OPEN ACCESS TECHNOLOGY INTERNATIONAL, INC.
3660 Technology Drive NE | Minneapolis, MN 55418
Phone 763.201.2000 | Fax 763.201.5333
www.oati.com

Renewal of the webCARES Root and New Issuing CA 2021 Certificates Frequently Asked Questions (FAQ)

This document contains a list of common questions and answers customers may have regarding testing and installing the webCARES Root or Issuer. If you are unable to find your question in this list or if you have additional questions or run into issues, feel free to reach out to your Project Manager or contact OATI Support at Support@oati.net or 763.201.2020.

Please use the table of contents on the next page to look for your topic and easily jump to that section of the document.

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 I" case that best meets your specific usage case for more information about the impacts of this change on you.

2. What if I just use an OATI client cert to connect to an OATI system?

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 certs?

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 OATI Issuing 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 certs?

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 OATI Issuing certificate. Please consult with your IT department or Web Hosting provider for more information on how to do this.

5. How do I install the new Issuing CA 2021 certificate 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 Issuing CA 2021 certificate
  - Download the http://www.oaticerts.com/repository/OATIIA2021.crt certificate and save it as C:\Program Files\Java\jreXXX\bin\OATIIA2021.cer

- Import the new Issuing CA 2021 certificate
  - C:\Program Files\Java\jreXXX\bin>keytool -import -trustcacerts -alias OATIissuing2021 -file OATIIA2021.cer -keystore cacerts -storepass changeit
  - Trust this certificate? [no]: Yes Certificate was added to keystore
- Confirm the new Issuing CA 2021 certificate has been added to the cacerts keystore
  - C:\Program Files\Java\j2re1.5.0\bin>keytool -list -keystore cacerts -storepass changeit -alias OATIissuing2021
  - The cacerts keystore should include this entry: oatiissuing2021, Month Day, Year, trustedCertEntry,
    Certificate fingerprint (SHA1):
    84:F0:67:56:2C:59:72:15:B3:CF:6B:FD:D3:C7:1F:DF:21:64:BE:F8
  - 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\j2re1.5.0\lib\security\

6. How do I install the webCARES Root and new Issuing CA 2021 certificates into my Mozilla Firefox browser?

- From the Tools Menu > Options > Advanced section > Certificates tab > "View Certificates" button > Authorities tab
- Click the "Import" button. Find and open the OATI webCARES Root CA file (OATICA2.cer) downloaded from http://www.oaticerts.com/repository/OATICA2.crt
- Select each check box to trust the "OATI webCARES Root CA" for identifying web sites, email users, and software developers, and click “OK”
- Click the "Import" button. Find and open the webCARES Issuing CA 2021 certificate file (OATIIA2021.cer) downloaded
  from http://www.oaticerts.com/repository/OATIIA2021.crt
- Select each check box to trust the "webCARES Issuing CA 2021" for identifying web sites, email users, and software developers, and click “OK”
- Verify the webCARES Issuing CA 2021 and OATI webCARES Root CA are installed under the Open Access Technology International heading

7. I am an End User. How do I install the webCARES Root and new Issuing CA 2021 certificates into my Microsoft IE browser?

OATI is part of the Microsoft Root Certificate distribution program so the webCARES Root and new Issuing CA 2021 certificates will be automatically downloaded during an SSL/TLS session or installed during the normal renewal, export, and installation of your End User certificate by your webCARES Security Officer (by selecting "Include all certificates in the certification path (if possible)".)

Note: If you are an End User and are missing these certificates, you can install both of them into your IE browser using the OATIIA2021.p7b file. This file can NOT be used to install certificates for applications, programs, etc.

- End Users: Installing the Root & Issuing Certificates
  - Download http://www.oaticerts.com/repository/OATIIA2021.p7b
  - Right click on file and choose “Install Certificate”
  - Click “Next”
  - Choose “Automatically select the certificate store based on the type of certificate”
    Note: The certificates are installed into the currently logged on user's Windows profile. Each Windows user must install the certificates into their own Windows profile.
  - Choose “Next,” “Finish,” “OK” (to Security Warning) and “OK”

8. I am an Administrator. How do I install the webCARES Root and new Issuing CA 2021 certificates into my Microsoft IIS web server or application?

- Services & Applications: Installing the Root certificate
  - Download http://www.oaticerts.com/repository/OATICA2.crt
  - Right click on file and choose “Install Certificate”
  - Click “Next”
  - Choose “Place all certificates in the following store”
  - Click “Browse”
  - Select “Trusted Root Certification Authorities”
  - Click “OK,” “Next,” “Finish,” and “OK”
- Services & Applications: Installing the Issuing CA 2021 certificate
  - Download http://www.oaticerts.com/repository/OATIIA2021.crt
  - Right click on file and choose “Install Certificate”
  - Click “Next”
  - Choose “Place all certificates in the following store”
  - Click “Browse”
  - Select “Intermediate Certification Authorities”, "Local Computer"

  - Click “OK,” “Next,” “Finish,” and “OK”.

9. We do not use your certificates. Do we still need to install the webCARES Root and new Issuing CA 2021 certificates?

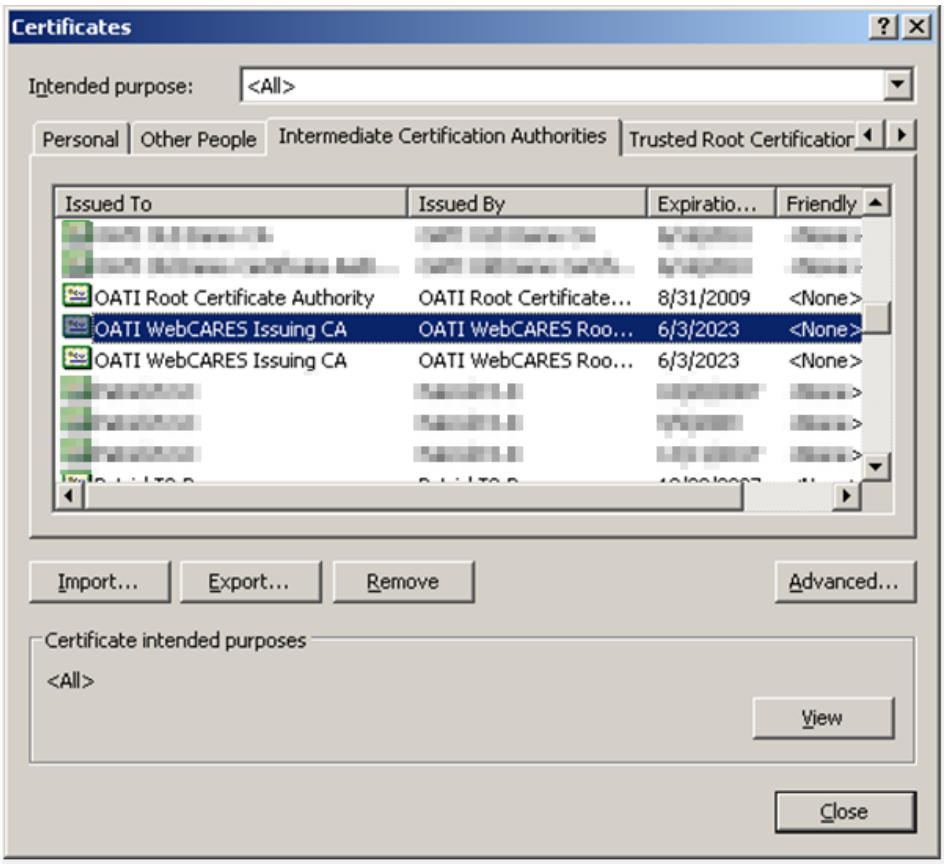
Yes. If you have a web site, web service, or application which accepts OATI webCARES certificates as part of the login, authentication, or authorization process, then you must install these certificates. If the certificates are NOT installed, an incomplete Certificate Trust List (CTL) will be sent to 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).

10. I am an End User and am getting the message "Client Certificate is untrusted or corrupt."

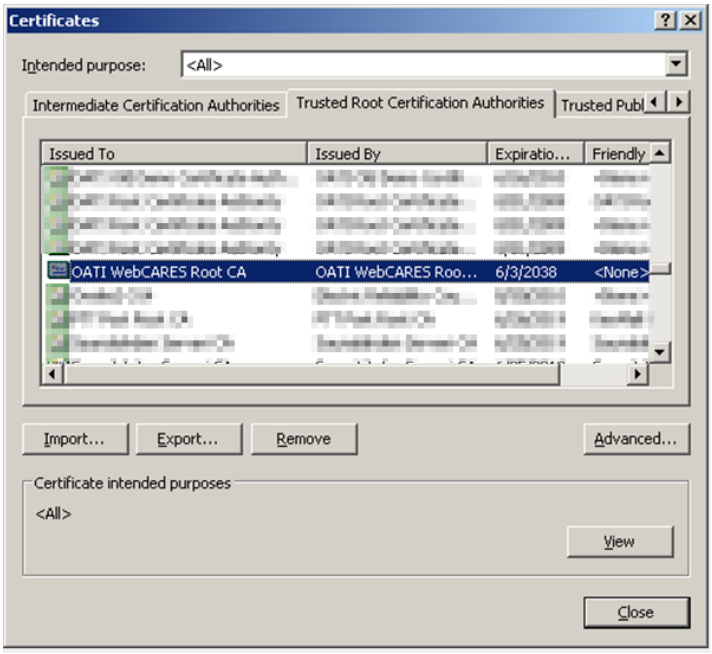
If you are seeing an error displayed in the browser similar to "Client certificate is untrusted or corrupt", the first step is to make sure the webCARES Root and new Issuing CA 2021 certificates are installed and present in the correct certificate stores (folders) and try again.

IMPORTANT: These troubleshooting steps are for an End User who is experiencing this issue. If a similar error is found in an application or program's log file, or given in the browser while testing the application, please see the FAQ I am an Administrator or developer and am getting the message "Client Certificate is untrusted or corrupt."

- Step 1: Confirm the webCARES Issuing CA 2021 certificate is present.
  - Internet Explorer > Tools > Internet Options > Content Tab > "Certificates" button > Intermediate Certification Authorities Tab
  - Confirm webCARES Issuing CA 2021 is present. If not present, click the "Import…" button and import the certificate downloaded from http://www.oaticerts.com/repository/OATIIA2021.crt



  - If present, delete the OATI webCARES Root CA certificate if it is present in this store. Note: The OATI webCARES Root CA should only be in the Trusted Root Certification Authorities certificate store (folder)
- Step 2: Confirm the OATI webCARES Root CA certificate is present.
  - Internet Explorer > Tools > Internet Options > Content Tab > "Certificates" button > Trusted Root Certification Authorities Tab
  - Confirm OATI WebCARES Root CA is present. If not present, click the "Import…" button and import the certificate downloaded from http://www.oaticerts.com/repository/OATICA2.crt



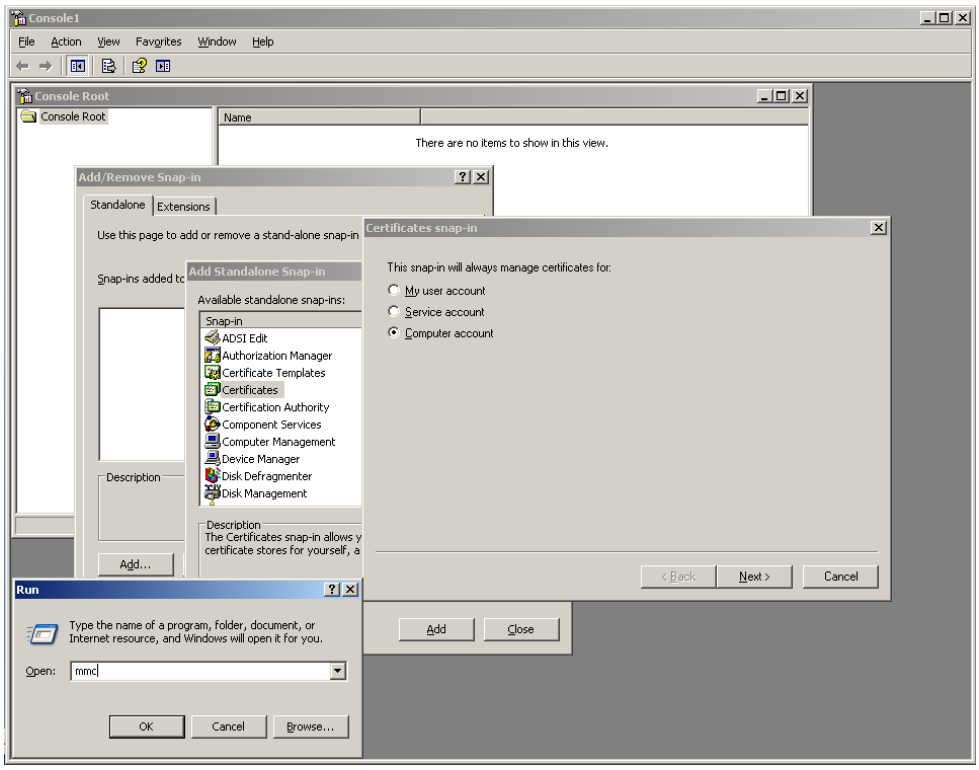
  - If present, delete the webCARES Issuing CA 2021 certificate if it is present in this store. Note: The webCARES Issuing CA 2021 certificate should only be in the Intermediate Certification Authorities certificate store (folder)
- Step 3: If steps 1 and 2 fail to fix the issue please reinstall the webCARES Root CA certificate and webCARES Issuing CA 2021 certificate. Even if these certificates are displayed, there are times when the link between the certificate and the corresponding keys can be broken. Reinstalling the certificate will reestablish this link. Please see the appropriate FAQ "How do I install the webCARES Root and new Issuing CA 2021 certificates into my browser?" for instructions on reinstalling the webCARES Root and new Issuing CA 2021 certificates.
- Step 4: If steps 1, 2, and 3 fail to fix the issue please reboot the machine.

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

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

IMPORTANT: You must be a Windows Administrator to complete these steps.

- Step 1: Confirm the webCARES Issuing CA 2021 and OATI webCARES Root CA certificates are present.
  - "Start" button > Run > MMC > "OK" button > this opens a blank Microsoft Management Console
  - File > Add/Remove Snap-in > Choose Certificates Snap-in > "Add" button > Computer Account > Next > Local Computer > Finish > Close > OK



- Click the plus ("+") sign to expand the Certificates (Local Computer) > Expand the Intermediate Certification Authorities store > Select the Certificates store (folder)

- Confirm webCARES Issuing CA 2021 is present. If not present right click on the Certificates folder and choose Import to import the certificate downloaded from http://www.oaticerts.com/repository/OATIIA2021.crt
- Delete the OATI webCARES Root CA certificate if it is present in this store. Note: The OATI webCARES Root CA certificate should only be in the Trusted Root Certification Authorities certificate store (folder)

- Step 2: Confirm the OATI webCARES Root CA certificate is present.
  - "Start" button > Run > MMC > OK button > this opens a blank Microsoft Management Console
  - File > Add/Remove Snap-in > Choose Certificates Snap-in > "Add" button > Computer Account > Next > Local Computer > Finish > Close > OK
  - Click the plus ("+") sign to expand Certificates (Local Computer) > Expand the Trusted Root Certification Authorities store > Select the Certificates store
  - Confirm the OATI WebCARES Root CA is present. If not present right click on the Certificates folder and choose Import to import the certificate downloaded from http://www.oaticerts.com/repository/OATICA2.crt

  - Delete the webCARES Issuing CA 2021 certificate if it is present in this store. Note: The webCARES Issuing CA 2021 certificate should only be in the Intermediate Certification Authorities certificate store (folder)
- Step 3: If steps 1 and 2 fail to solve the issue, please reinstall the OATI webCARES Root CA certificate and webCARES Issuing CA 2021 certificate. Even if these certificates are displayed, there are times when the link between the certificate and the corresponding keys can be broken. Reinstalling the certificate will reestablish this link. Please see the FAQ "How do I install the webCARES Root and new Issuing CA 2021 certificates into my Microsoft web server or application?" for instructions on reinstalling the webCARES Root and new Issuing CA 2021 certificates.
- Step 4: If steps 1, 2, and 3 fail to fix the issue, please reboot the machine

12. My application uses Java. How do I install your webCARES Root and new Issuing CA 2021 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 (http://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]: y

Certificate was added to keystore

- Step 3: Download the new webCARES Issuing CA 2021 certificate (http://www.oaticerts.com/repository/OATIIA2021.crt) and save it to your Java bin directory (i.e., C:\Program Files\Java\jreXXX\bin\OATIIA2021.cer)
- Step 4: Add the new Issuing CA 2021 file to your Java keystore

Note: If the OATI webCARES Root CA certificate is not already added to the keystore then you MUST add new Root CA certificate first (see Steps 1 and 2 above). To see if the OATI webCARES Root CA Certificate is installed, run Step 5 below.

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 OATIissuing2021 -file OATIIA2021.cer -keystore cacerts -storepass changeit

Trust this certificate? [no]: Y

Certificate was added to keystore

- Step 5: Confirm the webCARES Root and new Issuing CA 2021 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" and "oatiissuing2021" entries.

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

oatiroot2038, Month Day, Yr, trustedCertEntry,

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

oatiissuing2021, Month, Day, Yr, trustedCertEntry,

Certificate fingerprint (SHA1): 84:F0:67:56:2C:59:72:15:B3:CF:6B:FD:D3:C7:1F:DF:21:64:BE:F8

13. How do I request a test cert?

If you wish to test the different uses of the new OATI certificates in your environment, 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.

14. How can I test my API connection which uses an OATI client cert?

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 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://valid2021.oaticerts.com which uses a server certificate issued by the **new** issuer.
3. Your results should be "SUCCESS - If you are seeing this page you have successfully tested the OATI webCARES Issuing CA 2021 authority". 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** issuer:

1. Install the "Test webCARES Issuing CA 2021 Client Certificates.pfx" certificate located at http://www.oaticerts.com/repository/Test-webCARES-issuing-CA-2021-Client-Certificate.pfx (password is **Test1234**) so that your program has access and permission to use it. If questions on how to do this please let us know by replying to this email.
2. Point your program to https://valid2021.oaticerts.com which uses a server certificate issued by the new issuer.
3. Your results should be "SUCCESS - If you are seeing this page you have successfully tested the OATI webCARES Issuing CA 2021 authority". If a client certificate was not successfully passed to the test site you will see a "403" error or something similar.

15. 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 issuer.

1. Install the new webCARES Issuing CA 2021 certificate into your Microsoft IIS web server's "Intermediate Certification Authorities" certificate store on **each web site which uses an OATI webCARES Server certificate**. Once done continue to step 2 below.

NOTE: Please reach out to Support@oati.net if you use Apache Server (OpenSSL), Tomcat Server (Keytool) or other non-Microsoft web server and need assistance with these steps.

a. Download https://www.oaticerts.com/repository/OATIIA2021.crt
b. Right-click on file and choose "Install Certificate"
c. Click "Next"
d. Choose "Place all certificates in the following store"
e. Click "Browse"
f. Select "Intermediate Certification Authorities", "Local Computer"
g. Click "OK," "Next," "Finish," and "OK".

2. Test with a new "Test webCARES Issuing CA 2021 Client Certificate" client certificate from the **new** issuer:
   a. Install the "Test webCARES Issuing CA 2021 Client Certificates.pfx" certificate located at http://www.oaticerts.com/repository/Test-webCARES-issuing-CA-2021-Client-Certificate.pfx (password is Test1234) so that your browser or client API program has access and permission to use it. If questions on how to do this please let us know by replying to this email.
   b. **Point your browser or client API program to each of your company's web sites which uses an OATI webCARES Server certificate** (make sure the above test Step 1 has been done).
   c. Your browser should either prompt for the new "Test webCARES issuing CA 2021 Client Certificate" or automatically submit it (if it is the only certificate installed). If your browser or client API program does not successfully submit the "Test webCARES issuing CA 2021 Client Certificate" your login will fail or will see a "403 – Forbidden: Access is denied." or similar error.

If you have additional questions or run into issues, feel free to reach out to your Project Manager or contact OATI Support at Support@oati.net or 763.201.2020.