From: www.luckstar.com.tw

Date: 2014-07-30

Subject: Configuring SSL Certificates for VisualSVN Server

Ref:

<http://www.visualsvn.com/support/topic/00034/>

<http://www.visualsvn.com/support/topic/00035/>

VisualSVN Server supports secure connection over the HTTPS protocol (*Hypertext Transfer Protocol Secure*). This protocol is a combination of the *Hypertext Transfer Protocol* with the *SSL/TLS* protocol to provide encryption and secure identification of the server.

The main idea of HTTPS is to create a secure channel over an insecure network. This ensures reasonable protection from eavesdroppers and man-in-the-middle attacks, provided that adequate cipher suites are used and that the server certificate is verified and trusted.

**SSL Certificates**

In order to work over the HTTPS protocol, the VisualSVN Server should be equipped with an SSL certificate. A server certificate contains detailed identification information, such as the name of the organization that is affiliated with the server content, the name of the organization that issued the certificate, the name of the server and so on.

In most cases, certificate is signed by a trusted Certificate Authority (CA). It can be:

* Third-party Certificate Authority such as Verisign or GeoTrust.
* Domain Certificate Authority such as Active Directory Certificate Services.

An SSL certificate is automatically trusted by standard Subversion clients and web-browsers if it's signed by a trusted Certificate Authority. If a certificate is not trusted by client, the connection will be encrypted but it's not sure that client communicates with the true server.

**Self-signed SSL Certificates**

Self-signed SSL certificate is pre-generated during the first setup of VisualSVN Server. Self-signed certificate allows you to setup encrypted connection to the server but it's not trusted by standard Subversion clients and web-browsers.

You will receive the following warning message if you are connecting to the server that is configured to use self-signed certificate:

**Error validating server certificate for 'https://vt-2008:443':  
- The certificate is not issued by a trusted authority. Use the fingerprint to validate the certificate manually!  
Certificate information:  
- Hostname: VT-2008  
- Valid: from Wed, 16 Sep 2009 09:11:30 GMT until Sat, 14 Sep 2019 09:11:30 GMT  
- Issuer: VT-2008  
- Fingerprint: ca:95:89:77:43:86:42:ce:77:5b:7a:8c:01:99:0f:70:3f:26:c1:e7  
(R)eject, accept (t)emporarily or accept (p)ermanently?**

It's recommended to replace the default self-signed certificate for a certificate signed by trusted Certificate Authority (domain or third-party).

**Signing SSL certificate with a trusted Certificate Authority**

In order to obtain and install signed certificate from a trusted Certificate Authority, you are requested to:

* Prepare Certificate Signing Request (CSR) using the VisualSVN Server Manager.
* Submit this request to a Certificate Authority and obtain signed certificate.
* Import the signed certificate to VisualSVN Server.

If you are going to obtain certificate from a third-party Certificate Authority, you are requested to complete an appropriate form on the authority's web-site. Usually, this is a paid service. Some additional paperwork may be required.

If you wish to obtain certificate from your corporate *Active Directory Certificate Services*, contact your system administrator or follow the instructions provided in the article below:  
[How to sign server certificate with Active Directory Certificate Services](http://www.visualsvn.com/support/topic/00035/)

**Running VisualSVN Server with a self-signed SSL certificate**

Generally spoken, it's not recommended to use self-signed SSL certificates in production. In this case you're requested to manually accept the certificate based on its fingerprint. Note that certificates are accepted on a per user basis.

It's also possible to export a self-signed certificate from VisualSVN Server and save this certificate in the trusted certificates list on all client computers.

**See Also:**

[KB35: How to sign server certificate with Active Directory Certificate Services](http://www.visualsvn.com/support/topic/00035/)