**TLS 1.0 Disablement**

**FAQ - AD Users
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_**

**2020-3-16**

**FAQ:**

Q1: What is TLS?

A: TLS stands for “Transport Layer Security.” It is a protocol that provides privacy and data integrity between two communicating applications. It is deployed widely for web browsers and other applications that require data to be securely exchanged over a network. TLS includes two layers: the TLS Record protocol and the TLS Handshake protocol. The Record Protocol provides connection security. The Handshake protocol enables the server and client to authenticate each other and negotiate encryption algorithms and cryptographic keys before data exchange.

Q2: What is the reason for this change?

A: TLS aims to provide privacy and data integrity between two communicating applications. TLS 1.1 and above provide significantly higher security controls than TLS 1.0. Protecting your data is of the utmost importance for us, and this disablement will allow us to better ensure the security of your data. Our goal is to make this process as seamless as possible while maintaining the highest security standards.

Q3: When will this change happen?

A: TLS 1.0 disablement will take place on June 12, 2020. Ather this date, you will not be able to connect to Avery Dennison RBIS web-based applications (SSO, D2Comm, ACS, VIPS, GOS,JCPENNY) using browsers not compatible with TLS 1.1 or above. Avery Dennison encourages users to quickly abandon older versions of TLS to avoid exposure to security vulnerabilities.

Q4: How does TLS 1.0 Disablement affect me?

A: If your browser is not up to date, you may receive an error when you try to log in to Avery Dennison RBIS web-based applications (SSO, D2Comm, ACS, VIPS, GOS,JCPENNY). You will be required to update your internet browser.

Q5: What error message will return to a non-compliant connection?

A: The exact error messaging returned depends on the browser or application framework being used. Some examples include but are not limited to:

 -Unable to connect to the service

-Service not available

-Error in connection

**To resolve these errors, the browser or application framework must be updated to a version compatible with TLS 1.1 or above.**

Sample IE error message:

****

Q6: How to check what TLS version is running on your browser?

A: Microsoft Internet Explorer

1. Open Internet Explorer
2. From the menu bar, click **Tools->Internet Options->Advanced tab**
3. Scroll down to the **Securit**y category, check the option box for Use **TLS1.1 and TLS1.2**
4. Click **OK,** restart Internet Explorer

 Google Chrome

1. Open Google Chrome
2. Click **Alt-F** and select **Settings**.
3. Scroll to the bottom and select Show **advanced** settings
4. In the **System** section, click **Open your computer’s proxy settings**
5. Select the "**Advanced**" tab
6. Scroll down to the **Securit**y category, check the option box for Use **TLS1.1 and TLS1.2**
7. Click OK, restart Chrome



Mozilla Firefox

1. In the address bar, type **about:config** and press **Enter**
2. In the **Search** field, enter **tls**. Find and double-click the entry for **security.tls.version.min**
3. Set the integer value to 2 to force protocol of TLS 1.1
4. Click **OK**
5. Restart Mozilla Firefox

Q7: How to upgrade my browser?

A: Upgrade to the latest version of Internet Explorer at the [link](http://windows.microsoft.com/en-us/internet-explorer/download-ie) here. Preferred to use Internet Explorer 11. You can also reach out to your local IT support for assistance.

Q8: Who should I go to if I have connection problems after June 12, 2020?

A: You can contact the Avery Dennison Software Support Team or EIT Support Team mentioning that your browser setting is not working for TLS 1.1 or above and they will assist you.

1. Software Support Team: software.support@ap.averydennison.com

2. EIT Support Team: data.maintenance.vdm@eu.averydennison.com