TLS 1.0 Disablement Readiness Checklist

Have no fear.

Use this guide to help you prepare your Salesforce environment for the upcoming TLS 1.0 disablement.

Get started early and transition your environment to support TLS 1.1 and higher as soon as possible. Many of the Salesforce products and developer tools are already compatible with TLS 1.1 and higher.

Learn and Assess

Task	Reference
☐ Learn about TLS 1.0 and the industry-wide change to remove support for it	See the "Overview" section within the Salesforce disabling TLS 1.0 article.
☐ Know the Salesforce TLS 1.0 disablement timelines	See the "When will Salesforce disable TLS 1.0 encryption?" section within the Salesforce disabling TLS 1.0 article.
☐ Understand the Salesforce TLS 1.0 disablement impact on the following areas to determine the impact on your Salesforce environment: • Internet Browsers • Integrations • Salesforce features, which includes: o Microsoft email integration features o Data Loader o Salesforce mobile apps o Communities and Sites	See the following sections within the Salesforce disabling TLS 1.0 article: • Internet Browsers • API (inbound) integrations • Call-out (outbound) integrations • Impact on Salesforce Features • Impact on Developer Tools
☐ Identify users relying on incompatible browsers	Leverage the Login History to identify users. See the Browser compatibility section within the Salesforce disabling TLS 1.0 article for more details.
☐ Identify API (inbound) integrations relying on TLS 1.0. Examples include: • Interfaces or applications • Mobile apps Desktop clients	Coming in Summer '16: Leverage the new TLS protocol field in the Login History (Setup | Manage Users) to identify users and or integrations (via user accounts).
☐ Identify call-out (outbound) integrations relying on TLS 1.0. Examples include: • Delegated Authentication Single-Sign-On (SSO), • Outbound Messaging • Apex call-outs	Leverage the 2 methods detailed in the "How do I test the compatibility of a call-out (outbound) integration from Salesforce?" section within the Salesforce disabling TLS 1.0 article.

Develop Action Plan

Now that you have assessed the impact and understand the timeline, let's work on creating an action plan to get you ready for this change.

Task
☐ **Create an action plan:** • What is the impact on your users, integrations, etc.? (Will it impact your Finance department differently than your Sales department?) • Who or which teams do you need to bring together to get things done? • What action needs to be taken and who or which teams will do it? • Who's going to project manage the efforts and ensure that things get done?
☐ **Keep AppExchange apps working:** Determine if your AppExchange apps are compliant by engaging with the vendor and/or partner directly.
☐ **Over-communicate:** Create an internal communication plan. Target and tailor the message based on how this will impact different end-users and teams. For example, create a separate outreach for end-users using incompatible browsers. Don't be afraid of over-communicating; you don't want to miss anyone.
☐ **Message end-users directly from within your Salesforce org or your Communities:** Need other ways to reach both your internal and external Community users? Leverage the new TLS 1.0 Compatibility User Message AppExchange package or VisualForce page controller to deliver in-app user messages when TLS 1.0 is being used, and provide user instructions as needed. See the "How can I help my end users manage this change?" section within the Salesforce disabling TLS 1.0 article.
☐ **Leverage additional resources:** Are you a Premier Success customer? Contact your Support resource for guidance. You can also team with other Salesforce admins in the Salesforce Infrastructure Success Community Group.

Test and Transition

Now that you have assessed the impact and understand the timeline, let's work on creating an action plan to get you ready for this change.

Task
☐ If you have a sandbox environment, leverage it for end-to-end TLS 1.0 disablement testing via the new "Require TLS 1.1 or higher for HTTPS connections" Critical Console Update (CRUC) setting. See the TLS 1.0 Disablement Critical Update Console (CRUC) Setting article for more details. **Don't have a sandbox org?** You can also test the CRUC update for TLS 1.0 disablement in a free Developer Edition org. Sign up here.
☐ Validate your final testing by enabling the new CRUC setting in your production org prior to the Salesforce disablement to minimize disruptions.

Execute

You know that action plan you created above? Now execute on it! Remember to over-communicate so that nobody is surprised by this change!

Celebrate!

You've successfully prepared for and executed an industry-wide change through your organization. That's probably résumé-worthy ;)