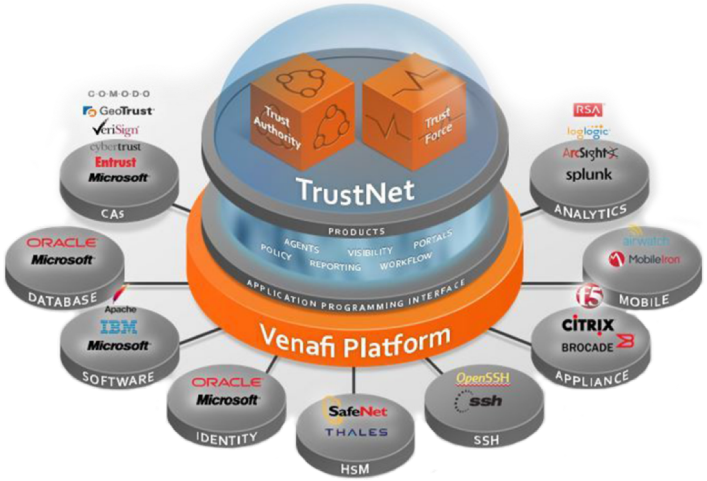
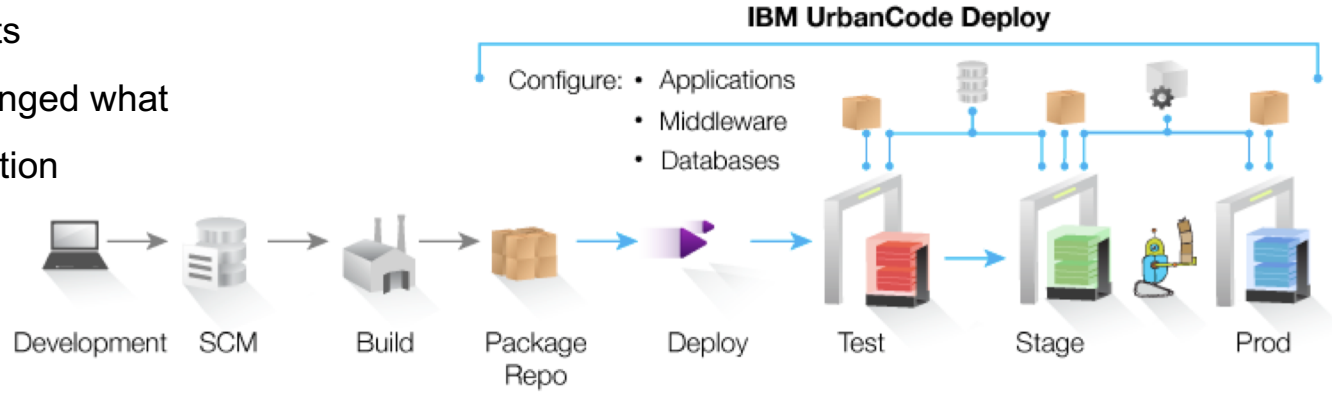
UrbanCode Deploy plugin for Venafi Trust Protection Platform

Mark Roberts
UrbanCode Technical Specialist

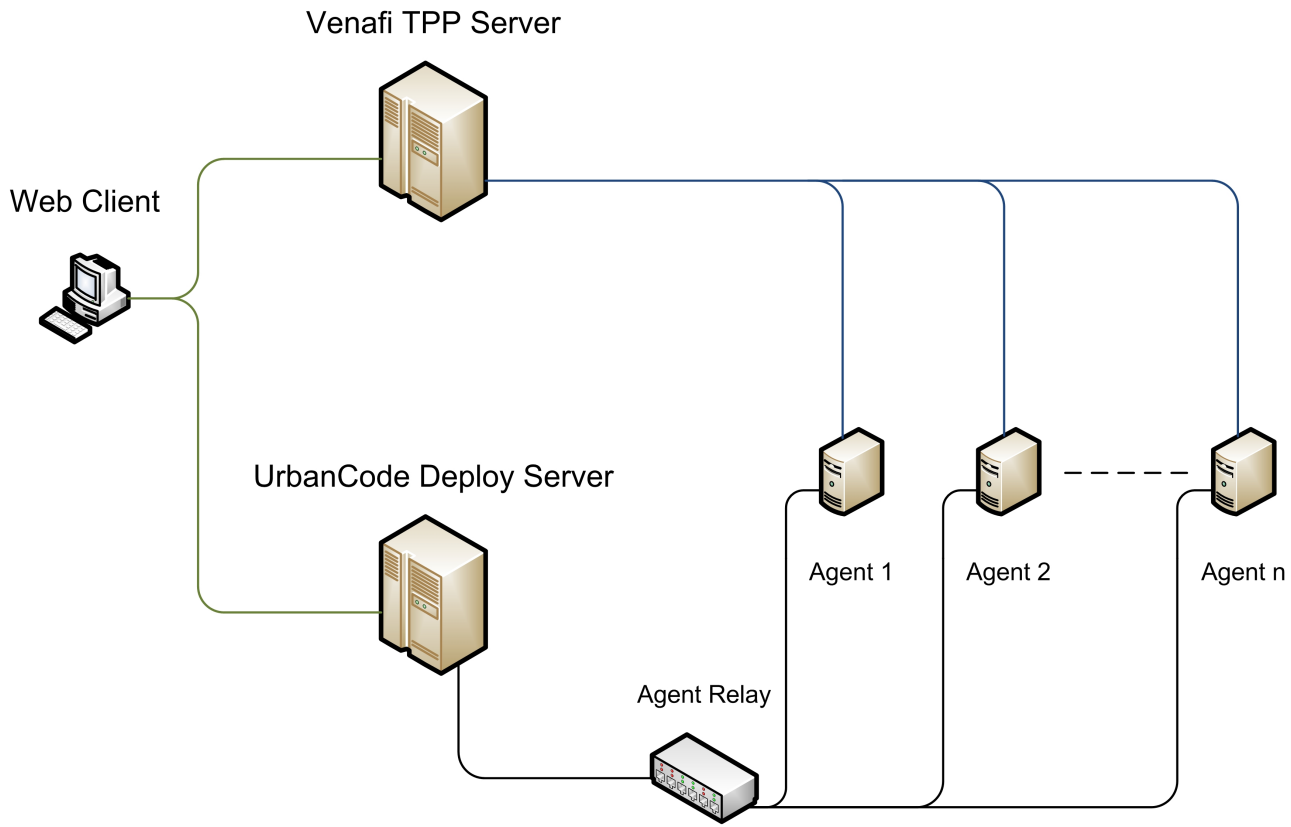
Venafi Trust Protection Platform & UrbanCode Deploy

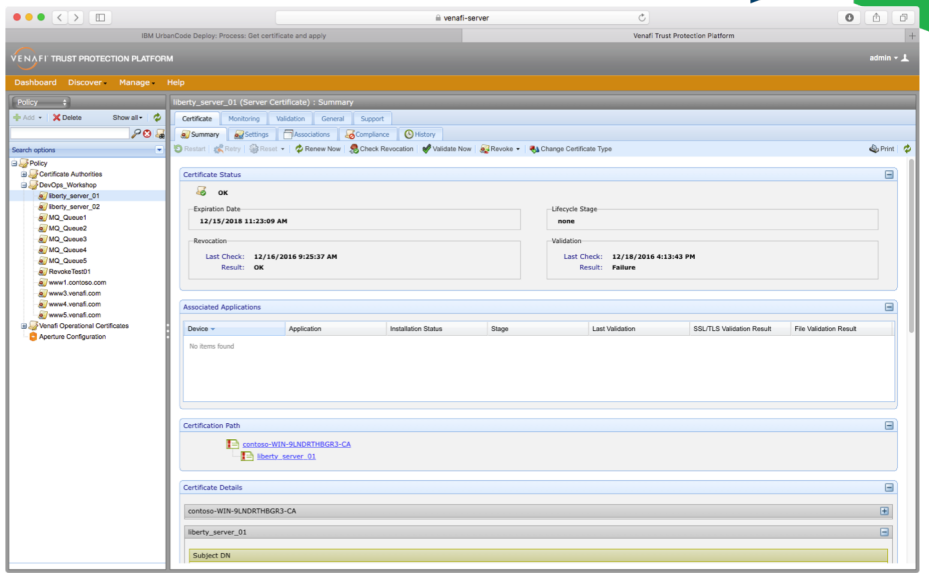
- Venafi Trust Protection Platform provides
  - Visibility and control over keys and certificates
  - Management of keys and certificates across mobile, desktops, application servers, devices
  - An ever-evolving intelligent response
  - Enforce security policy
  - Continuous monitoring of keys and certificates
- IBM UrbanCode Deploy provides
  - Automated, consistent deployments and rollbacks of application
  - Automated provisioning, updating, and de-provisioning of cloud environments
  - A plugin framework for technology specific extensions – Over 180 plugins available
  - Orchestration of changes across servers, tiers and components
  - Clear inventory visibility: what is deployed where and who changed what
  - Integrated with middleware, provisioning and service virtualization
  - Configuration and security differences across environments
  - Underpin your DevOps strategy

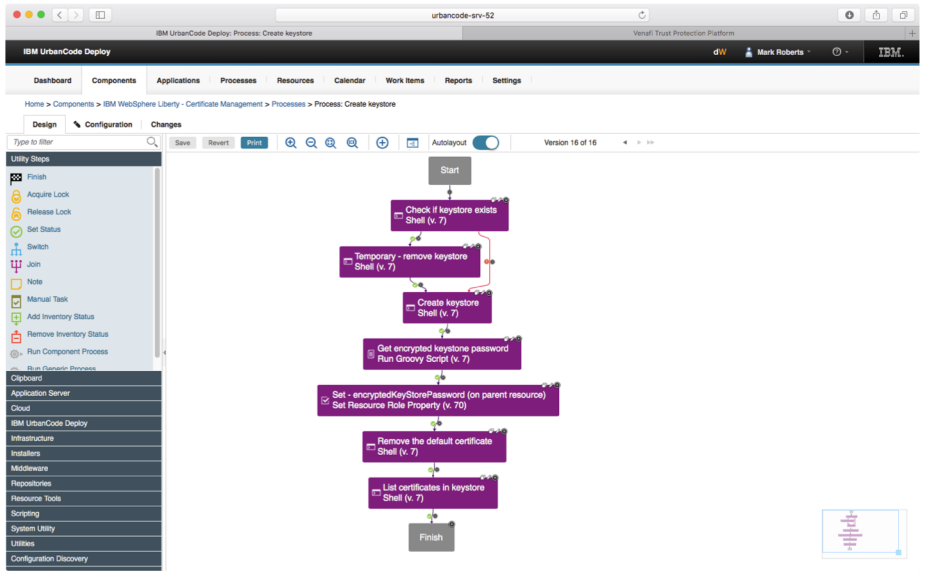




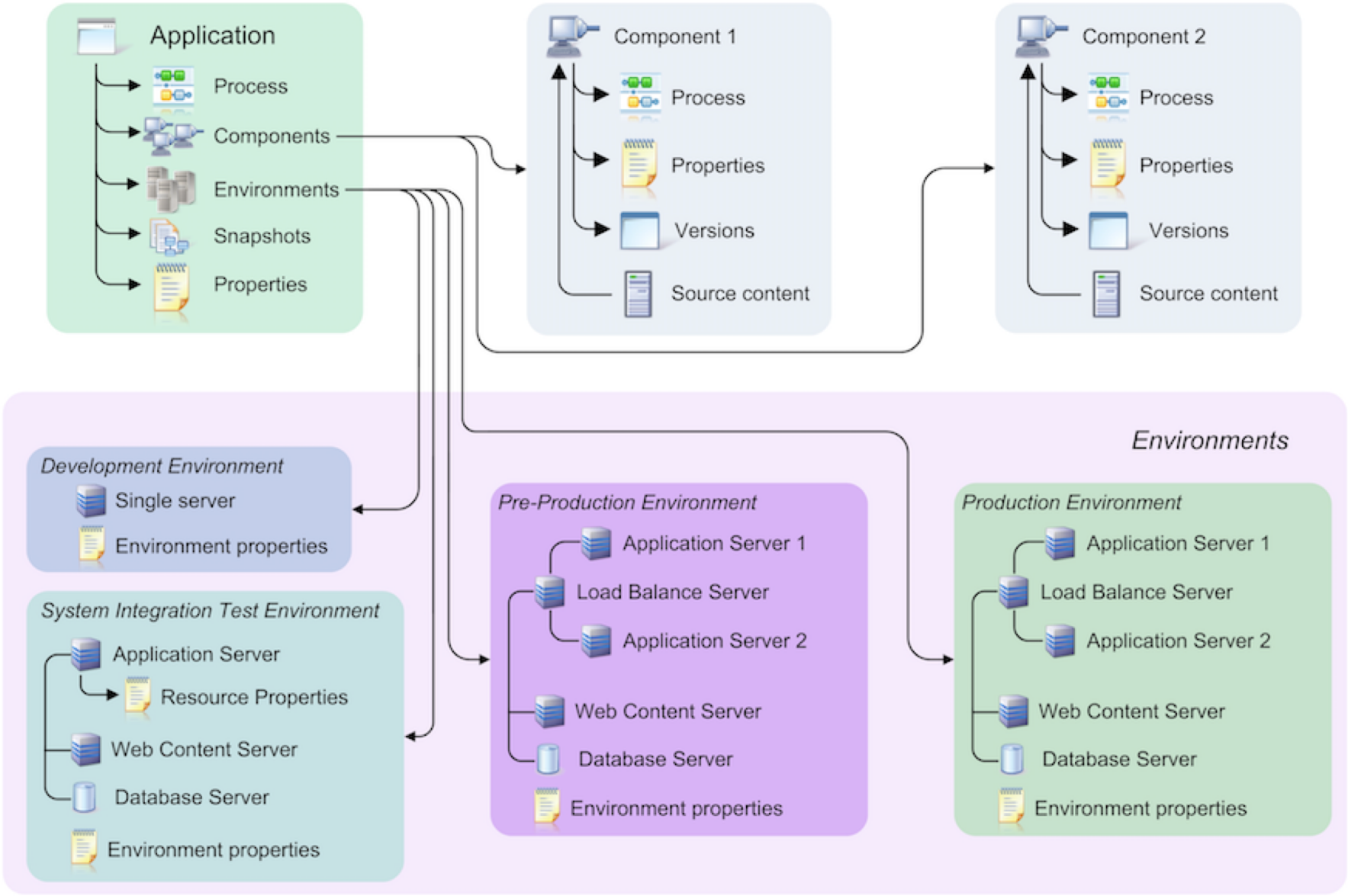
Physical Infrastructure and Interaction







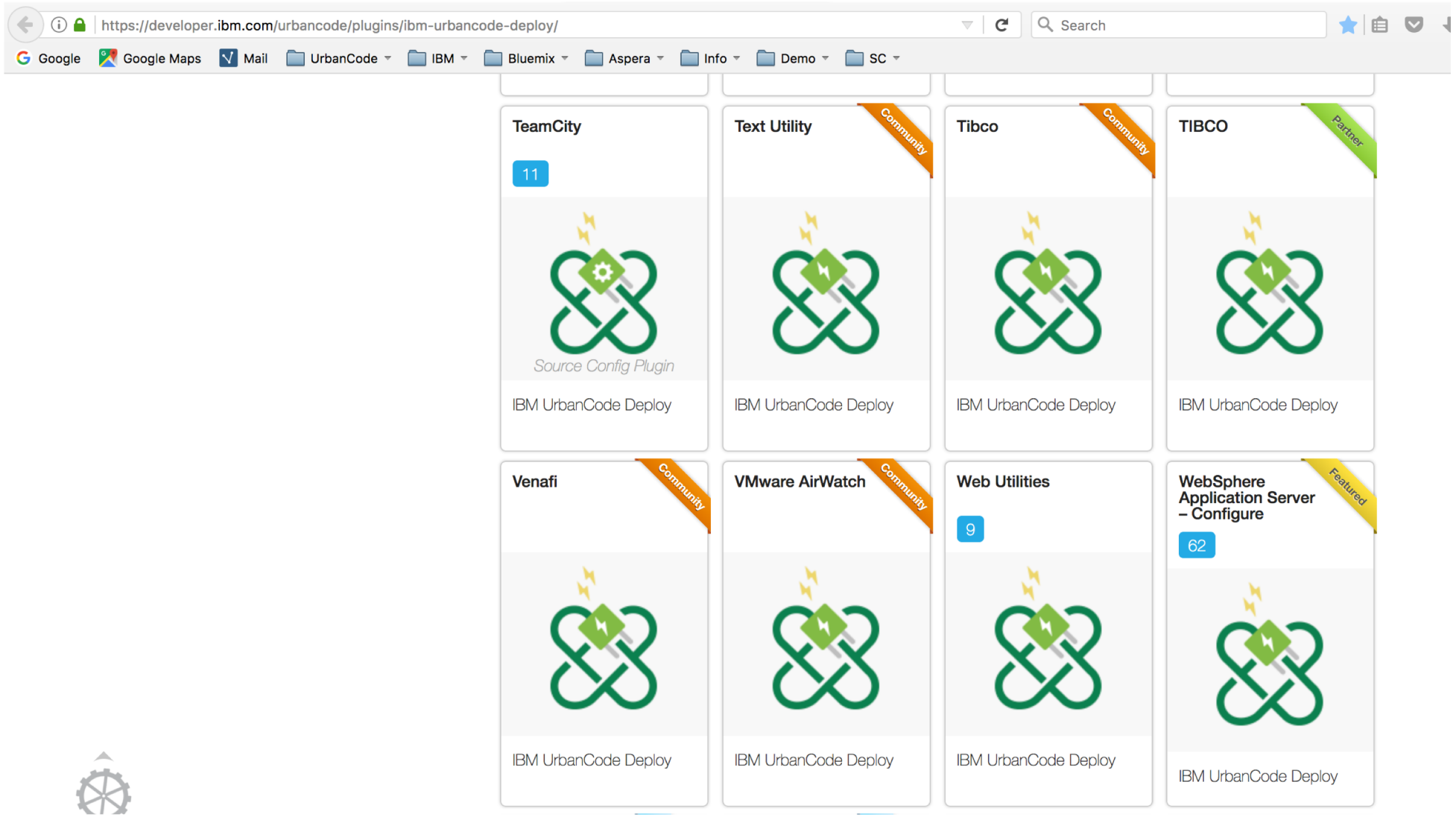
UrbanCode Deploy Application Structure



UrbanCode Deploy Plugins

- Over 200 plugins available
- Provided by IBM, UrbanCode user community, partner organisations, IBM specialists
- Written in Groovy
- Interact with third parties using direct API's, REST interfaces, HTTPS communication
- Customers are encouraged to create plugins for their specific needs
- Development process
  - Create standard plugin file and directory structure
  - Add technology specific libraries and interfaces
  - Create test harness scripts and simulated input data files
  - Validate plugin code
  - Create plugin.xml file to connect plugin code to the UrbanCode Deploy user interface to create steps

https://developer.ibm.com/urbancode/plugins/ibm-urbancode-deploy/



Functions available in the Venafi plugin

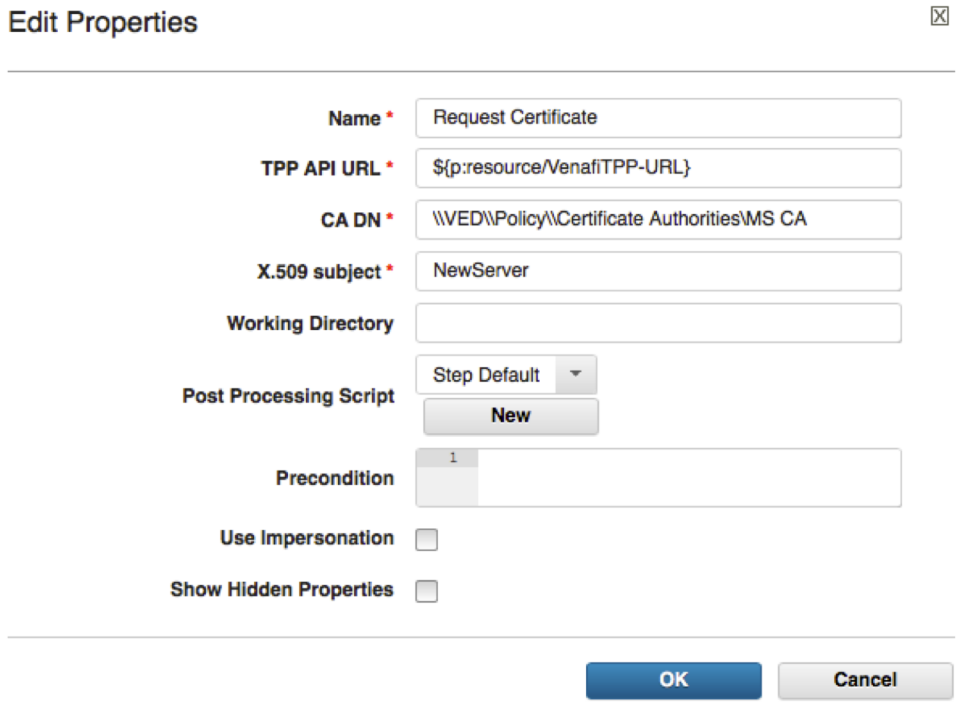
- Authentication test – Validate communications with the Venafi TPP server.
- Request certificate – Request a certificate from Venafi. The certificate is not delivered as a part of this step.
- Retrieve certificate – Retrieve a certificate from Venafi.
- Request certificate wait – Request a certificate and wait for it to be returned by Venafi.
- Get certificate status – Gather information about a specific certificate.
- Validate remaining days – Validate whether a certificate will stil be valid after a specific number of days.
- Revoke certificate – Revoke a certificate on Venafi.
- Renew certificate – Renew a certificate on the Venafi. The certificate is not delivered as a part of this step.
- New Steps …
- *Generate certificate CSR – Create a certificate signing request that may then be submitted to Venafi.*
- *Get Venafi Policy – Retreive the details of the Venafi policy associated with a specific policy folder.*
- *Submit CSR to Venafi – Submit the previously created CSR to Venafi for processing.*
- *Submit custom fields to Venafi – Suppliment a previously submitted certificate request with custom field values.*

Request certificate

- Request a new certificate is created
- Certificate is not downloaded at this time
- Provide
  - URL to the TPP Server and username / password
  - Certificate authority distinguished name
  - X.509 Subject (server or service for which the certificate is required)
- Output

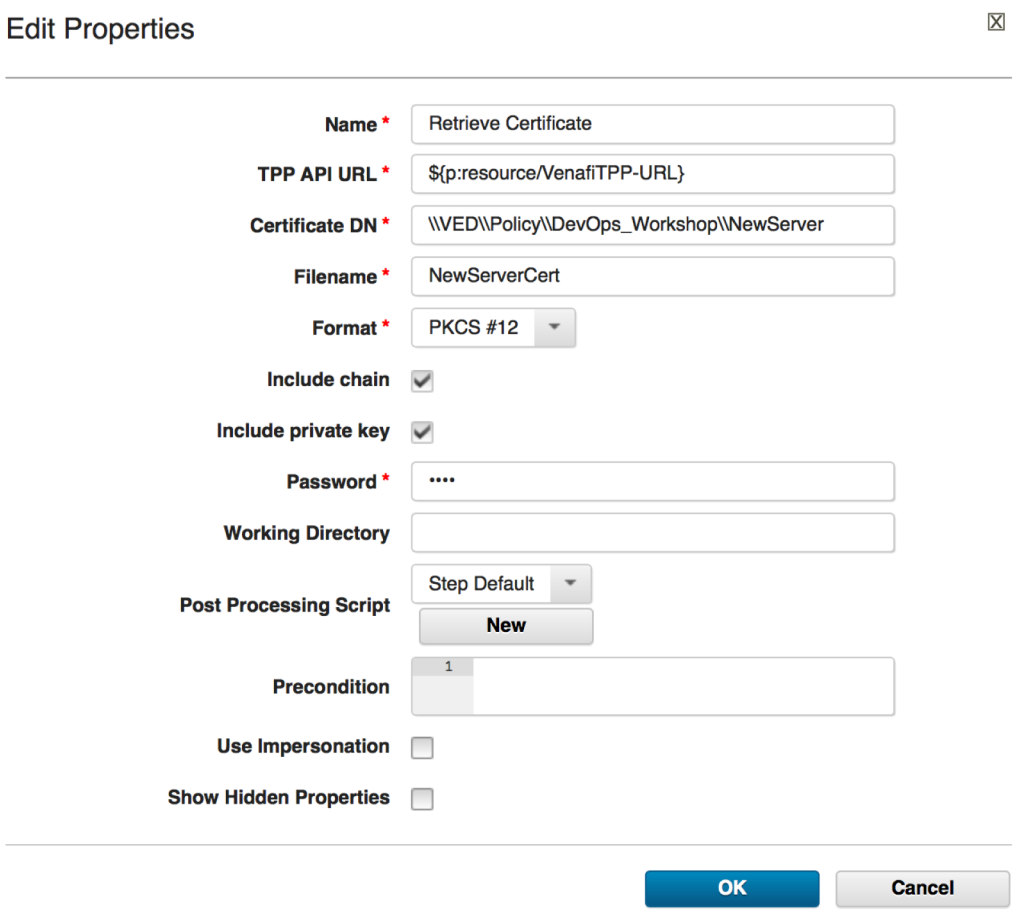
Output Properties - View Input Properties

Name	Value
certificateDN	\VED\Policy\NewServer
exitCode	0
LOI	
Status	Success
x509Subject	NewServer



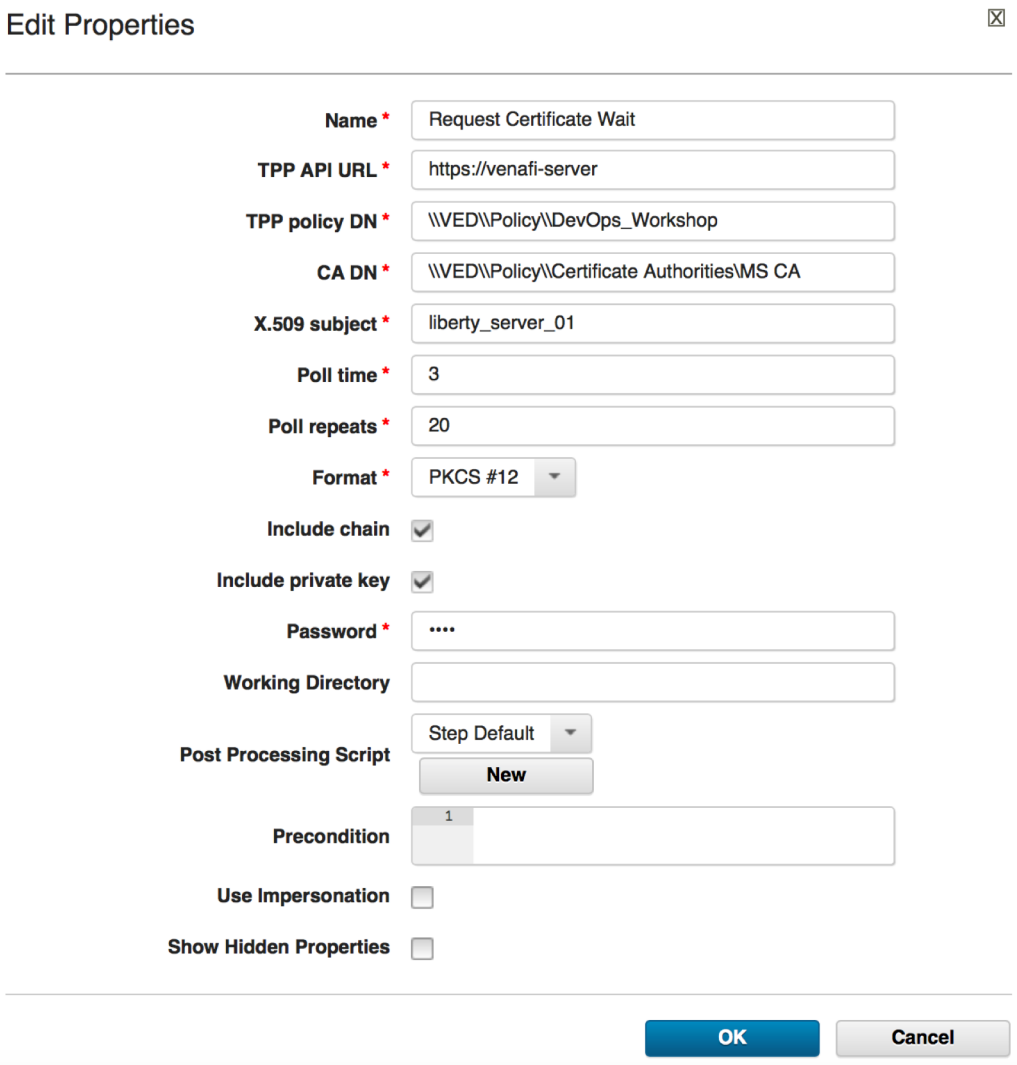
Retrieve certificate

- Retrieve an existing certificate from the Venafi TPP server
- Option to download the certificate chain and the private key
- Provide
  - URL to the TPP Server and username / password
  - Certificate authority distinguished name
  - Filename – Note that the extension is based on certificate format
  - Format – currently only P12
  - Password - A password to protect the downloaded package
- Output
  - Includes the filename for reference by further steps
  - Includes status to show successful retrieval



Request certificate - Wait

- Request a certificate from the Venafi TPP server and wait for it to be available
- Option to download the certificate chain and the private key
- Provide
  - URL to the TPP Server and username / password
  - Certificate authority distinguished name
  - Policy distinguished name – folder in TPP to hold the certificate
  - Filename – Note that the extension is based on certificate format
  - Format – currently only P12
  - Password - A password to protect the downloaded package
  - Poll time (wait between tries to get certificate)
  - Poll repeats (number of times to ask
- Output
  - Includes the filename for reference by further steps
  - Includes status to show successful retrieval

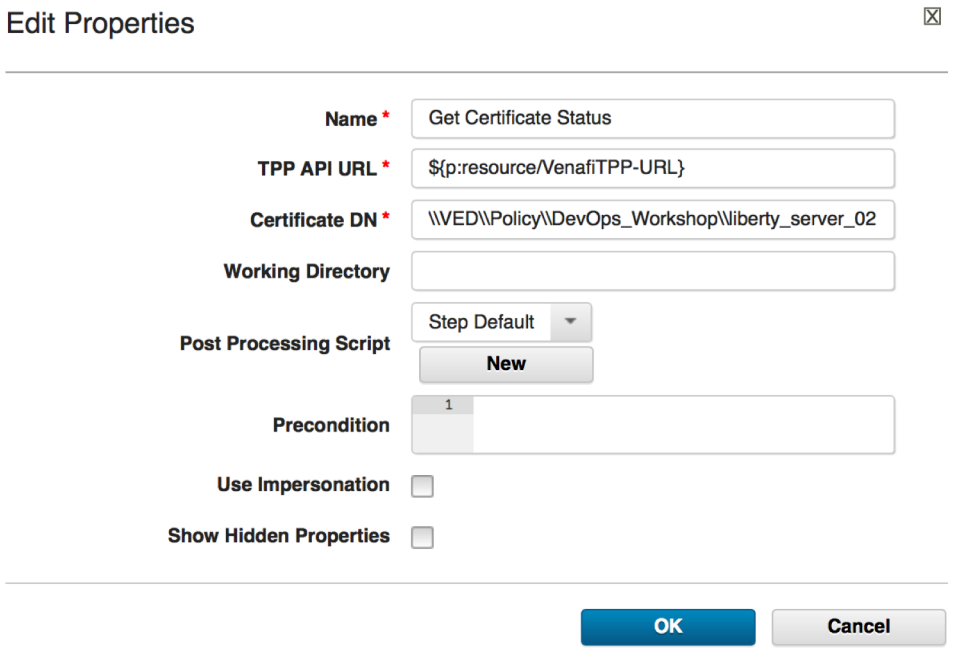


Get certificate status

- Gather information about a certificate
- Provide
  - URL to the TPP Server and username / password
  - Certificate distinguished name

Output Properties - View Input Properties

Name	Value
approverDN	\VED\Identity\admin
approverGUID	local:{6d81fc0d-502b-4ede-a925-0e77e1e30fc4}
contactDN	\VED\Identity\admin
contactGUID	local:{6d81fc0d-502b-4ede-a925-0e77e1e30fc4}
daysRemaining	730
exitCode	0
keySize	2048
LOI	
processingStage	N/A
processingStatus	N/A
Ready	true
signatureAlgorithm	sha256RSA
Status	Success
validFor	730
validFrom	2016-12-20T07:22:54.0000000Z
validTo	2018-12-20T07:22:54.0000000Z

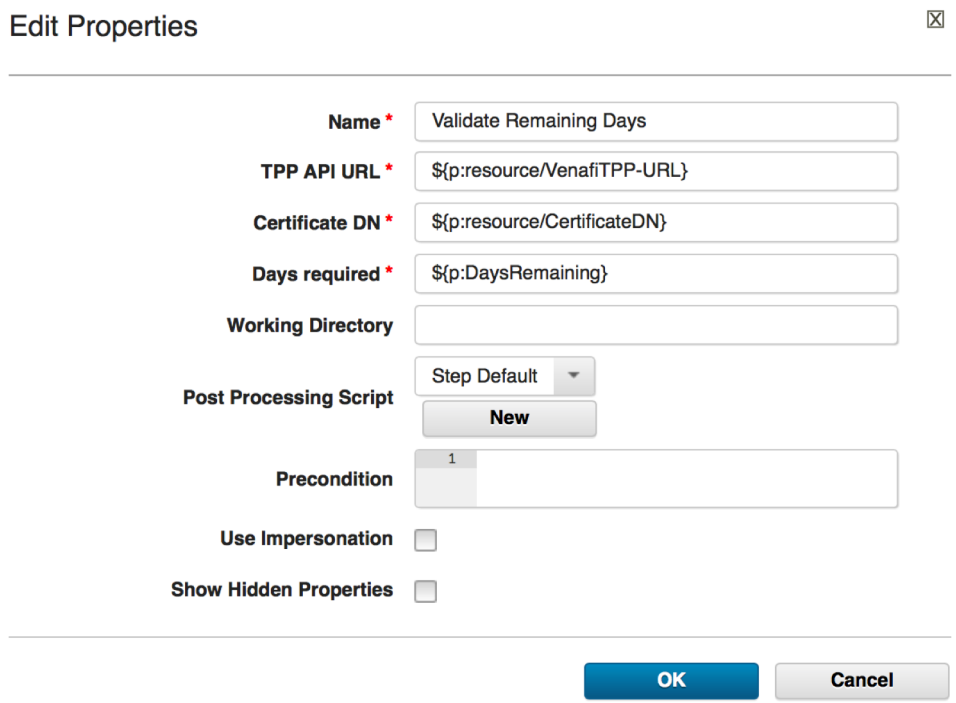


Validate remaining days

- Validate that a certificate is valid for at least a specific number of days
- Provide
  - URL to the TPP Server and username / password
  - Certificate distinguished name
  - Number of days for which the certificate should be valid
  - Dremaining is passed as a component process property in this example
- Step result
  - Step will fail if it cannot connect to Venafi server of find the certificate
  - Step will pass and report validity in ‘CertificateOK’
- Output

Output Properties - View Input Properties

Name	Value
CertificateOK	false
daysRemaining	729

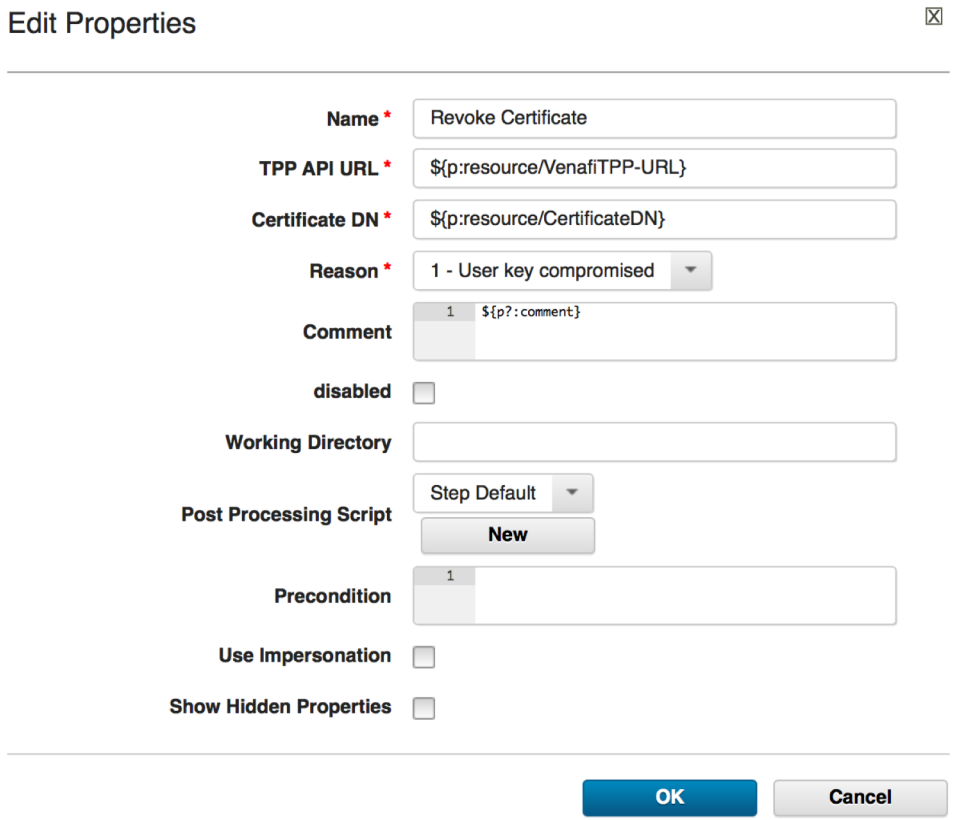


Revoke certificate

- Revoke a certificate on the Venafi TPP server
- Provide
  - URL to the TPP Server and username / password
  - Certificate distinguished name
  - Reason :
    - 1 – User key compromised
    - 2 – CA key compromised
    - 3 – User changed affiliation
    - 4 – Certificate superseded
    - 5 – Original use no longer valid
  - Comment – Optional component process property in example
- Step result

Output Properties - View Input Properties

Name	Value
exitCode	0
LOI	
RevokeStatus	true
Status	Success

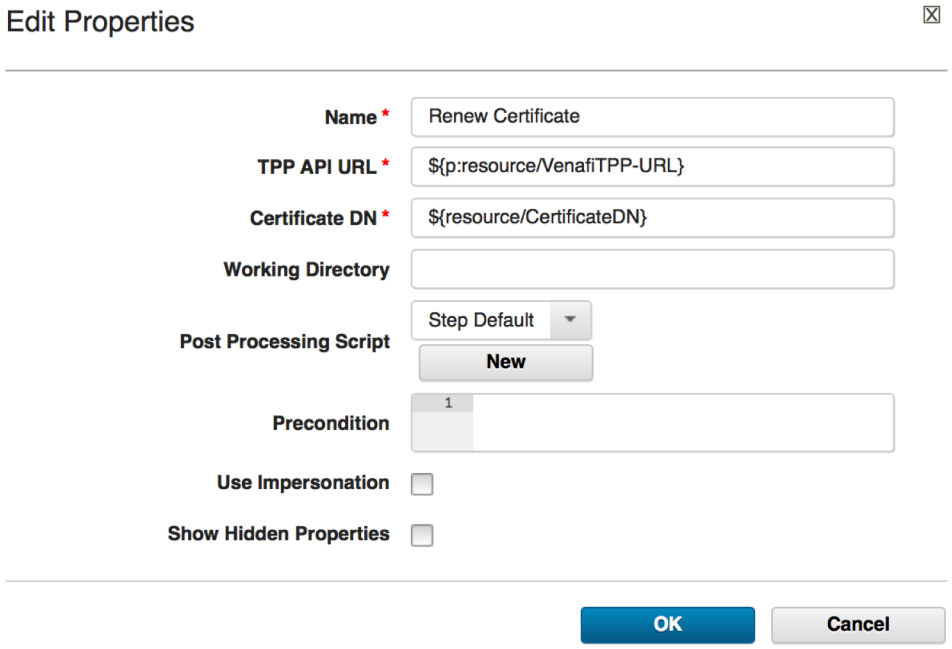


Renew certificate

- Renew a certificate on the Venafi TPP server
- Does not necessarily have to be a revoked certificate
- Does not download the certificate – need a retrieve certificate step
- Provide
  - URL to the TPP Server and username / password
  - Certificate distinguished name
- Step result

Output Properties - View Input Properties

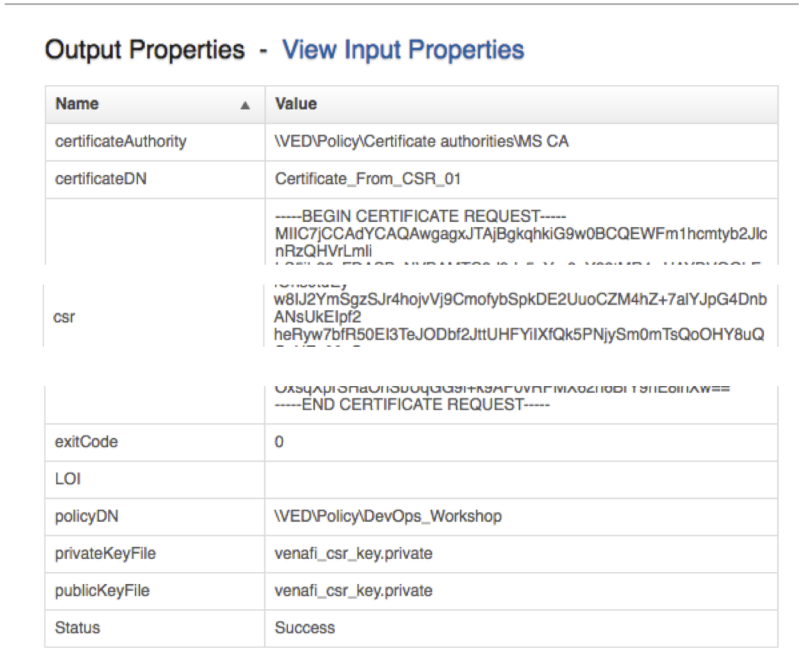
Name	Value
exitCode	0
LOI	
RenewalStatus	true
Status	Success

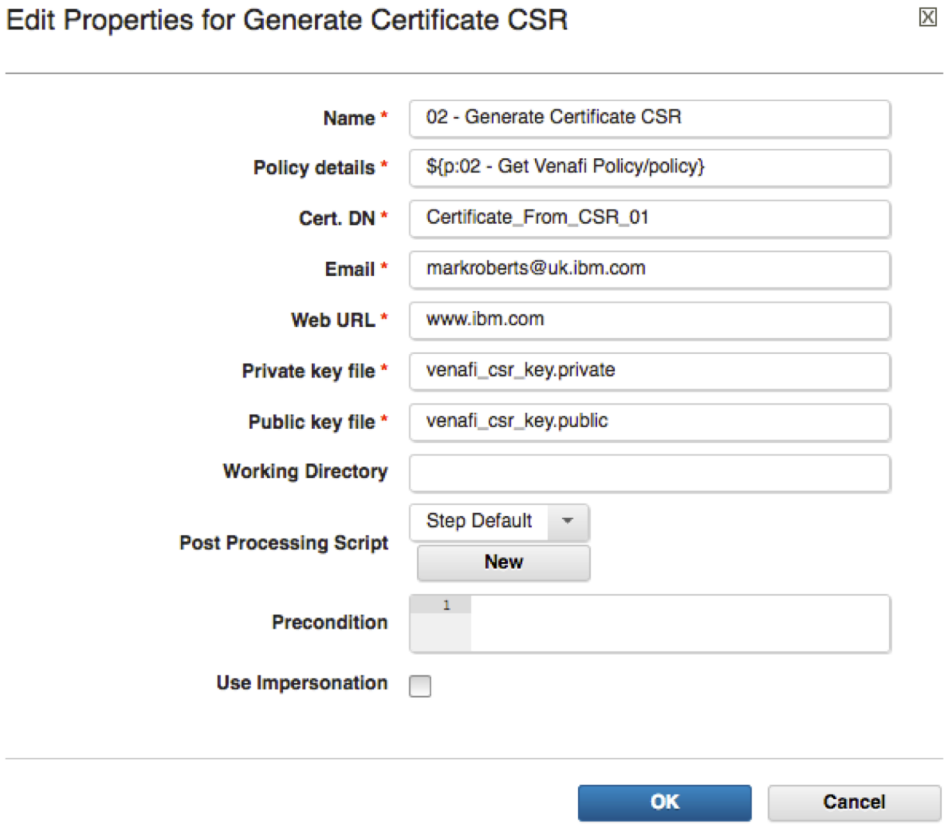


Generate certificate CSR

- Generate a CSR which is stored as an output property of the step. The CSR is not written to a file by this step.
- Uses the JSON formatted policy data from the step ‘Get Venafi Policy’
- Certificate DN – (actually the certificate Name)
- Public and private key files are written to the working directory of the step on the target on which the agent is installed
- Output Properties

(CSR text is cropped)



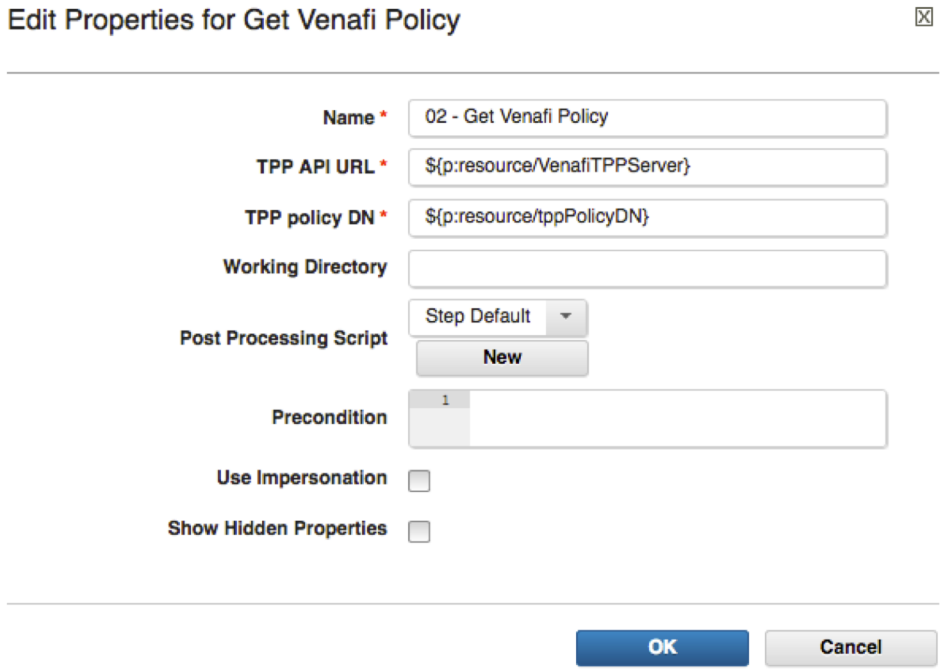


Get Venafi Policy

- Get the Venafi policy details for a specific folder
- Output is in JSON format as shown below
- Output Properties
  - City, state, country, organization, organizational unit
  - Key algorithm, Key bit strength, management type, manual CSR
  - Certificate authority, policy DN

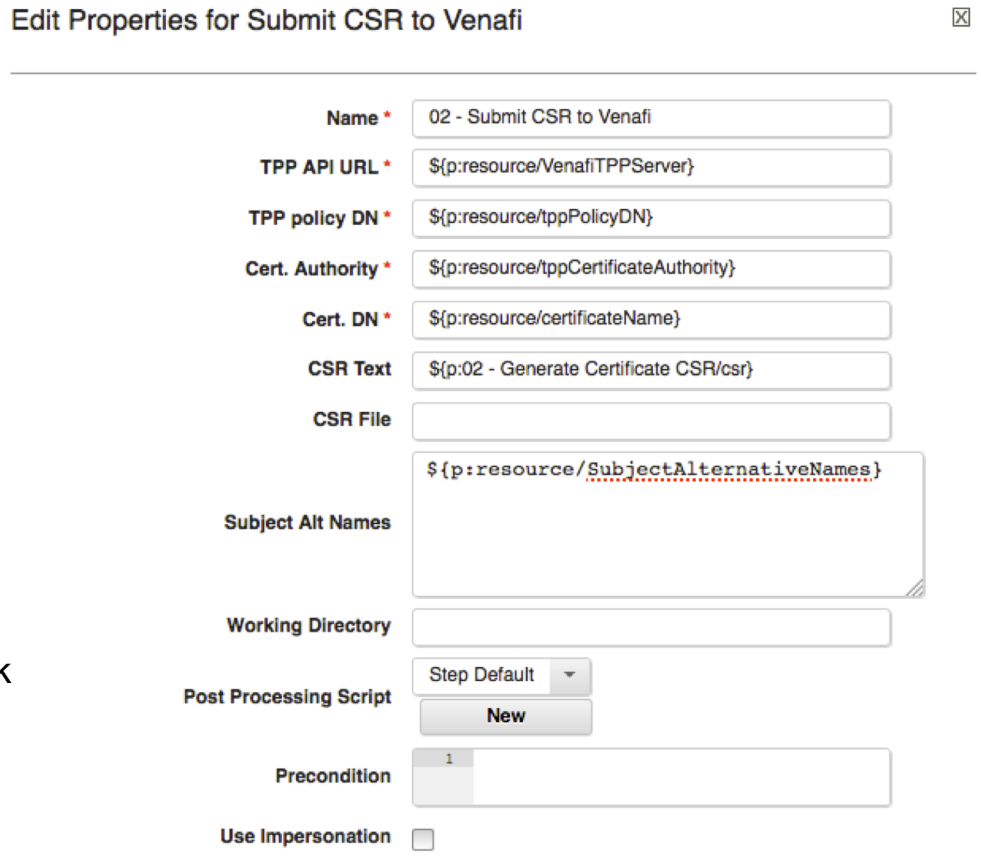
Output Properties - View Input Properties

Name	Value
certificateAuthority	\VED\Policy\Certificate authorities\MS CA
exitCode	0
LOI	
policy	{"city":"London","state":"West Midlands","country":"UK","organization":"IBM UK Ltd","organizationalUnit":"Hybrid Cloud Division","keyAlgorithm":"RSA","keyBitStrength":"2048","managementType":"Monitoring","manualCSR":"ServiceGenerated","certificateAuthority":"\\VED\\Policy\\Certificate authorities\\MS CA","policyDN":"\\VED\\Policy\\DevOps_Workshop"}
Status	Success



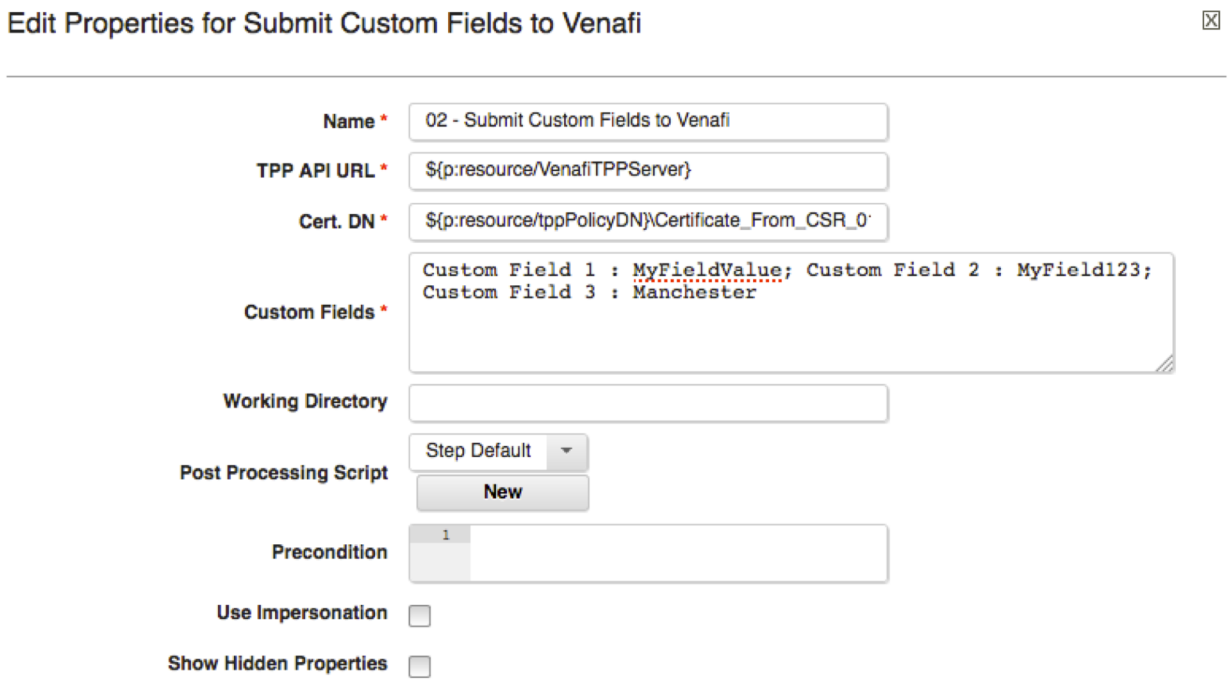
Submit CSR to Venafi

- Submit the CSR to Venafi for certificate generation
- Identify the policy in which the certificate should be generated. This must match the policy that was pulled from Venafi for the CSR creation process.
- CSR can be supplied as either a block of text passed from a previous step – 'Generate Certificate CSR' or a filename may be given that contains the CSR text.
- Subject alternative names may also be given in the format :
  - TYPE : value1; TYPE : value2 ; TYPE : value3
  - Type values available : DNS, URI, Email, IPAddress, OtherName
  - Example : DNS : www.google.com; DNS : www.venafi.com; DNS : www.bbc.co.uk



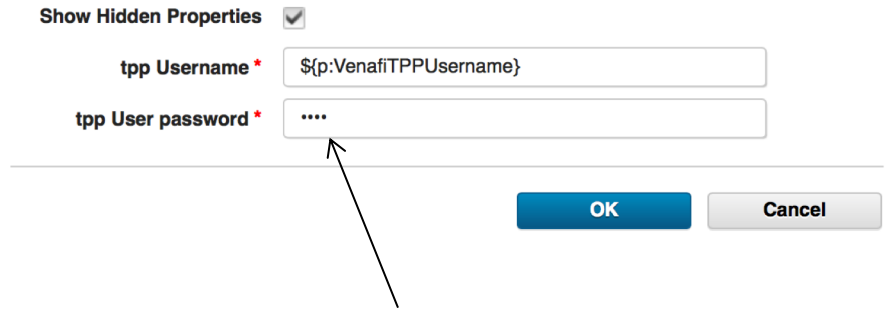
Submit Custom Fields to Venafi

- Submit the custom fields to Venafi to support a previously submitted certificate request
- Identify the certificate DN for the certificate to get the custom fields
- Custom fields in the format :
  - Custom field 1 name : value1; Custom field 2 name : value2 ; Custom field 3 name : value3



Venafi TPP User and password management

- All plugin steps require a login to the Venafi TPP server
- All requests for certificate actions are audited against each user
- Each plugin step requires Venafi username and password
  - tpp Username and tpp User password fields
  - Password field is a secure property
- Username and password values can be:
  - Typed into each step – not ideal as passwords change and would require one ‘generic’ user
  - Stored in the UrbanCode resource tree – not ideal from a security position
  - Typed in for each process execution – Not stored in UrbanCode and each user requesting a deployment must enter their credentials
- Create process properties to request passwords at deploy time



Note this field value is actually :
${p:VenafiTPPUserPassword}

Component Process Properties

Add Property

Name	Label	Pattern	Required	Default Value	Description	Actions
VenafiTPPUsername	Venafi User		true	admin	Venafi TPP User name	Edit Delete
VenafiTPPUserPassword	Venafi Password		true	****	Venafi TPP User Password	Edit Delete

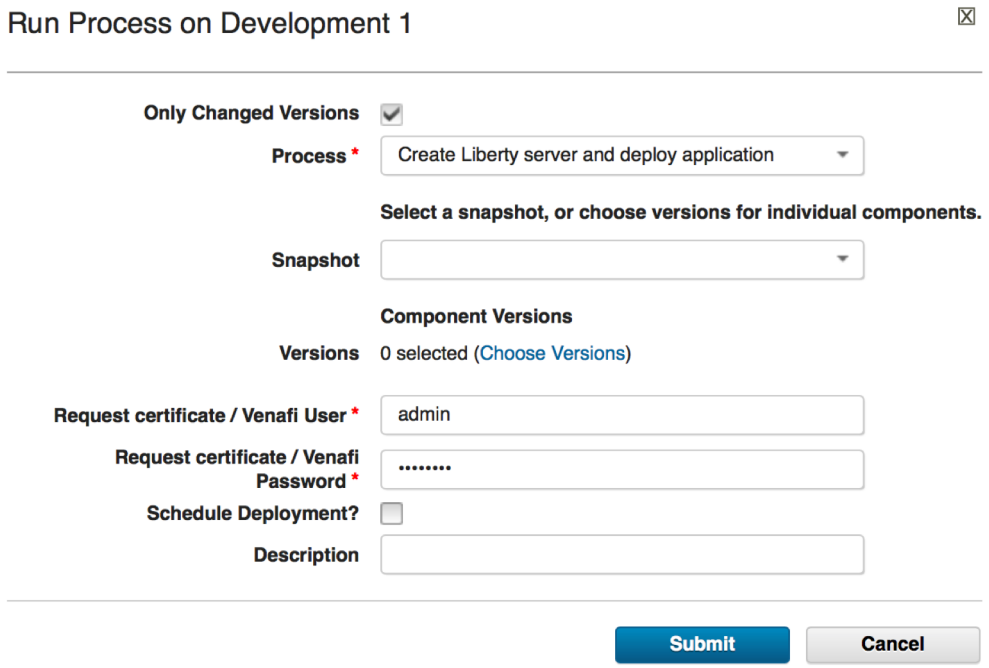
2 records - Refresh Print

1 / 1

Rows 10

Venafi TPP User and password management

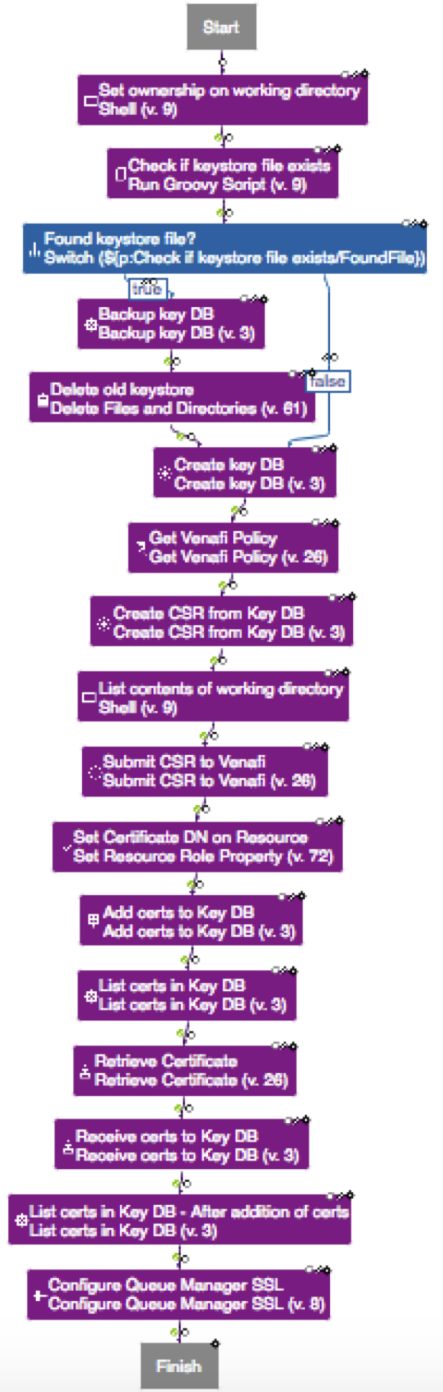
- At ’deploy’ time (execution of a process) the username and password for Venafi TPP are requested
- Password is stored as a secure property and passed to the relevant agents in an encrypted format
- Passwords are redacted in logs
- Each interaction between UrbanCode and Venafi is managed under a specific user ID
- Maintains Venafi audit trails with automation from UrbanCode



Example process : Request a new certificate and apply to WebSphere MQ

CSR based process

- Note that this process example uses the MQ Keys and Certificates plugin too
- Complete certificate management process for WebSphere MQ
  - If a keystore is found it is removed and replaced
  - Keystore is created
  - Venafi policy is retrieved
  - A CSR is generated using the keystore and the Venafi policy
  - The CSR is submitted to Venafi
  - The Certificate DN is stored on the UrbanCode Deploy resource for further interaction with Venafi later such as a certificate validation or renewal
  - Root and intermediate certificates are loaded into the keystore (note that root and intermediate certificate file must be downloaded from a component version store to the agent working directory before this step
  - Certificate is retrieved from Venafi
  - Certificate is imported into the keystore
  - Certificates are listed after importing so the user can validate if required



Example process : Maintain certificate process

Not CSR bases – simple process

- Check a certificate expiry date in Venafi TPP server records
  - – Validate the number of days remaining on the certificate (uses the stored Certificate DN)
  - – If the certificate has enough days left then do nothing, otherwise:
    - Request a new certificate on Venafi server
    - Import the new certificate
    - List the new certificate