TLS 1.0 and 1.1 Deprecation - July Update

Jul 13, 2020

Title
TLS 1.0 and 1.1 Deprecation - July Update

Content

Continuing from our previous communications, support for **TLS 1.1** is planned to be deprecated for **Web Apps only** from **14th July.** Due to current browsers supporting TLS 1.2, we anticipate this to be a low impact change.

Deprecation of support for TLS 1.0 and 1.1 for **SMTP** and **API** has been moved back to **October and December 2020** respectively. This is to allow our customers adequate time to complete any corrective work.

Service	**Deprecation Date**
Web Applications TLS 1.0	**17th April 2020 - Completed**
Web Applications TLS 1.1	**14th July 2020**
SMTP	**31st October 2020**
API	**31st December 2020**
POP3	**To be announced***

*Exchange 2010 does not support POP over TLS 1.2, therefore POP3 support deprecation date to be announced in the future.

Why are we deprecating TLS 1.0 and 1.1?

TLS 1.0 and 1.1 are legacy protocols that use outdated security configurations. Using TLS 1.2 and above will ensure greater security when accessing Mimecast products.

Mimecast is aligning timelines for the deprecation of support for TLS 1.0 and 1.1 with the announcement regarding the major browsers: Google Chrome, Internet Explorer, Safari, and Firefox as these will no longer support TLS 1.0 and 1.1 as of March 2020.

How this affects you

Using Mimecast Web Applications

Customers that use modern browsers that support TLS 1.2 will be unaffected. If older browsers that don't support TLS 1.2 are used after support for TLS 1.0 and 1.1 has been deprecated, then customers will be unable to access Mimecast Web Applications.

Mimecast Web Applications affected:

- Administration Console
- Mimecast Personal Portal
- Threat Dashboard
- Secure Messaging
- Large File Send
- Service Monitor
- Reviewer and Case Review

- Supervision

Please note, this will affect users who are external to your company if they use the Secure Messaging Portal.

Using Mimecast for Outlook

The current versions of Mimecast for Outlook, Mimecast for Mac and Mimecast Mobile all support TLS 1.2. However, customers who still have any versions of Mimecast for Outlook released prior to v7.1 R1 (released 15th December 2016) will need to upgrade to a newer version after support for TLS 1.0 and 1.1 are depreciated.

The latest version of Mimecast for Outlook can be found here.

Using Mimecast Synchronisation Engine (MSE)

Customers using Mimecast Synchronisation Engine (MSE) should ensure the server running MSE is compatible with the minimum requirements listed here to ensure connections are made using TLS 1.2.

Using the Mimecast Security Agent (MSA)

A version of Mimecast Security Agent (MSA) which supports TLS 1.2 is currently in development, once released customers are advised to upgrade to this version.

Further details will appear here with details.

Using SMTP

Mail servers should be configured to support TLS 1.2 as the default when sending/receiving messages.

Customers should upgrade their mail servers as necessary to ensure continuity of service. Please consult your vendor documentation for further details.

Customers with a high volume of traffic using TLS v1.0 / 1.1 will receive a targeted notification through the Administration Console.

For more information regarding impact for SMTP please see the dedicated Service Update: https://community.mimecast.com/s/article/Mimecast-to-disable-support-for-TLS-v1-0-TLS-v1-1-transport-encryption-for-SMTP

Using Mimecast API

Customers who use modern browsers, applications or services that support TLS 1.2 will be unaffected. If older browsers, applications, and services that don't support TLS 1.2 are used, then customers will be unable to use Mimecast Services after support for TLS 1.0 and 1.1 has been deprecated.

Original Service Update: https://community.mimecast.com/s/article/TLS-1-0-and-1-1-deprecation