SSL Certificate – Cisco

Installation Guide

webnic
accelerate your business

Please select your version

Installation Instructions for Cisco ISE

Installation Instructions for Cisco ACS 3.2

Installation Instructions for Cisco Secure ACS 4.2

Installation Instructions for Cisco ASA 5000 Series using the Command Line

Installation Instructions for Cisco ASA 5510

Installation Instruction for Cisco ASA 5520

Installation Instructions for Cisco ISE

Step 1: Obtain the SSL Certificate

1. The Symantec certificate will be sent by email. The certificate is included as an attachment (Cert.cer) and it is also imbedded in the body of the email.
2. Copy and paste the certificate into a text file using Vi or Notepad

   The text file should look like:
   -----BEGIN CERTIFICATE-----

   [encoded data]

   -----END CERTIFICATE-----

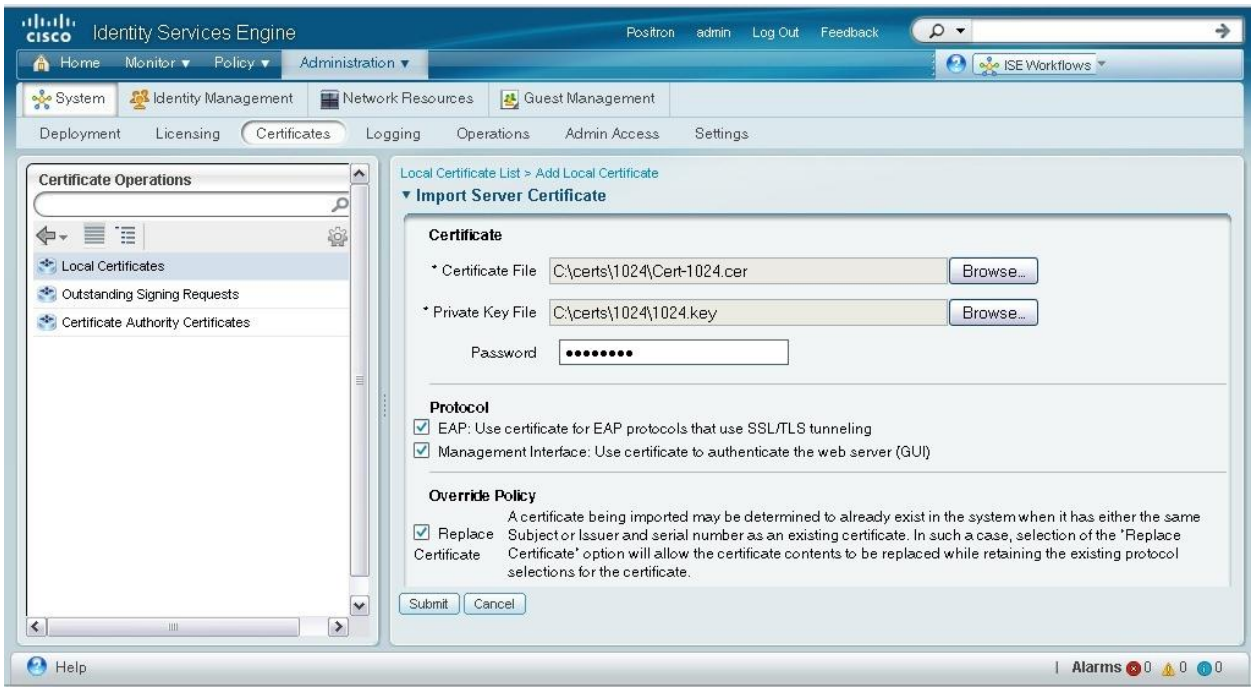
3. Save the file with extansion **.cer**

Step 2: Download the Symantec Intermediate CA Certificate

1. Download the **Intermediate CA certificate** from this link: AR657
   Select the appropriate Intermediate CA certificate for your SSL Certificate type.
   Copy the Intermediate CA certificate and paste it on a Notepad.
2. Save the files as **intermediate.cer**

Step 3: Install the SSL Certificate

1. Choose **Administration > System > Certificates**.
2. From the Certificate Operations navigation pane on the left, click **Local Certificates**.
   NOTE: To import a local certificate to a secondary node, choose **Administration > System > Server Certificate**.
3. Choose **Add > Import**.
4. The Import Local Server Certificate page appears as shown bellow



5. Click Browse to choose the certificate file and the private key from the system that is running your client browser.
6. If the private key is encrypted, enter the password to decrypt it.
7. In the Protocol area:

- Check the EAP check box to use this certificate for EAP protocols to identify the Cisco ISE node.
- Check the Management Interface check box to use this certificate to authenticate the web server (GUI).

  NOTE: If you check the Management Interface check box, ensure that the CN value in the Certificate Subject is the fully qualified

  domain name (FQDN) of the node. Otherwise, the import process will fail.

8. In the Override Policy area, check the Replace Certificate check box to replace an existing certificate with a duplicate certificate.

   NOTE: A certificate is considered a duplicate if it has the same subject or issuer and the same serial number as an existing certificate.

   This option updates the content of the certificate, but retains the existing protocol selections for the certificate.

9. Click Submit to import the local certificate.

   NOTE: If you import a local certificate to your primary Cisco ISE node, you must restart the secondary nodes connected to your primary

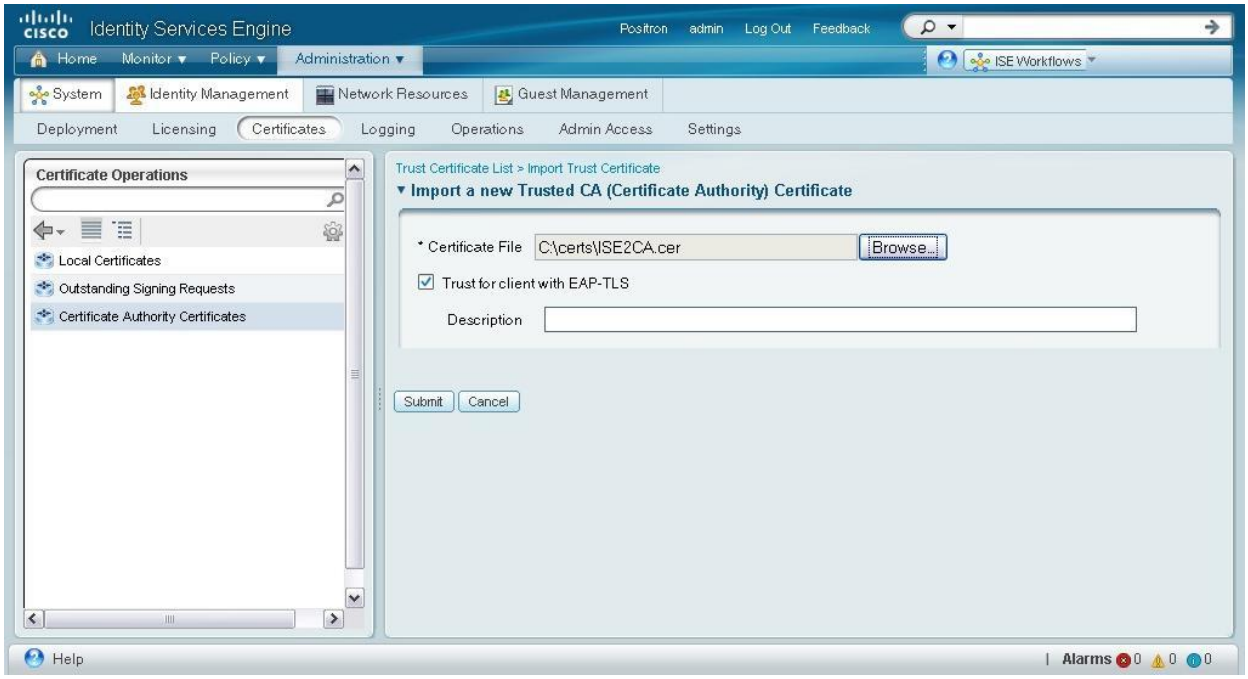
   Cisco ISE node. To restart the secondary nodes, from the command-line interface (CLI), enter the following commands:

   a. application stop ise

   b. application start ise

Step 4: Install the Intermediate CA Certificate

1. Choose Administration > **System > Certificates**.
2. From the Certificate Operations navigation pane on the left, click **Certificate Authority Certificates.**
3. The Certificate Authority Certificates page appears.
4. **Click Add**
5. The **Import** a new Trusted CA (Certificate Authority) Certificate page appears as shown bellow



6. Click **Browse** to choose the certificate authority certificate from the file system that is running the client browser.
7. Check the Trust for client with EAP-TLS check box if you want to use this certificate in the trust list for EAP-TLS protocols.

   NOTE: If you check the Trust for client with EAP-TLS check box, ensure that the keyUsage extension is present and the
   keyCertSign bit is set, and the basic constraints extension is present with the CA flag set to true.
8. **Add** an optional description.
9. Click Submit to save the certificate authority certificate.

   NOTE: If you add a certificate authority certificate to your primary Cisco ISE node, you must restart the secondary nodes connected to your primary Cisco ISE node.
   To restart the secondary nodes, from the command-line interface (CLI), enter the following commands:

   a. application stop ise

   b. application start ise

10. Verify the certificate installation uisng the Symantec Installation Checker

Installation Instructions for Cisco ACS 3.2

Step 1: Download the Symantec Intermediate CA Certificate

1. Download the **Intermediate CA certificate**.
   Select the appropriate Intermediate CA certificate for your SSL Certificate type.
2. Copy the Intermediate CA certificate and paste it on a Notepad.
3. Save the file as **intermediate.cer**

Step 2: Install CA Certificate

1. In the navigation bar, click **System Configuration**.
2. Click **ACS Certificate Setup**.
3. Click **ACS Certification Authority Setup**.
4. CiscoSecure ACS displays the CA Operations table on the Certification Authorities Setup page.
5. In the CA certificate file box, type the **full path** and **filename** for the certificate you want to use
6. Locate and import the **intermediate.cer**
7. Click **Submit**.

Step 3: Obtain the SSL Certificate

1. The Symantec certificate will be sent by email. The certificate is included as an attachment (Cert.cer) and it is also imbedded in the body of the email.
2. Copy and paste the certificate into a text file using Vi or Notepad.

   The text file should look like:

   -----BEGIN CERTIFICATE-----

   [encoded data]

   -----END CERTIFICATE-----

3. Save the file with extension **.cer**

Step 4: Install the SSL Certificate

1. In the navigation bar, click **System Configuration**.
2. Click **ACS Certificate Setup**.
3. Click **Install ACS Certificate**.
4. CiscoSecure ACS displays the Install ACS Certificate page.
5. Select the **Read certificate** from file option, and then type the **full directory path** and **filename** of the certificate file in the Certificate file box.
6. In the Private Key file box, type the **full directory path** and **name of the file** that contains the private key.
7. In the Private Key password box, type the **private key password**.
8. Click **Submit**.
9. To verify if your certificate is installed correctly, use the Symantec Installation Checker**.**

Cisco

For more information, see the Cisco Technical Support Center.

Installation Instructions for Cisco Secure ACS 4.2

Step 1: Obtain the SSL Certificates

1. The Symantec certificate will be sent by email. The certificate is included as an attachment (Cert.cer) and it is also imbedded in the body of the email.
2. Copy and paste the certificate into a text file using Vi or Notepad

   The text file should look like:

   -----BEGIN CERTIFICATE-----

   [encoded data]

   -----END CERTIFICATE-----

3. Save the file with extension **.cer**

Step 2: Download the Symantec Intermediate CA certificate

1. Download the **Intermediate CA certificate** from here.
   Select the appropriate Intermediate CA certificate for your SSL Certificate type.
   Copy the Intermediate CA certificate and paste it on a Notepad
2. Save the file as **intermediate.cer**

Step 3: Copy the Certificate and the CA Certificate to the ACS host:

1. Create a **\certs** directory on the ACS server.
2. Open a DOS command window.
3. To create a certificates directory, enter:
   mkdir <selected_drive>:\certs
   NOTE: Where selected_drive is the currently selected drive.
4. Copy the following files for example to the \certs directory:

ACS-1.nac.cisco.com.cer (server SSL certificate)

ACS-1.PrivateKey.txt (server certificate private key)

ca.nac.cisco.com.cer (CA certificate)

Step 4: Set Up the ACS Certification Authority

1. To set up the ACS certification authority download and install the Symantec Root CA.
2. In the navigation bar, click **System Configuration**.

   The System Configuration page opens.
3. Click **ACS Certificate Setup**.

   The ACS Certificate Setup page opens.
4. Click **ACS Certification Authority Setup**.

   The ACS Certificate Authority page opens as shown below.

5. Enter the path and filename for the certificate authority and then click **Submit**.
6. Restart ACS.

   To restart ACS, choose **System Configuration > Service Control** and then click **Restart**.

Step 5: Edit the Certificate Trust List

NOTE: After you set up the ACS certification authority, you must add the CA certificate to the ACS Certificate Trust list.

To add the certificate to the Certificate Trust list:

1. In the navigation bar, click **System Configuration**.

   The System Configuration page opens.
2. Choose **ACS Certificate Setup > Edit Certificate Trust List**.

   The Edit Certificate Trust List page opens.

3. In the list of certificates, locate the CA certificate that you installed and check the check box next to it.
4. Click **Submit**.
5. Restart ACS. To restart ACS, choose **System Configuration > Service Control** and then click **Restart**.

Step 6: Install the Symantec Intermediate CA Certificate

1. Choose **System Configuration > ACS Certificate Setup > ACS Certification Authority Setup**.

   The ACS Certification Authority Setup page appears, as shown below.

2. In the CA certificate file box, type the CA certificate location (path and name); for example: **c:\Certs\ca.cer**.
3. Click **Submit**.

Step 7: Install the SSL Certificate

1. In the navigation bar, click **System Configuration.**
2. The System Configuration page opens.
3. Click **ACS Certificate Setup**.
4. Click **Install ACS Certificate**.
5. The Install ACS Certificate page opens, as shown below

6. Click the **Read certificate from file** radio button.
7. In the Certificate file text box, enter the server certificate location (path and name); for example: **c:\Certs\server.cer**.
8. In the Private key file text box, type the server certificate private key location (path and name); for example: **c:\Certs\server.pvk**.
9. In the Private Key password text box, type the private key password; for example cisco123.
10. Click **Submit**.
11. ACS displays a message indicating that the certificate has been installed and instructs you to restart the ACS services.
12. Restart ACS. To restart ACS, choose **System Configuration > Service Control** and then click **Restart**.
13. Verify certificate installation using the Symantec Installation Checker.

Installation Instructions for Cisco ASA 5000 Series using the Command Line

Step 1: Download or pick up your SSL Certificate

1. The Symantec certificate will be sent by email. The certificate is included as an attachment (Cert.cer) and it is also imbedded in the body of the email.
2. Copy and paste the certificate into a text file using Vi or Notepad

   The text file should look like:

   -----BEGIN CERTIFICATE-----

   [encoded data]

   -----END CERTIFICATE-----

3. Save the file as **SSLCert.txt**

Step 2: Download the Symantec Intermediate CA Certificate

1. Download the Intermediate CA certificate for your certificate.
   Select the appropriate Intermediate CA certificate for your SSL Certificate type.
   Copy the Intermediate CA certificate and paste it on a Notepad.
2. Save the file as **intermediate.txt**

Step 3: Install Intermediate CA Certificate to your Trustpoint

1. To initiate the prompt to paste-in your Intermediate certificate files, perform the following command:

   ciscoasa(config)#**crypto ca authenticate <Trustpoint name>.Trustpoint**

2. You are then prompted with:"Enter the base 64 encoded CA certificate. End with the word "quit" on a line by itself".

3. Open the **intermediate.txt,** copy the entire content and paste this information in the command line
4. Make sure to include the "BEGIN CERTIFICATE" and "END CERTIFICATE" header and footer.

For Example

Enter the base 64 encoded certificate.
End with the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIE0DCCBDmgAwIBAgIQJQzo4DBhLp8rifcFTXz4/TANBgkqhkiG9w0BAQUFADBf
MQswCQYDVQQGEwJVUzEXMBUGA1UEChMOVmVyaVNpZ24sIEluYy4xNzA1BgNVBAsT
LkNsYXNzIDMgUHVibGljIFByaW1hcnkgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkw
HhcNMDYxMTA4MDAwMDAwWhcNMjExMTA3MjM1OTU5WjCByjELMAkGA1UEBhMCVVMx
FzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMR8wHQYDVQQLExZWZXJpU2lnbiBUcnVz
dCBOZXR3b3JrMTowOAYDVQQLEzEoYykgMjAwNiBWZXJpU2lnbiwgSW5jLiAtIEZv
ciBhdXRob3JpemVkIHVzZSBvbmx5MUUwQwYDVQQDEzxWZXJpU2lnbiBDbGFzcyAz
IFB1YmxpYyBQcmltYXJ5IENlcnRpZmljYXRpb24gQXV0aG9yaXR5IC0gRzUwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCvJAgIKXo1nmAMqudLO07cfLw8
RRy7K+D+KQL5VwijZIUVJ/XxrcgxiV0i6CqqpkKzj/i5Vbext0uz/o9+B1fs70Pb
ZmIVYc9gDaTY3vjgw2IIPVQT60nKWVSFJuUrjxuf6/WhkcIzSdhDY2pSS9KP6HBR
TdGJaXvHcPaz3BJ023tdS1bTlr8Vd6Gw9KIl8q8ckmcY5fQGBO+QueQA5N06tRn/
Arr0PO7gi+s3i+z016zy9vA9r911kTMZHRxAy3QkGSGT2RT+rCpSx4/VBEnkjWNH
iDxpg8v+R70rfk/Fla4OndTRQ8Bnc+MUCH7lP59zuDMKz10/NIeWiu5T6CUVAgMB
AAGjggGbMIIBlzAPBgNVHRMBAf8EBTADAQH/MDEGA1UdHwQqMCgwJqAkoC

KGIGh0
dHA6Ly9jcmwudmVyaXNpZ24uY29tL3BjYTMuY3JsMA4GA1UdDwEB/wQEAwIB
BjA9
BgNVHSAENjA0MDIGBFUdIAAwKjAoBggrBgEFBQcCARYcaHR0cHM6Ly93d3cu
dmVy
aXNpZ24uY29tL2NwczAdBgNVHQ4EFgQUf9Nlp8Ld7LvwMAnzQzn6Aq8zMTMwb
QYI
KwYBBQUHAQwEYTBfoV2gWzBZMFcwVRYJaW1hZ2UvZ2lmMCEwHzAHBgUr
DgMCGgQU
j+XTGoasjY5rw8+AatRIGCx7GS4wJRYjaHR0cDovL2xvZ28udmVyaXNpZ24uY29t
L3ZzbG9nby5naWYwNAYIKwYBBQUHAQEEKDAmMCQGCCsGAQUFBzABhhho
dHRwOi8v
b2NzcC52ZXJpc2lnbi5jb20wPgYDVR0lBDcwNQYIKwYBBQUHAwEGCCsGAQUF
BwMC
BggrBgEFBQcDAwYJYIZIAYb4QgQBBgpghkgBhvhFAQgBMA0GCSqGSIb3DQEB
BQUA
A4GBABMC3fjohgDyWvj4IAxZiGIHzs73Tvm7WaGY5eE43U68ZhjTresY8g3JbT5K
lCDDPLq9ZVTGr0SzEK0saz6r1we2uIFjxfleLuUqZ87NMwwq14lWAyMfs77oOghZ
tOxFNfeKW/9mz1Cvxm1XjRl4t7mi0VfqH5pLr7rJjhJ+xr3/
-----END CERTIFICATE-----
quit

Manually pasted certificate into CLI.
INFO: Certificate has the following attributes:
Fingerprint: 32 f3 08 82 62 2b 87 cf 88 56 c6 3d b8 73 df 08 53 b4 dd 27

5. Once you submit the intermediate c, you will be prompted if you would like to accept the certificate. You will want to submit "yes":

   Do you accept this certificate? [yes/no]: **yes**

   The output will display as follows:

   Trustpoint <name of Trustpoint> is a subordinate CA and

holds a non self-signed certificate.
Trustpoint CA certificate accepted.

% Certificate successfully imported
ciscoasa(config)#
ciscoasa(config-ca-trustpoint)# **exit**

6. Initiate the Trustpoint to install the secondary intermediate with the following command:

   ciscoasa(config)#**crypto ca authenticate <Trustpoint name>.Trustpoint**

7. You are then prompted with:"Enter the base 64 encoded CA certificate. End with the word "quit" on a line by itself".

Step 4: Install the SSL Certificate

1. To initiate the prompt to install your new certificate, you will need to run the following command:

   ciscoasa(config)#**crypto ca import <Trustpoint name>.Trustpoint certificate**

2. You are then prompted with: "Enter the base 64 encoded CA certificate. End with the word "quit" on a line by itself".
3. Open the file you have created in Step 1,**SSLCert.txt,** copy the entire contents and paste this information in the command line
4. Make sure to include the "BEGIN CERTIFICATE" and "END CERTIFICATE" header and footer.
   NOTE: Please do not copy/paste the actual certificate text below. This is just an example of what the SSL certificate text would look like.

   The fully-qualified domain name in the certificate will be: <common name of your certificate>
   Enter the base 64 encoded certificate.

End with the word "quit" on a line by itself

-----BEGIN CERTIFICATE-----
MIIFZjCCBE6gAwIBAgIQMs/oXuu9K14eMGSf0mYjfTANBgkqhkiG9w0BAQUFADCB
yzELMAkGA1UEBhMCVVMxFzAVBgNVBAoTDlZlcmlTaWduLCBJbmMuMTAwLgYDVQQL
EydGb3IgVGVzdCBQdXJwb3NlcyBPbmx5LiAgTm8gYXNzdXJhbmNlcy4xQjBABgNV
BAsTOVRlcm1zIG9mIHVzZSBhdCBodHRwczovL3d3dy52ZXJpc2lnbi5jb20vY3Bz
L3Rlc3RjYSAoYykwNTEtMCsGA1UEAxMkVmVyaVNpZ24gVHJpYWwgU2VjdXJlIFNl
cnZlciBUZXN0IENBMB4XDTA3MDcyNjAwMDAwMFoXDTA3MDgwOTIzNTk1OVowgbox
CzAJBgNVBAYTAlVTMRcwFQYDVQQIEw5Ob3J0aCBDYXJvbGluYTEQMA4GA1UEBxQH
UmFsZWlnaDEWMBQGA1UEChQNQ2lzY28gU3lzdGVtczEOMAwGA1UECxQFVFNXRUIx
OjA4BgNVBAsUMVRlcm1zIG9mIHVzZSBhdCB3d3cudmVyaXNpZ24uY29tL2Nwcy90
ZXN0Y2EgKGMpMDUxHDAaBgNVBAMUE2Npc2NvYXNhMS5jaXNjby5jb20wgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBAL56EvorHHlsIB/VRKaRlJeJKCrQ/9kER2JQ
9UOkUP3mVPZJtYN63ZxDwACeyNb+liIdKUegJWHI0Mz3GHqcgEkKW1EcrO+6aY1R
IaUE8/LiAZbA70+k/9Z/UR+v532B1nDRwbx1R9ZVhAJzA1hJTxSlEgryosBMMazg
5IcLhgSpAgMBAAGjggHXMIIB0zAJBgNVHRMEAjAAMAsGA1UdDwQEAwIFoDBDBgNV
HR8EPDA6MDigNqA0hjJodHRwOi8vU1ZSU2VjdXJlLWNybC52ZXJpc2lnbi5jb20v
U1ZSVHJpYWwyMDA1LmNybDBKBgNVHSAEQzBBMD8GCmCGSAGG+EUBBxUwMTAvBggr
BgEFBQcCARYjaHR0cHM6Ly93d3cudmVyaXNpZ24uY29tL2Nwcy90ZXN0Y2EwHQYD

UmFsZWlnaDEWMBQGA1UEChQNQ2lzY28gU3lzdGVtczEOMAwGA1UECxQFVFNXRUIx
Kn+rRsU2AgZwJ4daMHgGCCsGAQUFBwEBBGwwajAkBggrBgEFBQcwAYYYaHR0cDov
L29jc3AudmVyaXNpZ24uY29tMEIGCCsGAQUFBzAChjZodHRwOi8vU1ZSU2VjdXJl
LWFpYS52ZXJpc2lnbi5jb20vU1ZSVHJpYWwyMDA1LWFpYS5jZXIwbgYIKwYBBQUH
AQwEYjBgoV6gXDBaMFgwVhYJaW1hZ2UvZ2lmMCEwHzAHBgUrDgMCGgQUS2u5KJYG
DLvQUjibKaxLB4shBRgwJhYkaHR0cDovL2xvZ28udmVyaXNpZ24uY29tL3ZzbG9n
bzEuZ2lmMA0GCSqGSIb3DQEBBQUAA4IBAQAnym4GVThPIyL/9ylDBd8N7/yW3Ov3
bIirHfHJyfPJ1znZQXyXdObpZkuA6Jyu03V2CYNnDomn4xRXQTUDD8q86ZiKyMIj
XM2VCmcHSajmMMRyjpydxfk6CIdDMtMGotCavRHD9Tl2tvwgrBock/v/54o02lkB
SmLzVV7crlYJEuhgqu3Pz7qNRd8N0Un6c9sbwQ1BuM99QxzIzdAo89FSewy8MAIY
rtab5F+oiTc5xGy8w7NARAfNgFXihqnLgWTtA35/oWuy86bje1IWbeyqj8ePM9Td
0LdAw6kUU1PNimPttMDhcF7cuevntROksOgQPBPx5FJSqMiUZGrvju5O
-----END CERTIFICATE-----
quit

INFO: Certificate successfully imported
ciscoasa(config)#

Step 5: Define the Trustpoint that will supply the SSL certificate for the defined interface.

1. In order to use the updated Trustpoint, you will need to run the following commands:

ciscoasa(config)#**ssl trust-point <Trustpoint name>.Trustpoint outside**
ciscoasa(config)#**wr mem**

Building configuration...
Cryptochecksum: 694687a1 f75042af ccc6addf 34d2cb08

8808 bytes copied in 3.630 secs (2936 bytes/sec)

[OK]

ciscoasa(config)#

Step 6: Verify Certificate and Certificate Chain

1. To verify your certificate chain to see all the certificates you have just installed, input the following command:

   ciscoasa(config)#**show crypto ca certificates**

2. Verify certificate installation using the Symantec Installation Checker.

Installation Instructions for Cisco ASA 5510

Step 1: Download the Symantec Root and Intermediate CA Certificate

NOTE: For Cisco ASDM 6.3 and 6.1, you must install the Root and Intermediate CA Certificates first **before** generating your RSA key.

1. Click here to download the Symantec Root CA.
2. Click here to download Symantec **Intermediate CA certificate.**
   Select the appropriate Intermediate CA certificate for your SSL Certificate type.

Step 2: Install the Symantec Root CA Certificate

1. Within ASDM, click **Configuration** > **Device Management**
2. Click **Certificate Management** > **CA Certificates**
3. Click **Add**
4. Click **Paste certificate in PEM Format** > paste the root certificate into the text field
5. Click **Install Certificate**

A dialog box appears that confirms the installation was successful.

Step 3: Install the Symantec Intermediate CA Certificate

1. Within ASDM, click **Configuration** > **Device Management**
2. Click **Certificate Management** > **CA Certificates**
3. Click **Add**
4. Click **Paste certificate in PEM Format** > paste the Intermediate CA certificate into the text field
5. Click **Install Certificate**

A dialog box appears that confirms the installation was successful.

Step 4: Obtain the SSL Certificate

1. The Symantec certificate will be sent by email. The certificate is included as an attachment (Cert.cer) and it is also imbedded
   in the body of the email.
2. Copy and paste the certificate into a text file using Vi or a Notepad

   The text file should look like:

   -----BEGIN CERTIFICATE-----

   [encoded data]

   -----END CERTIFICATE-----

3. Save the file as **SSLcert.pem**

Step 5: Install the SSL Certificate

1. Click **Configuration** > **Device Management**
2. Click **Certificate Management** > **Identity Certificates**
3. Select the identity certificate you created (The Expiry Date should display Pending)
4. Click **Install**
5. Click **Paste the certificate data in base-64 format** > paste the certificate into the text field
6. Click **Install Certificate**

A dialog box appears that confirms the installation was successful.

Step 6: Activate the newly installed SSL certificate for use

1. Click **Configuration** > **Device Management**
2. Expand **Advanced**, and then expand **SSL Settings**
3. Under Certificates, select the interface that is used to termintate WebVPN sessions
4. Click **Edit**
5. In the Certificate drop-down list, choose the certificate that you just installed
6. Click **OK**

7. Click **Apply**
8. Your new certificate should now be activated for use with your ASA.
9. Verify your installation with the Symantec Installation Checker.

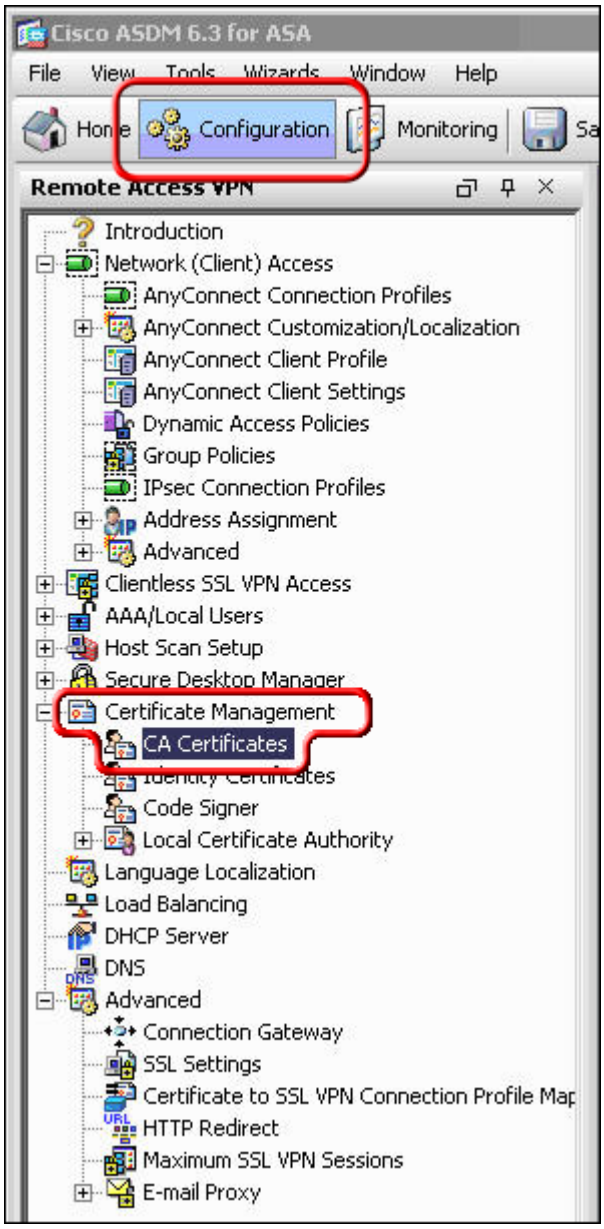
Installation Instruction for Cisco ASA 5520

Step 1: Obtain Symantec Intermediate CA Certificate

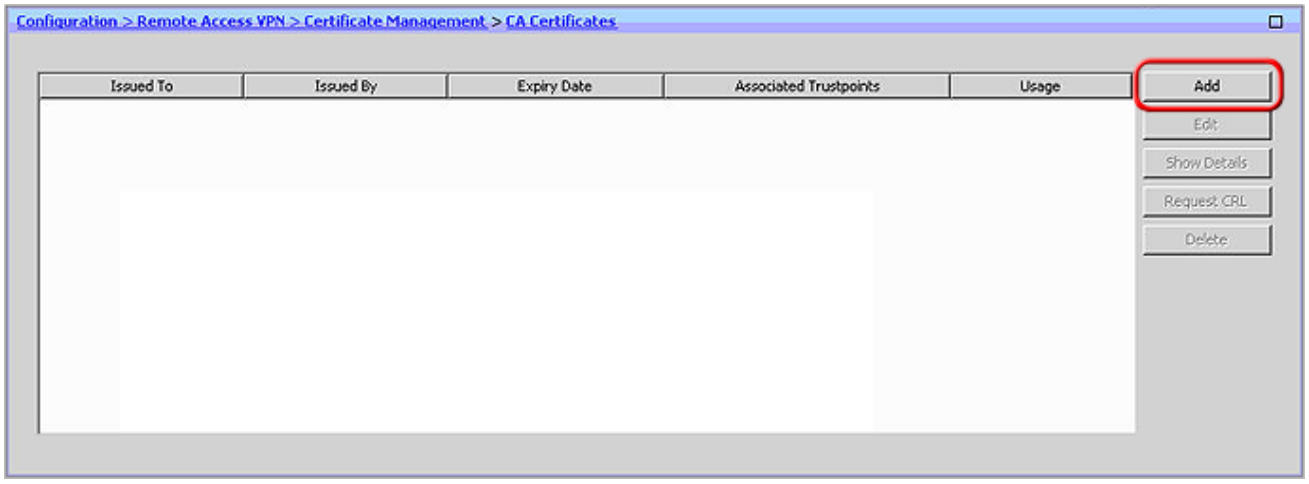
1. **Download Symantec Intermediate CA Certificate.**
   Select the appropriate Intermediate CA certificate for your SSL Certificate type.

2. Save the file as **intermediate.cr t**

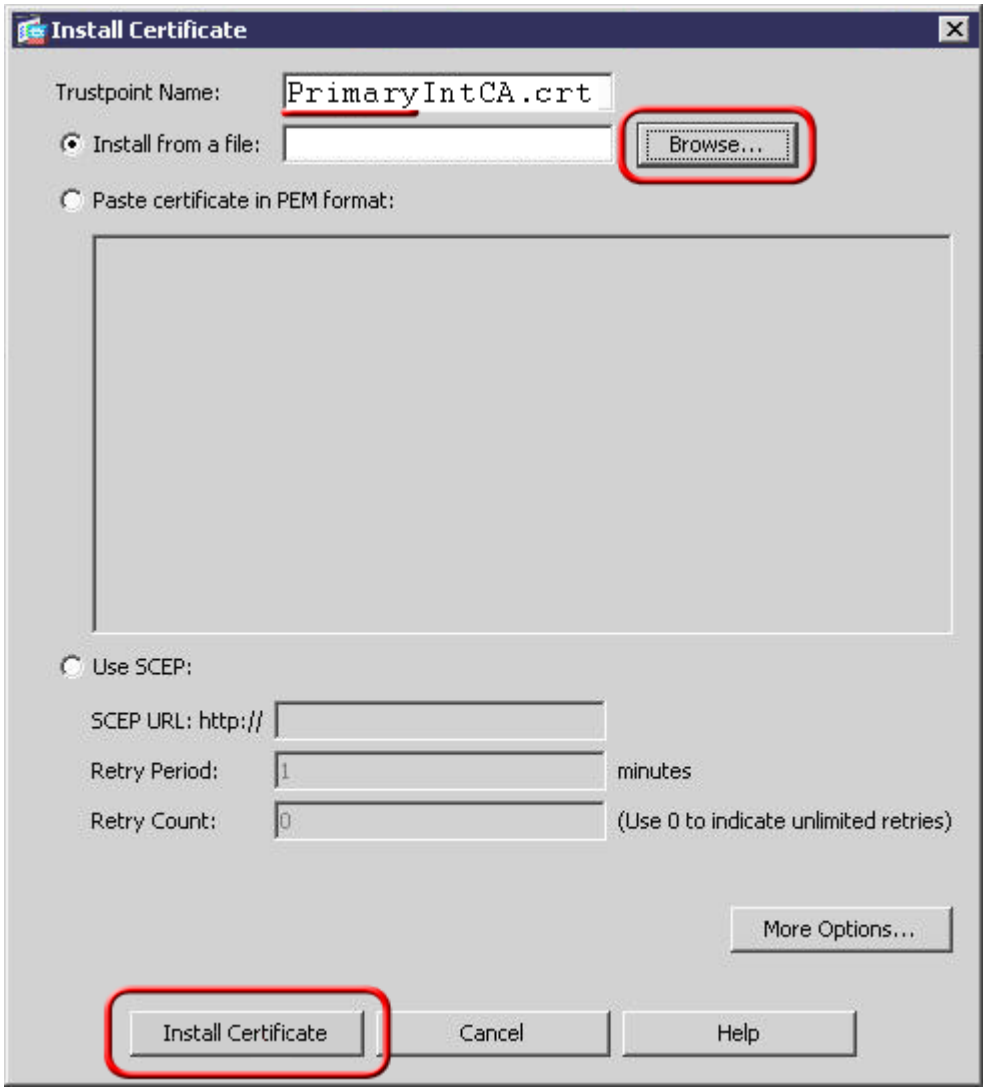
3. Open the Cisco ASDM, then Under the Remote Access VPN window pane, then in the **Configuration** tab, expand **Certificate Management** and click **CA Certificates**.


Cisco ASDM 6.3 for ASA
File
View
Tools
Wizards
Window
Help
Home
Configuration
Monitoring
Remote Access VPN
Introduction
Network (Client) Access
AnyConnect Connection Profiles
AnyConnect Customization/Localization
AnyConnect Client Profile
AnyConnect Client Settings
Dynamic Access Policies
Group Policies
IPsec Connection Profiles
Address Assignment
Advanced
Clientless SSL VPN Access
AAA/Local Users
Host Scan Setup
Secure Desktop Manager
Certificate Management
CA Certificates
Code Signer
Local Certificate Authority
Language Localization
Load Balancing
DHCP Server
DNS
Advanced
Connection Gateway
SSL Settings
Certificate to SSL VPN Connection Profile Map
HTTP Redirect
Maximum SSL VPN Sessions
E-mail Proxy

4. Click the **Add** button.



5. Assign a **Trustpoint Name** to the certificate (e.g. **intermediate.crt**), And select the **Install from a file:** radio button and browse to**intermediate.crt**. Click **Install Certificate**.



You should then see the Certificate listed with the Trustpoint Name you assigned to it.

Step 2: Install your SSL certificate

1. The Symantec certificate will be sent by email.
2. Copy the certificate imbedded in the body of the email and paste it into a text file using Vi or Notepad.

   Do not use Microsoft Word or other word processing programs that may add characters.

   The text file should look like:

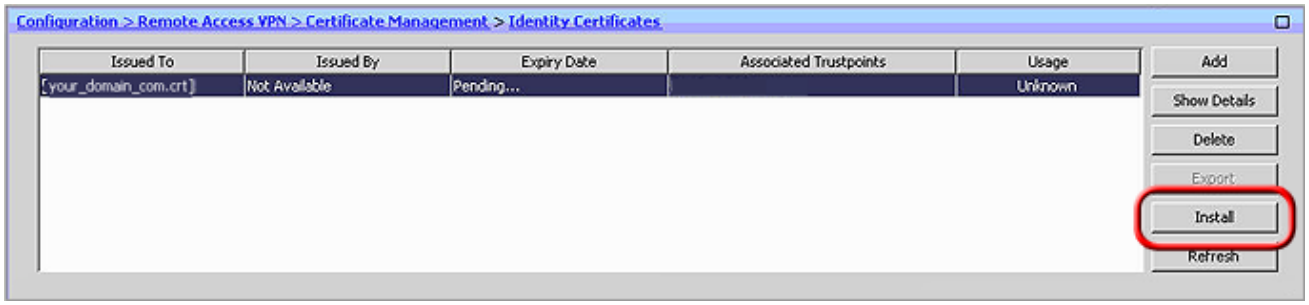
   -----BEGIN CERTIFICATE-----

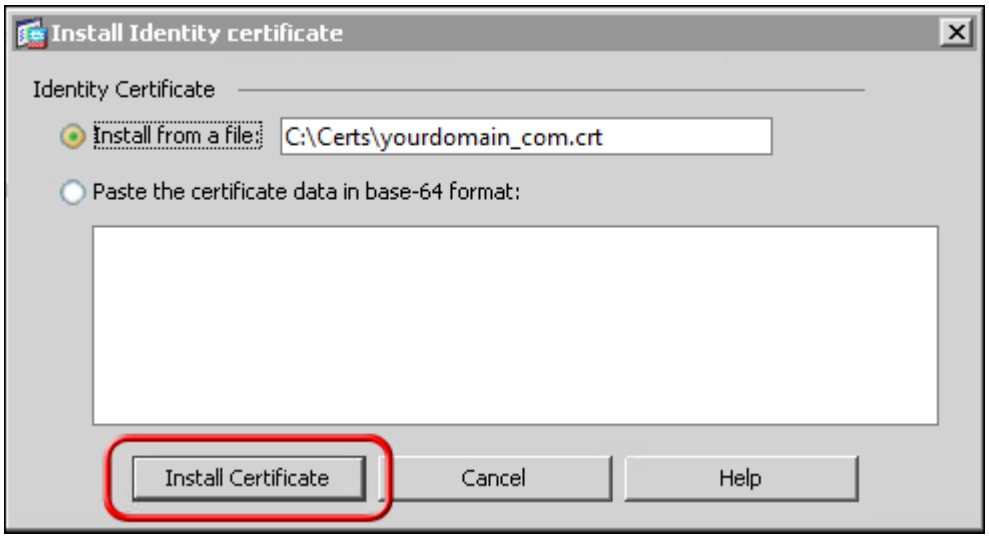
[encoded data]

-----END CERTIFICATE-----

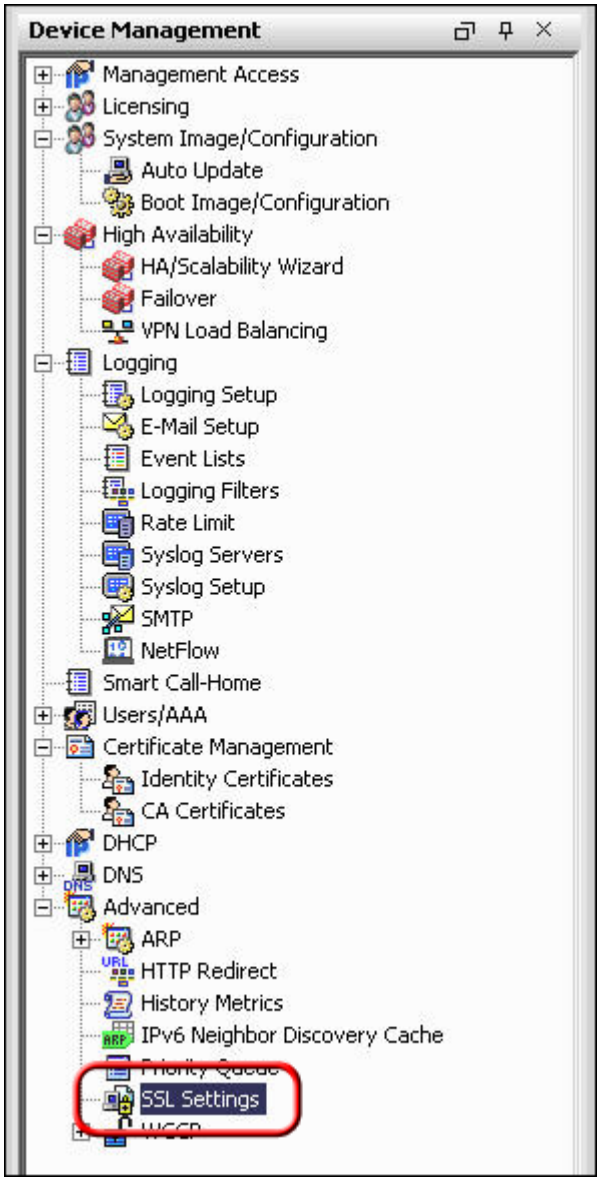
3. To follow the naming convention for Cisco, rename the certificate filename with the **.crt** extension.
   For example: **public.crt**
4. Under **Remote Access VPN**, expand **Certificate Management** > **Identity Certificates**.

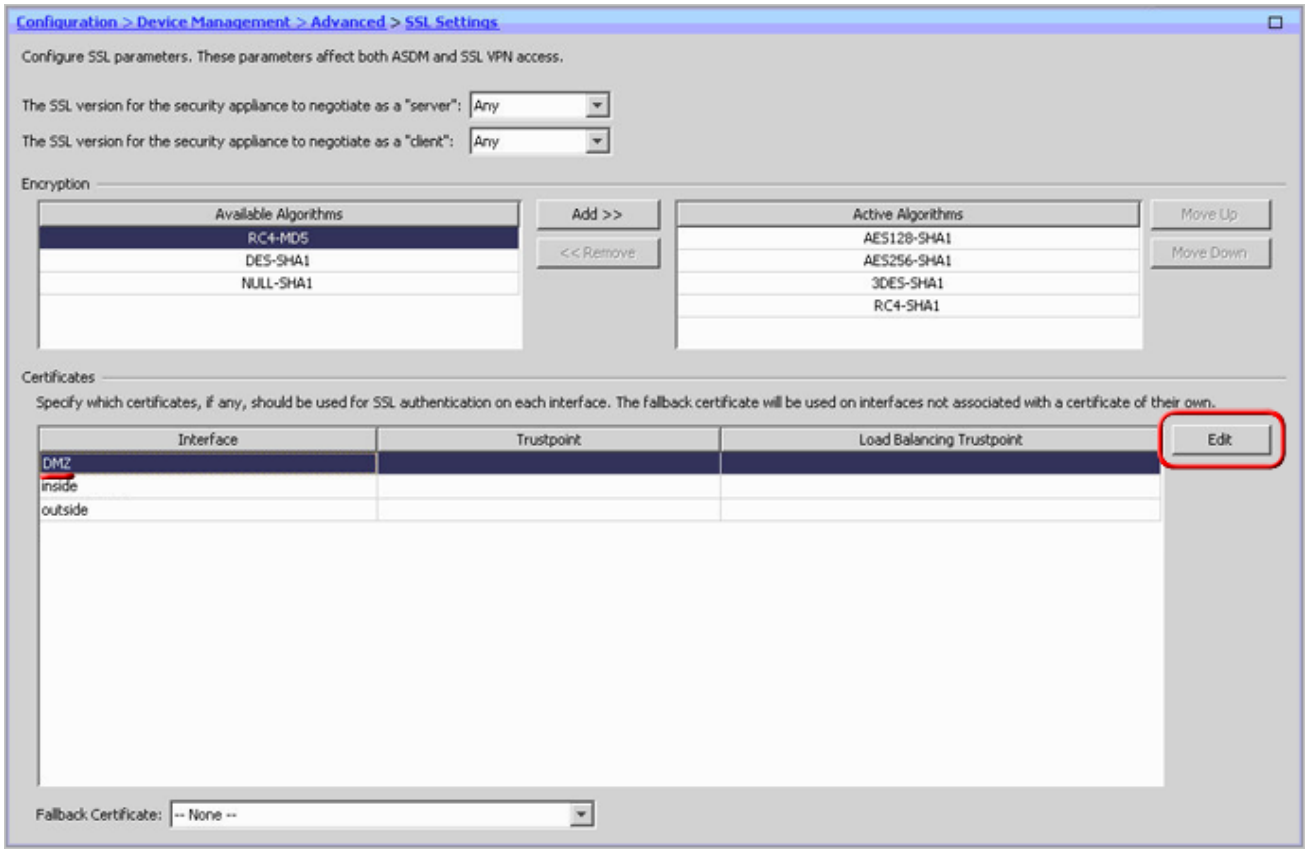
   Select the identity you created for the CSR with the **Expiry Date** shown as pending and click **Install**, select **yourdomain_com.crt** and click **Install Certificate**. Once installed the Expiry Date will no longer show 'Pending.'



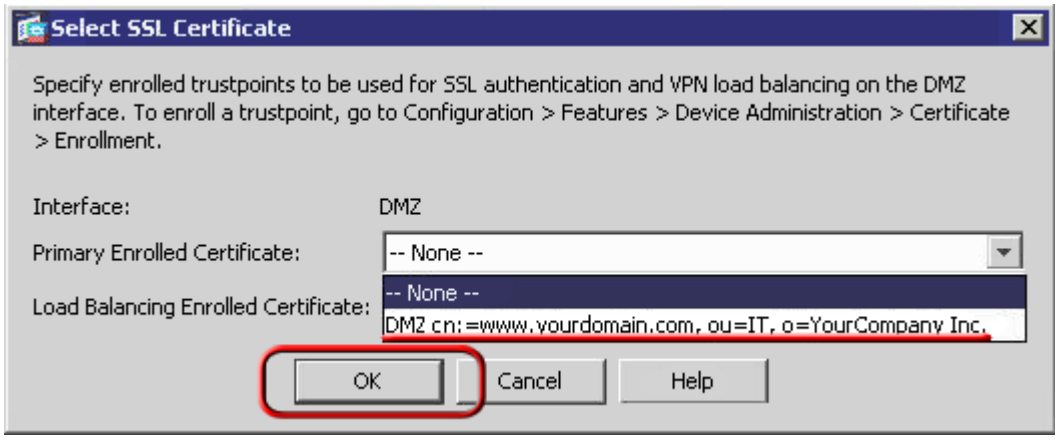


5. The certificate now needs to be enabled. On the lower left, click **Advanced** > **SSL Settings**. Then, select the interface you want SSL enabled for and click **Edit**.


Device Management
Management Access
Licensing
System Image/Configuration
Auto Update
Boot Image/Configuration
High Availability
HA/Scalability Wizard
Failover
VPN Load Balancing
Logging
Logging Setup
E-Mail Setup
Event Lists
Logging Filters
Rate Limit
Syslog Servers
Syslog Setup
SMTP
NetFlow
Smart Call-Home
Users/AAA
Certificate Management
Identity Certificates
CA Certificates
DHCP
DNS
Advanced
ARP
HTTP Redirect
History Metrics
IPv6 Neighbor Discovery Cache
SSL Settings



6. On the next screen, click the drop-down menu and for **Primary Enrolled Certificate** select your certificate then click **OK**.



7. The ADSM will then show your certificate details under trustpoint.

8. To verify if your certificate is installed correctly, use the [Symantec Installation Checker.]

Cisco ASA 5520

For more information, see the **Cisco Support** website.