

Installing true self-signed certificates for CAM/CAS communication

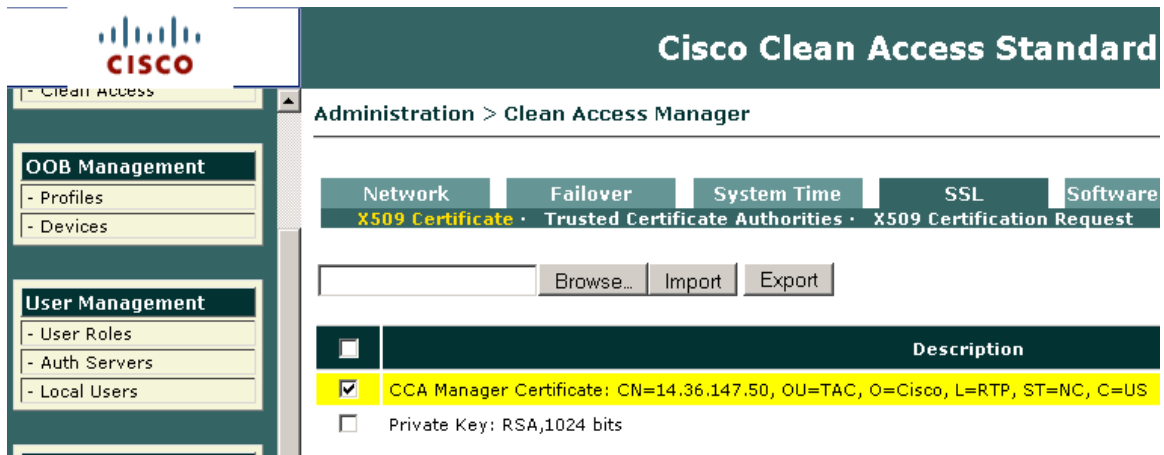
With CCA version 4.7 and above, the CAM and CAS act as the root CA which signs the identity certificate for themselves. Since the CAS and CAM rely on mutual verification of the certificates, what this means is that you have to take the CAS cert and import it in the CAM, and take the CAM cert and import it in the CAS.

If this is the first time you are adding your CAS to the CAM, you will need to do this certificate swap first before the CAS can be added to the CAM.

For this document, here's what we assume:

- CAM IP address: 14.36.147.50
- CAS IP address: 14.36.147.45

Open the CAM SSL page (CCA Manager -> SSL) , checkmark the certificate and click on export:



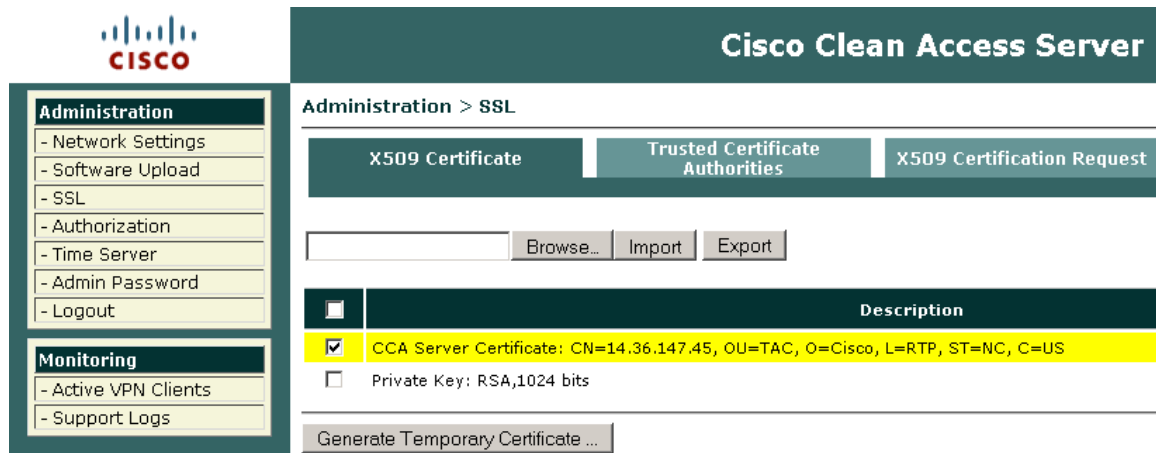
The screenshot shows the Cisco Clean Access Standard Administration interface. The left sidebar contains navigation menus for OOB Management (Profiles, Devices) and User Management (User Roles, Auth Servers, Local Users). The main content area is titled 'Administration > Clean Access Manager' and has tabs for Network, Failover, System Time, SSL, and Software. The SSL tab is active, showing a list of certificates. One certificate is selected with a checkmark:

<input type="checkbox"/>	Description
<input checked="" type="checkbox"/>	CCA Manager Certificate: CN=14.36.147.50, OU=TAC, O=Cisco, L=RTP, ST=NC, C=US
<input type="checkbox"/>	Private Key: RSA,1024 bits

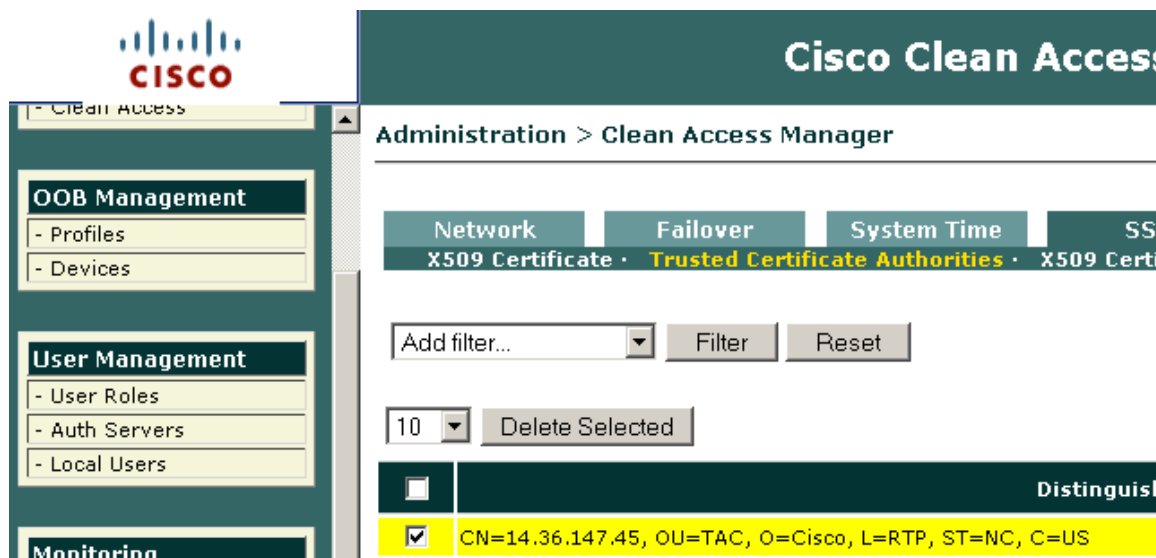
Buttons for 'Browse...', 'Import', and 'Export' are visible above the table.

Save this file as CAM_Cert.pem

Similarly, open the CAS page, and export the certificate from there. Save as CAS_Cert.pem:



Now open the CAM's Trusted Certificate Authorities tab (CCA Manager -> SSL -> Trusted Certificate Authorities) and click on browse. Select the CAS_Cert.pem and click on import. It should show up in the trusted store as follows:



Open the CAS's Trusted Certificate Authorities tab (SSL -> Trusted Certificate Authorities), click on browse, and import the CAM_Cert.pem. It should show up in the trusted store as follows:

The screenshot shows the Cisco ClearPass Administration console. The left sidebar contains a navigation menu with sections for Administration and Monitoring. The main content area is titled "Administration > SSL" and has two tabs: "X509 Certificate" and "Trusted Certificate Authorities". The "Trusted Certificate Authorities" tab is active. Below the tabs, there are filter controls: "Add filter..." with a dropdown arrow, "Filter", and "Reset" buttons. Below that, there is a "10" dropdown and a "Delete Selected" button. A table of certificate authorities is displayed below, with one entry selected (checkbox checked) and highlighted in yellow. The entry details are: CN=14.36.147.50, OU=TAC, O=Cisco, L=RTP, ST=NC, C=US.

<input type="checkbox"/>	Distinct
<input checked="" type="checkbox"/>	CN=14.36.147.50, OU=TAC, O=Cisco, L=RTP, ST=NC, C=US

Now the CAS/CAM communication will be effective since the CAS and CAM trust each other's certificates.

At this point (other things being configured properly) you should also be able to add the CAS to the CAM.