As part of our continued effort to maintain the highest security standards and align with industry best practices, Orchid Connect will be disabling the TLS 1.0 encryption protocol on **Saturday February 25, 2017.**

**How this change will impact Orchid Connect users:**

1) **Users who still use Internet Explorer 7 or lower will no longer be able to access Orchid Connect.**
2) **Users who access Orchid Connect with Internet Explorer 8, 9, or 10 will now be required to have TLS 1.1 or TLS 1.2 enabled in their browser.**
3) **Users who access Orchid Connect on computers which are still running Windows XP or Vista will no longer be able to access Orchid Connect if they are running any version of Internet Explorer.**

Please see the Internet Browser Compatibility guidelines for instructions on how to ensure your users are prepared for the upcoming change:

# Internet Browser Compatibility Guidelines

| Browser | Version | Compatibility Notes |
|---|---|---|
| Microsoft Internet Explorer (IE) | Desktop and mobile IE version 11 | Compatible with TLS 1.1 or higher by default |
| | Desktop IE versions 8, 9, and 10 | Compatible only when running Windows 7 or newer, but not by default. You need to enable it in IE by navigating to Tools → Internet Option → Advanced, and then scroll to the Security section of the Settings window and make sure the 2 checkboxes 'Use TLS 1.1' and 'Use TLS 1.2' are ticked:<br><br>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. |
| Microsoft Edge | Microsoft Edge | Compatible with TLS 1.1 or higher by default. |
| Mozilla Firefox | Firefox 27 and higher | Compatible with TLS 1.1 or higher by default. |
| | Firefox 23 to 26 | Compatible, but not by default.<br>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.<br><br>Windows XP (SP2+) and Vista are compatible and can be configured to support TLS 1.1 or TLS 1.2. |
| | Firefox 22 and below | Not compatible with TLS 1.1 or higher encryption. |
| Google Chrome | 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. |
| Apple Safari | 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. |

Why is disabling TLS 1.0 important: The US government's National Institute of Standards and Technology (NIST) issued a recommendation that all organizations migrate their online properties to the updated TLS protocol, version 1.1 or 1.2, to ensure a safe and secure operating environment for users. As a result of this update, older internet browsers which are inherently insecure and do not support the newer TLS 1.1 and 1.2 protocols will no longer be able to access websites which have been updated. Click here for more detail on the NIST recommendation.