

Dear Sir / Madam,

As per SEBI/Exchanges Instructions, the steps listed below need to be followed.

Please make sure you follow the steps provided below and deployed to our Backoffice application servers.

- Remove weak ciphers and TLS versions (1.0, 1.1) from your Backoffice server as per **Annexure I**.
- Update all Backoffice servers and client PCs with the latest security patch (like Microsoft OS/ Windows / MS SQL).
- Ensure that the well-known antivirus is installed on all your servers, and it should be up to date.
- Use well-known network firewalls to secure your network, and only allow the Web Backoffice Server access over HTTPS (secure) ports from external sources. For additional security, you can use Location Base policy (country Base for example India) and block all other ports.
- On everyday basis or weekly basis as per requirement of exchange we are updating required changes with latest Patch, please ensure that Latest Patch has been done In Techexcel Backoffice software, If you have any queries, please reach out to our Back office support team.
- Keep database and application file in safest place on daily basis.

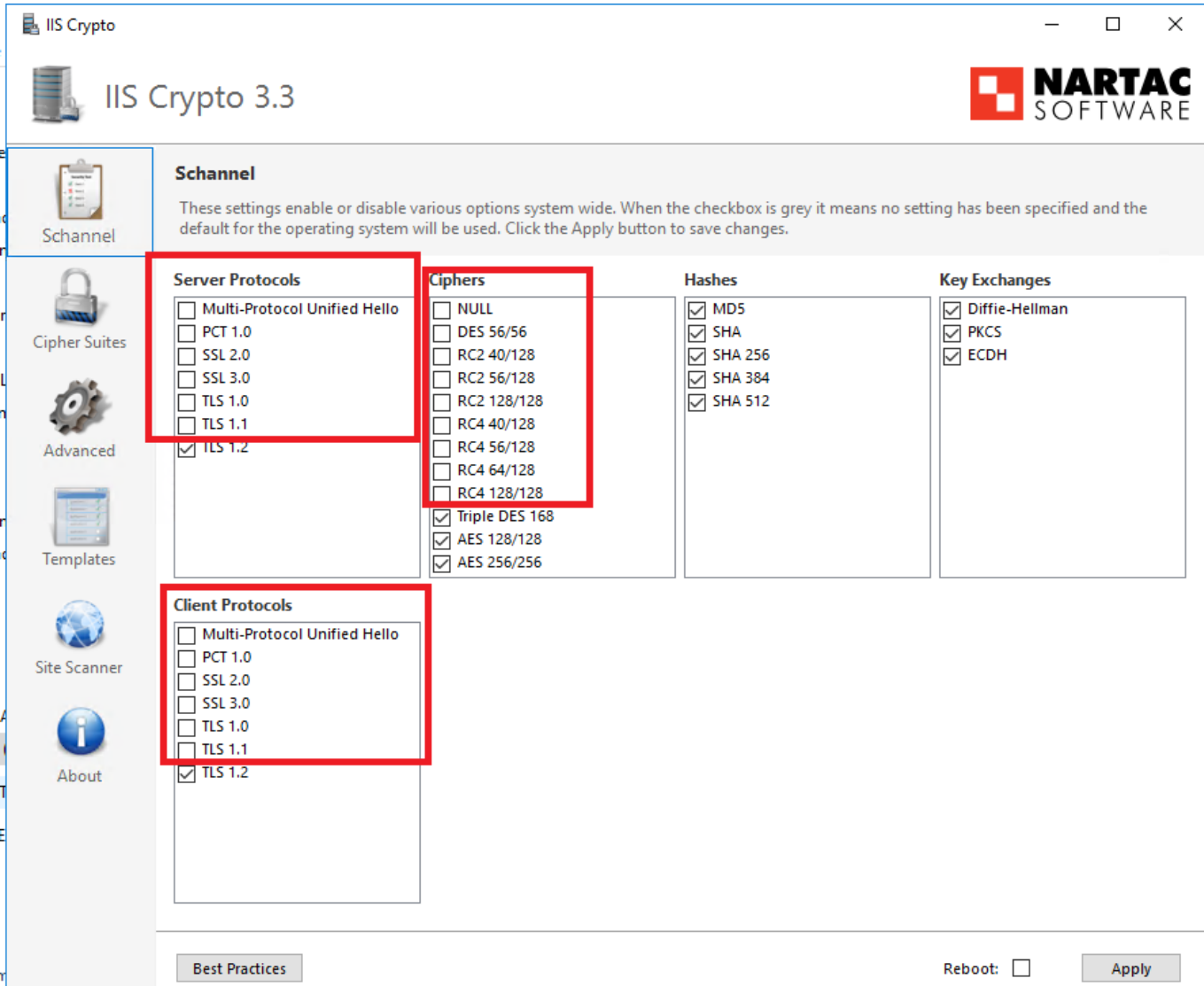
Note:

1. Perform the VAPT scan on our “webclient” product using the CERT-In auditor.
2. If you are already done then please ignore these points.
3. If you are not using our “webclient” then let us know so we will remove it from server.

In case any further clarification or assistance is needed, please feel free to reach us. Assuring you of great services as always.

Annexure I

We are removing all selected method as per best practices and TLS 1.0 and TLS 1.1



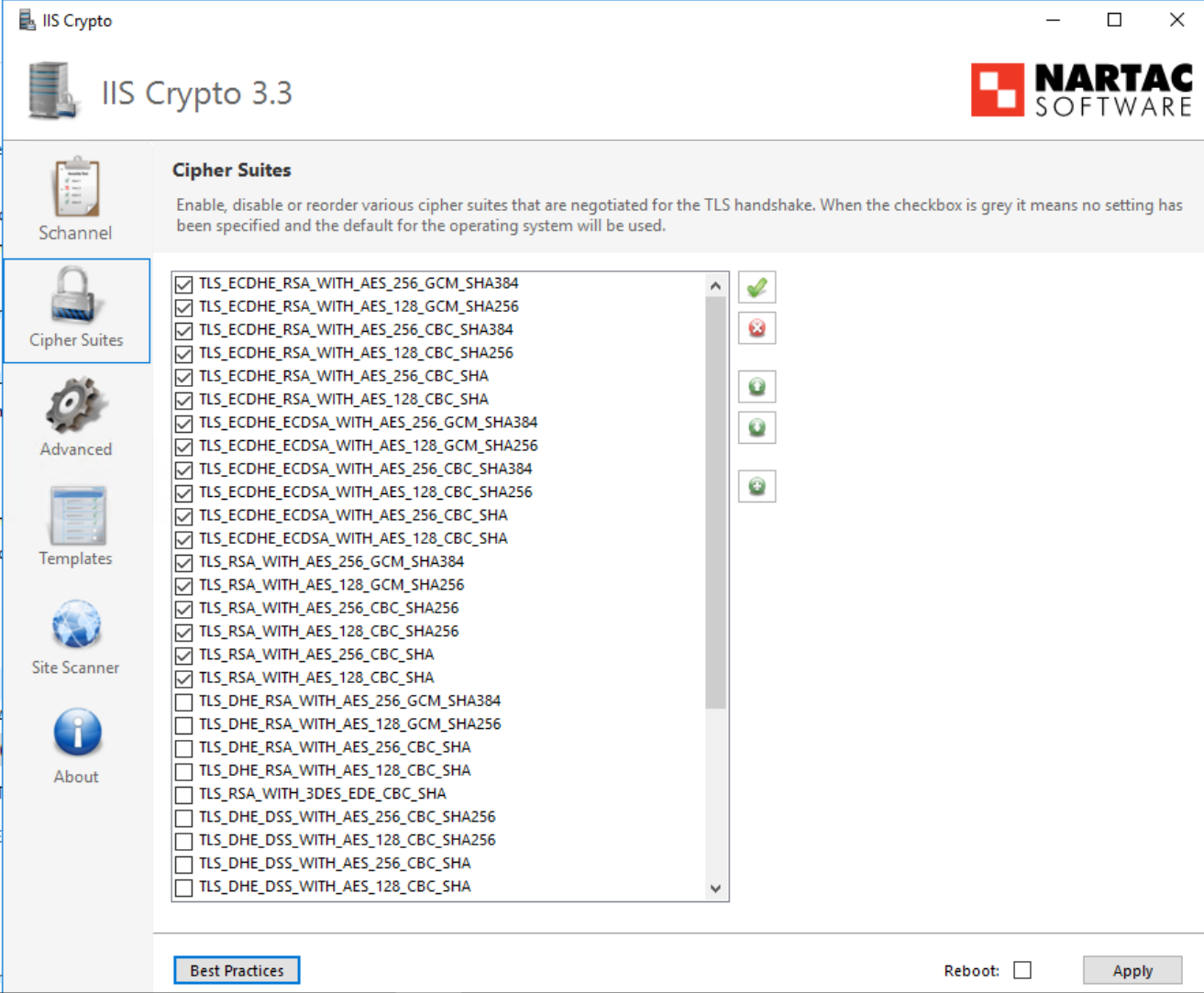
IIS Crypto 3.3 **NARTAC SOFTWARE**

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 checked="" 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 checked="" 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 type="checkbox"/> SSL 3.0
<input type="checkbox"/> TLS 1.0
<input type="checkbox"/> TLS 1.1
<input checked="" type="checkbox"/> TLS 1.2

Reboot:



IIS Crypto 3.3

NARTAC SOFTWARE

Cipher Suites

Enable, disable or reorder various cipher suites that are negotiated for the TLS handshake. When the checkbox is grey it means no setting has been specified and the default for the operating system will be used.

- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA256
- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA

Best Practices Reboot: Apply

Reference URL

<https://social.technet.microsoft.com/wiki/contents/articles/52234.exchange-2016-cipher-lockdown-with-iiscrypto-2-0.aspx?Redirected=true>