ManageEngine
ADAudit Plus

Prosty przewodnik krok po kroku do **konfiguracji SSL**

Spis treści

Wprowadzenie:

W celu zabezpieczenia komunikacji pomiędzy przeglądarkami internetowymi użytkowników a serwerem ADAudit Plus, należy zabezpieczyć połączenie między tymi dwoma elementami.

Protokół Secure Sockets Layer (SSL) to standardowe rozwiązanie internetowe pozwalające tworzyć zakodowane łącze pomiędzy serwerem a przeglądarką internetową. Pozwala to zapewnić bezpieczeństwo wszystkich danych przesyłanych pomiędzy serwerem a przeglądarką.

Włączanie protokołu SSL krok po kroku:

Opisujemy krok po kroku, jak włączyć SSL w ADAudit Plus:

KROK - 1

Określ port SSL

Zaloguj się do serwera ADAudit Plus z poziomu konta z uprawnieniami administratora

Przejdź do obszaru **Admin > General Settings > Connection.**

Włącz protokół SSL, zaznaczając odpowiednie pole, następnie wpisz numer portu [domyślnie: 8444], którego chcesz użyć w ADAudit Plus, a następnie zapisz zmiany.

A teraz wstrzymaj ADAudit Plus, przechodząc do obszaru **Start > All Programs > ADAudit Plus > Stop ADAudit Plus.**

KROK - 2

Utwórz element Keystore

Element Keystore to plik chroniony hasłem zawierający wszystkie klucze, które serwer wykorzysta w celu realizacji transakcji SSL.

- Aby utworzyć plik Keystore certyfikatu z poziomu <installation directory> \ jre \bin, wykonaj następujące polecenie z wiersza polecenia:

```
keytool -genkey -aliastomcat -keypass <your key password> -keyalg RSA -validity 1000
-keystore <domainName> .keystore
```

Podaj informacje na podstawie następujących wytycznych:

Imię i nazwisko?	**Nazwa NetBIOS** (jeśli nazwa domeny DNS to test.example.com, nazwa domeny NetBIOS to test) lub **nazwa FQDN** (nazwa FQDN teoretycznego serwera poczty może brzmieć mymail.example.com. Nazwa hosta to mymail, a jego lokalizacja to domainexample.com) **serwera, na którym zainstalowano ADAudit Plus.**
Jak nazywa się Jednostka organizacyjna?	Nazwa oddziału, która ma się pojawić na certyfikacie.
Jak nazywa się Twoja organizacja?	Podaj nazwę prawną organizacji.
Jak nazywa się Twoje miasto?	Podaj nazwę miasta podaną w adresie siedziby organizacji.
Jak nazywa się Twój region/ Twoje województwo?	Podaj nazwę regionu/województwa podaną w adresie siedziby organizacji.
Jaki jest kod Twojego kraju?	Podaj dwucyfrowy kod kraju, w którym znajduje się Twoja organizacja.
Hasło	Podaj hasło składające się z co najmniej 6 znaków.

KROK - 3

Wygeneruj Żądanie podpisania certyfikatu (CSR) i wyślij je do swojego Urzędu certyfikacji

1. Generowanie Certificate Signing Request (CSR)

A. Aby wygenerować plik csr (Certificate Signing Request — Żądanie podpisania certyfikatu) z **<installation directory> \ jre \ bin**, wykonaj następujące polecenie z wiersza polecenia:

```
keytool -certreq -alias  tomcat -keyalg RSA -keystore  .keystore -file  .csr
```

(lub)

B. Aby wygenerować Żądanie podpisania certyfikatu (CSR) z wykorzystaniem Alternatywnej nazwy podmiotu (Subject Alternative Name — SAN), wykonaj następujące polecenie z wiersza polecenia:

```
keytool -certreq -alias tomcat -keyalg RSA -ext
SAN=dns:server_name,dns:server_name.domain.com,dns:server_name.domain1.com
-keystore .keystore -file .csr
```

2. Prześlij plik CSR do swojego Urzędu certyfikacji (CA). Do pliku CSR prowadzi ścieżka <install_dir>\ADAudit Plus\jre\bin

KROK - 4

Dodaj podpisany przez Urząd certyfikacji certyfikat do Keystore

- Wypakuj certyfikaty odesłane przez Twój Urząd certyfikacji i umieść je w folderze <install_dir>/jre/bin
- Otwórz wiersz poleceń i przejdź do folderu <install_dir>/jre/bin
- A teraz wykonaj odpowiednie polecenia z poniższej listy odnoszące się do danego Urzędu certyfikacji:

Dla certyfikatów GoDaddy

i. keytool -import -alias root -keystore <domainName>.keystore -trustcacerts -file gd_bundle.crt

ii. keytool -import -alias cross -keystore <domainName>.keystore -trustcacerts -file gd_cross.crt

iii. keytool -import -alias intermed -keystore <domainName>.keystore -trustcacerts -file gd_intermed.crt

iv. keytool -import -alias tomcat -keystore <domainName>.keystore -trustcacerts -file <domainName>.crt

Dla certyfikatów Verisign

i. keytool -import -alias intermediateCA -keystore <domainName>.keystore -trustcacerts -file < your intermediate certificate.cer>

ii. keytool -import -alias tomcat -keystore <domainName>.keystore -trustcacerts -file <domainName>.cer

Dla certyfikatów Comodo

i. keytool -import -trustcacerts -alias root -file AddTrustExternalCARoot.crt -keystore <domainName>.keystore

ii. keytool -import -trustcacerts -alias addtrust -file UTNAddTrustServerCA.crt -keystore <domainName>.keystore

iii. keytool -import -trustcacerts -alias ComodoUTNServer -file ComodoUTNServerCA.crt - keystore <domainName>.keystore

iv. keytool -import -trustcacerts -alias essentialSSL -file essentialSSLCA.crt -keystore <domainName>.keystore

Dla certyfikatów Entrust

i. keytool -import -alias Entrust_L1C -keystore <keystore-name.keystore> -trustcacerts -file entrust_root.cer

ii. keytool -import -alias Entrust_2048_chain -keystore <keystore-name.keystore> -trustcacerts -file entrust_2048_ssl.cer

iii. keytool -import -alias -keystore <keystore-name.keystore> -trustcacerts -file <domain-name.cer>

Dla certyfikatów Thawte

Zakupionych bezpośrednio od Thawte

i. keytool -import -trustcacerts -alias tomcat -file <certificate-name.p7b> -keystore <keystore-name.keystore>

Zakupionych poprzez kanał sprzedaży Thawte:

i. keytool -import -trustcacerts -alias thawteca -file <SSL_PrimaryCA.cer> -keystore <keystore-name.keystore>

ii. keytool -import -trustcacerts -alias thawtecasec -file <SSL_SecondaryCA.cer> -keystore <keystore-name.keystore>

iii. keytool -import -trustcacerts -alias tomcat -file <certificate-name.cer> -keystore <keystore-name.keystore>

Dla certyfikatów z własnym podpisem (wewnętrzny Urząd certyfikacji):

Keytool –import –trustcacerts –alias tomcat –file certnew.p7b –keystore <keystore_name >.keystore

Uwaga: Jeśli otrzymasz certyfikat od Urzędu certyfikacji, który nie występuje na powyższej liście, skontaktuj się ze swoim Urzędem certyfikacji, aby uzyskać polecenia wymagane do dodania ich certyfikatów do elementu Keystore.

KROK - 5

Przypnij certyfikaty do ADAudit Plus

- kopiuj plik **<domainName>.keystore** z foldera **<install_dir>\jre\bin** i wklej go do folderu **<install_dir>\conf** folder
- Otwórz plik „**server.xml**" znajdujący się w folderze **<install_dir>\conf** folder
- Zmień wartość pliku **keystore** na „**./conf/<domainName>.keystore**", a hasło do **keystore** na hasło użyte w kroku 1.
- Zapisz plik „**server.xml**" i zamknij go
- Uruchom ponownie **ADAudit Plus,** aby zmiany zostały zastosowane.

Etapy instalacji istniejącego certyfikatu PFX/PKCS12 lub certyfikatu z wieloznaczną nazwą krok po kroku

Poniżej podano instrukcję korzystania z aktualnego certyfikatu PFX/PKCS12 lub certyfikatu z wieloznaczną nazwą podczas włączania protokołu SSL w ADAudit Plus.

KROK - 1

Określ port SSL

- Zaloguj się do ADAudit Plus z poziomu konta z uprawnieniami administratora. Przejdź do **Admin >General Settings > Connection.**
- Włącz protokół SSL, zaznaczając odpowiednie pole, następnie wpisz numer portu [domyślnie: 8444], którego chcesz użyć w ADAudit Plus, a następnie zapisz zmiany.
- A teraz wstrzymaj ADAudit Plus, przechodząc do **Start > All Programs > ADAudit Plus > Stop ADAudit Plus.**

KROK - 2

Eksportuj plik z certyfikatem PFX/PKCS12

- Eksportuj i zapisz swój plik PFX/PKCS12 w folderze **<installation_dir>\conf** (Domyślnie: C:\ManageEngine\ ADAudit Plus\ conf).

KROK - 3

Edytuj plik server.xml, uwzględniając certyfikat z wieloznaczną nazwą

- Otwórz plik „server.xml" umieszczony w folderze **<installation_dir>\conf** w edytorze tekstu lokalnego.
  (Zadbaj o utworzenie kopii zapasowej istniejącego pliku server.xml na wypadek, gdybyś zechciał go przywrócić).
- Przejdź na koniec pliku XML, przyjrzyj się znacznikowi łącznika **<Connector SSLEnabled="true"** ...../> i edytuj następujące wartości (uwzględniając wielkość liter) znacznika łącznika.

  keystoreFile="./conf/"

  keystorePass=" "

  keystoreType="PKCS12"

Na przykład: <Connector SSLEnabled="true" acceptCount="100" clientAuth="false" connectionTimeout="20000" debug="0" disableUploadTimeout="true" enableLookups="false" **keystoreFile=**"./conf/YOUR_CERT_FILE.pfx" **keystorePass=**"PASSWORD" **keystoreType=**"PKCS12" maxSpareThreads="75" maxThreads="150" minSpareThreads="25" name="SSL" port="443" scheme="https" secure="true" sslProtocol="TLS"/>

KROK - 4

Uruchom ADAudit Plus.

Glosariusz:

Co to takiego SSL?

Secure Socket Layer, w skrócie SSL, to technologia szyfrowania pozwalająca zabezpieczać przesył danych pomiędzy witryną a przeglądarką użytkownika odwiedzającego witrynę. Zazwyczaj, gdy użytkownik nawiązuje łączność z witryną i przekazuje informacje dotyczące swojej karty kredytowej, dane te są przesyłane do serwera jako zwykły tekst, przez co są narażone na kradzież danych. Z kolei dzięki szyfrowaniu, dane te nie mogą zostać odczytane, gdy wpadną w niepowołane ręce. Dlatego tak ważne jest zabezpieczenie witryny protokołem SSL.

Certyfikat SSL:

To tożsamość cyfrowa firmy, która stanowi gwarancję, że odwiedzający komunikuje się wyłącznie z docelową witryną, a wszelkie dane, jakie przesyła do witryny, są kodowane i docierają wyłącznie do niej. System działa analogicznie do systemów bankowych pozwalających rozpoznawać klientów po podpisie. W tym przypadku, przeglądarki (a tym samym także użytkownicy końcowi) są zaprogramowane tak, by akceptować świadectwa Urzędów certyfikacji (CA) jako wiarygodne źródła certyfikacji.

Urząd certyfikacji:

Organizacja regulacyjna, która w oparciu o standardowe polityki wydaje certyfikaty domenie o dowiedzionej wiarygodności. Każdy wygenerowany przez nią certyfikat jest wydawany wyłącznie dla danej certyfikowanej firmy, dzięki czemu łatwo go odnaleźć.

Urząd certyfikacji zabezpiecza wszystkie niezbędne informacje o firmie przed wydaniem certyfikatu oraz aktualizuje dane, co podnosi wiarygodność całego procesu. Do najbardziej znanych Urzędów certyfikacji należą Verisign, Comodo, GoDaddy itd.

CSR:

Aby Urząd certyfikacji mógł wygenerować certyfikat SSL dla firmy, w pierwszej kolejności gromadzi informacje na temat tego podmiotu oraz inne dane identyfikujące, takie jak klucz publiczny (podpis cyfrowy), a następnie przypina je wszystkie do certyfikatu. Tym samym generuje unikatowy identyfikator firmy. Dlatego za każdym razem proces wydawania certyfikatu rozpoczyna się od „żądania certyfikatu" ze strony firmy. Urzędy certyfikacji określają ten proces mianem Żądania podpisania certyfikatu (CSR). Urzędy certyfikacji zatwierdzają informacje oraz cyfrowe podpisy firm w pliku o specjalnym formacie, zwanym csr.