The Most Trusted Name In Energy™
7901 Computer Avenue | Bloomington, MN 55435
www.oati.com

Open Access Technology International, Inc.
webCARES 2025 Client and Server Issuing Certificates
Frequently Asked Questions (FAQ)

This document contains a list of common questions and answers customers may have regarding testing and installing the new webCARES Issuer certificates. If you are unable to find your question in this list or if you have additional questions or run into issues, please contact the OATI Help Desk via chat through the OATI Hub, e-mail at support@oati.net, or phone at 763-201-2020.

Table of Contents

1. What does this mean to me?

What this means to you could be several different things, depending on your situation. For most customers, this will be completely transparent. For others, this will require minor changes on their side to support this effort. Please review this FAQ and search for the "What If" case that best meets your specific usage case for more information about the impacts of this change for you.

2. What if I just use an OATI client certificate to log in to an OATI application?

If this is the case, you will likely not need to do anything to support this change. Except in a few cases, where some IT departments strongly control which Intermediate certificates are supported, the new certificates will just work for you. This is especially true of customers using Windows products, which will work with OATI systems by default unless some action has been taken by your IT department. If you are unsure about your IT department's restrictions on Intermediate Certificates, please feel free to forward them this information and check with them.

3. What if I run a site that accepts OATI client certificates?

If you run a site that accepts OATI client certificates for login credentials into your site, you will likely need to configure your Web Server software to trust the new webCARES Client Issuing CA certificate. Please consult with your IT department or Web Hosting provider for more information on how to do this.

4. What if I run a site that uses OATI server certificates?

If you run a site that uses OATI server certificates for hosting your site, you may need to configure your Web Server software to trust the new webCARES Server Issuing CA certificate. Please consult with your IT department or Web Hosting provider for more information on how to do this.

5. What if we do not use your certificates? Do we still need to install the new webCARES Client Issuing CA certificate?

Yes. If you have a web site, web service, or application which accepts OATI webCARES certificates as part of the login, authentication, or authorization process, then you must install

the new webCARES Client Issuing CA certificate. If this issuing certificate is NOT installed, an incomplete Certificate Trust List (CTL) will be sent to your users browser (or application) and they will be unable to choose the correct certificate when prompted (i.e., the browser's "Client Authentication" list of certificates will not show any certificates issued from the new CA certificates or an application will give a "certificate untrusted or corrupt" message).

6. How do I request a test certificate?

If you wish to test certificates issued from the new webCARES issuers, you can contact the OATI Help Desk for a single test certificate (client or server) to use for your testing. Please note that this certificate will count against your certificate count in the OATI webCARES system, as it is a real, valid certificate. Please also note that many OATI systems may not yet support these new certificates, so if you are looking to test against an OATI system, please consult with your OATI Project Manager or the OATI Help Desk for system support.

7. Why are there two new issuers, instead of just one?

This is due to the Certificate Authority/Browser (CA/B) Forum requirement, which states that an issuing certificate can only be used for one purpose, such as issuing server (website) certificates, client (end-user) certificates, etc.

8. How do I install the new webCARES Client & Server Issuing CA 2025 certificates into my Java Keystore?

- As an Administrator, copy the default Java CA Certificates keystore (cacerts) from the security to bin directory
    - (Windows Only) Right click on the Command Prompt and chose "Run As Administrator"
    - Copy "C:\Program Files\Java\jreXXX\lib\security\cacerts" "C:\Program Files\Java\jreXXX\bin" (Note: replace jreXXX with your actual directory name (i.e., jre1.8.0_131)
- Download the new Client/Server Issuing CA 2025 certificate
    - Download the https://www.oaticerts.com/repository/OATIIAClient2025.crt certificate and save it as C:\Program Files\Java\jreXXX\bin\OATIIAClient2025.cer
    - Download the https://www.oaticerts.com/repository/OATIIAServer2025.crt certificate and save it as C:\Program Files\Java\jreXXX\bin\OATIIAServer2025.cer

- Import the new Client Issuing CA 2025 certificate
    - Note: Your Java Keystore name and password may be different then what is used in this example.
    - C:\Program Files\Java\jreXXX\bin>keytool -import -trustcacerts -alias OATIIAClient2025 -file OATIIAClient2025.cer -keystore cacerts -storepass changeit
    - Trust this certificate? [no]: yes
- Confirm the new Client Issuing CA 2025 certificate has been added to the cacerts keystore
    - Note: Your Java Keystore name and password may be different then what is used in this example.
    - C:\Program Files\Java\jreXXX\bin>keytool -list -keystore cacerts -storepass changeit -alias OATIIAClient2025
    - The cacerts keystore should include this entry: OATIIAClient2025, Month Day, Year, trustedCertEntry,
      Certificate fingerprint (SHA1):
      04:56:9E:73:C4:5F:4F:B2:67:51:DB:35:BF:42:5F:15:D7:AE:B8:D4
- Import the new Server Issuing CA 2025 certificate
    - Note: Your Java Keystore name and password may be different then what is used in this example.
    - C:\Program Files\Java\jreXXX\bin>keytool -import -trustcacerts -alias OATIIAServer2025 -file OATIIAServer2025.cer -keystore cacerts -storepass changeit
    - Trust this certificate? [no]: yes
- Confirm the new Issuing Server CA 2025 certificate has been added to the cacerts keystore
    - Note: Your Java Keystore name and password may be different then what is used in this example.
    - C:\Program Files\Java\jreXXX\bin>keytool -list -keystore cacerts -storepass changeit -alias OATIIAServer2025
    - The cacerts keystore should include this entry: OATIIAServer2025, Month Day, Year, trustedCertEntry,
      Certificate fingerprint (SHA1):
      BB:17:0D:2B:F1:BF:19:93:B1:03:E1:5B:D6:81:30:C1:9F:76:04:A1
- As Administrator, copy default CA Certificates keystore (cacerts) from bin directory back to security directory as this is the default location which Java code looks for it
    - Copy C:\Program Files\Java\jreXXX\lib\security\

9. My application uses Java. How do I install your webCARES Root and the new webCARES Client & Server Issuing CA 2025 certificates so that my Java application will work?

- Go to Step 3 if the OATI webCARES Root CA certificate has already been installed
- Step 1: Download the OATI webCARES Root CA certificate (https://www.oaticerts.com/repository/OATICA2.crt) and save it to your Java bin directory (i.e., C:\Program Files\Java\jreXXX\bin\OATICA2.cer)
- Step 2: Add the new Root CA file downloaded in Step 1 to your Java keystore

  Note: Your Java Keystore name and password will be different than what is used in this example.

  C:\Program Files\Java\jreXXX\bin>keytool -import -trustcacerts -alias OATIroot2038 -file OATICA2.cer -keystore cacerts -storepass changeit

  Owner: CN=OATI WebCARES Root CA, O=Open Access Technology International Inc, L=Minneapolis, ST=MN, C=US

  Issuer: CN=OATI WebCARES Root CA, O=Open Access Technology International Inc, L=Minneapolis, ST=MN, C=US

  Serial number: 25762066a7560874f9004bfa1c82841

  Valid from: Tue Jun 03 14:28:31 CDT 2008 until: Thu Jun 03 14:36:00 CDT 2038

  Certificate fingerprints:

  MD5: 70:0C:AA:D0:49:E7:7B:0B:EB:93:77:FA:57:1D:19:73

  SHA1: 4B:6B:D2:D3:88:4E:46:C8:0C:E2:B9:62:BC:59:8C:D9:D5:D8:40:13

  Trust this certificate? [no]: yes

  Certificate was added to keystore

- Step 3: See Section 8 to add the new Client & Server Issuing CA 2025 to the Java keystore.

Note: If the OATI webCARES Root CA certificate is not already added to the keystore then you MUST add the Root CA certificate first (see Steps 1 and 2 above). To see if the OATI webCARES Root CA Certificate is installed, run Step 4 below.

- Step 4: Confirm the webCARES Root and new Client & Server Issuing CA 2025 Certificates are present in the Keystore

Note: Your Java Keystore name and password may be different then what is used in this example and you may have a different number of entries. Please confirm you have the "oatiroot2038", "OATIIAClient2025", and “OATIIAServer2025” entries.

- C:\Program Files\Java\jreXXX\bin>keytool -list -keystore cacerts -storepass changeit -alias oatiroot2038

- The cacerts keystore should include this entry: oatiroot2038, Month Day, Year, trustedCertEntry,
  Certificate fingerprint (SHA1):
  4B:6B:D2:D3:88:4E:46:C8:0C:E2:B9:62:BC:59:8C:D9:D5:D8:40:13

- C:\Program Files\Java\jreXXX\bin>keytool -list -keystore cacerts -storepass changeit -alias OATIIAClient2025

- The cacerts keystore should include this entry: OATIIAClient2025, Month Day, Year, trustedCertEntry,
  Certificate fingerprint (SHA1):
  04:56:9E:73:C4:5F:4F:B2:67:51:DB:35:BF:42:5F:15:D7:AE:B8:D4

- C:\Program Files\Java\jreXXX\bin>keytool -list -keystore cacerts -storepass changeit -alias OATIIAServer2025

- The cacerts keystore should include this entry: OATIIAServer2025, Month Day, Year, trustedCertEntry,
  Certificate fingerprint (SHA1):
  BB:17:0D:2B:F1:BF:19:93:B1:03:E1:5B:D6:81:30:C1:9F:76:04:A1

10. I am an Administrator. How do I install the webCARES Root and the new webCARES Client & Server Issuing CA 2025 certificates into my Microsoft IIS web server or application?

NOTE: You must be logged in as a Windows Administrator in order to complete these steps.

- Services & Applications: Installing the Root certificate
  1. Download the root certificate from http://www.oaticerts.com/repository/OATICA2.crt
  2. Right click on the file and choose the “Install Certificate” option.
  3. In the Wizard that appears, select “Local Machine” and click “Next”.
  4. Click the “Place all certificates in the following store” option.
  5. Click “Browse”.
  6. Select the “Trusted Root Certification Authorities” certificate store from the list and click “OK”.
  7. Click “Next” and “Finish” to complete the installation wizard.
  8. A dialog box should appear indicating successful install certificate installation. Click “OK” on this message.

- Services & Applications: Installing the Server Issuing CA 2025 certificate
  1. Download the Server Issuing CA 2025 certificate from http://www.oaticerts.com/repository/OATIIAServer2025.crt
  2. Right click on the file and choose the “Install Certificate” option.
  3. In the Wizard that appears, select “Local Machine” and click “Next”.

4. Click the “Place all certificates in the following store” option.
5. Click “Browse”.
6. Select the “Intermediate Certification Authorities” certificate store from the list and click “OK”.
7. Click “Next” and “Finish” to complete the installation wizard.
8. A dialog box should appear indicating successful install certificate installation. Click “OK” on this message.

- Services & Applications: Installing the Client Issuing CA 2025 certificate
    1. Download the Client Issuing CA 2025 certificate from http://www.oaticerts.com/repository/OATIIAClient2025.crt
    2. Right click on the file and choose the “Install Certificate” option.
    3. In the Wizard that appears, select “Local Machine” and click “Next”.
    4. Click the “Place all certificates in the following store” option.
    5. Click “Browse”.
    6. Select the “Intermediate Certification Authorities” certificate store from the list and click “OK”.
    7. Click “Next” and “Finish” to complete the installation wizard.
    8. A dialog box should appear indicating successful install certificate installation. Click “OK” on this message.

11. I am an Administrator or developer and am getting the message "Client Certificate is untrusted or corrupt."

If you are seeing error messages displayed in an application log file similar to "Client certificate is untrusted or corrupt". The first step is to make sure the new 2025 CA certificates and the root certificate are present in the correct certificate stores (folders) and try again.

NOTE: You must be logged in as a Windows Administrator in order to complete these steps.

Step 1 - Confirm that **both** of the new webCARES 2025 CA certificates are installed in the “Intermediate Certification Authorities” certificate store.

1. Open the start menu and search for “mmc.exe”.
2. A blank Microsoft Management Console (MMC) window should appear.
3. Go to “File” > “Add/Remove Snap-in…” > Select the “Certificates” Snap-in from the list of available snap-ins and click “Add”.
4. A message box should appear asking if you want to manage certificates for the currently logged in user account (“My user account”), a “Service account” or the “Computer account”. Select the “Computer account” option and click “Next”.
5. Select the “Local Computer” option and click “Finish”.
6. Confirm that the “Certificates (Local Computer)” Snap-in is now listed in the “Selected Snap-ins” section. Then click “OK”.
7. Expand the “Certificates (Local Computer)” item.
8. Expand the “Intermediate Certification Authorities” folder.
9. Once inside the “Intermediate Certification Authorities” folder, click on the “Certificates” folder to view all of the CA certificates that are installed and trusted by the operating system.

10. Confirm that both the “webCARES Client Issuing CA 2025” and the “webCARES Server Issuing CA 2025” certificates are present.
    a. If one (or both) of these certificates are missing, please follow the steps in question #10 " How do I install the webCARES Root and the new webCARES Client & Server Issuing CA 2025 certificates into my Microsoft IIS web server or application?"
        - NOTE: If you import any new certificates or make any other changes to the certificate store while the MMC window is still open you may be required to refresh the MMC display before your changes appear. To refresh the display, simply go to “Action” > “Refresh” in the MMC window).

Step 2 - Confirm that the OATI webCARES Root CA certificate is installed in the “Trusted Root Certification Authorities” certificate store.

1. Open the start menu and search for “mmc.exe”.
2. A blank Microsoft Management Console (MMC) window should appear.
3. Go to “File” > “Add/Remove Snap-in…” > Select the “Certificates” Snap-in from the list of available snap-ins and click “Add”.
4. A message box should appear asking if you want to manage certificates for the currently logged in user account (“My user account”), a “Service account” or the “Computer account”. Select the “Computer account” option and click “Next”.
5. Select the “Local Computer” option and click “Finish”.
6. Confirm that the “Certificates (Local Computer)” Snap-in is now listed in the “Selected Snap-ins” section. Then click “OK”.
7. Expand the “Certificates (Local Computer)” item.
8. Expand the “Trusted Root Certification Authorities” folder.
9. Once inside the “Trusted Root Certification Authorities” folder, click on the “Certificates” folder to view all of the root certificates that are installed and trusted by the operating system.
10. Confirm that the “OATI webCARES Root CA” is present.
    a. If the root certificate is missing, please follow the steps in question #10 "How do I install the webCARES Root and the new webCARES Client & Server Issuing CA 2025 certificates into my Microsoft IIS web server or application?"
        - NOTE: If you import any new certificates or make any other changes to the certificate store while the MMC window is still open you may be required to refresh the MMC display before your changes appear. To refresh the display, simply go to “Action” > “Refresh” in the MMC window).

Step 3 – Reinstall the OATI webCARES Root and both webCARES 2025 CAs certificates

If issues persist even after preforming steps 1 and 2. It may be necessary to reinstall the OATI webCARES Root and both webCARES 2025 CA certificates (“webCARES Client Issuing CA 2025” and “webCARES Server Issuing CA 2025”).

Even with all certificates installed in the proper certificate stores, there are situations where the link between the certificate and the corresponding keys may be broken. Reinstalling these certificates can help reestablish this link. Please see Question #10 "How do I install the webCARES Root and the new webCARES Client & Server Issuing CA 2025 certificates into my

Microsoft IIS web server or application?" for more details about how to reinstall the webCARES Root and new webCARES Issuing CA 2025 certificates.

Step 4 - Reboot the machine

12. How do I install the webCARES Root and the new webCARES Client & Server Issuing CA 2025 certificates into my Mozilla Firefox browser?

NOTE: If you are currently using the Mozilla Firefox browser to access OATI applications, installing the Root certificate may not be necessary. However, installing the Client & Server Issuing CA 2025 certificates will still be required.

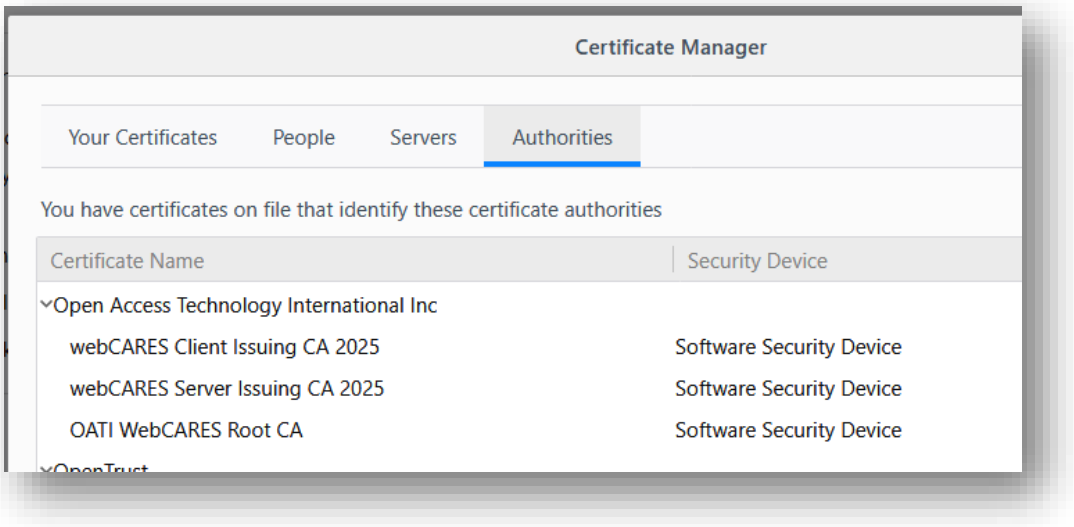
- Installing the webCARES Root certificate
  - From the Tools Menu > Options > Privacy & Security >scroll down to Certificates > "View Certificates" button > Authorities tab
  - Click the "Import" button. Find and open the OATI webCARES Root CA file (OATICA2.crt) downloaded from http://www.oaticerts.com/repository/OATICA2.crt
  - Select each check box to trust the "OATI webCARES Root CA" for identifying web sites (checkbox for email users and software developers can remain unchecked), and click “OK”.

- Installing the webCARES Client Issuing CA 2025 certificate
  - From the Tools Menu > Options > Privacy & Security >scroll down to Certificates > "View Certificates" button > Authorities tab
  - Click the "Import" button. Find and open the webCARES Client Issuing CA 2025 certificate file (OATIIAClient2025.crt) downloaded from https://www.oaticerts.com/repository/OATIIAClient2025.crt
  - Select each check box to trust the "webCARES Client Issuing CA 2025" for identifying web sites (checkbox for email users and software developers can remain unchecked), and click “OK”.

- Installing the webCARES Server Issuing CA 2025 certificate
  - From the Tools Menu > Options > Privacy & Security >scroll down to Certificates > "View Certificates" button > Authorities tab
  - Click the "Import" button. Find and open the webCARES Client Issuing CA 2025 certificate file (OATIIAServer2025.crt) downloaded from https://www.oaticerts.com/repository/OATIIAServer2025.crt
  - Select each check box to trust the "webCARES Server Issuing CA 2025" for identifying web sites (checkbox for email users and software developers can remain unchecked), and click “OK”.

- Verify the webCARES Root and the new webCARES Client & Server Issuing CA 2025 certificates are successfully installed
  - From the Tools Menu > Options > Privacy & Security >scroll down to Certificates > "View Certificates" button > Authorities tab

- Scroll down to 'Open Access Technology International Inc'.
- Verify that the webCARES Root CA and the webCARES Client & Server Issuing CA certificates are installed.



13. How can I test my API connection which uses an OATI client certificate?

Please follow these steps to test your programmatic access to our test site using client certificates issued by both the existing and the new issuer.

Test #1: Test with an existing client certificate from the existing issuer

1. Make sure your client API program is using a client certificate issued from existing issuer (i.e. same certificate you have been using during the past year).
2. Point your program to https://certtest2025.oaticerts.com/clientcertinfo/valid.wml which uses a server certificate issued by the **new** 2025 server issuer.
3. Your results should be a successful connection with the word 'VALID' being part of the response. If a client certificate was not successfully passed to the test site, you will see a '403' error or something similar.

Test #2: Test with a new client certificate from the new 2025 client issuer

1. Install the test client certificate issued from the **new** 2025 client issuer located at http://www.oaticerts.com/repository/TestOATIClient2025.pfx (password is **Test1234**) so that your client API program has access and permission to use it.
2. Point your program to https://certtest2025.oaticerts.com/clientcertinfo/valid.wml which uses a server certificate issued by the **new** 2025 server issuer.
3. Your results should be a successful connection with the word 'VALID' being part of the response. If a client certificate was not successfully passed to the test site, you will see a '403' error or something similar.

14. How can I test my site that uses an OATI server cert?

Please follow these steps to make sure each of your web sites which use an OATI webCARES Server certificate accepts client certificates from the new 2025 client issuer.

1. Install the new webCARES Client Issuing CA 2025 certificate on your web server's certificate store on each web site which uses an OATI webCARES Server certificate.
2. Test with a new client certificate from the new 2025 client issuer.
    a. Install the test client certificate issued from the **new** 2025 client issuer located at http://www.oaticerts.com/repository/TestOATIClient2025.pfx (password is **Test1234**) so that your browser or client API program has access and permission to use it.
    b. Point your browser or client API program to each of your company's web sites which uses an OATI webCARES Server certificate
    c. Your browser should either prompt for the new certificate installed in step 2 (a) or automatically submit it (if it is the only certificate installed). If your browser or client API program does not successfully submit the new client certificate, your login will fail or will see a '403 – Forbidden: Access is denied.' or similar error.