

Configuring a Secure Access Manual CA Certificate (NSM Procedure)

To manually upload CA certificates to the Secure Access device:

1. In the NSM navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to manually upload CA certificates.
2. Click the **Configuration** tab, and then select **System > Configuration > Certificates > Trusted Client CAs** tab.
3. Click **Trusted Client CA** . The New Trusted Client CA page appears.
4. Configure the server using the settings described in Table 1 .
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 1: Secure Access Manual CA Certificate Configuration Details

Option	Function	Your Action
Settings tab		
Subject	Specifies the CA certificate subject name.	Enter a subject name for the certificate.
Client certificate status checking	Specifies the method the device uses to verify client certificate status.	Select one of the following options: <ul style="list-style-type: none"> ■ None — Specifies that the device should not validate this trusted client certificate. ■ Use OCSP (Online Certificate Status Protocol) — Specifies that the device should use the OCSP method, validating the client certificate in real-time, as needed. After you select this option, you can specify options for OCSP. ■ Use CRLs (Certificate Revocation Lists)— Specifies that the device should use CRLs to validate the client certificate. After you select this option, you can specify options for CRL. ■ Use OCSP with CRL fallback—Specifies that the device should use the OCSP validation method when possible, but attempt to validate client certificates using CRLs should the OCSP method fail (for example, if the link to the OCSP Responder fails). After you select this option, you can specify options for both CRL and OCSP.

Table 1: Secure Access Manual CA Certificate Configuration Details (continued)

Option	Function	Your Action
Verify Trusted Client CA	Specifies if you want the device to validate the CRL from which the certificate is issued.	Select the check box.
Trusted for Client Authentication?	Specifies if you want this certificate when authenticating client certificates.	Select the check box. NOTE: If you added this certificate for nonauthentication purposes (such as for SAML signature verification or machine certificate validation), disable this option. This indicates that the device must not trust any client certificate issued by this CA.
Participate in Client Certificate Negotiation	Specifies if you want to have the CA participate in client certificate selection for authentication.	Select the check box. NOTE: In client certificate authentication or restriction, the device sends a list of all trusted client CAs configured in the trusted client CA store with this flag enabled to the user's browser for user certificate selection. The browser prompts the client certificates whose issuer CA and/or root CA is in that list. This option allows you to control which client certificate(s) are prompted for selection. Clearing this option for all certificates in a CA chain results in those certificates not being prompted.
Import from	Specifies the trusted client file that you can import from the database.	Use Browse to select and import the trusted client files from.
OCSP > Settings tab		
OCSP settings	Specifies the OCSP method that the device uses to verify client certificate status.	Select a value from the drop-down list. The list includes: <ul style="list-style-type: none"> ■ Responder specified in CA certificate ■ Manually configured responders ■ Responder specified in Client certificate
Device Certificate to sign the request	Specifies the device certificate that is used to sign for the request.	Select a value from the drop-down list.
Use Nonce	Specifies the device to use nonce.	Select the check box to enable this option.
CRL Settings tab		
CDP(s) specified in the Trusted Client CA	Specifies the CDP(s) in the trusted client CA.	Select the check box to enable this option.

Table 1: Secure Access Manual CA Certificate Configuration Details *(continued)*

Option	Function	Your Action
CDP(s) specified in the client certificate	Specifies the CDP(s) in the client certificate.	Select the check box to enable this option.
Manual configured CDP	Specifies the manual configured CDPs.	Select the check box to enable this option.
CRL Download Frequency (minutes)	Specifies the frequency of the CRL download.	Select the frequency of the CRL download. The default value is 1440.

- Related Topics**
- Configuring a Secure Access Certificate Server Instance (NSM Procedure)
 - Configuring a Secure Access SAML Server Instance (NSM Procedure)

Published: 2009-08-20