



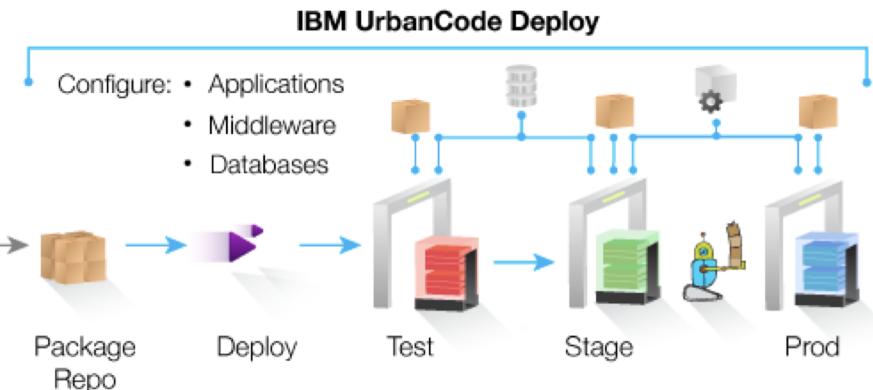
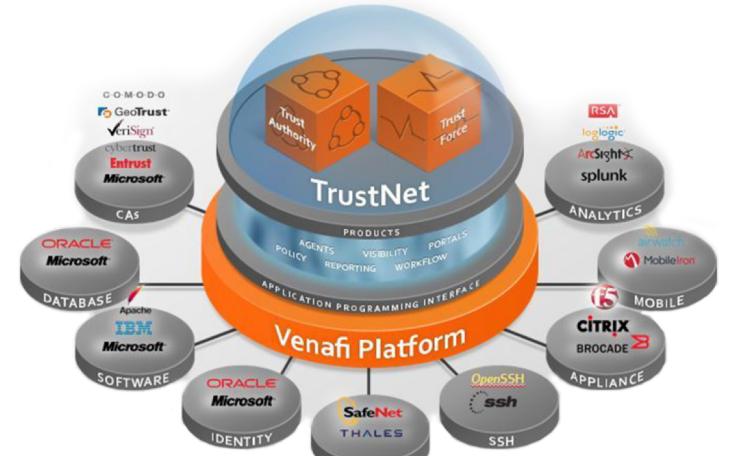
## UrbanCode Deploy plugin for Venafi Trust Protection Platform

Mark Roberts  
UrbanCode Technical Specialist

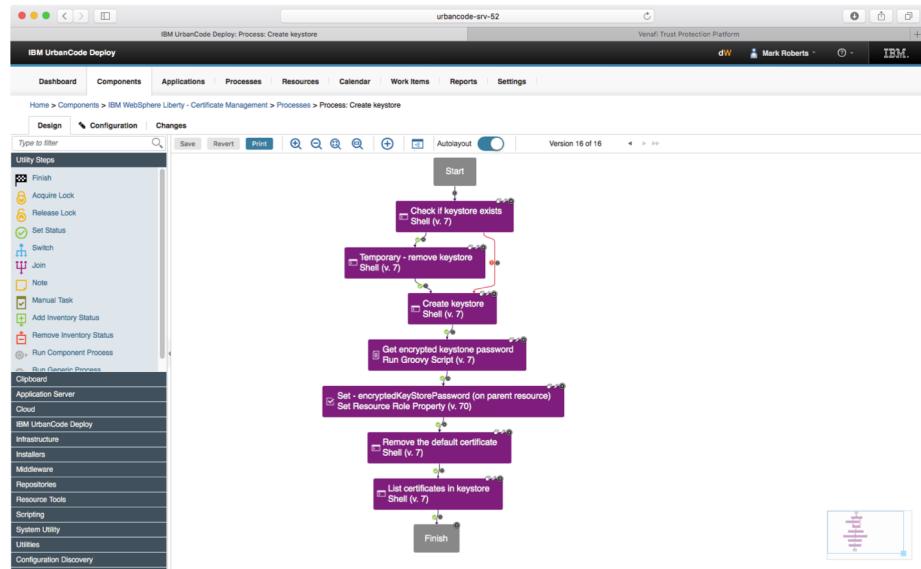
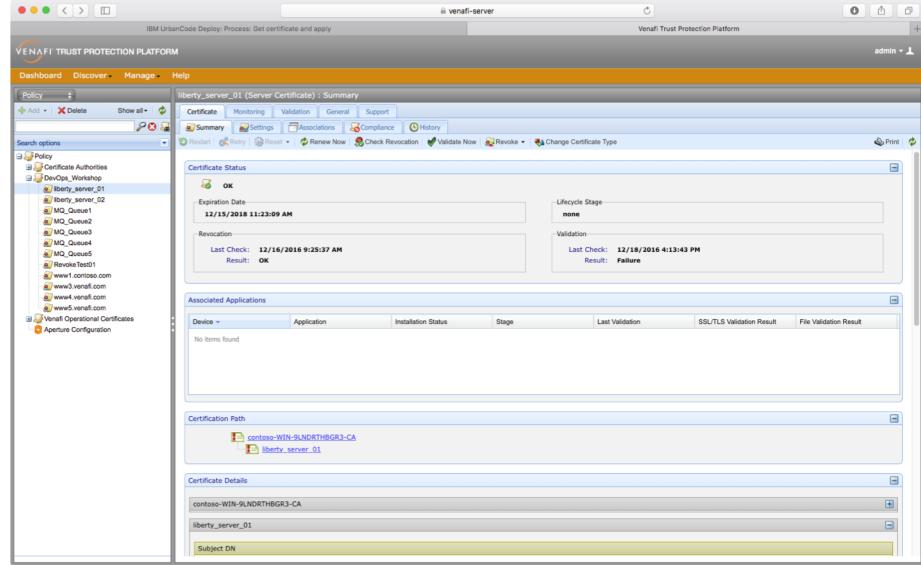
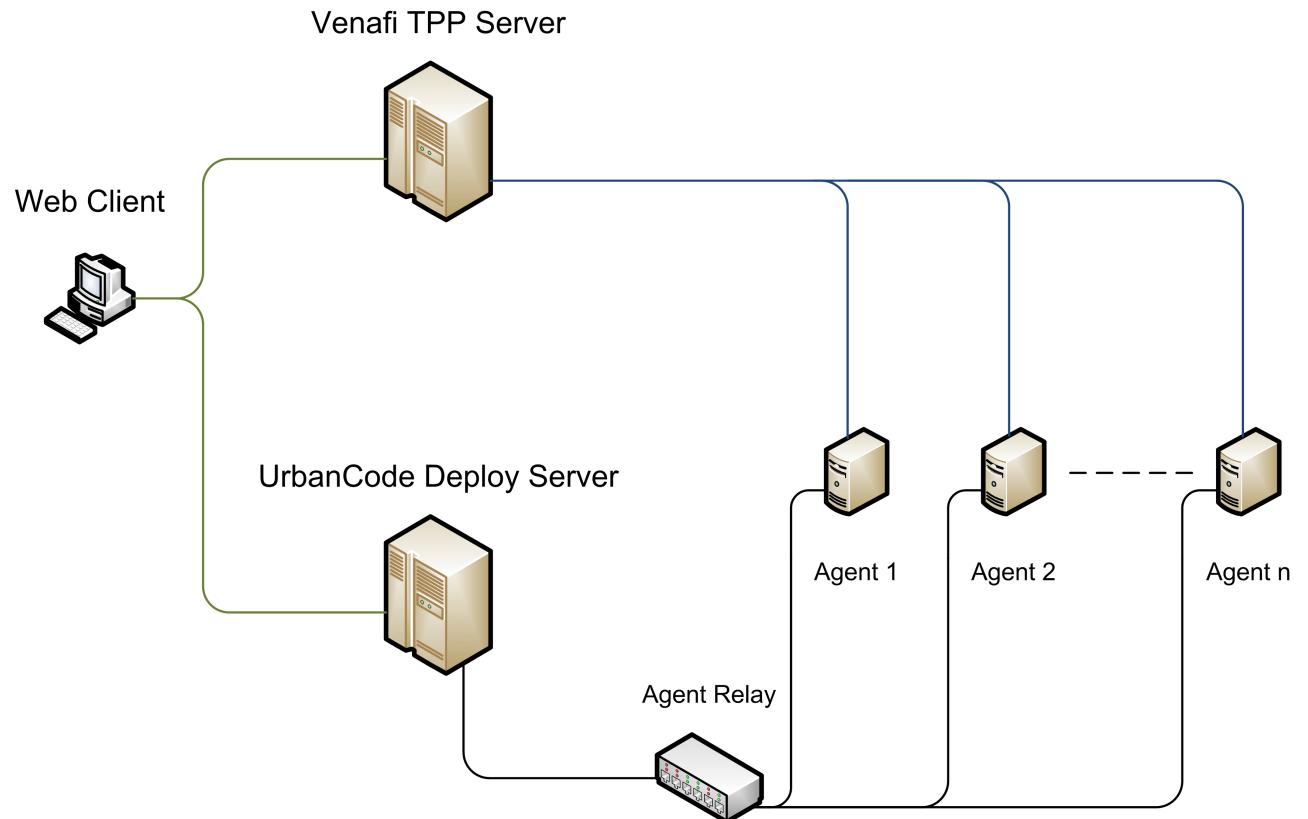


# Venafi Trust Protection Platform & UrbanCode Deploy

- 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

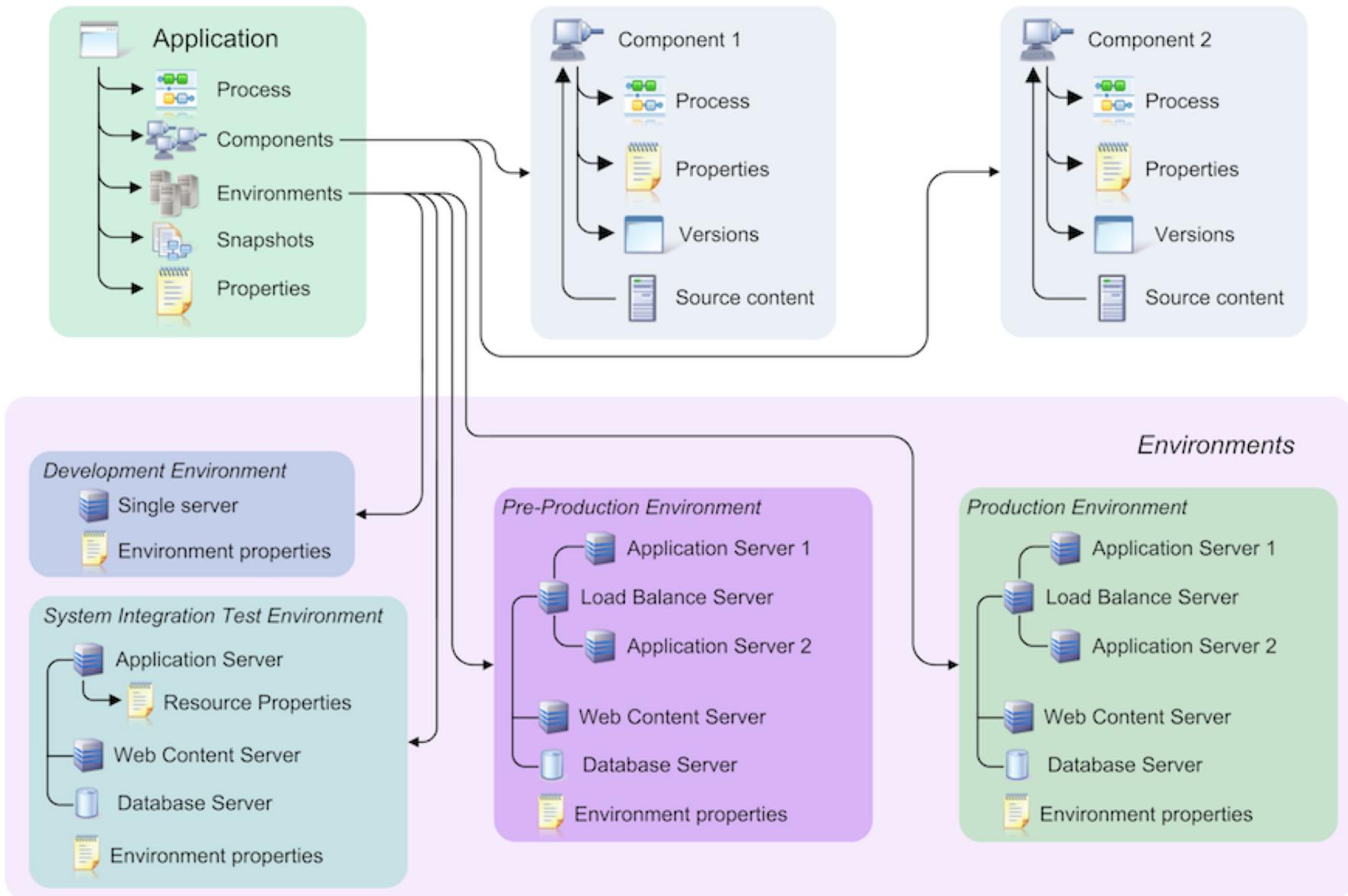


# Physical Infrastructure and Interaction





# 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/>

The screenshot shows a grid of eight plugin cards for IBM UrbanCode Deploy:

- TeamCity**: 11 integrations. Tagged as **Community**.
- Text Utility**: Tagged as **Community**.
- Tibco**: Tagged as **Community**.
- TIBCO**: Tagged as **Partner**.
- Venafi**: Tagged as **Community**.
- VMware AirWatch**: Tagged as **Community**.
- Web Utilities**: 9 integrations. Tagged as **Featured**.
- WebSphere Application Server - Configure**: 62 integrations. Tagged as **Featured**.

All cards feature a green interlocking gear icon with a lightning bolt symbol. The text "IBM UrbanCode Deploy" is present under each card.





## 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 still 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

Edit Properties

X

Name *	Request Certificate
TPP API URL *	\$(p:resource/VenafiTPP-URL)
CA DN *	\VED\Policy\Certificate Authorities\MS CA
X.509 subject *	NewServer
Working Directory	
Post Processing Script	Step Default New
Precondition	1
Use Impersonation	<input type="checkbox"/>
Show Hidden Properties	<input type="checkbox"/>

**OK** **Cancel**



## 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

### Edit Properties

Name *	Retrieve Certificate
TPP API URL *	\$(p:resource/VenafiTPP-URL}
Certificate DN *	\VVED\Policy\DevOps_Workshop\NewServer
Filename *	NewServerCert
Format *	PKCS #12
Include chain	<input checked="" type="checkbox"/>
Include private key	<input checked="" type="checkbox"/>
Password *	....
Working Directory	
Post Processing Script	Step Default <input type="button" value="New"/>
Precondition	1
Use Impersonation	<input type="checkbox"/>
Show Hidden Properties	<input type="checkbox"/>

OK

Cancel

## 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

Edit Properties

Name *	Request Certificate Wait
TPP API URL *	https://venafi-server
TPP policy DN *	\VVED\Policy\DevOps_Workshop
CA DN *	\VVED\Policy\Certificate Authorities\MS CA
X.509 subject *	liberty_server_01
Poll time *	3
Poll repeats *	20
Format *	PKCS #12
Include chain	<input checked="" type="checkbox"/>
Include private key	<input checked="" type="checkbox"/>
Password *	....
Working Directory	
Post Processing Script	Step Default <input type="button" value="New"/>
Precondition	1
Use Impersonation	<input type="checkbox"/>
Show Hidden Properties	<input type="checkbox"/>

OK

Cancel

# 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	2016-12-20T07:22:54.000000Z
validTo	2018-12-20T07:22:54.000000Z

Edit Properties

Get Certificate Status

TPP API URL \* \${p:resource/VenafiTPP-URL}

Certificate DN \* \VED\Policy\DevOps\_Workshop\liberty\_server\_02

Working Directory

Step Default New

Post Processing Script

Precondition 1

Use Impersonation

Show Hidden Properties

OK Cancel



## 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 or find the certificate
  - Step will pass and report validity in ‘CertificateOK’
- Output

Output Properties - [View Input Properties](#)

Name	Value
CertificateOK	false
daysRemaining	729

Edit Properties

X

Name *	Validate Remaining Days
TPP API URL *	\${p:resource/VenafiTPP-URL}
Certificate DN *	\${p:resource/CertificateDN}
Days required *	\${p:DaysRemaining}
Working Directory	
Post Processing Script	Step Default <input type="button" value="New"/>
Precondition	1
Use Impersonation	<input type="checkbox"/>
Show Hidden Properties	<input type="checkbox"/>

**OK** **Cancel**



# 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

## Edit Properties

X

Name *	Revoke Certificate
TPP API URL *	\${p:resource/VenafiTPP-URL}
Certificate DN *	\${p:resource/CertificateDN}
Reason *	1 - User key compromised
Comment	1 \${p?:comment}
disabled	<input type="checkbox"/>
Working Directory	
Post Processing Script	Step Default
	New
Precondition	1
Use Impersonation	<input type="checkbox"/>
Show Hidden Properties	<input type="checkbox"/>

[OK](#) [Cancel](#)

## 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

## Edit Properties

---

Name *	Renew Certificate
TPP API URL *	`\${p:resource/VenafiTPP-URL}`
Certificate DN *	`\${resource/CertificateDN}`
Working Directory	
Post Processing Script	<input type="button" value="Step Default"/> <input type="button" value="New"/>
Precondition	1
Use Impersonation	<input type="checkbox"/>
Show Hidden Properties	<input type="checkbox"/>

---



# 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)

Output Properties - [View Input Properties](#)

Name	Value
certificateAuthority	\VED\Policy\Certificate authorities\MS CA
certificateDN	Certificate_From_CSR_01
csr	<pre>-----BEGIN CERTIFICATE REQUEST----- MIIC7jCCAdYCAQAwgagxJTAjBgkqhkiG9w0BCQEWFm1hcmtby2Jlc nRzQHvrlml -----END CERTIFICATE REQUEST----- -----BEGIN PRIVATE KEY----- w8lJ2YmSgzSJr4hojVj9CmofybSpkDE2UuoCZM4hZ+7alYJpG4Dnb ANsUkElpf2 heRyw7bfR50El3TeJODbf2JtUHFYIXfQk5PNjySm0mTsQoOHY8uQ -----END PRIVATE KEY-----</pre>
exitCode	0
LOI	
policyDN	\VED\Policy\DevOps_Workshop
privateKeyFile	venafi_csr_key.private
publicKeyFile	venafi_csr_key.public
Status	Success

Edit Properties for Generate Certificate CSR

Name *	02 - Generate Certificate CSR
Policy details *	\$(p:02 - Get Venafi Policy/policy)
Cert. DN *	Certificate_From_CSR_01
Email *	markroberts@uk.ibm.com
Web URL *	www.ibm.com
Private key file *	venafi_csr_key.private
Public key file *	venafi_csr_key.public
Working Directory	
Post Processing Script	Step Default <input type="button" value="New"/>
Precondition	1
Use Impersonation	<input type="checkbox"/>

OK Cancel



## 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

### Edit Properties for Get Venafi Policy

Close

Name *	02 - Get Venafi Policy	
TPP API URL *	\${p:resource/VenafiTPPServer}	
TPP policy DN *	\${p:resource/tppPolicyDN}	
Working Directory		
Post Processing Script	Step Default <input type="button" value="New"/>	
Precondition	<table border="1"><tr><td>1</td></tr></table>	1
1		
Use Impersonation	<input type="checkbox"/>	
Show Hidden Properties	<input type="checkbox"/>	

OK

Cancel



## 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

Edit Properties for Submit CSR to Venafi X

---

Name *	02 - Submit CSR to Venafi
TPP API URL *	`\${p:resource/VenafiTPPServer}`
TPP policy DN *	`\${p:resource/tppPolicyDN}`
Cert. Authority *	`\${p:resource/tppCertificateAuthority}`
Cert. DN *	`\${p:resource/certificateName}`
CSR Text	`\${p:02 - Generate Certificate CSR/csr}`
CSR File	
Subject Alt Names	`\${p:resource/SubjectAlternativeNames}`
Working Directory	
Post Processing Script	<span style="border: 1px solid #ccc; padding: 2px;">Step Default</span> <span style="border: 1px solid #ccc; padding: 2px;">New</span>
Precondition	1
Use Impersonation	<input type="checkbox"/>



# 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

Edit Properties for Submit Custom Fields to Venafi

The dialog box contains the following fields:

- Name \*: 02 - Submit Custom Fields to Venafi
- TPP API URL \*: \${p:resource/VenafiTPPServer}
- Cert. DN \*: \${p:resource/tppPolicyDN}\Certificate\_From\_CSR\_0
- Custom Fields \*:

```
Custom Field 1 : MyFieldValue; Custom Field 2 : MyField123;
Custom Field 3 : Manchester
```
- Working Directory: [empty input field]
- Post Processing Script: Step Default ▾  
New
- Precondition: 1
- Use Impersonation: [unchecked checkbox]
- Show Hidden Properties: [unchecked checkbox]



# 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

Show Hidden Properties

tpp Username *	<input type="text" value="\${p:VenafiTPPUsername}"/>
tpp User password *	<input type="password" value="...."/>

**OK** **Cancel**

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

### Run Process on Development 1 ✖

Only Changed Versions

Process \* Create Liberty server and deploy application ▼  
Select a snapshot, or choose versions for individual components.

Snapshot ▼

Component Versions

Versions 0 selected ([Choose Versions](#))

Request certificate / Venafi User \* admin

Request certificate / Venafi Password \* ..... ▼

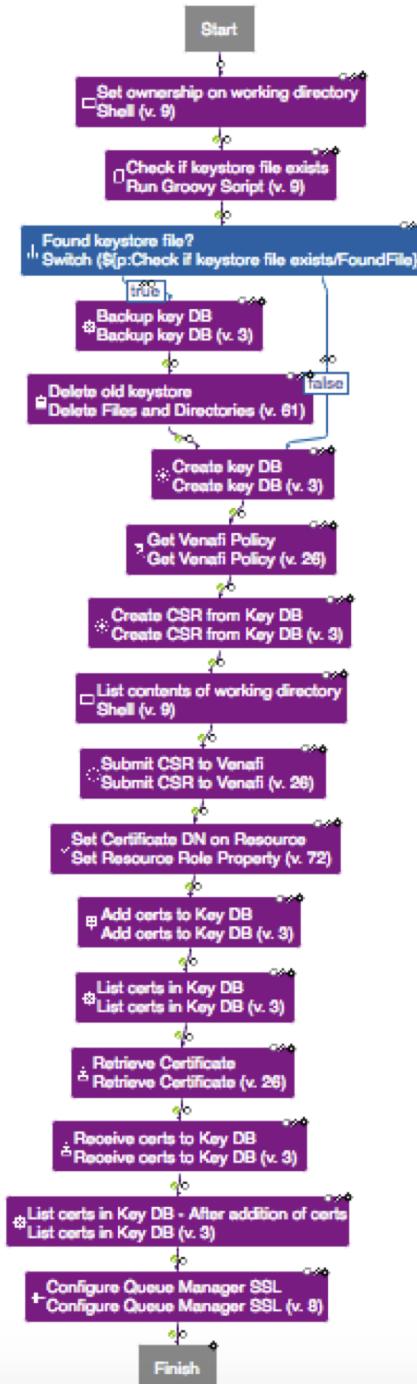
Schedule Deployment?

Description ▼

Submit Cancel

## 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

