

webnames.ca[®]

SSL Configuration and Installation Guide

v1.8

10/25/2011

Table of Contents

Preface **3**

Configuration..... **3**

 Overview 3

 Generation of Certificate Signing Request (CSR) key:..... 3

 3rd Party Webservers 4

 Webnames Hosting..... 4

 Webnames ASP.NET Hosting 4

 Configuration of Certificate via Webnames.ca Account 5

Approval and Validation..... **6**

 Overview 6

 Domain Validated Certificates 6

 Approval..... 6

 Business Validated Certificates 7

 Confirmation of Domain Registration and Registrant / Organization name 7

 Authentication of the Business Identity 7

 Address Authentication 7

 Verification of Certificate Contact 8

 Extended Validation Certificates 8

 Acknowledgement Agreement 8

 Authentication of the Business Identity 9

 Verify Operational Existence 9

 Address Authentication 9

 Obtain Third Party Telephone Number 9

 Verification of Certificate Contact 10

 Confirmation of Domain Registration and Registrant / Organization name 10

 Verification..... 10

Issuance and Installation **11**

 Overview 11

 Issuance..... 11

 Installation..... 11

 3rd Party Webservers 11

 Webnames Hosting..... 11

 Webnames ASP.NET Hosting 12

 Site Seal Installation..... 12

 Overview 12

Reissuance..... **13**

 Overview 13

 Process 14

Renewals **15**

 Overview 15

 3rd Party Webservers 15

 Webnames Hosting..... 15

 Webnames ASP.NET Hosting 16

 Renewal via Webnames.ca Account 16

 Approval & Validation 16

 Issuance & Installation 16

Preface

The scope of this guide is to provide procedural information pertaining to the configuration, issuance, reissuance and renewal of SSL Certificates obtained through Webnames.ca. This guide makes the assumption that the SSL Certificate of choice has already been purchased and resides within your Webnames.ca account via My Account -> SSL Certificates.

For more information on the current line of SSL Certificates available through Webnames.ca please visit <http://www.webnames.ca/services/ssl>

Configuration

Overview

Configuration consists of submitting the following information so that request can be validated and SSL Certificate issued:

- Information from webserver (CSR key)
- Requestor information (Individual and organization information)
- Address that SSL Certificate should be sent to once generated

Generation of Certificate Signing Request (CSR) key:

NOTE: For the purposes of increased security, the requirements established by the Certificate Authority Browser Forum for Extended Validation Certificates now state that a minimum of 2048-bit CSR keys must be utilized for certificates that expire after December 31st, 2010.

Reflective of this, **Webnames.ca will require all CSR key submissions for certificates that will have a future renewal date of after December 31st, 2010 to utilize 2048 bits.** The vast majority of fully-patched server platforms will be able to generate 2048-bit CSR keys without issue.

We encourage all administrators responsible for existing SSL Certificates to ensure that their server platforms are patched and/or upgraded as necessary well in advance of their SSL Certificate renewal date.

Please see SP 800-57 at <http://csrc.nist.gov/publications/PubsSPs.html> for additional background regarding this change.

When generating a CSR

- Fully spell out the state and locality – no abbreviations are allowed
- The Organization name must include the corporate identifier

SSL Configuration and Installation Guide

3rd Party Webservers

The required CSR key needs to be generated via the physical server in which the SSL Certificate will ultimately be installed. If you have direct access to this server, then a CSR key can be generated via the applicable link below. If you utilize another Vendor for your hosting services, you will need to contact them for assistance with obtaining a CSR key. The process in this case will vary from one Vendor to another.

Reference

GeoTrust: <http://www.geotrust.com/support/generate-csr/>

Verisign: https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=AR235&actp=LIST&viewlocale=en_US

Webnames Hosting

1. Log into the (Plesk) Hosting Control Panel for the related domain
2. Click on **Domains**, and then the related domain name.
3. Click **SSL Certificates** in the bottom right. A list of SSL certificates that you have in your repository will be displayed.
4. Click **Add SSL Certificate**.
5. Specify the certificate properties:
 - a. **Certificate name.** This will help you identify this certificate in the repository.
 - b. **Encryption level.** Choose the encryption level of your SSL certificate. It is required that you choose 2048 bit.
 - c. **Your location and organization name.** The values you enter should not exceed the length of 64 symbols.
 - d. The **domain name** for which you want to purchase an SSL certificate. This should be a fully qualified domain name. Example: www.your-domain.com.
 - e. The website administrator's e-mail address and **organizational unit/department**
6. Make sure that all the provided information is correct and accurate, as it will be used to generate your private key.
7. Click **Request**. Your private key and certificate signing request will be generated and stored in the repository.
8. In the list of certificates, click the name of the certificate you need. A page showing the certificate properties opens.
9. Locate the CSR section on the page, and copy the text that starts with the line -----BEGIN CERTIFICATE REQUEST----- and ends with the line -----END CERTIFICATE REQUEST----- to the clipboard.
10. Use the generated CSR information as part of the Configuration process, which is outlined in the next section of this document.

Webnames ASP.NET Hosting

CSR keys must be generated directly from our hosting servers. Please contact us at hosting@webnames.ca or 1 866 221-7878 and one of our staff will be happy to initiate this process.

Note: There is a utility within the Control Panel to generate a CSR, however it will only generate one which utilizes a 1024-bit length. This length is no longer accepted by more SSL Certificate Vendors, and thus Webnames.ca support staff will need to facilitate the generation of a 2048-bit CSR key as per the process noted above.

SSL Configuration and Installation Guide

Configuration of Certificate via Webnames.ca Account

1. Once logged into your account at www.webnames.ca, browse to:
My Account > SSL Certificates > Configure button
2. Enter Certificate background info
 - **Display Name:** Only used for identifying the Certificate in the list of existing SSL Certificates within your Webnames.ca account. Enter the display name of your choice.
 - **Hostname:** This field is pre-populated with the domain the certificate is applicable to.
 - **Server Type:** The correct value for the server type should be selected from the list.
3. Paste in the aforementioned CSR key in its entirety.
4. Specify the SSL Contact information for the Certificate. *Typically the domain's existing Administrative, Billing and Technical Contact information is the best information to use. Do not use any shift characters in any of the enrollment fields. If your company has an & or @ symbol in its name, you must spell out the symbol or omit it from the related Contact field.

Note: *This information should match the WHOIS information for the domain. Additionally, the WHOIS information for the domain must be publically viewable so that the applicant information submitted via this step can be verified via a WHOIS lookup by the Certificate Vendor (GeoTrust, Verisign etc.).

5. Click Continue to Proceed to the next page.
6. Specify address that the Approval email and eventual SSL Certificate will be sent to once generated. Only the Administrative email address of the domain, as well as several generic predetermined alternatives can be used.

Approval and Validation

Overview

Once the SSL Certificate configuration data has been submitted to the certificate Vendor, the Vendor will validate the domain, the control thereof, and optionally the business identity, depending on the type of SSL Certificate being purchased.

Domain Validated Certificates

Domain Validated Certificates verify the person responsible for the domain. They do not include authentication of the business identity.

- GeoTrust QuickSSL
- GeoTrust QuickSSL Premium

Two steps are performed for Domain Validated Certificates

1. Confirm that the Domain Name is registered
2. Confirm that the Domain Approver has control over the Domain via an Approval Email process

Note: If the order is for a Major Corporation, a well-known Trademark, or any Financial Institution, the Certificate Contact must be an employee of the company. Additional verification will also be performed in this case via telephone.

Approval

The Vendor issuing the Certificate will send the previously specified Contact an Approval Email, which must be reviewed and the instructions followed. Once approval has been given by the Contact as per the instructions Email, the Vendor will proceed to the next step of Issuance. The Contact which will be sent the subsequent Issuance Email (which includes the SSL Certificate itself) is listed within either the Approval Email or the webpage the Approval Email links to.

If this Approval email is not received or is lost, the Reissuance process can be utilized to reinitiate the Approval process. Please refer to the Reissuance section of this document.

SSL Configuration and Installation Guide

Business Validated Certificates

In addition to performing the checks featured within Domain Validated Certificates, Business Validated Certificates also include authentication of the business identity.

- GeoTrust True Business ID
- GeoTrust True Business ID Wildcard
- Verisign Secure Site
- Verisign Secure Site Pro

Four steps are performed for Business Validated Certificates

1. Confirm that the Domain Name is registered, and that the Registrant information matches the Organization name submitted during Configuration
2. Confirm the existence and validity of the Business Entity
3. Confirm the Address of the Business Entity
4. Verify the Certificate Contact's employment within the Business Entity

Confirmation of Domain Registration and Registrant / Organization name

If the Registrant and Organization information submitted during Configuration is not an exact match, the domain administrator will be contacted via phone or email to confirm that the Organization has exclusive control of the domain.

Authentication of the Business Identity

The Organization's full legal name as it is registered with a government agency must be verified and in good standing in the location listed in the Configuration data..

No misspellings or abbreviations are permitted

If the Organization cannot be verified using standard means, government-filed business registration documents may need to be produced.

Acceptable documents include:

- Articles of Incorporation
- Business License
- Charter Documents
- Fictitious Name Statement
- Registration of Trade Name

Address Authentication

The Organization address must also be confirmed via a verifiable third party resource, which includes but is not limited to:

- 3rd party Telephone number database
- Valid Dun and Bradstreet report
- WHOIS Registrant

SSL Configuration and Installation Guide

- Verbal verification through a verified phone number from one of the resources listed above
- Verbal verification through a phone number listed on the website to which the certificate order is applicable.

Verification of Certificate Contact

The Certificate Contact defined during the Configuration process will have their employment within the Business Entity / Organization verified.

It is recommended that the Certificate Contact's email address be registered to the Organizational domain, or one of their verified Parent / Subsidiaries. A verification call with the Certificate Contact using a verified telephone number may be required.

Note: The normal processing time for True Business ID certificates is 2 business days if no documents are required.

To expedite your order please ensure:

- The Organization is active and in good standing
- The Domain is registered to the Organization submitted during Configuration
- The Corporate Contact is a permanent employee if the Organization

Extended Validation Certificates

Extended Validation Certificates have a more rigorous validation process. This process is applicable to

- GeoTrust True Business ID EV
- Verisign Secure Site with EV
- Verisign Secure Site Pro with EV

Eight steps are performed for Business Validated Certificates

1. Acknowledgement Agreement
2. Authentication of the Business Identity
3. Verify Operational Existence.
4. Address Authentication
5. Obtain Third Party Telephone Number
6. Verification of Certificate Contact
7. Confirmation of Domain Registration and Registrant / Organization name
8. Verification

Acknowledgement Agreement

Certificate Contact must sign and return the Acknowledgement Agreement (to the Vendor). To expedite processing, this Agreement includes the option to identify the Human Resources contact within the Organization. The HR contact will be contacted to complete the employment verification.

SSL Configuration and Installation Guide

Authentication of the Business Identity

The Organization's full legal name as it is registered with a government agency must be verified and in good standing in the location listed in the Configuration data.

No misspellings or abbreviations are permitted

If the Organization cannot be verified using standard means, government-filed business registration documents may need to be produced.

Acceptable documents include:

- Articles of Incorporation
- Business License
- Charter Documents
- Fictitious Name Statement
- Registration of Trade Name

Verify Operational Existence

Organization must be registered and in existence for over 3 years. For Organizations in existence for less than three years, verification can be achieved via:

- A valid Dun & Bradstreet report
- Verifying the Organization has a demand deposit account, such as a chequing account via a document issued by a regulated financial institution, or a Professional Opinion Letter

Address Authentication

The Organization address must also be confirmed via a verifiable third party resource, which includes but is not limited to:

- Government Agency used during Organization Authentication
- Valid Dun and Bradstreet report
- Global Authentication and Verification Report
- A Professional Opinion Letter

Obtain Third Party Telephone Number

The telephone number must be under the Organization name, and must match the verified business address

The telephone number must be obtained through an approved resource

- 3rd party Telephone number database
- Valid Dun and Bradstreet report
- Government POR database used to authenticate the Organization
- A Professional Opinion Letter

SSL Configuration and Installation Guide

Verification of Certificate Contact

The Certificate Contact defined during the Configuration process will have their employment and authority within the Business Entity / Organization verified.

It is recommended that the Certificate Contact's email address be registered to the Organizational domain, or one of their verified Parent / Subsidiaries. A verification call with the Certificate Contact using a verified telephone number may be required.

The Corporate Contact's employment can be confirmed several ways:

- If the Corporate Contact is listed as an office of executive of the organization in:
 - The Business Registration used during Organization Authentication
 - Valid Dun and Bradstreet report
 - Global Authentication and Verification Report
- Confirmation with the Organization's HR department
- A Professional Opinion Letter

Authority indicates that the Corporate Contact is authorized to purchase the EV certificate on the behalf of the Organization.

- Authority of the Corporate Contact is confirmed if the Corporate Contact's job title is confirmed in the Organization's business filings or by Human Resources as someone with 'deemed authority', whereby 'Deemed Authority' is someone with the title of Director or higher
- Authority can also be confirmed in the Acknowledgement Agreement
- If the corporate contact is not someone with 'deemed authority', confirmation of the Authority can be confirmed with someone with 'deemed authority' or the individual Human Resources confirms as the Corporate Contact's direct manager.

Confirmation of Domain Registration and Registrant / Organization name

The Registrant and Organization information submitted during Configuration must be an exact match. If an exact match cannot be facilitated, the domain administrator will be contacted via phone or email to confirm that the Organization has exclusive control of the domain.

Verification

A verification telephone call must be completed with the Certificate Contact. This call is placed using the verified third party telephone number confirmed during the Authentication process.

Reference

GeoTrust: <http://www.geotrust.com/ssl/compare-ssl-certificates.html>

Verisign: https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=AR1640&actp=search&viewlocale=en_US&searchid=1307660643732#how_long_to_process

Issuance and Installation

Overview

Upon issuance, the SSL Certificate is received and then installed on the web server hosting the domain that the Certificate applies to. The certificate renewal date anniversary is its date of issuance, as opposed to purchase.

Issuance

At the conclusion of the Validation process, the SSL Certificate will be issued by way of a Fulfillment email. The issued Certificate is sent via email to Contact specified in the Configuration process. This Contact is also listed in the previous Approval process.

Aside from the SSL Certificate itself, the Fulfillment email contains installation instructions for the Certificate, any necessary Intermediate Certificates, as well as Site Seals for use on the associated website.

Installation

3rd Party Webservers

The SSL Certificate needs to be installed onto the physical server which hosts the website which the Certificate is applicable to. If you have direct access to this server, then you may install the Certificate yourself via the applicable link below. If you utilize another Vendor for your hosting services, you will need to contact them for assistance with installing your SSL Certificate. The process in this case will vary from one Vendor to another.

GeoTrust: https://knowledge.geotrust.com/support/knowledge-base/index?page=content&id=SO15065&actp=LIST&viewlocale=en_US

Verisign: https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=AR212&actp=LIST&viewlocale=en_US

Webnames Hosting

1. When you receive your SSL certificate, save it on your local machine or network.
2. Return to the **SSL certificates repository (Domains > Domain Name > SSL Certificates)**.
3. Upload your certificate and your intermediate file. The certificate file goes into the certificate box, and the intermediate goes into the **CA bundle box**. Click **Send File** or **Submit**. This will upload and install the certificate against the corresponding private key.
4. To install the certificate on a site, return to the **Websites & Domains** tab, and click Web Hosting Settings.
5. From the **SSL certificate menu**, select your SSL certificate and click **OK**.
6. Content for the secure portion of your website should be placed into the **httpsdocs** folder as opposed to the **httpdocs** folder.
7. The use of your SSL Certificate within our shared hosting environment will require that your hosting plan be set to utilize a dedicated IP address. Please contact us at hosting@webnames.ca or 1 866 221-7878 and one of our staff will be happy to initiate this process.

SSL Configuration and Installation Guide

Note: Please allow up to 48 hours for the dedicated IP address configuration process and necessary DNS propagation time to complete.

Webnames ASP.NET Hosting

1. Log into the Web Hosting control panel located at <http://hosting.webnameshosting.ca/OS4/>
2. Once logged in, click on the **Security** link at the top of the page.
3. Then click on the **SSL Manager** link in the menu that appears on the left.
4. Once in the SSL Manager, select the **Upload your Certificate** radio button, and then click **Next**
5. Paste the SSL Certificate in to the box on this page. As with the CSR key, the entirety of the text even the start and end indicator must be inserted.
6. The use of your SSL Certificate within our shared hosting environment will require that your hosting plan be set to utilize a dedicated IP address. Please contact us at hosting@webnames.ca or 1 866 221-7878 and one of our staff will be happy to initiate this process.

Note: Please allow up to 48 hours for the dedicated IP address configuration process and necessary DNS propagation time to complete.

Site Seal Installation

Overview

Included with each SSL Certificate is a related site seal for display on the applicable website. This Seal informs site visitors that the appropriate pages of the site have been secured.

Information for how to locate and/or code to have this seal displayed on the applicable website differs from one vendor to another. Instructions are included in the SSL Certificate Issuance email, or can be found below:

GeoTrust: <https://knowledge.geotrust.com/support/knowledge-base/index?page=content&id=SO5702&searchid=1312831631989>

Verisign: https://knowledge.verisign.com/support/trust-seal-support/index?page=content&id=AR1266&actp=LIST&viewlocale=en_US

Reissuance

Overview

This process allows customers to have previously issued SSL Certificates reissued. It can also be used to reinitiate the Approval process. The following are examples of when reissuance would be relevant:

- Private Key file loss.
- Private Key pass phrase loss.
- Private Key file has been compromised due to the server being hacked.
- Changes in Server Software Platform: Incorrect server software was selected during the enrollment process;
 - Server software platform has been upgraded to the latest version;
 - Moving to a different ISP or Hosting Company.
- If your Organizational Unit changes
- Changes to domain name:
 - Host name was left out when the Key/CSR pair was generated on the server:
Example: The Key/CSR pair was generated on the server for domain.com but domain name being secured is www.domain.com
 - Incorrect host name filled in when the Key/CSR pair was generated on the server:
Example: The Key/CSR pair was generated on the server for secure.domain.com but domain name being secured is shoppingcart.domain.com
 - Host name changes, provided that the top-level domain name remains the same:
Example: The Certificate was requested for secure.domain.com but the secure area is now being moved to shopping.domain.com

You **cannot** apply for a replacement if any of the following changes:

- Company Name
- Entire Domain Name:
 - Example 1:** The original Certificate was requested for www.domain.com but the domain name is being changed to [www.anotherdomain.com](#)
 - Example 2:** The original Certificate was requested for www.domain.com but the domain name no longer exists and the domain name for the site is changing to www.domain.net
 - Example 3:** The original Certificate was issued to www.domain.com, but the hostname needs to change to mail.domain.com. For this scenario, the only solution is to cancel the certificate and purchase a new one using the correct hostname. A refund for the canceled certificate is available within the first seven days of issuance.
- Province/State/Locality/Country

SSL Configuration and Installation Guide

If any of the above changes, then you will have to go through the process of purchasing a brand new Certificate. This is because the existing Validation information is no longer valid, and the Validation process must be undertaken once again.

Process

The reissuance process is conducted entirely through the issuing Vendor. Each Vendor provides a step-by-step process which can be completed online.

Reference

GeoTrust: <https://products.geotrust.com/orders/orderinformation/authentication.do>

Verisign: <http://www.verisign.com/ssl/current-ssl-customers/ revoke-replace-ssl/index.html>

Renewals

Note: Certificates may be renewed beginning 90 days prior to the expiration date.

Overview

Prior to the expiration of an existing SSL Certificate, it must be renewed in order for functionality to continue and not be disrupted.

The renewal process can, depending on your web server platform, require the use of a new CSR upon each renewal.

The following web server types require that a new CSR key be used upon each SSL Certificate Renewal:

- All versions of Microsoft's IIS server
- Tomcat servers
- All Java based servers

For these server types, begin the Renewal process by obtaining a new CSR (or 'Renewal Request) from the relevant web server.

3rd Party Webservers

Renewals for servers requiring that a new CSR be utilized

The required CSR key (or 'renewal request') needs to be generated via the physical server in which the existing SSL Certificate is installed. If you have direct access to this server, then a CSR key / renewal request can be generated via the applicable link below. If you utilize another Vendor for your hosting services, you will need to contact them for assistance with obtaining a CSR key for the purposes of renewing. The process in this case will vary from one Vendor to another.

Reference

GeoTrust: https://knowledge.geotrust.com/support/knowledge-base/index?page=content&id=SO12639&actp=search&viewlocale=en_US&searchid=1307727928245

Verisign: <https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=AR235>

Webnames Hosting

Webnames.ca hosting packages do not require new CSR keys to be used for the purposes of renewal. Webnames.ca hosting customers can disregard this section of the renewal process and proceed to the next section.

SSL Configuration and Installation Guide

Webnames ASP.NET Hosting

Webnames.ca hosting packages do not require new CSR keys to be used for the purposes of renewal. Webnames.ca hosting customers can disregard this section of the renewal process and proceed to the next section.

Renewal via Webnames.ca Account

Once a current CSR key has been obtained, or if your server type does not require that a new CSR key be used for the purposes of renewal, perform the following steps:

1. Once logged into your account at www.webnames.ca, browse to:
My Account > SSL Certificates > Renew button
2. Proceed with payment via our website Shopping cart.
3. Once the payment for the renewal is complete, returned to:
My Account > SSL Certificates > Configure button
4. Paste in the aforementioned CSR key in its entirety if *your server type requires that a new CSR be used*.
5. Specify the SSL Contact information for the Certificate. *Typically the domain's existing Administrative, Billing and Technical Contact information is the best information to use. Do not use any shift characters in any of the enrollment fields. If your company has an & or @ symbol in its name, you must spell out the symbol or omit it from the related Contact field.

Note: *This information should match the WHOIS information for the domain. Additionally, the WHOIS information for the domain must be publically viewable so that the applicant information submitted via this step can be verified via a WHOIS lookup by the Certificate issuing party (GeoTrust, Verisign etc.).

7. Click Continue to Proceed to the next page.
8. Specify address that the Approval email and eventual SSL Certificate will be sent to once generated. Only the Administrative email address of the domain, as well as several predetermined generic alternatives can be used.

Approval & Validation

The approval and Validation steps for renewals are the same as that of new certificate purchases, which are covered in a [previous section](#) of this guide.

All certificate orders undergo a stringent Authentication process to confirm the legitimacy of the submitted Organization and Common Name. Authentication for additional or renewal certificates could take as little as 1 hour, or up to several days, depending on if the information provided has already been Authenticated in past orders. If any information has been updated from a previous order, the Certificate vendor will need to re-validate it before issuing.

Issuance & Installation

The Issuance and Installation steps for renewals are the same as that of new certificate purchases, which are covered in a [previous section](#) of this guide.