



راهاندازی و پیکربندی امن پروتکل SSL/TLS بر روی سرویسدهنده پست الکترونیک MDaemon server 13

APA-AMIRKABIR-13950704-	شماره مستند1
۴ مهر ۱۳۹۵	تاریخ نگارش
۱/۰	شماره نگارش
آپای امیر کبیر	نگارش
عادی	طبقەبندى

فهرست مطالب

1	۱ مقدمه۱
۲нтт	۲ فعالسازی ار تباطات PS
ضا۲	۲-۱ ساخت گواهی خود-ام
ر شده از مراکز صدور گواهی۶	۲-۲ استفاده از گواهی صاد
۲SSL/TLS	۳ پیکربندی امن پروتکل ز
SSLv3 و SSLv3	SLv2 غیر فعال کردن SLv2
تمهای رمزنگاری ضعیف	۲-۳ غيرفعال سازي الگورية
۱۱HSTS	۳-۳ اضافه کردن سرآیند ۲
14	۴ منابع۴





ا مقدمه

شرکتها و سازمانهای کوچک عمدتاً از شرکتهای سرویسدهنده Hosting برای پست الکترونیک خود استفاده میکنند اما شرکتهای متوسط و بزرگ به دلیل مسائل امنیتی و حساسیت سرویس پست الکترونیک برای آنان، ناچار به استفاده از یک Mail Server اختصاصی در محل خود هستند.

برای تأمین محرمانگی و جامعیت دادههای مبادله شده می توان از پروتکلهای استانداردی که بدین منظور طراحی شده استفاده کرد. در حال حاضر مهم ترین پروتکل رمزنگاری که در سطح اینترنت برای رمزنگاری دادههای لایه کاربرد و تأمین امنیت ارتباطات استفاده می شود، پروتکل SSL/TLS است. یکی از سرویس دهندههای پست الکترونیک، MDaemon است که در این گزارش به پیکربندی امن پروتکل SSL/TLS در آن می پردازیم. قابل ذکر است که MDaemon برای فراهم کردن سرویس SSL، متکی به ویندوز است و تنظیمات مربوط به ویندوز را مورد استفاده قرار می دهد. در این گزارش مراحل راهاندازی پروتکل SSL/TLS را روی SSL/TLS را در ویندوز سرور که می می می در این گزارش مراحل داماندازی پروتکل SSL/TLS را در ویندوز است و می کنیم.







HTTPS فعال سازی ارتباطات

برای پیکربندی سرویسدهنده HTTPS و استفاده از این پروتکل ابتدا باید گواهینامه دیجیتال مربوطه را از مراکل مراکلی مراکلی مراکلی مراکلی مراکلی (CA) معتبر دریافت کرد (یا گواهی خود-امضا^۲ را تولید کرد). گرفتن گواهی دارای مراحلی است که برای اطلاعات بیشتر در این زمینه میتوانید به گزارش ارائه شده توسط پژوهشکده آپای دانشگاه صنعتی امیرکبیر که در آدرس زیر قرار دارد مراجعه کنید:

http://apa.aut.ac.ir/?p=971

1-4 ساخت گواهی خود-امضا

در اینجا بیان می کنیم که چگونه می توان با تولید و استفاده از یک گواهی خود-امضا، ار تباطات از نوع HTTPS در WorldClient برقرار کرد.

در نوار ابزار گزینه Setup و سپس Web & IM Services را انتخاب می کنیم.

۲. گزینه SSL & HTTPS را انتخاب می کنیم و در اینجا می توانیم مواردی مثل طول کلید رمزنگاری و نام میزبان را وارد کرد.

^r Self-signed



[\] Certificate Authority





Services	×
Web & IM Services WorldClient (web mail) Web Server St & HTTPS ComAgent & IM Calendar RelayFax Options WebAdmin (web configuration) Attachment Linking	Accept the Following Connection Types HTTP only HTTP and HTTPS HTTPS port 3001 HTTPS only HTTP redirected to HTTPS Subject Issuer Expiration date WIN-AESS23JVP WIN-AESS23JVPSO 1/28/2026 Delete Host name (ex: wc.altn.com) mail.apa.local Delete Organization / company name Mcompany Alternative host names (separate multiple entries with a comma)
	Encryption key length 1024 Country / region United States US Create certificate Restart web server
	Ok Cancel Apply Help

۳. با انتخاب گزینه Create certificate، می توان گواهی مورد نظر را ایجاد کرد.

🖉 Web & IM Services				×
Web & IM Services	Accept the Following Connec C HTTP only C H C HTTPS only C H Subject Iss mail.apa.local mail WIN-AESS29JVP WI Host name (ex: wc.altn.com) Organization / company name Alternative host names (separa Encryption key length	ction Types TTP and HTTPS TTP redirected to HTT suer all.apa.local IN-AESS29JVPSO mail.apa.local Mcompany ate multiple entries with 1024	HTTPS port PS Expiration date 4/17/2020 1/28/2026 a comma)	X 3001 Delete
	Country / region Create certificate Res	United States L start web server	JS	•
		Ok Cance	I Apply	Help



مرکز پژوهشی آپا (آگاهیرسانی، پشتیبانی، امداد برای آسیب پذیریها و حوادث امنیتی سایبری) تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ <u>https://apa.aut.ac.ir</u> - Email: <u>autcert@aut.ac.ir</u> ک



مرکز پژوهشی آپا - دانشگاه صنعتی امیرکبیر



🧐 Security Settings - MDaemon				— ×				
Security Settings Sender Authentication Screening SSL & TLS MDaemon WorldClient (web mail) Remote Administration	Enable SSL, STARTTLS, and STLS Enable the dedicated SSL ports for SMTP, IMAP, PDP3 servers SMTP server sends mail using STARTTLS when possible SMTP server requires SSL on MSA port DomainPOP/MultiPOP servers use STLS whenever possible							
← STARTTLS White List STARTTLS Required List ⊕- Other	Subject example.com Create certificate	Issuer example.com Restart servers	Expiration date 2/26/2019	Delete				
		Ok C	ancel Apply	Help				

- فعال سازی STARTTLS ، SSL و STLS است. با کلیک بر روی این گزینه سرور شما قادر به این گزینه برای فعال سازی پروتکل SSL/TLS است. با کلیک بر روی این گزینه سرور شما قادر به پشتیبانی از SSL/TLS خواهد بود و بعد از انتخاب این گزینه شما باید گواهی نامه مورد نظر خود را از لیست مربوطه انتخاب کنید.
- تخصیص پورتهای SSL اختصاصی برای سرویسهای IMAP ، SMTP و POP3 و POP3
 این گزینه برای تخصیص پورتهای SSL اختصاصی به سرورهای IMAP ، SMTP و POP3 است و صفحه مربوط به تظیمات پورتها به صورت زیر است:





مرکز پژوهشی آپا - دانشگاه صنعتی امیرکبیر



- Server Settings	SMTP, ODMR, & MSA P	orts		
- Delivery	SMTP inbound port	25	SMTP outbound port	25
- Servers	MSA inbound port	587	ODMR inbound port	366
- Ports - DNS	SMTP SSL port	465		
— IPv6 — Binding	POP & IMAP Ports			
- Timeouts	POP inbound port	110	POP outbound port	110
- Sessions	IMAP inbound port	143		
— Mail Release — Archiving	POP SSL port	995	IMAP SSL port	993
— Pruning — Unknown Mail	Other Ports			
- Message Recall	DNS outbound port	53	LDAP port	389
- Domain Sharing - Priority Mail	Remote Admin port	1000	Minger port	4069
-Header Translation	Return port settings to	defaults	Bind to new	port values now
Default Signatures Public & Shared Folders DomainPOP				
⊕-RAS				
⊕- LDAP				
🖶 Loaaina	Ŧ			

• انتخاب گواهی نامه برای استفاده از HTTPS/SSL در این قسمت، گواهی نامه های SSL شما نمایش داده می شود تا بتوانید گزینه مورد نظر خود را برای

استفاده MDaemon انتخاب کنید.

ساخت گواهی نامه

در اینجا شما میتوانید گواهینامه SSL مورد نظر خود را بسازید.

Create SSL Certificate	
Certificate Details	
Host name (ex: wc.altn.com)	mail.example.com
Organization / company name	Alt-N Technologies
Alternative host names (separate mu	Iltiple entries with a comma)
Encryption key length	2048 🔻
Hash algorithm	SHA2 🔻
Country / region	United States US 🔹



مرکز پژوهشی آپا (آگاهیرسانی، پشتیبانی، امداد برای آسیب پذیریها و حوادث امنیتی سایبری) تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ Email: autcert@aut.ac.ir که بستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: Meb: https://apa.aut.ac.ir





بعد از تکمیل شکل بالا، بر روی گزینه Restart servers کلیک کنید تا سرورهای SMTP/IMAP/POP راهاندازی راهاندازی مجدد شوند. در واقع هر زمانی که تغییر در گواهینامه انجام شود، سرویس دهندهها باید راهاندازی مجدد شوند.

۲-۲ استفاده از گواهی صادر شده از مراکز صدور گواهی

وقتی یک گواهینامه از مرکز صدور گواهی گرفته اید، می توانید با استفاده از Microsoft وقتی یک گواهینامه از مرکز صدور گواهی مورد استفاده MDaemon انتقال دهید. برای انجام این مورد، باید موارد زیر را انجام دهید:

- ۱. به مسیر ...Start » Run بروید و "mmc /a" را در در قسمت مربوطه بنویسید و روی OK کلیک کنید.
 - ۲. در پنجره باز شده، به مسیر ...File » Add/Remove Snap-in بروید.
 - ۳. روی Add کلیک کنید.
 - ۴. روی Certificates و سپس Add کلیک کنید.
 - ۵. Computer account را انتخاب و سپس روی Next کلیک کنید.
 - ۶. Local computer را انتخاب و سپس روی Finish کلیک کنید.
 - ۷. روی Close و سپس Ok کلیک کنید.
- ۸. در پنجره سمت چپ روی گزینه Personal و سپس Certificates کلیک کنید (برای گواهیهای خود-امضا، باید قسمت Trusted Root Certification Authorities را انتخاب کنید).
- ۹. در منوی اصلی به مسیر ...Action » All Tasks » Import بروید و سپس روی Next کلیک کنید.
 - ۱۰. فایل گواهی مورد نظر را انتخاب کرده و سپس مراحل بعدی را به پایان برسانید.







SSL/TLS پیکربندی امن پروتکل SSL/TLS

در این بخش چگونگی پیکربندی امن پروتکل SSL/TLS را در ویندوز سرور ۲۰۱۲ برای استفاده سرویس دهنده پست الکترونیک MDaemon بیان می کنیم. مواردی همچون استثنا کردن برخی الگوریتمهای رمزنگاری به منظور کاهش حملاتی شبیه به CRIME، FREAK و LogJAM، غیرفعال سازی نسخههای ناامن SSL، برقرار کردن رمزنگاریهای قوی که از (FS) Forward Secrecy پشتیبانی می کنند و فعال سازی HSTS را بیان می کنیم. قابل ذکر است که MDaemon برای فراهم کردن سرویس SSL/TLS، متکی به ویندوز است و تنظیمات ویندوز را مورد استفاده قرار می دهد. در ادامه پیکربندی امن پروتکل SSL/TLS را در ویندوز سرور ۲۰۱۲ بیان می کنیم.

برای بررسی وضعیت امنیتی پروتکل SSL/TLS سرویس دهنده خود، می توانید به ابزاری که بدین منظور توسط پژوهشکده آپای دانشگاه صنعتی امیر کبیر طراحی شده و در آدرس زیر قرار دارد، مراجعه کنید. https://sslcheck.certcc.ir

۲-۳ غیر فعال کردن SSLv2 و SSLv3

SSLv2 و SSLv3 ناامن هستند و باید غیرفعال شوند. برای غیرفعال سازی آنها، به صورت زیر عمل می کنیم.

- ۱. پنجره ویرایشگر Registry را به صورت دسترسی مدیر (Run as administrator) باز کنید.
 - ۲. در این پنجره به مسیر زیر بروید:

 $HKEY_LOCAL_MACHINE \SYSTEM \CurrentControlSet \Control\SecurityProviders \Schannel \Protocols \Control\SecurityProviders \Schannel \Protocols \Schannel \Protocols \Schannel \Protocols \Protocols \Schannel \Protocols \P$





مرکز پژوهشی آپا (آگاهیرسانی، پشتیبانی، امداد برای آسیب پذیریها و حوادث امنیتی سایبری) تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ <u>autcert@aut.ac.ir</u> ۶۶۴۶۰۳۰۸





- _ **D** X Registry Editor File Edit View Favorites Help PCW Name Data Туре PnP ab (Default) REG_SZ (value not set) Power Print ⊳ PriorityControl ProductOptions SafeBoot ScEvents ScsiPort SecureBoot SecurePipeServers SecurityProviders 퉬 SaslProfiles SCHANNEL Ciphers CipherSuites Hashes KeyExchangeAlgorithms ⊿ I Protocols. Collapse - SSL WDigest New Key ServiceGroup Find... String Value ServiceProvid Delete **Binary Value** Session Mana SNMP Rename DWORD (32-bit) Value Þ --SQMServiceL QWORD (64-bit) Value Export D- Srp Multi-String Value Permissions... SrnFxtension(Expandable String Value Computer\HKEY_LOCAL_MACHINE\SYS Copy Key Name
- ۳. روی Protocols کلیک راست کرده و سپس روی New > Key کلیک کنید.

- ۴. نام آن را "SSL 3.0" قرار دهید.
- ۵. روی SSL 3.0 کلیک راست کرده و روی New > Key کلیک کنید.





مرکز پژوهشی آپا (آگاهیرسانی، پشتیبانی، امداد برای آسیب پذیریها و حوادث امنیتی سایبری) تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور - ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ :web: <u>https://apa.aut.ac.ir</u> - Email





- ۶. نام آن را "Client" قرار دهید.
- ۲. دوباره مرحله ۵ را تکرار کرده و نام آن را این بار "Server" قرار دهید.
- ۸. روی Client کلیک راست کرده و به مسیر New > DWORD (32-bit) Value بروید.

<u>الله</u>						Registry Edi	tor		
File	Edit	View	Favorites Help						
			a 🌗 Schannel	^	Name		Туре	Data	
			Ciphers		ab (De	fault)	REG_SZ	(value not set)	
			CipherSuites		👪 Disa	abledByDefault	REG_DWORD	0x00000001 (1)	
			Hashes			-			
				jorithms					
			⊿ → Protocols						
			SSL 2.0						
			⊿ - 🦺 SSL 3.0						
			Client Serve	Expand					
			🛯 🐌 WDigest	New	•	Key			
			ServiceGroupOrder	Find		String Value			
			ServiceProvider	Delete		Binary Value			
			SNMP	Rename		DWORD (32-b	oit) Value		
				Export		QWORD (64-b	oit) Value		
		1	Srp	Permissions		Multi-String V	/alue		
			Stillmage	Copy Key Name		Expandable St	tring Value		
			Storage Storage						

۹. نام آن را "DisabledByDefault" و مقدار آن را "۱" قرار دهید.

B Registry Editor	_	x
File Edit View Favorites Help		
P - PCW Name Type Data		
▶ - → PnP abb (Default) REG SZ (value not set)		
Edit DWORD (32-bit) Value		
Value name:		
Disabled By Default		
Value data: Base		
1 O Hexadecimal		
OK Cancel		
- B Ciphers		
CipherSuites		
Hashes		
SL 2.0		
4 - 1 SSL 3.0		
Williamst		
b - ServiceProvider		
Session Manager		
SIMP V		
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\SSL 3.0\Client		



مرکز پژوهشی آپا (آگاهیرسانی، پشتیبانی، امداد برای آسیب پذیریها و حوادث امنیتی سایبری) تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ Reb: <u>https://apa.aut.ac.ir</u> - Email: <u>autcert@aut.ac.ir</u>





۱۰. روی Server کلیک راست کرده و به مسیر New > DWORD (32-bit) Value بروید.

đ					R	egistry Editor				x
File	Edit	View	Favorites Help							
			SCHANNEL Ciphers Ciphers KeyExchangeAlg A-Protocols P-SSL 2.0 Ciphers SSL 2.0 Ciphers ServiceGroupOrder ServiceGroupOrder ServiceProvider	Expand New	Name	Type It) REG d REG	SZ DWORD	Data (value not set) 0x00000000 (0)		
			Session Manager	Delete		String Value Binary Value				
			SQMServiceList	Rename		DWORD (32-bit) V	alue			
			 →→ Srp →→ SrpExtensionConfig →→ Stillmage →→ Storage →→ Storage 	Export Permissions Copy Key Name		QWORD (64-bit) \ Multi-String Value Expandable String	alue Value			

۱۱. نام آن را "Enabled " و مقدار آن را "۰" قرار دهید.

<u>ه</u>	Registry Edito	or		_	x
File Edit View Favorites Help					
PCW ^	Name	Туре	Data		
▶ - 🎍 PnP	ab (Default)	REG SZ	(value not set)		
Edit DWORD (32-bit) Value	8 Enabled	REG_DWORD	0x00000000 (0)		
Value name:					
Enabled					
Value data: Base					
O Hexadecimal					
OK Cancel					
	- T				
Ciphers					
Hashes					
KeyExchangeAlgorithms					
⊿ 📙 Protocols					
⊳ - 퉲 SSL 2.0					
⊿ 🍶 SSL 3.0					
Client					
Server					
ServiceGroupOrder					
ServiceOroupOrder					
Session Manager					
SNMP					
Computer\HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control	\SecurityProviders\SCH	ANNEL\Protocols\SSL 3	.0\Server		

۱۲. ویندوز را راهاندازی مجدد کنید.

توجه: به همبن طریق میتوانید SSLv2 را هم غیر فعال کنید. فقط لازم است در مرحله ۴، نام آن را " SSL 2.0" قرار دهید.









۲-۳ غیرفعال سازی الگوریتمهای رمزنگاری ضعیف

پیشنهاد می شود مراحل زیر را برای استفاده از الگوریتم های رمزنگاری قوی و غیرفعال سازی رمزنگاری های ضعیف انجام دهید. دقت کنید که ترتیب الگوریتم ها خیلی مهم است زیرا الگوریتم ها به ترتیب انتخاب می شوند.

- ۱. پنجره gpedit.msc را به صورت دسترسی مدیر (Run as administrator) باز کنید.
 - ۲. به مسیر زیر بروید:

Computer Configuration >> Administrative Templates >> Network >> SSL Configuration Settings

- ۲. روی SSL Cipher Suite Order به منظور ویرایش الگوریتمهای رمزنگاری مورد پذیرش، کلیک کنید. توجه کنید که ویرایشگر تنها 1023 بایت را قبول خواهد کرد و بیشتر از این، بدون هیچ هشداری مورد قبول واقع نمی شود.
- ۴. رمزنگاریهای مورد پذیرش آن را به صورت زیر تغییر دهید (رمزنگاریهای پیشنهاد شده برای استفاده
 ۴. در در ویندوز ۸٫۱ و ویندوز سرور R2 2012):

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA_P256

TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA_P256

TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256_P256

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384_P384

TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256_P256

TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256

TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256_P256

TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 *

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 *

HSTS اضافه کردن سرآیند HSTS

در صورت امکان شما باید ویژگی HSTS^۱ را فعال کنید برای اینکه مرورگرها فقط با پروتکل HTTPS بتوانند با سایت شما ارتباط برقرار کنند.

۱. پنجره IIS Manager را باز کنید و 'HTTP Response Headers' را انتخاب کنید.

¹ HTTP Strict Transport Security



تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور - ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم

Web: <u>https://apa.aut.ac.ir</u> - Email: <u>autcert@aut.ac.ir</u> ۶۶۴۶۰۳۰۸ تلفکس: ۱۵۹۱۶۳۴۳۱۱



مرکز پژوهشی آپا - دانشگاه صنعتی امیرکبیر



e ^j	Internet Information Services (IIS) Manager	_
SCOTT-TEST-SR	/ ▶ Sites ▶ Default Web Site ▶	🖸 🛛 🟠 🔞 🗸
<u>F</u> ile <u>V</u> iew <u>H</u> elp		
Eile View Help Connections Start Page SCOTT-TEST-SRV (SCOTT-TE Application Pools A Sites b O Default Web Site	Default Web Site Home Filter: • • •	Actions Open Feature Explore Edit Permissions Edit Site Bindings Basic Settings View Applications View Virtual Directories Manage Website Compose Vebsite Start Start Stop Browse Vebsite Browse *:80 (http) Advanced Settings Configure Limits
Image: state	Features View کو Content View کو تیر کلیک کنید. بق شکل زیر کلیک کنید. Internet Information Services (IIS) Manager	Help ♥ ۱۱۹۹۱ ۲۰۱۹ ۱۱۹۹۱ ۲۰۱۹ ۲۰۱۹ ۱۱۹۹۱ ۲۰۱۹ ۲۰۱۹ ۲۰۱۹ ۲۰۱۹ ۱۱۹۹۱ ۲۰۱۹ ۲۰۱۹ ۲۰۱۹ ۲۰۱۹ ۲۰۱۹ ۲۰۱۹
	Siter > Default Web Site >	
Eila View Hale		
Connections Connections Constant Start Page	HTTP Response Headers	Actions Add





مرکز پژوهشی آپا (آگاهیرسانی، پشتیبانی، امداد برای آسیب پذیریها و حوادث امنیتی سایبری) تهران - بالاتر از چهارراه ولیعصر - نبش کوچه بالاور – ساختمان معاونت پژوهشی دانشگاه صنعتی امیرکبیر - طبقه سوم کد پستی: ۱۵۹۱۶۳۴۳۱۱ تلفکس: ۶۶۴۶۰۳۰۸ <u>aut.ac.ir</u> هیتی: ۱۵۹۱۶۳۴۳۱۱ یا Web: <u>https://apa.aut.ac.ir</u>



13



۳. اطلاعات خواسته شده را به صورت زیر در پنجره مربوطه وارد کنید.

strict-transport-security
max-age=31536000; includeSubdomains

Add Custom HTTP Response Header ? ×			
Name:			
strict-transport-security			
<u>V</u> alue:			
max-age=31536000; includeSubdomains			
OK Cancel			

۴. روی OK کلیک کنید.









- 1 http://help.altn.com/mdaemon/en/ssl_mdaemon.htm
- 2 https://www.ssl.com/how-to/require-strong-ciphers-in-windows-iis-7-5-and-8/
- 3 https://msdn.microsoft.com/en-gb/library/windows/desktop/aa374757(v=vs.85).aspx
- 4 https://www.zensoftware.co.uk/kb/Knowledgebase/Configuring-SSL-for-SMTP,-IMAP-and-POP3-in-MDaemon
- 5 https://www.digicert.com/ssl-support/iis-disabling-ssl-v3.htm
- 6 http://help.altn.com/mdaemon/en/ssl_creating_and_using_ssl_certifi.htm
- 7 https://scotthelme.co.uk/getting-an-a-on-the-qualys-ssl-test-windows-edition/

