# Revision History

<table>
<thead>
<tr>
<th>Revision</th>
<th>Purpose for Change</th>
<th>Author</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>GA</td>
<td>D. Jecker</td>
<td>Oct 2019</td>
</tr>
<tr>
<td>01</td>
<td>Title</td>
<td>D. Jecker</td>
<td>Oct 2019</td>
</tr>
</tbody>
</table>
## Contents

1. **About This Guide** ............................................................................................................. 1  
   1.1 Related Documentation ......................................................................................... 1  
2. **Introduction** ................................................................................................................. 2  
3. **Google Chrome** .......................................................................................................... 3  
4. **Mozilla Firefox** ......................................................................................................... 11  
5. **Microsoft Edge** ......................................................................................................... 15  
6. **Apple Safari** ............................................................................................................... 19
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

<table>
<thead>
<tr>
<th>Document Name</th>
<th>Version</th>
<th>File Type</th>
<th>Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ocularis 5.8 Release Notes</td>
<td>5.8</td>
<td>PDF</td>
<td>October 2019</td>
</tr>
<tr>
<td>Add-on Documentation</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
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

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.
5. Select the section ‘Manage certificates’.

6. Select the tab ‘Trusted Root Certification Authorities’.
7. Click **Import…** to start the Certificate Import Wizard.

8. Click **Next**.

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

12. Click **Finish**.
13. At ‘The import was successful’ pop-up, click **OK**.


**Figure 8 Completing the Import**

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.
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
20. Click **Finish**.

**Figure 12 Complete the Import Wizard**

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

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

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

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**.

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

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

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

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

8. Click **Next**.

Figure 23 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](image)

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

![Certificate warning screen](image)

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

**Figure 28 Import Items...**

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

**Figure 29 Select the certificate**

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](image)

11. Expand **Trust**.

![Figure 31 Expand Trust](image)

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**.
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**

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.