Integrated Capture Points Guide

Server Certificate

5/9/2025

Contents

Server Certificate

The server certificate is used for server authentication (by the client) and ensures that server can be trusted. The Web Service Capture Point requires a server certificate to support SSL.

This page provides an example of generating a server certificate and putting it in the client's trusted certificates store.

Generate a server certificate

First generate a server certificate, along with a private key:

```
openssl req -x509 -days 365 -subj "/C=US/ST=California/L=Daly City/CN
=zoolander.us.int.genesyslab.com" -newkey rsa:2048 -keyout wscpserver.pem -out wscpserver.pem
```

The output file `wscpserver.pem` contains a private key along with a certificate. During the private key generation, the user is prompted for a password, which will be required later. The user will be asked to come up with a *PEM pass phrase,* which will be later used in the WSCP configuration, along with the generated `.pem` file. The server certificate can also be a self-signed certificate or a certificate signed by any Certificate Authority (CA). The certificate generated for the server must be imported or copied into the client's trusted certificates store. Use the procedure and tools appropriate for your platform.

The private key should **never** be copied or given to anyone. It should be password protected (encoded) and should be accessible to the server only. The client is given only the certificate (public key) to put into the trusted certificates store.

The following is a procedure for putting server certificates into client's trusted certificates store for Windows, using the `openssl` utility.

Put server certificate in client's store

Start

1. Convert the generated certificate to DER format:

   ```
   openssl x509 -outform der -in wscpserver.pem -out wscpserver.cer
   ```

   The output file `wscpserver.cer` contains a public server certificate, which will be added to the trusted certificates of the client using the Web Service Capture Point.

2. Import the generated .CER server certificate into the trusted certificates store (for browser and .NET client):
   a. Start Microsoft Management Console.
   b. On the `File` menu, select `Add or Remove Snap-ins`.
   c. Choose `Certificates`, then click `Add`.

d. When prompted, choose `Computer account` and `Local Computer`.

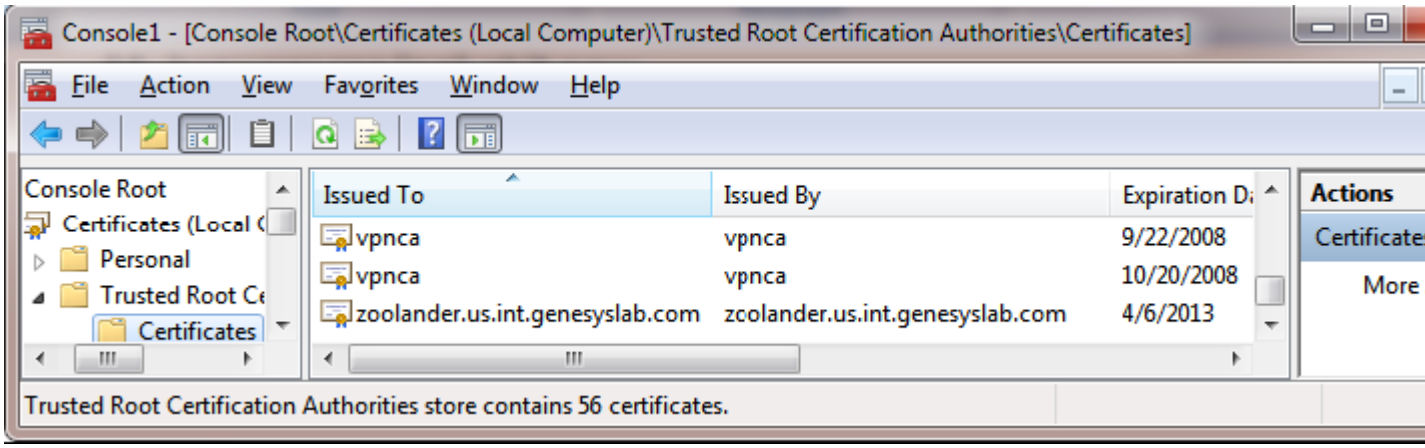
e. Click `Finish`, then `OK`.

f. Right-click `Certificates > Trusted Root Certification Authorities > Certificates`.

g. Choose `All tasks > Import"`

h. Choose `wscpserver.cer` for import.

The certificate is added to the trusted certificates, as shown below.



Certificate Added to Trusted Certificates

3. For Java clients only, import the generated .CER server certificate into a Java keystore. Assuming that a standard JDK is present on the client host, add the server certificate to a trust store on the client host:

```
keytool -import -keystore truststore.jks -file wscpserver.cer -alias wscpserver
```

End

Client Certificate for Browser and .NET Client

A client certificate is required for mutual SSL authentication. If the Web Service Capture Point is configured for server authentication only, the client certificate is not required.

Examples are available of generating the certificate for .NET and for Windows.