Protocolo TLS 1.2

Actualizaciones importantes para la compatibilidad con la Plataforma ArcGIS y el protocolo Transport Layer Security (TLS)

Esri está comprometida con la creación y provisión de gran seguridad en la Plataforma ArcGIS y la ayuda a nuestros clientes a través del uso de los protocolos de seguridad más recientes. Nos esforzamos por implementar los estándares de seguridad más elevados, incluido TLS, para mejorar la integridad de los datos y la seguridad de red.

Para cumplir con estos estándares, Esri pone a tu disposición información sobre la configuración y, en caso necesario, te ofrece actualizaciones de software en toda la Plataforma ArcGIS para admitir TLS 1.2. Como parte de la mejora de la seguridad de ArcGIS Online, Esri planea que **las conexiones TLS 1.2 para los servicios de ArcGIS Online sean obligatorias a partir de abril de 2019**. Por este motivo, será necesario tomar acciones antes de este cambio para garantizar el acceso continuado a estos servicios de ArcGIS Online.

¿QUÉ ES TLS?

TLS, siglas de "Transport Layer Security" (seguridad de la capa de transporte) es un protocolo de seguridad de red muy utilizado. Proporciona privacidad e integridad de los datos entre aplicaciones que se comunican por una red. Los usuarios usan TLS siempre que acceden a los servicios de ArcGIS Online, como mapas base, servicios de geoprocesamiento y Living Atlas, desde ArcGIS Desktop, ArcGIS Enterprise y otras aplicaciones.

¿CÓMO SE VE AFECTADA LA PLATAFORMA ArcGIS?

La Plataforma ArcGIS usa el protocolo TLS como componente clave de su seguridad para conexiones de API de servicios y web. Se incluyen las conexiones entre nuestro software, como ArcGIS Desktop, ArcGIS Enterprise y ArcGIS Online. Este último admite actualmente las conexiones que usen las siguientes versiones de TLS: 1.0, 1.1 y 1.2. A partir de abril de 2019, los servicios de ArcGIS Online solo aceptarán las conexiones que usen TLS 1.2.

Hay software, como ArcGIS Pro, que ya está habilitado para TLS 1.2. Otro software de Esri, como ArcGIS Desktop, usa TLS 1.0, un software que requiere un cambio de configuración o un parche para admitir las conexiones TLS 1.2. **Esri va a presentar parches e instrucciones para actualizar el software existente y admitir así estas conexiones.**

¿ME AFECTA LA ACTUALIZACIÓN A TLS 1.2?

TLS forma parte de la infraestructura de seguridad de Internet de nivel bajo y generalmente no se ve, salvo que una organización aplique niveles más elevados de seguridad de red, normalmente deshabilitando las versiones vulnerables anteriores de TLS y SSL. **La práctica recomendada de TI actual es iniciar el traslado a TLS 1.2 para mejorar la seguridad del transporte en la red.** ¿Cómo te afecta?

¿En tus flujos de trabajo necesitas tener acceso a los mapas base de ArcGIS Online, story maps, Living Atlas, elementos alojados u otros servicios de ArcGIS Online? Si es así, será necesario que el software que uses para acceder a ArcGIS Online sea compatible con las conexiones TLS 1.2 con aquellos servicios que se inicien a mediados de abril de 2019.

¿Alojas un portal de SIG con ArcGIS Enterprise que se conecta a ArcGIS Online? Si es así, deberás asegurarte de que tu implementación de ArcGIS Enterprise, incluidos ArcGIS Server y Portal for ArcGIS, esté actualizada para que sea compatible con las conexiones TLS 1.2 con ArcGIS Online a partir de mediados de abril de 2019.

¿Utilizas aplicaciones de ArcGIS o de terceros creadas en ArcGIS Runtime que acceden a ArcGIS Online desde tu dispositivo móvil o de sobremesa? Si es así, deberás asegurarte de que dichas aplicaciones y configuraciones del sistema operativo de los dispositivos sean compatibles con las conexiones TLS 1.2 con ArcGIS Online a partir de mediados de abril de 2019.

¿Has creado alguna aplicación personalizada que accede a ArcGIS Online? Si es así, deberás asegurarte de que dichas aplicaciones y configuraciones del sistema operativo de los dispositivos sean compatibles con las conexiones TLS 1.2 con ArcGIS Online a partir de mediados de abril de 2019.

¿Tu organización está elevando sus requisitos de seguridad de red para exigir TLS 1.2 o posteriores y está deshabilitando las versiones anteriores de TLS y SSL? Si es así, deberás asegurarte de que los entornos de su sistema operativo y software estén actualizados para ser compatibles con los nuevos requisitos internos de TI admitiendo TLS 1.2.

Para mayor información, visita https://support.esri.com/en/tls

ArcGIS Enterprise

	CUÁNDO AFECTA	QUÉ HACER
ArcGIS Server **(+info)**	Depende de la compatibilidad del sistema operativo	
	Windows Server 2008** NO admite TLS 1.2. ***AFECTADO	Actualización de S.O
	Windows Server 2008 R2 y Windows Server 2012** ***PUEDE QUE ESTÉ AFECTADO. Ver *Qué hacer.*	Puede que sea necesario habilitar explícitamente la compatibilidad con TLS 1.2 en la cuenta de ArcGIS Server (Si está instalado Internet Explorer 11, la configuración del sistema se actualiza para habilitar TLS 1.2 de forma predeterminada. Si Internet Explorer 11 no está instalado en el servidor, puede que sea necesario habilitar explícitamente la compatibilidad con TLS 1.2 en la cuenta de ArcGIS Server)
	Windows Server 2012 R2 y Windows Server 2016** ***NO SE VEN AFECTADOS y tampoco necesitan configuración adicional.	
	Linux** ***NO AFECTADO	
Portal for ArcGIS **(+info)**	Depende de la versión de Portal for ArcGIS	
	Versiones 10.4 o inferiores** ***AFECTADO	Actualizar a versión de Portal for ArcGIS posterior a 10.4
	Versiones 10.4.1 o superiores** ***NO AFECTADO	

ArcGIS Desktop

	CUÁNDO AFECTA	QUÉ HACER
ArcMap **(+info)**	Depende de la versión de ArcMap	
	Versiones 10.6.1 o inferiores** ***AFECTADO	**OPCIÓN 1 (Recomendada):** Instalar el parche ArcGIS Desktop TLS Patch. Para ver cómo instalar el parche pincha este **link**. **OPCIÓN 2:** Configurar el sistema operativo para que use TLS 1.2. De esta manera todas las aplicaciones instaladas en el sistema que dependen de Microsoft .NET Framework, usarán TLS 1.2. Para ver cómo configurar TLS 1.2 en Windows para ArcGIS Desktop pincha este **link**.
	Versiones 10.7 o superiores** ***NO AFECTADO	
ArcGIS Pro **(+info)**	Depende de la versión de ArcGIS Pro	
	Versiones 1.0-1.2 o inferiores** ***AFECTADO	**OPCIÓN 1 (Recomendada):** Actualizar a una versión de ArcGIS Pro que soporte TLS 1.2 **OPCIÓN 2:** Configurar el sistema operativo para que use TLS 1.2. De esta manera todas las aplicaciones instaladas en el sistema que dependen de Microsoft .NET Framework, usarán TLS 1.2. Para ver cómo configurar TLS 1.2 en Windows para ArcGIS Desktop pincha este **link**.
	Versiones 1.3-2.3 o superiores** ***NO AFECTADO	

ArcGIS Runtime SDKs

	CUÁNDO AFECTA	QUÉ HACER
ArcGIS Runtime SDK for Android **(+info)**	Depende de la versión API de Android y del SDK de ArcGIS Runtime	
	Android 4.4 (API 19) con SDK de ArcGIS Runtime 10.2.9 o 100.x o inferiores** ***AFECTADO	Se deberá añadir código a la aplicación para que actualice el proveedor de seguridad del dispositivo tal y como se describe en el siguiente documento para desarrolladores de Android: "Update your security provider to protect against SSL exploits". **Link**
	Android 5 (API 21) con SDK de ArcGIS Runtime 10.2.9 o 100.x o superiores** ***NO AFECTADO	
ArcGIS Runtime SDK for Qt **(+info)**	Depende de la versión de Qt Framework y OpenSSL	
	Versiones 10.2.6 y 100.x de ArcGIS Runtime for Qt** ***PUEDE QUE ESTÉ AFECTADO. Ver *Qué hacer*.	Utilizar la última versión de Qt Framework o la última compatible con ArcGIS Runtime SDK for Qt. Además, para Windows, Android y Linux, instalar las librerías de OpenSSL versión 1.0.1 o superior. Desde Qt 5.5, iOS y macOS soportan TLS 1.2 por defecto.
ArcGIS Runtime SDK for iOS, macOS **(+info)**	***iOS ArcGIS Runtime SDK versión 100.4 y 10.2.x** ***NO AFECTADO***	
	macOS ArcGIS Runtime SDK versión 100.4 y 10.2.x** ***NO AFECTADO	
ArcGIS Runtime SDK for Java **(+info)**	Depende de la versión de Java y del SDK de ArcGIS Runtime	
	ArcGIS 10.2.x y Java 7 o inferior** ***AFECTADO	Actualizar la aplicación para que use la versión Java 8 update 181 o superior
	ArcGIS 100.4 y 10.2.x y Java 8 update o superior** ***NO AFECTADO	
ArcGIS Runtime SDK for .NET **(+info)**	Depende de la versión del SDK de ArcGIS Runtime	
	ArcGIS Runtime SDK for .NET versión 100.0 o superior** ***NO AFECTADO	
	ArcGIS Runtime SDK for .NET (WPF API) 10.2.7** ***AFECTADO	**OPCIÓN 1 (Recomendada):** Recompilar y republicar utilizando Microsoft .NET Framework 4.6 **OPCIÓN 2:** Indicar el uso de TLS 1.2 de ServicePointManager SecurityProtocol = SecurityProtocolType.Tls12
	ArcGIS Runtime SDK for .NET (Windows Store 8.1 API) 10.2.7** ***AFECTADO	NO SOPORTADO
	ArcGIS Runtime SDK for .NET (Windows Phone 8.1 API) 10.2.7** ***AFECTADO	NO SOPORTADO
ArcGIS Engine Java Interops **(+info)**	Depende de la versión de ArcGIS Engine	

	***ArcGIS 10.2.1-10.3.1 vienen con Java 7**
	AFECTADO
		OPCIÓN 1 (Recomendada): Actualizar a una versión de ArcGIS Engine que soporte Java 8.
		
		OPCIÓN 2: Incluir el siguiente código fuente para utilizar TLS 1.2 y seguir con Java 7.
		
		`try {`
		`  SSLContext ctx = SSLContext.getInstance("TLSv1.2");`
		`  ctx.init(null, null, null);`
		`  SSLContext.setDefault(ctx);`
		`} catch (Exception e) {`
		`  System.out.println(e.getMessage());`
		`}`

	ArcGIS 10.4-10.7 vienen con Java 8** ***NO AFECTADO	

Apps

	CUÁNDO AFECTA	QUÉ HACER
ArcGIS Business Analyst Desktop **(+info)**	***Versiones 10.6.1-10.5** ***AFECTADO***	Descarga y actualización del parche para TLS específico. ArcGIS Business Analyst Desktop TLS Patch **aquí**.
ArcGIS Earth **(+info)**	***Versiones 1.5-1.95** ***NO AFECTADO***	
	Versiones 1.0-1.4** ***AFECTADO	**OPCIÓN 1 (Recomendada):** Actualizar la versión ArcGIS Earth a la última disponible. **OPCIÓN 2:** Configurar el sistema operativo para que use TLS 1.2. **Link**
Drone2Map for ArcGIS **(+info)**	***Versión 1.3.2** ***NO AFECTADO***	
	Versión 1.3.1 o inferior** ***AFECTADO	**OPCIÓN 1 (Recomendada):** Actualizar la versión de Drone2Map for ArcGIS a la última disponible. **OPCIÓN 2:** Configurar el sistema operativo para que use TLS 1.2. **Link**
Operations Dashboard for ArcGIS (Windows)	***AFECTADO***	Configurar el sistema operativo para que use TLS 1.2. **Link**
Web AppBuilder for ArcGIS (Developer Edition)	***PUEDE QUE ESTÉ AFECTADO***	Las aplicaciones creadas con Web AppBuilder for ArcGIS (Developer Edition) no necesitan ser republicadas. Las aplicaciones implementadas dependen del navegador que se utiliza para realizar solicitudes a través de TLS 1.2. Los navegadores modernos en sistemas operativos modernos harán esto, pero los sistemas más antiguos, como Windows XP, pueden no hacerlo. Si estás trabajando con capas operativas alojadas fuera de ArcGIS Online, tu servidor tendrá que soportar TLS 1.2 para conectarse y añadir datos a ArcGIS Online.
ArcGIS for AutoCAD **(+info)**	***Versión 370 o inferior** ***AFECTADO***	Configurar el sistema operativo para que use TLS 1.2. **Link**
ArcPad **(+info)**	***Windows Desktop** ***NO AFECTADO***	
	Windows Mobile** ***AFECTADO	Los servicios de sincronización de funciones y los paquetes de carga/descarga de ArcPad no funcionan en Windows Mobile con TLS 1.2.
Collector for ArcGIS (Android)	***Versión 5.0 (API 21) o superior** ***NO AFECTADO***	
	*Versión 4.4 (API 19) o inferior ***AFECTADO***	Utilizar un dispositivo con versión 5.0 o superior
Explorer for ArcGIS (Android)	***Versión 5.0 (API 21) o superior** ***NO AFECTADO***	
	*Versión 4.4 (API 19) o inferior ***AFECTADO***	Utilizar un dispositivo con versión 5.0 o superior
Navigator for ArcGIS (Android)	***Versión 5.0 (API 21) o superior** ***NO AFECTADO***	
	*Versión 4.4 (API 19) o inferior ***AFECTADO***	Utilizar un dispositivo con versión 5.0 o superior
Tracker for ArcGIS (Android)	***Versión 5.0 (API 21) o superior** ***NO AFECTADO***	
	*Versión 4.4 (API 19) o inferior ***AFECTADO***	Utilizar un dispositivo con versión 5.0 o superior
Workforce for ArcGIS (Android)	***Versión 5.0 (API 21) o superior** ***NO AFECTADO***	
	*Versión 4.4 (API 19) o inferior ***AFECTADO***	Utilizar un dispositivo con versión 5.0 o superior