Heartbleed Venafi TrustForce Directions

With Venafi TrustForce you have the ability to generate all new private keys and certificates and securely deliver them to their applications. You can utilize this to help recover at maximum speed from the OpenSSL Heartbleed bug.

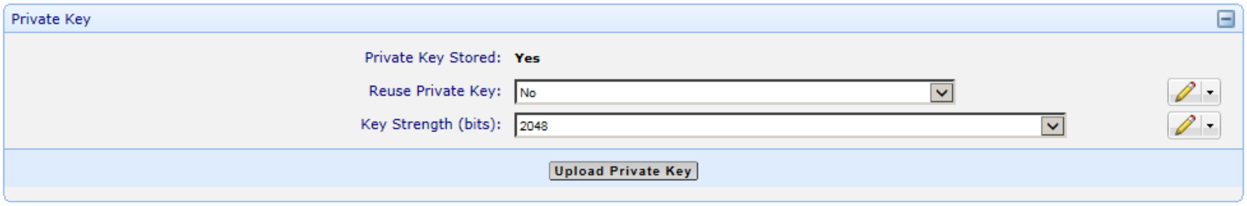
https://support.venafi.com/entries/51178636

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. Securely 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



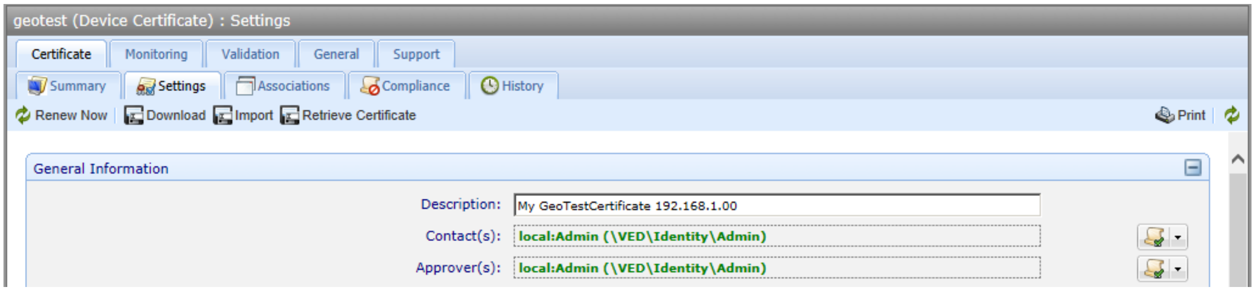
Private Key Stored: Yes

Reuse Private Key: No

Key Strength (bits): 2048

One at a time:

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

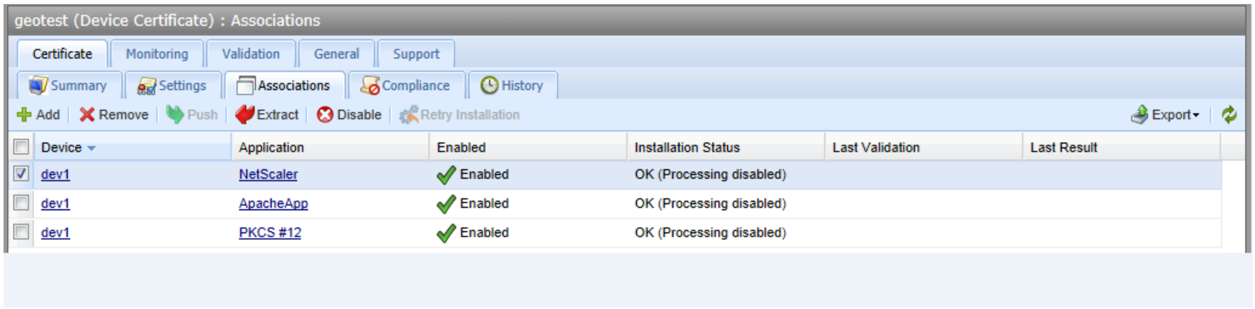


Description: My GeoTestCertificate 192.168.1.00

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

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

2. Your certificate will be processed and securely placed into your certificate's associated applications.



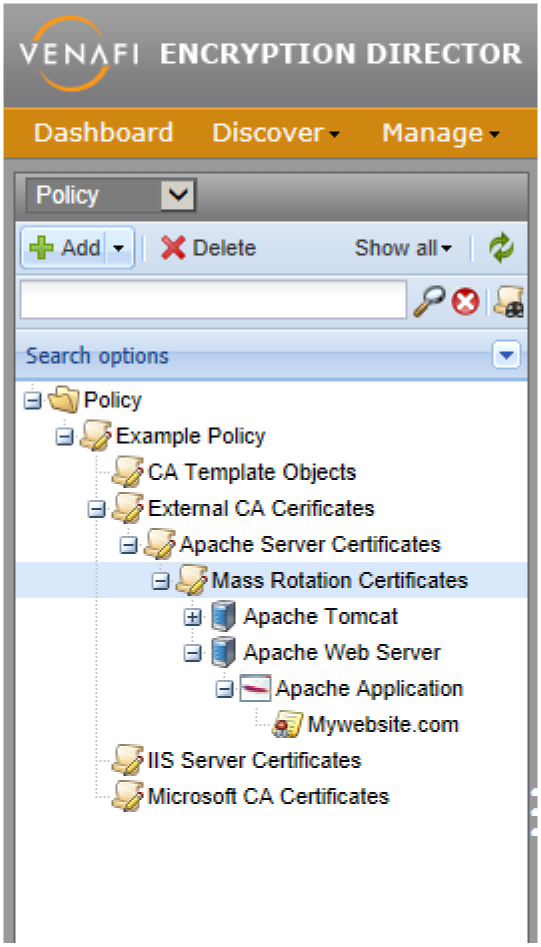
	Device	Application	Enabled	Installation Status	Last Validation	Last Result
☑	dev1	NetScaler	✓ Enabled	OK (Processing disabled)		
□	dev1	ApacheApp	✓ Enabled	OK (Processing disabled)		
□	dev1	PKCS #12	✓ Enabled	OK (Processing disabled)		

Mass rotation:

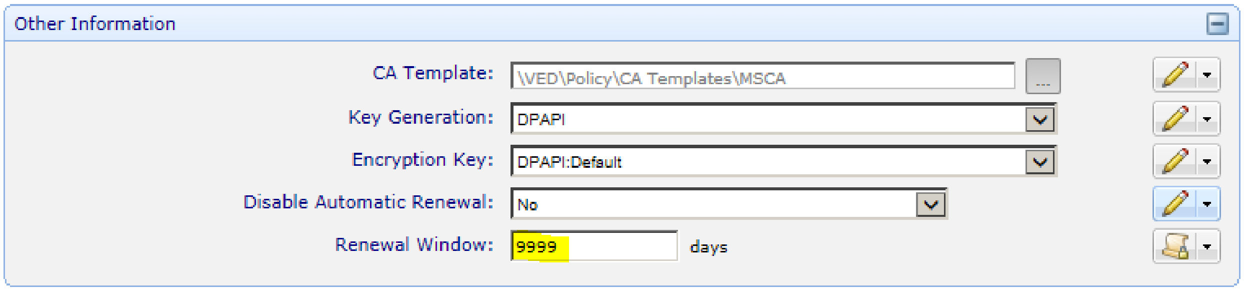
NOTE: Best practice is that certificates are only valid for 1 year or less

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.



2. Setting it to 9999 is about a 27 yr. cert so anything expiring before 27 years should renew.



Other Information

CA Template: \VED\Policy\CA Templates\MSCA

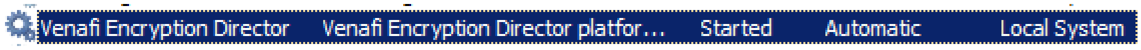
Key Generation: DPAPI

Encryption Key: DPAPI:Default

Disable Automatic Renewal: No

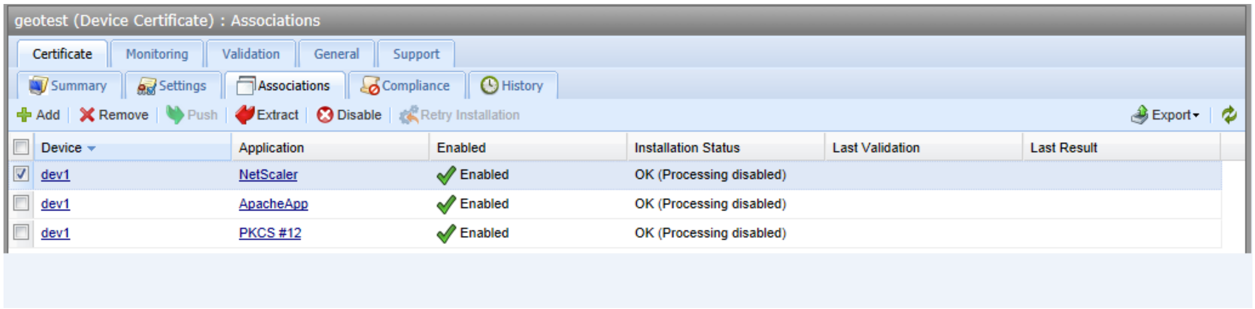
Renewal Window: 9999 days

3. Restart your services for immediate certificate processing.



Venafi Encryption Director	Venafi Encryption Director platfor…	Started	Automatic	Local System

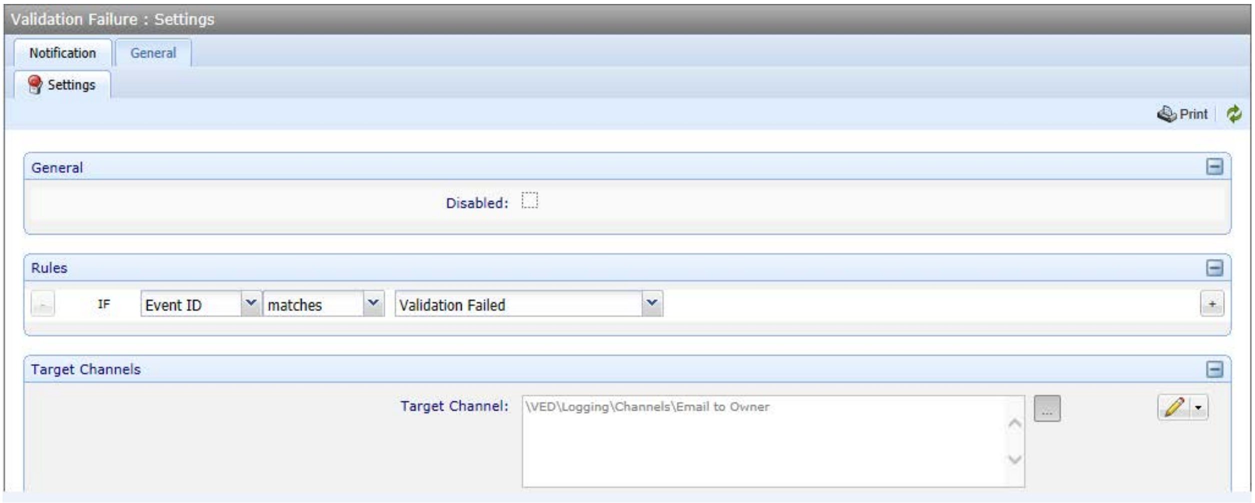
4. Your certificates will all be processed and securely delivered to your applications.



geotest (Device Certificate) : Associations

☐	Device	Application	Enabled	Installation Status	Last Validation	Last Result
☑	dev1	NetScaler	✓ Enabled	OK (Processing disabled)		
☐	dev1	ApacheApp	✓ Enabled	OK (Processing disabled)		
☐	dev1	PKCS #12	✓ Enabled	OK (Processing disabled)		

5. If your certificate for some reason does not get correctly sent to your application you will be notified upon a failed validation.



Validation Failure : Settings

General

Disabled: ☐

Rules

IF Event ID matches Validation Failed

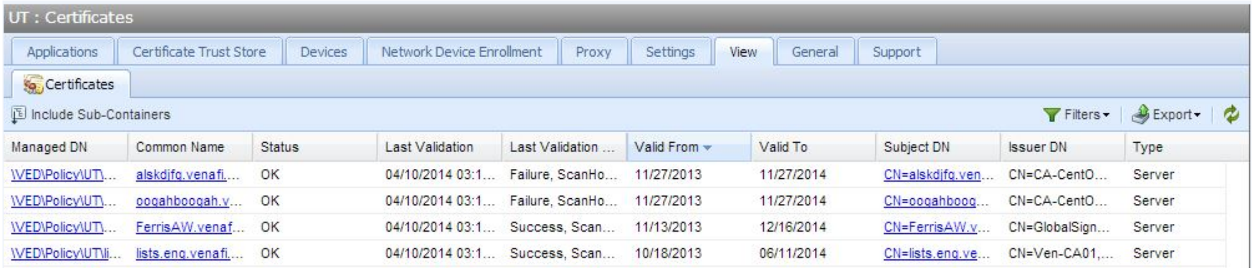
Target Channels

Target Channel: \VED\Logging\Channels\Email to Owner

*Provide Key rotation evidence

How do you prove that you have rotated your keys?

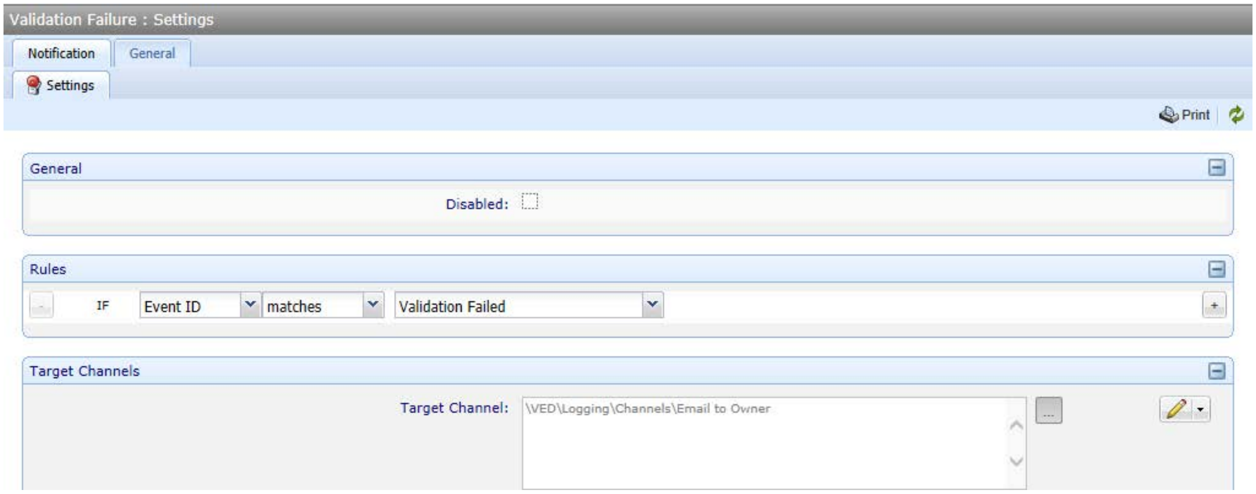
1. Discover certs again and view new Valid from column or in your Policy tree go to View Certificates and select Include Sub Containers.



UT : Certificates

Managed DN	Common Name	Status	Last Validation	Last Validation …	Valid From	Valid To	Subject DN	Issuer DN	Type
\VED\Policy\UT\…	alskdjfg.venafi.…	OK	04/10/2014 03:1…	Failure, ScanHo…	11/27/2013	11/27/2014	CN=alskdjfg.ven…	CN=CA-CentO…	Server
\VED\Policy\UT\…	oogahboogah.v…	OK	04/10/2014 03:1…	Failure, ScanHo…	11/27/2013	11/27/2014	CN=oogahboog…	CN=CA-CentO…	Server
\VED\Policy\UT\…	FerrisAW.venaf…	OK	04/10/2014 03:1…	Success, Scan…	11/13/2013	12/16/2014	CN=FerrisAW.v…	CN=GlobalSign…	Server
\VED\Policy\UT\li…	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. View Certificate list within Policy tree. If the Valid From date is newer than your patch date you are good.
3. 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

General

Disabled: □

Rules

IF Event ID matches Validation Failed

Target Channels

Target Channel: \VED\Logging\Channels\Email to Owner