Ocularis Web – WebRTC Configuration Guide

Version 5.8

October, 2019

PROPRIETARY AND CONFIDENTIAL INFORMATION

All information contained herein is confidential, proprietary and the exclusive property of Qognify Ltd and its affiliates (“Qognify”). This document and any parts thereof must not be reproduced, copied, disclosed or distributed without Qognify's written approval and any content or information hereof shall not be used for any unauthorized purpose. The software described herein and any other feature or tools are provided "AS IS" and without any warranty or guarantee of any kind.

TO THE MAXIMUM EXTENT PERMITTED BY LAW, QOGNIFY HEREBY DISCLAIMS ALL OTHER WARRANTIES OF ANY KIND WITH RESPECT TO THE SOFTWARE DESCRIBED HEREIN EITHER EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE OR USE

Revision History

Revision	Purpose for Change	Author	Date
00	GA	D. Jecker	Oct 2019
01	Title	D. Jecker	Oct 2019

Contents

List of Tables

List of Figures

1 About This Guide

This document describes how to import certificates in a browser for use with Ocularis Web..

1.1 Related Documentation

Related documents are listed below.

Table 1-1: Related Documents

Document Name	Version	File Type	Date
Ocularis 5.8 Release Notes	5.8	PDF	October 2019
Add-on Documentation			

2 Introduction

WebRTC (Web Real-Time Communication) provides web browsers with real-time communication via a simple application programming interface. It replaces Adobe Flash in Ocularis Web v5.7. In order to take advantage of this technology, a certificate must be imported into the browser used to view Ocularis Web video. This process need only be done once. These steps assume that Ocularis Media Server (OMS) has already been upgraded to v5.7.

Keep in mind that with WebRTC, TCP Port 8420 must be open as it is used for live video. Port 1935 is still used when sending M2O video from the Ocularis Mobile App to Ocularis Media Server.

Note: The Microsoft Internet Explorer browser is no longer supported.

Supported Browsers:

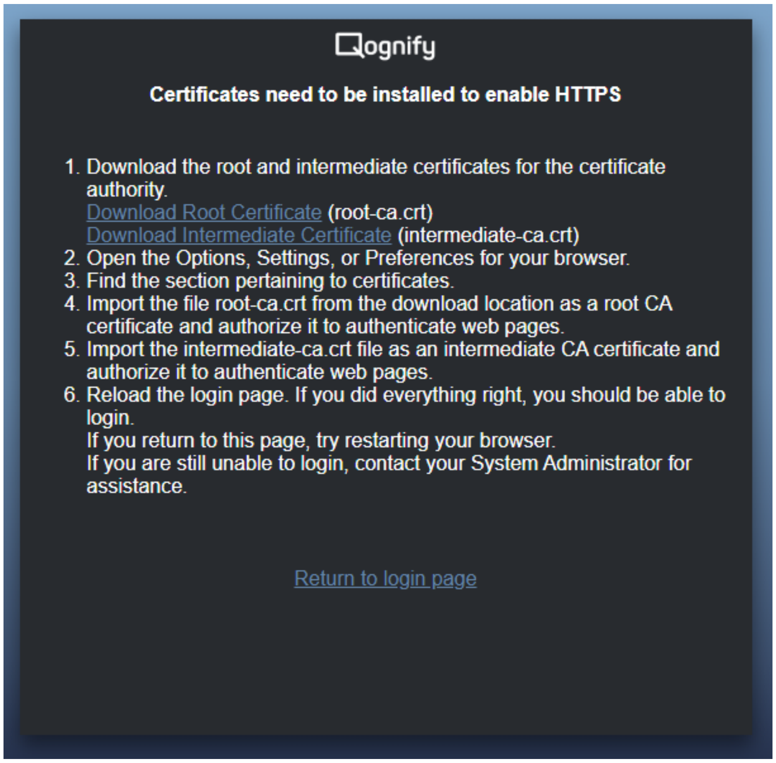
- Google Chrome
- Mozilla Firefox
- Microsoft Edge
- Apple Safari

3 Google Chrome

These steps are required in order to proceed with Ocularis Web. They only need to be done once for this browser.

1. Open the browser and enter the IP address of the Ocularis Media Server in the URL field. You should see the following screen:

Figure 1 Initial Message for Google Chrome Browser



Certificates need to be installed to enable HTTPS

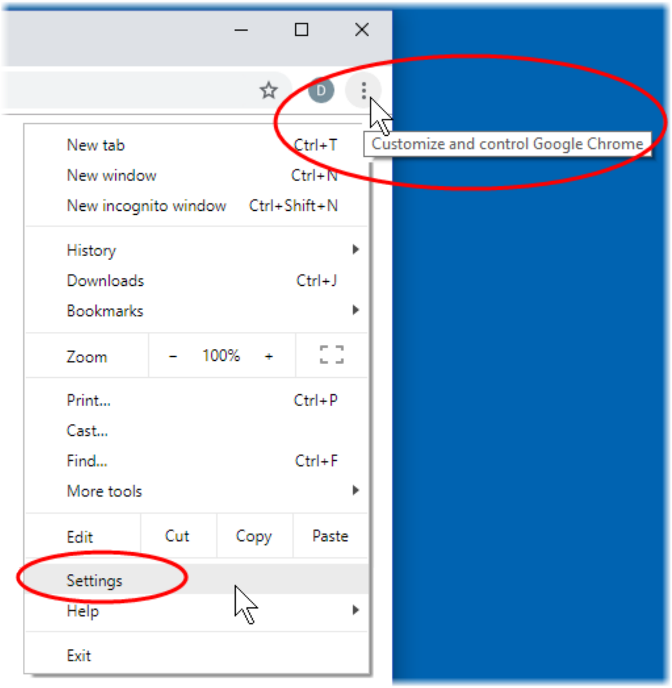
1. Download the root and intermediate certificates for the certificate authority.
   Download Root Certificate (root-ca.crt)
   Download Intermediate Certificate (intermediate-ca.crt)
2. Open the Options, Settings, or Preferences for your browser.
3. Find the section pertaining to certificates.
4. Import the file root-ca.crt from the download location as a root CA certificate and authorize it to authenticate web pages.
5. Import the intermediate-ca.crt file as an intermediate CA certificate and authorize it to authenticate web pages.
6. Reload the login page. If you did everything right, you should be able to login.
   If you return to this page, try restarting your browser.
   If you are still unable to login, contact your System Administrator for assistance.

Return to login page

2. Click the corresponding links to download the root and intermediate certificates for the certificate authority. Remember where you store the downloaded files.
   - Root Certificate (root-ca.crt)
   - Intermediate Certificate (intermediate-ca.crt)

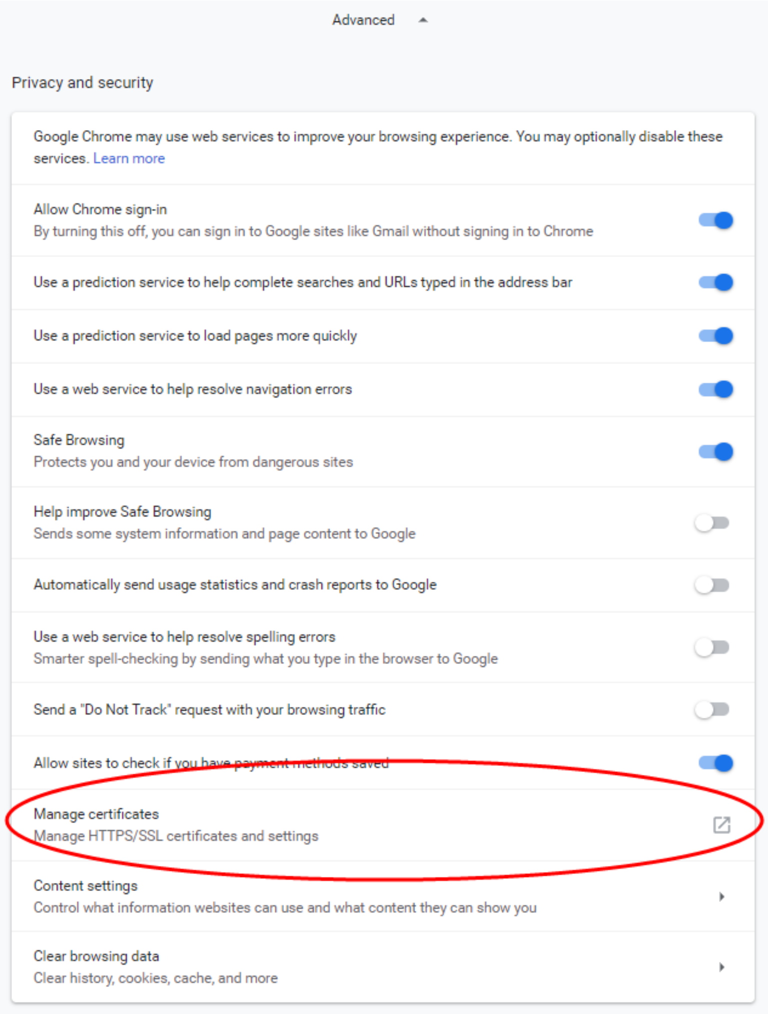
3. Click the ‘Customize and Control Google Chrome’ icon to the right of the URL bar and select ‘Settings’.

Figure 2 Customize...Settings



4. Scroll the page and click ‘Advanced’ to expand the ‘Privacy and security’ section.

Figure 3 Manage certificates



Advanced

Privacy and security

Google Chrome may use web services to improve your browsing experience. You may optionally disable these services. Learn more

Allow Chrome sign-in
By turning this off, you can sign in to Google sites like Gmail without signing in to Chrome

Use a prediction service to help complete searches and URLs typed in the address bar

Use a prediction service to load pages more quickly

Use a web service to help resolve navigation errors

Safe Browsing
Protects you and your device from dangerous sites

Help improve Safe Browsing
Sends some system information and page content to Google

Automatically send usage statistics and crash reports to Google

Use a web service to help resolve spelling errors
Smarter spell-checking by sending what you type in the browser to Google

Send a "Do Not Track" request with your browsing traffic

Allow sites to check if you have payment methods saved

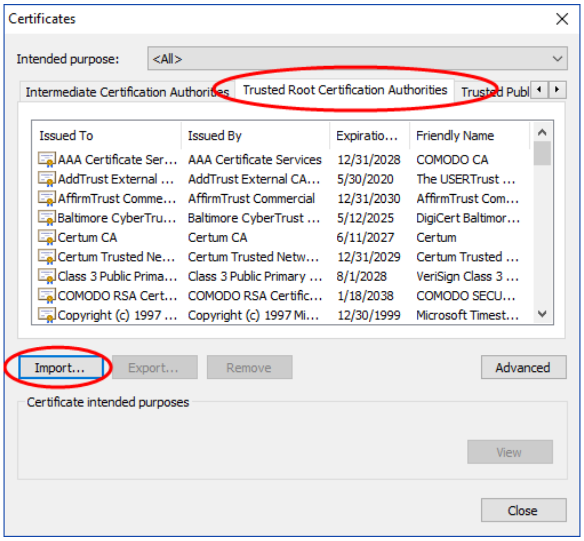
Manage certificates
Manage HTTPS/SSL certificates and settings

Content settings
Control what information websites can use and what content they can show you

Clear browsing data
Clear history, cookies, cache, and more

5. Select the section ‘Manage certificates’.
6. Select the tab ‘Trusted Root Certification Authorities’.

Figure 4 Import the certificate



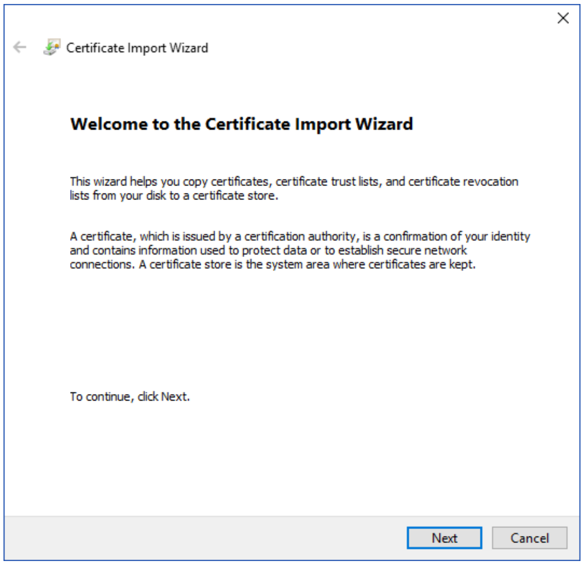
Certificates
Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ
Import...
Export...
Remove
Advanced
Certificate intended purposes
View
Close

Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
AAA Certificate Ser...	AAA Certificate Services	12/31/2028	COMODO CA
AddTrust External ...	AddTrust External CA...	5/30/2020	The USERTrust ...
AffirmTrust Comme...	AffirmTrust Commercial	12/31/2030	AffirmTrust Com...
Baltimore CyberTru...	Baltimore CyberTrust ...	5/12/2025	DigiCert Baltimor...
Certum CA	Certum CA	6/11/2027	Certum
Certum Trusted Ne...	Certum Trusted Netw...	12/31/2029	Certum Trusted ...
Class 3 Public Prima...	Class 3 Public Primary ...	8/1/2028	VeriSign Class 3 ...
COMODO RSA Cert...	COMODO RSA Certific...	1/18/2038	COMODO SECU...
Copyright (c) 1997 ...	Copyright (c) 1997 Mi...	12/30/1999	Microsoft Timest...

7. Click **Import…** to start the Certificate Import Wizard.

Figure 5 Certificate Import Wizard



Welcome to the Certificate Import Wizard

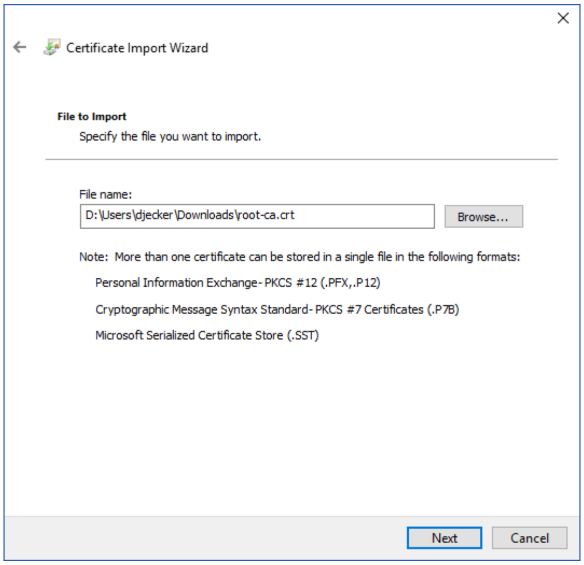
This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

8. Click **Next**.
9. Click **Browse…** and locate the file ‘root-ca.crt’ from the download location. Select the file and click **Open**.

Figure 6 Import the root-ca certificate



File to Import

Specify the file you want to import.

File name:

D:\Users\djecker\Downloads\root-ca.crt

Note: More than one certificate can be stored in a single file in the following formats:

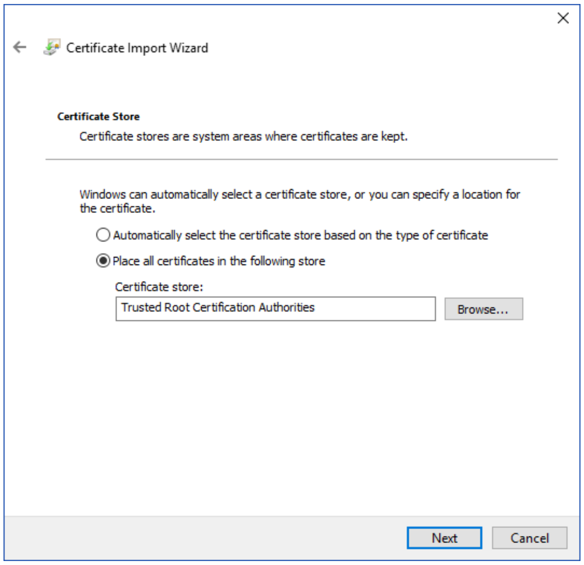
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

10. Click **Next**.
11. Leave the default selection ‘Place all certificates in the following store’ and verify the store is ‘Trusted Root Certification Authorities’. Click **Next**.

Figure 7 Place certificate in Trusted Root Certification Authorities Store



Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

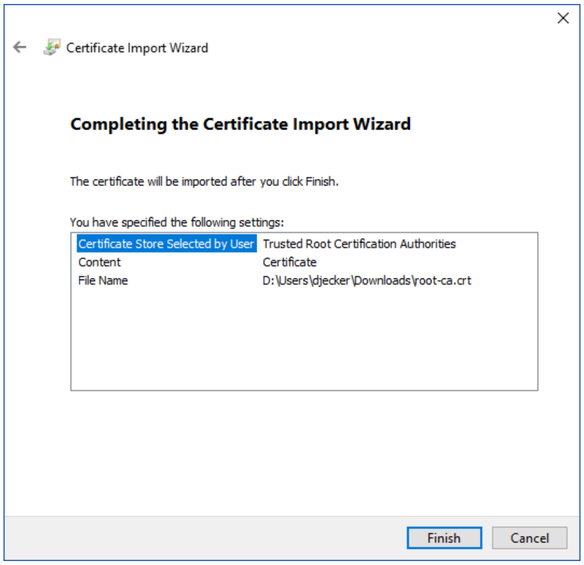
● Place all certificates in the following store

Certificate store:

Trusted Root Certification Authorities

12. Click **Finish**.

Figure 8 Completing the Import



Completing the Certificate Import Wizard

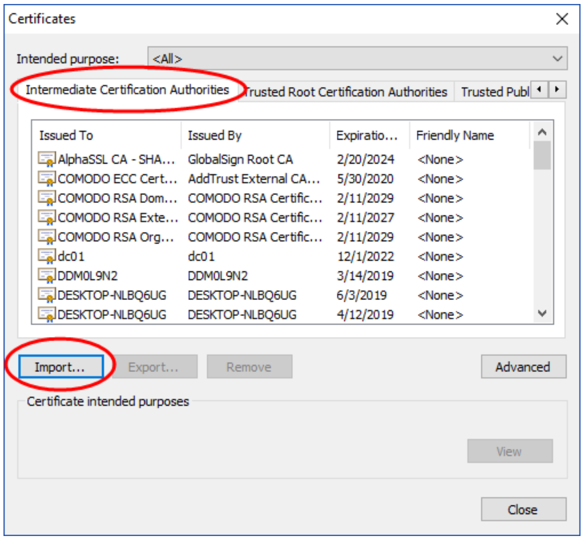
The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate
File Name	D:\Users\djecker\Downloads\root-ca.crt

13. At 'The import was successful' pop-up, click **OK**.
14. Next, import the 'intermediate-ca.crt' file. Select the tab 'Intermediate Certification Authorities'.

Figure 9 Import the Intermediate Certificate file

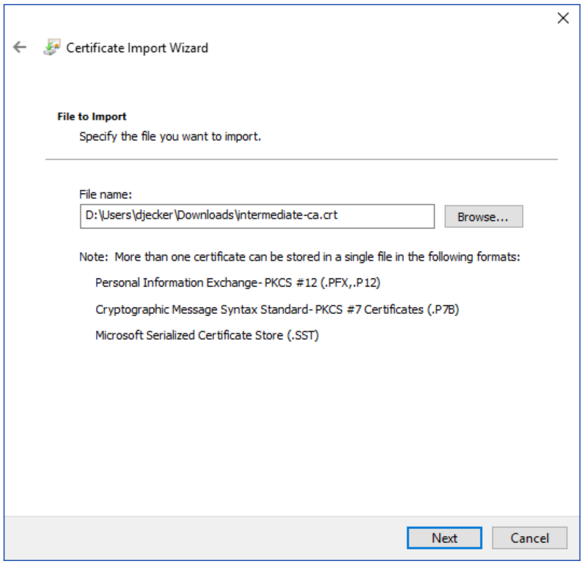

Certificates
Intermediate Certification Authorities
Trusted Root Certification Authorities
Trusted Publ
Import...
Export...
Remove
Advanced
Certificate intended purposes
View
Close

Intended purpose: <All>

Issued To	Issued By	Expiratio...	Friendly Name
AlphaSSL CA - SHA...	GlobalSign Root CA	2/20/2024	<None>
COMODO ECC Cert...	AddTrust External CA...	5/30/2020	<None>
COMODO RSA Dom...	COMODO RSA Certific...	2/11/2029	<None>
COMODO RSA Exte...	COMODO RSA Certific...	2/11/2027	<None>
COMODO RSA Org...	COMODO RSA Certific...	2/11/2029	<None>
dc01	dc01	12/1/2022	<None>
DDM0L9N2	DDM0L9N2	3/14/2019	<None>
DESKTOP-NLBQ6UG	DESKTOP-NLBQ6UG	6/3/2019	<None>
DESKTOP-NLBQ6UG	DESKTOP-NLBQ6UG	4/12/2019	<None>

15. Click **Import…** to launch the Certificate Import Wizard (see Figure 5).
16. Click **Next**.
17. Click **Browse…** and locate the file 'intermediate-ca.crt' from the download location.

Figure 10 Import the Intermediate Certificate



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

D:\Users\djecker\Downloads\intermediate-ca.crt

Note: More than one certificate can be stored in a single file in the following formats:

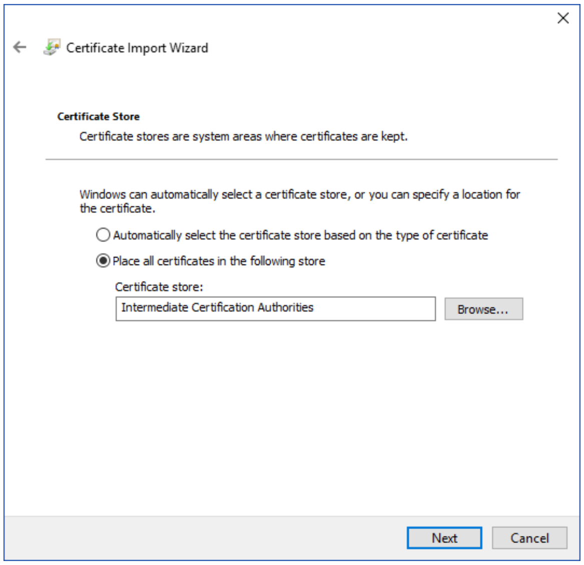
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

18. Click **Next**.
19. Leave the default selection ‘Place all certificates in the following store’ and verify the store is ‘Intermediate Certification Authorities’. Click **Next**.

Figure 11 Place certificate in Intermediate Store



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

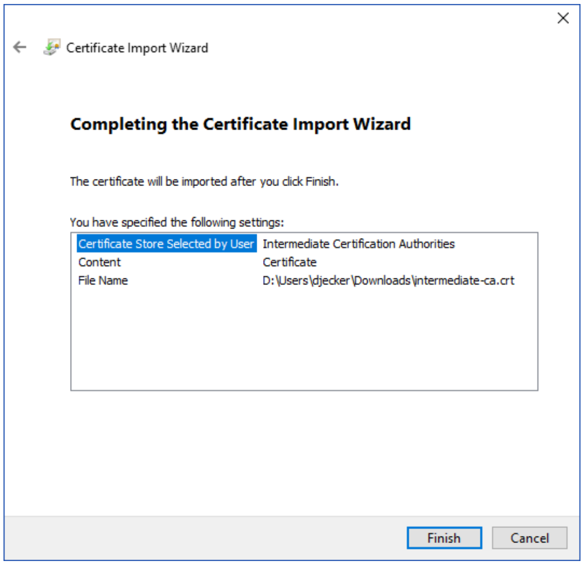
● Place all certificates in the following store

Certificate store:

Intermediate Certification Authorities

20. Click **Finish**.

Figure 12 Complete the Import Wizard



Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Intermediate Certification Authorities
Content	Certificate
File Name	D:\Users\djecker\Downloads\intermediate-ca.crt

21. At 'The import was successful' pop-up, click **OK**.
22. Click **Close** on the 'Certificates' pop-up.
23. Reload the login page or click 'Return to login page'. If you did everything right, you should be able to login.

    If you return to this page, try restarting your browser.

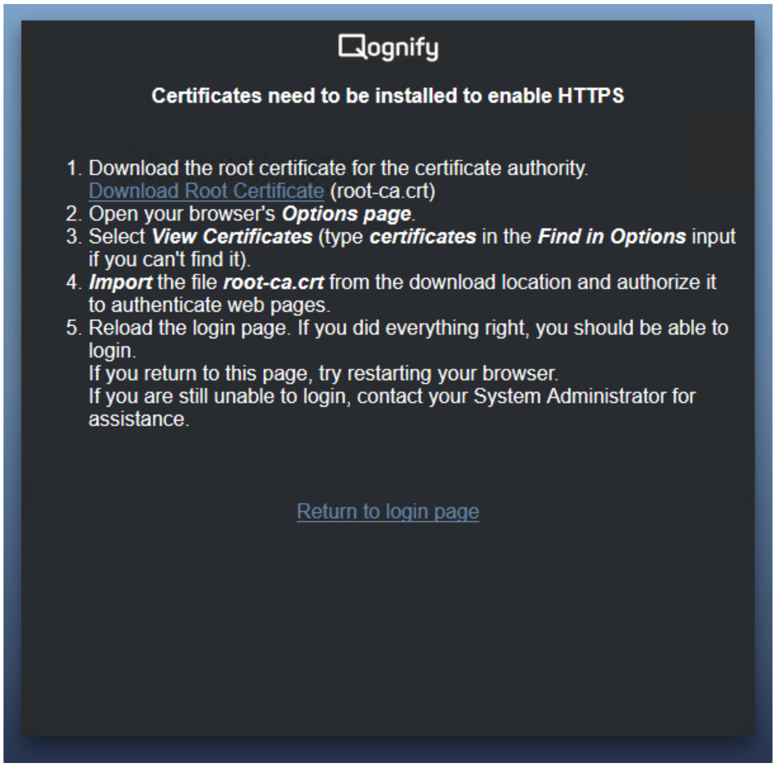
    If you are still unable to login, contact your System Administrator for assistance.

4 Mozilla Firefox

These steps are required in order to proceed with Ocularis Web. They only need to be done once for this browser. You may need to install Microsoft's Feature Pack for some operating systems. A message appears in Firefox if this is necessary.

1. Open the browser and enter the IP address of the Ocularis Media Server in the URL field. You should see the following screen:

Figure 13 Initial screen Mozilla Firefox



Qognify

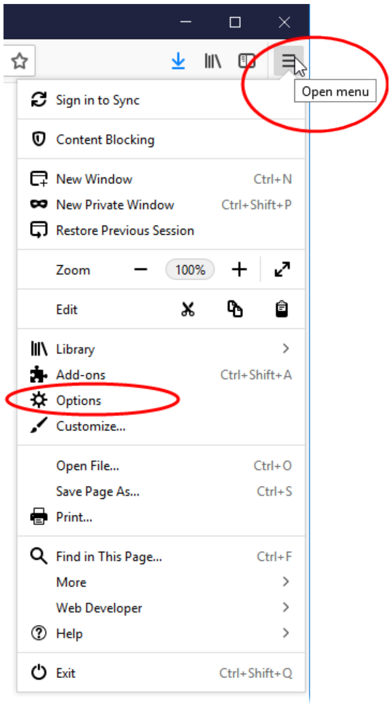
Certificates need to be installed to enable HTTPS

1. Download the root certificate for the certificate authority.
   Download Root Certificate (root-ca.crt)
2. Open your browser's ***Options page***.
3. Select ***View Certificates*** (type ***certificates*** in the ***Find in Options*** input if you can't find it).
4. ***Import*** the file ***root-ca.crt*** from the download location and authorize it to authenticate web pages.
5. Reload the login page. If you did everything right, you should be able to login.
   If you return to this page, try restarting your browser.
   If you are still unable to login, contact your System Administrator for assistance.

Return to login page

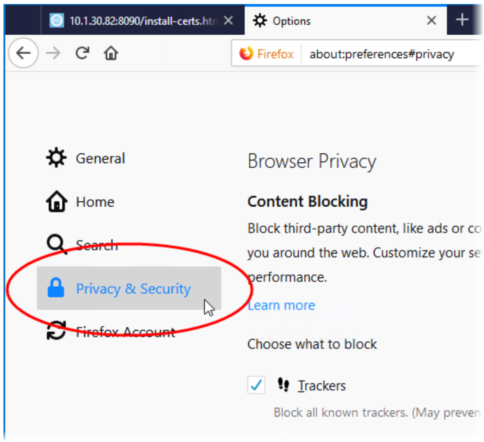
2. Click the link to download the root certificate (root-ca.crt) for the certificate authority. Remember where you store the downloaded file.
3. Open your browser's Options page. Click the 'Open menu' icon to the right of the URL bar. Then select 'Options'.

Figure 14 Open Menu...Options



4. Click ‘Privacy & Security’ from the menu on the left.

Figure 15 Privacy & Security



Browser Privacy

Content Blocking

Block third-party content, like ads or co you around the web. Customize your se performance.

Learn more

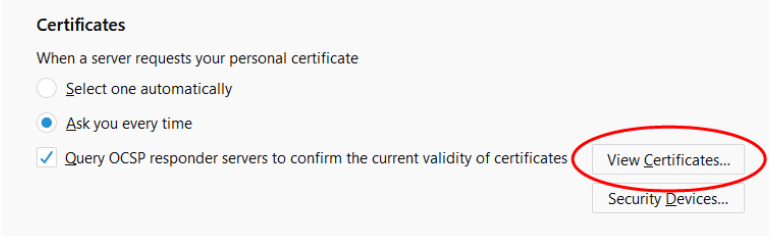
Choose what to block

✓ Trackers

Block all known trackers. (May preven

5. Scroll down until you see the section on **Certificates**.
6. Select ‘View Certificates…’ (type certificates in the Find in Options input if you can't find it).

Figure 16 View Certificates



Certificates

When a server requests your personal certificate

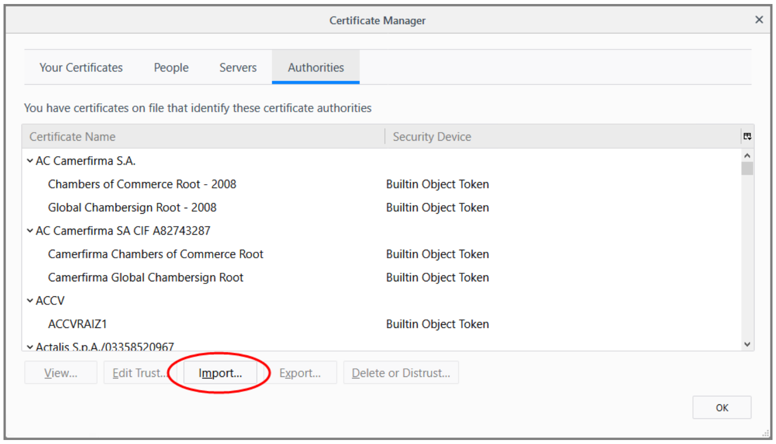
○ Select one automatically

● Ask you every time

☑ Query OCSP responder servers to confirm the current validity of certificates

7. Import the file 'root-ca.crt' from the download location and authorize it to authenticate web pages. Click **Import…**

Figure 17 Import the certificate



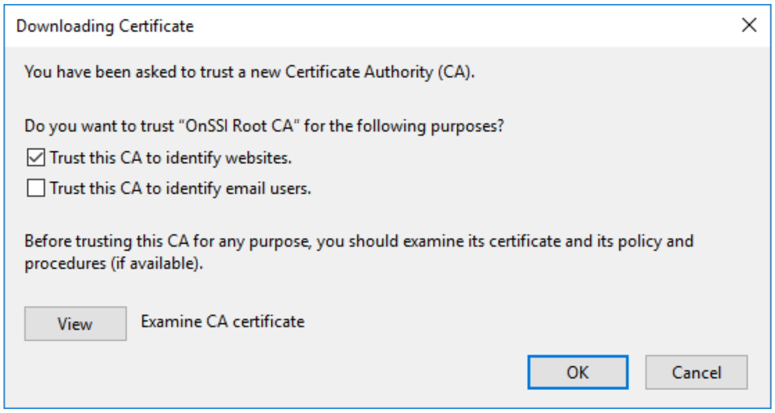
Certificate Manager

You have certificates on file that identify these certificate authorities

Certificate Name	Security Device
⌄ AC Camerfirma S.A.	
Chambers of Commerce Root - 2008	Builtin Object Token
Global Chambersign Root - 2008	Builtin Object Token
⌄ AC Camerfirma SA CIF A82743287	
Camerfirma Chambers of Commerce Root	Builtin Object Token
Camerfirma Global Chambersign Root	Builtin Object Token
⌄ ACCV	
ACCVRAIZ1	Builtin Object Token
⌄ Actalis S.p.A./03358520967	

8. Browse to the 'root.ca.crt' file. Select the file and click **Open**.
9. Check the box for 'Trust this CA to identify websites' and click **OK**.

Figure 18 Trust CA



Downloading Certificate

You have been asked to trust a new Certificate Authority (CA).

Do you want to trust "OnSSI Root CA" for the following purposes?

☑ Trust this CA to identify websites.

☐ Trust this CA to identify email users.

Before trusting this CA for any purpose, you should examine its certificate and its policy and procedures (if available).

Examine CA certificate

10. Click **OK** again on the Certificate Manager screen.

11. Reload the login page or click ‘Return to login page’. If you did everything right, you should be able to login.

If you return to this page, try restarting your browser.

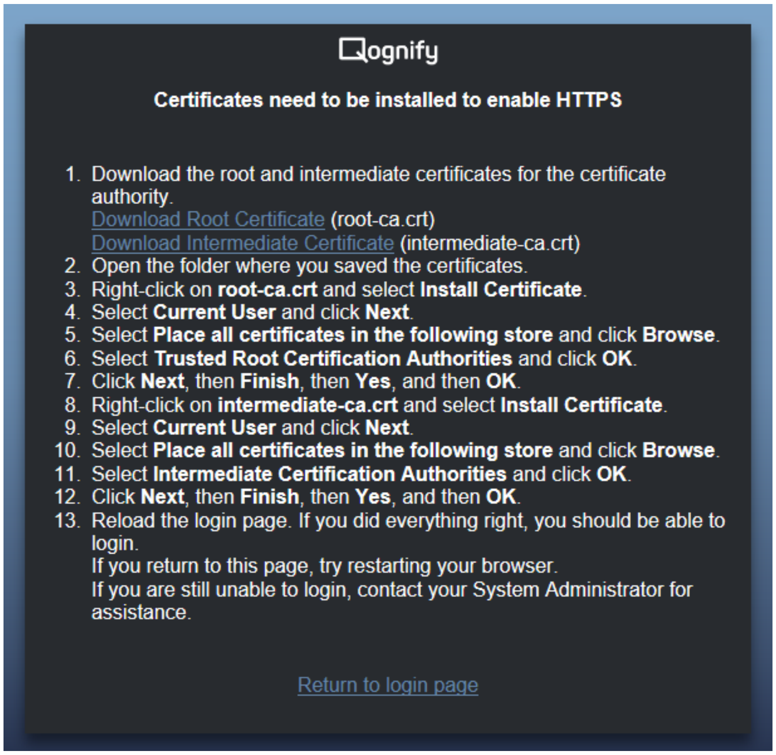
If you are still unable to login, contact your System Administrator for assistance.

5 Microsoft Edge

These steps are required in order to proceed with Ocularis Web. They only need to be done once for this browser.

1. Open the browser and enter the IP address of the Ocularis Media Server in the URL field. You should see the following screen:

Figure 19 Initial message for Microsoft Edge



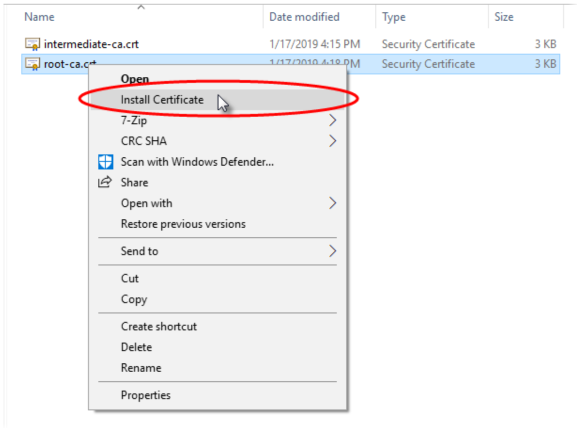
Certificates need to be installed to enable HTTPS

1. Download the root and intermediate certificates for the certificate authority.
   Download Root Certificate (root-ca.crt)
   Download Intermediate Certificate (intermediate-ca.crt)
2. Open the folder where you saved the certificates.
3. Right-click on **root-ca.crt** and select **Install Certificate**.
4. Select **Current User** and click **Next**.
5. Select **Place all certificates in the following store** and click **Browse**.
6. Select **Trusted Root Certification Authorities** and click **OK**.
7. Click **Next**, then **Finish**, then **Yes**, and then **OK**.
8. Right-click on **intermediate-ca.crt** and select **Install Certificate**.
9. Select **Current User** and click **Next**.
10. Select **Place all certificates in the following store** and click **Browse**.
11. Select **Intermediate Certification Authorities** and click **OK**.
12. Click **Next**, then **Finish**, then **Yes**, and then **OK**.
13. Reload the login page. If you did everything right, you should be able to login.
    If you return to this page, try restarting your browser.
    If you are still unable to login, contact your System Administrator for assistance.

Return to login page

2. Click the corresponding links to download the root and intermediate certificates for the certificate authority. Remember where you store the downloaded files.
3. Use Windows Files Explorer to open the folder where the certificates reside.

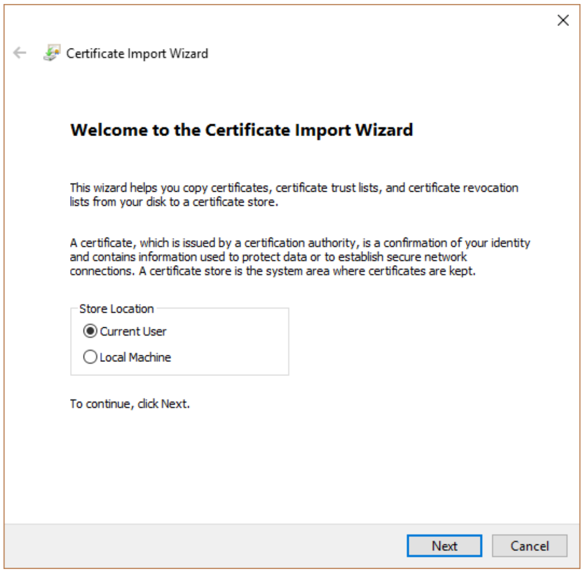
Figure 20 Right-click file and select Install Certificate



Name	Date modified	Type	Size
intermediate-ca.crt	1/17/2019 4:15 PM	Security Certificate	3 KB
root-ca.crt	1/17/2019 4:18 PM	Security Certificate	3 KB

4. If you get a security warning about opening the file, click **Open**. A **Certificate Import Wizard** appears.

Figure 21 Certificate Import Wizard



Certificate Import Wizard

Welcome to the Certificate Import Wizard

This wizard helps you copy certificates, certificate trust lists, and certificate revocation lists from your disk to a certificate store.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

Store Location

● Current User

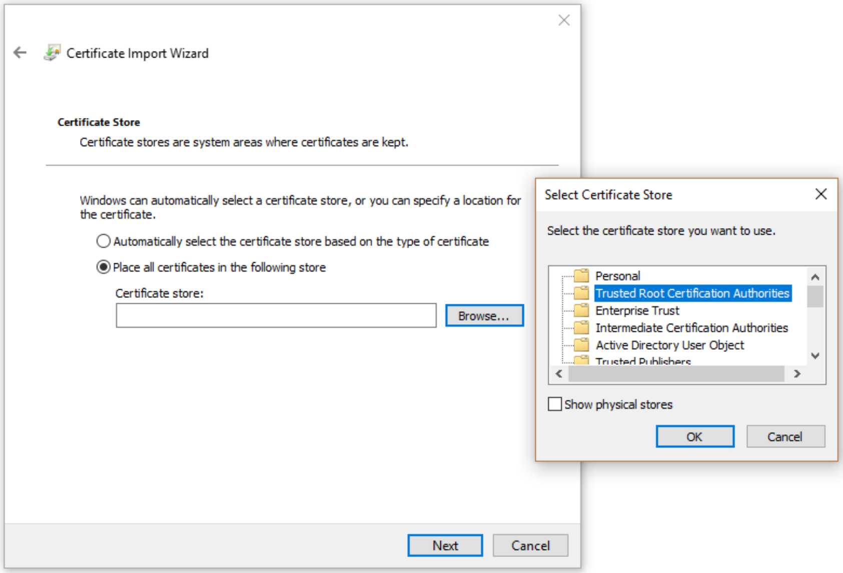
○ Local Machine

To continue, click Next.

5. Leave the default selection of **Current User** selected and click **Next**.

6. Select **Place all certificates in the following store** and click **Browse…**

Figure 22 Select Certificate Store



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

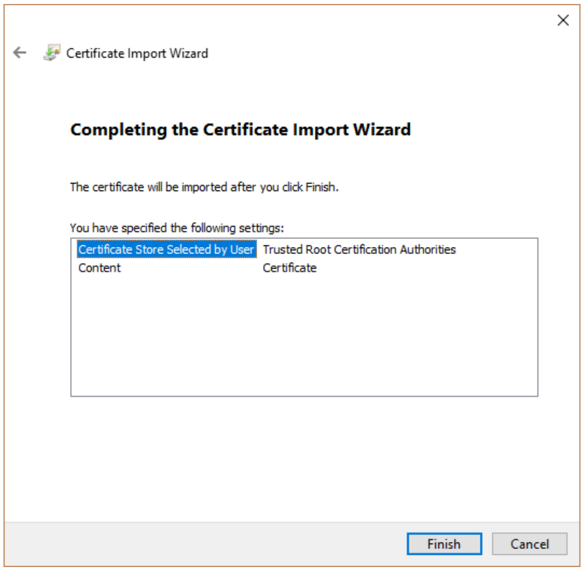
Select Certificate Store

Select the certificate store you want to use.

Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Active Directory User Object
Trusted Publishers
□ Show physical stores
OK
Cancel

7. Select the store **Trusted Root Certification Authorities** and click **OK**.
8. Click **Next**.

Figure 23 Completing the Certificate Import Wizard



Certificate Import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

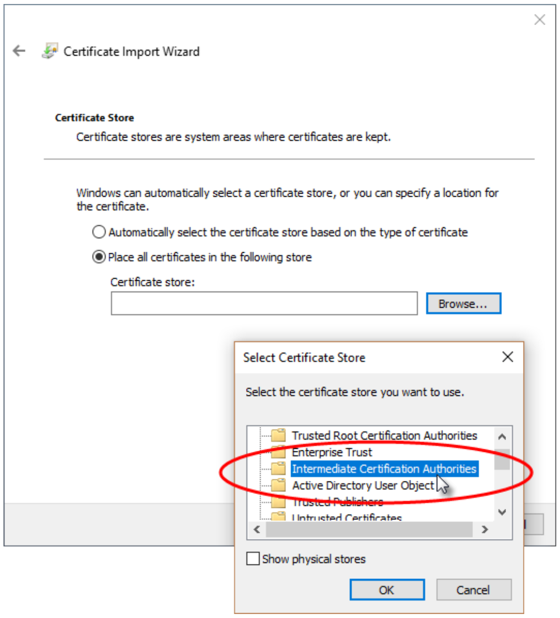
Certificate Store Selected by User	Trusted Root Certification Authorities
Content	Certificate

Figure 24 Completing the Certificate Import Wizard

9. Click **Finish**.
10. At the **Import was successful** pop-up, click **OK**.

11. Repeat the steps for the other certificate. From within Windows File Explorer, right-click the **intermediate-ca.crt** file and select **Install Certificates**.
12. If you get a security warning about opening the file, click **Open**.
13. At the **Certificate Import Wizard**, leave the default selection of **Current User** selected and click **Next**.
14. Select **Place all certificates in the following store** and click **Browse…**
15. Select the store **Intermediate Certification Authorities** and click **OK**.

Figure 25 Select Intermediate Certification Authorities



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store:

Select Certificate Store

Select the certificate store you want to use.

- Trusted Root Certification Authorities
- Enterprise Trust
- Intermediate Certification Authorities
- Active Directory User Object
- Trusted Publishers
- Untrusted Certificates

□ Show physical stores

16. Click **Next** at the **Certificate Import Wizard**.
17. Click **Finish** at the Completing the **Certificate Import Wizard** screen.
18. At the **Import was successful** pop-up, click **OK**.
19. Reload the login page or click ‘Return to login page’. If you did everything right, you should be able to login.

    If you return to this page, try restarting your browser.

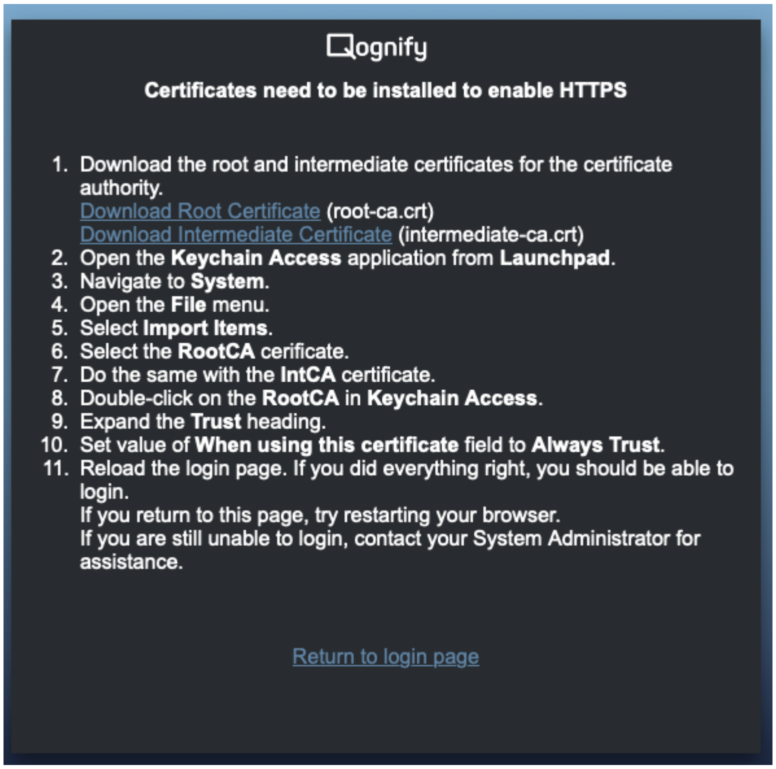
    If you are still unable to login, contact your System Administrator for assistance.

6 Apple Safari

These steps are required in order to proceed with Ocularis Web. They only need to be done once for this browser.

1. Open the browser and enter the IP address of the Ocularis Media Server in the URL field. You should see the following screen:

Figure 26 Initial Screen on Apple Safari



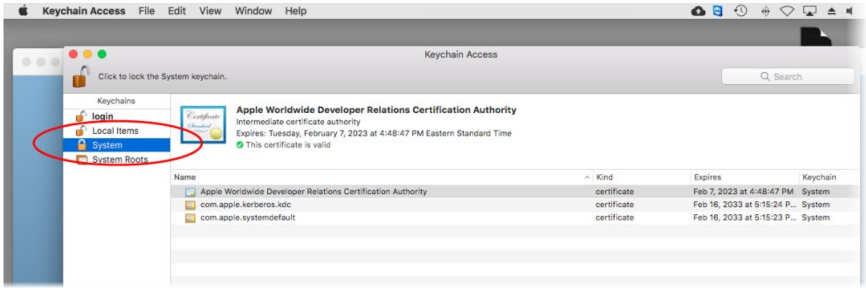
Certificates need to be installed to enable HTTPS

1. Download the root and intermediate certificates for the certificate authority.
   Download Root Certificate (root-ca.crt)
   Download Intermediate Certificate (intermediate-ca.crt)
2. Open the **Keychain Access** application from **Launchpad**.
3. Navigate to **System**.
4. Open the **File** menu.
5. Select **Import Items**.
6. Select the **RootCA** cerificate.
7. Do the same with the **IntCA** certificate.
8. Double-click on the **RootCA** in **Keychain Access**.
9. Expand the **Trust** heading.
10. Set value of **When using this certificate** field to **Always Trust**.
11. Reload the login page. If you did everything right, you should be able to login.
    If you return to this page, try restarting your browser.
    If you are still unable to login, contact your System Administrator for assistance.

Return to login page

2. Click the corresponding links to download the root and intermediate certificates for the certificate authority. Remember where you store the downloaded files.
   - Root Certificate (root-ca.crt)
   - Intermediate Certificate (intermediate-ca.crt)
3. Open 'Keychain Access'.
4. Select 'System' if not already selected.

Figure 27 Select System

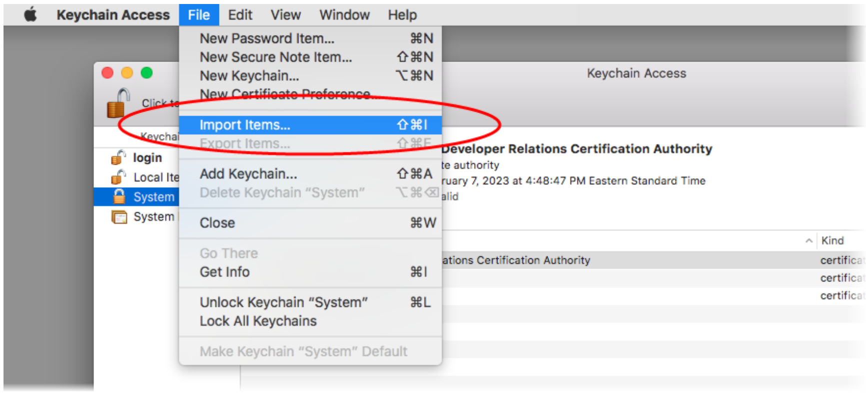

Keychain Access File Edit View Window Help
Keychain Access
Click to lock the System keychain.
Search
Keychains
login
Local Items
System
System Roots

Apple Worldwide Developer Relations Certification Authority
Intermediate certificate authority
Expires: Tuesday, February 7, 2023 at 4:48:47 PM Eastern Standard Time
This certificate is valid

Name	Kind	Expires	Keychain
Apple Worldwide Developer Relations Certification Authority	certificate	Feb 7, 2023 at 4:48:47 PM	System
com.apple.kerberos.kdc	certificate	Feb 16, 2033 at 5:15:24 P...	System
com.apple.systemdefault	certificate	Feb 16, 2033 at 5:15:23 P...	System

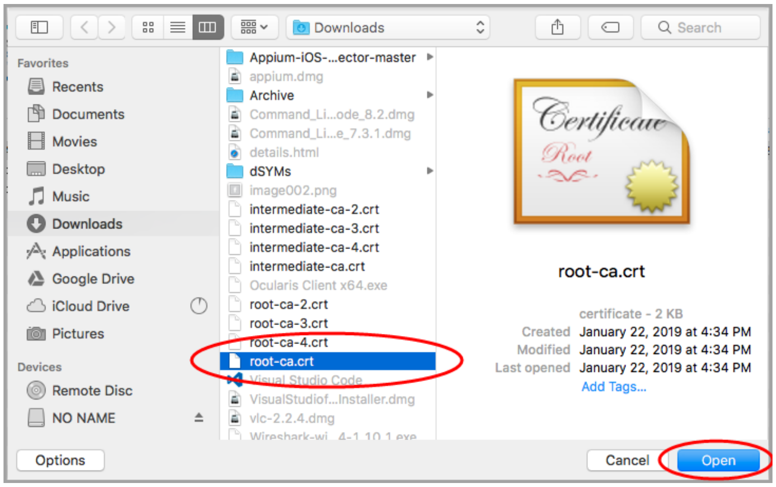
5. From the top Keychain Access bar, select the **File** menu and then select 'Import Items..."

Figure 28 Import Items...


Keychain Access File Edit View Window Help
New Password Item... ⌘N
New Secure Note Item... ⇧⌘N
New Keychain... ⌥⌘N
New Certificate Preference...
Import Items... ⇧⌘I
Export Items... ⇧⌘E
Add Keychain... ⇧⌘A
Delete Keychain "System" ⌥⌘⌫
Close ⌘W
Go There
Get Info ⌘I
Unlock Keychain "System" ⌘L
Lock All Keychains
Make Keychain "System" Default
Keychain Access
Click to
Keycha
login
Local Ite
System
System
Developer Relations Certification Authority
te authority
ruary 7, 2023 at 4:48:47 PM Eastern Standard Time
alid
Kind
ations Certification Authority
certifica
certifica
certifica

6. Select the certificate 'root-ca.crt' and click **Open**.

Figure 29 Select the certificate

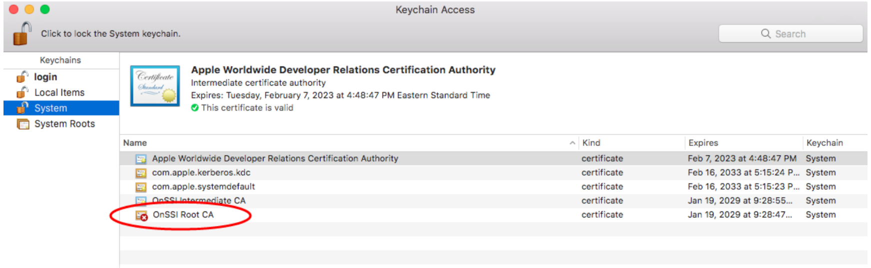


root-ca.crt
certificate - 2 KB
Created January 22, 2019 at 4:34 PM
Modified January 22, 2019 at 4:34 PM
Last opened January 22, 2019 at 4:34 PM
Add Tags...

7. If prompted, enter the password of the mac and click the **Modify Keychain** button.

8. Again, from the top Keychain Access bar, select the **File** menu and then select 'Import Items..."
9. Select the certificate 'intermediate-ca.crt' and click **Open**. If prompted, enter the password of the mac and click the **Modify Keychain** button.
10. Double-click the certificate 'root-CA.crt'.

Figure 30 Double-click the certificate

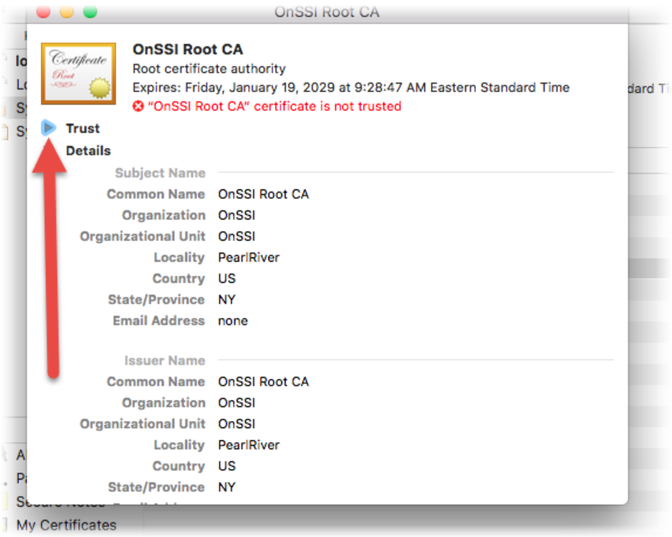


Apple Worldwide Developer Relations Certification Authority
Intermediate certificate authority
Expires: Tuesday, February 7, 2023 at 4:48:47 PM Eastern Standard Time
✓ This certificate is valid

Name	Kind	Expires	Keychain
Apple Worldwide Developer Relations Certification Authority	certificate	Feb 7, 2023 at 4:48:47 PM	System
com.apple.kerberos.kdc	certificate	Feb 16, 2033 at 5:15:24 P...	System
com.apple.systemdefault	certificate	Feb 16, 2033 at 5:15:23 P...	System
OnSSI Intermediate CA	certificate	Jan 19, 2029 at 9:28:55...	System
OnSSI Root CA	certificate	Jan 19, 2029 at 9:28:47...	System

11. Expand **Trust**.

Figure 31 Expand Trust

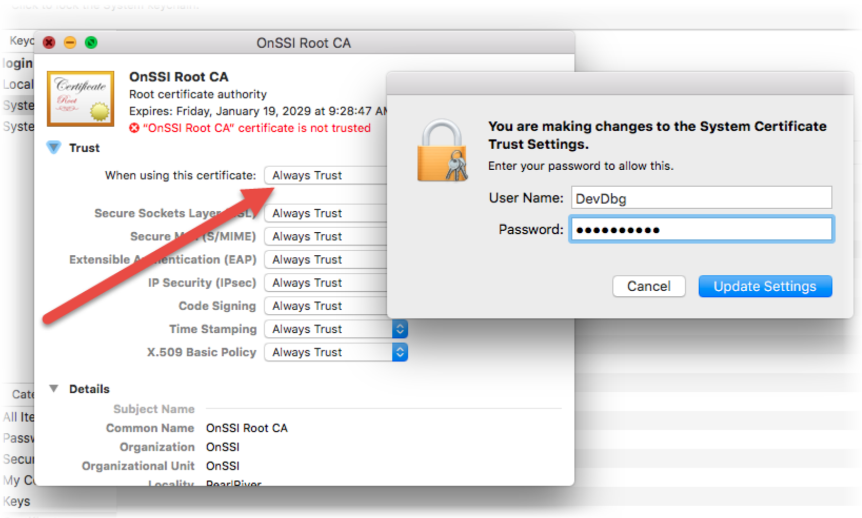


OnSSI Root CA
Root certificate authority
Expires: Friday, January 19, 2029 at 9:28:47 AM Eastern Standard Time
✗ "OnSSI Root CA" certificate is not trusted

Subject Name	
Common Name	OnSSI Root CA
Organization	OnSSI
Organizational Unit	OnSSI
Locality	PearlRiver
Country	US
State/Province	NY
Email Address	none
Issuer Name	
Common Name	OnSSI Root CA
Organization	OnSSI
Organizational Unit	OnSSI
Locality	PearlRiver
Country	US
State/Province	NY

12. Change the top item 'When using this certificate:' to **Always Trust**.
13. Close the window. You may be asked to provide the machine password. Enter it and click **Update Settings**.

Figure 32 Always Trust Root CA



OnSSI Root CA

OnSSI Root CA
Root certificate authority
Expires: Friday, January 19, 2029 at 9:28:47 AM
“OnSSI Root CA” certificate is not trusted

Trust

When using this certificate: Always Trust
Secure Sockets Layer (SSL): Always Trust
Secure Mail (S/MIME): Always Trust
Extensible Authentication (EAP): Always Trust
IP Security (IPsec): Always Trust
Code Signing: Always Trust
Time Stamping: Always Trust
X.509 Basic Policy: Always Trust

Details

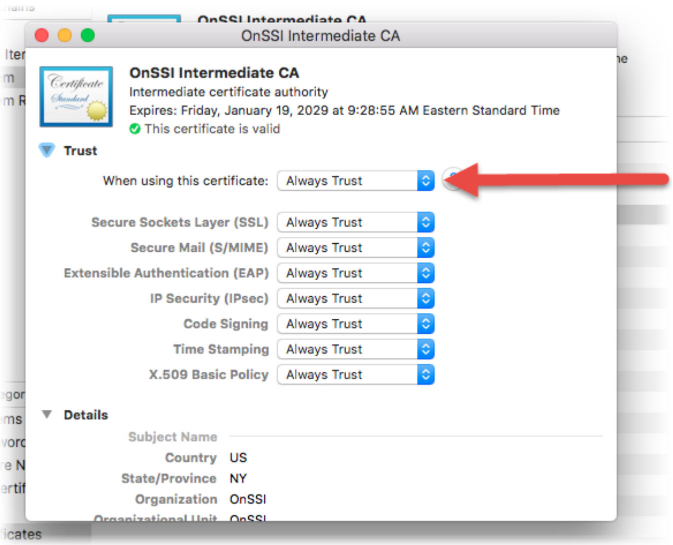
Subject Name
Common Name: OnSSI Root CA
Organization: OnSSI
Organizational Unit: OnSSI
Locality: PearlRiver

You are making changes to the System Certificate Trust Settings.
Enter your password to allow this.

User Name: DevDbg
Password: ●●●●●●●●●●●

14. Repeat for the other certificate. Double-click the 'Intermediate-CA.crt'
15. Expand **Trust**.
16. Change the top item 'When using this certificate:' to **Always Trust**.

Figure 33 Always Trust Intermediate CA



OnSSI Intermediate CA

OnSSI Intermediate CA
Intermediate certificate authority
Expires: Friday, January 19, 2029 at 9:28:55 AM Eastern Standard Time
This certificate is valid

Trust

When using this certificate: Always Trust
Secure Sockets Layer (SSL): Always Trust
Secure Mail (S/MIME): Always Trust
Extensible Authentication (EAP): Always Trust
IP Security (IPsec): Always Trust
Code Signing: Always Trust
Time Stamping: Always Trust
X.509 Basic Policy: Always Trust

Details

Subject Name
Country: US
State/Province: NY
Organization: OnSSI
Organizational Unit: OnSSI

17. Close the window. You may be asked to provide the machine password. Enter it and click **Update Settings**.
18. Now, go back to the browser and reload the login page or click ‘Return to login page’. If you did everything right, you should be able to login. If you return to this page, try restarting your browser.
    If you are still unable to login, contact your System Administrator for assistance.