

StoneGate SSL VPN Technical Note 2073

---

# **Creating a Certificate Request**

---

# Table of Contents

---

Introduction . . . . . page 3

Overview . . . . . page 3

Creating a Certificate Request with makecsr . . . . . page 3

Activating a Signed Certificate. . . . . page 7

Feedback. . . . . page 7

# Introduction

This technical note describes the procedure of generating a Certificate Signing Request using the `makecsr` scripts. It also explains the process of importing the signed certificate to the system and activating it for the Administration Service and the Access Point.

Changes since the previous revision (SG\_SVTN\_2073\_20070628) are marked in the left margin with a change bar as seen here to the left of this and the previous paragraph.

## Prerequisites

This technical note assumes a thorough understanding of StoneGate SSL VPN and of certificates in particular. Use the further reading to gain the required knowledge.

## Further Reading

More information on StoneGate SSL VPN administration can be found in the *StoneGate SSL VPN Administrator's Guide*, the Online Help, and the Technical Note repository provided with the product. Another source of information is the Stonesoft Support site, which can be found at <http://www.stonesoft.com/support/>.

For more information on related subjects, please visit the following resources:

- [TN2068 Adding Bundled Certificates](#)
- <http://archives.java.sun.com/cgi-bin/wa?A2=ind0311&L=java-security&P=R460&I=3>
- <http://www.bouncycastle.org>

## Overview

The process of generating a private key in both `.key` format and `.pk8` (PKCS#8) format and a Certificate Signing Request (CSR) is a tedious and sometimes error prone task. It involves a number of steps and a fair deal of knowledge of OpenSSL commands. StoneGate SSL VPN provides a script, `makecsr`, that allows you to make all the necessary items in one go, and in the right format for use with StoneGate SSL VPN Administrator.

A CSR is a request to sign a digital certificate. When you generate a certificate, the certificate signing request is usually given to a trusted Certificate Authority (CA), such as VeriSign or Thawte. The CSR is read and a signed certificate is returned to you.

Follow the instructions below to generate a CSR and a private key.

## Creating a Certificate Request with `makecsr`

To make use of the `makecsr` script you need to copy a number of files.

---

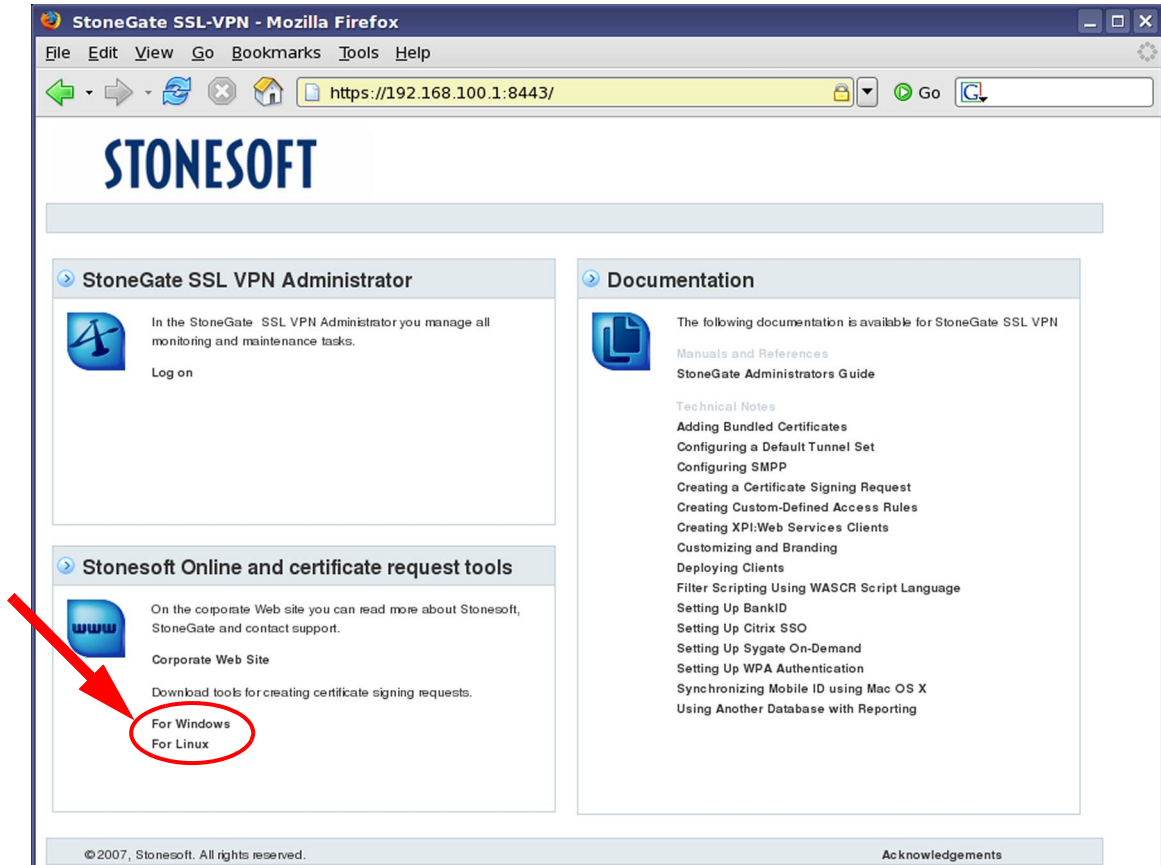
**Note** – You can run the `makecsr` script using any operating system. It is not necessary to run the script on Linux, even though that is the operating system that the StoneGate appliance uses.

---

### ▼ To copy the necessary files

1. Start by making a directory on your hard drive and call it CSR.
2. Download the required files as an archive from the front page of the StoneGate SSL VPN Administrator, in the section **Stonesoft Online and certificate request tools** ([Illustration 1](#))

Illustration 1 Link for Obtaining the Necessary files



- The following files are included:

TABLE 1 Files Included in Archive

| Archive              | Files Included  |
|----------------------|---|
| makescr_Windows.zip  | 512.tpl<br>1024.tpl<br>2048.tpl<br>openssl.exe<br>makecsr.bat<br>yn.com |
| makescr_Linux.tar.gz | 512.tpl<br>1024.tpl<br>2048.tpl<br>makecsr.sh                           |

3. Navigate to the previously created CSR directory and unpack the files there.
4. Type in `makescr` at the command prompt to start the certificate request generation.
5. The first thing the script will ask for is the cipher strength of the key. The available options are listed in parentheses, in this case it is either 512 bit, 1024 bit, or 2048 bit.

Enter the requested cipher strength (512, 1024 or 2048).  
Cipher strength: 1024

- In this example, we enter 1024.
6. Choose whether you want to have the private key encrypted with a password. Enter 'y' for YES and 'n' for NO. If you chose no your key will not be encrypted and the process will continue with step 7 below.

```
Shall the private key be encrypted? [y/n]
Note! The password will be visible when you type.
Encryption password: secret
```

- In this example we entered the password "secret".
7. After generating the private key, supply information needed in the CSR process.

```
Country Name (2 letter code) [US]:FI
State or Province Name (full name) [Some-State]:.
Locality Name (eg, city) [Some-City]:Helsinki
Organization Name (eg, company) [Acme Ltd]:Example Inc
Organizational Unit Name (eg, section) [Marketing]:Sales
Common Name (eg, fully qualified server domain name) [www.acme.com]:www.example.com
Email Address (optional) []:.
```

- The information in this section is outlined below. For some fields there is a default value. Those are listed in brackets. Some fields are optional and can be left blank. To leave a field blank you enter a period ('.'). This is a requirement of the underlying OpenSSL tool. This information is used to construct a Distinguished Name or DN, which will be used in the CSR process.
  - **Country:** The two-letter ISO abbreviation for your country. The default value is "US" and in this example we used "FI" for Finland.
  - **State or Province:** The state or province where your organization is legally located. This entry can not be abbreviated. The default value is "Some-State" and in this example we exercised our right to leave this field blank by typing a period ('.').
  - **Locality Name:** The city where your organization is legally located. The default value is "Some-City". In this example we entered "Helsinki".
  - **Organization Name:** The exact legal name of your organization. Do not abbreviate your organization name. The default value is "Acme Ltd", and in this example we used "Example Inc".
  - **Organization Unit Name:** This entry is for the name of the unit in your organization. The default value is "Marketing". In this example we entered "Sales".
  - **Common Name:** A fully qualified domain name for your web server. For example, if you intend to secure the URL <https://www.yourdomain.com>, then the common name of the CSR must be [www.yourdomain.com](https://www.yourdomain.com). This must be an exact match. The default value is "www.acme.com" and in this example we entered "www.example.com".
  - **Email Address:** This is an optional field for entering an contact e-mail address. The default value is empty and in this example we have left it blank by typing a period ('.').
- After the information is entered, a number of files are generated:
  - `private.key`
  - `private.pk8`
  - `server.csr`

- Finally, the script outputs the certificate request information for verification. This looks like this in our example above:

```
Certificate Request:
Data:
  Version: 0 (0x0)
  Subject: C=FI, L=Helsinki, O=Example Inc, OU=Sales,
  CN=www.example.com
  Subject Public Key Info:
    Public Key Algorithm: rsaEncryption
    RSA Public Key: (1024 bit)
    Modulus (1024 bit):
      00:bf:e0:44:5e:70:f0:35:01:9d:21:2c:d3:ab:ef:
      32:57:ca:26:a6:0f:d5:2e:de:95:b0:3e:d4:59:ea:
      b3:82:f5:30:c1:ad:06:22:9b:91:c5:1b:66:39:27:
      6d:ac:e6:22:dd:e8:f6:7f:56:ea:7f:d3:39:26:43:
      ab:95:12:97:fc:00:a4:7d:df:41:e1:5d:70:4d:fc:
      ba:04:3a:e4:b5:19:4c:94:91:a1:2b:ce:92:bb:03:
      15:8e:86:d4:39:8c:86:7a:ba:62:ec:d2:41:b2:5c:
      d1:61:7a:d2:cc:71:7c:09:9f:1a:84:c1:cf:da:64:
      ed:c1:34:6d:dc:24:96:f2:13
    Exponent: 65537 (0x10001)
  Attributes:
    a0:00
  Signature Algorithm: md5WithRSAEncryption
  04:08:ed:8a:01:8b:8c:ef:6a:03:d6:29:d2:b0:e0:09:7e:81:
  52:52:4a:31:5a:7e:62:1b:b1:78:9e:39:a9:ac:4f:5d:8f:8c:
  1b:06:68:6a:dd:53:83:57:01:f9:a3:61:d2:a3:27:b3:b7:79:
  42:78:14:d8:20:bd:3d:96:b1:29:32:64:38:d7:d0:57:73:51:
  b3:e2:65:96:46:b1:4a:7b:7f:19:9a:9a:9e:7c:9d:2a:d7:68:
  8f:de:8a:9e:7d:7b:7c:66:27:2f:40:5f:6d:ec:2e:f3:33:e7:
  0a:b2:ac:b2:17:67:57:ae:55:b9:88:51:92:45:6b:12:23:05:
  ce:6a
```

8. Submit the CSR according to the guidelines of the selected CA.

- This information varies depending on which CA you are using. Consult your CA for information on how to submit your CSR.

Once the CSR has been processed you will receive a signed certificate. The next step is to import the new server certificate in the StoneGate SSL VPN Administrator and change the Administrator to use it. Proceed to Activating a Signed Certificate.

# Activating a Signed Certificate

---

**Note** – If your certificate is a bundled certificate, which may contain intermediate certificates, you must split the certificate before adding it to the StoneGate SSL VPN Administrator. See [TN2068 Adding Bundled Certificates](#) for information on how to do this.

---

## ▼To activate the new certificate in StoneGate SSL VPN Administrator

1. Log in to the StoneGate SSL VPN Administrator, and go to the **Manage System** section.
2. Click the **Certificates** link in the menu on the left and select **Add Server Certificate...**
3. Enter a suitable display name and enter the paths to the certificate and private key files (use the key file with the .pk8 extension). If you created an encrypted key when you generated the certificate request, enter the same password here.
4. Click **Save**.
5. Click the **Administration Service** link in the menu on the left.
6. Change the **Server Certificate** selection to the new certificate and click **Save** at the bottom of the page.
7. Click the **Access Points** link in the menu on the left and select the access point to open its details.
8. Change the **Server Certificate** selection to the new certificate and click **Save** at the bottom of the page.

## Feedback

---

Stonesoft is always interested in feedback from our users.

- For comments regarding Stonesoft's products, contact [feedback@stonesoft.com](mailto:feedback@stonesoft.com).
- For comments regarding this technical note, contact [documentation@stonesoft.com](mailto:documentation@stonesoft.com).

## Trademarks and Patents

Stonesoft, the Stonesoft logo and StoneGate are all trademarks or registered trademarks of Stonesoft Corporation. Multi-link technology, multi-link VPN, and the StoneGate clustering technology-as well as other technologies included in StoneGate-are protected by patents or pending patent applications in the U.S. and other countries. All other trademarks or registered trademarks are property of their respective owners.

SSL VPN Powered by PortWise

## Copyright and Disclaimer

Copyright © 2000–2008 Stonesoft Corporation. All rights reserved.

These materials, Stonesoft products and related documentation are protected by copyright and other laws, international treaties and conventions. All rights, title and interest in the materials, Stonesoft products and related documentation shall remain with Stonesoft and its licensors. All registered or unregistered trademarks in these materials are the sole property of their respective owners. No part of this document or related Stonesoft products may be reproduced in any form, or by any means without written authorization of Stonesoft Corporation.

Stonesoft provides these materials for informational purposes only. They are subject to change without notice and do not represent a commitment on the part of Stonesoft. Stonesoft assumes no liability for any errors or inaccuracies that may appear in these materials or for incompatibility between different hardware components, required BIOS settings, NIC drivers, or any NIC configuration issues. Use these materials at your own risk. Stonesoft does not warrant or endorse any third party products described herein.

THESE MATERIALS ARE PROVIDED "AS-IS." STONESOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO, THE INFORMATION CONTAINED HEREIN. IN ADDITION, STONESOFT MAKES NO EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE WITH RESPECT THE INFORMATION CONTAINED IN THESE MATERIALS.

IN NO EVENT SHALL STONESOFT BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL OR INCIDENTAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING FROM THE USE OF THESE MATERIALS, EVEN IF ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH DAMAGES.

SG\_SVTN\_2073\_20080520

---

**STONESOFT**

**Stonesoft Corp.**

Itälahdenkatu 22a

FIN-00210 Helsinki

Finland

tel. +358 9 4767 11

fax +358 9 4767 1234

[www.stonesoft.com](http://www.stonesoft.com)

**Stonesoft Inc.**

1050 Crown Pointe Parkway

Suite 900

Atlanta, GA 30338 USA

tel. +1 770 668 1125

fax +1 770 668 1131