Title:                        Creating and Importing CA-Signed Certificates into ArcSight ESM Components

Document ID:          KM1262078

Product - Versions: arcsight enterprise security manager

**How can I create or replace a CA-Signed Certificate for my Manager and other ArcSight components?**

**Solution:**

Configuring CA-signed SSL certificates for Manager server and its other components is a complex procedure.

The 6 Phases listed below will lead you through the configuration of your system with CA-Signed SSL certificates.

**Note:** These steps assume that your Manager has been configured with default mode.

**1. Obtain a key pair for CA-signed SSL certificate**

**2. Send the CSR to Certificate Authority**

**3. Import CA root certificate in the Truststore**

**4. Import CA-Signed SSL certificate in the keystore**

**5. Restart Manager**

**6. Extra steps if adding more ArcSight components (Web, Console, SmartConnectors)**

**Before starting the CA-signed SSL certifcate procedure, you must backup your current keystore, as follows:**

1. Login as the arcsight user and navigate to **<ARCSIGHT\_HOME>/config/jetty** directory

2. Make a backup copy of keystore file. This allows you to rollback to the previous SSL mode while you are waiting for the CA reply for CA-Signed SSL certificate or in a case when the CA-Signed SSL certificate operation fails.

3. Remove the keystore file from the current directory completely. If you need to roll back to the original SSL option, you must move the backup keystore file back into this directory and restart the Manager.

**Phase 1: Obtain a key pair for CA-signed SSL server certificate for Manager**

1. Create a key pair on the Manager server using the following steps:

a. Launch the keytoolgui utility from **<**[**ARCSIGHT\_HOME**](https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM1271661)**>/bin** with this command:

*arcsight keytoolgui*

b. Click File menu, select **New keystore** to create a new keystore.

**Note:** Select keystore type **JKS (**It supports java keystore type)

c. Click Tools menu, select **Generate Key Pair**

d. Enter the required information, for the certificate including validity (in days), common name, etc.

**Note:** Enter the fully qualified domain name of the Manager server in Common Name (CN) section

e. Specify an alias name as <mykey>

**Note:** ArcSight only uses or recognizes the alias name *mykey*.

f. Enter Key pair password.

g. Choose **Save Keystore**.

2. Click File menu, select **Save Keystore as**, and save as **keystore**

3. Enter password for the Keystore.

**Note:** The password for the Keystore MUST be the same as the password for the new key pair <mykey>.

4. Enter the name of the Keystore as 'Keystore.request'

**Note:** Keep the **keystore.request** file in a secure place and remember the password of the key pair/Keystore. You need to reuse this file after receiving the reply from CA.

**Phase 2: Send a Certificate Signing request (CSR) to CA**

1. Create a certificate signing request (CSR

a. In the keytoolgui utility, right-click the new key pair you just created (mykey)

b. Select **Generate CSR** to create a certificate signing request (CSR)

c. Choose a path and file name (such as **certreq.csr**)

d. Click **Generate** button

2. Send the CSR to your chosen Certificate Authority

**Phase 3: Import the CA root certificate into the Truststore file**

1. Obtain a root certificate from the CA. When you receive the email CSR reply from the CA, you should also receive the instructions on getting the Root CA certificate

2. Save the Root CA certificate as a file **rootca.cer**

3. Repeat the below procedure on Manager server machines:

a. Launch the keytoolgui utility on Manager server machine

b. Click **File** menu, select **Open Keystore**, select the Truststore file located at **<ARCSIGHT\_HOME>/jre/lib/security/cacerts**. Use the default password **changeit** to open cacerts.

**NOTE:** If the password of the cacerts file is not 'changeit' you get the following error:

*Could not open CA Certs '<manager-home>/jre/lib/security/cacerts' as a KeyStore. Attempts were made for KeyStore types JKS, JCEKS, PKCS12, BKS and UBER.*

If the password of the cacerts file is lost, a new cacerts file must be recreated.

c. Click Tools menu, select **Import Trusted Certificate**, and pick the **rootca.cer** file.

d. You will see the following warning message: *Could not establish a trust path for the certificate. The certificate information will now be displayed after which you may confirm whether or not you trust the certificate*

e. Click **OK** to finish.

**Notes:**

1. If the CA root certificate has a chain, you must also follow the same procedure to import all intermediate CA certificates into the Truststore.

2. Skip Phase 3 if you renew the CA-signed certificate that is issued by the same root CA.

4. Update CA root certificate on other ArcSight components

a. Do the same step 3 (a)-(d) on one of Consoles

b. Copy that updated cacerts to other PCs, which are installed Logger Appliance, Connector Appliance, Consoles, SmartConnectors, FlexConnectors, etc

Note: All services must be restarted after the new cacerts is copied.

**Phase 4: Import a CA-signed certificate into Manager's Keystore**

The CA-signed SSL certificate that you receive from CA will look similar to this text string:  
  
*-----BEGIN CERTIFICATE-----MIICjTCCAfagAwIBAgIDWnWvMA0GCSqGSIb3DQEBBAUAMIGHMQswCQYDVQQGEwJaQT EiMCAGA1UECBMZRk9SIFRFU1RJTkcgUFVSUE9TRVMgT05     MWTEdMBsGA1UEChMUVGhh d3RlIENlcnRpZmljYXRpb24xFzAVBgNVBAsTDlRFU1QgVEVTVCBURVNUMRwwGgYDVQ QDExNUaGF3dGUgVGVzdCBDQSBSb290MB4XDTAyMDkyNzIzMzI0MVoXDTAyMTAxODIZ MzI0MVowaDELMAkGA1UEBhMCrVMxDTALBgNVBAgTBGJsYWgxDTALBgNVBAcTBGJsYW gxDTALBgNVBAoTBGJsYWgxDTALBgNVBAsTBGJsYWgxHTAbBgNVBAMTFHppZXIuc3Yu YXJjc2lnaHQuY29tMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCZRGnVfQwG1b BgABd/p8UhsaNov5AjaagAoBmouJCwgW2vwN4JViC CSBkDpiqVF7K11Sx4ZVSXX4 VQ6k4gT5G0kDNvQeN05wWkzEMygMB ZBnYqPA/XtWR ZtjxvH MoqS JEqHruiMLITC6q0reUB/txby6 S9zNo/fUG1pkIcQIDAQABoyUwIzATBgNVHS UEDDAKBggrBgEFBQcDATAMBgNVHRMBAg8EAjAAMA0GCSqGSIb3DQEBBAUAA4GBAFY3 7E60 P4b3zTLnaG7EVM57GtkED6PwCIilB6ixjvNL4MNGRubPa8kyaZp5fEDoNUPQV QxnpABjzTalRfYgjNFJ6ltI6ZKjBO5kim9UBeCnKiNNzhIyDyFwbHXOPB/JaLIV jG ugYNS7hf/ay0BXKlfueO07EgjhhB/mQFs2JB  
-----END CERTIFICATE-----*

1. Copy and paste the text string to a text editor (include the line "-----BEGIN CERTIFICATE-----" and line "-----END CERTIFICATE-----".

**Note**: Ensure that there are no extra spaces before and after the test string.

2. Save it to a file named **ca\_reply.txt** in the Manager in the **<ARCSIGHT\_HOME>/config/jetty** directory

3. Launch the keytoolgui utility again.

4. Click File menu, select **Open Keystore**, and then select the **Keystore.request** file that you have saved in Phase 1.

**Note**: You will also need to provide the same password as you save this keystore.

5. Right-click the key pair named as <mykey>

6. Select **Import CA Reply** from the menu.

7. Select the CA reply certificate file (ca\_reply.txt) and click **Import**

**Notes**:

1. If this operation fails, the Certificate Details dialog appears for manual verification. Acknowledge the certificate by clicking **OK** and answering **Yes** to the subsequent challenge. Answer **No** if the certificate is not trustworthy for some reason.

2. If the password of the cacerts is not 'changeit' you get the following error:

*Could not open CA Certs '<manager-home>/jre/lib/security/cacerts' as a KeyStore. Attempts were made for KeyStore types JKS, JCEKS, PKCS12, BKS and UBER.*

If the password of the cacerts file is lost, a new cacerts file must be recreated.

8. Choose **Save** from the File menu. The key store is now ready for use by the ArcSight Manager or ArcSight Web.

9. Make a backup the existing Keystore

10. Rename **<ARCSIGHT\_HOME>/config/jetty/keystore** to **<ARCSIGHT\_HOME>/config/jetty/keystore.old**

11. Rename 'keystore.request' to 'keystore'.

**Phase 5: Restart Manager**

Restart the Manager service to load the new certificate.

**Phase 6: Extra Steps if Adding Additional ArcSight Components**

1. Adding additional Managers

You do not need to add the CA root certificate to the Truststore-cacerts file again. However, you must copy the cacerts file from the existing Manager to the new Manager.

2. Other ArcSight Components (Console, Web, and SmartConnectors).

When installing a new Console, you must copy the 'cacerts' file from the existing Console, which has been updated in the Phase 3, to the newly installed Console. This configuration procedure of Manager Ca-signed SSL certificate can be applied on Web server unless both components are installed on the same machine.

3. For ArcSight Web, use the *webserversetup* utility after the certificate is updated to confirm the certificate is valid, as follows:

a. Login as an arcsight user on Web server machine.

b. Execute the following command from **<ARCSIGHT\_HOME>/bin**:

*./arcsight webserversetup*

c. Restart the Web server.

**Recommendations:**

1.  Your Manager may fail to start if the password of Key pair does not match the password of the keystore (which is encrypted in server.properties). If you do not remember the keystore password, run the Manager setup wizard and change the password of your existing keystore first.

Refer to [KM1271309](https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM1271309) or [KM1270207](https://softwaresupport.hp.com/group/softwaresupport/search-result/-/facetsearch/document/KM1270207) for more details on this process.

2. Verify the status of your certificates by following these steps:

a. Open a Command line, navigate to <ARCSIGHT\_HOME> and enter the command: *arcsight tempca -i*

The output shows which CA issuer signs the SSL CA-signed certificate, certificate type, a status of a validation of the certificate, etc.

b. Open a browser to **https://<manager\_hostname>:8443** to test it.

See details on this procedure in ESM 4.0.3 Admin Guide, page 37 - 41.

3. Remove Demo certificate, as follows:

**Note:** After installing a CA-signed SSL certificate on the ArcSight Manager, all Consoles and SmartConnectors which were communicating with the Manager using the previous certificate will cease communication until their keystores are populated with the new certificate.

a. The demo certificate can be removed by using the tempca script located in **<ARCSIGHT\_HOME>/bin** on the Manager host, and issuing the following command on all Console installations:

*arcsight tempca -rc*

b. For SmartConnectors, you can run the tempca script using the following command:

*arcsight agent tempca -rc*

Internal Response

Nellie10212012: added the below information:

**Before starting the CA-signed SSL ceritifcate procedure, you need to backup your current keystore**

1. Login as arcsight user to <ARCSIGHT\_HOME>/config/jetty directory

2. Make a copy of keystore as back up file

   It allows you to rollback to the previous SSL mode while you are waiting for the CA reply for CA-Signed SSL certificate or in a case when the CA-Signed SSL certificate operation fails.

3. Remove the keystore file from the current directory completely

   In a case to roll back to the original SSL option, you need to move the backup keystore file back (require to restart Manager)