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 to enable SSL

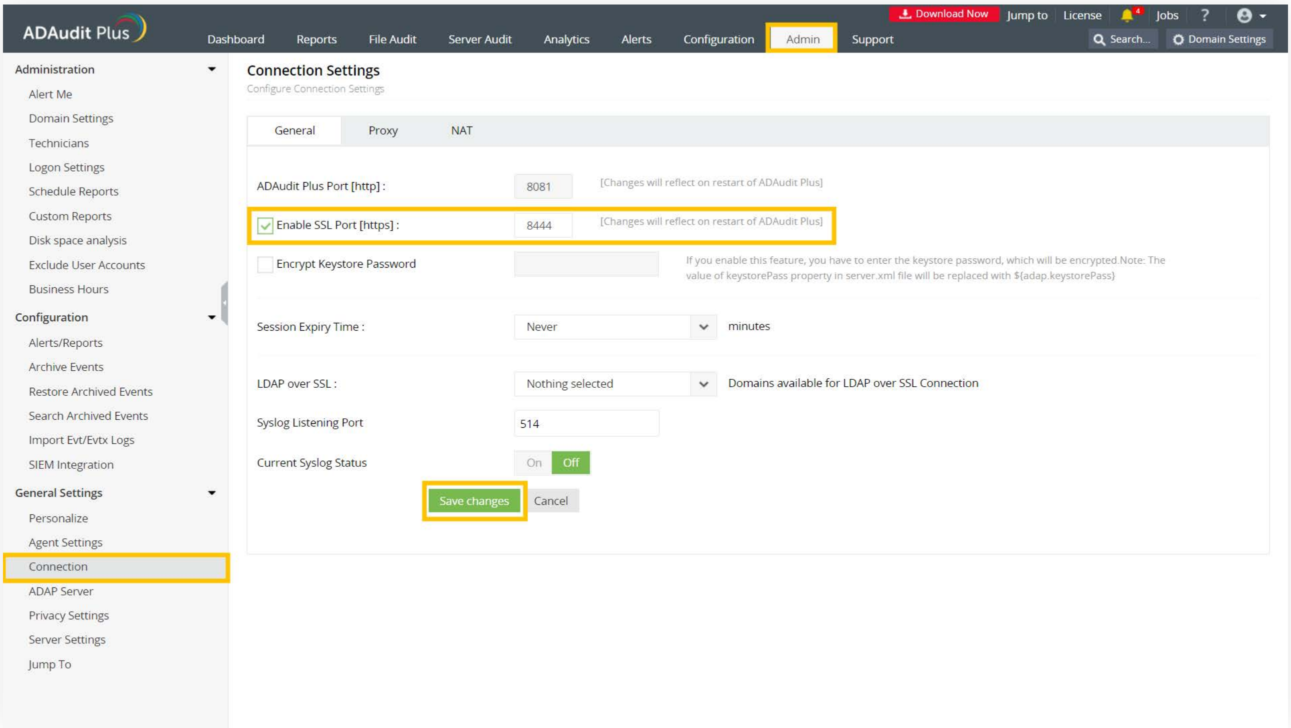
The following steps will guide you through enabling SSL in ADAudit Plus.

STEP - 1

Define the SSL port

- Log in to ADAudit Plus with an account that has administrative privileges.
- Navigate to **Admin > General Settings > Connection.**
- Check the **Enable SSL Port [https]** box. The default port number 8444 is selected automatically.
- Click **Save changes**.
- Restart ADAudit Plus for the changes to take effect.

Note: If you want to install an existing **PFX or PKCS #12 certificate**, skip to the PFX or PKCS #12 format section in Step 5.



Connection Settings

Configure Connection Settings

ADAudit Plus Port [http] : 8081 [Changes will reflect on restart of ADAudit Plus]

☑ Enable SSL Port [https] : 8444 [Changes will reflect on restart of ADAudit Plus]

□ Encrypt Keystore Password — If you enable this feature, you have to enter the keystore password, which will be encrypted.Note: The value of keystorePass property in server.xml file will be replaced with ${adap.keystorePass}

Session Expiry Time : Never minutes

LDAP over SSL : Nothing selected Domains available for LDAP over SSL Connection

Syslog Listening Port 514

Current Syslog Status On [✓ Off]

STEP - 2

Create the keystore

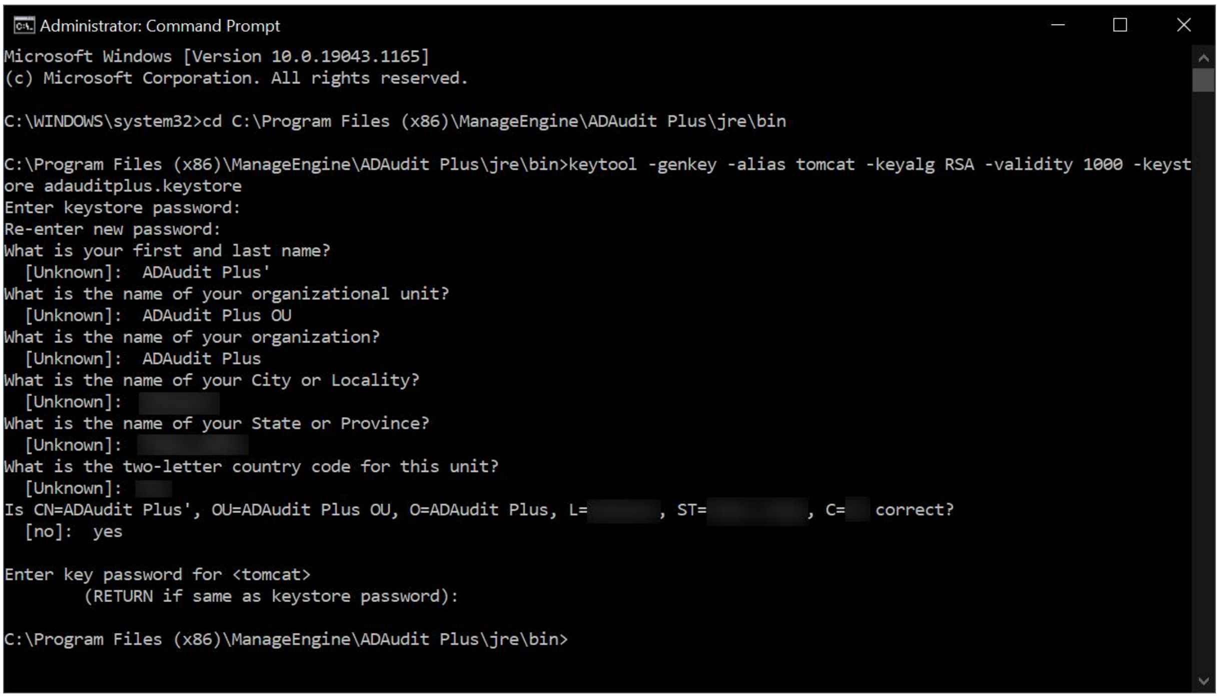
A keystore is a password-protected file that contains the keys and certificates for the server to encrypt and decrypt data.

- To create a certificate keystore file and generate encryption keys, run **Command Prompt** as an administrator, navigate to <product_installation_directory>\jre\bin, and execute the following command:

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

- Replace <domainName> with the name of your domain.
- Type in your keystore password.
- Provide information based on the following guidelines:

What is your first and last name?	Provide the machine name or the fully qualified domain name of the server hosting ADAudit Plus.
What is the name of your organizational unit?	Enter 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 or Locality?	Enter the city name as provided in your organization's registered address.
What is the name of your State or Province?	Enter the state or province as provided in your organization's registered address.
What is the two-letter country code for this unit?	Provide the two-letter code of the country in which your organization is located.
Enter key password for <tomcat>	Enter the same password as the keystore password. **Note:** If you choose to enter a different password, note it down because the key password will be required later.



```
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 -keyst
ore 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]:  [redacted]
What is the name of your State or Province?
  [Unknown]:  [redacted]
What is the two-letter country code for this unit?
  [Unknown]:  [redacted]
Is CN=ADAudit Plus', OU=ADAudit Plus OU, O=ADAudit Plus, L=[redacted], ST=[redacted], C=[redacted] correct?
  [no]:  yes

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

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

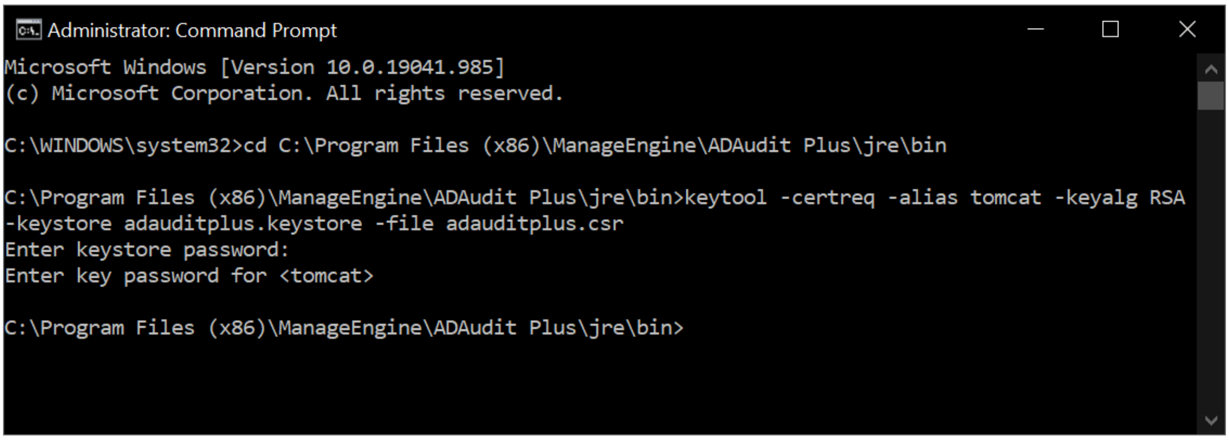
STEP - 3

Generate the certificate signing request (CSR)

- To create a CSR with a subject alternative name (SAN), execute the following command in **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
```

Replace <domainName> with the name of your domain and provide the appropriate SANs as shown in the image below:



```
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>
```

STEP - 4

Issue the SSL certificate

In this step, you will connect to a certificate authority (CA), submit the CSR to the specific CA, and get the SSL certificate issued to you.

A. Issue the SSL certificate using an external CA

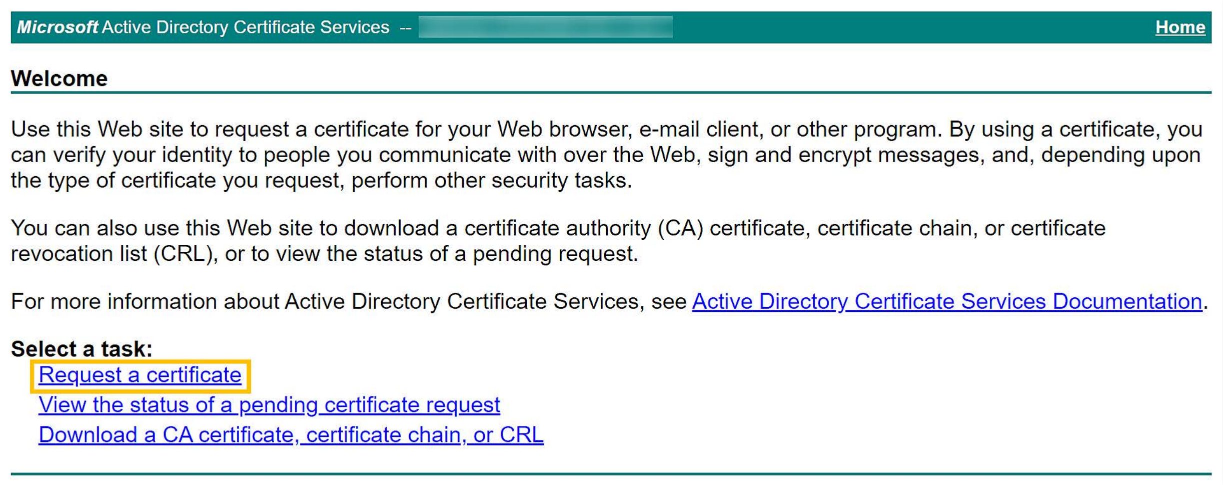
- To request a certificate from an external CA, submit the CSR to that CA. You can locate the CSR file in the <product_installation_directory>\jre\bin folder.
- Unzip the certificates returned by your CA and put them in the <product_installation_directory>\jre\bin folder.

Note: After the SSL certificate is issued by the external CA, proceed to Step 5 to install the certificate.

B. Issue the SSL certificate using an internal CA

An internal CA is a member server or domain controller in a specific domain that has been assigned the CA role.

- Connect to the **Microsoft Active Directory Certificate Services** of your internal CA and click the **Request a certificate** link.



Microsoft Active Directory Certificate Services -- [redacted] Home

Welcome

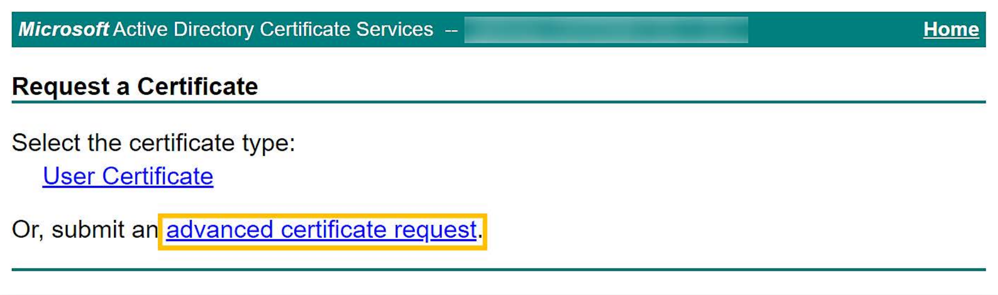
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security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

- On the Request a Certificate page, click the **advanced certificate request** link.



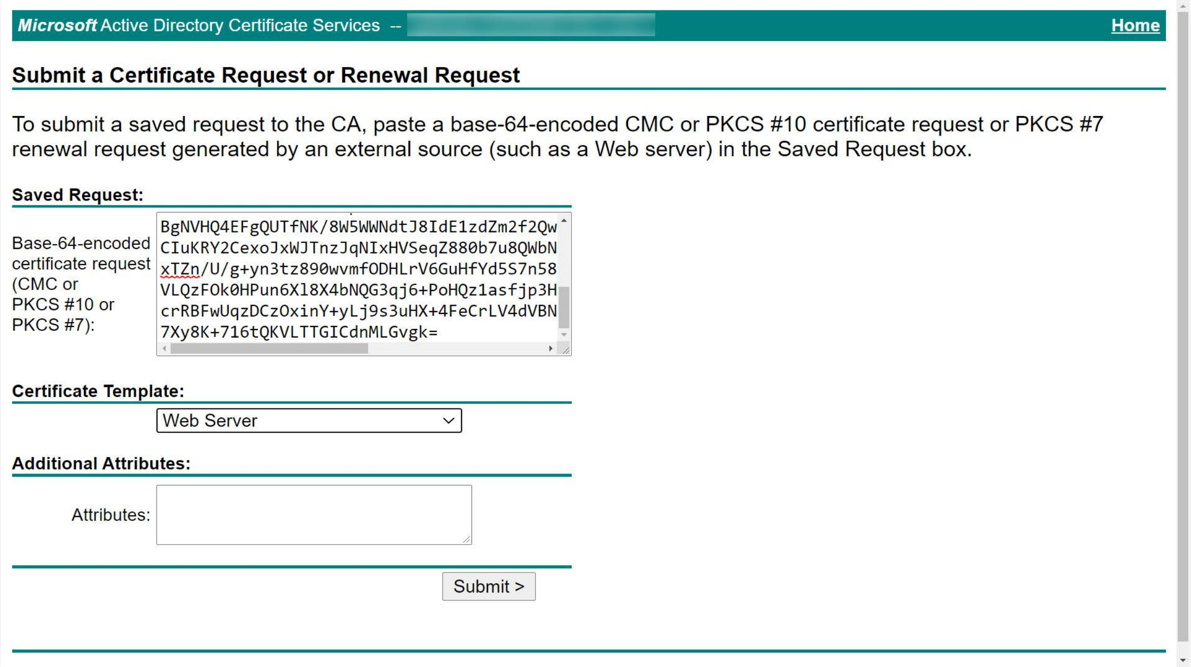
Microsoft Active Directory Certificate Services -- [redacted] Home

Request a Certificate

Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

- On the Submit a Certificate Request or Renewal Request page, copy the content from your CSR file and paste it in the **Saved Request** field.
- Select **Web Server** or the appropriate template for Tomcat under **Certificate Template** and click **Submit.**



Microsoft Active Directory Certificate Services -- [redacted]

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
VLQzFOk0HPun6Xl8X4bNQG3qj6+PoHQz1asfjp3H
crRBFwUqzDCzOxinY+yLj9s3uHX+4FeCrLV4dVBN
7Xy8K+716tQKVLTTGICdnMLGvgk=
```

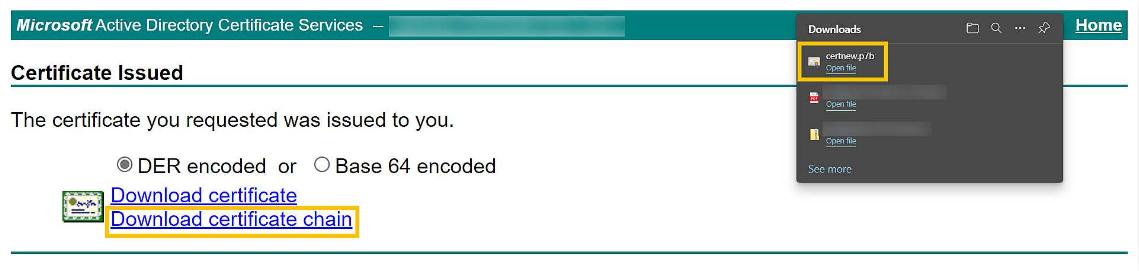
Certificate Template:

Web Server

Additional Attributes:

Attributes:

- The certificate will be issued when you click the **Download certificate chain** link. The downloaded certificate will be in the P7B file format.



Microsoft Active Directory Certificate Services -- [redacted]

Certificate Issued

The certificate you requested was issued to you.

● DER encoded or ○ Base 64 encoded

Download certificate
Download certificate chain

- Copy the P7B file to the <product_installation_directory>\jre\bin folder.

STEP - 5

Import the certificate

Follow the steps given below that correspond with the format in which you want to import the certificate.

A. Privacy-enhanced mail (PEM) format

To import the certificate into the keystore file in PEM format, open Command Prompt, navigate to <product_installation_directory>\jre\bin, and run the commands from the list below that applies to your CA.

General commands

- 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

Vendor-specific commands

For GoDaddy certificates

- 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

For Verisign certificates

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

For Comodo certificates

- 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

For Entrust certificates

- 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>

For certificates purchased through the Thawte reseller channel

- 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>

Once the certificate is installed, proceed to Step 6 to bind the certificate to ADAudit Plus.

Note:

If you are receiving the certificates from a CA that is not listed above, then contact your CA to get the commands required to add its certificates to the keystore.

B. P7B or PKCS #7 format

To import the certificate into the keystore file in P7B or PKCS #7 format, open Command Prompt, navigate to <product_installation_directory>\jre\bin, and execute the following command:

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

Once the certificate is installed, proceed to Step 6 to bind the certificate to ADAudit Plus.

C. PFX or PKCS #12 format

To import the certificate into the keystore file in P7B or PKCS #7 format, open Command Prompt, navigate to <product_installation_directory>\jre\bin, and execute the following command:

- Copy and save your PFX or PKCS #12 file in the <product_installation_directory>\conf folder.
- Open the **server.xml** file present in the <product_installation_directory>\conf folder with a local text editor. Create a backup of the existing server.xml file just in case you wish to restore it.
- Find the connector tag that contains *<Connector ... SSLEnabled="true"*... ***name="SSL"***.../>.
- Within the connector tag, make the following changes:
    - Replace the value of *keystoreFile* with "***./conf/<YOUR_CERT_FILE.pfx>***".
    - Add ***keystoreType="PKCS12".***
- Save and close the *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:

After modifying the *server.xml file*, skip to the "Encrypt the keystore password" section in Step 6.

STEP - 6

Bind the certificates to ADAudit Plus

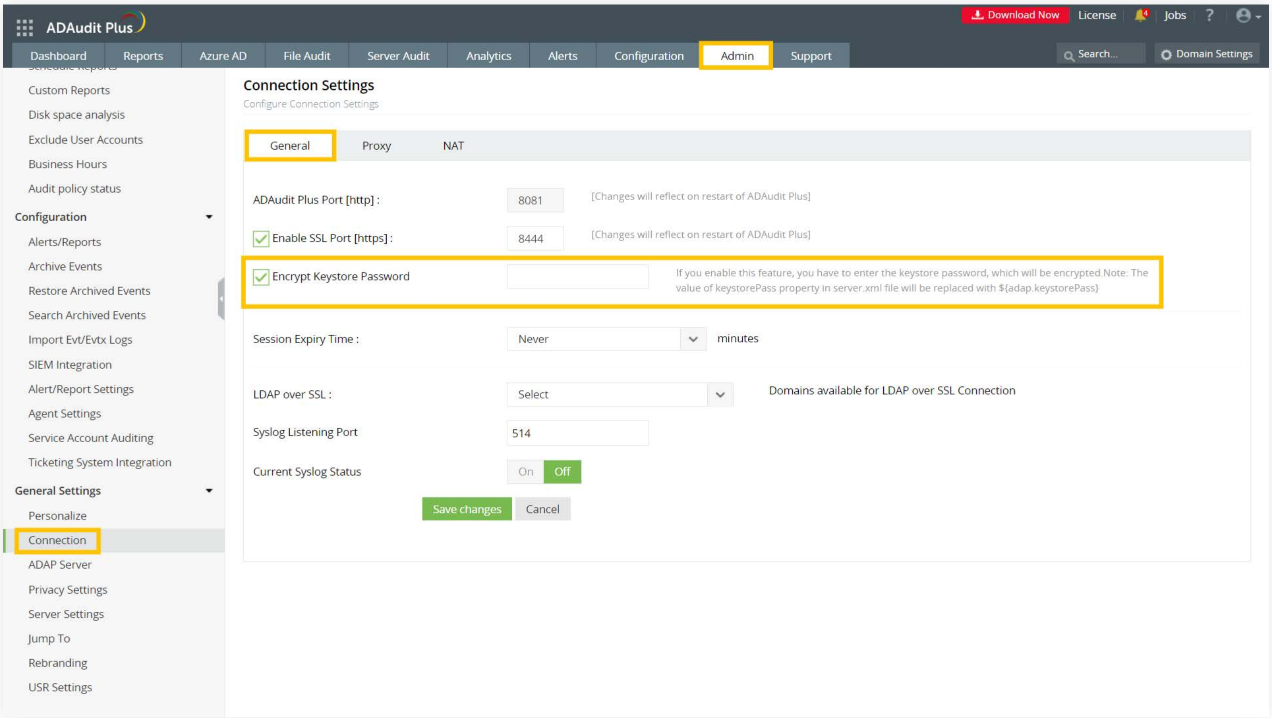
- Copy the ***<domainName>.keystore*** file from the *<product_installation_directory>\jre\bin* folder and paste it in the *<product_installation_directory>\conf* folder.
- Open the ***server.xml*** file present in the *<product_installation_directory>\conf* folder with a local text editor. Create a backup of the existing *server.xml* file just in case you wish to restore it.
- Find the connector tag that contains *<Connector … SSLEnabled="true"… **name="SSL"…/>***.
- Within the connector tag, replace the value of *keystoreFile* with "***./conf/<Your_Domain_Name>.keystore***".

```
<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="*********" maxSpareThreads="75"
maxThreads="150" minSpareThreads="25" name="SSL" port="8444" scheme="https" secure="true"
sslEnabledProtocols="TLSv1,TLSv1.1,TLSv1.2" sslProtocol="TLS"/>
```

- Save and close the *server.xml* file.

Encrypt the keystore password

- Log in to your ADAudit Plus web console and navigate to **Admin > General Settings > Connection.**
- Select the **General** tab, check the **Encrypt Keystore Password** box, and enter the keystore password you used while generating the CSR for this certificate file.
- Click **Save changes.**
- Restart ADAudit Plus again for the changes to take effect.



Connection Settings

Configure Connection Settings

ADAudit Plus Port [http] : 8081 [Changes will reflect on restart of ADAudit Plus]

☑ Enable SSL Port [https] : 8444 [Changes will reflect on restart of ADAudit Plus]

☑ Encrypt Keystore Password — If you enable this feature, you have to enter the keystore password, which will be encrypted.Note: The value of keystorePass property in server.xml file will be replaced with ${adap.keystorePass}

Session Expiry Time : Never minutes

LDAP over SSL : Select — Domains available for LDAP over SSL Connection

Syslog Listening Port 514

Current Syslog Status On [✓ Off]

Note:

If you want to modify the TLS versions and ciphers attribute, refer to our security hardening guide.

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.