ManageEngine
ADAudit Plus

A simple step-by-step guide to **SSL configuration**

www.adauditplus.com

Table of Contents

Introduction:

To secure the communication between users' web browsers and ADAudit Plus server, the connection between these two entities must be secured.

Secure Sockets Layer (SSL) is the de facto standard on the web for establishing an encrypted link between a server and a web browser. It ensures that all data transferred between the server and the browser remains secure.

Steps for enabling SSL:

The following steps will guide you through enabling SSL in ADAudit Plus:

STEP - 1

Defining the SSL port

Logon to ADAudit Plus with an account that has administrative privileges

Navigate to **Admin > General Settings > Connection.**

Enable SSL by checking the checkbox, then enter the port number [default: 8444] you plan on using for ADAudit Plus and save changes.

Now stop ADAudit Plus by navigating through **Start > All Programs > ADAudit Plus > Stop ADAudit Plus.**

STEP - 2

Create the keystore

The keystore is a password protected file that contains all the keys that the server will use for SSL transactions.

- To create the certificate keystore file, from **<installation directory> \ jre \bin,** execute the following command in the command prompt:

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

Provide information based on the following guidelines:

What is the first and last name?	**The NetBIOS** (if the DNS domain name is test.example.com, the NetBIOS domain name is test) **or FQDN name** (an FQDN for a hypothetical mail server might be mymail.example.com. The hostname is mymail, and the host is located within the domain example.com) **of the server on which ADAudit Plus is running.**
What is the name of your Organizational Unit?	The department name that you want to appear in the certification.
What is the name of your organization?	Provide the legal name of your organization.
What is the name of your city?	Enter the city name as provided in your organization's registered address.
What is the name of your state/province?	Enter the State/Province as provided in your organization's registered address.
What is your country code?	Provide the 2-letter code of the country your organization is located in.
Password	Enter a password of at least 6 characters.

STEP - 3

Generate a Certificate Signing Request (CSR) and submit it to your Certifying Authority

1. Creating a Certificate Signing Request (CSR)

A. To create a csr (Certificate Signing Request) file from the **<installation directory> \ jre \ bin,** execute the following command in the command prompt:

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

(or)

B. To create a Certificate Signing Request (CSR) with Subject Alternative Name (SAN), execute the following command in the command prompt:

```
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
```

2. Submit the CSR file to your Certifying Authority (CA). You can locate the CSR file at <install_dir>\ADAudit Plus\jre\bin

STEP - 4

Add the CA signed certificates to the keystore

- Unzip the certificates returned by your CA and put them in **<install_dir>/jre/bin** folder
- Open the command prompt and navigate to **<install_dir>/jre/bin** folder
- Now, run the respective commands from the below list as applicable to your CA:

For "GoDaddy" certificates

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

For "Verisign" certificates

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

For "Comodo" certificates

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

For Entrust certificates

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>

For Thawte certificates

Purchased directly from Thawte

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

Purchased through the Thawte reseller channel:

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>

For self signed (Internal CA) certificates:

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

Note: If you are receiving the certificates from a CA who is not in the list provided above, then contact your CA to get the commands required to add their certificates to the keystore.

STEP - 5

Bind the certificates to ADAudit Plus

- **Copy** the **<domainName>.keystore** file from **<install_dir>\jre\bin** folder and **paste** it in **<install_dir>\conf** folder
- Open '**server.xml**' file located at **<install_dir>\conf** folder
- Replace the value of **keystoreFile** with '**./conf/<domainName>.keystore**' and **keystorePass** with the **password** that you used in Step 1
- **Save** '**server.xml**' file and close it
- Restart **ADAudit Plus** again for the changes to take effect.

Steps to install an existing PFX/PKCS12 or wildcard certificate.

The following steps will guide you through using your existing PFX/ PKCS12 or wildcard certificate file while enabling SSL for ADAudit Plus.

STEP - 1

Defining the SSL port

- Logon to ADAudit Plus with an account that has administrative privileges. Navigate to **Admin > General Settings > Connection.**
- Enable SSL by checking the checkbox, then enter the port number [default: 8444] you plan on using for ADAudit Plus and save changes.
- Now stop ADAudit Plus by navigating through **Start > All Programs > ADAudit Plus > Stop ADAudit Plus.**

STEP - 2

Export the PFX/PKCS12 certificate file

- Export and save your PFX/PKCS12 file under the **<installation_dir>\conf** folder (By default: C:\ManageEngine\ ADAudit Plus\ conf).

STEP - 3

Edit the server.xml file to include the wildcard certificate

- Open the **server.xml** file present in the **<installation_dir>\conf** folder in a local text editor. (Ensure that you create a backup of the existing server.xml file just in case you wish to restore it).
- Navigate to the end of the XML file, look for the connector tag **<Connector SSLEnabled="true" ...../>**, and edit the following values (case-sensitive) within this connector tag.

keystoreFile="./conf/"

keystorePass=" "

keystoreType="PKCS12"

For example: <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"/>

STEP - 4

Start ADAudit Plus.

Glossary:

What is SSL?

Abbreviated as SSL, Secure Socket Layer is an encryption technology to secure the data exchange between a website and its visitor's web browser. Normally, when a user communicates with a website, say submits his credit card information, the data travels to the server in plain text, which is susceptible to data theft. Whereas if this data is encrypted, then no eavesdropper can read it. Thus, it's essential to secure a website with SSL.

SSL Certificate:

This is a digital identity of a company, which ensures that a visitor is talking only to its intended website and whatever data he submits to the site is encoded and reaches only the intended site. This system is analogous to banks recognizing their customers by their signatures. In this case, the browsers (thereby the end-users) are programmed to trust these Certifying Authority (CA) presented certificates.

Certifying Authority:

Regulatory organizations, with the help of standard policies, issue certificates to a domain declaring it trustworthy. Every certificate they generate is unique to the company they are certifying, which makes identification easy.

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:

In order for a CA to generate an SSL certificate for a company, it first collects information about that company and other identifiers such as public key (digital signature), and then binds them all with its certificate. In doing so, it generates a unique identifier for the company.

Thus every certificate issuance process begins with a "certificate request" from the company. Certifying Authorities refer to this process as Certificate Signing Request (CSR). The Certifying Authorities accept the company information and digital signatures in a special file format, namely **.csr** format.

Overview of ADAudit Plus:

ADAudit Plus is a web-based, real-time Active Directory change auditing tool that helps you:

- Track all changes to Windows AD objects including users, groups, computers, GPOs, and OUs.
- Monitor every user's logon and logoff activity, including every successful and failed logon attempt across network workstations.
- Audit Windows file servers, failover clusters, NetApp, and EMC storage to document changes to files and folders.
- Monitor system configurations, program files, and folder changes to ensure file integrity.
- Track changes across Windows servers, printers, and USB devices with a summary of events.

To learn more about how ADAudit Plus can help you with all your Active Directory auditing needs, please visit: https://www.manageengine.com/products/active-directory-audit/

$ Get Quote Download