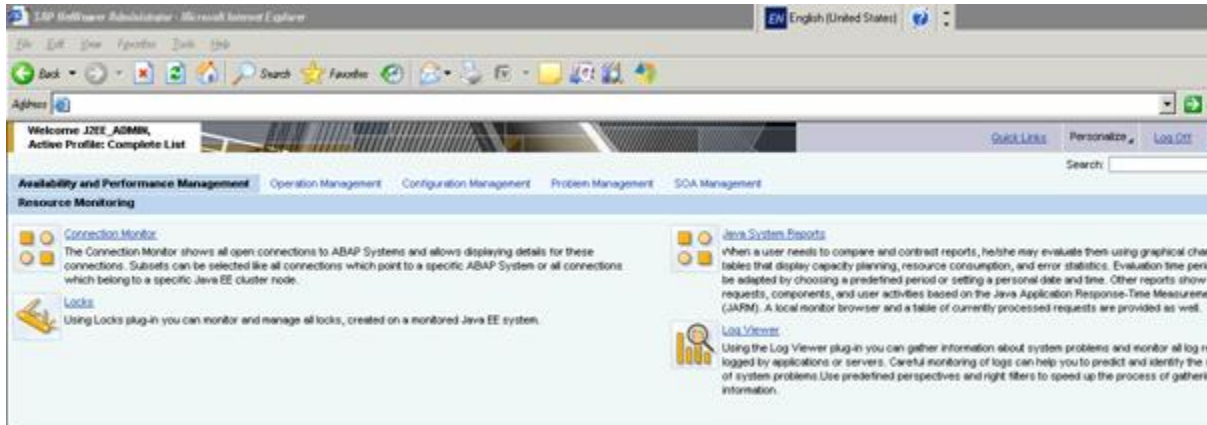
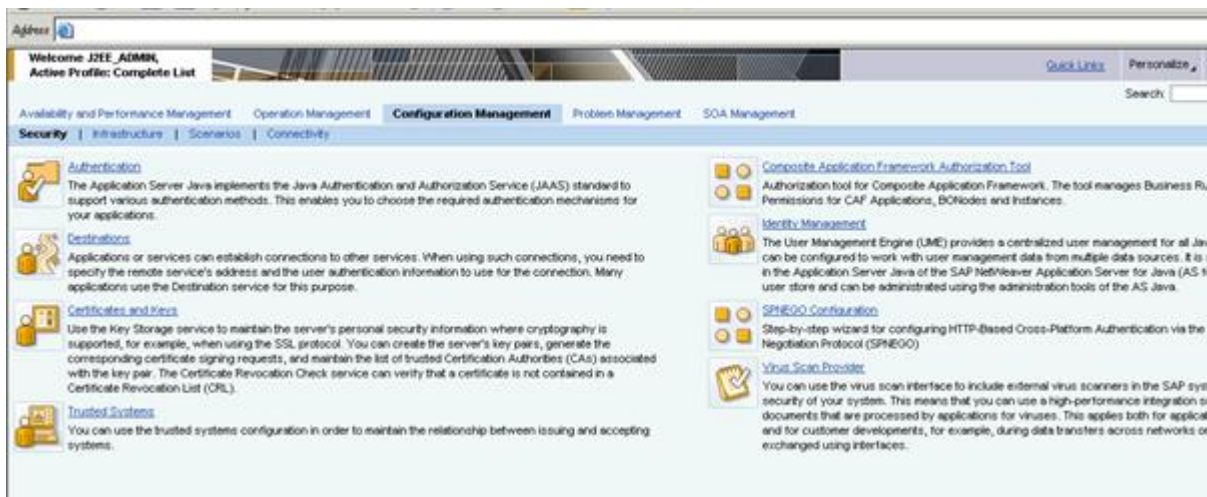


SAP-PI SERVER CSR Generation Procedure:

1. Open NetWeaver Administrator (<http://<FQDN>:5<XX>00/nwa>)



2. Go to **Configuration Management --> Certificates and Keys**



3. Select **ICM_SSL_<ID>** and you will find the default **Private key** and **Certificate** when SSL has not yet been configured.

Status	Name	Entry Type	Algorithm	Valid From	Valid To
DEFAULT		SYSTEM		Public view for common use by all components	
ICM_SSL_1009966		SYSTEM		ICM Server SSL credentials store	
TREXKeyStore		USER		Contains keys and certificates used by the TREP service	
TicketKeyStore		SYSTEM		Contains the key-pair to use for issuing logon and assertion tickets, as well as the certificates for all trusted ticket issuing systems	
TrustedCAs		USER		Template view that contains trusted server certificates	
UMKeyStore		USER		Contains a key-pair used by the User Management Engine (UME) provider service	
WebServiceSecurity		USER		Web Services own keys and certificates for outbound communication	
WebServiceSecurity_Certs		USER		Web Services Security: Encryption certificates of other parties for message security (encrypt)	

Key Storage View Details					
Entries		Properties			
Status	Name	Entry Type	Algorithm	Valid From	Valid To
ICM_SSL_1009966	SAPPassportCA	CERTIFICATE	RSA	Tue Jul 18 10:00:00 UTC 2000	Sun Jul 18 10:00:00 UTC 2010
ICM_SSL_1009966	ssl-credentials	PRIVATE KEY	RSA	Thu Mar 30 06:39:00 UTC 2006	Tue Mar 30 07:54:36 UTC 2027
ICM_SSL_1009966	ssl-credentials-cert	CERTIFICATE	RSA	Thu Mar 30 06:39:00 UTC 2006	Tue Mar 30 07:54:36 UTC 2027

4. Rename or delete the old/obsolete certificates.

Key Storage View Details

Entries Properties

Create Delete Rename Copy Entry Import Entry Export Entry Generate CSR Request Import CSR Response

Status	Name	Entry Type	Algorithm	Valid From	Valid To
	SAPPassportCA	CERTIFICATE	RSA	Tue Jul 18 10:00:00 UTC 2006	Sun Jul 18 10:00:00 UTC 2010
	ssl-credentials	PRIVATE KEY	RSA	Thu Mar 30 06:39:00 UTC 2006	Tue Mar 30 07:54:36 UTC 2007
	ssl-credentials-cert	CERTIFICATE	RSA	Thu Mar 30 06:39:00 UTC 2006	Tue Mar 30 07:54:36 UTC 2007

Entry Details

PRIVATE KEY entry
 Creation date : Thu Mar 30 06:40:134 UTC 2006 (30 Mar 2006 06:40:134 GMT)
 Version : PKCS#8 RSA
 Key Size : 1024 bits
 Certificate[0] : -----
 Version : ver-3 X.509
 Algorithm : RSA
 Key Size : 1024 bits
 Subject name : CN=localhost,OU=ssl-enabled-server,O=app-server
 Issuer name : CN=localhost,OU=ssl-enabled-server,O=app-server
 Serial number : 260957037
 Signature Algorithm : MD5withRSAEncryption (1,2,840.113549.1.1.4)
 Validity :
 not before : Thu Mar 30 06:39:00 UTC 2006 (30 Mar 2006 06:39:00 GMT)
 not after : Tue Mar 30 07:54:36 UTC 2007 (30 Mar 2007 07:54:36 GMT)
 Public key fingerprint : 30:52:98:16:A2:93:FB:DB:D9:0D:63:F9:09:74:1E:AD:14
 Certificate fingerprint(MD5) : 5F:FB:44:CD:FF:14:45:41:3C:79:87:39:BE:1D:5A:5C:1E
 Certificate extensions :
 [critical]
 [non-critical]
 subjectKeyIdentifier: 92:122:1C5:BB:13:1A:41:D2:04:C3:60:79:BB:BE:1F:C1:BB:0E:1A:E1:9E:18:1E2

Key Storage View Details

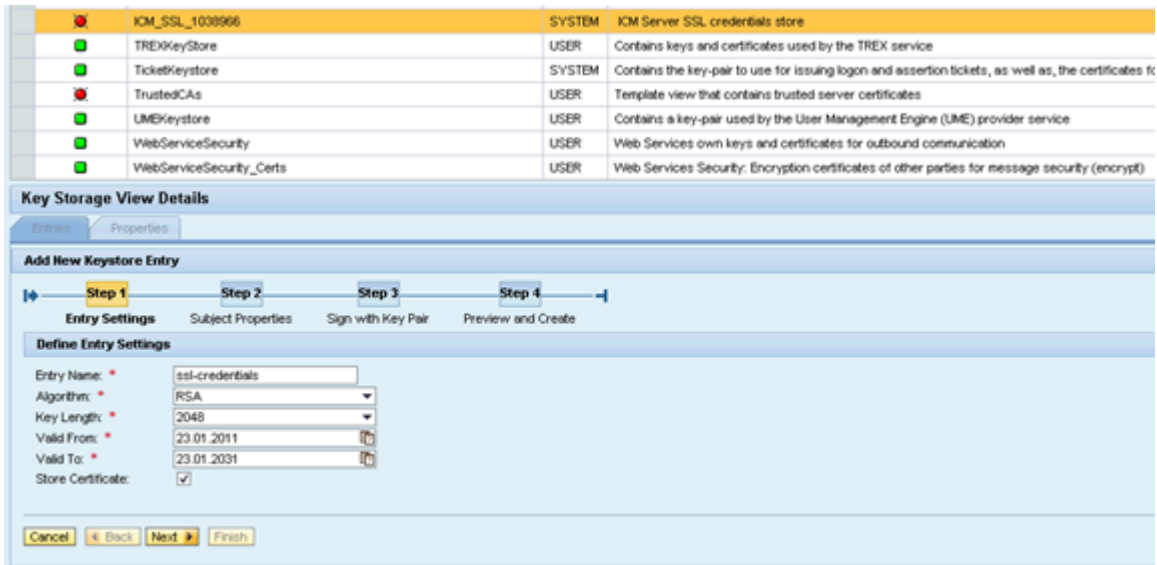
Entries Properties

Create Delete Rename Copy Entry Import Entry Export Entry Generate CSR Request Import CSR Respo

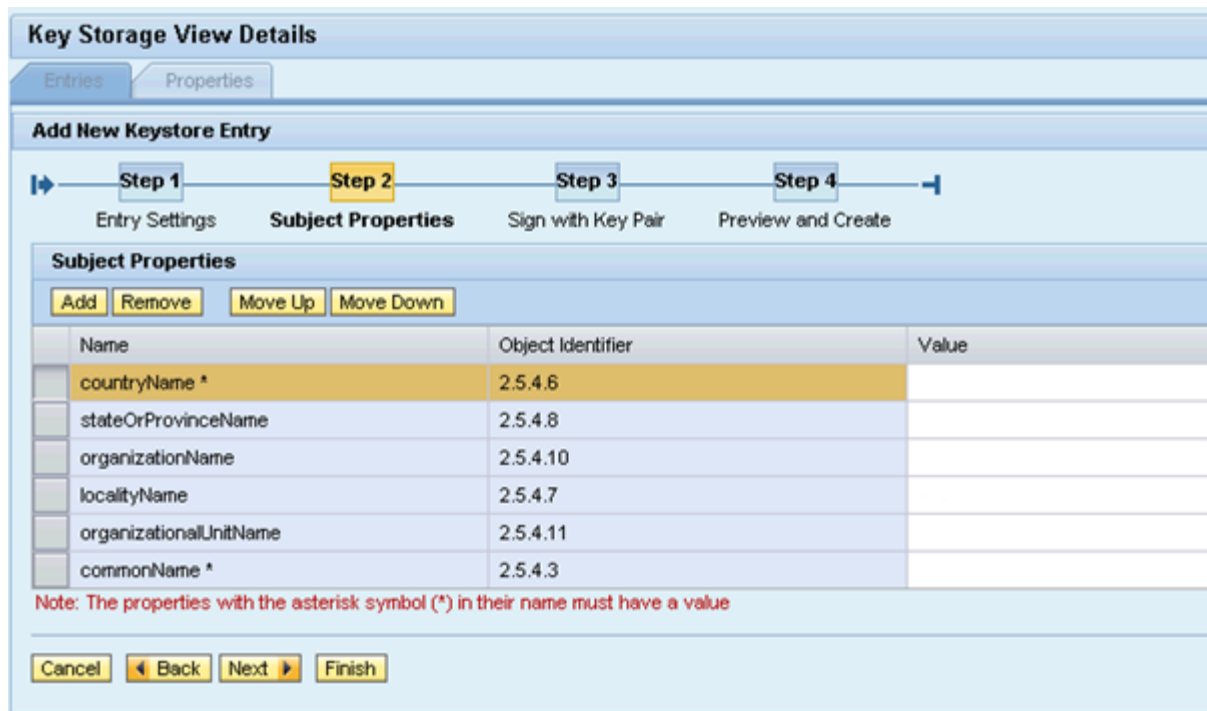
Status	Name	Entry Type	Algorithm
	SAPPassportCA	CERTIFICATE	RSA
	ssl-credentials-cert-old	CERTIFICATE	RSA
	ssl-credentials-old	PRIVATE KEY	RSA

Entry Details

5. Create new Private Key (**ssl-credentials**) as shown in the below screenshots.



Note: Certificate (**ssl-credentials-cert**) will be generated automatically when we choose 'Store Certificate' in the above screenshot.



- Country Name and Common Name (CN) are mandatory fields.

- Just click NEXT

The screenshot shows the 'Key Storage View Details' window with the 'Properties' tab selected. The 'Add New Keystore Entry' wizard is in progress, with Step 3, 'Sign with Key Pair', highlighted. The progress bar shows four steps: Step 1 (Entry Settings), Step 2 (Subject Properties), Step 3 (Sign with Key Pair), and Step 4 (Preview and Create). Below the progress bar, the section 'Sign Entry with the Following Key Pair' contains a 'Select Key Pair' button and an empty table with columns 'Key' and 'Value'. At the bottom, there are buttons for 'Cancel', 'Back', 'Next', and 'Finish'.

- Click Finish

The screenshot shows the 'Key Storage View Details' window with the 'Properties' tab selected. The 'Add New Keystore Entry' wizard is in progress, with Step 4, 'Preview and Create', highlighted. The progress bar shows four steps: Step 1 (Entry Settings), Step 2 (Subject Properties), Step 3 (Sign with Key Pair), and Step 4 (Preview and Create). Below the progress bar, the section 'Preview and Create Entry' displays the following details:

Entry Name:	ssl-credentials
Algorithm:	RSA
Key Length:	2048
Valid From:	23.01.2011
Valid To:	23.01.2031

Below this, the 'Subject Properties' section contains a table with columns 'Name' and 'Value':

Name	Value
countryName *	
stateOrProvinceName	
organizationName	
localityName	
organizationalUnitName	
commonName *	

At the bottom, there are buttons for 'Cancel', 'Back', 'Next', and 'Finish'.

