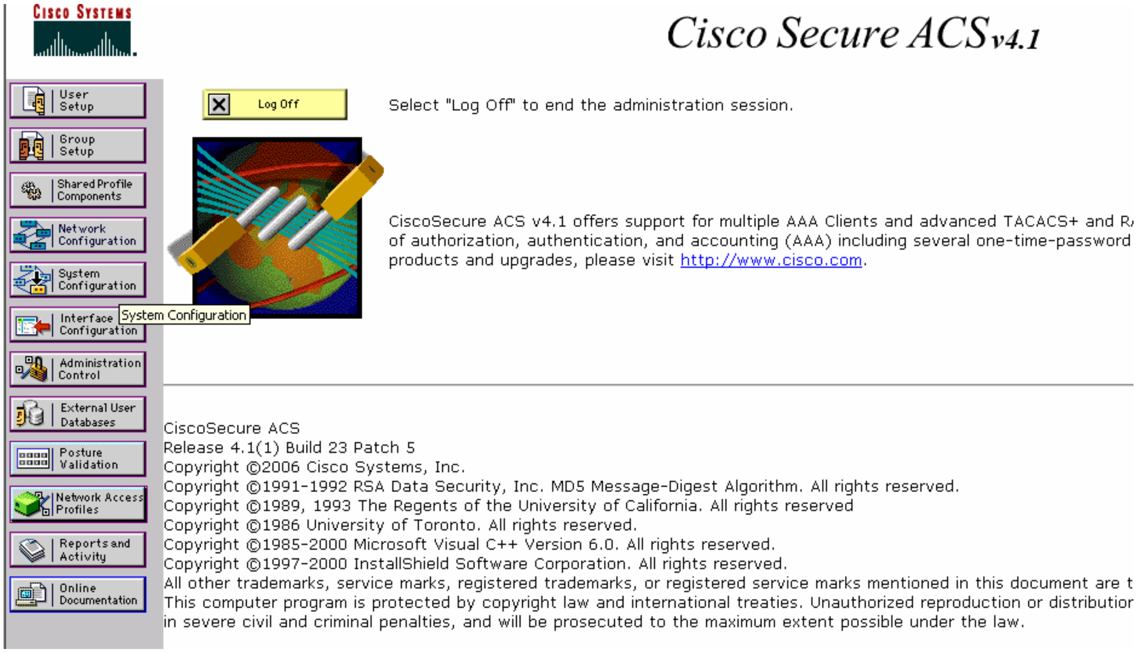
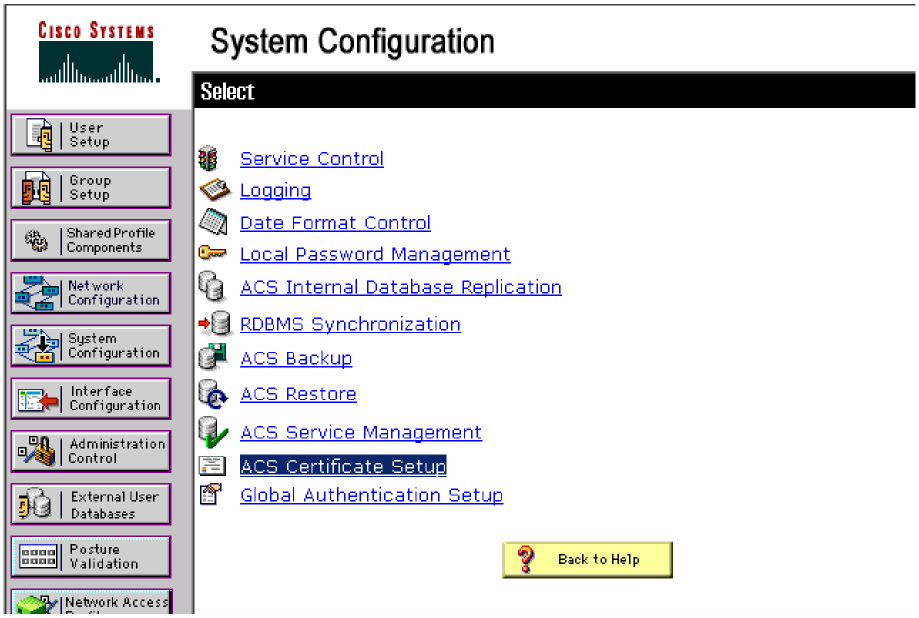


Cisco Secure ACSv4.1

Select "Log Off" to end the administration session.

CiscoSecure ACS v4.1 offers support for multiple AAA Clients and advanced TACACS+ and R
of authorization, authentication, and accounting (AAA) including several one-time-password
products and upgrades, please visit http://www.cisco.com.

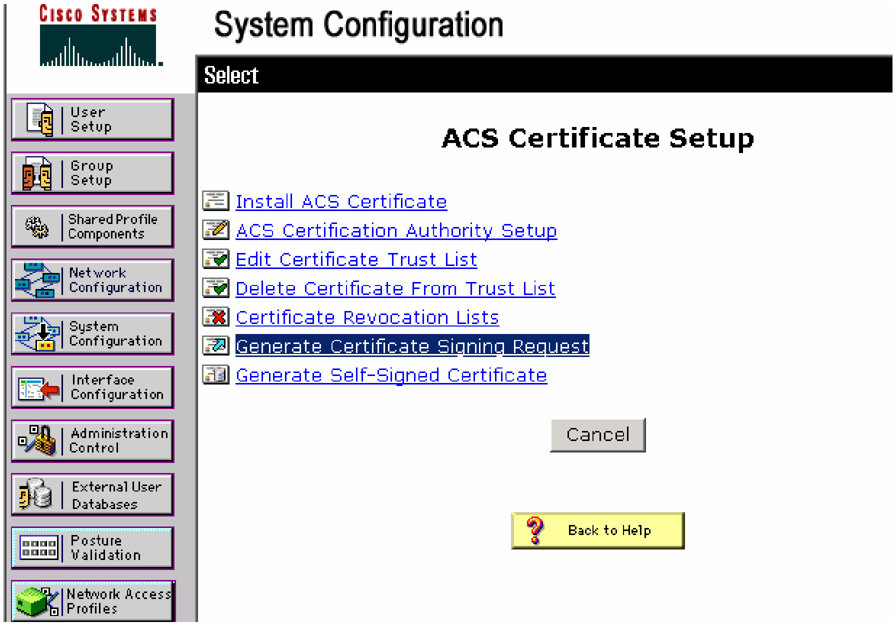
CiscoSecure ACS
Release 4.1(1) Build 23 Patch 5
Copyright ©2006 Cisco Systems, Inc.
Copyright ©1991-1992 RSA Data Security, Inc. MD5 Message-Digest Algorithm. All rights reserved.
Copyright ©1989, 1993 The Regents of the University of California. All rights reserved
Copyright ©1986 University of Toronto. All rights reserved.
Copyright ©1985-2000 Microsoft Visual C++ Version 6.0. All rights reserved.
Copyright ©1997-2000 InstallShield Software Corporation. All rights reserved.
All other trademarks, service marks, registered trademarks, or registered service marks mentioned in this document are t
This computer program is protected by copyright law and international treaties. Unauthorized reproduction or distributior
in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.



System Configuration

Select

- Service Control
- Logging
- Date Format Control
- Local Password Management
- ACS Internal Database Replication
- RDBMS Synchronization
- ACS Backup
- ACS Restore
- ACS Service Management
- ACS Certificate Setup
- Global Authentication Setup

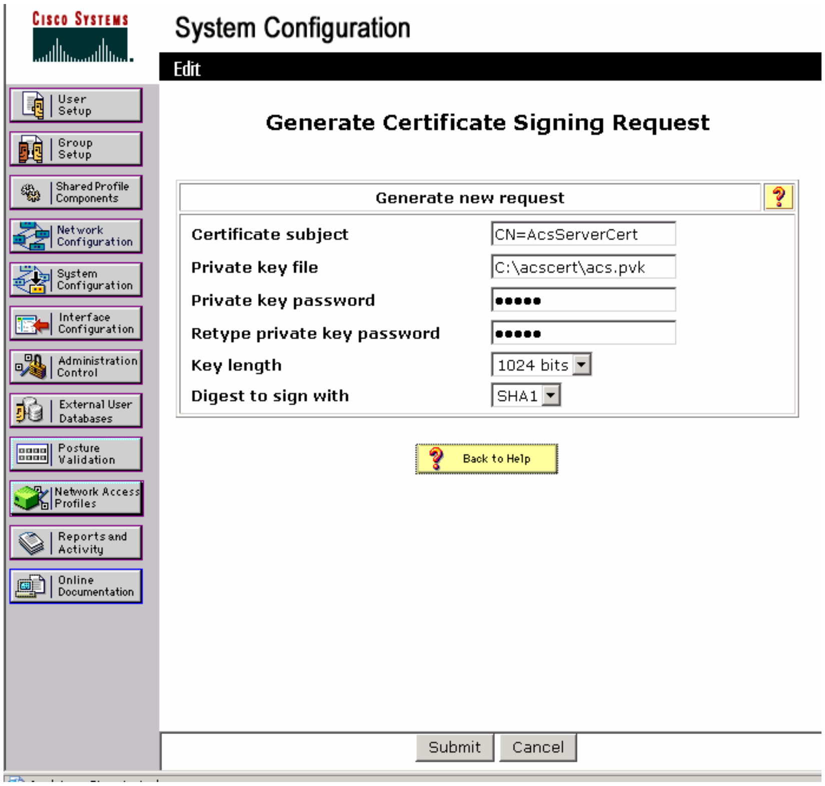


System Configuration

Select

ACS Certificate Setup

- Install ACS Certificate
- ACS Certification Authority Setup
- Edit Certificate Trust List
- Delete Certificate From Trust List
- Certificate Revocation Lists
- Generate Certificate Signing Request
- Generate Self-Signed Certificate

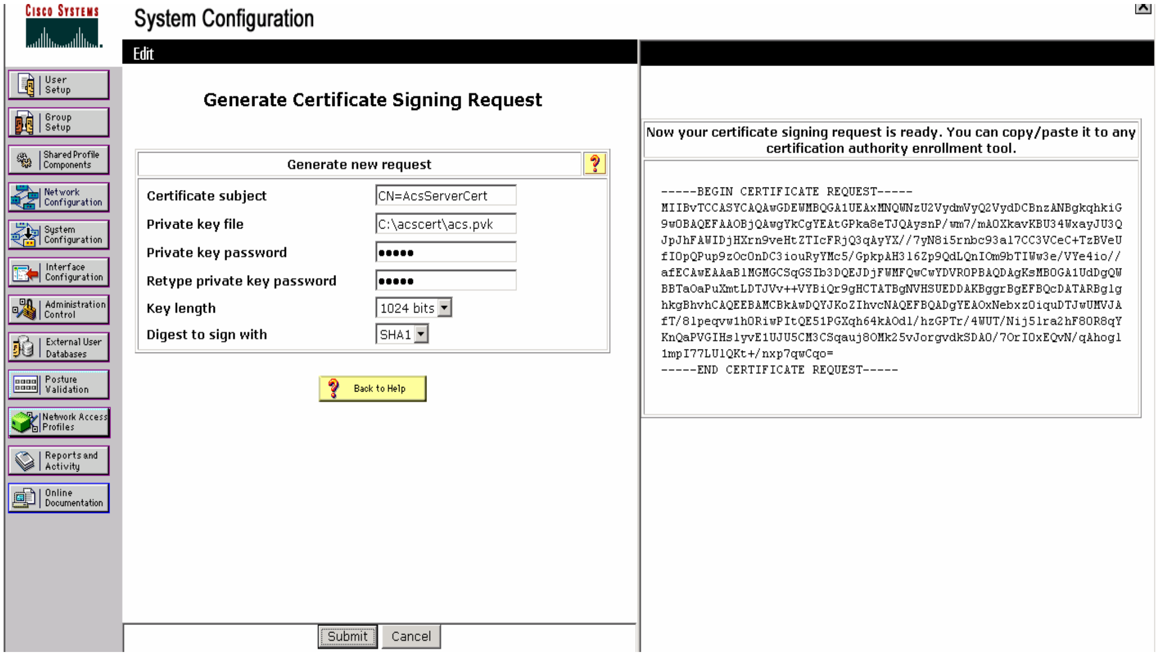


System Configuration

Edit

Generate Certificate Signing Request

Generate new request	
Certificate subject	CN=AcsServerCert
Private key file	C:\acscert\acs.pvk
Private key password	●●●●●
Retype private key password	●●●●●
Key length	1024 bits
Digest to sign with	SHA1



System Configuration

Generate Certificate Signing Request

Generate new request

Certificate subject	CN=AcsServerCert
Private key file	C:\acscert\acs.pvk
Private key password	●●●●●
Retype private key password	●●●●●
Key length	1024 bits
Digest to sign with	SHA1

Now your certificate signing request is ready. You can copy/paste it to any certification authority enrollment tool.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBvTCCASYCAQAwGDEWMBQGA1UEAxMNQWNzU2VydmVyQ2VydDCBnzANBgkqhkiG
9w0BAQEFAAOBjQAwgYkCgYEAtGPka8eTJQAysnP/wm7/mAOXkavKBU34WxayJU3Q
JpJhFAWIDjHXrn9veHtZTIcFRjQ3qAyYX//7yN8i5rnbc93al7CC3VCeC+TzBVeU
fIOpQPup9zOcOnDC3iouRyYMc5/GpkpAH3l6Zp9QdLQnIOm9bTIWw3e/VYe4io//
afECAwEAAaBlMGMGCSqGSIb3DQEJDjFWMFQwCwYDVR0PBAQDAgKsMBOGA1UdDgQW
BBTaOaPuXmtLDTJVv++VYBiQr9gHCTATBgNVHSUEDDAKBggrBgEFBQcDATARBglg
hkgBhvhCAQEEBAMCBkAwDQYJKoZIhvcNAQEFBQADgYEAOxNebxzOiquDTJwUMVJA
fT/8lpeqvw1hORiwPItQE51PGXqh64kAOdl/hzGPTr/4WUT/Nij5lra2hF8OR8qY
KnQaPVGIHslyvE1UJU5CM3CSqauj8OMk25vJorgvdkSDAO/7OrIOxEQvN/qAhogl
1mpI77LUlQKt+/nxp7qwCqo=
-----END CERTIFICATE REQUEST-----
```

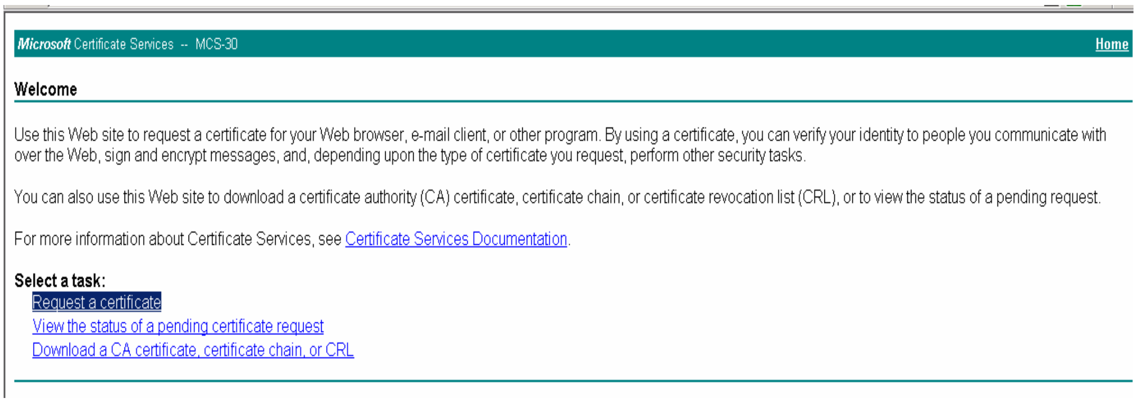
Copy the CSR on Right, and take it to Certificate Authority.

Access CA from Web Browser as,

http://<CA location>/certsrv

OR

https://<CA location>/certsrv



Welcome

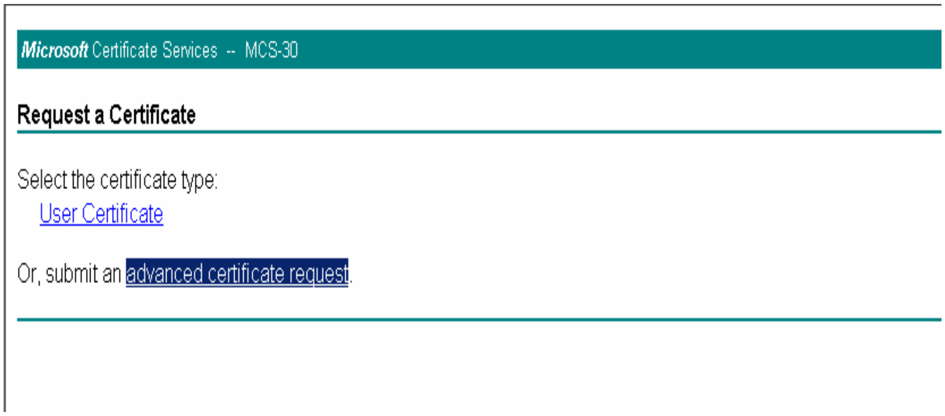
Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

Select a task:

- Request a certificate
- View the status of a pending certificate request
- Download a CA certificate, certificate chain, or CRL



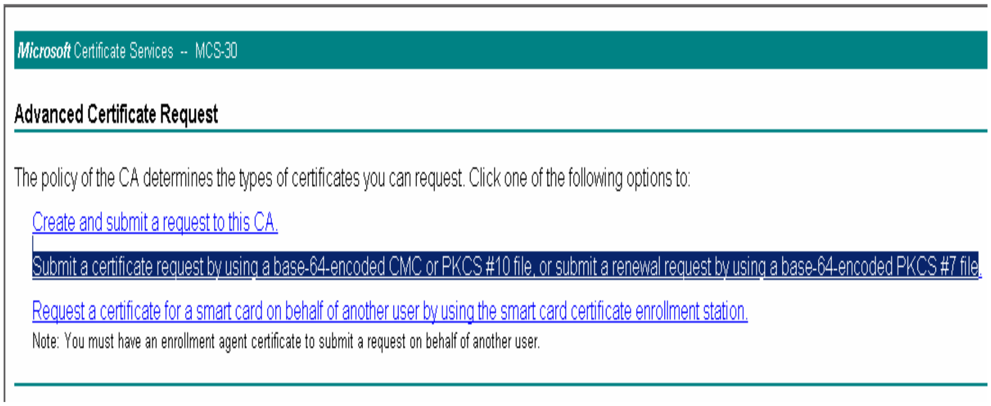
Microsoft Certificate Services -- MCS-30

Request a Certificate

Select the certificate type:

User Certificate

Or, submit an advanced certificate request.



Microsoft Certificate Services -- MCS-30

Advanced Certificate Request

The policy of the CA determines the types of certificates you can request. Click one of the following options to:

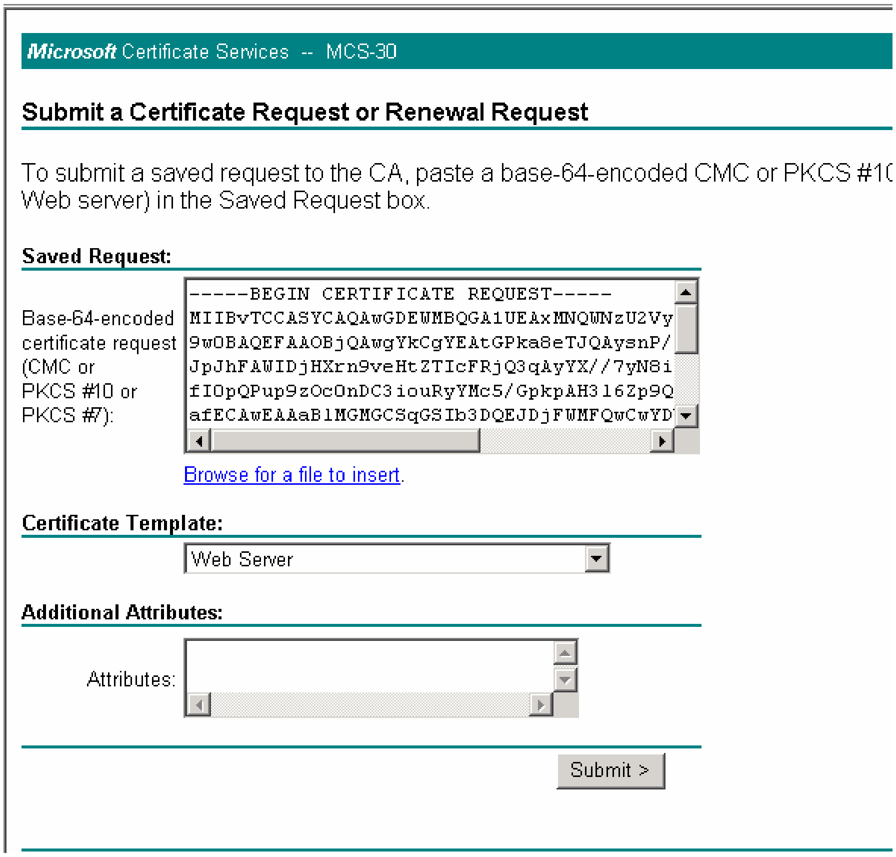
Create and submit a request to this CA.

Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station.

Note: You must have an enrollment agent certificate to submit a request on behalf of another user.

Paste the CSR generated from ACS into the box below. And choose Certificate Template as Web Server. Then press Submit.



Microsoft Certificate Services -- MCS-30

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #1(
Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBvTCCASYCAQAwGDEWMBQGA1UEAxMNQWNzU2Vy
9wOBAQEFAAOBjQAwgYkCgYEAtGPka8eTJQAysnP/
JpJhFAWIDjHXrn9veHtZTIcFRjQ3qAyYX//7yN8i
fIOpQPup9zOcOnDC3iouRyYMc5/GpkpAH316Zp9Q
afECAwEAAaB1MGMGCSqGSIb3DQEJDjFWMFQwCwYD
```

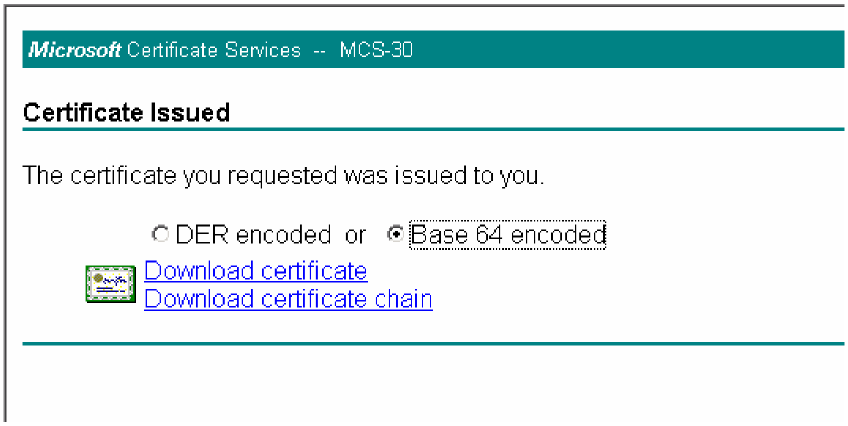
Browse for a file to insert.

Certificate Template:

Web Server

Additional Attributes:

Attributes:



Microsoft Certificate Services -- MCS-30

Certificate Issued

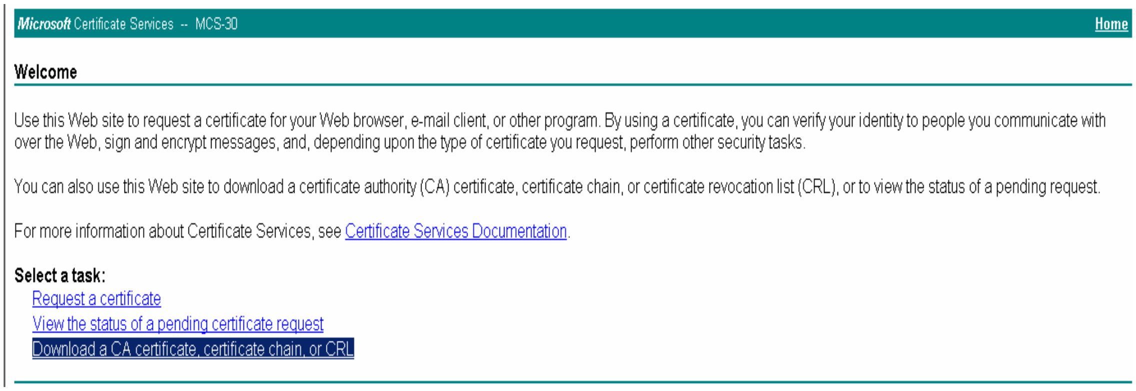
The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

Download certificate
Download certificate chain

Click on “Download certificate” and save that certificate with a recognizable name.

Go back to home page of CA,



Microsoft Certificate Services -- MCS-30 Home

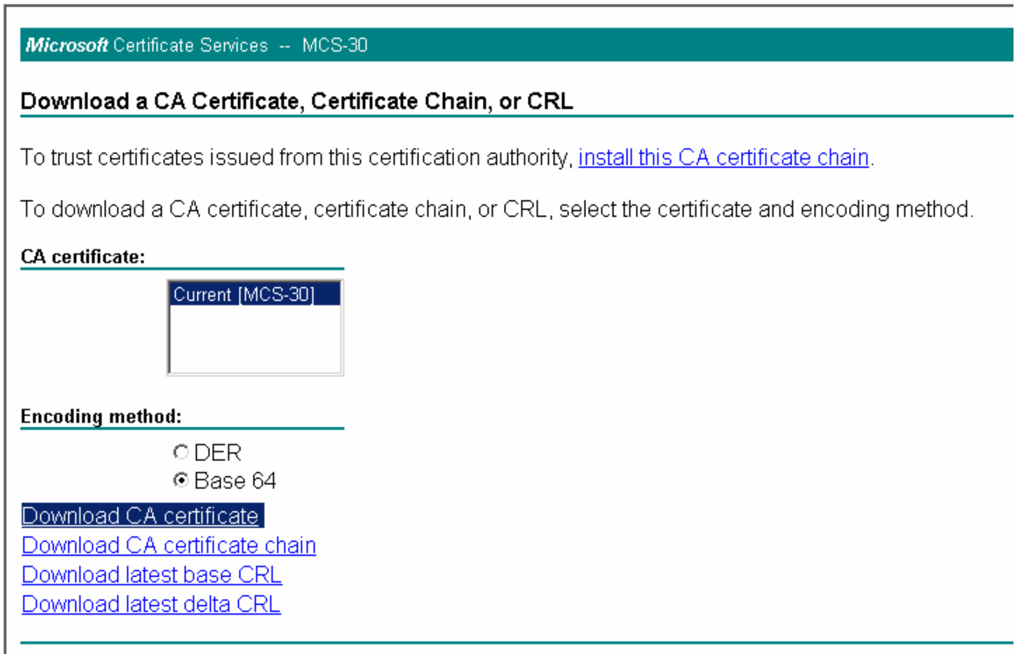
Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your identity to people you communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security tasks.

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to view the status of a pending request.

For more information about Certificate Services, see Certificate Services Documentation.

Select a task:
Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL



Microsoft Certificate Services -- MCS-30

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate chain.

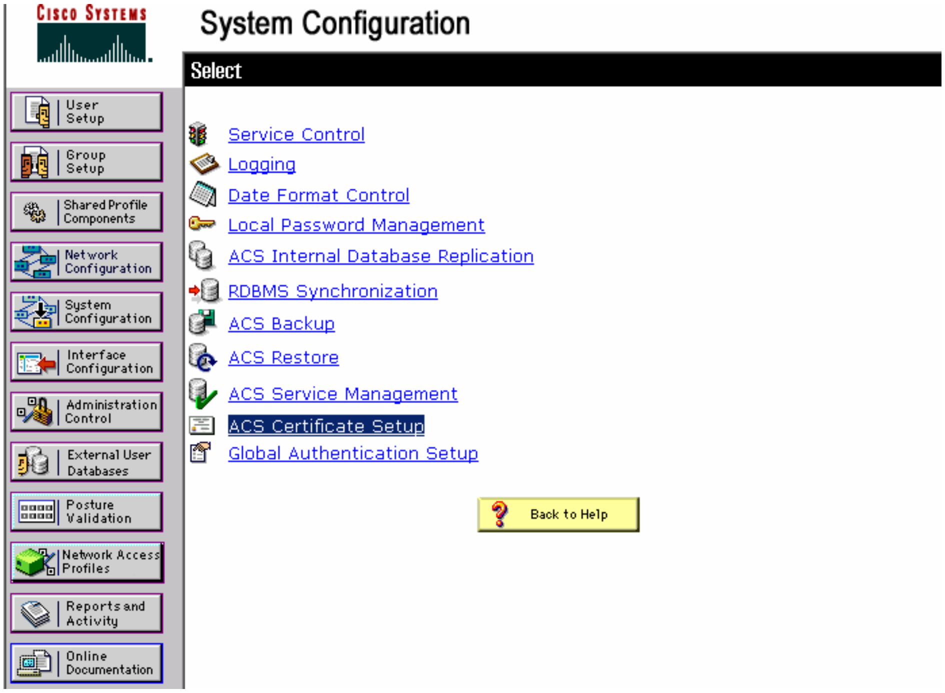
To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

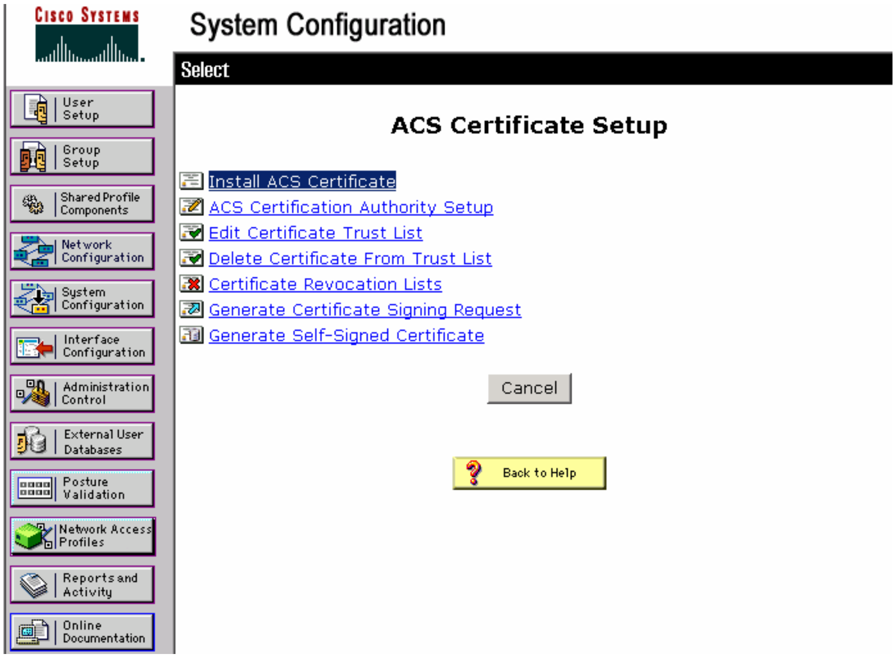
CA certificate:
Current [MCS-30]

Encoding method:
○ DER
● Base 64

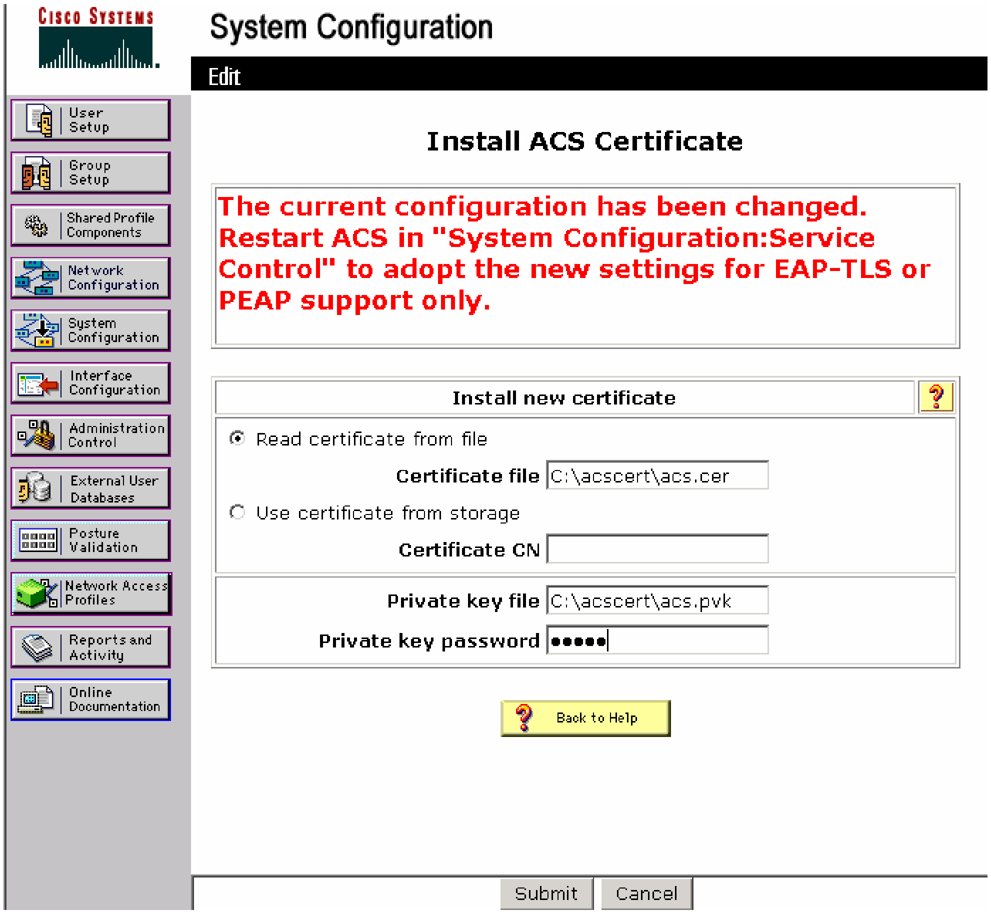
Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

Save the CA certificate with some recognizable name. This certificate is different from the Web Server certificate that we got for ACS.


Cisco Systems
System Configuration
Select
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
Service Control
Logging
Date Format Control
Local Password Management
ACS Internal Database Replication
RDBMS Synchronization
ACS Backup
ACS Restore
ACS Service Management
ACS Certificate Setup
Global Authentication Setup
Back to Help


Cisco Systems
System Configuration
Select
User Setup
Group Setup
Shared Profile Components
Network Configuration
System Configuration
Interface Configuration
Administration Control
External User Databases
Posture Validation
Network Access Profiles
Reports and Activity
Online Documentation
ACS Certificate Setup
Install ACS Certificate
ACS Certification Authority Setup
Edit Certificate Trust List
Delete Certificate From Trust List
Certificate Revocation Lists
Generate Certificate Signing Request
Generate Self-Signed Certificate
Cancel
Back to Help

Then click on Install New Certificate,



System Configuration

Install ACS Certificate

The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.

Install new certificate

● Read certificate from file

Certificate file C:\acscert\acs.cer

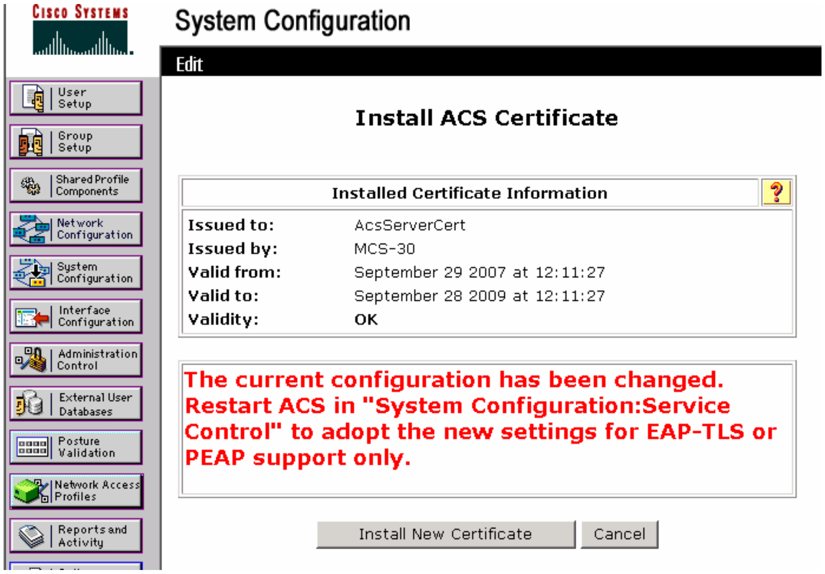
○ Use certificate from storage

Certificate CN

Private key file C:\acscert\acs.pvk

Private key password ●●●●●

Specify the ACS server certificate location and re-type the private key password, then press “Submit”



System Configuration

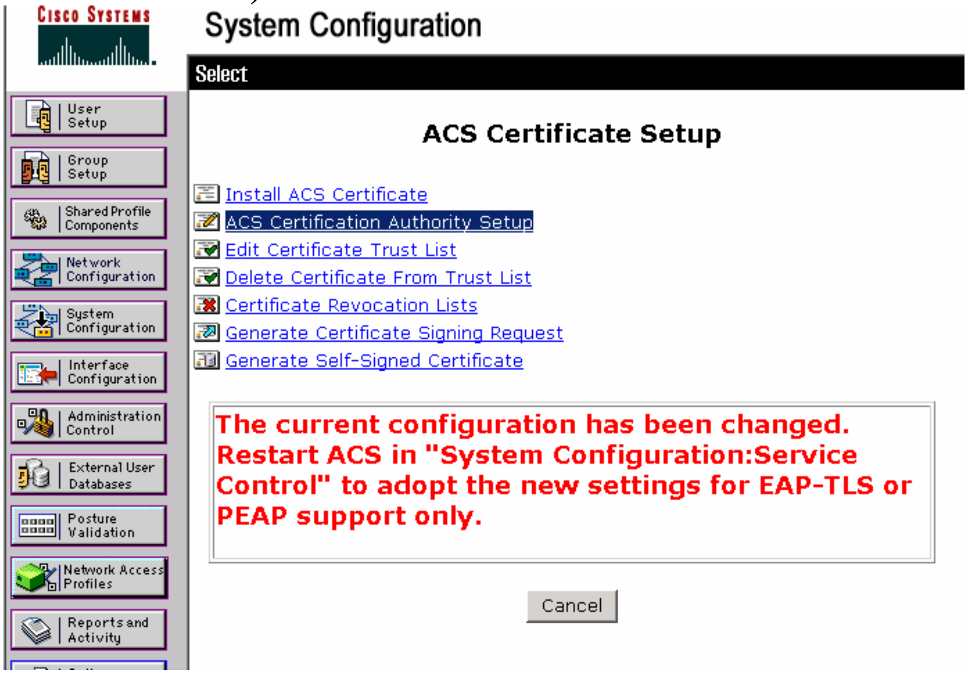
Install ACS Certificate

Installed Certificate Information

Issued to:	AcsServerCert
Issued by:	MCS-30
Valid from:	September 29 2007 at 12:11:27
Valid to:	September 28 2009 at 12:11:27
Validity:	OK

The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.

Then go to ACS Certificate Authority Setup. And specify the root certificate(CA Certificate location)



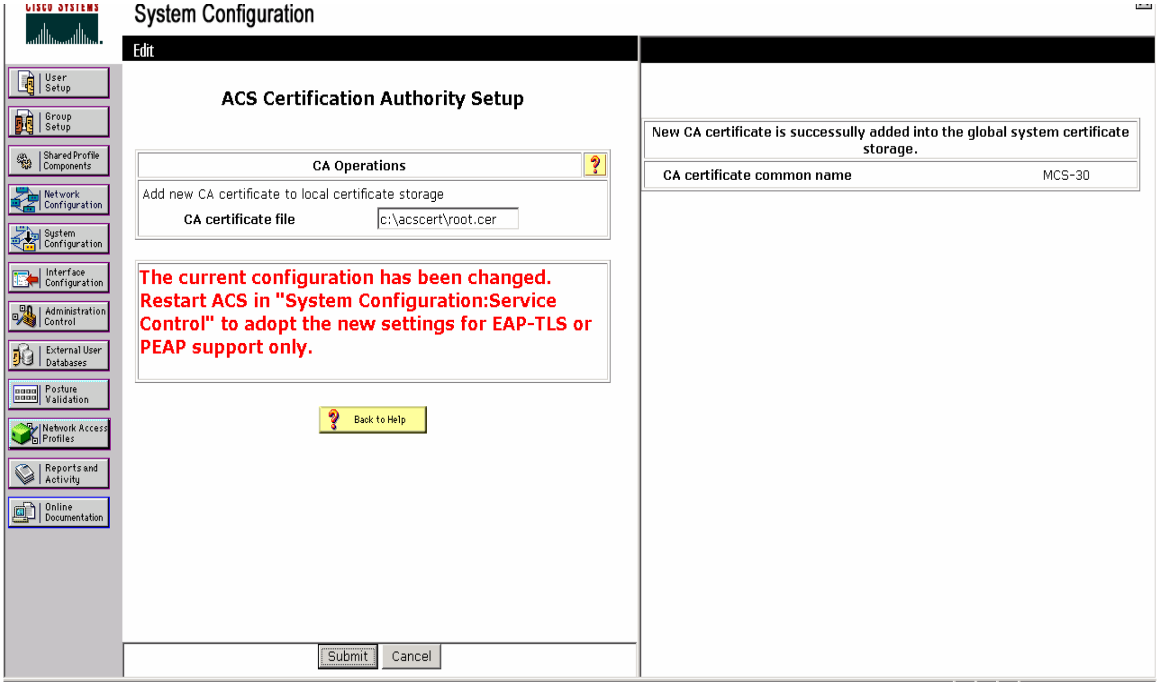
System Configuration

Select

ACS Certificate Setup

- Install ACS Certificate
- ACS Certification Authority Setup
- Edit Certificate Trust List
- Delete Certificate From Trust List
- Certificate Revocation Lists
- Generate Certificate Signing Request
- Generate Self-Signed Certificate

The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.



System Configuration

Edit

ACS Certification Authority Setup

CA Operations

Add new CA certificate to local certificate storage

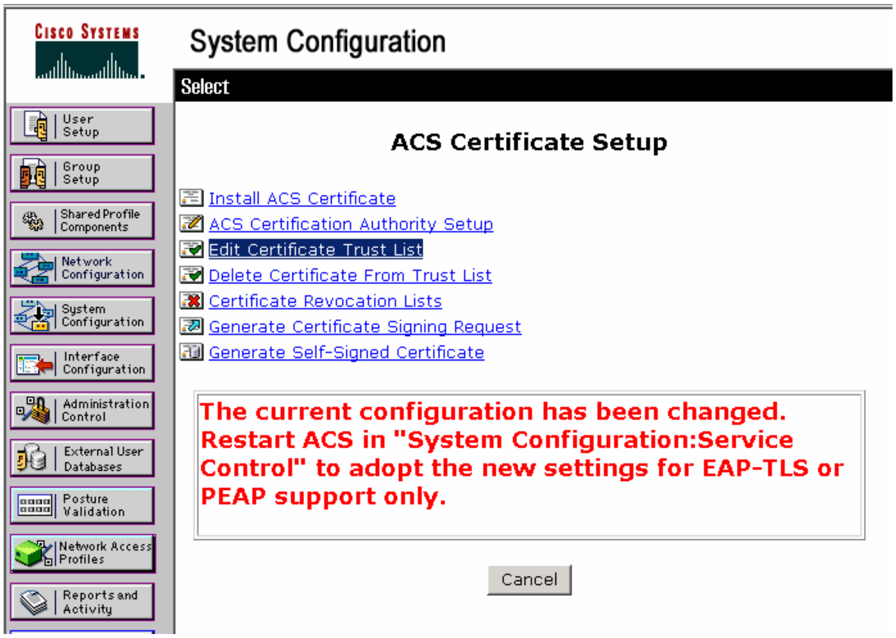
CA certificate file: c:\acscert\root.cer

The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.

New CA certificate is successully added into the global system certificate storage.

CA certificate common name: MCS-30

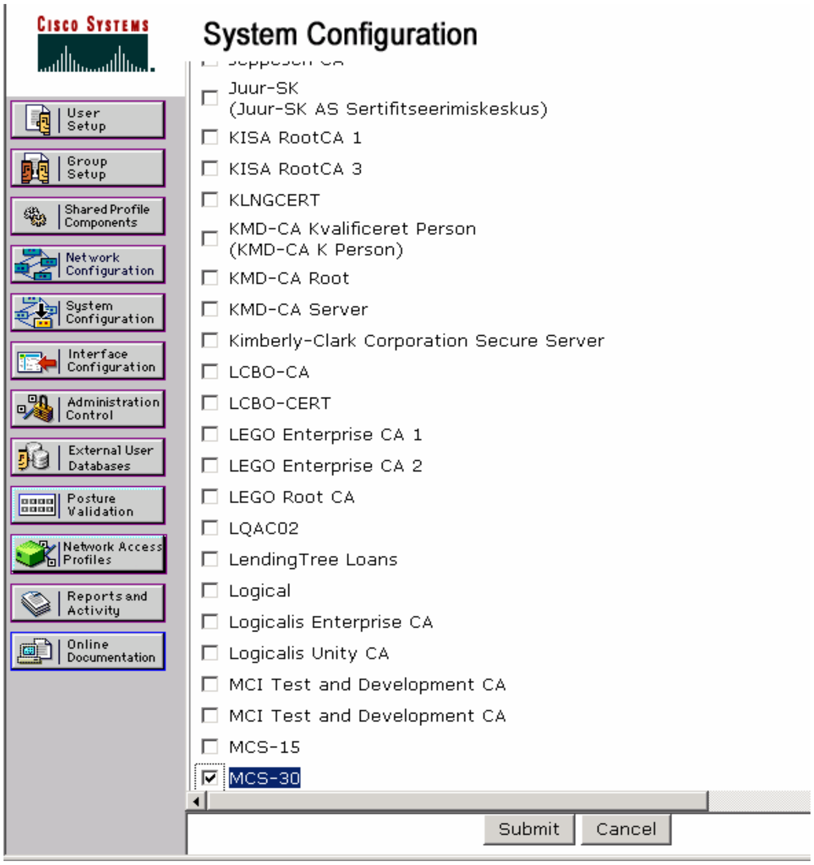
My Lab CA server(Root Certificate Authority) is MCS-30. So I'll now check the newly installed CA certificate (Root certificate) on ACS.



ACS Certificate Setup

- Install ACS Certificate
- ACS Certification Authority Setup
- Edit Certificate Trust List
- Delete Certificate From Trust List
- Certificate Revocation Lists
- Generate Certificate Signing Request
- Generate Self-Signed Certificate

The current configuration has been changed. Restart ACS in "System Configuration:Service Control" to adopt the new settings for EAP-TLS or PEAP support only.



□ Juur-SK (Juur-SK AS Sertifitseerimiskeskus)
□ KISA RootCA 1
□ KISA RootCA 3
□ KLNGCERT
□ KMD-CA Kvalificeret Person (KMD-CA K Person)
□ KMD-CA Root
□ KMD-CA Server
□ Kimberly-Clark Corporation Secure Server
□ LCBO-CA
□ LCBO-CERT
□ LEGO Enterprise CA 1
□ LEGO Enterprise CA 2
□ LEGO Root CA
□ LQAC02
□ LendingTree Loans
□ Logical
□ Logicalis Enterprise CA
□ Logicalis Unity CA
□ MCI Test and Development CA
□ MCI Test and Development CA
□ MCS-15
☑ MCS-30

Now Finally Go to System Configuration > Service Control > Restart.