**Upgrade TLS 1.0 to TLS 1.1 or TLS 1.2**

**Critical Update from Salesforce:**



Salesforce is requiring an upgrade to TLS 1.1 or higher by July 22, 2017 in order to align with industry best practices for security and data integrity. On that date we will begin disabling TLS 1.0. Action is required prior to this date to prevent any disruption to your production instance.

After Salesforce disables TLS 1.0, any inbound connections to or outbound connections from your Salesforce org that rely on TLS 1.0 will fail. This will impact a number of Salesforce services (listed below), including access to websites including Salesforce Communities, Customer and Partner portals, Force.com sites and Site.com.

|  |  |
| --- | --- |
| TLS Disablement in Sandbox orgs | June 25, 2016, After this date and time, all sandbox orgs whether existing, refreshed, or new will have TLS 1.0 automatically disabled and will require TLS 1.1 or later in HTTPS connections to or from the sandbox org. The "Require TLS 1.1 or higher for HTTPS connections" CRUC setting will not be available. |
| TLS Disablement in Production orgs | Begins on **July 22, 2017**. |

**Impacts with the Disablement of TLS 1.0**

|  |  |  |
| --- | --- | --- |
| Impacted Channels | Impact? Yes/ No | Comments |
| [Internet browsers](https://help.salesforce.com/articleView?id=000221207&language=en_US&type=1#InternetBrowsers) | Yes | Follow the following article to handle Browser related issues. To check the browser compatibility use the link Open the link to test the browser compatibility to pass TLS 1.1 or 1.2 check <https://tls1test.salesforce.com/> |
| [API (inbound) integrations](https://help.salesforce.com/articleView?id=000221207&language=en_US&type=1#Inboundintegrations) | Yes | Inbound callouts (SOAP / REST) will be impacted.  to check the Compatibility of API client follow the article. |
| [Call-out (outbound) integrations](https://help.salesforce.com/articleView?id=000221207&language=en_US&type=1#OutboundIntegrations) | Yes | We need to make sure the other end, where the services hosted to support TLS 1.1 and TLS 1.2.  To check the compatibility follow the article. |
| Partner Or Customer Portals | Yes | We are not Using |
| Communities & Sites | Yes | We are not using Communities and Sites |
| Outlook Salesforce Sync | Yes | We are not Using |
| Salesforce Mobile App | Yes | We are not Using |
| Data Loader | Yes | To Support Data loader, customer would need to download newer version of Data loader  <https://releasenotes.docs.salesforce.com/en-us/spring16/release-notes/rn_forcecom_data_data_loader.htm> |
| CTI | Yes | We are not Using CTI Toolkit |
| Chatter Desktop | Yes | We are not using, if any end users are using it they need to upgrade IE browser to support TLS 1.1 or higher. |
| SSO | Yes | Users required to use compatible browsers TLS1.1 or Higher. |
| Force.com IDE and Force.com Migration Tools | Yes | Users need to upgrade to compatible TLS1.1 or higher. Users using Java 8 will automatically get TLS1.1 enabled. |

Article to verify the compatibility of browser, Inbound, Outbound callouts.

<https://help.salesforce.com/articleView?id=000221207&language=en_US&type=1>

**Internet Browsers check**

Open the link to test the browser compatibility to pass TLS 1.1 or 1.2 check <https://tls1test.salesforce.com/>

If you experience errors, you need to ensure your browsers are compatible with TLS 1.1 or higher. If your browser is not compatible with TLS 1.1 or higher after we make this change, your users will NOT be able to access Salesforce. We recommend that you begin planning to support TLS 1.1 and TLS 1.2 as soon as possible.

**How can I help my end users manage this change?**

You can provide your users (including both internal and external community users) with a notification when they access Salesforce using TLS 1.0 that advises them to either update their web browser setting or upgrade their web browser.

Use the App to test the TLS1.0 compatibility in the end user device. <https://appexchange.salesforce.com/listingDetail?listingId=a0N3000000DpyiJEAR>

Install and configure this app and then end users can view the error message.

