



دانشگاه صنعتی امیرکبیر  
(پلی تکنیک تهران)



# راه اندازی و پیکربندی امن پروتکل SSL/TLS بر روی سرویس دهنده پست الکترونیک MDaemon server 13

شماره مستند ..... APA-AMIRKABIR-13950704-1  
تاریخ نگارش ..... ۴ مهر ۱۳۹۵  
شماره نگارش ..... ۱/۰  
نگارش ..... آپای امیرکبیر  
طبقه بندی ..... عادی

## فهرست مطالب

۱	مقدمه	۱
۲	فعال سازی ارتباطات HTTPS	۲
۲-۱	ساخت گواهی خود-امضا	۲
۲-۲	استفاده از گواهی صادر شده از مراکز صدور گواهی	۶
۳	پیگیربندی امن پروتکل SSL/TLS	۷
۳-۱	غیر فعال کردن SSLv2 و SSLv3	۷
۳-۲	غیرفعال سازی الگوریتم‌های رمزنگاری ضعیف	۱۱
۳-۳	اضافه کردن سرآیند HSTS	۱۱
۴	منابع	۱۴

## ۱ 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 می‌توان از پروتکل‌های استاندارد که بدین منظور طراحی شده استفاده کرد. در حال حاضر مهم‌ترین پروتکل رمزنگاری که در سطح اینترنت برای رمزنگاری داده‌های لایه کاربرد و تأمین امنیت ارتباطات استفاده می‌شود، پروتکل SSL/TLS است. یکی از سرویس‌دهنده‌های پست الکترونیک، MDaemon است که در این گزارش به پیکربندی امن پروتکل SSL/TLS در آن می‌پردازیم. قابل ذکر است که MDaemon برای فراهم کردن سرویس SSL، متکی به ویندوز است و تنظیمات مربوط به ویندوز را مورد استفاده قرار می‌دهد. در این گزارش مراحل راه‌اندازی پروتکل SSL/TLS را روی MDaemon server 13.5.1 و پیکربندی امن پروتکل SSL/TLS را در ویندوز سرور ۲۰۱۲ بیان می‌کنیم.

## ۲ فعال سازی ارتباطات HTTPS

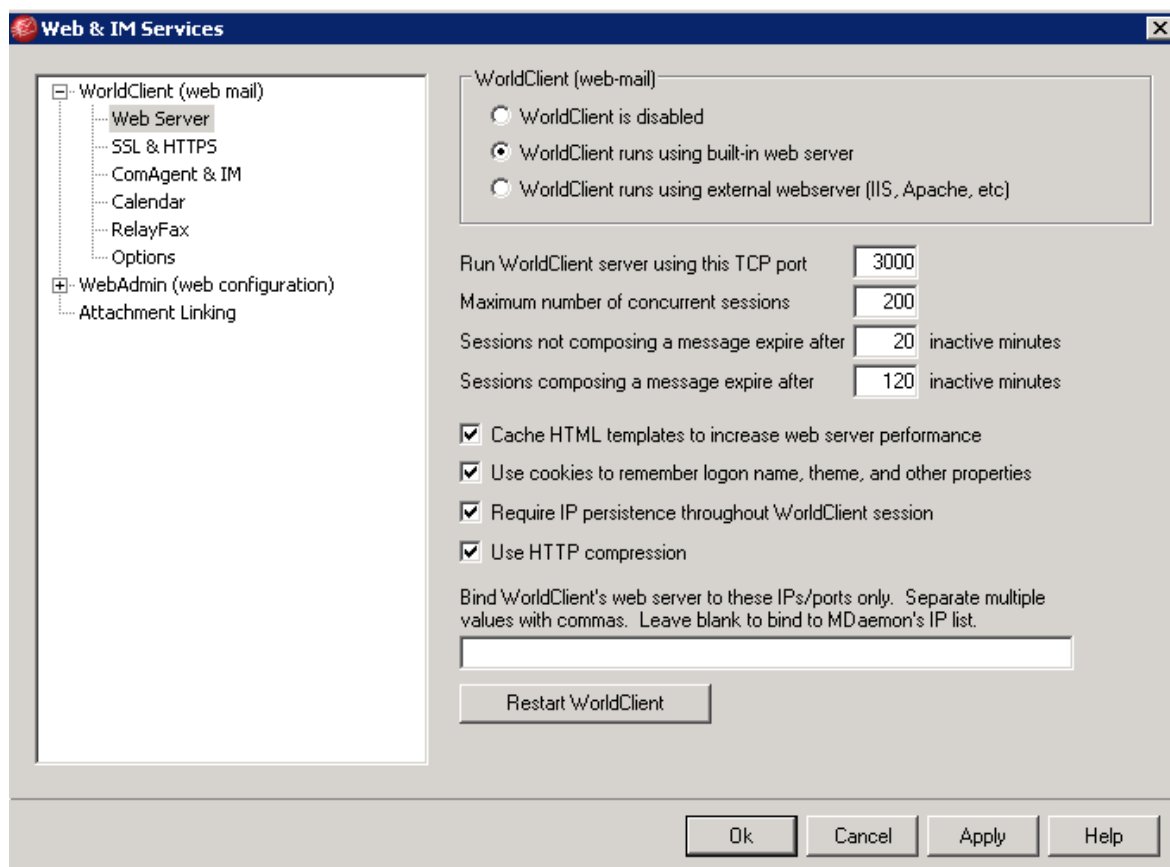
برای پیکربندی سرویس دهنده HTTPS و استفاده از این پروتکل ابتدا باید گواهی نامه دیجیتال مربوطه را از مراکز صدور گواهی (CA)<sup>۱</sup> معتبر دریافت کرد (یا گواهی خود-امضا<sup>۲</sup> را تولید کرد). گرفتن گواهی دارای مراحل است که برای اطلاعات بیشتر در این زمینه می توانید به گزارش ارائه شده توسط پژوهشکده آپای دانشگاه صنعتی امیرکبیر که در آدرس زیر قرار دارد مراجعه کنید:

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

### ۱-۲ ساخت گواهی خود-امضا

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

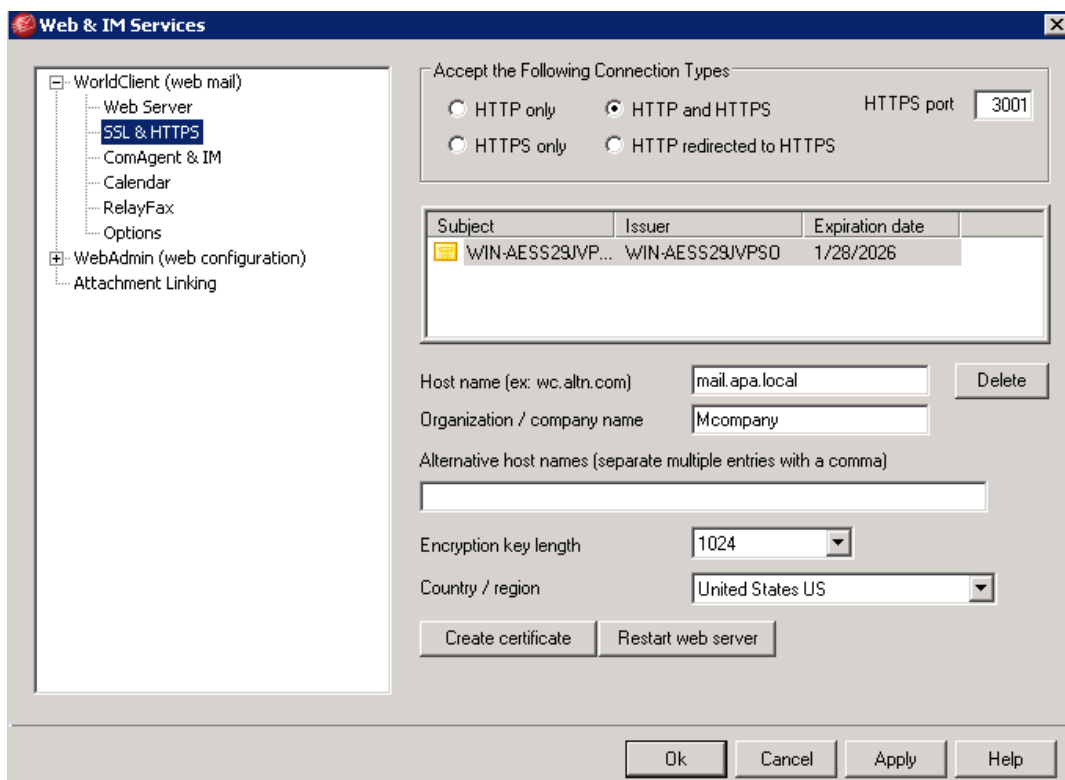
۱. در نوار ابزار گزینه Setup و سپس Web & IM Services را انتخاب می کنیم.



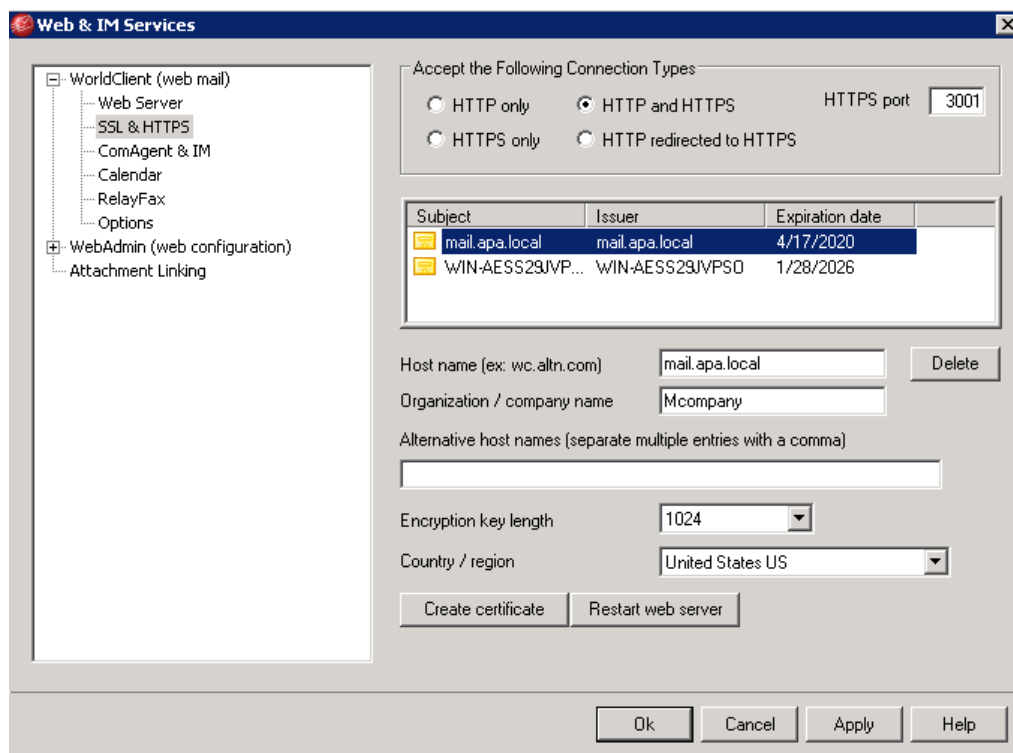
۲. گزینه SSL & HTTPS را انتخاب می کنیم و در اینجا می توانیم مواردی مثل طول کلید رمزنگاری و نام میزبان را وارد کرد.

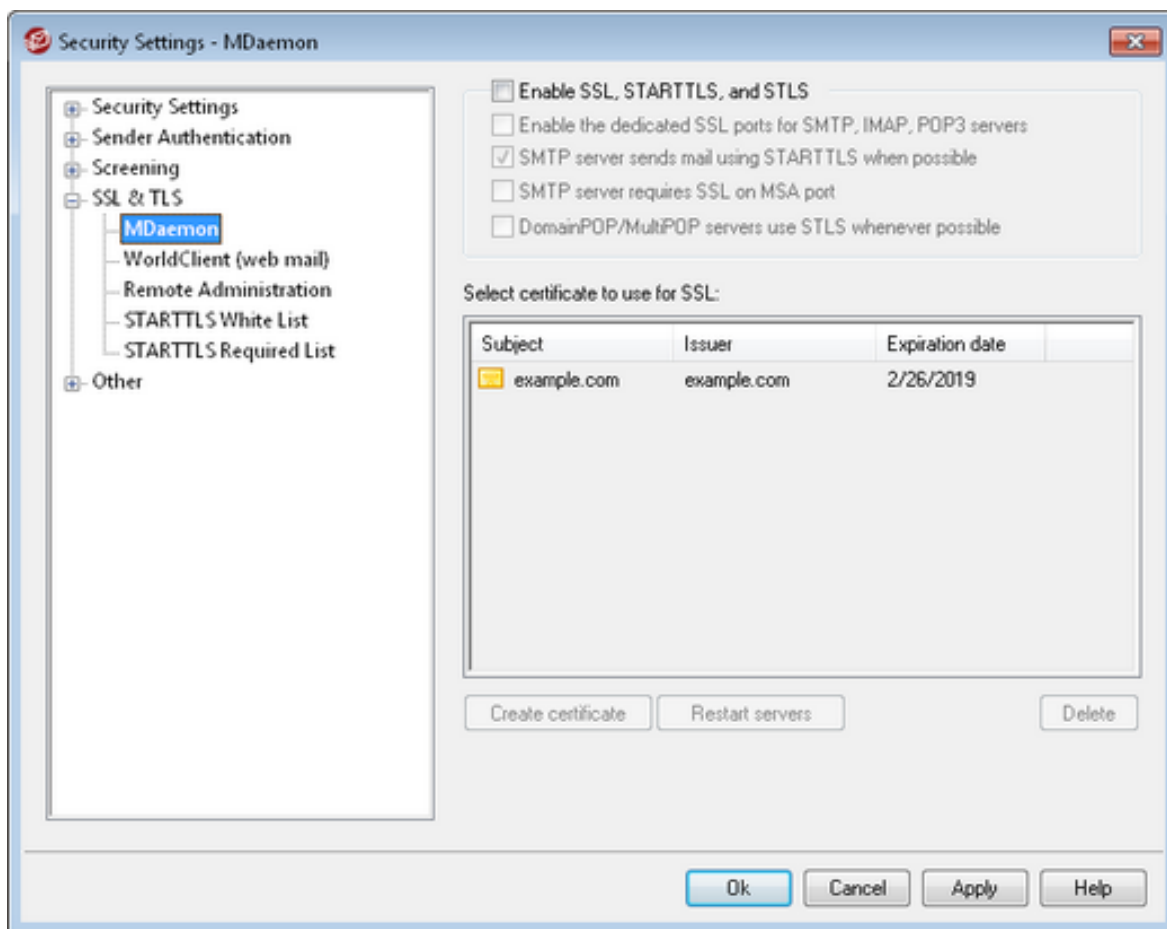
<sup>۱</sup> Certificate Authority

<sup>۲</sup> Self-signed

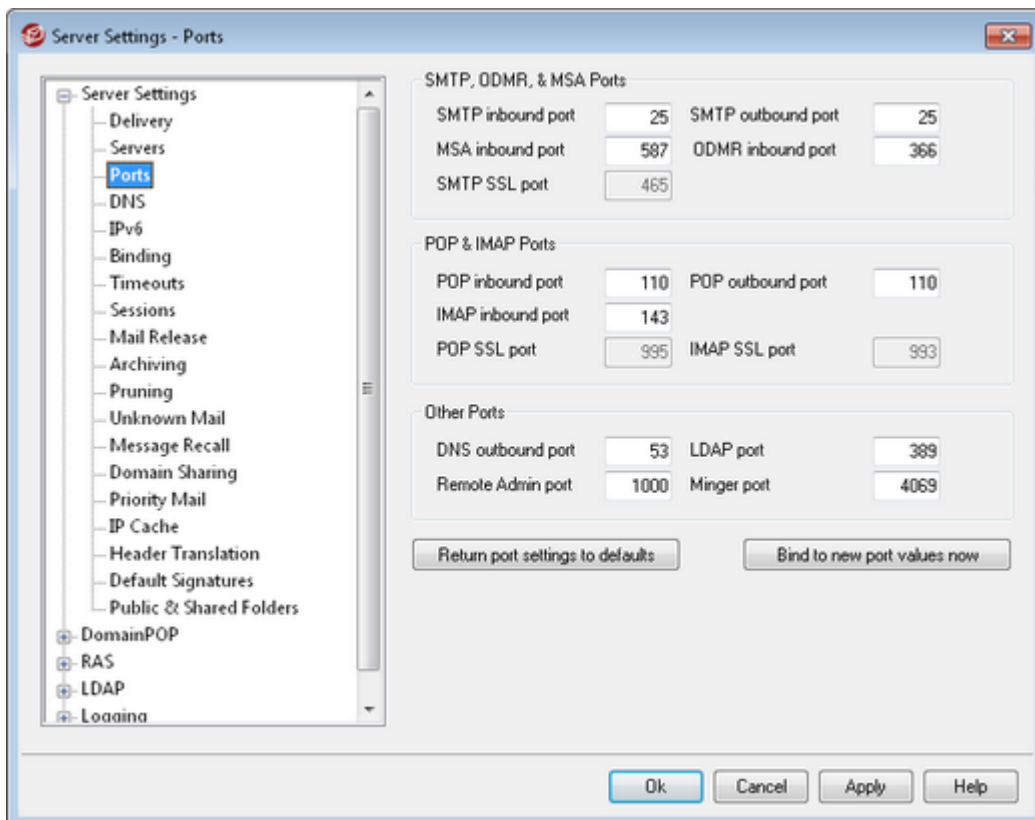


۳. با انتخاب گزینه Create certificate، می‌توان گواهی مورد نظر را ایجاد کرد.



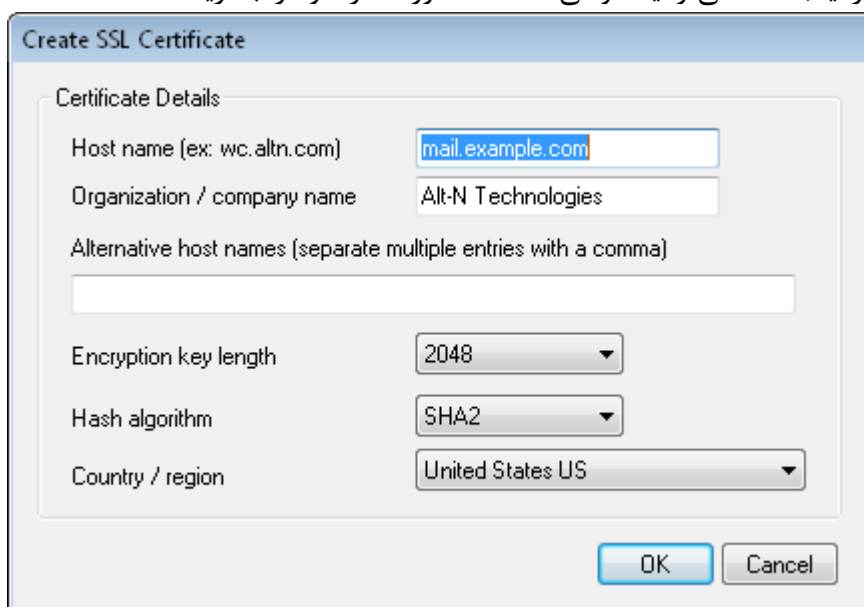


- فعال‌سازی SSL، STARTTLS و STLS  
این گزینه برای فعال‌سازی پروتکل SSL/TLS است. با کلیک بر روی این گزینه سرور شما قادر به پشتیبانی از SSL/TLS خواهد بود و بعد از انتخاب این گزینه شما باید گواهی‌نامه مورد نظر خود را از لیست مربوطه انتخاب کنید.
- تخصیص پورت‌های SSL اختصاصی برای سرویس‌های SMTP، IMAP و POP3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



- انتخاب گواهی نامه برای استفاده از HTTPS/SSL در این قسمت، گواهی نامه‌های SSL شما نمایش داده می‌شود تا بتوانید گزینه مورد نظر خود را برای استفاده MDAemon انتخاب کنید.

- ساخت گواهی نامه در اینجا شما می‌توانید گواهی نامه SSL مورد نظر خود را بسازید.



بعد از تکمیل شکل بالا، بر روی گزینه Restart servers کلیک کنید تا سرورهای SMTP/IMAP/POP راه اندازی مجدد شوند. در واقع هر زمانی که تغییر در گواهی نامه انجام شود، سرویس دهنده ها باید راه اندازی مجدد شوند.

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

وقتی یک گواهی نامه از مرکز صدور گواهی گرفته اید، می توانید با استفاده از Microsoft Management Console آن را به بخش ذخیره 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 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 گواهی های 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.



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

برای بررسی وضعیت امنیتی پروتکل SSL/TLS سرویس دهنده خود، می‌توانید به ابزاری که بدین منظور توسط پژوهشکده آپای دانشگاه صنعتی امیرکبیر طراحی شده و در آدرس زیر قرار دارد، مراجعه کنید.

<https://sslcheck.certcc.ir>

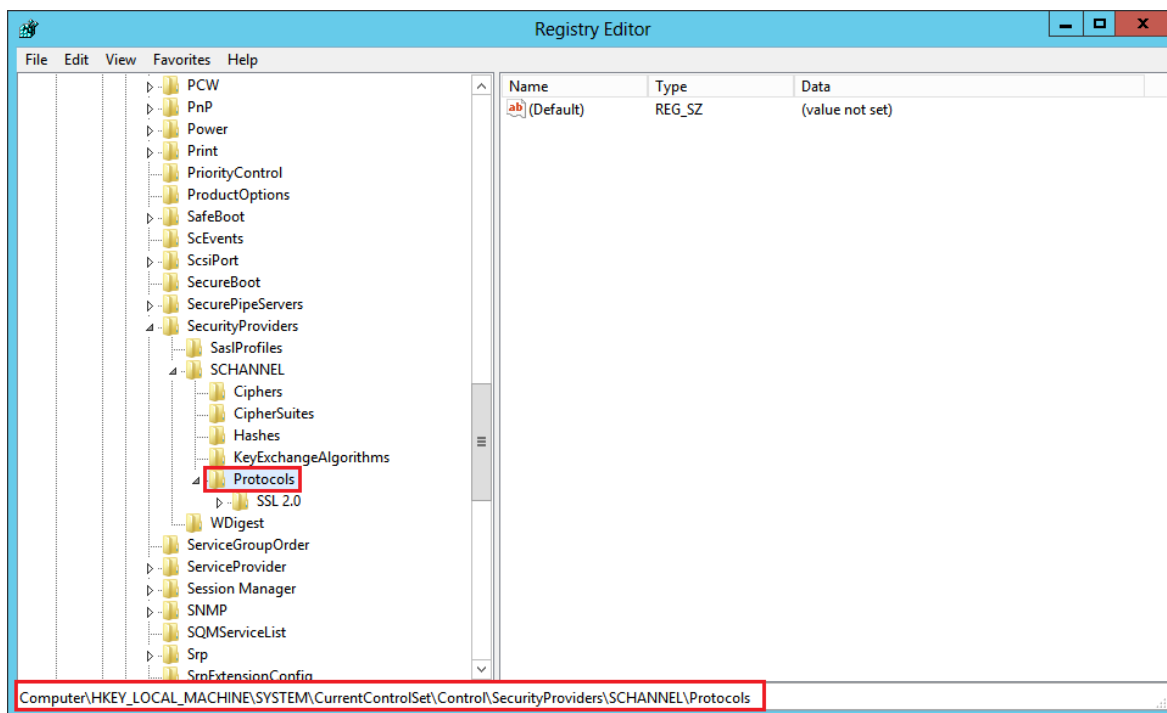
## ۱-۳ غیر فعال کردن SSLv2 و SSLv3

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

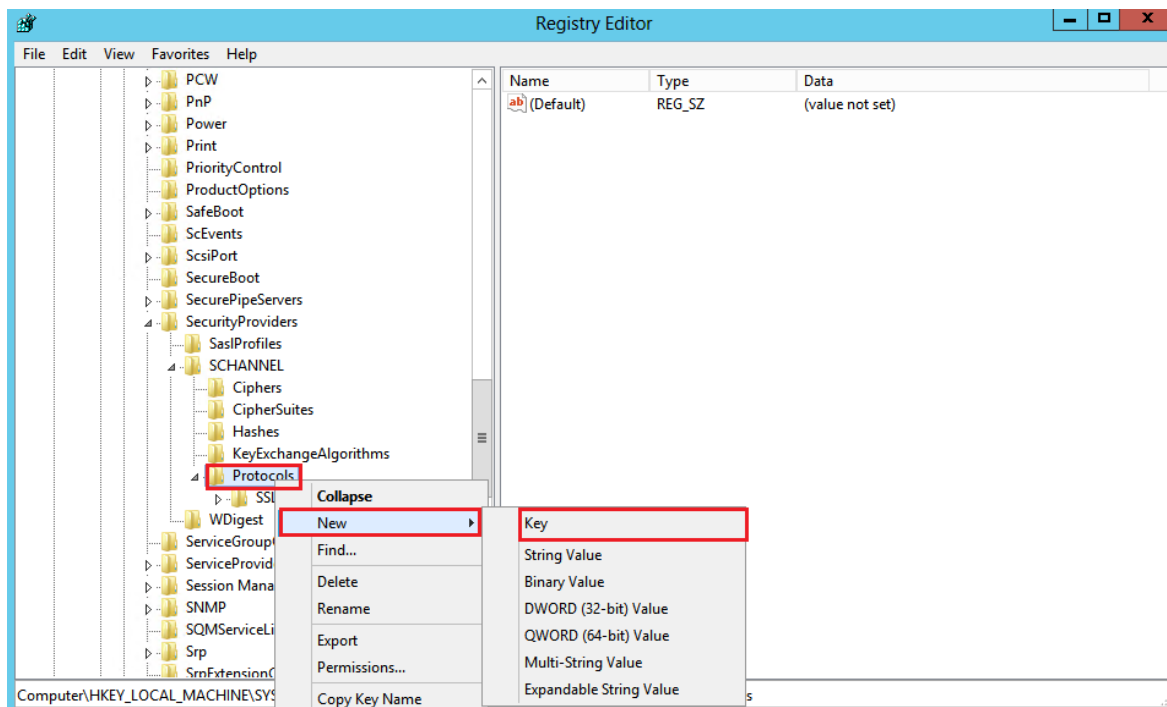
۱. پنجره ویرایشگر Registry را به صورت دسترسی مدیر (Run as administrator) باز کنید.

۲. در این پنجره به مسیر زیر بروید:

HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\Schannel\Protocols\

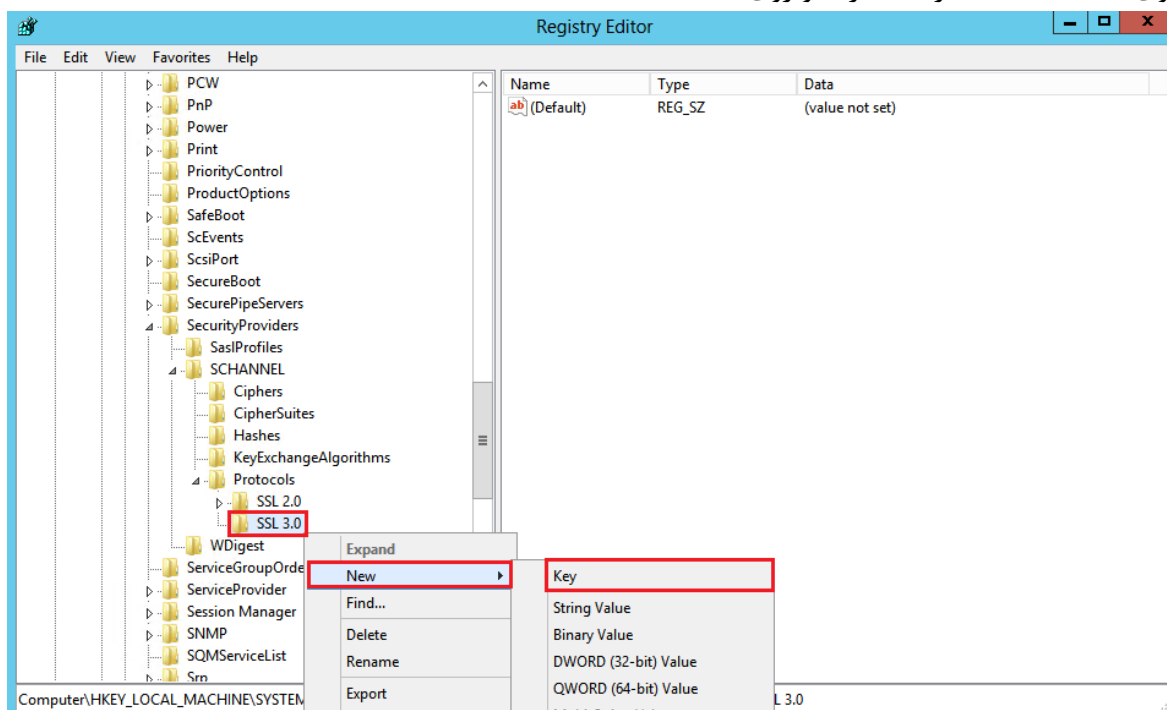


۳. روی Protocols کلیک راست کرده و سپس روی Key > New کلیک کنید.

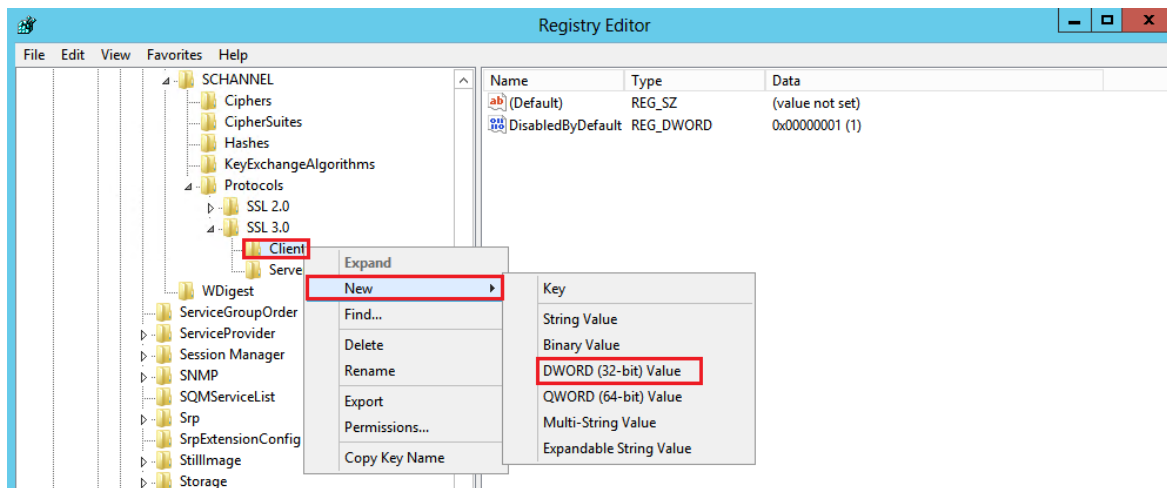


۴. نام آن را "SSL 3.0" قرار دهید.

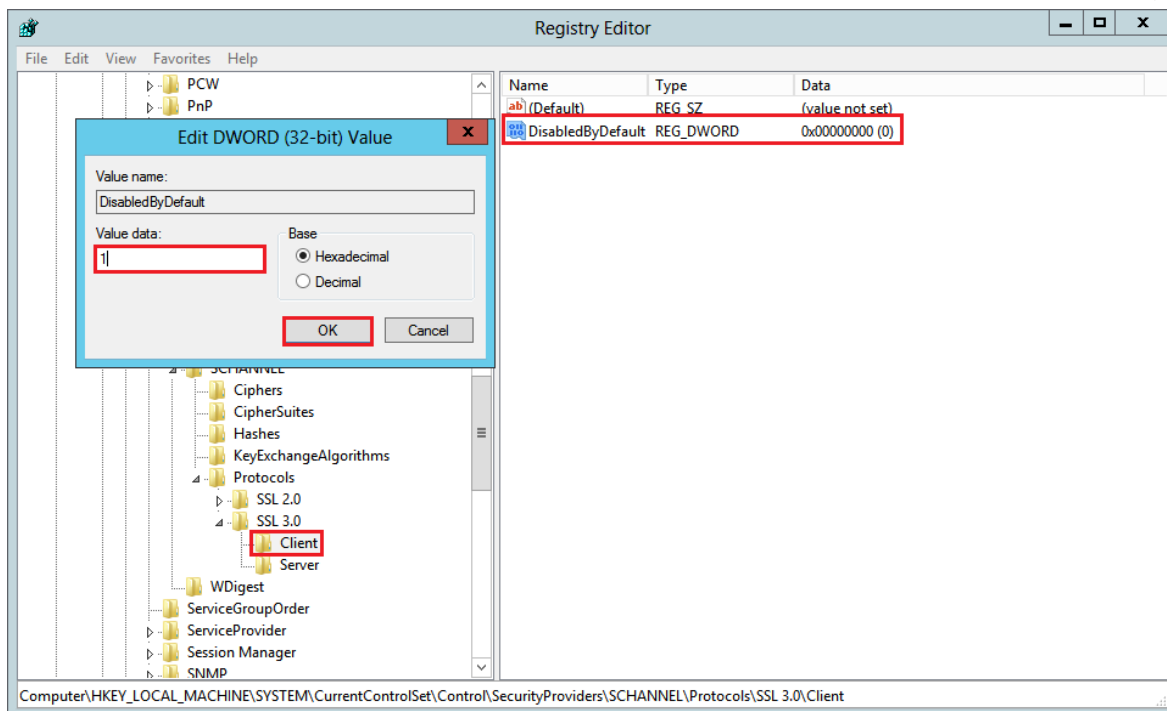
۵. روی SSL 3.0 کلیک راست کرده و روی Key > New کلیک کنید.



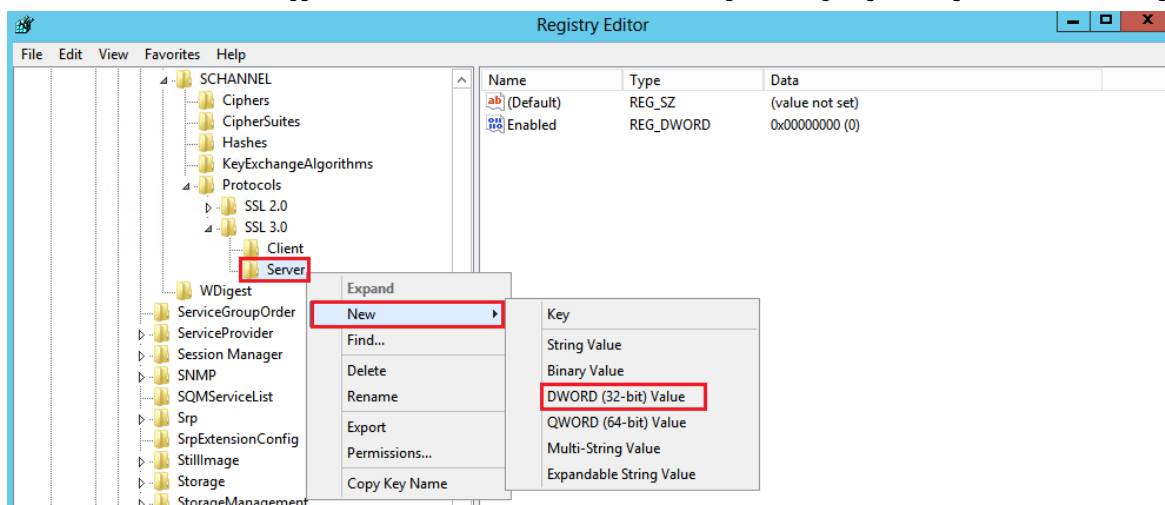
۶. نام آن را "Client" قرار دهید.
۷. دوباره مرحله ۵ را تکرار کرده و نام آن را این بار "Server" قرار دهید.
۸. روی Client کلیک راست کرده و به مسیر New > DWORD (32-bit) Value بروید.



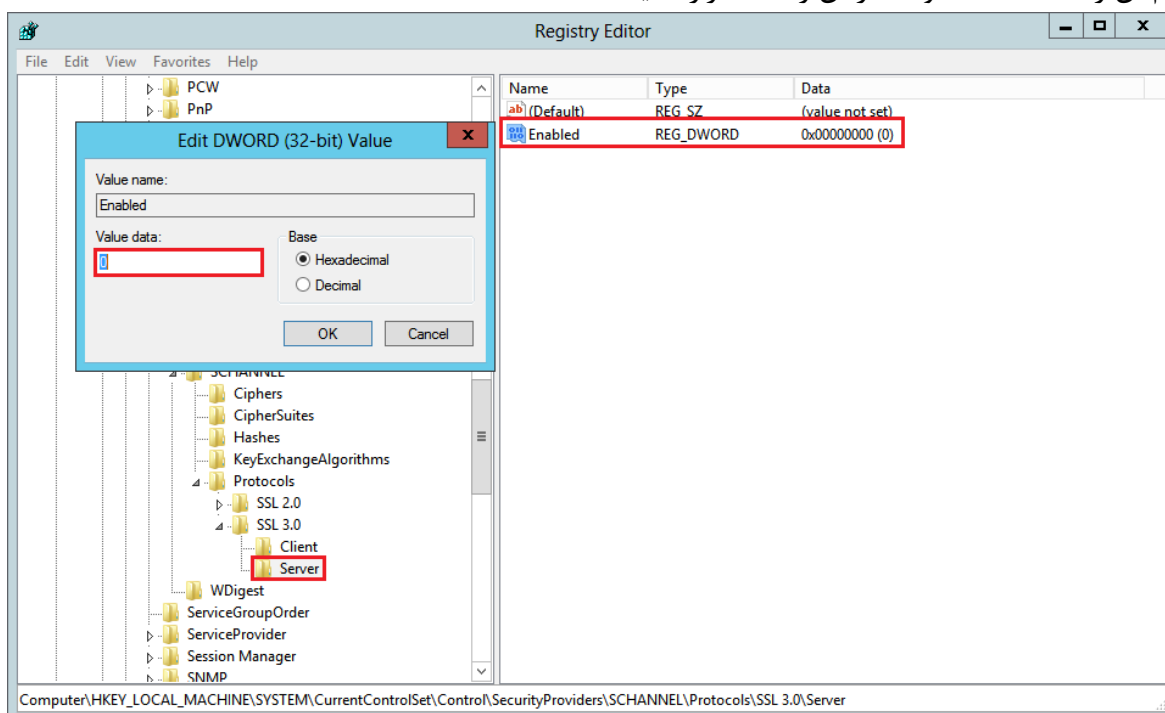
۹. نام آن را "DisabledByDefault" و مقدار آن را "۱" قرار دهید.



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



۱۱. نام آن را "Enabled" و مقدار آن را "0" قرار دهید.



۱۲. ویندوز را راه اندازی مجدد کنید.

توجه: به همین 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 می‌شود مراحل زیر را برای استفاده از الگوریتم‌های رمزنگاری قوی و غیرفعال سازی رمزنگاری‌های ضعیف انجام دهید. دقت کنید که ترتیب الگوریتم‌ها خیلی مهم است زیرا الگوریتم‌ها به ترتیب انتخاب می‌شوند.

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

۳. 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 هشداري مورد قبول واقع نمی‌شود.

۴. رمزنگاری‌های مورد پذیرش آن را به صورت زیر تغییر دهید (رمزنگاری‌های پیشنهاد شده برای استفاده 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 \*

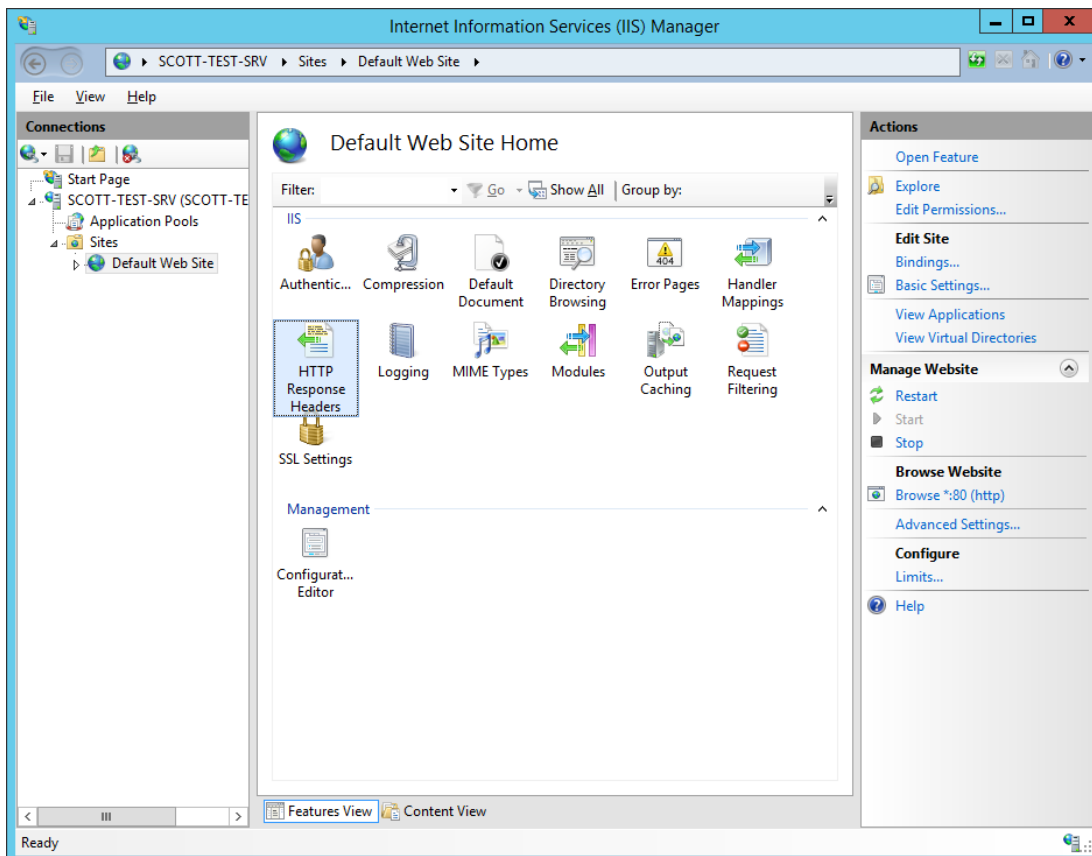
TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384 \*

## ۳-۳ اضافه کردن سرآیند HSTS

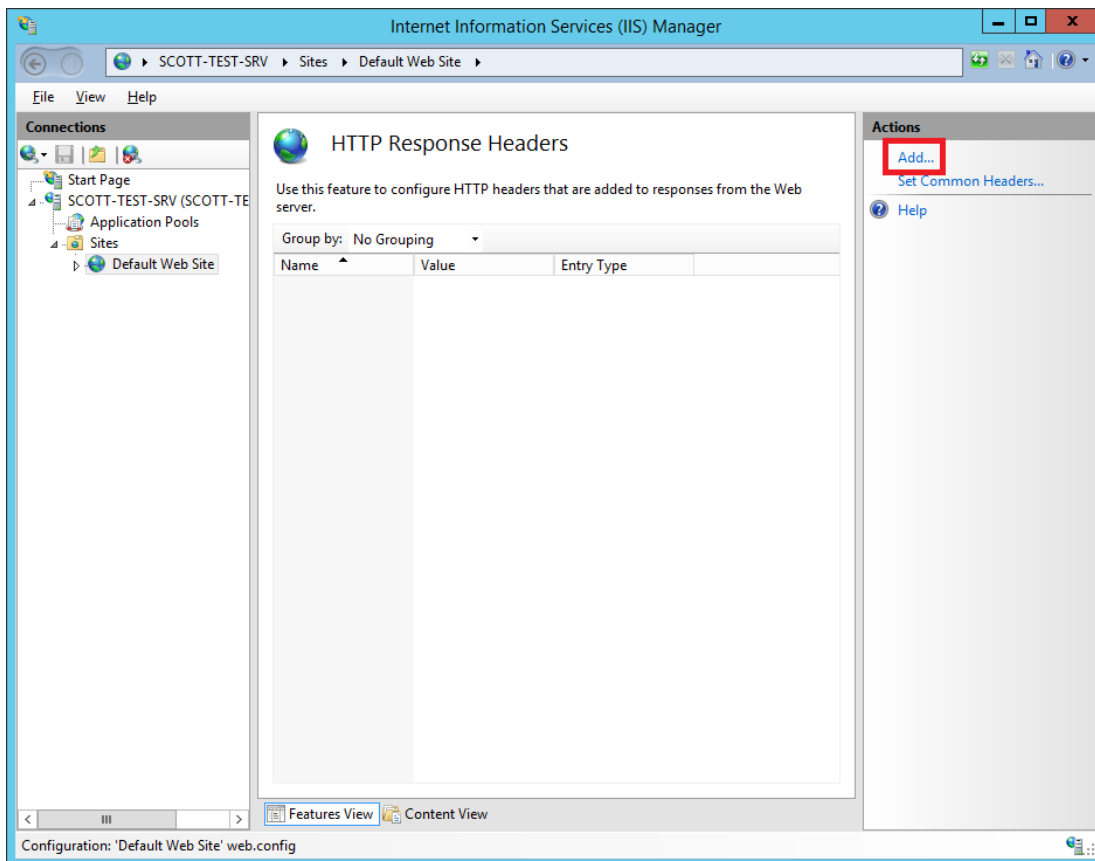
در صورت امکان شما باید ویژگی HSTS<sup>۱</sup> را فعال کنید برای اینکه مرورگرها فقط با پروتکل HTTPS بتوانند با سایت شما ارتباط برقرار کنند.

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

<sup>۱</sup> HTTP Strict Transport Security

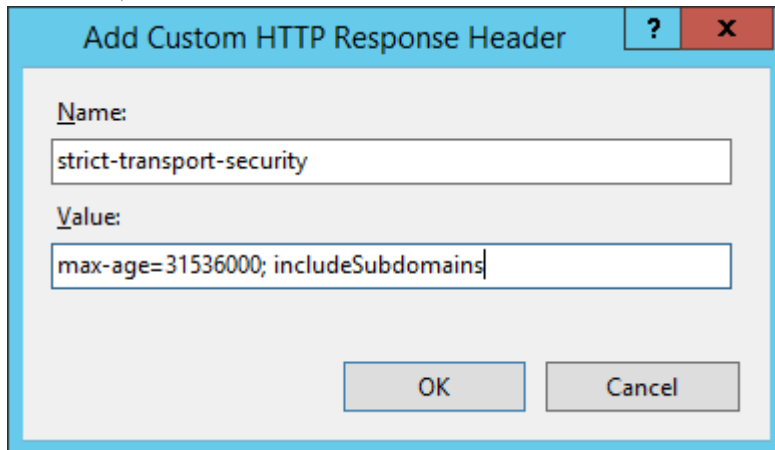


۲. بر روی دکمه Add مطابق شکل زیر کلیک کنید.



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

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



۴. روی OK کلیک کنید.

## ۴ منابع

- 1 [http://help.altn.com/mdaemon/en/ssl\\_mdaemon.htm](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](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](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/>

