© 2019 Welch Allyn. All rights are reserved. To support the intended use of the product described in this publication, the purchaser of the product is permitted to copy this publication, for internal distribution only, from the media provided by Welch Allyn. No other use, reproduction, or distribution of this publication, or any part of it, is permitted without written permission from Welch Allyn. Welch Allyn assumes no responsibility for any injury to anyone, or for any illegal or improper use of the product, that may result from failure to use this product in accordance with the instructions, cautions, warnings, or statement of intended use published in this manual.

Software in this product is Copyright 2019 Welch Allyn or its vendors. All rights are reserved. The software is protected by United States of America copyright laws and international treaty provisions applicable worldwide. Under such laws, the licensee is entitled to use the copy of the software incorporated with this instrument as intended in the operation of the product in which it is embedded. The software may not be copied, decompiled, reverse-engineered, disassembled, or otherwise reduced to human-perceivable form. This is not a sale of the software or any copy of the software; all right, title, and ownership of the software remain with Welch Allyn or its vendors.

This product may contain software known as “free” or “open source” software (FOSS). Welch Allyn uses and supports the use of FOSS. We believe that FOSS makes our products more robust and secure, and gives us and our customers greater flexibility. To learn more about FOSS that may be used in this product, please visit our FOSS website at http://www.welchallyn.com/opensource. Where required, a copy of FOSS source code is available on our FOSS website.


Welch Allyn, Inc.
4341 State Street Road
Skaneateles Falls, NY 13153 USA
www.welchallyn.com

Revision date: 2019-04
Contents

About this guide .............................................................................................................. 1
  RetinaVue architecture for USB connected camera workflow ................................. 2
  RetinaVue architecture for Wi-Fi connected camera workflow .............................. 3
  RetinaVue EMR connected workflow ....................................................................... 4
  RetinaVue EMR connectivity project overview ....................................................... 4
  Log in to the RetinaVue Network EMR Deployment Portal ..................................... 4

Features of the RetinaVue Network EMR Deployment Portal ............................... 5
  Prerequisites ............................................................................................................. 6

Choose an EMR security configuration and method of receiving exam results ................................................................................................................................. 7
  Configure EMR connection properties ..................................................................... 8
  Step 1 — set up EMR ............................................................................................. 8
  Step 2 — set up Clinics ......................................................................................... 9
  Select one of following sections ............................................................................. 9
  VPN secure communication — results server ..................................................... 11
  VPN secure communication — results client ....................................................... 12
  Certificates secure communication — results server .......................................... 13
  Certificates secure communication — results client .......................................... 14

Allscripts TouchWorks and Professional EHR integrations ................................ 15
  Allscripts RetinaVue configuration ................................................................. 16

Athenahealth integrations .................................................................................. 19
  Athenahealth RetinaVue configuration .............................................................. 19

Update Deployment ......................................................................................... 21

Troubleshooting ............................................................................................... 23

Appendix ............................................................................................................ 27
  Sandbox servers ................................................................................................. 27
  Production servers .............................................................................................. 27
  Configure the RetinaVue Client Application to connect to the RetinaVue Sandbox Server ......................................................................................................................... 27
  Certificate export and installation for server and client authentication ................... 31
About this guide

This EMR Deployment guide is for RetinaVue Network system Administrators or other IT professionals involved in:

- setting up the EMR Server Application to connect with the RetinaVue Server
- configuring the RetinaVue Network to connect to an EMR (or similar system)
- managing a RetinaVue Network EMR connection (or similar system)
- troubleshooting a RetinaVue Network EMR deployment

Related documents

When using this manual, refer to the following:

- Welch Allyn RetinaVue HL7 Interface Design Specification
- Welch Allyn RetinaVue™ 100 Imager — Directions for use
- Welch Allyn RetinaVue™ Network — Network guide
- RetinaVue Network — Software installation instructions (USB only connected camera workflow)
- Welch Allyn RetinaVue website: www.RetinaVue.com

For information on clinical use or using the device that connects to the RetinaVue Network system, consult the Directions for use that came with the device.
RetinaVue architecture for USB connected camera workflow

The RetinaVue architecture diagram shows the relationship between the RetinaVue Server, the RetinaVue Client Application (when using the USB connected camera workflow), the EMR Server Application, and the over-read Physician’s Portal.

The RetinaVue architecture diagram also depicts the 10 interactions of the workflow:

1. Provider enters an order in the EMR Client Application.
2. EMR Client Application sends order to the EMR Server Application.
3. EMR Server Application sends an HL7 compliant order, or multiple orders, (via HTTPS TLS1.2) to the RetinaVue Server.
4. RetinaVue Server sends an order, or multiple orders, to the RetinaVue Client Application (via HTTPS TLS1.2).
5. An order, or multiple orders, appear as a patient list in the camera.
6. Clinician takes an eye exam and sends the exam to the RetinaVue Client Application.
7. Exam data is sent from the camera to the RetinaVue Client Application.
8. Exam data is sent (via HTTPS TLS1.2) from the RetinaVue Client Application to the RetinaVue Server.
9. A board-certified ophthalmologist performs an over-read through the Physician’s Portal.
10. Test results (report or images) are sent to the EMR Server Application (via HTTPS TLS1.2).
RetinaVue architecture for Wi-Fi connected camera workflow

The RetinaVue architecture diagram shows the relationship between the RetinaVue Server (when using the Wi-Fi connected camera workflow), the EMR Server Application, and the over-read Physician’s Portal.

The RetinaVue architecture diagram also depicts the 8 interactions of the Wi-Fi workflow:

1. Provider enters an order in the EMR Client Application.
2. The EMR Client Application sends an HL7 compliant order, or multiple orders, (via HTTPS TLS1.2) to the EMR Server Application.
3. The EMR Server Application sends the order to the RetinaVue Server.
4. RetinaVue Server sends an order (via HTTPS TLS1.2), or multiple orders, as a patient list to the camera.
5. Clinician takes an eye exam with the camera.
6. Exam data is sent from the camera (via HTTPS TLS1.2) to the RetinaVue Server.
7. A board-certified ophthalmologist performs an over-read through the Physician’s Portal.
8. Test results (report or images) are sent to the EMR Server Application (via HTTPS TLS1.2).
RetinaVue EMR connected workflow

The RetinaVue EMR Connected Workflow diagram shows the interaction between the referring provider, the clinician, and the board-certified ophthalmologist (specialist) working in an EMR-connected environment.

RetinaVue EMR connectivity project overview

The seven phases of connecting to the RetinaVue Network include:

1. completing the pre-sales activities
2. completing the RetinaVue connectivity configuration
3. completing the interface development
4. confirming the workflow
5. testing
6. training
7. moving to a production server to go live

Log in to the RetinaVue Network EMR Deployment Portal

1. Use a web browser to navigate to the Welch Allyn RetinaVue Network EMR Deployment Portal at: https://retinavue-emr.net.
2. Enter your User Name and Password and click Log In. The RetinaVue Network Company Information screen appears.
Features of the RetinaVue Network EMR Deployment Portal

The following features are available on the RetinaVue Network EMR Deployment Portal:

- Company information overview
- RetinaVue to EMR connectivity configuration
- EMR clinic mapping configuration
- Certificate generation
- Message transaction viewing
- Post configuration checklist to verify proper operation
- Deployment and certificate status
- Access to interface and deployment portal documentation
- Updating EMR connectivity deployments

Deployment and Certificate status

- Grey - information is still required and certificate signing requests need to be uploaded
- Red - waiting for certificates to be signed
- Yellow - certificates are ready (signed) and deployment is ready to be enabled once the appropriate certificates are uploaded
- Green - deployment is enabled and certificates are deployed

Transactions (only available for completed deployments)

- Search for Transaction Orders
- Search for Transaction Results

Checklists (only available for completed deployments)

- View a Created Checklist
- Create a Checklist
Prerequisites

All integrations

- The customer account and clinics must be set up in the RetinaVue Network.
- If your organization requires a security questionnaire for RetinaVue solutions connecting to the EMR, that questionnaire must be completed before the EMR deployment starts.

HL7 Integrations (Epic, NextGen, etc.)

- Establish an outgoing port to send orders to the RetinaVue Network.
- If VPN is being used, the VPN connection needs to be set up prior to connecting RetinaVue to the EMR.

Allscripts

- Work with the Welch Allyn project manager to license the RetinaVue Network EMR Interface application for the Allscripts Unity server.
- The EHR client must be updated to create orders for RetinaVue fundus exams. This includes configuration of the additional order questions for TouchWorks integrations.

Athenahealth

- Work with the Welch Allyn Project Manager and Athenahealth to grant API key access to your practice’s table space.
- Work with the Welch Allyn Project Manager and Athenahealth to enable the RetinaVue work flow for your practice.

eClinicalWorks

- Work with the Welch Allyn Project Manager and eCW to enable connectivity between the eCW Hub and RetinaVue.

If you are configuring an Allscripts Unity integration, please go to the Allscripts RetinaVue configuration instructions.

If you are configuring an Athenahealth integration, please go to the Athenahealth RetinaVue configuration instructions.

If you are configuring an HL7 integration (Epic, NextGen, etc.), please continue with the following instructions.

**Note** This includes eClinicalWorks integrations which always use the VPN/Results Server configuration.
Choose an EMR security configuration and method of receiving exam results

The following definitions describe the security methods and the roles that the EMR will play in the connectivity. Please use these definitions when deciding on your connectivity configuration.

- **VPN Security Configuration** - The EMR establishes a VPN connection with the Welch Allyn RetinaVue Server.
- **Certificates Security Configuration** - The EMR uses certificates issued by Welch Allyn.
- **Results Server** - The EMR is acting as a Server and listening for results.
- **Results Client** - The EMR is acting as a Client and requesting results.

**Note** Before proceeding, confirm that all the *Prerequisites for secure communication* have been fulfilled and then determine which one of the security configurations and methods of receiving exam results best suits your EMR needs. Choose from the following 4 options:

- Certificates secure communication — results server
- Certificates secure communication — results client
- VPN secure communication — results server
- VPN secure communication — results client

Follow these common steps that apply to each of the EMR configurations that connect with the RetinaVue Server:

<table>
<thead>
<tr>
<th>Task</th>
<th>For instructions or more information</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Set up the EMR</td>
<td>“Configure EMR connection properties”</td>
</tr>
<tr>
<td>a. Select the Security Configuration</td>
<td>“Step 1 — set up EMR”</td>
</tr>
<tr>
<td>b. Select the Exam Results Configuration</td>
<td></td>
</tr>
<tr>
<td>c. Enter the Send Orders Port Number</td>
<td></td>
</tr>
<tr>
<td>d. Enter the EMR IP Address.</td>
<td></td>
</tr>
<tr>
<td>e. Enter the Receive Results Port Number.</td>
<td></td>
</tr>
<tr>
<td>f. Enter the Receive Results Polling Interval (minutes)</td>
<td></td>
</tr>
<tr>
<td>2. Set up the Clinics</td>
<td>“Step 2 — set up Clinics”</td>
</tr>
</tbody>
</table>
Configure EMR connection properties

1. From the RetinaVue Network Company Information screen, use the drop-down menu to select the EMR type.

2. Use the drop-down menu to select the Security Configuration. Select the VPN or Certificates option.

3. Use the drop-down menu to select the Exam Results Configuration. Select the Server or Client option.

4. When you have completed the EMR configuration information, the Step 1. EMR screen appears.

Step 1 — set up EMR

This section describes:

- adding or updating contact email
- specifying IP Address and port information

1. Enter at least one contact e-mail address. For multiple email addresses, separate with a semicolon (;).

   **Note** The Welch Allyn RetinaVue Network Server IP Address is preset.

2. Enter the Send Orders Port Number.

3. Enter the EMR IP Address.

   **Note** This is the location that results will be sent to. Not required for the Results Client configurations.

4. Enter the Receive Results Port Number.

   **Note** The Send Orders and the Receive Results Ports are the same for the Results Client configurations.
5. Enter the Receive Results Polling Interval (minutes)

   **Note**  RetinaVue Network periodically sends results to the EMR based on this setting. Not required for the Results Client configurations.

6. When you have completed the EMR information, click **Next**. The **Step 2. Clinics** screen appears.

### Step 2 — set up Clinics

When orders are submitted to the RetinaVue Network for each clinic, an EMR Clinic ID needs to be present in the order.

1. Review that all clinic information is included in the **Step 2. Clinics** screen and begin entering your EMR ID for any new clinics.

2. Enter the EMR Clinic ID for at least one clinic.

3. When you have completed the EMR Clinic ID for at least one clinic, click **Next**.

**STOP**

Select **one** of following sections

### Choose the security configuration and method of receiving exam results

Select one of the security configurations and methods of receiving exam results from the following table that best matches your EMR needs and follow the instructions in the applicable section for your EMR. The table summarizes the Certificates or VPN options and the Server or Client method of receiving exam results.

<table>
<thead>
<tr>
<th>Security Configuration</th>
<th>Method of Receiving Exam Results</th>
<th>Instruction Section</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificates</td>
<td>Server</td>
<td>&quot;Certificates secure communication — results server&quot;</td>
</tr>
<tr>
<td>Security Configuration</td>
<td>Method of Receiving Exam Results</td>
<td>Instruction Section</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td>Certificates</td>
<td>Client</td>
<td>“Certificates secure communication — results client”</td>
</tr>
<tr>
<td>VPN</td>
<td>Server</td>
<td>“VPN secure communication — results server”</td>
</tr>
<tr>
<td>VPN</td>
<td>Client</td>
<td>“VPN secure communication — results client”</td>
</tr>
</tbody>
</table>
VPN secure communication — results server

**VPN Security Configuration** - The EMR establishes a VPN connection with the Welch Allyn RetinaVue Server.

**Results Server** - The EMR is acting as a Server and listening for results.

**Step 3 — Submit Certificate Signing Requests (CSRs)**

The RetinaVue Network requires secure communication using TLS 1.2 with all connecting applications, which includes the RetinaVue Network EMR Interface. One certificate will be created and used internally within RetinaVue. Follow the instructions on the EMR Deployment Portal to generate and submit a certificate signing request.

**Step 4 — Complete the Certificate Signing Requests (CSRs)**

**Note**

The newly uploaded certificate signing requests typically take a few minutes to be signed by the certificate authority. When the certificates are ready, the certificate status will only change by clicking Refresh.

Click **Refresh** to change the certificate status from red to yellow.

**Step 5 — Accept and Finish**

Follow the instructions on the EMR Deployment Portal to finish your set up. When complete, the resulting certificate will be used by the RetinaVue Network EMR Interface to secure all communication with the RetinaVue Network. This certificate is not used by the EMR and will be automatically installed within the RetinaVue Network EMR interface.
VPN secure communication — results client

VPN Security Configuration - The EMR establishes a VPN connection with the Welch Allyn RetinaVue Server.

Results Client - The EMR is acting as a Client and requesting results.

Step 3 — Submit Certificate Signing Requests (CSRs)

The RetinaVue Network requires secure communication using TLS 1.2 with all connecting applications, which includes the RetinaVue Network EMR Interface. Follow the instructions on the EMR Deployment Portal to generate and submit a certificate signing request. One certificate will be created and used internally within RetinaVue.

Step 4 — Complete the Certificate Signing Requests (CSRs)

Note The newly uploaded certificate signing requests typically take a few minutes to be signed by the certificate authority. When the certificates are ready, the certificate status will only change by clicking Refresh.

Click Refresh to change the certificate status from red to yellow.

Step 5 — Accept and Finish

Follow the instructions on the EMR Deployment Portal to finish your set up. When complete, the resulting certificate will be used by the RetinaVue Network EMR Interface to secure all communication with the RetinaVue Network. This certificate is not used by the EMR and will be automatically installed within the RetinaVue Network EMR interface.
Certificates secure communication — results server

**Certificates Security Configuration** - The EMR uses certificates issued by Welch Allyn.

**Results Server** - The EMR is acting as a Server and listening for results.

**Step 3 — Submit Certificate Signing Requests (CSRs)**

The RetinaVue Network EMR Interface and the RetinaVue Network require secure communication using TLS 1.2 with all connecting applications. Follow the instructions on the EMR Deployment Portal to generate and submit certificate signing requests.

**Step 4 — Complete the Certificate Signing Requests (CSRs)**

*Note* The newly uploaded certificate signing requests typically take a few minutes to be signed by the certificate authority. When the certificates are ready, the certificate status will only change by clicking Refresh.

Click **Refresh** to change the certificate status from red to yellow.

**Step 5 — Accept and Finish**

Follow the instructions on the EMR Deployment Portal to finish your set up. When complete, the resulting certificates will be used by the EMR to secure communication with the RetinaVue Network EMR Interface and by the RetinaVue Network EMR Interface to secure communication with the RetinaVue Network. See appendix - "Certificate export and installation for server and client authentication" for instructions on how to obtain the completed certificates.
Certificates secure communication — results client

Certificates Security Configuration - The EMR uses certificates issued by Welch Allyn.
Results Client - The EMR is acting as a Client and requesting results.

Step 3 — Submit Certificate Signing Requests (CSRs)

The RetinaVue Network EMR Interface and the RetinaVue Network require secure communication using TLS 1.2 with all connecting applications. Follow the instructions on the EMR Deployment Portal to generate and submit certificate signing requests.

Step 4 — Complete the Certificate Signing Requests (CSRs)

Note The newly uploaded certificate signing requests typically take a few minutes to be signed by the certificate authority. When the certificates are ready, the certificate status will only change by clicking Refresh.

Click Refresh to change the certificate status from red to yellow.

Step 5 — Accept and Finish

Follow the instructions on the EMR Deployment Portal to finish your set up. When complete, the resulting certificates will be used by the EMR to secure communication with the RetinaVue Network EMR Interface and by the RetinaVue Network EMR Interface to secure communication with the RetinaVue Network. See appendix - "Certificate export and installation for server and client authentication" for instructions on how to obtain the completed certificates.
Allscripts TouchWorks and Professional EHR integrations

RetinaVue Allscripts connectivity overview

The following diagram shows the components involved, workflow steps (in green), and the RetinaVue Allscripts EHR Connectivity points (in yellow):

Connected workflow

After successfully configured, an Allscripts EHR client (Touchworks and Professional) creates orders for a RetinaVue fundus exam. Once a fundus exam is complete the results are returned to the Unity server and are available in the EHR client.

The connected workflow is summarized in the following steps:
1. The RetinaVue Allscripts EMR Service uses the Unity API to detect an open fundus exam.
2. A RetinaVue order is created for the exam and sent to the RetinaVue Network.
3. The RetinaVue Client/Camera can now access the order and perform the fundus exam.
4. The fundus exam results are over-read and diagnosis data and report are generated.
5. The RetinaVue Allscripts EMR Service sees that the diagnosis and a report is available.
6. The results are returned to the Unity server, and are available in the EHR client.

For instructions about connecting RetinaVue to Allscripts EHRs please follow the Allscripts RetinaVue configuration instructions below.

**Allscripts RetinaVue configuration**

Configure the EMR interface between an Allscripts EMR and RetinaVue by using the Welch Allyn EMR Deployment Portal and by following the steps below.

**Note** Before proceeding, confirm that the Prerequisites have been fulfilled. The Unity service must be licensed before completing the steps.

**Step 1 — set up EMR**

1. Select Allscripts as the EMR type.
2. Enter at least one contact e-mail address. For multiple email addresses, separate with a semicolon (;).
3. Enter your Allscripts URL, User name, Password, Ubiquity Id (Optional.) This configuration information will be used to access the Unity Server. These credentials must be able to read and update orders and be able to store exam results.
4. Click **Validate Configuration Items** to discover potential Allscripts server configuration issues.
5. When you have completed the EMR information, click **Next**. The **Step 2. Clinics** screen appears.

**Step 2 — set up Clinics**

Each RetinaVue Network Clinic must be mapped to a unique Allscripts Site for Touchworks EHR.

Follow the instructions on the EMR Deployment Portal to specify Allscripts configuration information for each RetinaVue Network clinic.

**Step 3 — Submit Certificate Signing Requests (CSRs)**

The RetinaVue Network requires secure communication using TLS 1.2 with all connecting applications, which includes the RetinaVue Network EMR Interface. Follow the instructions on the EMR Deployment Portal to generate and submit a certificate signing request. One certificate will be created and used internally within RetinaVue.
Step 4 — Complete the Certificate Signing Requests (CSRs)

**Note** The newly uploaded certificate signing requests typically take a few minutes to be signed by the certificate authority. When the certificates are ready, the certificate status will only change by clicking Refresh.

Click **Refresh** to change the certificate status from red to yellow.

Step 5 — Accept and Finish

Follow the instructions on the EMR Deployment Portal to finish your set up. When complete, the resulting certificate will be used by the RetinaVue Network EMR Interface to secure all communication with the RetinaVue Network. This certificate is not used by the EMR. By completing this step, the certificate has been installed within the RetinaVue Network.
Athenahealth integrations

Athenahealth RetinaVue configuration

Configure the EMR interface between your Athenahealth Practice EMR and RetinaVue by using the Welch Allyn EMR Deployment Portal and by following the steps below.

**Note** Before proceeding, confirm that the Prerequisites have been fulfilled. API key Access to your practice’s table space must be granted before completing these steps.

**Step 1 — set up EMR**

1. Select Athenahealth as the EMR type.
2. Enter at least one contact e-mail address. For multiple email addresses, separate with a semicolon (;).
3. Provide your Athenahealth Practice Id.
4. When you have completed the EMR information, click **Next**. The **Step 2. Clinics screen appears**.

**Step 2 — set up Clinics**

At least one RetinaVue Network Clinic must be mapped to an Athenahealth Department.

Follow the instructions on the EMR Deployment Portal to map your RetinaVue Network Clinics to your Athenahealth Departments.

**Step 3 — Submit Certificate Signing Requests (CSRs)**

The RetinaVue Network requires secure communication using TLS 1.2 with all connecting applications, which includes the RetinaVue Network EMR Interface. Follow the instructions on the EMR Deployment Portal to generate and submit a certificate signing request. One certificate will be created and used internally within RetinaVue.
Step 4 — Complete the Certificate Signing Requests (CSRs)

Note  The newly uploaded certificate signing requests typically take a few minutes to be signed by the certificate authority. When the certificates are ready, the certificate status will only change by clicking Refresh.

Click Refresh to change the certificate status from red to yellow.

Step 5 — Accept and Finish

Follow the instructions on the EMR Deployment Portal to finish your set up. When complete, the resulting certificate will be used by the RetinaVue Network EMR Interface to secure all communication with the RetinaVue Network. This certificate is not used by the EMR. By completing this step, the certificate has been installed within the RetinaVue Network.
Update Deployment

Returning RetinaVue company administrators with administrative rights may need to:

- update EMR Clinic ID mapping
- update EMR port numbers
- update certificates or refresh the certificate status
- delete and create a new deployment after a server change

**Note**  
New client and server certificates need to be signed by a certificate authority. This process typically takes a few minutes. Click the refresh button to refresh the RetinaVue Network Company Information screen.

From the RetinaVue Network Company Information screen, click **Refresh** to refresh the RetinaVue Network Company Information screen. The status of the deployment is indicated by the grey, red, yellow, or green status indicator icon located in the upper-right corner of the RetinaVue Network Company Information screen.

**Note**  
When the status turns green, the deployment is complete.

**Update Clinic IDs**

1. Enter the revised EMR ID for a clinic.

2. When you have completed the clinic EMR ID change, click **Next**.

**Update Certificates (Optional)**

Follow the steps in the Client and Server Certificate Signing Requests (CSR) topic to download and update the Client and Server certificates.

**Delete Deployment (Optional)**
1. Click **Delete Deployment**.
2. At the dialogue box "Are you sure you want to delete the deployment?", click **OK**. The *RetinaVue Network Company Information* screen appears.
Troubleshooting

This section presents a table of problem descriptions, possible causes, and suggested actions that can resolve the issue.

<table>
<thead>
<tr>
<th>Symptom</th>
<th>Possible cause</th>
<th>Suggested action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unable to send HL7 messages from the EMR Server Application to the RetinaVue Network</td>
<td>The EMR does not have internet connectivity</td>
<td>Establish internet connectivity for the EMR.</td>
</tr>
<tr>
<td></td>
<td>The RetinaVue EMR Server Application is not listening on the correct port</td>
<td>Use the EMR Deployment Portal to verify that the Orders port is configured correctly and correct if needed. Redeploy integration.</td>
</tr>
<tr>
<td></td>
<td>The RetinaVue EMR Server is not targeting the correct RetinaVue EMR Server Application IP Address/Port</td>
<td>Use the EMR Deployment Portal to verify that the Orders port is configured correctly and correct if needed. Redeploy integration.</td>
</tr>
<tr>
<td></td>
<td>The RetinaVue EMR Server Application is down</td>
<td>Contact Welch Allyn technical support. Ensure the VPN is established and running. Use the EMR Deployment Portal to verify the certificates are deployed correctly. Verify the certificates created in the RetinaVue EMR Deployment Portal have been deployed in the EMR Server. If needed, create new certificates and follow the instructions to redeploy certificates on the RetinaVue Server and the EMR Server Application.</td>
</tr>
<tr>
<td></td>
<td>VPN security configuration: The VPN has not been established or is down. Certificates security configuration: The self signed client certificate is not being used to send HL7 messages.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>The EMR is not trusting the Welch Allyn EMR Server’s certificate.</td>
<td>Obtain and add Welch Allyn EMR Server’s certificate root to the EMR’s trusted certificate store.</td>
</tr>
<tr>
<td></td>
<td>The HL7 message is invalid</td>
<td>Use the RetinaVue Deployment Portal to check the RetinaVue EMR Server Application message logs for more information.</td>
</tr>
<tr>
<td>The EMR received a NACK from the RetinaVue EMR Server Application</td>
<td>The EMR is not using the correct Client certificate</td>
<td>Use the EMR Deployment Portal to verify the certificates are deployed correctly. Verify the certificates created in the RetinaVue EMR Deployment Portal have been deployed in the EMR Server. If needed, create new certificates and follow the instructions to redeploy certificates on the RetinaVue Server and the EMR Server Application.</td>
</tr>
<tr>
<td>Symptom</td>
<td>Possible cause</td>
<td>Suggested action</td>
</tr>
<tr>
<td>------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------</td>
<td>------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>The EMR Server Application is not using correct Client certificate</td>
<td>Use the EMR Deployment Portal to verify the certificates are deployed correctly. Verify the certificates created in the RetinaVue EMR Deployment Portal have been deployed in the EMR Server Application. If needed, create new certificates and follow the instructions to redeploy certificates on the RetinaVue server and the EMR server.</td>
<td></td>
</tr>
<tr>
<td>The site is unable to activate the RetinaVue Client Application</td>
<td>See the topic Install the RetinaVue™ Network software in the Welch Allyn RetinaVue™ Network — Network guide.</td>
<td></td>
</tr>
<tr>
<td>The RetinaVue Client Application is not showing pending exams</td>
<td>The site does not have internet connectivity available for the RetinaVue Client Application.</td>
<td>Establish internet connectivity.</td>
</tr>
<tr>
<td>The RetinaVue Client Application is not configured correctly to connect to the RetinaVue Server</td>
<td>• In the test environment:</td>
<td>• See the topic Configure the RetinaVue Client Application to connect to the RetinaVue Sandbox Server in the appendix.</td>
</tr>
<tr>
<td></td>
<td>• In the production environment:</td>
<td>• See the topic Step 2 — set up Clinics in the section Configure the EMR information.</td>
</tr>
<tr>
<td></td>
<td>• In the production environment:</td>
<td>• See the topic Finding exams topic in the Troubleshooting section of the Network Guide.</td>
</tr>
<tr>
<td>The RetinaVue Server is down</td>
<td>Contact Welch Allyn technical support.</td>
<td></td>
</tr>
<tr>
<td>The site IT infrastructure is blocking access to the RetinaVue Server</td>
<td>Ensure that the RetinaVue Server is accessible. ([Use port number 443.)</td>
<td></td>
</tr>
<tr>
<td>The camera is not connected to the RetinaVue Client Application PC</td>
<td>Connect the camera to the RetinaVue Client Application PC.</td>
<td></td>
</tr>
<tr>
<td>The RetinaVue Client Application is not recognizing the connected camera</td>
<td>Ensure that the camera is powered on and not in sleep mode.</td>
<td></td>
</tr>
<tr>
<td>The camera is not docked correctly</td>
<td>Ensure that the camera is docked correctly such that the communication pins are securely aligned.</td>
<td></td>
</tr>
<tr>
<td>The RetinaVue Client Application is not configured for the camera being used Wireless Camera: The wireless camera is not activated against the correct clinic.</td>
<td>See the View or change the Camera Settings topic in the Network Guide. See the RetinaVue Network Troubleshooting.</td>
<td></td>
</tr>
<tr>
<td>The site’s RetinaVue Client Application pending exams</td>
<td>The camera is not connected to the RetinaVue Client Application PC.</td>
<td>Connect the camera to the RetinaVue Client Application PC.</td>
</tr>
<tr>
<td>Symptom</td>
<td>Possible cause</td>
<td>Suggested action</td>
</tr>
<tr>
<td>--------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td>-----------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>The list is not being updated with completed exams</td>
<td>The RetinaVue Client Application is not recognizing a connected camera</td>
<td>Ensure that the camera is powered on and not in sleep mode.</td>
</tr>
<tr>
<td></td>
<td>The camera is not docked correctly</td>
<td>Ensure that the camera is docked correctly such that the communication pins are securely aligned.</td>
</tr>
<tr>
<td></td>
<td>The RetinaVue Client Application is not configured for the camera being used</td>
<td>See the View or change the Camera Settings topic in the Network Guide.</td>
</tr>
<tr>
<td>Unable to submit an exam for over-read</td>
<td>The site does not have internet connectivity</td>
<td>Establish internet connectivity.</td>
</tr>
<tr>
<td>The site IT infrastructure is blocking access from the RetinaVue Client Application to the RetinaVue Server</td>
<td></td>
<td>Ensure that the RetinaVue Server is accessible. (Use port 443.)</td>
</tr>
<tr>
<td>The RetinaVue Server is down</td>
<td></td>
<td>Contact Welch Allyn technical support.</td>
</tr>
<tr>
<td>The RetinaVue EMR Server Application has not polled for results since the over-read result has been completed</td>
<td></td>
<td>Wait for the polling to occur. (Polling occurs every 20 minutes.)</td>
</tr>
<tr>
<td>The RetinaVue EMR Server Application is down</td>
<td></td>
<td>Contact Welch Allyn technical support.</td>
</tr>
<tr>
<td>The EMR Server is not targeting the correct RetinaVue EMR Server Application IP Address/Port</td>
<td>Use the EMR Deployment Portal to verify the correct IP/Ports are being used. If needed, update the deployment. Redeploy integration.</td>
<td></td>
</tr>
<tr>
<td>Site is not listening on the correct port</td>
<td>Update the EMR configuration to listen for completed results on the correct port.</td>
<td></td>
</tr>
<tr>
<td>The EMR is unable to receive results from the RetinaVue EMR Server Application</td>
<td>The EMR does not have internet connectivity</td>
<td>Contact Welch Allyn technical support.</td>
</tr>
<tr>
<td></td>
<td>VPN security configuration: The VPN has not been established or is down.</td>
<td>Use the EMR Deployment Portal to verify the certificates are deployed correctly. Verify the certificates created in the RetinaVue EMR Deployment Portal have been deployed in the EMR Server. If needed, create new certificates and follow the instructions to redeploy certificates on the RetinaVue Server and the EMR Server Application.</td>
</tr>
<tr>
<td></td>
<td>Certificates security configuration: The server certificate is not being used to receive results.</td>
<td></td>
</tr>
<tr>
<td>The RetinaVue EMR Server Application received a NACK from the EMR upon sending a result</td>
<td>Result is invalid</td>
<td>Using the EMR Deployment Portal, check the EMR Server Application logs for more information. The result will continue to be sent every 20 minutes until the issue is resolved.</td>
</tr>
<tr>
<td>The deployment status remains red</td>
<td>The deployment has not completed</td>
<td>Follow the deployment configuration steps to ensure that the status change from red to green. Additionally, click Refresh to change the certificate status from red to yellow. (When the certificates are ready, the certificate status will only change by clicking Refresh.)</td>
</tr>
<tr>
<td>Symptom</td>
<td>Possible cause</td>
<td>Suggested action</td>
</tr>
<tr>
<td>---------</td>
<td>---------------</td>
<td>-----------------</td>
</tr>
</tbody>
</table>

**Note**

The newly uploaded certificate signing requests typically take a few minutes to be signed by the certificate authority.
Appendix

Sandbox servers

This section provides the links to the RetinaVue Network Customer Portal and EMR Deployment Sandbox Servers.

The Customer Portal (RetinaVue Network Sandbox Server) address is:

The EMR Deployment Portal (RetinaVue Network Sandbox Server) address is:

Production servers

This section provides the links to the RetinaVue Network Customer Portal and EMR Deployment Production Servers.

The Customer Portal (RetinaVue Network Production Server) address is:

The EMR Deployment Portal (RetinaVue Network Production Server) address is:
https://retinavue-emr.net

Configure the RetinaVue Client Application to connect to the RetinaVue Sandbox Server

These instructions explain how to connect to a test server to check the complete process of sending orders and receiving results.

Connect to the RetinaVue Sandbox Server

Log in to the RetinaVue Network Customer Portal Sandbox Server using the User Name and Password that you entered during the initial account set up. (For additional information, see the topics: Set up process and First time set up of the company in the Network Guide.)

Install and configure the latest version of the RetinaVue Network software application to connect to the Sandbox Server.
b. Log in with your User Name and Password credentials that you entered during the initial account set up.
c. Click Download.
d. Click RetinaVue Network Software Download and the save the .exe file to the desktop.

e. After the RetinaVueNetworkSetup.exe file finishes downloading, open Windows Explorer to locate the RetinaVueNetworkSetup.exe file. Right-click on the executable file and select Run as administrator.
f. Click Install.
g. In the RetinaVue Network window, click Exit.
h. Using Windows Explorer®, navigate to C:\RetinaVue Network\Client.
i. Make a backup of the RetinaVue Network.exe.config file.
j. Right-click on the RetinaVue Network.exe.config file -> Open With -> Notepad.
k. Update the <configuration><system.serviceModel><client><endpoint

from: https://www.reтинавю.net/RN_WebService/RN_WebSrvc.svc
to: https://sandbox.retinavue.net/RN_WebService/RN_WebSrvc.svc
l. Close and save the RetinaVue Network.exe.config file.

m. On the desktop, double click the RetinaVue Network shortcut that was created during the installation process.

n. Enter your RetinaVue Network Software Activation Key from the RetinaVue Network Customer Portal Download page into the RetinaVue Network software and click Next. (See example screens from the Customer Portal Download page and the RetinaVue Network software.)
o. Select the camera from the drop-down menu.

p. Select your clinic where you will be using the software by highlighting the clinic.

q. Select the state where the exams will take place.

   **Note** If the exams take place in the same state as the clinic, click **Yes** and proceed to the next step. If the exams do not take place in the same state as the clinic, click **No** and use the drop-down menu to choose your state.

r. Click **Next** to restart the software with the new settings. Click **OK**.
Certificate export and installation for server and client authentication

RetinaVue Network EMR Deployment certificate export and usage instructions

These instructions explain how to export the certificates that were generated during the EMR Deployment certificate creation process for use with EMR connectivity applications.

Overview

Once the certificates required for connectivity with the RetinaVue Network have been created they will likely need to be moved to their point of use. The location where each certificate will be used will depend on the application that is used to connect to the RetinaVue Network. These instructions are provided as a convenience with the intent to guide the exporting of certificates created through the EMR Deployment process.

Access the Certificate Snap-in within the Microsoft Management Console

1. From the Windows® taskbar, click Run ..., type MMC, and then click OK to launch the Microsoft Management Console.

2. From the Microsoft Management Console, select File -> Add/Remove Snap-in....

3. From the Available Snap-ins menu, select Certificates, and click Add >.
4. From the **Certificates Snap-in** menu, select **Computer Account** and click **Next >**.

5. From the **Select Computer** menu, choose **Local computer: (the computer this console is running on)** and then click **Finish**.

6. From the **Available Snap-ins** menu, click **OK**.

7. From the **Console Root** menu select, **Certificates (Local Computer) -> Personal -> Certificates**.

---

### Export client certificate

These instructions provide the details on how to export the client certificate needed to send encrypted RetinaVue Network order messages.

1. In the Console window, right click on company<CompanyID>.local (where <CompanyID> is your RetinaVue Network Company’s ID).

2. From the **Action** menu, select **All Tasks -> Export....**
3. From the Certificate Export Wizard window, click **Next >**.
4. Select **Yes, export the private key** and then click **Next >**.
5. Select **Personal Information Exchange - PKCS #12 (.PFX)**, Include all certificates in the certification path if possible, and then click **Next >**.
6. Create your password and click **Next >**.

**Note**

Ensure that your password is managed per appropriate security policy and store it in a safe place.

7. Click **Browse**, provide a file name, and click **Save**.
8. Click **Next** and **Finish**.

   From the Certificate Export Wizard pop up window, click **OK**. This certificate is now stored and password protected for later use.

### Export server certificate

These instructions provide the details on how to export the server certificate needed to receive encrypted RetinaVue Network result messages.

**Note**  
Not required for the Results Client configurations.

1. In the Console window, right click on `<CompanyID>.rvn.welchallyn.local`, (where `<CompanyID>` is your RetinaVue Network Company’s ID).

2. From the **Action** menu, select **All Tasks -> Export...**
3. From the Certificate Export Wizard window, click **Next >**.
4. Select **Yes, export the private key** and then click **Next >**.
5. Select **Personal Information Exchange -PKCS #12 (>PFX)**, **Include all certificates in the certification path if possible**, and then click **Next >**.
6. Create your password and click **Next >**.

**Note** Ensure that your password is managed per appropriate security policy and store it in a safe place.

7. Click **Browse**, provide a file name, and click **Save**.
8. Click **Next** and **Finish**.

From the Certificate Export Wizard pop up window, click **OK**. This certificate is now stored and password protected for later use.