

Un guide simple, étape
par étape pour la
configuration SSL



Table des matières

Introduction	1
Étapes à suivre pour activer le SSL	1
Étape 1	
Définition du port SSL	1
Étape 2	
Créer le Keystore	2
Étape 3	
Générer un CSR (Certificate Signing Request)	3
Étape 4	
Délivrer le certificat SSL	4
• A. Délivrer le certificat SSL en utilisant un CA externe	4
• B. Délivrer le certificat SSL en utilisant un CA interne	4
Étape 5	
Importer le certificat	6
• A. Format PEM (Privacy-Enhanced Mail)	6
• B. Format P7B ou PKCS	8
• C. Format PFX or PKCS	8
Étape 6	
Liez les certificats à ADAudit Plus	9

Introduction

Pour sécuriser la communication entre les navigateurs web des utilisateurs et le serveur ADAudit Plus, la connexion entre ces deux entités doit être sécurisée.

Le protocole SSL (Secure Sockets Layer) est la norme standard sur le web pour établir un lien chiffré entre un serveur et un navigateur web. Il garantit que toutes les données transférées entre le serveur et le navigateur restent sécurisées.

Étapes à suivre pour activer le SSL

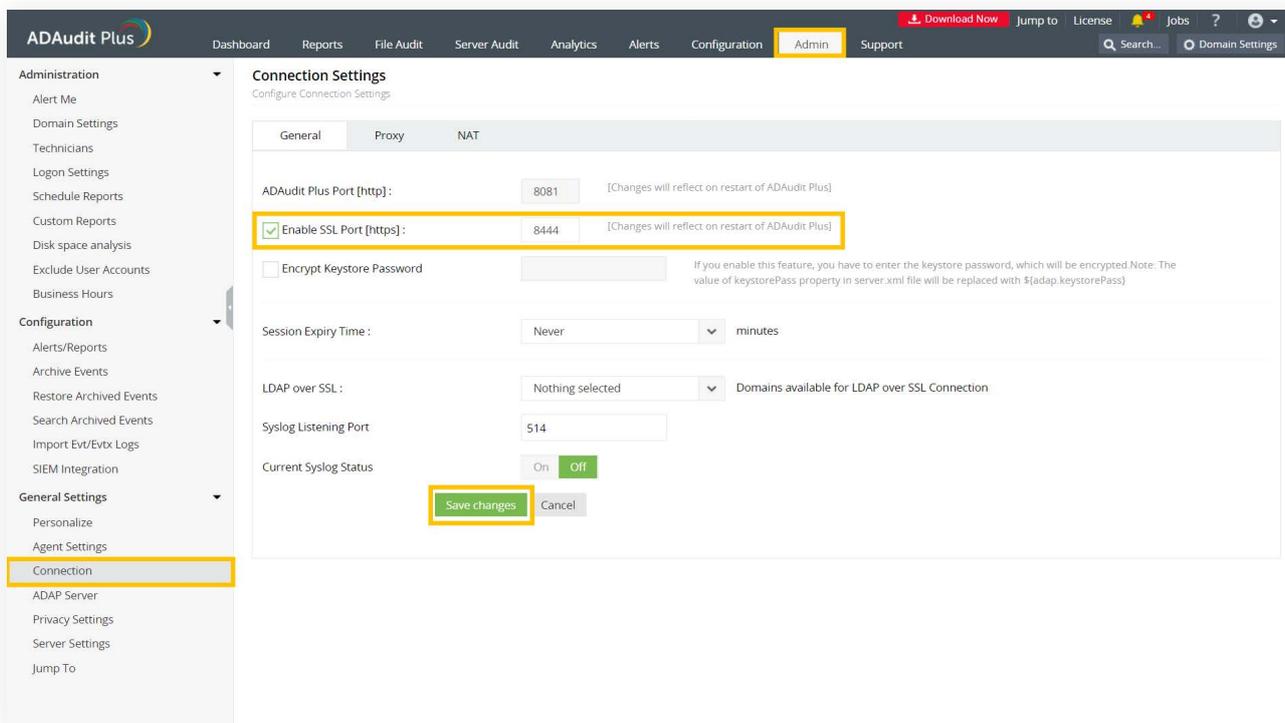
Les étapes suivantes vous guideront dans l'activation du SSL dans ADAudit Plus.

ÉTAPE- 1

Définir le port SSL

- Ouvrez une session dans ADAudit Plus avec un compte qui a des privilèges administrateur.
- **Accédez à Admin > General Settings > Connection.**
- Cochez la case **Enable SSL Port [https]**. Le numéro de port par défaut 8444 est sélectionné automatiquement.
- Cliquez sur **Save changes**.
- Redémarrez ADAudit Plus pour que les changements prennent effet.

Note: Si vous voulez installer un certificat **PFX or PKCS #12 existant**, passez à la section [PFX or PKCS #12 format section de l'étape 5](#).



The screenshot shows the ADAudit Plus Admin interface. The top navigation bar includes 'Dashboard', 'Reports', 'File Audit', 'Server Audit', 'Analytics', 'Alerts', 'Configuration', 'Admin', and 'Support'. The 'Admin' menu is expanded, showing 'Administration' and 'Configuration'. Under 'Administration', 'Connection' is selected. The 'Connection Settings' page is displayed, with the 'General' tab active. The 'Enable SSL Port [https]' checkbox is checked, and the port number is 8444. The 'Save changes' button is highlighted with a green box.

ÉTAPE 2

Créer le Keystore

Un Keystore est un fichier protégé par un mot de passe qui contient toutes les clés que le serveur utilisera pour les transactions SSL.

- Pour créer un fichier Keystore et générer des clés de chiffrement, exécutez l'**invite de commandes** en tant qu'administrateur, accédez à <product_installation_directory>\jre\bin, et exécutez la commande suivante :

```
keytool -genkey -alias tomcat -keyalg RSA -validity 1000 -keystore <domainName>.keystore
```

- Remplacez <domainName> par le nom de votre domaine.
- Saisissez le mot de passe de votre Keystore.
- Fournissez des informations basées sur les directives suivantes

What is your first and last name?	Fournissez le nom de la machine ou le nom de domaine complet du serveur hébergeant ADAudit Plus.
What is the name of your organizational unit?	Entrez le nom du service que vous voulez voir apparaître dans la certification.
What is the name of your organization?	Indiquez le nom légal de votre entreprise.
What is the name of your City or Locality?	Entrez le nom de la ville tel qu'indiqué dans l'adresse enregistrée de votre entreprise.
What is the name of your State or Province?	Entrez l'état tel qu'indiqué dans l'adresse enregistrée de votre entreprise.
What is the two-letter country code for this unit?	Indiquez le code à deux lettres du pays dans lequel votre entreprise est située.
Enter key password for <tomcat>	Saisissez le même mot de passe que celui du Keystore. Note: si vous choisissez d'entrer un mot de passe différent, notez-le car le mot de passe de la clé sera requis ultérieurement.

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19043.1165]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd C:\Program Files (x86)\ManageEngine\ADAudit Plus\jre\bin

C:\Program Files (x86)\ManageEngine\ADAudit Plus\jre\bin>keytool -genkey -alias tomcat -keyalg RSA -validity 1000 -keystore
adauditplus.keystore
Enter keystore password:
Re-enter new password:
What is your first and last name?
[Unknown]: ADAudit Plus'
What is the name of your organizational unit?
[Unknown]: ADAudit Plus OU
What is the name of your organization?
[Unknown]: ADAudit Plus
What is the name of your City or Locality?
[Unknown]:
What is the name of your State or Province?
[Unknown]:
What is the two-letter country code for this unit?
[Unknown]:
Is CN=ADAudit Plus', OU=ADAudit Plus OU, O=ADAudit Plus, L= , ST= , C= correct?
[no]: yes

Enter key password for <tomcat>
(RETURN if same as keystore password):

C:\Program Files (x86)\ManageEngine\ADAudit Plus\jre\bin>
```

ÉTAPE- 3

Générer le CSR (Certificate Signing Request)

- Pour créer un CSR avec un SAN (Subject Alternative Names), exécutez la commande suivante dans l'invite de commande :

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

Remplacez <domainName> par le nom de votre domaine et fournissez les SAN appropriés comme indiqué dans l'image ci-dessous :

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19041.985]
(c) Microsoft Corporation. All rights reserved.

C:\WINDOWS\system32>cd C:\Program Files (x86)\ManageEngine\ADAudit Plus\jre\bin

C:\Program Files (x86)\ManageEngine\ADAudit Plus\jre\bin>keytool -certreq -alias tomcat -keyalg RSA
-keystore adauditplus.keystore -file adauditplus.csr
Enter keystore password:
Enter key password for <tomcat>

C:\Program Files (x86)\ManageEngine\ADAudit Plus\jre\bin>
```

ÉTAPE- 4

Délivrer le certificat SSL

Dans cette étape, vous vous connecterez à un CA (Certificate Authority), soumettez le CSR à la CA spécifique et obtiendrez le certificat SSL.

A. Délivrer le certificat SSL en utilisant un CA externe

- Pour demander un certificat à un CA externe, soumettez le CSR à ce CA. Vous pouvez trouver le fichier CSR dans le dossier <product_installation_directory>\jre\bin.
- Décompressez les certificats renvoyés par votre CA et placez-les dans le dossier <product_installation_directory>\jre\bin folder.

Note: Une fois le certificat SSL émis par le CA externe, passez à l'[Étape 5](#) pour installer le certificat.

B. Délivrer le certificat SSL en utilisant un CA interne

Un CA interne est un serveur membre ou un contrôleur de domaine dans un domaine spécifique qui s'est vu attribuer le rôle de CA.

- Connectez-vous aux **Microsoft Active Directory Certificate Services** de votre CA interne et cliquez sur le lien **Request a certificate**.

Microsoft Active Directory Certificate Services -- Home

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Active Directory Certificate Services, see [Active Directory Certificate Services Documentation](#).

Select a task:

- [Request a certificate](#)
- [View the status of a pending certificate request](#)
- [Download a CA certificate, certificate chain, or CRL](#)

- Sur la page Request a Certificate, cliquez sur le lien **advanced certificate request**.

Microsoft Active Directory Certificate Services -- Home

Request a Certificate

Select the certificate type:

- [User Certificate](#)

Or, submit an [advanced certificate request](#).

- Sur la page Submit a Certificate Request or Renewal Request, copiez le contenu de votre fichier CSR et collez-le dans le champ **Saved Request**
- Sélectionnez **Web Server** ou le modèle approprié pour Tomcat sous **Certificate Template** et cliquez sur **Submit**.

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
BgNVHQ4EFgQUTfNK/8W5WwNdtJ8IdE1zdZm2f2Qw
CIuKRY2CexoJxWJTnzJqNIxHVSeqZ880b7u8QWbN
xTZn/U/g+yn3tz890wvmfODHLrV6GuHFYd5S7n58
VLQzFOk0HPun6X18X4bNQG3qj6+PoHQz1asfjp3H
crRBFwUqzDCz0xinY+yLj9s3uHX+4FeCrLV4dVBN
7Xy8K+716tQKVLTTGICdnMLGvGk=
```

Certificate Template:

Web Server

Additional Attributes:

Attributes:

Submit >

- Le certificat sera émis lorsque vous cliquerez sur le lien **Download certificate chain**. Le certificat téléchargé sera au format de fichier P7B.

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded

 [Download certificate](#)
[Download certificate chain](#)

Downloads window: certnew.p7b

- Copiez le fichier P7B dans le dossier <product_installation_directory>\jre\bin.

Importer le certificat

Suivez les étapes indiquées ci-dessous qui correspondent au format dans lequel vous souhaitez importer le certificat.

A. Format PEM (Privacy-Enhanced Mail)

Pour importer le certificat dans le fichier Keystore au format PEM, ouvrez l'invite de commandes, naviguez dans <product_installation_directory>\jre\bin, et exécutez les commandes de la liste ci-dessous qui s'applique à votre CA.

Commandes générales

- `keytool -importcert -alias root -file <root.cert.pem> -keystore <your.domain.com>.keystore -trustcacerts`
- `keytool -importcert -alias intermediate -file <intermediate.cert.pem> -keystore <your.domain.com>.keystore -trustcacerts`
- `keytool -importcert -alias intermediat2 -file <intermediat2.cert.pem> -keystore <your.domain.com>.keystore -trustcacerts`
- `keytool -importcert -alias tomcat -file <server.cert.pem> -keystore <your.domain.com>.keystore -trustcacerts`

Commandes spécifiques au fournisseur

Pour les certificats GoDaddy

- `keytool -import -alias root -keystore <domainName>.keystore -trustcacerts -file gd_bundle.crt`
- `keytool -import -alias cross -keystore <domainName>.keystore -trustcacerts -file gd_cross.crt`
- `keytool -import -alias intermed -keystore <domainName>.keystore -trustcacerts -file gd_intermed.crt`
- `keytool -import -alias tomcat -keystore <domainName>.keystore -trustcacerts -file <domainName>.crt`

Pour les certificats Verisign

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

Pour les certificats Comodo

- `keytool -import -trustcacerts -alias root -file AddTrustExternalCARoot.crt -keystore <domainName>.keystore`
- `keytool -import -trustcacerts -alias addtrust -file UTNAddTrustServerCA.crt -keystore <domainName>.keystore`
- `keytool -import -trustcacerts -alias ComodoUTNServer -file ComodoUTNServerCA.crt -keystore <domainName>.keystore`
- `keytool -import -trustcacerts -alias essentialSSL -file essentialSSLCA.crt -keystore <domainName>.keystore`

Pour les certificats Entrust

- `keytool -import -alias Entrust_L1C -keystore <keystore-name.keystore> -trustcacerts -file entrust_root.cer`
- `keytool -import -alias Entrust_2048_chain -keystore <keystore-name.keystore> -trustcacerts -file entrust_2048_ssl.cer`
- `keytool -import -alias -keystore <keystore-name.keystore> -trustcacerts -file <domainName.cer>`

Pour les certificats achetés par le canal des revendeurs Thawte

- `keytool -import -trustcacerts -alias thawteca -file <SSL_PrimaryCA.cer> -keystore <keystore-name.keystore>`
- `keytool -import -trustcacerts -alias thawtecasec -file <SSL_SecondaryCA.cer> -keystore <keystore-name.keystore>`
- `keytool -import -trustcacerts -alias tomcat -file <certificate-name.cer> -keystore <keystore-name.keystore>`

Une fois le certificat installé, passez à l'[Étape 6](#) pour lier le certificat à ADAudit Plus.

Note: Si vous recevez les certificats d'un CA qui n'est pas énuméré ci-dessus, alors contactez votre CA pour obtenir les commandes requises pour ajouter ses certificats au Keystore.

B. Format P7B or PKCS

Pour importer le certificat dans le fichier Keystore au format P7B ou PKCS, ouvrez l'invite de commandes, naviguez vers `<product_installation_directory>\jre\bin`, et exécutez la commande suivante :

```
keytool -import -trustcacerts -alias tomcat -file certnew.p7b -keystore <keystore_name>.keystore
```

Une fois le certificat installé, passez à l'[étape 6](#) pour lier le certificat à ADAudit Plus.

C. Format PFX ou PKCS

Pour importer le certificat dans le fichier Keystore au format P7B ou PKCS, ouvrez l'invite de commandes, naviguez vers `<product_installation_directory>\jre\bin`, et exécutez la commande suivante :

- Copiez et enregistrez votre fichier PFX ou PKCS dans le dossier `<product_installation_directory>\conf.f` folder.
- Ouvrez le fichier `server.xml` présent dans le dossier `<product_installation_directory>\conf` avec un éditeur de texte local. Créez une sauvegarde du fichier `server.xml` existant au cas où vous souhaiteriez le restaurer.
- Accédez à la fin du fichier `server.xml` et recherchez les balises qui contiennent `<Connector ... SSLEnabled="true"/>`.
- Modifiez les valeurs suivantes (qui sont sensibles à la casse) dans les balises, sans apporter de modifications aux autres valeurs.
 - Remplacer les valeurs du `keystoreFile` avec `"/conf/<YOUR_CERT_FILE.pfx>`.
 - Ajouter `keystoreType="PKCS12"`.
- Enregistrer et fermer le `server.xml` file.

```
<Connector SSLEnabled="true" URIEncoding="UTF-8" acceptCount="100"
ciphers="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TL
S_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WIT
H_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,TL
S_RSA_WITH_AES_256_CBC_SHA" clientAuth="false" connectionTimeout="20000" debug="0"
disableUploadTimeout="true" enableLookups="false" keystoreFile="/conf/<YOUR_CERT_FILE.pfx>"
keystorePass="*****" keystoreType="PKCS12"maxSpareThreads="75" maxThreads="150"
minSpareThreads="25" name="SSL" port="8444" scheme="https" secure="true"
sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2" sslProtocol="TLS"/>
```

Note:

Après avoir modifié le fichier `server.xml`, vous pouvez passer à la section 6.

Lier les certificats à ADAudit Plus

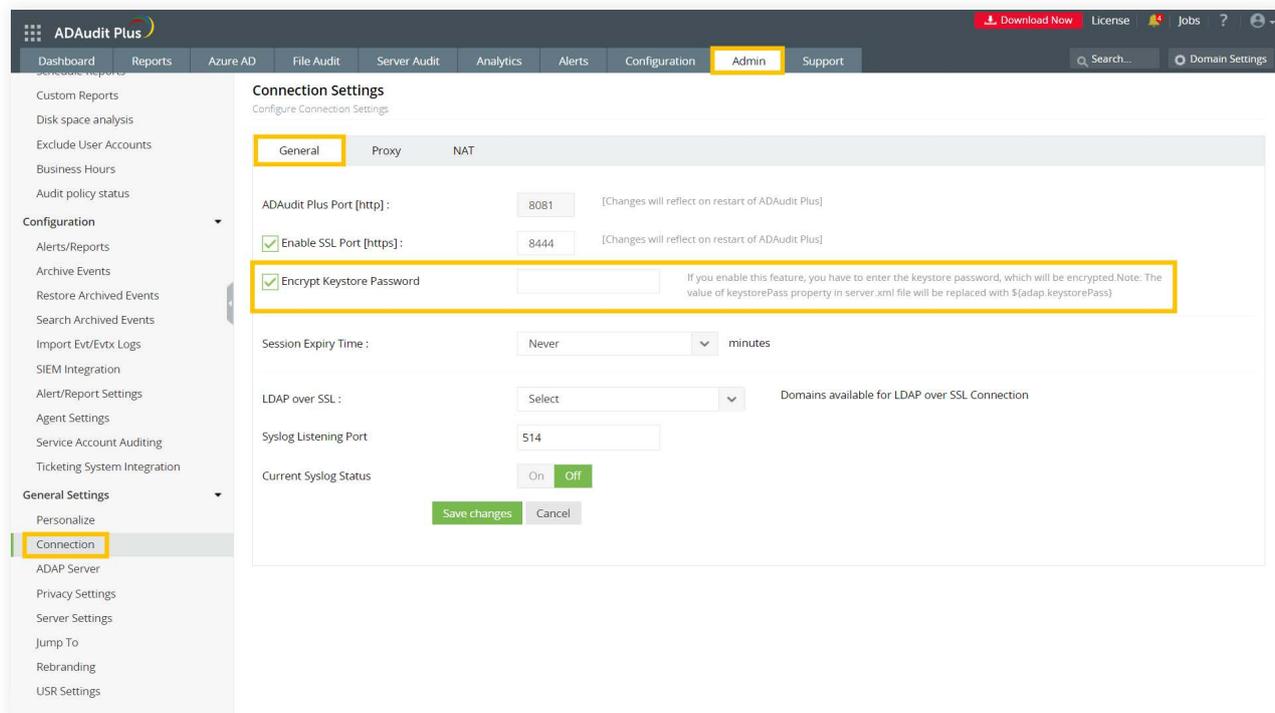
- Copiez le fichier `<domainName>.keystore` du dossier `<product_installation_directory>\jre\bin` et collez-le dans le dossier `<product_installation_directory>\conf`.
- Ouvrez le fichier `server.xml` présent dans le dossier `<product_installation_directory>\conf` avec un éditeur de texte local. Créez une sauvegarde du fichier `server.xml` existant au cas où vous souhaiteriez le restaurer.
- Accédez à la fin du fichier `server.xml` et recherchez les balises qui contiennent `<Connector ... SSLEnabled="true"/>`.
- Modifiez les valeurs suivantes (qui sont sensibles à la casse) dans les balises.

```
<Connector SSLEnabled="true" URIEncoding="UTF-8" acceptCount="100"
ciphers="TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256,TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TL
S_ECDHE_RSA_WITH_AES_256_CBC_SHA384,TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA,TLS_RSA_WIT
H_AES_128_CBC_SHA256,TLS_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_256_CBC_SHA256,TL
S_RSA_WITH_AES_256_CBC_SHA" clientAuth="false" connectionTimeout="20000" debug="0"
disableUploadTimeout="true" enableLookups="false"
keystoreFile="./conf/<Your_Domain_Name>.keystore" keystorePass="*****" m axSpareThreads="75"
maxThreads="150" minSpareThreads="25" name="SSL" port="8444" scheme="https" secure="true"
sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2" sslProtocol="TLS"/>
```

- Remplacez la valeur du `keystoreFile` par `./conf/<domainName>.keystore`.

Encrypt the keystore password

- Connectez-vous sur la console ADAudit Plus et allez à **Admin > General Settings > Connection**.
- Remplacez la valeur du `keystorePass` par le mot de passe Keystore que vous avez utilisé lors de la génération du CSR pour ce fichier.
- **Sauvegardez le fichier `server.xml` et fermez-le.**
- Redémarrez ADAudit Plus à nouveau pour que les changements prennent effet.



Glossary

■ Qu'est-ce que le SSL?

L'abréviation SSL (Secure Socket Layer) désigne une technologie de chiffrement permettant de sécuriser l'échange de données entre un site web et le navigateur web de son visiteur. Normalement, lorsqu'un utilisateur communique avec un site web, par exemple en soumettant les informations relatives à sa carte de crédit, les données sont transmises au serveur en texte clair, ce qui peut entraîner un vol de données. Alors que si ces données sont chiffrées, aucune personne malveillante ne peut les lire. Il est donc essentiel de sécuriser un site web avec le protocole SSL.

■ Certificat SSL:

Il s'agit de l'identité numérique d'une entreprise, qui garantit qu'un visiteur ne parle qu'au site web prévu et que les données qu'il soumet au site sont codées et ne parviennent qu'au site prévu. Ce système est analogue à celui des banques qui reconnaissent leurs clients par leur signature. Dans ce cas, les navigateurs (et donc les utilisateurs finaux) sont programmés pour faire confiance à ces certificats présentés par le CA (Certificate Authority).

■ Autorité de certification:

Les organismes de réglementation, à l'aide de politiques standard, délivrent des certificats à un domaine en le déclarant digne de confiance. Chaque certificat qu'ils génèrent est unique pour l'entreprise qu'ils certifient, ce qui facilite l'identification.

CAs secure all necessary information about a company before issuing a certificate and also keep their records updated, which adds to the trustworthiness. Some of the popular CAs include Verisign, Comodo & GoDaddy etc.

■ CSR

Pour qu'un CA puisse générer un certificat SSL pour une entreprise, elle recueille d'abord des informations sur cette entreprise et d'autres identifiants tels que la clé publique (signature numérique), puis elle les lie tous à son certificat. En procédant ainsi, elle génère un identifiant unique pour l'entreprise.

Chaque processus d'émission de certificat commence par une "certificate request" de la part de l'entreprise. Les autorités de certification appellent ce processus CSR (Certificate Signing Request). Les autorités de certification acceptent les informations sur l'entreprise et les signatures numériques dans un format de fichier spécial, à savoir le format .csr.

Nos produits

AD360 | Log360 | ADManager Plus | ADSelfService Plus | DataSecurity Plus | M365 Manager Plus

Vue d'ensemble d'ADAudit Plus:

[ADAudit Plus](#) est un outil d'audit des changements Active Directory en temps réel, basé sur le web, qui vous aide à :

- Suivre [toutes les modifications](#) apportées aux objets AD Windows, y compris les utilisateurs, groupes, ordinateurs, GPO et OU.
- Surveiller l'[activité d'ouverture et de fermeture de session](#), de chaque utilisateur, y compris chaque tentative d'ouverture de session réussie ou non sur les [postes de travail](#).
- Auditer [Les serveurs de fichiers Windows, clusters de basculement, Netapp](#) et [stockage EMC](#) pour documenter les modifications apportées aux fichiers et aux dossiers.
- Surveiller les configurations système, program files et changements de dossiers pour garantir l'[intégrité des fichiers](#)
- Suivez les changements sur les [serveurs Windows, imprimantes](#) et [périphériques USB](#) avec un résumé des événements

Pour en savoir plus sur la façon dont ADAudit Plus peut vous aider avec tous vos besoins d'audit Active Directory, veuillez visiter : <https://www.manageengine.fr/ada>

Obtenir une cotation

↓ Télécharger

PG Software EUROPE

commercial@pgsoftware.fr

0 805 296 540 Service & appel gratuits