



ESTANDAR DE CONFIGURACION TLS

Versión 1.0

Arquitectura y Estándares TI

25/02/2020



Tabla de contenido

1. Objetivos	3
2. Consideraciones para la configuración.	3
3. Configuración Schannel.....	3
4. Configuración Cipher Suites	6

1. Objetivos

El documento tiene como objetivo estandarizar la configuración TLS en los servidores de Desarrollo y certificación, para las aplicaciones creadas dentro del Banco de Crédito de Bolivia SA.

2. Consideraciones para la configuración.

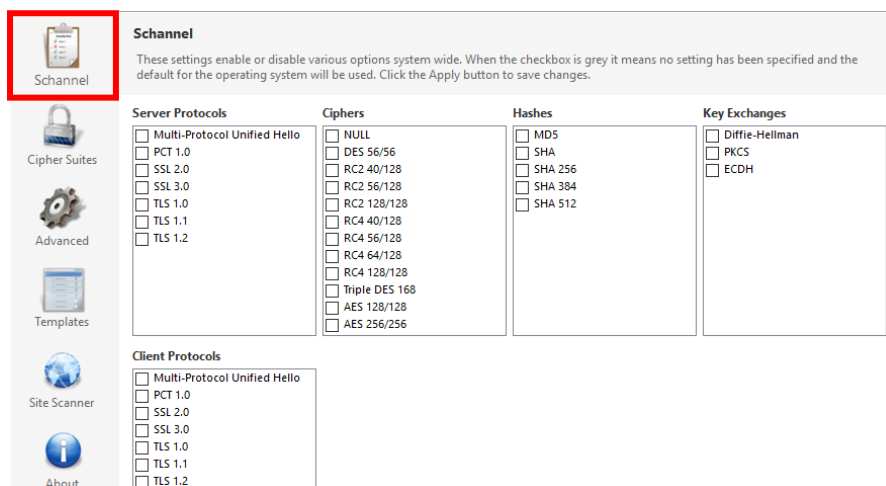
Para la configuración de TLS utilizaremos “IIS Crypto” es una herramienta gratuita que brinda a los administradores la capacidad de habilitar o deshabilitar protocolos, cifrados, hashes y algoritmos de intercambio de claves en Windows Server 2008, 2012, 2016 y 2019.

NOTA: La configuración en ambientes de desarrollo puede ser realizada por el equipo de desarrollo.

La configuración en ambientes de certificación y producción debe ser realizada por el equipo de servidores.

3. Configuración Schannel

Inicialmente ingresaremos a la opción Schannel.



3.1. Configuración Server Protocols

Para la configuración de Server Protocols es requerido que habilite la opción TLS 1.2, como muestra a imagen.

Server Protocols

<input type="checkbox"/>	Multi-Protocol Unified Hello
<input type="checkbox"/>	PCT 1.0
<input type="checkbox"/>	SSL 2.0
<input type="checkbox"/>	SSL 3.0
<input type="checkbox"/>	TLS 1.0
<input type="checkbox"/>	TLS 1.1
<input checked="" type="checkbox"/>	TLS 1.2

3.2. Configuración de Ciphers

Para la configuración de Ciphers habilite las siguientes opciones “AES 128/128” y “AES 256/256” como muestra la imagen.

Ciphers

<input type="checkbox"/>	NULL
<input type="checkbox"/>	DES 56/56
<input type="checkbox"/>	RC2 40/128
<input type="checkbox"/>	RC2 56/128
<input type="checkbox"/>	RC2 128/128
<input type="checkbox"/>	RC4 40/128
<input type="checkbox"/>	RC4 56/128
<input type="checkbox"/>	RC4 64/128
<input type="checkbox"/>	RC4 128/128
<input type="checkbox"/>	Triple DES 168
<input checked="" type="checkbox"/>	AES 128/128
<input checked="" type="checkbox"/>	AES 256/256

3.3. Configuración Hashes

Por defecto deben estar seleccionados todas las casillas de la opción “Hashes”

Hashes

<input checked="" type="checkbox"/>	MD5
<input checked="" type="checkbox"/>	SHA
<input checked="" type="checkbox"/>	SHA 256
<input checked="" type="checkbox"/>	SHA 384
<input checked="" type="checkbox"/>	SHA 512

NOTA: Las nuevas aplicaciones/desarrollos NO deben utilizar los algoritmos “MD5” y “SHA”.

3.4. Configuración Key Exchanges

Para la configuración de Key Exchanges debe estar seleccionado la casilla de “PKCS” y “ECDH” como muestra la imagen.

Key Exchanges

<input type="checkbox"/>	Diffie-Hellman
<input checked="" type="checkbox"/>	PKCS
<input checked="" type="checkbox"/>	ECDH

3.5. Configuración Client Protocols

Para la configuración de Client Protocols debe seleccionar las casillas “SSL 3.0, TLS 1.0, TLS 1.1, TLS 1.2” como muestra la imagen.

Client Protocols

<input type="checkbox"/>	Multi-Protocol Unified Hello
<input type="checkbox"/>	PCT 1.0
<input type="checkbox"/>	SSL 2.0
<input checked="" type="checkbox"/>	SSL 3.0
<input checked="" type="checkbox"/>	TLS 1.0
<input checked="" type="checkbox"/>	TLS 1.1
<input checked="" type="checkbox"/>	TLS 1.2

Al finalizar la configuración Schannel debería quedar la siguiente manera.

Schannel

These settings enable or disable various options system wide. When the checkbox is grey it means no setting has been specified and the default for the operating system will be used. Click the Apply button to save changes.

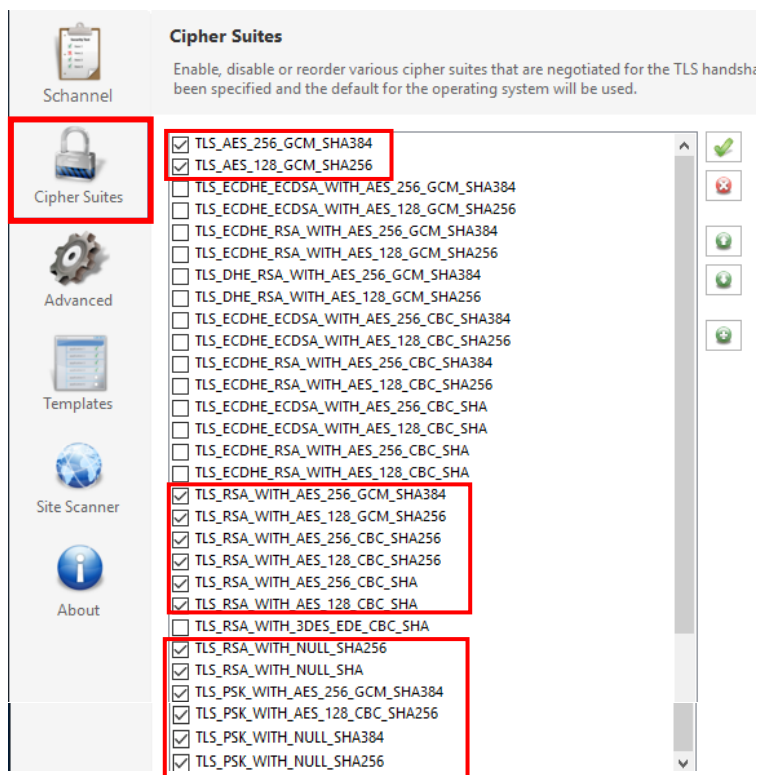
Server Protocols	Ciphers	Hashes	Key Exchanges
<input type="checkbox"/> Multi-Protocol Unified Hello	<input type="checkbox"/> NULL	<input checked="" type="checkbox"/> MD5	<input type="checkbox"/> Diffie-Hellman
<input type="checkbox"/> PCT 1.0	<input type="checkbox"/> DES 56/56	<input checked="" type="checkbox"/> SHA	<input checked="" type="checkbox"/> PKCS
<input type="checkbox"/> SSL 2.0	<input type="checkbox"/> RC2 40/128	<input checked="" type="checkbox"/> SHA 256	<input checked="" type="checkbox"/> ECDH
<input type="checkbox"/> SSL 3.0	<input type="checkbox"/> RC2 56/128	<input checked="" type="checkbox"/> SHA 384	
<input type="checkbox"/> TLS 1.0	<input type="checkbox"/> RC2 128/128	<input checked="" type="checkbox"/> SHA 512	
<input type="checkbox"/> TLS 1.1	<input type="checkbox"/> RC4 40/128		
<input checked="" type="checkbox"/> TLS 1.2	<input type="checkbox"/> RC4 56/128		
	<input type="checkbox"/> RC4 64/128		
	<input type="checkbox"/> RC4 128/128		
	<input type="checkbox"/> Triple DES 168		
	<input checked="" type="checkbox"/> AES 128/128		
	<input checked="" type="checkbox"/> AES 256/256		

Client Protocols

<input type="checkbox"/>	Multi-Protocol Unified Hello
<input type="checkbox"/>	PCT 1.0
<input type="checkbox"/>	SSL 2.0
<input checked="" type="checkbox"/>	SSL 3.0
<input checked="" type="checkbox"/>	TLS 1.0
<input checked="" type="checkbox"/>	TLS 1.1
<input checked="" type="checkbox"/>	TLS 1.2

4. Configuración Cipher Suites

Para la configuración de la opción Cipher Suites seleccione las siguientes casillas:



NOTA: Para los Cipher Suites las siguientes casillas

- DHE
- ECOHE
- 3DES

Deben estar deshabilitados, de otro modo el servidor esta vulnerable.