

## Important Notice:

### How to Test Your Browser Compatibility

If you are able to view the Salesforce test site (<https://tls1test.salesforce.com/s>) which has TLS 1.0 disabled—without errors, access to Salesforce via your browser should not be impacted by this change, and no action is required.

### What Is Happening?

Salesforce will require Transport Layer Security (TLS) 1.1 and later encryption protocol to maintain the highest security standards and promote the safety of customer data. Moving to TLS 1.1 or higher provides a more secure environment and prepares you for continued PCI compliance.

### When Is It Happening?

Salesforce is disabling TLS 1.0 on July 22, 2017 at 9:30 AM PDT, if you are accessing MSAR portal thru a Web browser, it's required that the TLS setting is TLS 1.1 or higher.

### What is the impact of TLS 1.0 disablement?

User browser access – Browser incompatibility will prevent users from accessing your Salesforce org, Communities and Sites.

### Internet Browser Access

Users will experience issues accessing Salesforce via your browser if non-supported browsers are in use or if you have disabled the supported encryption protocols in the browser.

[List of browsers supported by Salesforce Classic](#) (Jan 2017)

### Action Required for Browser Compatibility

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.

**NOTE:** The minimum required action is to enable TLS 1.1 or TLS 1.2 encryption protocol within your browser security settings. Although we recommend disabling TLS 1.0 for a more secure browsing experience, it is not required. For example, if a user has protocols TLS 1.0, TLS 1.1, and TLS 1.2 enabled within their browser's security settings, they will be able to successfully connect to Salesforce with that browser after Salesforce disables TLS 1.0 on March 4, 2017.

### Browser Compatibility Details

Browser	Compatibility Notes
<b>Microsoft Internet Explorer (IE)</b> Review the <a href="#">Enabling TLS 1.1 and TLS 1.2 in Internet Explorer knowledge</a> article for more details.	
Desktop and mobile IE version	Compatible with TLS 1.1 or higher by default

11	If you see the "Stronger security is required" error message, you may need to turn off the TLS 1.0 setting in the Internet Options   Advanced Settings list.
Desktop IE versions 8, 9, and 10	Compatible only when running Windows 7 or newer, but not by default. Review the <a href="#">Enabling TLS 1.1 and TLS 1.2 in Internet Explorer</a> article to enable TLS 1.1 or higher encryption.  Windows Vista, XP and earlier are incompatible and cannot be configured to support TLS 1.1 or TLS 1.2.
Desktop IE versions 7 and below	Not compatible with TLS 1.1 or higher encryption.
Mobile IE versions 10 and below	Not compatible with TLS 1.1 or higher encryption.
<b>Mozilla Firefox</b>	
Compatible with the most version, regardless of operating system.	
Firefox 27 and higher	Compatible with TLS 1.1 or higher by default.
Firefox 23 to 26	Compatible, but not by default. Use about:config to enable TLS 1.1 or TLS 1.2 by updating the security.tls.version.max config value to 2 for TLS 1.1 or 3 for TLS 1.2.
Firefox 22 and below	Not compatible with TLS 1.1 or higher encryption.
<b>Google Chrome</b>	
Compatible with the most recent version, regardless of operating system.	
Google Chrome 38 and higher	Compatible with TLS 1.1 or higher by default.
Google Chrome 22 to 37	Compatible when running on Windows XP SP3, Vista, or newer (desktop), OS X 10.6 (Snow Leopard) or newer (desktop), or Android 2.3 (Gingerbread) or newer (mobile).
Google Chrome 21 and below	Not compatible with TLS 1.1 or higher encryption.
<b>Google Android OS Browser</b>	
Android 5.0 (Lollipop) and higher	Compatible with TLS 1.1 or higher by default.

Android 4.4 (KitKat) to 4.4.4	May be compatible with TLS 1.1 or higher. Some devices with Android 4.4.x may not support TLS 1.1 or higher.
Android 4.3 (Jelly Bean) and below	Not compatible with TLS 1.1 or higher encryption.
<b>Apple Safari</b>	
Desktop Safari versions 7 and higher for OS X 10.9 (Mavericks) and higher	Compatible with TLS 1.1 or higher by default.
Desktop Safari versions 6 and below for OS X 10.8 (Mountain Lion) and below	Not compatible with TLS 1.1 or higher encryption.
Mobile Safari versions 5 and higher for iOS 5 and higher	Compatible with TLS 1.1 or higher by default.
Mobile Safari for iOS 4 and below	Not compatible with TLS 1.1 or higher encryption.