



# راه‌اندازی و پیکربندی امن پروتکل SSL/TLS بر روی سرویس‌دهنده وب WebSphere 8.0

**شماره مستند** ..... APA-AMIRKABIR-13950707-1

**تاریخ نگارش** ..... ۷ مهر ۱۳۹۵

**شماره نگارش** ..... ۲/۰

**نگارش** ..... آپای امیرکبیر

**طبقه‌بندی** ..... عادی

# فهرست مطالب

# ۱ مقدمه

برای تأمین محرمانگی و جامعیت داده‌های مبادله شده می‌توان از پروتکل‌های استانداردی 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. در این گزارش مراحل راه‌اندازی گواهی‌نامه SSL و امن‌سازی پروتکل SSL/TLS بر روی سرویس‌دهنده وب WebSphere نسخه 8.0 بیان می‌شود.

# ۲ فعال‌سازی ارتباطات HTTPS

برای پیکربندی سرویس‌دهنده HTTPS و استفاده از این پروتکل ابتدا باید گواهی‌نامه دیجیتال مربوطه را از مراکز صدور گواهی (CA)[۱] معتبر دریافت کرد (یا گواهی خود-امضا 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

برای پشتیبانی از یک ارتباط رمزنگاری شده، می‌توانید یک گواهی‌نامه خود-امضا بسازید و سپس سرور IBM HTTP را برای رمزنگاری ترافیک، تنظیم کنید. اگر شما از این نوع گواهی‌نامه استفاده کنید، به علت عدم امضا شدن این گواهی توسط یک مرکز معتبر صدور گواهی، این امکان وجود دارد که کاربران پیغام اخطار در مرورگر خود دریافت کنند. برای رفع مشکل شما باید از یک گواهی‌نامه که از یک مرکز صدور گواهی مورد اعتماد است، استفاده کنید.

اگر شما در هنگام نصب IBM Connections گزینه تنظیم سرور HTTP را انتخاب کنید، این عملیات می‌تواند در هنگام نصب انجام شود به جای اینکه در بعد از عملیات نصب انجام شود. برای تنظیم سرور IBM HTTP برای رمزگذاری ارتباطات، مراحل زیر را دنبال کنید:

۱. یک فایل کلید بسازید.

a. یک رابط کاربری iKeyman را آغاز کنید. برای اطلاعات بیشتر، آدرس زیر (آغاز کردن برنامه مدیریت کلید) را در مرکز اطلاعات سرور IBM HTTP ببینید.
http://www.ibm.com/support/knowledgecenter/SSAW57_8.0.0/com.ibm.websphere.ihs.doc/info/ihs/ihs/tihs_keymangui.html

b. بر روی Key Database File در رابط کاربری اصلی کلیک کنید، سپس بر روی New کلیک کنید. بر روی CMS برای نوع کلید، کلیک کنید. سرور IBM HTTP انواع دیگر پایگاه‌های داده را به جز CMS پشتیبانی نمی‌کند.

c. نام فایل کلید جدید را وارد کنید. برای مثال، hostname-key.kdb. بر روی OK کلیک کنید.

توجه: فایل پیش‌فرض Plugin-key.kdb را overwrite نکنید زیرا امکان دارد این فایل توسط نرم‌افزارهای دیگر در حال استفاده باشد.

[۱] Certificate Authority


مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها 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: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

d. در کادر Password Prompt، کلمه عبور را وارد کرده و سپس کلمه عبور را تأیید کنید. Stash the password to a file را انتخاب کنید و سپس بر روی OK کلیک کنید. پایگاه داده کلید جدید باید در نرم‌افزار iKeyman نمایش داده شود.

۲. یک گواهی‌نامه خود-امضا بسازید.

a. در کادر پایگاه داده کلید بر روی Personal Certificates کلیک کرده و سپس بر روی New Self-Signed کلیک کنید.

b. اطلاعات مورد نیاز را در ارتباط با فایل کلید، سرور وب و سازمان خودتان را در کادر مربوطه وارد کنید.

c. بر روی OK کلیک کنید.

۳. سرور IBM HTTP را متوقف کنید.

۴. در کنسول مدیریتی وارد شوید و Servers > Server types > Web servers را انتخاب کنید.

۵. از لیست سرورهای وب، بر روی وب سروری که برای این مشخصات تعیین کردید، کلیک کنید.

۶. در صفحه تنظیمات این وب سرور، بر روی لینک Configuration file کلیک کنید. این عمل، فایل تنظیمات httpd.conf بر روی Deployment Manager را باز می‌کند.

۷. متنی که در ادامه می‌آید را به انتهای فایل تنظیمات اضافه کنید:

```
LoadModule ibm_ssl_module modules/mod_ibm_ssl.so
<IfModule mod_ibm_ssl.c>
Listen 0.0.0.0:443
<VirtualHost *:443>
ServerName server_name
SSLEnable
</VirtualHost>
</IfModule>
SSLDisable
Keyfile "path_to_key_file"
SSLStashFile "path_to_stash_file"
```

که:

- server_name نام میزبان سرور IBM HTTP است.
- path_to_key_file مسیری است به فایل کلید که شما توسط نرم‌افزار iKeyman ساخته‌اید.
- path_to_stash_file مسیری است به فایل ذخیره مربوطه

برای مثال:

- AIX®:
  - Keyfile "/usr/IBM/keyfiles/*key_file*.kdb"
  - SSLStashFile "/usr/IBM/keyfiles/*key_file*.sth"
- Linux:
  - Keyfile "/opt/IBM/keyfiles/*key_file*.kdb"
  - SSLStashFile "/opt/IBM/keyfiles/*key_file*.sth"


مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها 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: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

- Microsoft Windows:

در ویندوز از ’/‘ (اسلش) در فایل httpd.conf استفاده کنید.

  - Keyfile "C:/IBM/keyfiles/*key_file*.kdb"
  - SSLStashFile "C:/IBM/keyfiles/*key_file*.sth"

که key_file نامی است که برای فایل کلید و فایل ذخیره انتخاب کردید.

۸. بر روی Apply کلیک کرده و سپس بر روی OK کلیک کنید.
۹. برای اعمال تغییرات، سرور IBM HTTP را راه‌اندازی مجدد کنید.
۱۰. تنظیمات جدید را امتحان کنید: یک صفحه مرورگر باز کنید و مطمئن شوید که به صورت موفقیت‌آمیز به https://server_name دسترسی دارید. ممکن است از شما خواسته شود تا گواهی‌نامه خود-امضا را در مرورگر خود تأیید کنید.

# ۳ پیکربندی امن پروتکل SSL/TLS

در این بخش چگونگی پیکربندی امن SSL/TLS را در سرویس‌دهنده وب WebSphere بیان می‌کنیم. مواردی همچون استثنا کردن برخی الگوریتم‌های رمز به منظور کاهش حملاتی شبیه به FREAK، CRIME و LogJAM، غیرفعال سازی نسخه‌های ناامن SSL، برقرار کردن رمزنگاری‌های قوی که از (FS) Forward Secrecy پشتیبانی می‌کنند و فعال سازی HSTS را بیان می‌کنیم.

برای بررسی وضعیت امنیتی پروتکل SSL/TLS سرویس‌دهنده 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

## ۳–۱ غیرفعال سازی SSLv2 و SSLv3

SSLv2 و SSLv3 (به خاطر حمله POODLE) ناامن هستند و باید غیرفعال شوند. برای غیرفعال سازی آنها، مراحل زیر را انجام می‌دهیم:

**توجه:** این تنظیمات در نسخه‌های 8.5.5.x، 8.5.0.x، 8.0.0.x و 7.0.0.x قابل انجام است.

**توجه:** پورت پیش‌فرض پروتکل HTTP، 9060 است و پورت پیش‌فرض پروتکل HTTPS، 9043 است.

۱. ابتدا به صورت زیر وارد کنسول مدیریتی WebSphere شوید:

الف. در Linux، AIX، IBM i و Developer

- `http://yourserver:9060/ibm/console`
- `https://yourserver:9043/ibm/console`

ب. در Windows

Start > All Programs > IBM WebSphere > Application Server v8.0 > Administrative Console

۲. به مسیر زیر بروید:

Security > SSL certificate and key management > SSL configurations

۳. مجموعه‌ای از همه پیکربندی‌های SSL لیست شده است که برای هر کدام از آنها نیاز است تا پروتکل SSL آن را به TLS تغییر دهیم.

۴. یک پیکربندی SSL را انتخاب کنید و سپس روی Quality of protection (QoP) settings در قسمت Additional Properties واقع در سمت راست کلیک کنید.

۵. در پنل Quality of protection (QoP) settings، گزینه TLS را از قسمت Protocol انتخاب کنید.

۶. در انتها، روی Apply و سپس Save کلیک کنید.



مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها 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: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir

## ۳–۲ غیرفعال سازی الگوریتم‌های رمزنگاری ضعیف

Forward Secrecy اطمینان می‌دهد که صحت[۱] یک کلید جلسه[۲] حتی وقتی که کلیدهای زیادی مورد مخاطره قرار گرفتند، حفظ می‌شود. FS کامل[۳] این مورد را با استخراج یک کلید جدید برای هر جلسه، به انجام می‌رساند. این بدان معناست که زمانی که کلید خصوصی به مخاطره افتاد، نمی‌تواند برای رمزگشایی ترافیک SSL مورد استفاده قرار گیرد.

پیشنهاد می‌شود مراحل زیر را را برای استفاده از الگوریتم‌های رمزنگاری قوی و غیرفعال سازی رمزنگاری‌های ضعیف، انجام دهید.

در کنسول مدیریتی WebSphere، شما می‌توانید همه پیکربندی‌های SSL را برای WebSphere انجام دهید.

۱. وارد کنسول مدیریتی شوید.
۲. به قسمت Security بروید.
۳. به مسیر زیر بروید:

SSL certificate and key management > SSL configurations > NodeDefaultSSLSettings > Quality of protection (QoP)

۴. در این قسمت می‌توانید الگوریتم‌های رمزنگاری ضعیف و آسیب‌پذیر را حذف کنید. به عنوان مثال می‌توانید با انتخاب الگوریتم‌های رمزنگاری *RC4* و سپس کلیک روی دکمه Remove، آنها را حذف کنید.
۵. در انتها روی دکمه Apply و سپس Save کلیک کنید.

## ۳–۳ اضافه کردن سرآیند HSTS

در صورت امکان شما باید ویژگی HSTS[۴] را فعال کنید برای اینکه مرورگرها فقط با پروتکل HTTPS بتوانند با سایت شما ارتباط برقرار کنند.

برای فعال سازی HSTS باید مراحل زیر را انجام دهید:

۱. ابتدا ماژول mod_headers را جهت افزودن قابلیت دستکاری در سرآیند[۵]ها فعال کنید.

در فایل httpd.conf دستور Load Module را برای ماژول mod_hedears فعال کنید.

```
LoadModule headers_module modules/mod_headers.so
```

۲. سیاست HSTS را برای مشتریان تعریف کنید.

تغییرات زیر را برای فایل httpd.conf اعمال کنید.

---

[۱] Integrity
[۲] Session Key
[۳] Perfect Forward Secrecy
[۴] HTTP Strict Transport Security
[۵] Header

a. سرآیند مناسب را اضافه کنید.

برای مثال Header ای که در ادامه می‌آید، انتخاب‌های مفید را برای تعیین کردن سیاست HSTS شما مشخص می‌کند. این دستور، مشخص می‌کند که سرور همیشه به ارتباطات HTTPS نیاز دارد. ارتباطات HTTPS بر روی دامنه و تمامی زیردامنه‌ها اعمال می‌شود.

```
Header always set Strict-Transport-Security "max-age=31536000;
includeSubDomains; preload
```

b. دستور header را به هر بخش میزبان مجازی (<virtualhost>) که SSL فعال است اضافه کنید.

۳. درخواست‌های میزبان‌های مجازی را که برای SSL فعال نشده‌اند، به حالت فعال تغییر دهید.

```
RewriteEngine on
RewriteRule ^/(.*) https://%{HTTP_HOST}/$1 [R,L]
```

# ۴ منابع


1. http://www.ibm.com/support/knowledgecenter/prodconn_1.0.0/com.ibm.scenarios.wmqwassecure.doc/topics/cfgssl_was.htm
2. http://www.ibm.com/support/knowledgecenter/SSYGQH_5.5.0/admin/install/t_exchange_keys_network.html
3. http://www.websphere.pe.kr/xe/was_issue/31714?ckattempt=1
4. http://www.websphere.pe.kr/xe/was_issue/31714?ckattempt=1
5. http://www.ibm.com/support/knowledgecenter/SSYGQH_5.5.0/admin/install/t_configure_ihs.html
6. http://www.ibm.com/support/knowledgecenter/SSYGQH_5.5.0/admin/install/t_exchange_keys_network.html




مرکز پژوهشی آپا (آگاهی‌رسانی، پشتیبانی، امداد برای آسیب‌پذیری‌ها 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: https://apa.aut.ac.ir - Email: autcert@aut.ac.ir