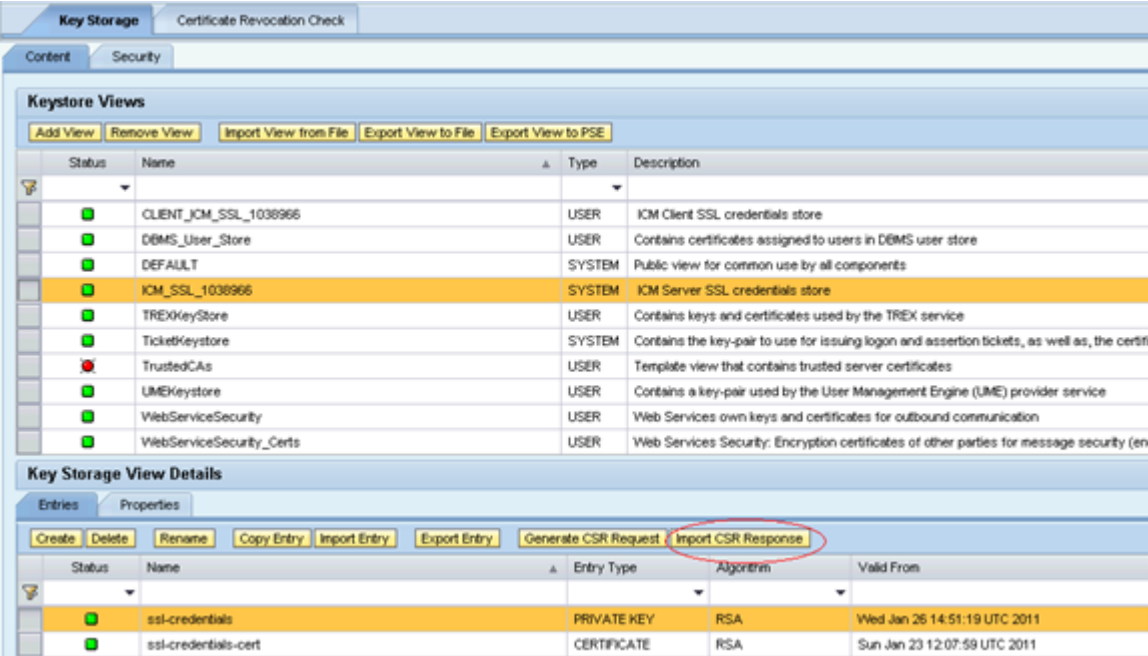


SAP PI Server SSL Certificate Installation Steps:

1. Go to NWA-->Configuration Management --> Certificates and Keys and select ICM_SSL_<ID>.
2. Click on 'Import CSR response'



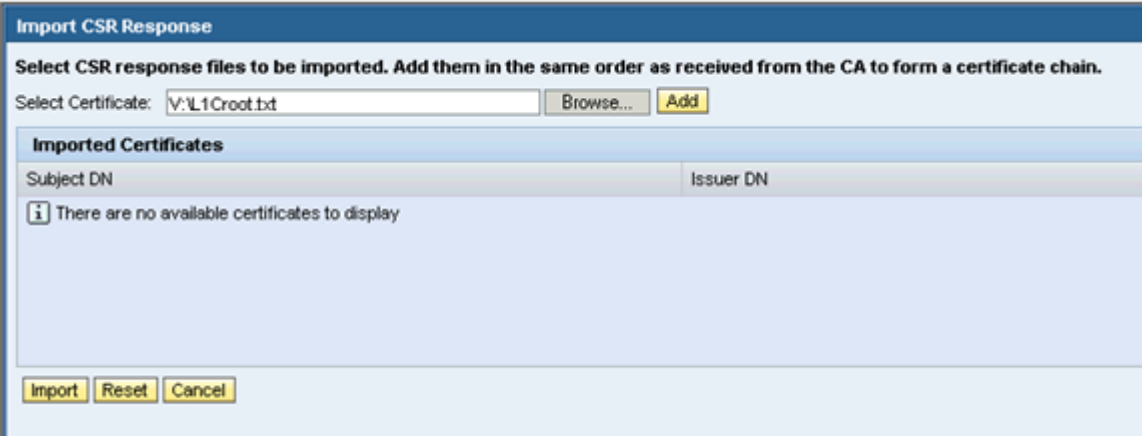
The screenshot shows the 'Key Storage' interface. The 'Keystore Views' table lists various keystore views, with 'ICM_SSL_1038966' selected. The 'Key Storage View Details' section shows the 'Import CSR Response' button circled in red.

Status	Name	Type	Description
✓	CLIENT_ICM_SSL_1038966	USER	ICM Client SSL credentials store
✓	DBMS_User_Store	USER	Contains certificates assigned to users in DBMS user store
✓	DEFAULT	SYSTEM	Public view for common use by all components
✓	ICM_SSL_1038966	SYSTEM	ICM Server SSL credentials store
✓	TREXKeyStore	USER	Contains keys and certificates used by the TREX service
✓	TicketKeystore	SYSTEM	Contains the key-pair to use for issuing logon and assertion tickets, as well as, the certifi
✗	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 (en

Status	Name	Entry Type	Algorithm	Valid From
✓	ssl-credentials	PRIVATE KEY	RSA	Wed Jan 26 14:51:19 UTC 2011
✓	ssl-credentials-cert	CERTIFICATE	RSA	Sun Jan 23 12:07:59 UTC 2011

Note: We will get 3 certificates from CA, Web Server, Entrust cross and Entrust root. Import them in the same order.

3. Once all 3 certificates are added, and then only click on 'Import' button.



The screenshot shows the 'Import CSR Response' dialog box. It includes a text input field for 'Select Certificate:' with the value 'V:\L1Croot.txt', a 'Browse...' button, and an 'Add' button. Below this is a table for 'Imported Certificates' with columns for 'Subject DN' and 'Issuer DN'. A message box indicates 'There are no available certificates to display'. At the bottom, there are 'Import', 'Reset', and 'Cancel' buttons.

Import CSR Response

Select CSR response files to be imported. Add them in the same order as received from the CA to form a certificate chain.

Select Certificate:

Imported Certificates	
Subject DN	Issuer DN
CN=Entrust.net Certification Authority (2048),OU=(c) 1999 Entrust.net Limited,OU=www.entrust.net/CPS_2048_incorp. by ref. (limits lib.),O=Entrust.net	CN=Entrust.net Certification Authority (2048),OU=(c) 1
CN=Entrust Certification Authority - L1C,OU=(c) 2009 Entrust, Inc.,OU=www.entrust.net/ipa is incorporated by reference,O=Entrust, Inc.,C=US	CN=Entrust.net Certification Authority (2048),OU=(c) 1

4. Now you should be able to see chain certificates Certificate [0], Certificate[1] and Certificate[2] and Issuer name as 'Entrust Certification Authority'.

Object Name	Object Type	Algorithm	Creation Date	Expiration Date
ssl-credentials	PRIVATE KEY	RSA	Sun Jan 23 06:58:01 UTC 2011	Wed Jan 23 14:03:39 UTC 2013
ssl-credentials-cert	PRIVATE KEY	RSA	Sun Jan 23 06:31:42 UTC 2011	Thu Jan 23 06:31:42 UTC 2011
ssl-credentials-cert-old	CERTIFICATE	RSA	Thu Mar 30 06:39:00 UTC 2006	Tue Mar 30 07:54:36 UTC 2027
ssl-credentials-old	PRIVATE KEY	RSA	Thu Mar 30 06:39:00 UTC 2006	Tue Mar 30 07:54:36 UTC 2027

Entry Details

```

PRIVATE KEY entry
Creation date       : Sun Jan 23 06:47:35 UTC 2011 (23 Jan 2011 06:47:35 GMT)
Version            : PKCS#8 RSA
Key size           : 2048 bits
Certificate[0]
-----
Version           : ver.3 X.509
Algorithm          : RSA
Key size           : 2048 bits
Subject name       : CN=www.entrust.net/ipa is incorporated by reference,O=Entrust, Inc.,OU=www.entrust.net/ipa is incorporated by reference,ST=Florida,C=US
Issuer name        : CN=Entrust Certification Authority - L1C,OU=(c) 2009 Entrust, Inc.,OU=www.entrust.net/ipa is incorporated by reference,O=Entrust, Inc.,C=US
Serial number      : 1276747847
Signature Algorithm : SHA1w/rsaEncryption (1.2.840.113549.1.1.5)
Validity
not before         : Sun Jan 23 06:58:01 UTC 2011 (23 Jan 2011 06:58:01 GMT)
not after          : Wed Jan 23 14:03:39 UTC 2013 (23 Jan 2013 14:03:39 GMT)
Public key fingerprint : 15:AB:88:94:47:9C:90:F7:2C:E6:AC:F4:EC:AE:AA:B6
Certificate fingerprint(MD5) : 0C:EA:12:1D:09:8E:18:4E:7A:9F:88:94:6A:79:0E:1E
Certificate extensions :
[critical]
[non critical]
CertificatePolicies: certificatePolicy[0]: policyIdentifier: 1.2.840.113533.7.75.2
policyQualifiers[0]: policyQualifierId: id-pkix-cps
CPS URI: http://www.entrust.net/ipa
SubjectKeyIdentifier: A112710419910313B18413C1781781421641071BE1441DA1721771DE1C3
BasicConstraints: CA: no
AuthorityKeyIdentifier: KeyIdentifier: 1E1F1AB1891061F814910F101331771EE13417A1EE11917C19312814D
AuthorityInfoAccess: accessMethod: OBJECT ID = ocsp
accessLocation: uniformResourceIdentifier: http://ocsp.entrust.net
CRLDistributionPoints: Distributionpoint: uniformResourceIdentifier: http://crl.entrust.net/level1c.crl
ExtendedKeyUsage: keyPurposeId: TLS web server authentication
keyUsage: digitalSignature | keyEncipherment
Certificate[1]
-----
Version           : ver.3 X.509
  
```

```

    ORIDistributionPoints: DistributionPoint: uniformResourceIdentifier http://crl.entrust.net/levelsc.crl
    ExtendedKeyUsage: keyPurposeId 0: TLS web server authentication
    KeyUsage: digitalSignature | keyEncipherment

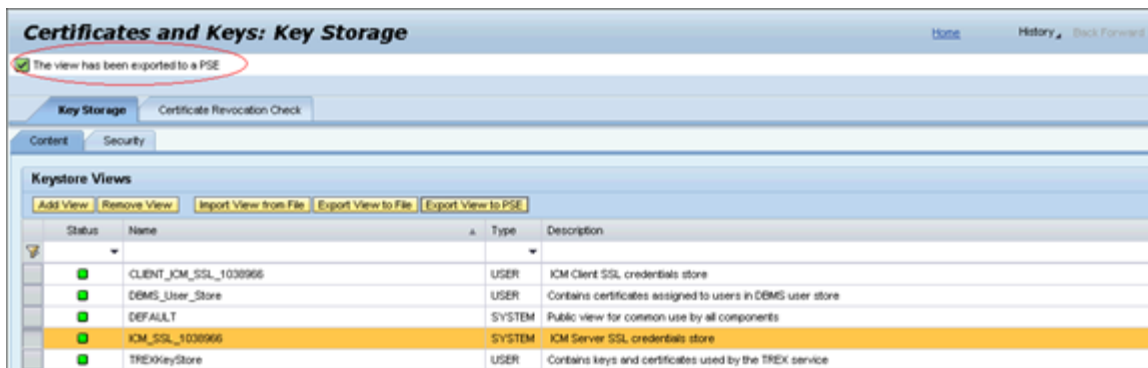
Certificate[1] -----
version                : ver.3 X.509
algorithm              : RSA
key size               : 2048 bits
subject name          : CN=Entrust Certification Authority - L3C,O=(C) 2009 Entrust, Inc.,OU=www.entrust.net/vpa IS Incorporated by reference,O=Entrust, Inc.,C=US
issuer name            : CN=Entrust.net Certification Authority (2048),O=(C) 1999 Entrust.net Limited,OU=www.entrust.net/CPS_2048 Incorpor. by ref. (limits
serial number         : 946072060
signature algorithm    : SHA1WITHRSAEncryption (1.2.840.113549.1.1.5)
validity
not before             : Thu Dec 10 20:43:54 UTC 2009 (10 Dec 2009 20:43:54 GMT)
not after              : Tue Dec 10 21:13:54 UTC 2019 (10 Dec 2019 21:13:54 GMT)
public key fingerprint : F4:BF:67:8C:A8:34:38:03:1F:4:06:EA:09:63:03:A0:50
certificate fingerprint : 2F:83:00:1F2:FA:12:7B:80:82:95:70:05:94:17:0B:8E
certificate extensions :
[critical]
basicConstraints: CA:yes
keyUsage: keyCertSign | cRLSign
[not critical]
certificatePolicies: certificatePolicyId: policyIdentifier: anyPolicy
policyQualifiers[0]: policyQualifierId: 10-phk-cps
CPS URI: http://www.entrust.net/vpa
subjectKeyIdentifier: 1E1F31A82891061F814910F01331771EE1847A1EE1397C1932814D
authorityKeyIdentifier: keyIdentifier: SE:E4:81:D1:11:86:08:89:69:08:A3:31:9F:AL:24:09:16:89:70
authorityInfoAccess: accessMethod: OBJECT ID = ocsp
accessLocations: uniformResourceIdentifier: http://ocsp.entrust.net

    ORIDistributionPoints: DistributionPoint: uniformResourceIdentifier http://crl.entrust.net/2048ca.crl

Certificate[2] -----
version                : ver.3 X.509
algorithm              : RSA
key size               : 2048 bits
subject name          : CN=Entrust.net Certification Authority (2048),O=(C) 1999 Entrust.net Limited,OU=www.entrust.net/CPS_2048 Incorpor. by ref. (limits
issuer name            : CN=Entrust.net Certification Authority (2048),O=(C) 1999 Entrust.net Limited,OU=www.entrust.net/CPS_2048 Incorpor. by ref. (limits
serial number         : 946069940
signature algorithm    : SHA1WITHRSAEncryption (1.2.840.113549.1.1.5)
validity
not before             : Fri Dec 24 17:50:51 UTC 1999 (24 Dec 1999 17:50:51 GMT)
not after              : Tue Jul 24 14:15:12 UTC 2029 (24 Jul 2029 14:15:12 GMT)
public key fingerprint : 91:FA:04:183:F3:481482:A8:A6:98:58:88:05:C0:88:3A
certificate fingerprint : EE:39:31:8C:32:7E:9A:68:68:86:FF:51:B4:34:71:90
certificate extensions :
[critical]
basicConstraints: CA:yes
keyUsage: keyCertSign | cRLSign
[not critical]
  
```

5. We should do Export View to PSE after steps 1 and 2 are completed successfully.

You should be able to see successful message at the top left screen.



6. Restart SSL Provider service.

Start & Stop: Java EE Services [Home](#)

Java EE Instances **Java EE Services** Java EE Applications

Services

Start Stop Restart Refresh

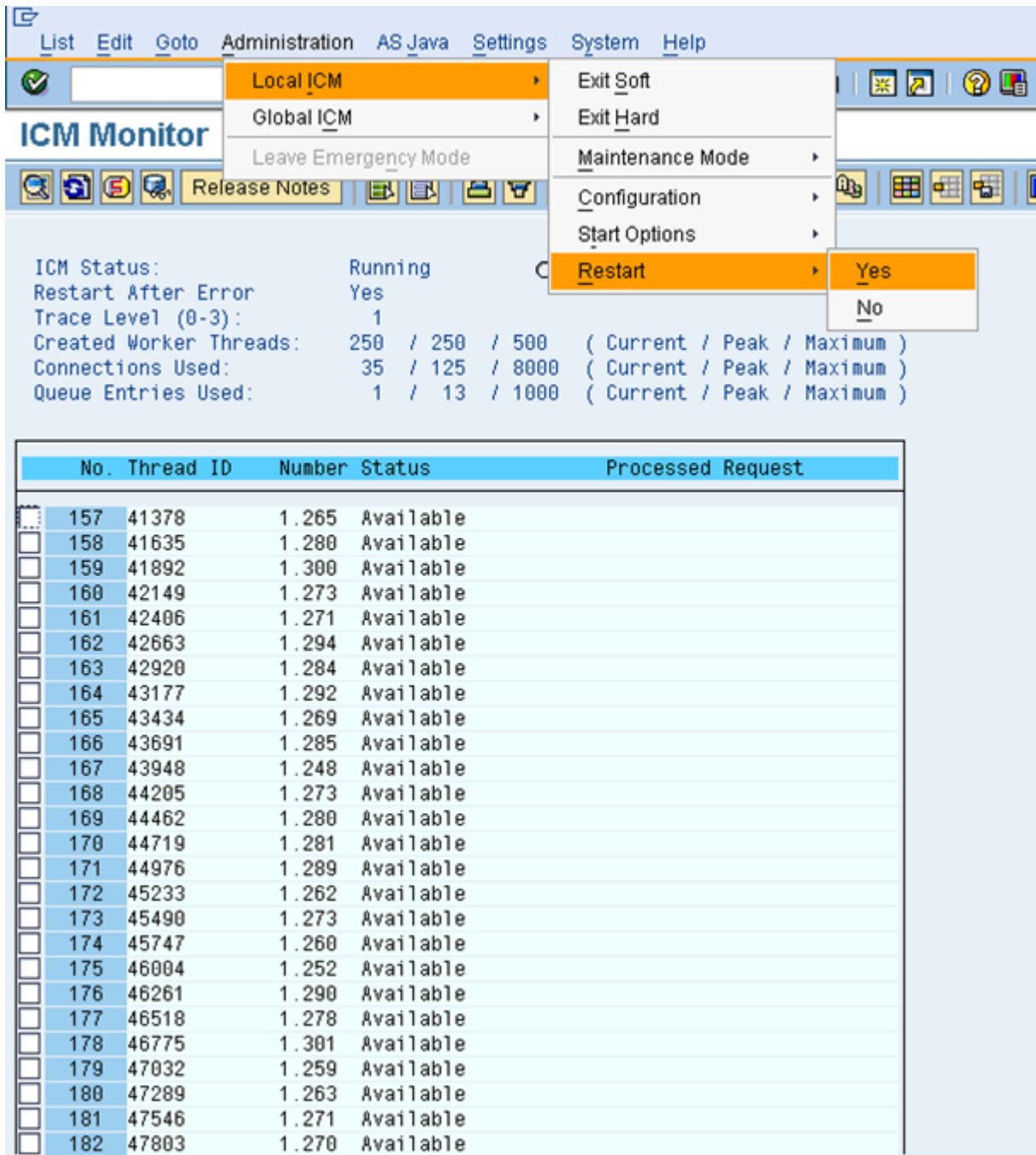
Name	Service Component Name	Status
SLD Data Supplier	sap.com/sld	Started
SRC.zip content handler	sap.com/je-src.zip-content-handler	Started
SSL Provider	sap.com/ssl	Started
Schedüler	sap.com/scheduler	Started
Schedüler API	sap.com/je-scheduler-api	Started
SchedülerRuntime	sap.com/scheduler-runtime	Started
Schema Processor Service	sap.com/schemaprocessor-srv	Started
Secure Storage	sap.com/sec-securestorage-service	Started
Security Destination Facade	sap.com/security-destination-facade	Started
Security Facade	sap.com/security-facade	Started

Service per Instance

Start Stop Restart Refresh

Service per Instance	Host	Status
SSL Provider		
• DVEBMS10 (Instance ID1038966)	pcvix100	Started

7. Restart ICM from transaction SMICM.



The screenshot shows the ICM Monitor application interface. The menu bar includes 'List', 'Edit', 'Goto', 'Administration', 'AS_Java', 'Settings', 'System', and 'Help'. The 'Local ICM' menu is open, showing options: 'Exit_Soft', 'Exit_Hard', 'Maintenance Mode', 'Configuration', 'Start Options', and 'Restart'. The 'Restart' option is highlighted, and a sub-menu is open with 'Yes' and 'No' options. Below the menu, the ICM Status is displayed as 'Running'. Other status information includes 'Restart After Error: Yes', 'Trace Level (0-3): 1', and resource usage statistics for worker threads, connections, and queue entries.

ICM Status: Running

Restart After Error: Yes

Trace Level (0-3): 1

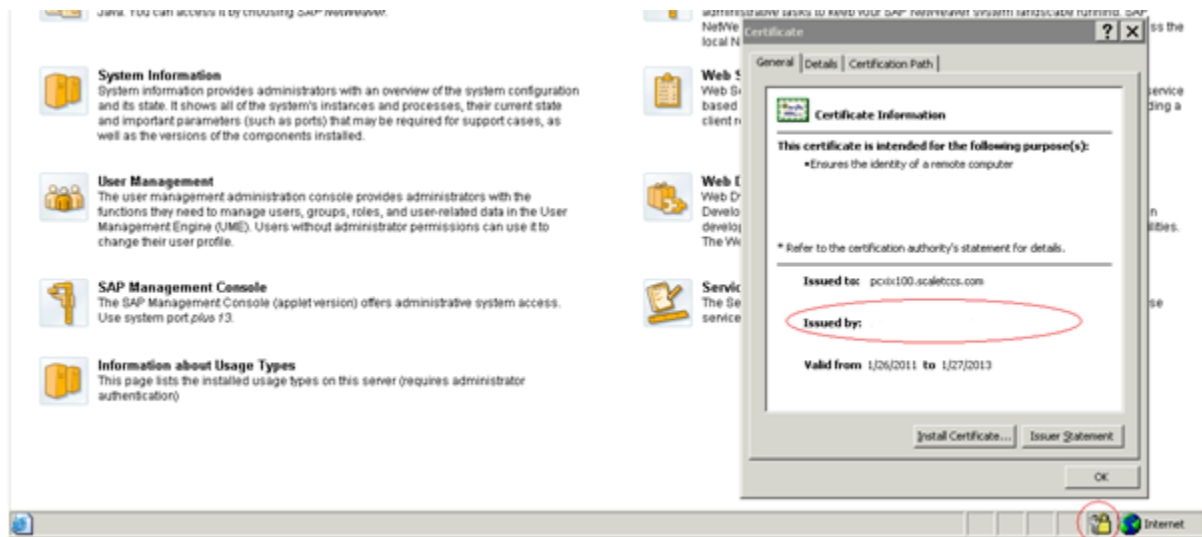
Created Worker Threads: 250 / 250 / 500 (Current / Peak / Maximum)

Connections Used: 35 / 125 / 8000 (Current / Peak / Maximum)

Queue Entries Used: 1 / 13 / 1000 (Current / Peak / Maximum)

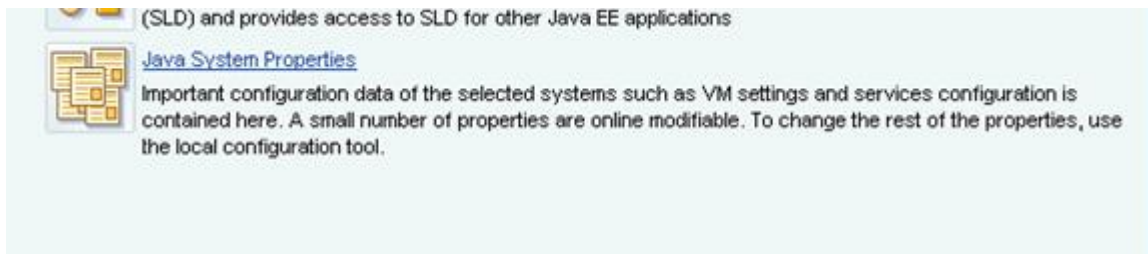
No.	Thread ID	Number	Status	Processed Request
<input type="checkbox"/>	157	41378	1.265	Available
<input type="checkbox"/>	158	41635	1.280	Available
<input type="checkbox"/>	159	41892	1.300	Available
<input type="checkbox"/>	160	42149	1.273	Available
<input type="checkbox"/>	161	42406	1.271	Available
<input type="checkbox"/>	162	42663	1.294	Available
<input type="checkbox"/>	163	42920	1.284	Available
<input type="checkbox"/>	164	43177	1.292	Available
<input type="checkbox"/>	165	43434	1.269	Available
<input type="checkbox"/>	166	43691	1.285	Available
<input type="checkbox"/>	167	43948	1.248	Available
<input type="checkbox"/>	168	44205	1.273	Available
<input type="checkbox"/>	169	44462	1.280	Available
<input type="checkbox"/>	170	44719	1.281	Available
<input type="checkbox"/>	171	44976	1.289	Available
<input type="checkbox"/>	172	45233	1.262	Available
<input type="checkbox"/>	173	45490	1.273	Available
<input type="checkbox"/>	174	45747	1.260	Available
<input type="checkbox"/>	175	46004	1.252	Available
<input type="checkbox"/>	176	46261	1.290	Available
<input type="checkbox"/>	177	46518	1.278	Available
<input type="checkbox"/>	178	46775	1.301	Available
<input type="checkbox"/>	179	47032	1.259	Available
<input type="checkbox"/>	180	47289	1.263	Available
<input type="checkbox"/>	181	47546	1.271	Available
<input type="checkbox"/>	182	47803	1.270	Available

8. Double click on lock symbol at the bottom of the browser and now you should be able to see **Issued by: <Certificate Authority>**.

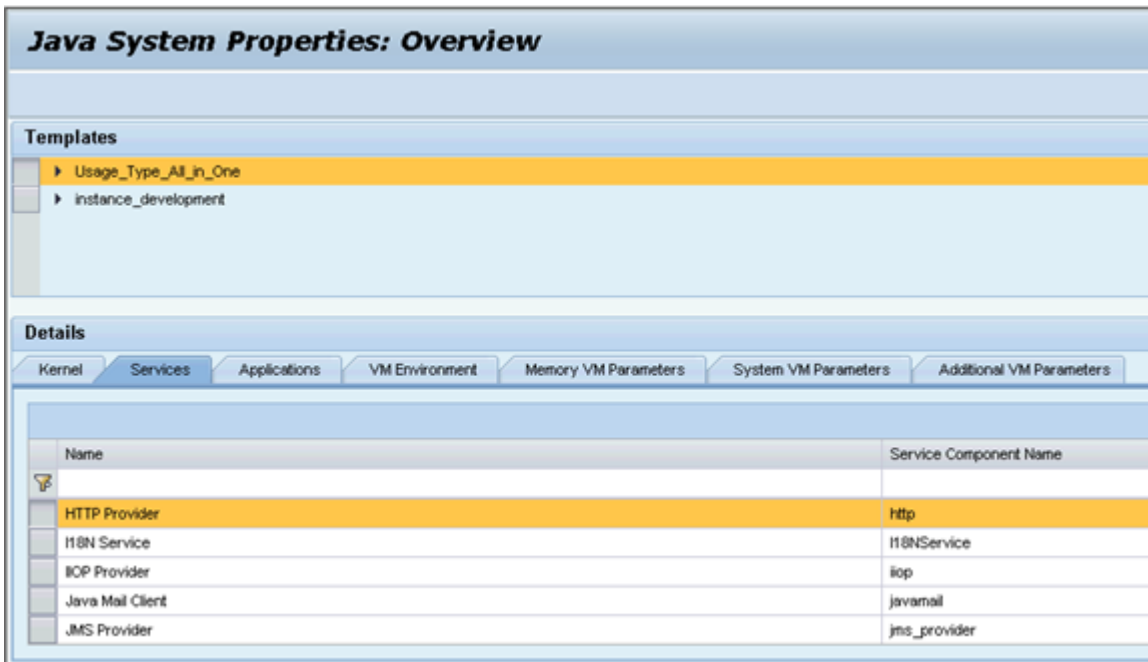


Setup HTTPS Auto Redirect, If Necessary.

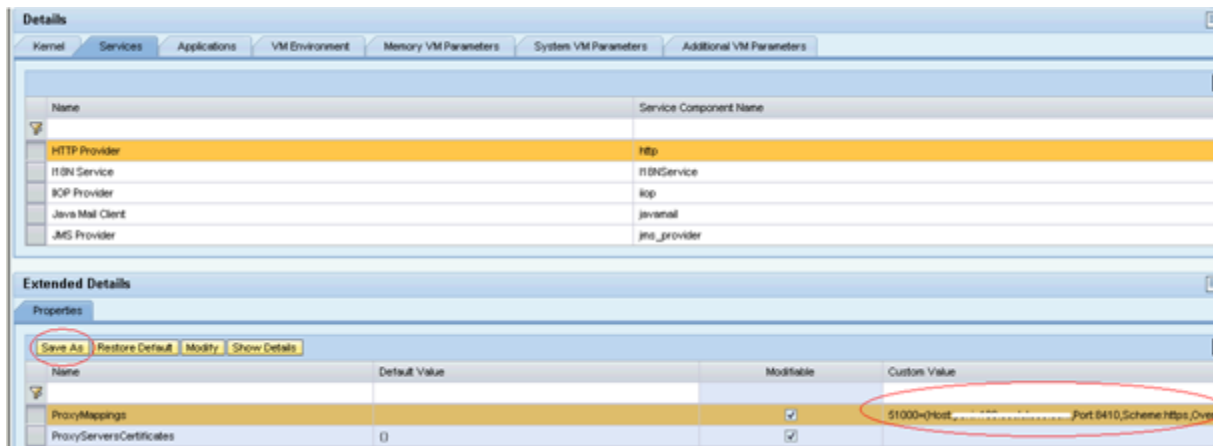
1. Open **NWA-->Configuration Management --> Infrastructure --> Java System Properties**



2. Select **HTTP Provider** service and update **Proxy Mappings** field.



ProxyMappings 5<XX>00=(Host:<FQDN>,Port:84<XX>,Scheme:https,Override:true)



3. Click **SAVE AS** to save the settings.