General instructions for installing a new SSL cert on BMC server

Created Date	Updated Date	Affects version	Fix Version
09 Apr 2020	02 Sep 2022	All	

Description

These general instructions can be used to install a new SSL certificate on a BMC server, please note that when exporting/generating the certificate for use with the BMC the private key needs to be included along with the full certificate chain.

Instructions

Check current certificate from BMC Keystore:

```
keytool -list -v -keystore “C:\Program Files\Blancco\Blancco Management Console\apache-tomcat\conf\keystore.jks”
```

CER

Using the Java **keytool.exe**, you can follow the steps below to install a new SSL certificate on your BMC server.

Run commands on Command Prompt which is opened with administrator privileges

Step 1: Stop the BMC service.

Step 2: Create the new keystore/keypair.

keytool -keystore "path_to\keystore_name.jks" -genkeypair -keyalg RSA -keysize 2048 -validity #of days -dname "cn=domain name, ou=yourOrgUnit , o=yourOrgOrCompany, l=City/locality, st=State/Canton/Province/Land, c=Country_ISO3166-digraph" -alias "domain name"

DN	Information	Description	Example
	Validity	Number of days how long keystore is valid.	365
CN	Common Name	This is fully qualified domain name that you wish to secure	example.com
o	Organization Name	Usually the legal name of a company or entity and should include any suffixes such as Ltd., Inc., or Corp.	Example Inc
OU	Organizational Unit	Internal organization department/division name	IT
l	Locality	Town, city, village, etc. name	Helsinki
st	State	Province, region, county or state	North Karelia
c	Country	The two-letter ISO code for the country where your organization is located	FI

(Optional - if "**subject alternative name (SAN)**" needs to be used):

keytool -keystore "path_to\keystore_name.jks" **-ext san=dns:Name1,dns:Name2** -genkeypair -keyalg RSA -keysize 2048 -validity #of days -dname "cn=domain name, ou=yourOrgUnit , o=yourOrgOrCompany, l=City/locality, st=State/Canton/Province/Land, c=Country_ISO3166-digraph" -alias "domain name"

Step 3: Create a new CSR, Certificate Signing Request, for your new keystore/keypair.

keytool -keystore "path_to\keystore_name.jks" -certreq -alias domain_name -file "path_to\filename.csr"

(Optional - if "**subject alternative name (SAN)**" needs to be used):

keytool -keystore "path_to\keystore_name.jks" **-ext san=dns:Name1,dns:Name2** -certreq -alias domain_name -file "path_to\filename.csr"

Step 4: Send the CSR to a CA (Certificate Authority) to create the new certificate, this can be either an internal CA if one is available or a trusted third party CA.

Step 5: Import the Root CA cert, then the Intermediate CA cert.

keytool -keystore "path_to\keystore_name.jks" -importcert -alias rootCA -file "path_to\root.cer"
keytool -keystore "path_to\keystore_name.jks" -importcert -alias intCA -file "path_to\int.cer"

Step 5: Import CA-signed certificate and apply the same to the keypair.

keytool -keystore path_to\keystore_name.jks -importcert -alias original_keypair_alias -file path_to\CAsigned.cer

Step 6: Update the "keystoreFile" and "keystorePass" values in the server.xml file located under "C:\Program Files\Blancco\Blancco Management Console\apache-tomcat\conf" to reflect any changes associated with key/cert.

keystoreFile="path_to\keystore_name.jks" keystorePass="keystore password"

Step 7: Start the BMC service.

PFX

1. Stop BMC Service
2. Copy .pfx format certificate file to "\Blancco Management Console\apache-tomcat\conf" folder.
3. Open server.xml file in text editor located \Blancco Management Console\apache-tomcat\conf and edit following details.
    a. keystoreFile="Certificate_name.pfx"
    b. keystorePass="PFX_certificate_Password"
    c. Add a new value keystoreType="PKCS12" after KeystorePass.
4. Save the server.xml file.
5. Start BMC Service.

- License Snaphot
- "Failed to load workflow" when editing or creating a new workflow
- How to export a summary report
- General instructions for installing a new SSL cert on BMC server
- Installing CA signed certificate to authenticate Management Console AD integration via LDAPS