6.2 Cisco Secure ACS 3.2 Appliance

This exercise will enable the Cisco Secure ACS 3.2 appliance to have identical configuration and parameter settings with the existing Cisco Secure 3.2 server version.

The configuration requires back-up of the existing Cisco Secure ACS 3.2 server database which will generate a backup database. This file will be uploaded to the Cisco Secure ACS 3.2 appliance using the 'ACS restore' utility.

The configuration process involves the following activities:

i. Initialization of Cisco Secure 3.2 appliance
ii. Uploading of current Cisco Secure ACS 3.2 server database (configuration parameters only) into Cisco Secure ACS 3.2 appliance
iii. Generate certificate signing request for digital certificate issuance
iv. Digital certificate installation
v. Add and configure Cisco Remote Agent

In summary, the configuration will replicate existing Cisco Secure ACS 3.2 server configuration settings into the ACS 3.2 appliance, except:

- Digital certificate – both ACS 3.2 applications need unique digital certificate as proof of identity.
- Log files for successful and failed authentication attempts

The following Figure 10 is the Home menu of Cisco Secure ACS 3.2 appliance.

Figure 1. Cisco Secure ACS 3.2 Home menu

Configuration Procedures

The Cisco Secure ACS 3.2 configuration procedures will be executed in the following sequence:

a. Initialization of ACS 3.2 appliance
b. Uploading database file
c. Generate certificate signing request
d. Install digital certificate
e. Add Cisco Remote Agent to the Cisco ACS 3.2 appliance
f. Configure Cisco Remote Agent for Windows Remote Agent Selection

Task 1. Initialization of Cisco Secure ACS 3.2 appliance

Purpose:- To configure appliance with network parameters (IP Address, netmask and gateway), assigning Hostname and Domain Name and setting up the admin access via web-browser.

Requirements:- Cisco ACS 3.2 appliance needs to be accessed via console port in Command Line Interface (CLI) mode. It requires a DB-9-to-RJ45 console adapter, a RJ-45 console cable and any pc/workstation with console (COM) port.

Prepare connection to the network by connecting the appliance network port to the network switch using a straight-through RJ-45 cable.

Note:- The Cisco router DB-9 console adapter and console cable can be used to access the console port.

Step 1. Connect the DB-9 console adapter and console cable to the appliance console port. Make sure the COM port of the workstation (running on Microsoft)

intended to configure the appliance is working fine.

Step 2. Use the HyperTerminal utility (or any console session utility) to initialize communication with the COM port. Set all values to default, except for the baud rate. Configure the baud rate to 115200.

Baud = 115200
Databits = 8
Parity = N
Stops = 1
Flow control = None

Step 3. Power on the ACS appliance.

Step 4. Login to the appliance, using the following (default) access ID:

Username: Administrator
Password : setup

Step 5. Follow the configuration wizard to configure the following:

- Hostname
- Domain name
- New Administrator account name and password
  New admin and password account is "***admin***" and "***umacsc|sc0***"
- IP Address
- Default Gateway
- DNS Server
- Ping test
- Time

Step 6. Verify the configuration parameters. Reboot the appliance using the '*reboot'* command.

Step 7. Open a web browser (Internet Explorer 5.5 or higher). Key in the assigned IP Address in the URL text field, as follow:

http://10.8.100.250:2002/

Note:- the '2002' refers to the ACS application port number

At any time, all available commands can be displayed using the '?'.

Task 2. Uploading Backup Database File

Purpose:- To upload the existing Cisco Secure ACS 3.2 server configuration parameters into ACS appliance. This is to minimize configuration activities.

Requirements:-

a. PTM's Cisco ACS 3.2 server administrator need to backup current ACS server configuration into a database file via the 'ACS Backup' utility in the existing ACS server. The database file needs to be uploaded into the ACS appliance via FTP process.

b. FTP utility software

c. Network connectivity is up and running between Cisco ACS 3.2 appliance and management station (workstation used to access ACS 3.2 application via web-browser). If the backup database file exists in this machine, the FTP utility software must be installed here as well.

Note:-

i. The database can only be loaded into ACS with identical ACS version and service pack.

ii. The backup file can be loaded from the existing CS ACS 3.2 server or any other server. The FTP utility software must exist in the same server.

Step 1. Launch a web-browser. Key-in the ACS 3.2 appliance IP Address, as follow:

http://10.8.100.250:2002

Step 2. Access the ACS 3.2 application using the administrator username and password configured in Task 1 section. The ACS 3.2 home main menu will appear (refer to the previous Figure 10).

Step 3. Click on the 'System Configuration'. The 'System Configuration' menu will appear (Figure 11)

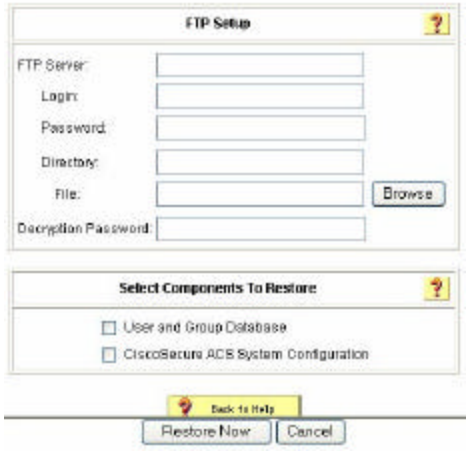
Figure 2. System Configuration Menu

Step 4. Click 'ACS Restore' link (Figure 12). The ACS Restore process requires the use of

FTP to upload and synchronize the configuration the ACS 3.2 appliance with the existing ACS 3.2 server.

The FTP Server is required to upload the database configuration file. The database configuration refers to the ACS 3.2 server configuration file that generated from the existing ACS 3.2 Server.

Figure 3. ACS Restore – FTP Setup



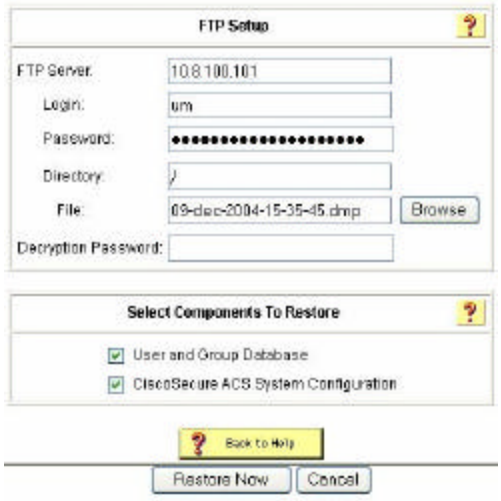
Step 5. Key-in the following information to the text fields:

FTP server : IP Address of FTP Server
Login : FTP user_name
Password : FTP user password
Directory : / (refers to FTP home directory
File : <database configuration file to upload>
Decryption Password: -none-

Select Components To Restore:
- Choose both - User and Group Database & CiscoSecure ACS System Configuration

The following Figure 13 shows the FTP upload process.

Figure 4. FTP Upload Process



Step 6. Click ‘Restore Now’ button to upload the database configuration.
When completed, the ACS 3.2 appliance will have identical configuration similar to the existing ACS 3.2 server.

However, digital certificate is excluded and requires manual configuration.

Task 3. Generate certificate signing request

Purpose:- To generate own private key and hashed information that need to be submitted to the root CA server to obtain digital certificate. This certificate will be used by the ACS 3.2 application as identity certificate.

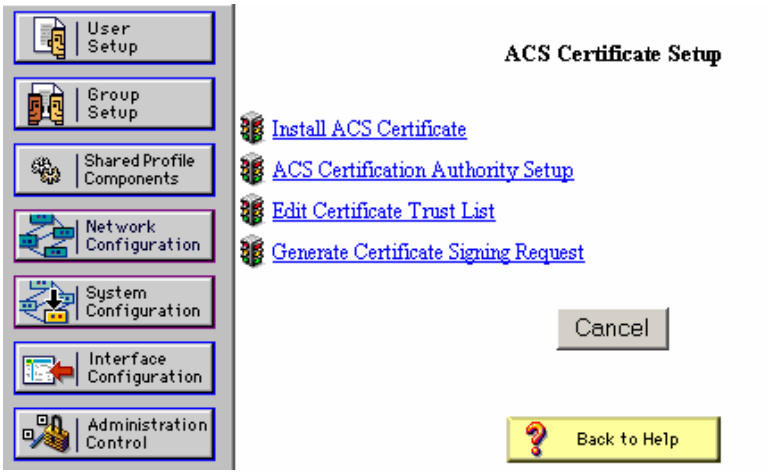
Requirements:-

a. CA Server is ready to generate an issue digital certificate

Note:-
At this section, please follow configuration steps as instructed to avoid ACS 3.2 application rejects the generate private key file.

Step 1. From the ACS 3.2 ‘System Configuration’ menu, click the ‘ACS Certificate setup’ link.
The menu will appear, as shown in Figure 14.

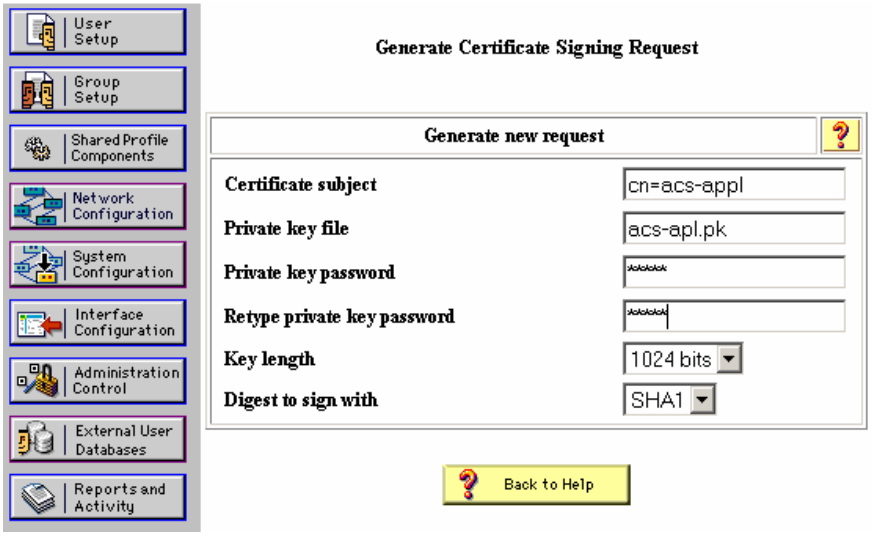
Figure 5. ACS Certificate Setup



Step 2. Click the 'Generate Certificate Signing Request'. Key-in the following parameters in the required text fields, as shown in Figure 15:

Certificate subject	: cn=acs-appl
Private key file	: acs-apl.pk
Private key password	: cisco
Retype private key password	: cisco
Key length	: 1024 (default value)
Digest to sign with	: SHA1 (default value)

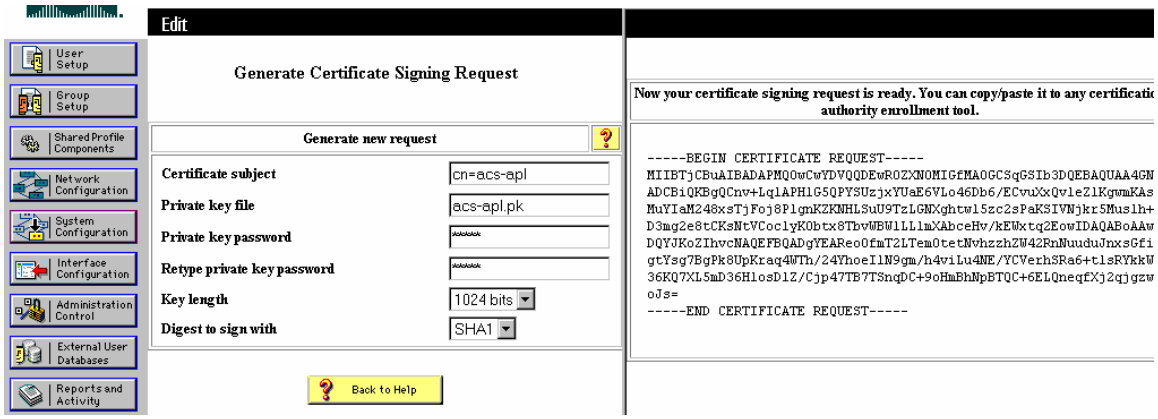
Figure 6. Generate Certificate Signing Request menu



Step 3. Click submit to proceed. The hashed information value will be displayed on the ACS 3.2 right-hand screen (Figure 16). Copy the value into a text file.

Note:- Do not exit from this current ‘Generate Certificate Signing Request’ screen.

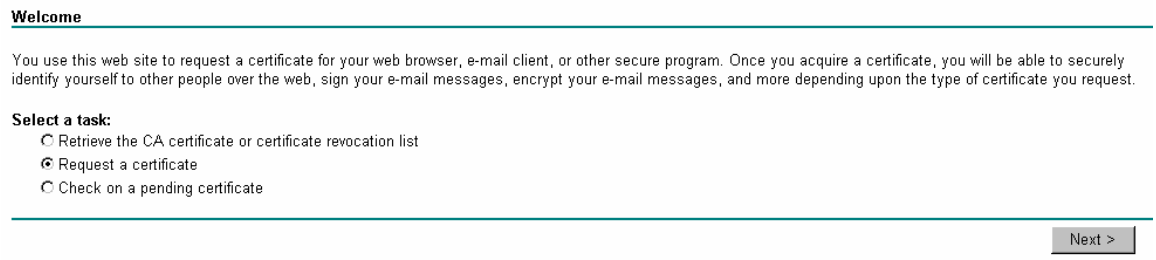
Figure 7. CS ACS 3.2 Self Generated Certificate



Step 4. Go to the CA Server menu and login as administrator.

Step 5. From the main menu, under ‘Select a task:’, select the ‘Request a certificate’ radio box and click ‘Next’ button (Figure 17).

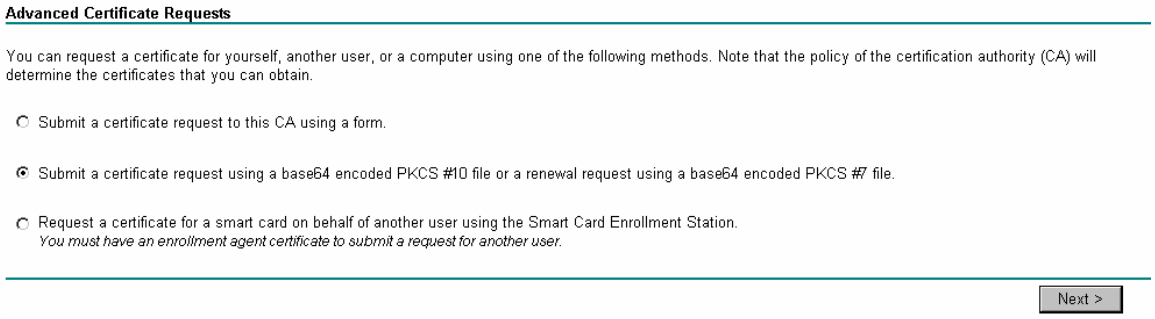
Figure 8. Request a certificate menu



Step 6. In the '**Choose Request Type**', select the 'Advanced request', and click '**Next**'.

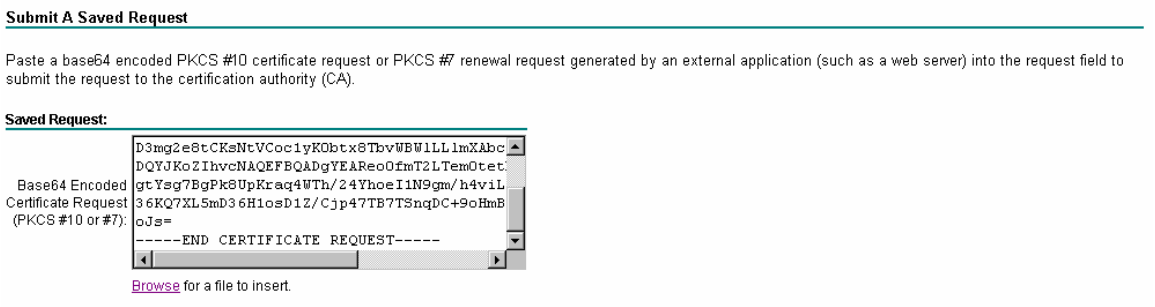
Step 7. In the '**Advanced Certificate Requests**' (Figure 18), select the '**Submit a certificate request using a base64 encoded PKCS#10 file or renewal request using a base64 encoded PKCS #7 file**' and click '**Next**'.

Figure 9. Advanced Certificate Requests menu



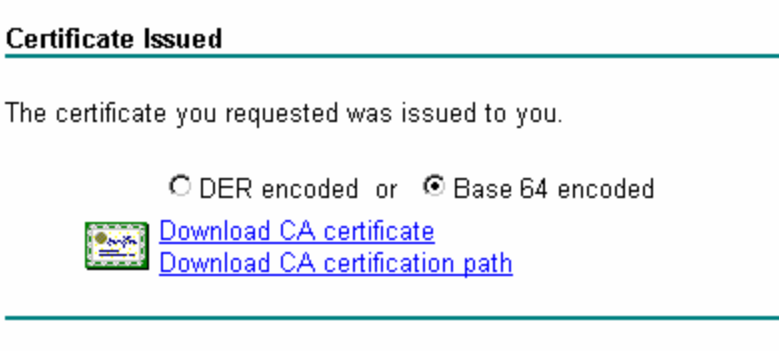
Step 8. Under the '**Submit A Saved Request**' (Figure 19), paste the hashed information value generated by the Cisco Secure ACS 3.2 in the previous Step 3 in the text box. Click 'Next' to proceed.

Figure 10. Submit A Saved Request



Step 9. Under '**Certificate Issued**' (Figure 20), choose the '**Base 64 encoded**' and '**Download CA certificate**'.

Figure 11. Certificate Issued



Choose the 'Base 64 encoded' value and download the generated digital certificate into a directory. You may rename the certificate to reflect the ACS 3.2 name.

Task 4. Install digital certificate

Purpose:- To install digital certificate for ACS 3.2 application. This certificate will be used by ACS to proof its identity and validated by the root CA server.

Requirement:-
The FTP utility software is required to upload the digital certificate into ACS 3.2 appliance.

Step 1. Return to the ACS 3.2 'Generate Certificate Signing Request' screen (refer to the previous Figure 16 in Step 3).

Step 2. Go to the 'System Configuration' and click the 'Install ACS Certificate'.

Step 3. Click Install ACS Certificate.
Cisco Secure ACS displays the Install new certificate table on the Install ACS Certificate page.

Step 4. To install a new certificate, select the Read certificate from file option and then click the Download certificate file link. The Download Certificate File page appears.

Step 5. To download the certificate file to Cisco Secure ACS, in the Download File table, follow these steps:

a. In the FTP Server box, type the IP address or hostname of the FTP server that has the certificate file you want to download.
b. In the Login box, type a valid username that Cisco Secure ACS can use to access the FTP server.
c. In the Password box, type the password for the username you specified in the Login box.
d. In the Remote FTP Directory box, type relative path from the FTP server root directory to the directory containing the certificate file you want Cisco Secure ACS to download from the FTP server.
e. e. In the Remote FTP File Name box, type the name of the certificate file you want Cisco Secure ACS to download from the FTP server.

f. Click Submit.

The system downloads the certificate file and displays the file name in Certificate file box of the Install ACS Certificate page.

Step 6. If you generated the request using Cisco Secure ACS, click the Download private key file link. The Download Private Key File page appears.

Step 7. To download the private key file to the Cisco Secure ACS, follow these steps:

a. In the FTP Server box, type the IP address or hostname of the FTP server that has the private key file you want to download.
b. In the Login box, type a valid username that Cisco Secure ACS can use to access the FTP server.
c. In the Password box, type the password for the username you specified in the Login box.
d. In the Remote FTP Directory box, type the relative path from the FTP server root directory to the directory containing the private key file you want Cisco Secure ACS to download from the FTP server.
e. In the Remote FTP File Name box, type the name of the private key file you want Cisco Secure ACS to download from the FTP server.
f. f. Click Submit.

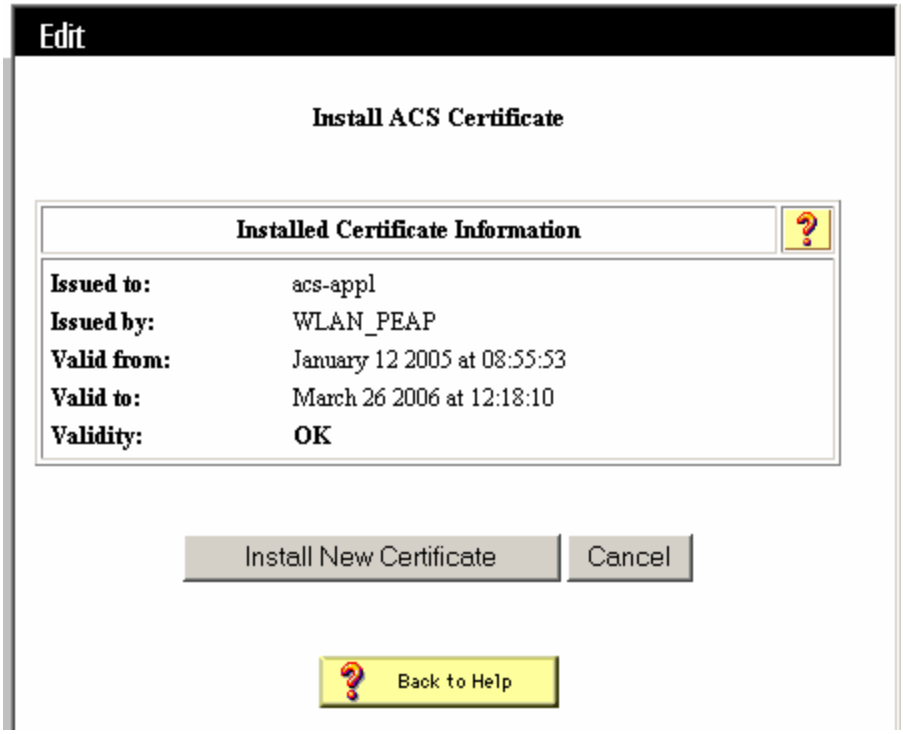
The system downloads the private key file and displays the filename in Private key file box of the Install ACS Certificate page. In the Private key password box, type the private key password.

Step 8. Click Submit.

To show that the certificate setup is complete, Cisco Secure ACS displays the Installed Certificate Information table (Figure 21), which contains the following certificate information:

Issued to: certificate subject
Issued by: CA common name
Valid from:
Valid to:
Validity

Figure 12. Installed Certificate Information


Edit
Install ACS Certificate
Installed Certificate Information
Issued to: acs-appl
Issued by: WLAN_PEAP
Valid from: January 12 2005 at 08:55:53
Valid to: March 26 2006 at 12:18:10
Validity: OK
Install New Certificate
Cancel
Back to Help