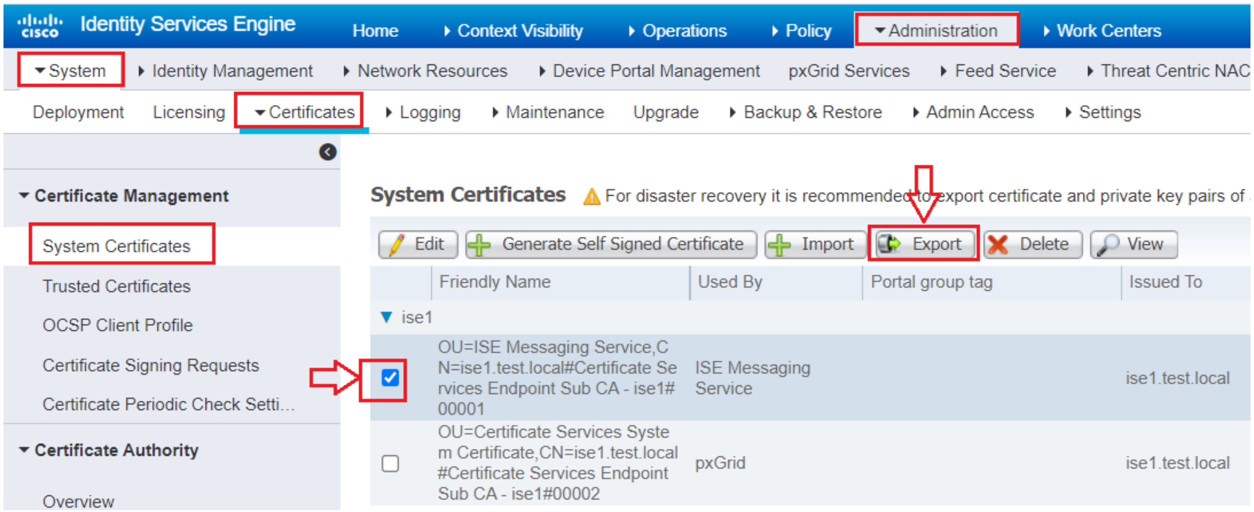
Export and Import Certificates in ISE:

ISE uses certificates for various purposes such as Web UI, Web Portals, EAP, pxGrid etc. It is important to take a backup of certificates installed on ISE nodes. There are two steps involved to import the certificate on ISE. Find out if the certificate is self-signed or 3rd party signed certificate. If the certificate is self-signed, import the public key of the certificate under trusted certificates. If the certificate is signed by some third-party certificate authority, Import Root and all other intermediate certificates of the certificate.

Export Certificate in ISE:

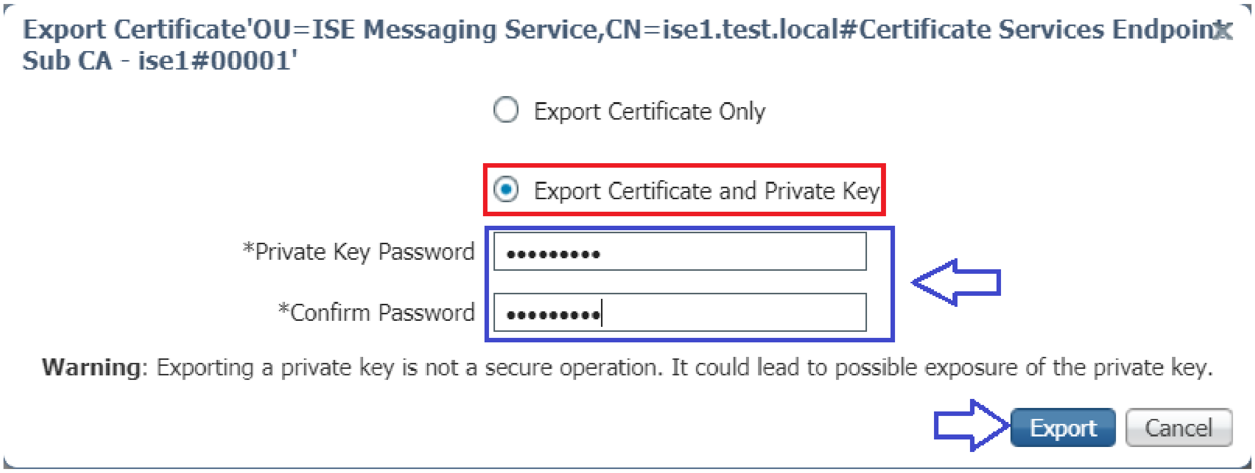
Navigate to Administration > System > Certificates > Certificate Management> System Certificates. Expand the node, select the certificate, and click Export.



System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of

	Friendly Name	Used By	Portal group tag	Issued To
▼ ise1				
☑	OU=ISE Messaging Service,CN=ise1.test.local#Certificate Services Endpoint Sub CA - ise1#00001	ISE Messaging Service		ise1.test.local
□	OU=Certificate Services System Certificate,CN=ise1.test.local#Certificate Services Endpoint Sub CA - ise1#00002	pxGrid		ise1.test.local

Select Export Certificate and Private Key. Enter a minimum 8 character in length alpha numeric password. This password is required to restore the certificate.



Export Certificate'OU=ISE Messaging Service,CN=ise1.test.local#Certificate Services Endpoint Sub CA - ise1#00001'

○ Export Certificate Only

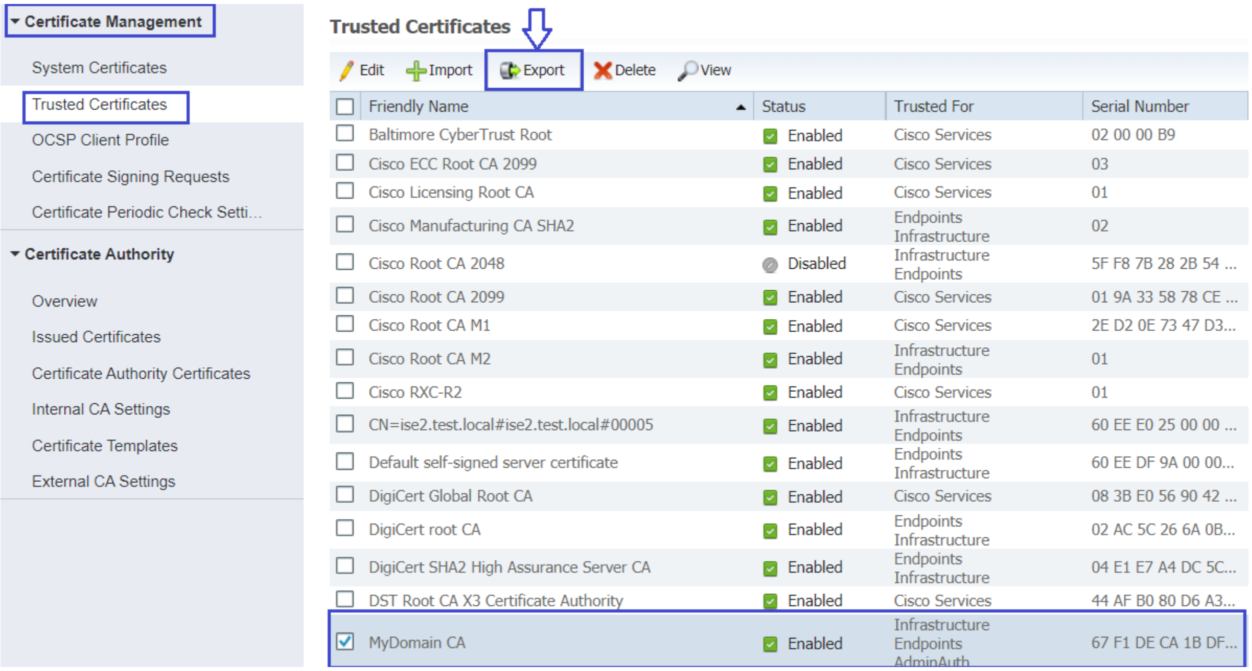
● Export Certificate and Private Key

*Private Key Password ••••••••••

*Confirm Password ••••••••••

Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private key.

Navigate to Administration > System > Certificates > Certificate Management> Trusted Certificates. Expand the node, select the certificate, and click Export.



▾ Certificate Management

System Certificates

Trusted Certificates

OCSP Client Profile

Certificate Signing Requests

Certificate Periodic Check Setti...

▾ Certificate Authority

Overview

Issued Certificates

Certificate Authority Certificates

Internal CA Settings

Certificate Templates

External CA Settings

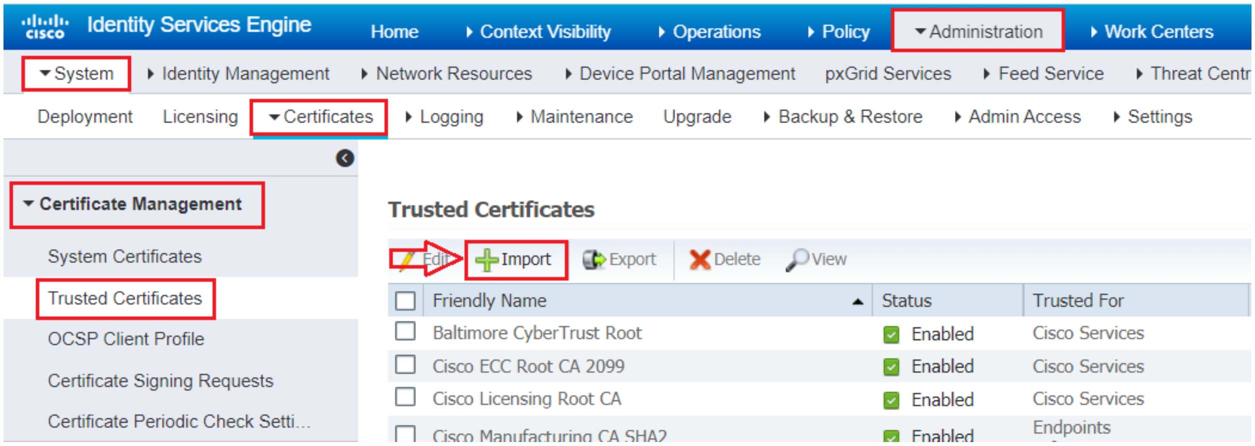
Trusted Certificates

Edit | Import | Export | Delete | View

☐	Friendly Name ▲	Status	Trusted For	Serial Number
☐	Baltimore CyberTrust Root	✓ Enabled	Cisco Services	02 00 00 B9
☐	Cisco ECC Root CA 2099	✓ Enabled	Cisco Services	03
☐	Cisco Licensing Root CA	✓ Enabled	Cisco Services	01
☐	Cisco Manufacturing CA SHA2	✓ Enabled	Endpoints Infrastructure	02
☐	Cisco Root CA 2048	● Disabled	Infrastructure Endpoints	5F F8 7B 28 2B 54 ...
☐	Cisco Root CA 2099	✓ Enabled	Cisco Services	01 9A 33 58 78 CE ...
☐	Cisco Root CA M1	✓ Enabled	Cisco Services	2E D2 0E 73 47 D3...
☐	Cisco Root CA M2	✓ Enabled	Infrastructure Endpoints	01
☐	Cisco RXC-R2	✓ Enabled	Cisco Services	01
☐	CN=ise2.test.local#ise2.test.local#00005	✓ Enabled	Infrastructure Endpoints	60 EE E0 25 00 00 ...
☐	Default self-signed server certificate	✓ Enabled	Endpoints Infrastructure	60 EE DF 9A 00 00...
☐	DigiCert Global Root CA	✓ Enabled	Cisco Services	08 3B E0 56 90 42 ...
☐	DigiCert root CA	✓ Enabled	Endpoints Infrastructure	02 AC 5C 26 6A 0B...
☐	DigiCert SHA2 High Assurance Server CA	✓ Enabled	Endpoints Infrastructure	04 E1 E7 A4 DC 5C...
☐	DST Root CA X3 Certificate Authority	✓ Enabled	Cisco Services	44 AF B0 80 D6 A3...
☑	MyDomain CA	✓ Enabled	Infrastructure Endpoints AdminAuth	67 F1 DE CA 1B DF...

Import Certificate in ISE:

Navigate to Administration > System > Certificates > Certificate Management > Trusted Certificates, click Import



cisco Identity Services Engine | Home | ▸ Context Visibility | ▸ Operations | ▸ Policy | ▾ Administration | ▸ Work Centers

▾ System | ▸ Identity Management | ▸ Network Resources | ▸ Device Portal Management | pxGrid Services | ▸ Feed Service | ▸ Threat Centr

Deployment | Licensing | ▾ Certificates | ▸ Logging | ▸ Maintenance | Upgrade | ▸ Backup & Restore | ▸ Admin Access | ▸ Settings

▾ Certificate Management

System Certificates

Trusted Certificates

OCSP Client Profile

Certificate Signing Requests

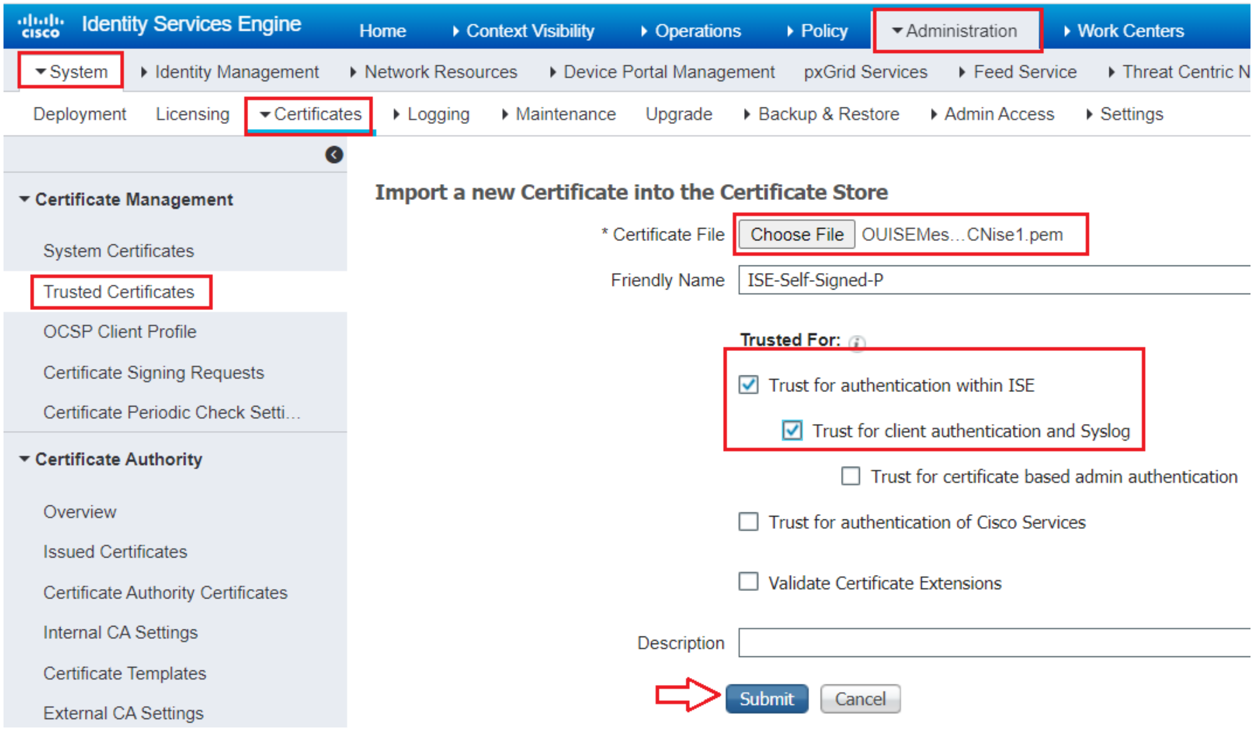
Certificate Periodic Check Setti...

Trusted Certificates

Edit | Import | Export | Delete | View

☐	Friendly Name ▲	Status	Trusted For
☐	Baltimore CyberTrust Root	✓ Enabled	Cisco Services
☐	Cisco ECC Root CA 2099	✓ Enabled	Cisco Services
☐	Cisco Licensing Root CA	✓ Enabled	Cisco Services
☐	Cisco Manufacturing CA SHA2	✓ Enabled	Endpoints

If the certificate is self-signed, import the public key of the certificate under trusted certificates. Click on Choose File to browse self-singed public key, provide Friendly name and click Submit.



Import a new Certificate into the Certificate Store

* Certificate File [Choose File] OUISEMes…CNise1.pem

Friendly Name ISE-Self-Signed-P

Trusted For:

☑ Trust for authentication within ISE

☑ Trust for client authentication and Syslog

☐ Trust for certificate based admin authentication

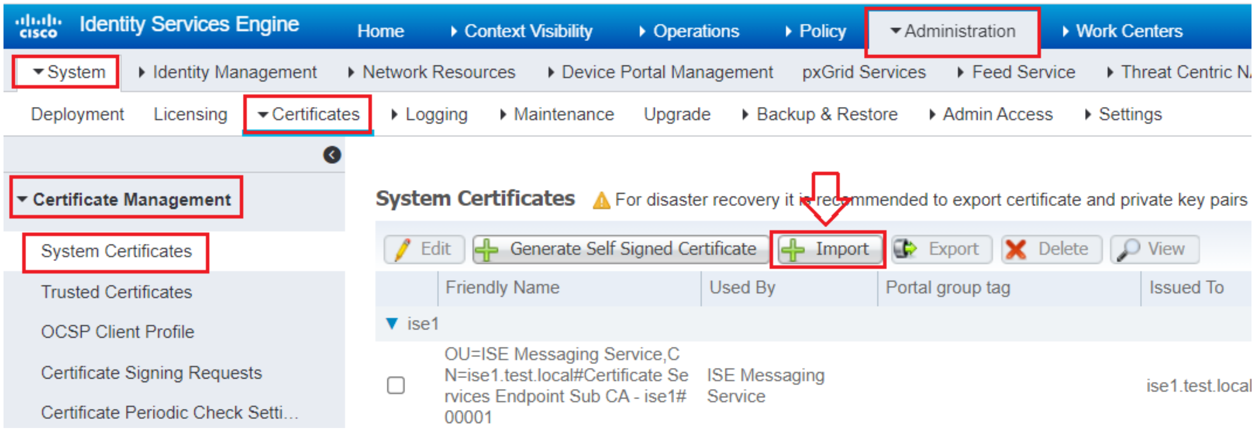
☐ Trust for authentication of Cisco Services

☐ Validate Certificate Extensions

Description

[Submit] [Cancel]

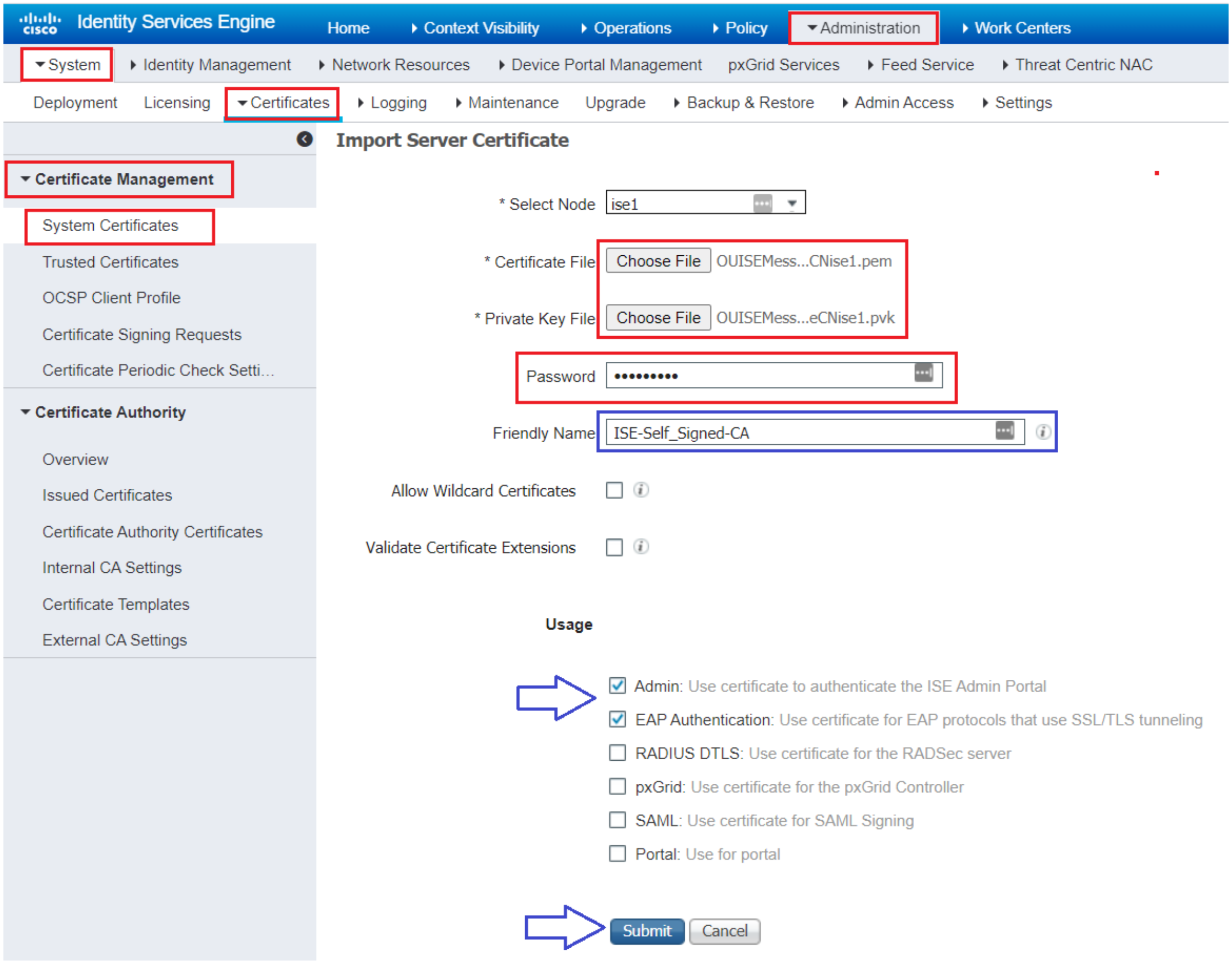
Import the actual certificate. Navigate to Administration > System > Certificates > Certificate Management> System Certificates, click Import.



System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs

	Friendly Name	Used By	Portal group tag	Issued To
▼ ise1				
☐	OU=ISE Messaging Service,CN=ise1.test.local#Certificate Services Endpoint Sub CA - ise1#00001	ISE Messaging Service		ise1.test.local

Select the node for which you want to import the certificate. Browse the public and private keys. Enter the password for the private key of the certificate and select the desired role. Now click Submit.



Import Server Certificate

* Select Node: ise1

* Certificate File: Choose File OUISEMess...CNise1.pem

* Private Key File: Choose File OUISEMess...eCNise1.pvk

Password: •••••••••

Friendly Name: ISE-Self_Signed-CA

Allow Wildcard Certificates □

Validate Certificate Extensions □

Usage

☑ Admin: Use certificate to authenticate the ISE Admin Portal

☑ EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling

□ RADIUS DTLS: Use certificate for the RADSec server

□ pxGrid: Use certificate for the pxGrid Controller

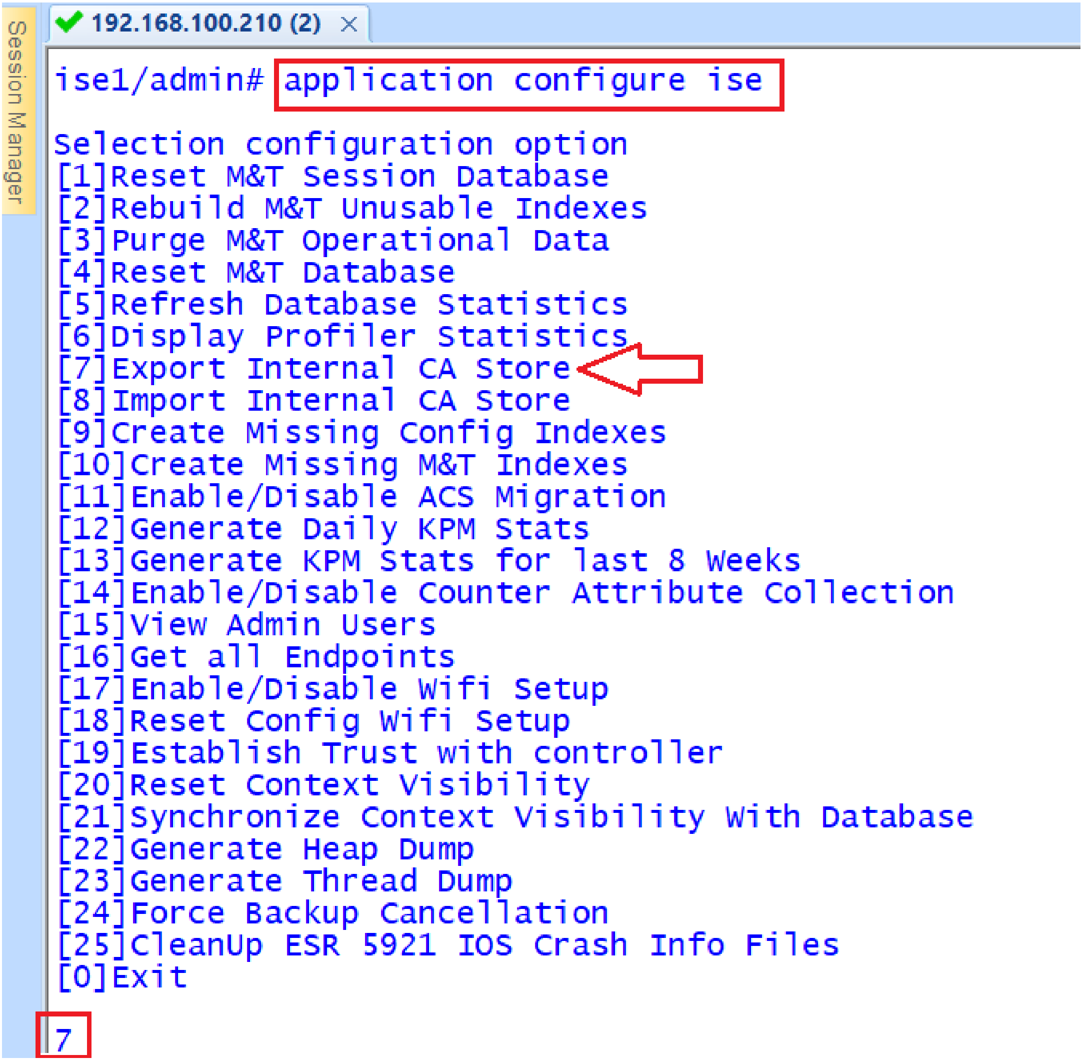
□ SAML: Use certificate for SAML Signing

□ Portal: Use for portal

Backup ISE Certificates CLI:

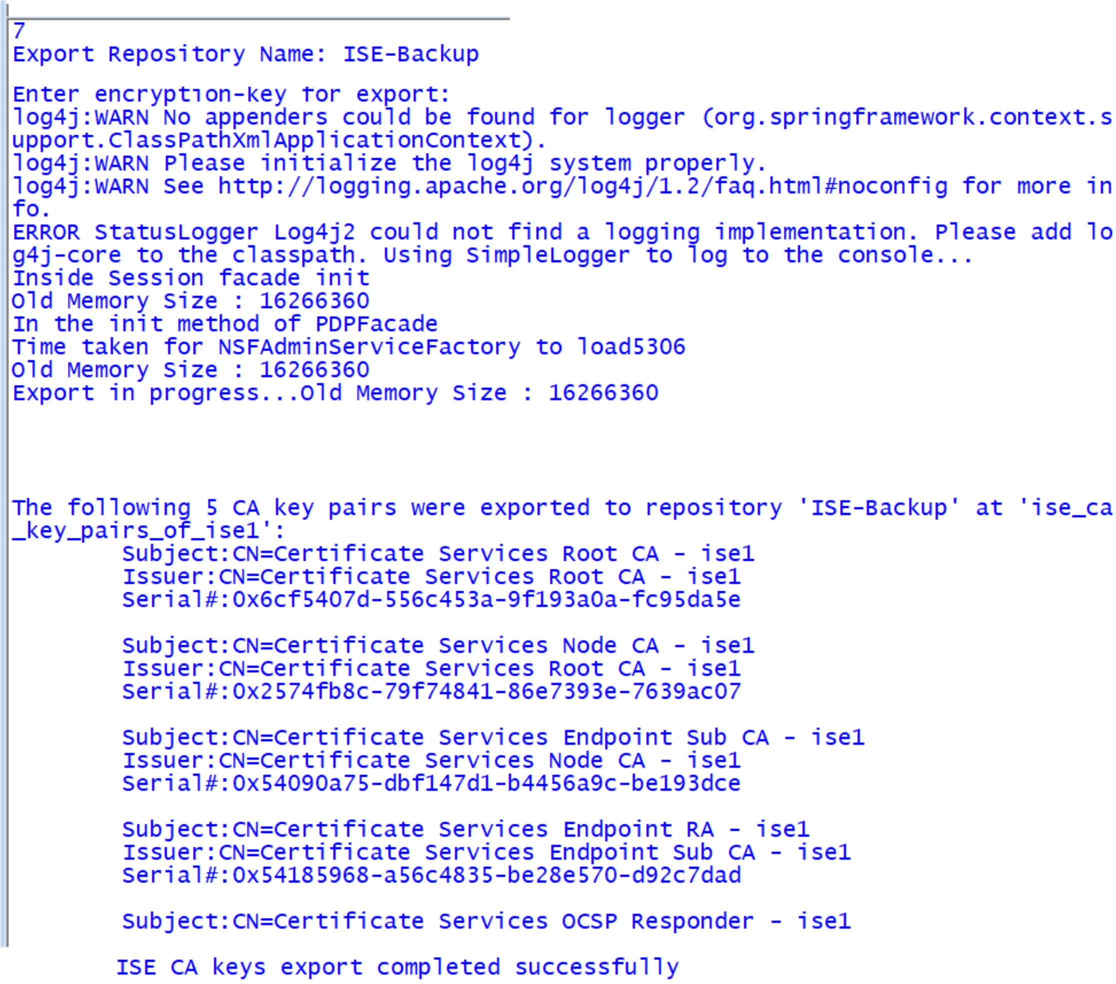
To perform Cisco ISE certification backup, you need to login CLI and run below command. Then select **option 7** and fill all the data accordingly.

ise1/admin# **application configure ise**



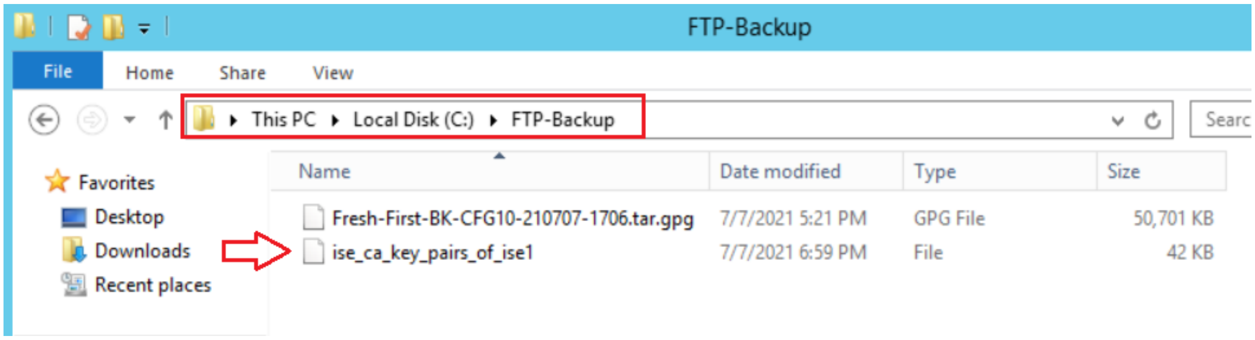
```
ise1/admin# application configure ise

Selection configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[11]Enable/Disable ACS Migration
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Enable/Disable Counter Attribute Collection
[15]View Admin Users
[16]Get all Endpoints
[17]Enable/Disable Wifi Setup
[18]Reset Config Wifi Setup
[19]Establish Trust with controller
[20]Reset Context Visibility
[21]Synchronize Context Visibility With Database
[22]Generate Heap Dump
[23]Generate Thread Dump
[24]Force Backup Cancellation
[25]CleanUp ESR 5921 IOS Crash Info Files
[0]Exit

7
```

After type 7 to Export Internal CA Store. Type the Export Repository Name and encrypted Password to start exporting Certificates.



```
7
Export Repository Name: ISE-Backup

Enter encryption-key for export:
log4j:WARN No appenders could be found for logger (org.springframework.context.s
upport.ClassPathXmlApplicationContext).
log4j:WARN Please initialize the log4j system properly.
log4j:WARN See http://logging.apache.org/log4j/1.2/faq.html#noconfig for more in
fo.
ERROR StatusLogger Log4j2 could not find a logging implementation. Please add lo
g4j-core to the classpath. Using SimpleLogger to log to the console...
Inside Session facade init
Old Memory Size : 16266360
In the init method of PDPFacade
Time taken for NSFAdminServiceFactory to load5306
Old Memory Size : 16266360
Export in progress...Old Memory Size : 16266360



The following 5 CA key pairs were exported to repository 'ISE-Backup' at 'ise_ca
_key_pairs_of_ise1':
        Subject:CN=Certificate Services Root CA - ise1
        Issuer:CN=Certificate Services Root CA - ise1
        Serial#:0x6cf5407d-556c453a-9f193a0a-fc95da5e

        Subject:CN=Certificate Services Node CA - ise1
        Issuer:CN=Certificate Services Root CA - ise1
        Serial#:0x2574fb8c-79f74841-86e7393e-7639ac07

        Subject:CN=Certificate Services Endpoint Sub CA - ise1
        Issuer:CN=Certificate Services Node CA - ise1
        Serial#:0x54090a75-dbf147d1-b4456a9c-be193dce

        Subject:CN=Certificate Services Endpoint RA - ise1
        Issuer:CN=Certificate Services Endpoint Sub CA - ise1
        Serial#:0x54185968-a56c4835-be28e570-d92c7dad

        Subject:CN=Certificate Services OCSP Responder - ise1

        ISE CA keys export completed successfully
```

Within next few minutes you will be able to see Cisco ISE Certificates files in your FTP root directory. How much time it will take, it depends.

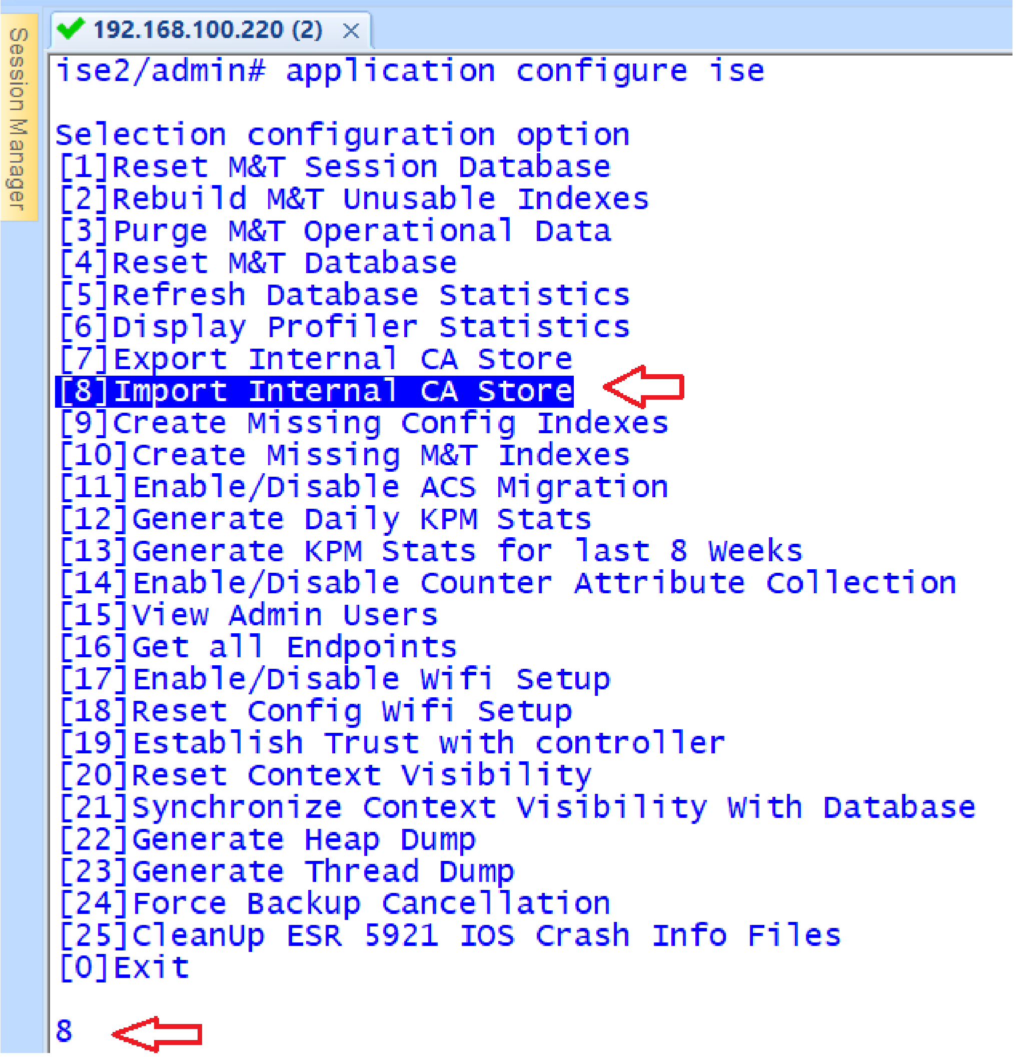


Name	Date modified	Type	Size
Fresh-First-BK-CFG10-210707-1706.tar.gpg	7/7/2021 5:21 PM	GPG File	50,701 KB
ise_ca_key_pairs_of_ise1	7/7/2021 6:59 PM	File	42 KB

Restore ISE Certificates CLI:

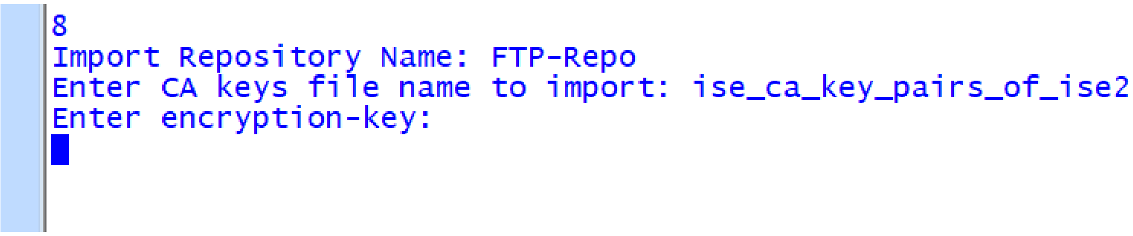
To perform Cisco ISE certification restore, you need to login CLI and run below command. Then select **option 8** and fill all the data accordingly.

ise1/admin# **application configure ise**



```
ise2/admin# application configure ise

Selection configuration option
[1]Reset M&T Session Database
[2]Rebuild M&T Unusable Indexes
[3]Purge M&T Operational Data
[4]Reset M&T Database
[5]Refresh Database Statistics
[6]Display Profiler Statistics
[7]Export Internal CA Store
[8]Import Internal CA Store
[9]Create Missing Config Indexes
[10]Create Missing M&T Indexes
[11]Enable/Disable ACS Migration
[12]Generate Daily KPM Stats
[13]Generate KPM Stats for last 8 Weeks
[14]Enable/Disable Counter Attribute Collection
[15]View Admin Users
[16]Get all Endpoints
[17]Enable/Disable Wifi Setup
[18]Reset Config Wifi Setup
[19]Establish Trust with controller
[20]Reset Context Visibility
[21]Synchronize Context Visibility With Database
[22]Generate Heap Dump
[23]Generate Thread Dump
[24]Force Backup Cancellation
[25]CleanUp ESR 5921 IOS Crash Info Files
[0]Exit

8
```

After type 8 to Import Internal CA Store. Type the Import Repository Name, File name and encrypted Password to start Importing Certificates.



```
8
Import Repository Name: FTP-Repo
Enter CA keys file name to import: ise_ca_key_pairs_of_ise2
Enter encryption-key:
```