will affect Trend Micro Customers

- All SHA-1 certificates expiring after June 1, 2016 will display degraded HTTPS feedback in the address bar. Affects Trend Micro 2-year certificates issued on or after June 1, 2014.

Chrome release 41, January 12, 2015 – Will affect Trend Micro Customers

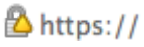
- All SHA-1 certificates expiring after December 31, 2015 will display degraded HTTPS feedback in the address bar.

In response to this recent change, Trend Micro has accelerated its SHA-256 support plans. On October 14, 2014, we will release full support for SHA-256 certificates.

How this affects you

Google defines a SHA-1 certificate as a certificate that is either signed using the SHA-1 hashing algorithm or issued from an intermediate issuing Certification Authority (CA) that has a SHA-1 signed certificate. Currently, all certificates issued by Trend Micro use a SHA-1 signed intermediate CA. The effect of the Google announcement is that all certificates issued by Trend Micro before our October 14 release and expiring after December 31, 2015 (whether SHA-1 or SHA-2), will eventually show a degraded HTTPS session symbol.

Although not finalized by Google, the following images indicate the expected address bar treatment.



The site uses SSL and is secure but Google Chrome has detected minor issues.

The site uses SSL, but Google Chrome has detected either high-risk insecure content on the page or problems with the site's certificate.

Trend Micro Deep Security for Web Apps Support for SHA-256

The October 14 update to Deep Security for Web Apps will enable you to issue SHA-256 certificates with a certificate chain that includes a SHA-256 intermediate certificate, fully supporting all Google Chrome requirements. All certificates issued from our SHA-1 intermediate CA will continue to be indicated as either SHA-1 or SHA-2 certificates, while all certificates issued from our new SHA-256 intermediate CA will be indicated as SHA-256 certificates.

What you can do

We recommend that you replace all of your SHA-1 and SHA-2 certificates with the following timeline as guidance:

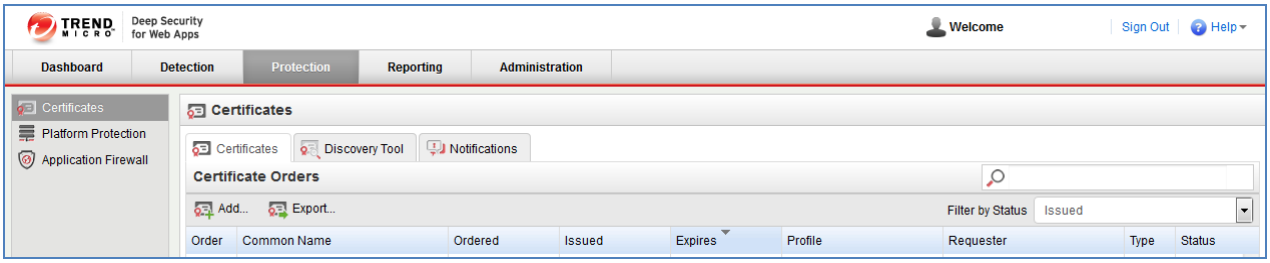
Between our October 14 release and the release of Chrome r40, replace your SHA-1 and SHA-2 certificates expiring between June 1, 2016 and December 31, 2016 with new SHA-256 certificates.

Between our October 14 release and the release of Chrome r41, replace your SHA-1 and SHA-2 certificates expiring after December 31, 2015 with SHA-256 certificates.

Starting immediately, SHA-1 and SHA-2 certificates should only be issued with a "1 Year" validity period to minimize the number of SHA-1 and SHA-2 certificates with expiration dates after December 31, 2015. You may also start replacing affected SHA-1 and SHA-2 certificates with new 1-year certificates expiring in 2015.

How to find and replace affected certificates:

1. Sign into your Trend Micro Deep Security for Web Apps account and go to the certificate order management page: Protection -> Certificates.
2. Select "Filter by status" = Issued
3. Click on the "Expires" column header to sort your issued certificates by expiration date. You may also use the "Export" button to create a CSV file.



4. Find all certificates expiring in 2016. These should all be replaced using the timeline outlined above.
5. We recommend that you use the "Re-Issue" function to quickly generate new certificates. Then use the "Unused" function to properly tag the old certificates (don't use the "Revoke" function because it is reserved for certificates with a genuine security problem, such as key compromise).

To Recap

- Google has recently announced that upcoming releases of the Chrome browser will cause degraded HTTPS session indicators for SHA-1 certificates.
- You should replace all of your affected Trend Micro SHA-1 and SHA-2 certificates utilizing the guidance above.
- You should also plan a transition of all your certificates to SHA-256 by the end of 2015.

There is no additional cost to issue new 1-year SHA-1 certificates or SHA-256 certificates due to Trend Micro's unlimited SSL licensing model.

A list of servers and applications that are compatible with SHA-256 is available at the following link https://casecurity.org/wp-content/uploads/2014/09/SHA-256-Support-List.pdf.

Please contact us at ssl_support@trendmicro.com if you have any questions.