

## Heartbleed Venafi TrustAuthority Directions

With Venafi TrustAuthority you have the ability to generate all new private keys and certificates. You can utilize this to help recover from the OpenSSL Heartbleed bug.

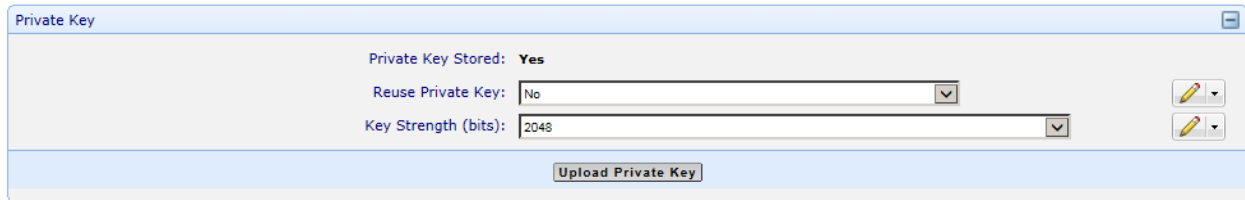
<https://support.venafi.com/entries/51178636>

General Steps:

1. Discover what Servers are at risk or vulnerable.
2. Locate them in the Policy tree and process them.  
\*Advised to replace all keys and certificates
3. Deliver the new keys and certificates to the applications they belong on.

### \*Rotate keys

Note: Ensure your certificate does not have the "Reuse Private key" option selected



Private Key

Private Key Stored: Yes

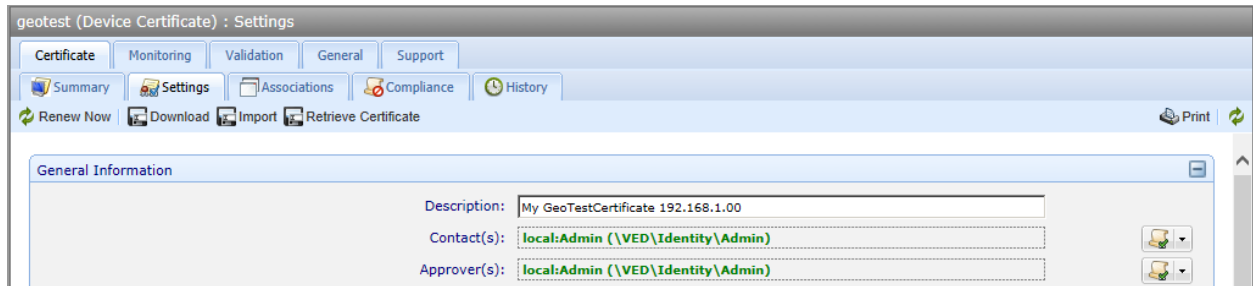
Reuse Private Key: No

Key Strength (bits): 2048

Upload Private Key

One at a time:

1. Press Renew one at a time on your certificate object



geotest (Device Certificate) : Settings

Certificate Monitoring Validation General Support

Summary Settings Associations Compliance History

Renew Now Download Import Retrieve Certificate Print

General Information

Description: My GeoTestCertificate 192.168.1.00

Contact(s): local:Admin (\\VED\\Identity\\Admin)

Approver(s): local:Admin (\\VED\\Identity\\Admin)

2. Download your renewed certificate and key.

**Download Certificate**

Include Private Key:

Include Root Chain:

Format:  Base64 (PKCS #8)  
 Base64 (OpenSSL)  
 DER  
 PKCS #7  
 PKCS #12

Friendly Name:

Password:

Confirm Password:

Download Cancel

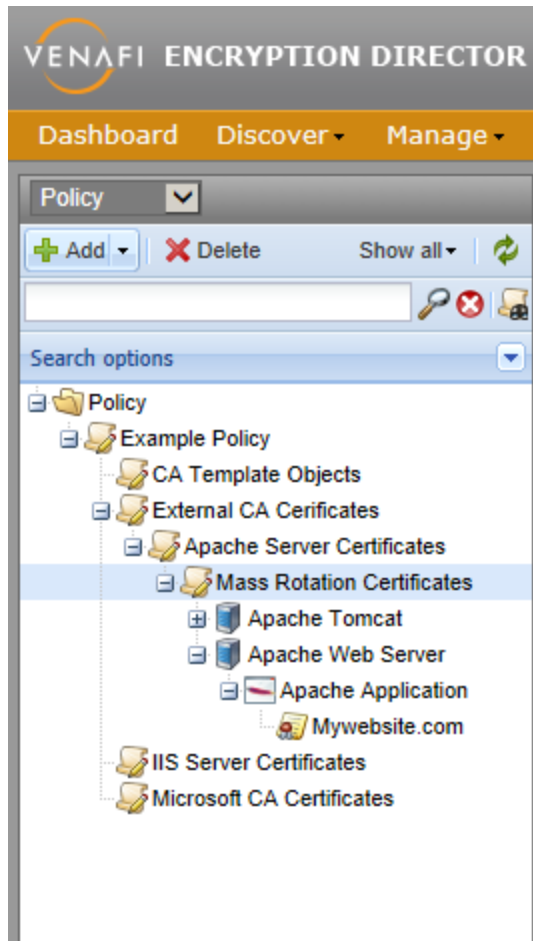
3. Manually transport the certificate and key to your end application.

Mass rotation:

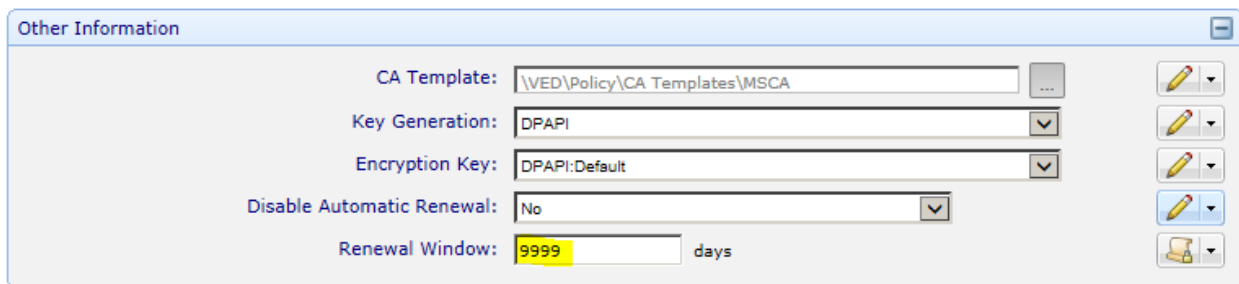
NOTE: Best practice is that certificates are only valid for 1 year or less

NOTE: May have to revoke first or set certs to replace. Depends on the CA (VeriSign)

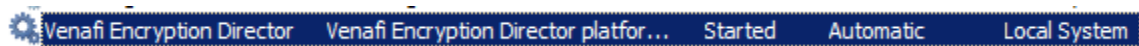
1. Configure a policy object containing your keys to renew to auto renew in a quantity of days greater than your expiration date of certs. Default = 30 days  
\*Recommended to set at root Policy object to rotate all keys and certificates



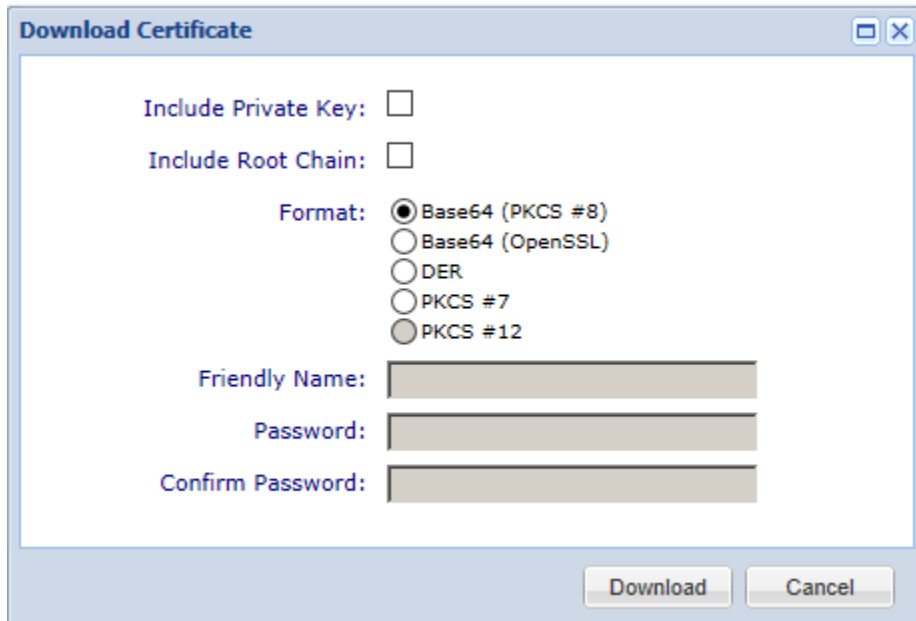
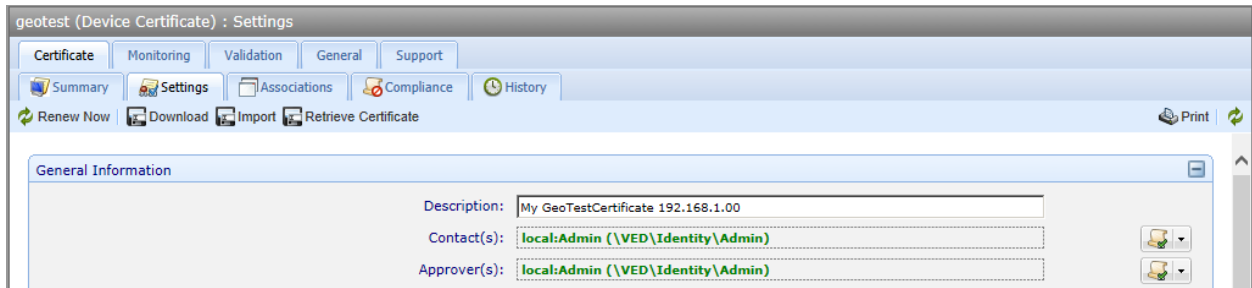
2. Configure auto renew days to a greater number than your expiration. Default = 30 days.



3. Restart your VED service to immediately initiate your processing.



4. Download your newly completed certificates and keys for manual distribution to applications.



**\*Provide Key rotation evidence**

How do you prove that you have rotated your keys?

1. View Certificate list within Policy tree Excel export check Valid from dates. If it is newer than your patch date you are good.

Managed DN	Common Name	Status	Last Validation	Last Validation ...	Valid From	Valid To	Subject DN	Issuer DN	Type
WEDI/Policy/UT/...	alskdifo.venafi...	OK	04/10/2014 03:1...	Failure, ScanHo...	11/27/2013	11/27/2014	CN=alskdifo.ven...	CN=CA-CentO...	Server
WEDI/Policy/UT/...	ooqahboogah.v...	OK	04/10/2014 03:1...	Failure, ScanHo...	11/27/2013	11/27/2014	CN=ooqahboog...	CN=CA-CentO...	Server
WEDI/Policy/UT/...	FerrisAW.venaf...	OK	04/10/2014 03:1...	Success, Scan...	11/13/2013	12/16/2014	CN=FerrisAW.v...	CN=GlobalSign...	Server
WEDI/Policy/UT/...	lists.eng.venafi...	OK	04/10/2014 03:1...	Success, Scan...	10/18/2013	06/11/2014	CN=lists.eng.ve...	CN=Ven-CA01,...	Server

2. If someone does not get the new certificate out to the application and you do your nightly Validation. You will be alerted that your new certificate does not match the certificate out on the application and you can then take steps to correct it.

Validation Failure : Settings

Notification

General

Settings

Print

General

Disabled:

Rules

IF

Event ID

matches

Validation Failed

Target Channels

Target Channel:

\\VED\Logging\Channels\Email to Owner

