



Hillrom™

**Welch Allyn®
RetinaVue® Network**

EMR Deployment Portal Guide

Software version 1.X

© 2021 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.

Legal Statement. Welch Allyn, Inc. ("Welch Allyn") assumes no responsibility for any injury to anyone that may result from (i) failure to properly use the product in accordance with the instructions, cautions, warnings, or statement of intended use published in this manual, or (ii) any illegal or improper use of the product.

Software in this product is Copyright 2021 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). Hill-Rom 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 hillrom.com/opensource. Where required, a copy of FOSS source code is available on our FOSS website.

PATENTS / PATENT hillrom.com/patents.

May be covered by one or more patents. See above Internet address. The Hill-Rom companies are the proprietors of European, US, and other patents and pending patent applications.

For information about any product, contact Hillrom Technical Support: hillrom.com/en-us/about-us/locations/.

REF DIR 80022176 Ver. G
Welch Allyn, Inc.
4341 State Street Road
Skaneateles Falls, NY 13153 USA

hillrom.com

Welch Allyn, Inc. is a subsidiary of Hill-Rom Holdings, Inc.

Revision date: 2021-05

This manual applies to the **#** 901078 SOFTWARE DATA INTERFACE



Contents

About this guide	1
RetinaVue architecture for USB connected camera workflow	2
RetinaVue architecture for Wi-Fi connected camera workflow	2
RetinaVue EMR connected workflow	3
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	9
Configure EMR connection properties	10
Step 1 — set up EMR	10
Step 2 — set up Clinics	11
Select one of following sections	12
VPN secure communication — results server	13
VPN secure communication — results client	13
Certificates secure communication — results server	14
Certificates secure communication — results client	15
Allscripts TouchWorks and Professional EHR integrations	17
Allscripts RetinaVue configuration	18
Athenahealth integrations	19
Athenahealth RetinaVue configuration	19
Greenway Prime Suite RetinaVue integrations	21
Greenway Prime Suite RetinaVue configuration	21
DICOM RetinaVue integrations	23
DICOM RetinaVue configuration	23
Update Deployment	25
Troubleshooting	27
Appendix	31
Sandbox servers	31
Production servers	31

Configure RetinaVue 700 to connect to the RetinaVue Sandbox Server	31
Configure RetinaVue Client Application to connect to the RetinaVue Sandbox Server	33
Certificate export and installation for server and client authentication	37

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

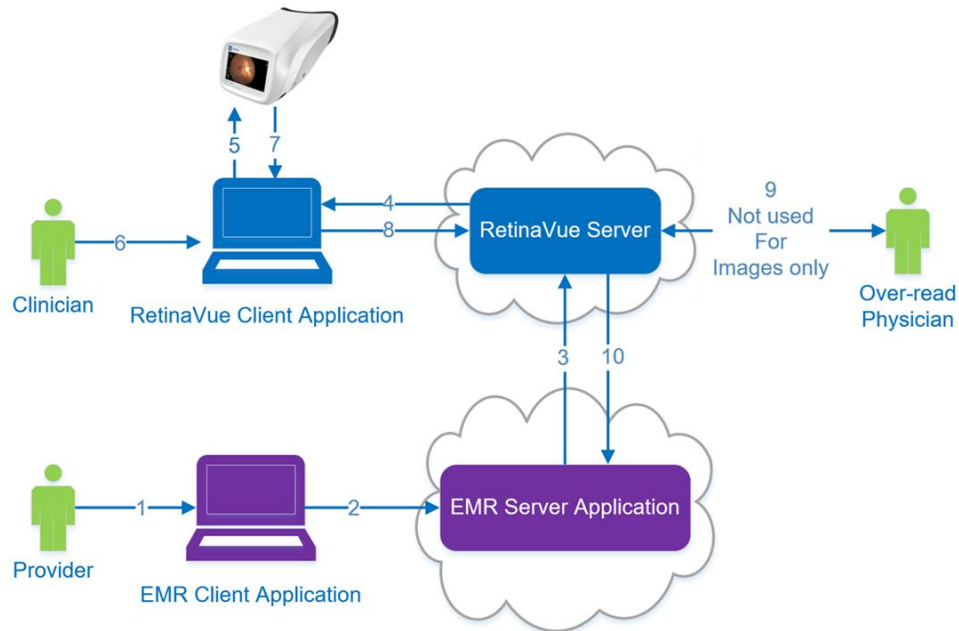
When using this manual, refer to the following:

- *Welch Allyn RetinaVue HL7 Interface Design Specification*
- *RetinaVue DICOM Interface Conformance Statement*
- *Welch Allyn RetinaVue™ 100 Imager — Directions for use*
- *Welch Allyn RetinaVue™ 700 Imager — Instructions for use*
- *Welch Allyn RetinaVue™ Network — Instructions for use*
- *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, consult the *Instructions 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.

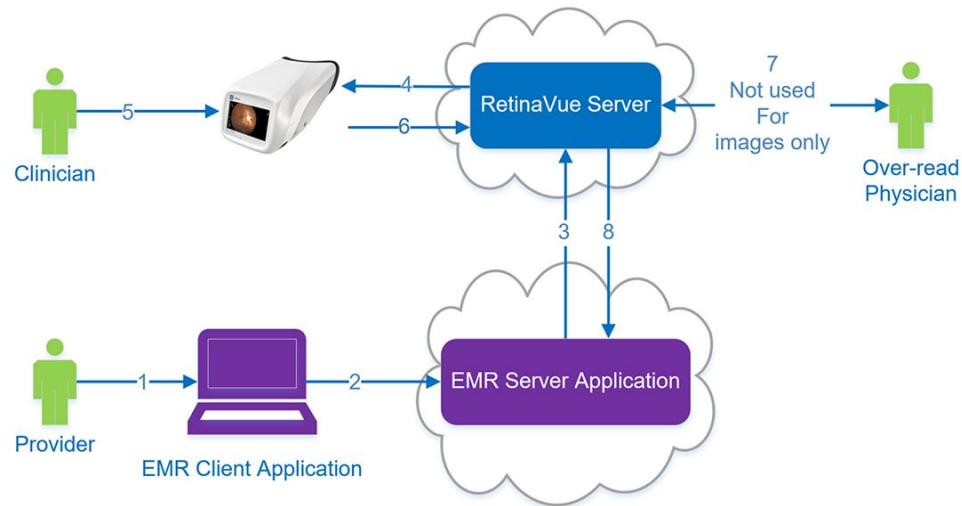


The RetinaVue architecture diagram also depicts the 10 interactions of the workflow:

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.

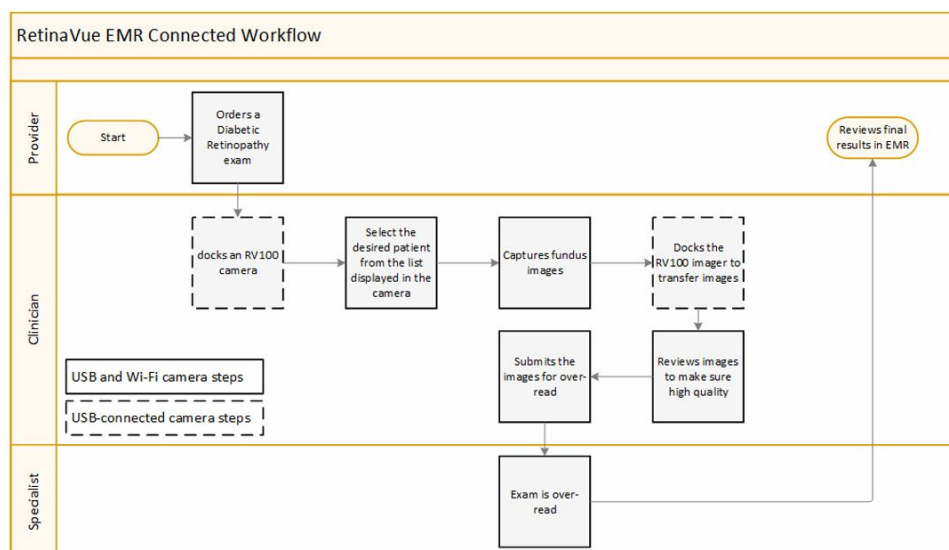


The RetinaVue architecture diagram also depicts the 8 interactions of the Wi-Fi workflow:

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.



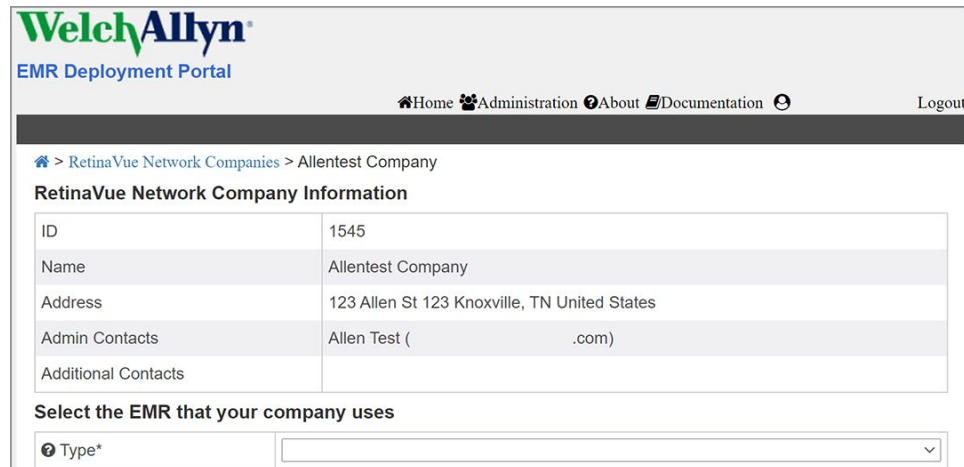
RetinaVue EMR connectivity project overview

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 Companies* information screen appears.



The screenshot shows the Welch Allyn EMR Deployment Portal interface. At the top, there is a navigation bar with links for Home, Administration, About, Documentation, and Logout. Below the navigation bar, the breadcrumb trail reads: Home > RetinaVue Network Companies > Allentest Company. The main content area is titled "RetinaVue Network Company Information" and contains a table with the following data:

ID	1545
Name	Allentest Company
Address	123 Allen St 123 Knoxville, TN United States
Admin Contacts	Allen Test (.com)
Additional Contacts	

Below the table, there is a section titled "Select the EMR that your company uses" with a dropdown menu labeled "Type*".

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 (optional, depending on the integration type)**
- **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 or they have expired.
- Yellow—certificates are ready (signed) and deployment is ready to be enabled once the appropriate certificates are uploaded. The status also is yellow when certificates are about to expire within 30 days.
- 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 you are using the Results Server with Certificates, ensure that the server receiving results is externally accessible and the port is open through the firewall.
- If VPN is being used, you need to set up the VPN connection before connecting RetinaVue to the EMR.

Allscripts

- Work with the RetinaVue Integration project manager to license the RetinaVue Network EMR Interface application for the Allscripts Unity server.
- For Touchworks Integrations, update the EHR client to create orders for RetinaVue fundus exams, and to configure the additional order questions.
- For Professional Integrations, you do not need to update the EHR client configuration. By default, procedure codes with 92250 are used to identify and create orders for RetinaVue fundus exams.

Athenahealth

- Work with the RetinaVue Integration project manager and Athenahealth to grant API key access to your practice's table space.
- Work with the RetinaVue Integration project manager and Athenahealth to enable the RetinaVue workflow for your practice.

eClinicalWorks

- Work with the RetinaVue Integration project manager and eCW to enable connectivity between the eCW Hub and RetinaVue.

Greenway Prime Suite

- Work with the RetinaVue Integration project manager and Greenway to enable the RetinaVue workflow for your practice.
- Work with the RetinaVue Integration project manager and Greenway to map your existing RetinaVue network clinics to your Greenway practices.
- Work with the Welch Allyn Project Manager and Greenway to ensure connectivity between the Greenway Prime Suite and RetinaVue.

DICOM Integrations

- VPN is the only connection option available. You must set up the VPN before connecting RetinaVue to the Digital Imaging and Communications in Medicine (DICOM) imaging server.
- Establish a connection to your modality worklist server for the RetinaVue Network server to poll for orders.
- Establish a listening connection before connecting RetinaVue to the DICOM imaging server.

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 a Greenway Prime Suite integration, please go to the Greenway Prime Suite RetinaVue configuration instructions.

If you are configuring a DICOM integration, please go to the DICOM RetinaVue configuration instructions.

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



NOTE This information includes eClinicalWorks integrations that 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:

Task	For instructions or more information
1. Set up the EMR	"Configure EMR connection properties"
a. Select the Security Configuration	"Step 1 — set up EMR"
b. Select the Exam Results Configuration	
c. Enter the Send Orders Port Number	
d. Enter the EMR IP Address.	
e. Enter the Receive Results Port Number.	
f. Enter the Receive Results Polling Interval (minutes)	
2. Set up the Clinics	"Step 2 — set up Clinics"

10 Choose an EMR security configuration and method of receiving exam results

Task

3. Create Certificates

For instructions or more information

See the detailed, step-by-step, instructions on the EMR Deployment Portal

Configure EMR connection properties

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

Select the EMR that your company uses

Type*

- Allscripts
- Athena MDP
- DICOM
- eClinicalWorks
- Epic
- Greenway Prime Suite
- Medent
- NextGen
- Other HL7

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

How will you configure your EMR to secure communication with RetinaVue?

Security Configuration*

- Certificates - The EMR will use certificates issued by Welch Allyn
- VPN - The EMR will establish a VPN connection with Welch Allyn

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

How will you configure your EMR to receive exam results from RetinaVue?

Exam Results Configuration*

- Server - The EMR will use a TCP/IP listener to receive results
- Client - The EMR will periodically poll RetinaVue to receive results

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 present.

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.

The **Test Connection** button allows a user to verify the connection that can be established between the RetinaVue server to the host system. Use this button to verify the network path and the security certificates.



NOTE The Send Orders and the Receive Results Ports are the same for the Results Client configurations.

5. Enter the Health Notifications Interval.

This interval is when the system determines if there are errors sending messages to the host system. When a consecutive error threshold is reached, an e-mail notification is sent to the company's contact e-mail addresses. The e-mail contains a description of the error and the URL of the error transaction.

6. Enter the Receive Results Polling Interval (minutes).

The **Poll for Results** button allows the user to poll RetinaVue for results, such as reports or images, and send any unsent results to the host system.



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

7. 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.

ID	Name	EMR ID
2	Family Practice 1	2
6	Plaza Family Practice 2	6

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



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.

Security Configuration	Method of Receiving Exam Results	Instruction Section
Certificates	Server	"Certificates secure communication — results server"
Certificates	Client	"Certificates secure communication — results client"
VPN	Server	"VPN secure communication — results server"
VPN	Client	"VPN secure communication — results client"

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.



NOTE If you use the default settings to create a TCP connection and send HL7 results messages to the EMR results server:

- The TCP connection remains open until closed by the results server.
- Minimum Lower Layer Protocol (MLLP) framing is used to transmit the results message.
- The default response timeout is 5 seconds.

For more details on the HL7 interface, refer to the *HL7 Interface Design Specification (IDS)* on the Documentation tab in the EMR Deployment Portal.

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.

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 are 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.

For instructions on how to obtain the completed certificates, see appendix, "Certificate export and installation for server and client authentication."



NOTE Certificates expire 2 years after creation. When your certificates are nearing expiration, an e-mail reminder is sent to the contact e-mail addresses set in step 1. For instructions on how to recreate your certificates, when necessary, refer to "Update Certificates" in the "Update Deployment" section.



NOTE If you use the default settings to create a TCP connection and send HL7 results messages to the EMR results server:

- The TCP connection remains open until closed by the results server.
- Minimum Lower Layer Protocol (MLLP) framing is used to transmit the results message.
- The default response timeout is 5 seconds.

For more details on the HL7 interface, refer to the *HL7 Interface Design Specification (IDS)* on the Documentation tab in the EMR Deployment Portal.

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 are 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.

For instructions on how to obtain the completed certificates, see appendix, "Certificate export and installation for server and client authentication."



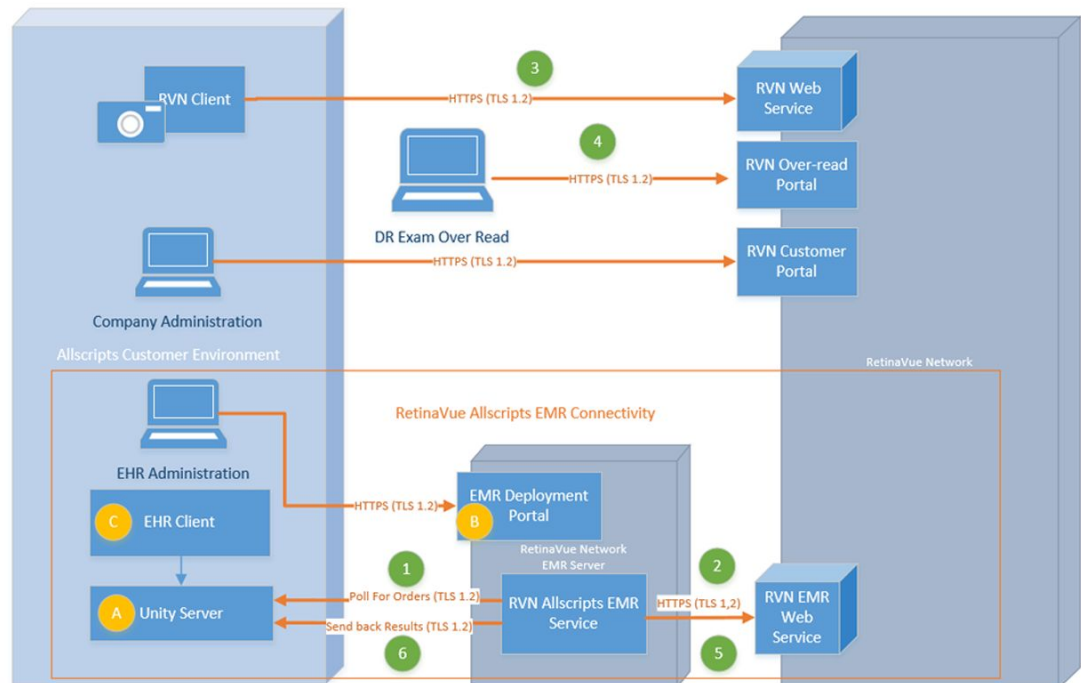
NOTE Certificates expire 2 years after creation. When your certificates are nearing expiration, an e-mail reminder is sent to the contact e-mail addresses set in step 1. For instructions on how to recreate your certificates, when necessary, refer to "Update Certificates" in the "Update Deployment" section.

16 Choose an EMR security configuration and method of receiving exam results

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.



NOTE Allscripts Professional EHR configurations may use only one clinic per deployment.

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.

Greenway Prime Suite RetinaVue integrations

Greenway Prime Suite RetinaVue configuration

Configure the EMR interface between your Greenway 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.

Step 1 — set up EMR

1. Select Greenway Prime Suite as the EMR type.
2. Enter at least one contact e-mail address. For multiple email addresses, separate with a semicolon (;).
3. 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 a Greenway Practice.

The RetinaVue Network Clinic ID is used as the mapping value. This should only be changed for testing purposes, or at the request of RetinaVue Integration or Greenway Project Management.

DICOM RetinaVue integrations

DICOM RetinaVue configuration

Configure the EMR interface between your DICOM compatible system 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.

Step 1 — set up EMR

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

24 DICOM RetinaVue integrations

Step 1. EMR Step 2. Clinics

[Show Instructions](#)

Type	DICOM
Configuration	VPN, Results Server
Contact Email Address(es)*	<input type="text" value="Company@test.com"/>
RetinaVue Network's IP Address	<input type="text" value="40.121.4.185"/>
Your Modality Worklist Server's IP Address*	<input type="text" value="137.116.92.191"/>
Your Modality Worklist Server's Port Number*	<input type="text" value="6712"/>
Request Worklist Polling Interval (minutes)*	<input type="text" value="1"/>
RetinaVue AE Title When Querying for a Worklist (optional)	<input type="text" value="RVN"/>
Your Modality Worklist Server's AE Title (optional)	<input type="text" value="ORTHANC"/>
Modality (optional)	<input type="text" value="OP"/>
Only return items in the worklist scheduled for today (UTC)*	<input checked="" type="checkbox"/>
Institution Name (optional)	<input type="text"/>
Your DICOM Image Server's IP Address*	<input type="text" value="137.116.92.191"/>
Your DICOM Image Server's Port Number*	<input type="text" value="6712"/>
RetinaVue AE Title when sending DICOM Images (optional)	<input type="text"/>
Your DICOM Image Server's AE Title (optional)	<input type="text"/>
Receive Results Polling Interval (minutes)*	<input type="text" value="1"/> <input type="button" value="Poll for Results"/>
Health Notifications Interval	<input type="text" value="1"/> <input type="text" value="Days"/>

Step 2 — set up Clinics

At least one RetinaVue Network Clinic must be mapped.

The RetinaVue Network Clinic ID is used as the mapping value. This should only be changed for testing purposes, or at the request of RetinaVue Integration or customer project management.

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.

ID	Name	EMR ID
9	Automation	1
11	Cool Clinic	2
10	New Clinic	3

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

Update Certificates (Optional)

If you are using the *Certificates Security Configuration*, you might need to update certificates.

1. If you need to update certificates because they have become lost or expired, refer to the instructions in steps 3–5 for your method of receiving exam results (**results client** or **results server**) for instructions on how to recreate certificates for your deployment.
2. If you are using the results server method to receive exam results, and need to update certificates because the IP address of the results server changed, do the following:
 - a. Perform step 1 in the *Configure EMR connection properties* section to set the new results server IP address.
 - b. Then follow steps 3–5 to recreate the certificates for your deployment with the new results server IP address.

Delete Deployment (Optional)

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

Troubleshooting

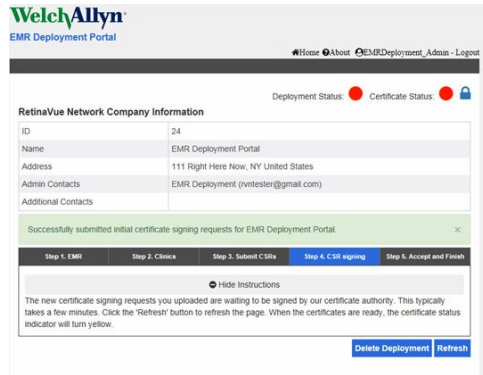
This section presents a table of problem descriptions, possible causes, and suggested actions that can resolve the issue.

Symptom	Possible cause	Suggested action
	The EMR does not have internet connectivity	Establish internet connectivity for the EMR.
	The RetinaVue EMR Server Application is not listening on the correct port	Use the EMR Deployment Portal to verify that the Orders port is configured correctly and correct if needed. Redeploy integration.
	The RetinaVue EMR Server is not targeting the correct RetinaVue EMR Server Application IP Address/Port	Use the EMR Deployment Portal to verify that the Orders port is configured correctly and correct if needed. Redeploy integration.
Unable to send HL7 messages from the EMR Server Application to the RetinaVue Network	<p>The RetinaVue EMR Server Application is down</p> <p>VPN security configuration: The VPN has not been established or is down.</p> <p>Certificates security configuration: The self signed client certificate is not being used to send HL7 messages.</p>	<p>Contact Welch Allyn technical support.</p> <p>Ensure the VPN is established and running.</p> <p>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.</p>
	The EMR is not trusting the Welch Allyn EMR Server's certificate.	Obtain and add Welch Allyn EMR Server's certificate root to the EMR's trusted certificate store.
	The HL7 message is invalid	Use the RetinaVue Deployment Portal to check the RetinaVue EMR Server Application message logs for more information.
The EMR received a NACK from the RetinaVue EMR Server Application	The EMR is not using the correct Client certificate	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

Symptom	Possible cause	Suggested action
		needed, create new certificates and follow the instructions to redeploy certificates on the RetinaVue Server and the EMR Server Application.
	The EMR Server Application is not using correct Client certificate	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.
The site is unable to activate the RetinaVue Client Application		See the topic <i>Install the RetinaVue™ Network software</i> in the <i>Welch Allyn RetinaVue™ Network — Network guide</i> .
	The site does not have internet connectivity available for the RetinaVue Client Application	Establish internet connectivity.
	The RetinaVue Client Application is not configured correctly to connect to the RetinaVue Server	
	<ul style="list-style-type: none"> In the test environment: 	<ul style="list-style-type: none"> See the topic <i>Configure the RetinaVue Client Application to connect to the RetinaVue Sandbox Server</i> in the appendix.
The RetinaVue Client Application is not showing pending exams	<ul style="list-style-type: none"> In the production environment: 	<ul style="list-style-type: none"> See the topic <i>Step 2 — set up Clinics</i> in the section <i>Configure the EMR information</i>. See the topic <i>Finding exams</i> topic in the Troubleshooting section of the <i>Network Guide</i>.
	The RetinaVue Server is down	Contact Welch Allyn technical support.
	The site IT infrastructure is blocking access to the RetinaVue Server	Ensure that the RetinaVue Server is accessible. (Use port number 443.)
	The camera is not connected to the RetinaVue Client Application PC	Connect the camera to the RetinaVue Client Application PC.
The camera's patient list is not being updated with pending exams	The RetinaVue Client Application is not recognizing the connected camera	Ensure that the camera is powered on and not in sleep mode.
	The camera is not docked correctly	Ensure that the camera is docked correctly such that the communication pins are securely aligned.

Symptom	Possible cause	Suggested action
	The RetinaVue Client Application is not configured for the camera being used	See the <i>View or change the Camera Settings</i> topic in the <i>Network Guide</i> .
	Wireless Camera: The wireless camera is not activated against the correct clinic.	See the RetinaVue Network Troubleshooting.
The site's RetinaVue Client Application pending exams list is not being updated with completed exams	The camera is not connected to the RetinaVue Client Application PC	Connect the camera to the RetinaVue Client Application PC.
	The RetinaVue Client Application is not recognizing a connected camera	Ensure that the camera is powered on and not in sleep mode.
	The camera is not docked correctly	Ensure that the camera is docked correctly such that the communication pins are securely aligned.
	The RetinaVue Client Application is not configured for the camera being used	See the <i>View or change the Camera Settings</i> topic in the <i>Network Guide</i> .
Unable to submit an exam for over-read	The site does not have internet connectivity	Establish internet connectivity.
	The site IT infrastructure is blocking access from the RetinaVue Client Application to the RetinaVue Server	Ensure that the RetinaVue Server is accessible. (Use port 443.)
	The RetinaVue Server is down	Contact Welch Allyn technical support.
The EMR is unable to receive results from the RetinaVue EMR Server Application	The RetinaVue EMR Server Application has not polled for results since the over-read result has been completed	Wait for the polling to occur. (Polling occurs every 20 minutes.)
	The RetinaVue EMR Server Application is down	Contact Welch Allyn technical support.
	The EMR Server is not targeting the correct RetinaVue EMR Server Application IP Address/Port	Use the EMR Deployment Portal to verify the correct IP/Ports are being used. If needed, update the deployment. Redeploy integration.
	Site is not listening on the correct port	Update the EMR configuration to listen for completed results on the correct port.
		Contact Welch Allyn technical support.
	The EMR does not have internet connectivity	Ensure the VPN is established and running.
	VPN security configuration: The VPN has not been established or is down. Certificates security configuration: The server certificate is not being used to receive results.	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

Symptom	Possible cause	Suggested action
		certificates on the RetinaVue Server and the EMR Server Application.
The RetinaVue EMR Server Application received a NACK from the EMR upon sending a result	Result is invalid	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.
The deployment status remains red	The deployment has not completed	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.)



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:

https://sandbox.retinavue.net/RN_CustomerPortal.

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

<https://sandbox.retinavue-emr.net/EMRDeploymentPortal>.

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:

https://www.retinavue.net/RN_CustomerPortal.

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

<https://retinavue-emr.net>.

Configure RetinaVue 700 to connect to the RetinaVue Sandbox Server

These instructions explain how to disconnect from the production server and connect the RetinaVue 700 imager to the sandbox server. For more information about setting up the imager, see *Welch Allyn RetinaVue™ 700 Imager — Instructions for use*.

Remove RetinaVue 700 from the Production Customer Portal

Log in to the RetinaVue Network Customer Portal at https://www.retinavue.net/RN_CustomerPortal using your User Name and Password. (For additional information, see the topics: *Set up process* and *First time set up of the company* in the *Network Guide*.)

1. Select **Manage Devices**.
2. Click **Next**.
3. Select **Edit** next to the RetinaVue 700 imager.
4. Uncheck the Clinic that is associated with the RetinaVue 700 imager.
5. Click **Save**.

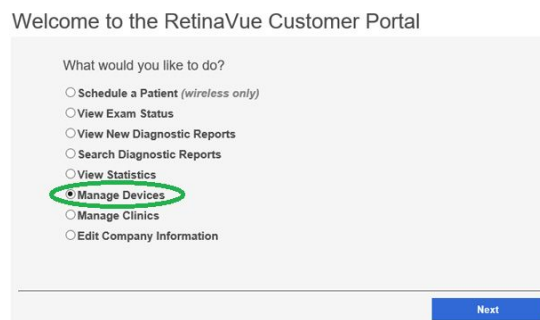
A popup appears with the following message, *Do you want to deregister the device?*

6. Select **Deregister**.
Your RetinaVue 700 imager is now disconnected from the Production Customer Portal.

Connect RetinaVue 700 to the RetinaVue Sandbox Server

Follow these steps to connect the RetinaVue 700 imager to the RetinaVue Sandbox Server. First, set up the imager, then log in to the Sandbox Server to connect the device.

1. Turn on the RetinaVue 700 imager.
2. On your RetinaVue 700 imager, touch **Menu**.
3. Touch **Settings**.
4. Select **Advanced Settings**.
5. Select **Restore Factory Defaults**.
6. Select **Restore Settings** and **OK**.
7. Select a **Language**.
8. Update the **Time, Date, Continent,** and **Location**.
9. Select **No – Take me to registration**.
10. Select **RetinaVue Network – Wi-Fi**.
11. Touch **Next**.
12. Connect the imager to the Wi-Fi network.
13. Enter a *Passphrase*.
14. Touch **Connect**.
15. Touch **Dev Tools**.
16. Select *I have a test server that I want to send test images to*.
17. Touch **Next**.
18. Note the registration code XXXX-XXXX.
19. Log into the Sandbox (test) Customer Portal at https://sandbox.retinavue.net/rn_customerportal/ with your User Name and Password to finish setting up the imager.
 - a. Select **Manage Devices** and click **Next**.



- b. Click **Add Device**.
 - c. Enter the Device Registration Code using the code XXXX-XXXX on the camera display.
 - d. Click **Enter**.
 - e. Enter the **Device Name**.
 - f. Select the clinic check box that is associated with the camera.
 - g. Click **Save**.
20. Return to the imager to verify that the RetinaVue 700 setup is complete.
The *Camera registered successfully* message displays.
21. Touch **OK** on the *Setup Complete* screen.
You are now ready to use this RetinaVue 700 imager with the Sandbox Server.

Configure RetinaVue Client Application to connect to the RetinaVue Sandbox Server

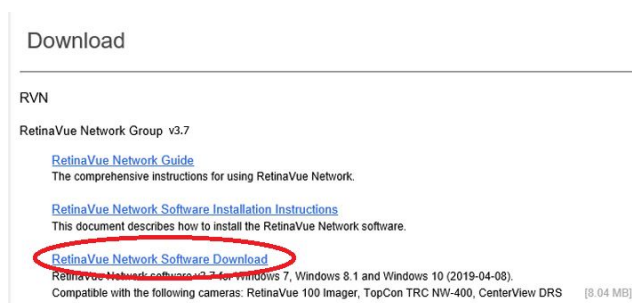
These instructions explain how to connect to a test server to check the complete process of sending orders and receiving results.

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.

- a. Run Internet Explorer® as an administrator and navigate to https://sandbox.retinavue.net/RN_CustomerPortal.
- 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 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 address=""> value from: https://www.retinavue.net/RN_WebService/RN_WebSvc.svc

```

RetinaVue Network.exe.config - Notepad
File Edit Format View Help
<configProtectedData defaultProvider="RVNConfigurationProvider4">
  <providers>
    <!-- NOTE: All provider names defined below must be in sync with those in the ProtectConfig custom
    action project within the installer solution -->
    <add name="RVNConfigurationProvider2"
    type="System.Configuration.RsaProtectedConfigurationProvider, System.Configuration, Version=2.0.0.0,
    Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a"
    description="Uses RsaCryptoServiceProvider from .NET 2 runtime to encrypt and decrypt"
    keyContainerName="RVNConfigurationKey" cspProviderName="" useMachineContainer="true"
    useOAEP="false" />
    <add name="RVNConfigurationProvider4"
    type="System.Configuration.RsaProtectedConfigurationProvider, System.Configuration, Version=4.0.0.0,
    Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a"
    description="Uses RsaCryptoServiceProvider from .NET 4 runtime to encrypt and decrypt"
    keyContainerName="RVNConfigurationKey" cspProviderName="" useMachineContainer="true"
    useOAEP="false" />
  </providers>
</configProtectedData>
<system.serviceModel>
  <bindings>
    <wsHttpBinding>
      <binding name="WSHttpBinding_IRN_WebSvc" sendTimeout="00:10:00"
      maxBufferPoolSize="524288" maxReceivedMessageSize="2147483647" useDefaultWebProxy="true"
      allowCookies="false">
        <security mode="Transport" />
      </binding>
    </wsHttpBinding>
  </bindings>
  <client>
    <endpoint address="https://www.retinavue.net/RN_WebService/RN_webSvc.svc"
    binding="WSHttpBinding" bindingConfiguration="WSHttpBinding_IRN_WebSvc"
    contract="RN_WebService.IRN_WebSvc" name="WSHttpBinding_IRN_WebSvc">
      <identity>

```

to: https://sandbox.retinavue.net/RN_WebService/RN_WebSvc.svc

```

File Edit Format View Help
<configProtectedData defaultProvider="RVNConfigurationProvider4">
  <providers>
    <!-- NOTE: All provider names defined below must be in sync with those in the ProtectConfig custom
    action project within the installer solution -->
    <add name="RVNConfigurationProvider2"
    type="System.Configuration.RsaProtectedConfigurationProvider, System.Configuration, Version=2.0.0.0,
    Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a"
    description="Uses RsaCryptoServiceProvider from .NET 2 runtime to encrypt and decrypt"
    keyContainerName="RVNConfigurationKey" cspProviderName="" useMachineContainer="true"
    useOAEP="false" />
    <add name="RVNConfigurationProvider4"
    type="System.Configuration.RsaProtectedConfigurationProvider, System.Configuration, Version=4.0.0.0,
    Culture=neutral, PublicKeyToken=b03f5f7f11d50a3a"
    description="Uses RsaCryptoServiceProvider from .NET 4 runtime to encrypt and decrypt"
    keyContainerName="RVNConfigurationKey" cspProviderName="" useMachineContainer="true"
    useOAEP="false" />
  </providers>
</configProtectedData>
<system.serviceModel>
  <bindings>
    <wsHttpBinding>
      <binding name="WSHttpBinding_IRN_WebSvc" sendTimeout="00:10:00" maxBufferPoolSize="524288"
      maxReceivedMessageSize="2147483647" useDefaultWebProxy="true" allowCookies="false">
        <security mode="None" />
      </binding>
    </wsHttpBinding>
  </bindings>
  <client>
    <endpoint address="https://sandbox.retinavue.net/RN_WebService/RN_webSvc.svc"
    binding="WSHttpBinding" bindingConfiguration="WSHttpBinding_IRN_WebSvc"
    contract="RN_WebService.IRN_WebSvc" name="WSHttpBinding_IRN_WebSvc" />
  </client>
</system.serviceModel>
<startup>
  <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5" />

```

- 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.)



NOTE Ensure that the activation key is captured from the correct customer portal (sandbox vs. production) per the associated URLs in the instructions.

RetinaVue Network Group v3.7

[RetinaVue Network Guide](#)
The comprehensive instructions for using RetinaVue Network.

[RetinaVue Network Software Installation Instructions](#)
This document describes how to install the RetinaVue Network software.

[RetinaVue Network Software Download](#)
RetinaVue Network software v3.7 for Windows 7, Windows 8.1 and Windows 10 (2019-04-08).
Compatible with the following cameras: RetinaVue 100 Imager, TopCon TRC NW-400, CenterView DRS [8.04 MB]

[RetinaVue Network Quick Start Guide for the RetinaVue 100 Imager](#)
A guide to explain how to use the RetinaVue 100 Imager with the RetinaVue Network software.

[RetinaVue Network Quick Start Guide for the TopCon TRC NW-400](#)
A guide to explain how to use the TopCon TRC NW-400 with the RetinaVue Network software.

RetinaVue Network Software Activation Key:
XXXXXXXX-XXXX-XXXX-XXXXXXXX

Activation - Step 1

RetinaVue™ Network must be activated to continue.

Enter the activation key below then click **Next** to continue:
[\(found on the RetinaVue™ Network customer portal Installers page\)](#)

XXXXXXXX-XXXX-XXXX-XXXXXXXX

- 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**.

Interface health notifications

The RetinaVue Network detects when the orders and results interfaces are not functioning properly. When this issue occurs, the RetinaVue Network sends an interface health notification with the error description to the configured contact e-mail addresses.

If you receive an interface health notification, correct the error.

In this example, the Health Notifications Interval is set to one day.

Step 1. EMR	Step 2. Clinics
⊕ Show Instructions	
Type	Other HL7
Configuration	VPN, Results Client
Contact Email Address(es)*	<input type="text" value="RVNTester@gmail.com"/>
RetinaVue Network's IP Address	40.121.4.185
Send Orders and Result Requests Port Number* (Acceptable Ranges: 6767-6882)	<input type="text" value="6658"/>
Health Notifications Interval	<input type="text" value="1"/> <input type="text" value="Days"/>
Next >	
Delete Deployment Refresh	

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 likely will 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.

Obtain the Certificate Identification information from the deployment information

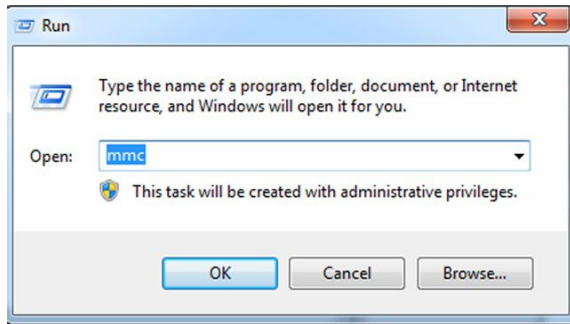
The EMR Deployment Portal presents the Certificate common name and thumbprint that you can use to locate the certificate to export from the Windows Keystore. You will use this information in subsequent steps.

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.
3. Note the common name and thumbprint for both the Send Orders and Receive Results certificates.

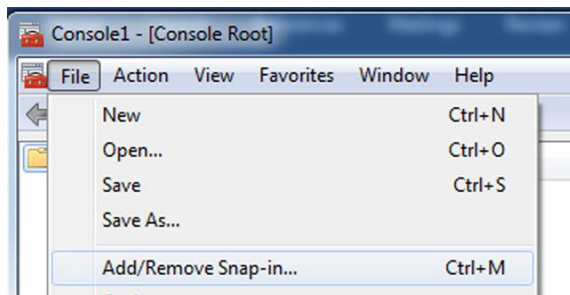
Step 1. EMR	Step 2. Clinics	Step 3. Submit CSRs	Step 4. CSR Signing	Step 5. Accept and Finish
+ Show Instructions				
Type	Other HL7			
Configuration	Certificates, Results Server			
Contact Email Address(es)*	<input type="text" value="rvntester@gmail.com"/>			
RetinaVue Network's Domain Name or IP Address	<input type="text" value="dev.retinavue-emr.net"/>			
Send Orders Port Number* (Acceptable Ranges: 6650-6766)	<input type="text" value="6652"/>			
Send Orders Certificate Common Name	<input type="text" value="company58.local"/>			
Send Orders Certificate Thumbprint	<input type="text" value="002D6F03F87789EFF6062BF97A18B496E410C592"/>			
Your EMR's Domain Name or IP Address*	<input type="text" value="127.0.0.1"/>			
Receive Results Port Number* (Acceptable Ranges: 1025-49151)	<input type="text" value="443"/>	<input type="button" value="Test Connection"/>		
Receive Results Polling Interval (minutes)*	<input type="text" value="1"/>	<input type="button" value="Poll for Results"/>		
Health Notifications Interval	<input type="text" value="1"/>	Days <input type="button" value="v"/>		
Receive Results Certificate Common Name	<input type="text" value="58.rvn.welchallyn.local"/>			
Receive Results Certificate Thumbprint	<input type="text" value="FBB23D0BCF65DC8797EF19BC746E56FBBCD6D9E0"/>			
				<input type="button" value="Next >"/>
<input type="button" value="Download Active Certificates"/>		<input type="button" value="Delete Deployment"/>		<input type="button" value="Refresh"/>

Access the Certificate Snap-in within the Microsoft Management Console

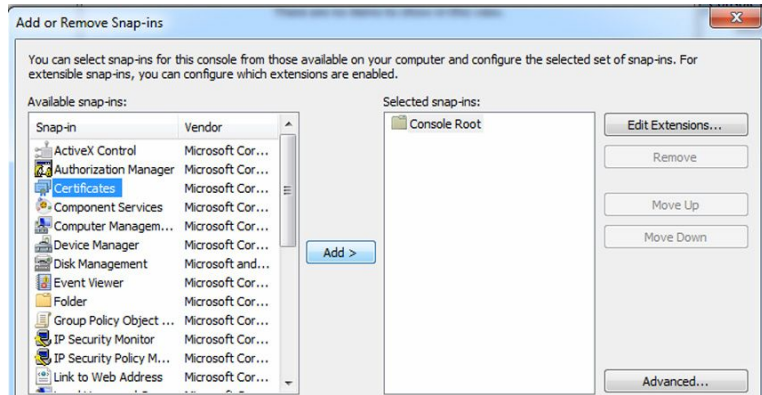
1. From the Windows® taskbar, click **Run ...**, type *MMC*, and then click **OK** to launch the Microsoft Management Console.



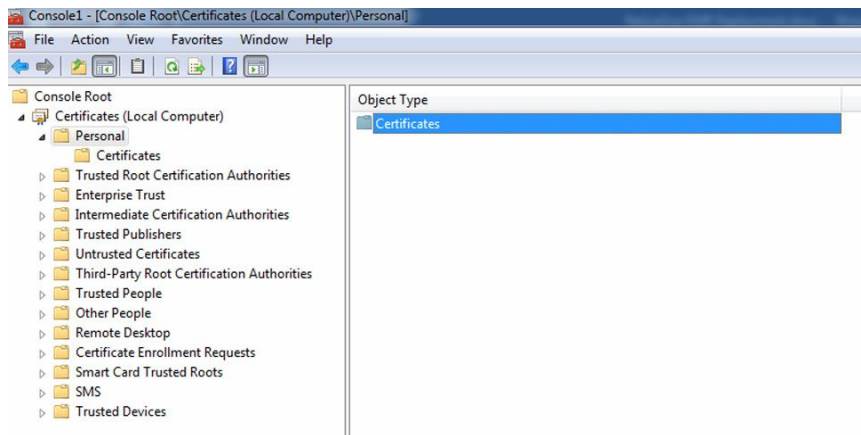
2. From the Microsoft Management Console, select **File -> Add/Remove Snap-in...**



3. From the *Available Snap-ins* menu, select *Certificates*, and click **Add >**.



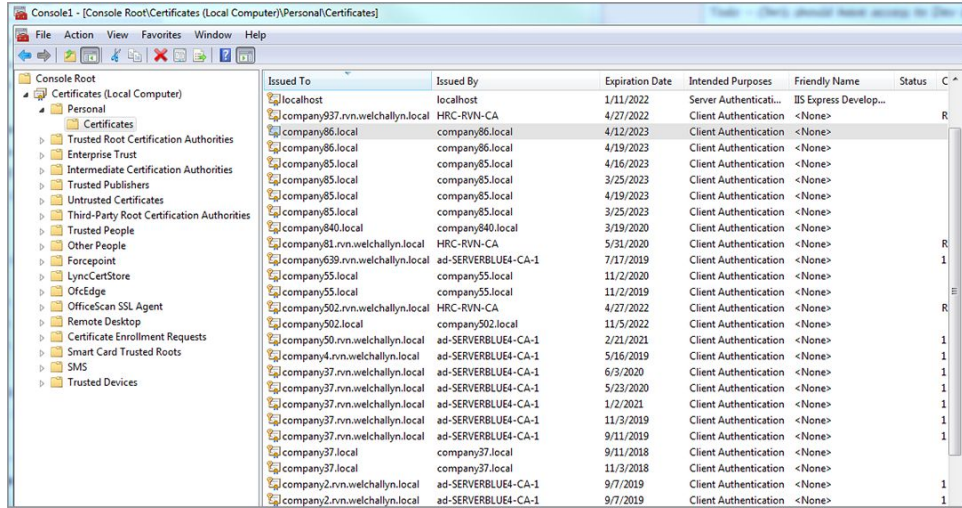
4. From the *Certificates Snap-in* menu, select **Computer Account** and click **Next >**.
5. From the *Select Computer* menu, choose **Local computer: (the computer this console is running on)** and then click **Finish**.
6. From the *Available Snap-ins* menu,click **OK**.
7. From the *Console Root* menu select, **Certificates (Local Computer) -> Personal -> Certificates**.



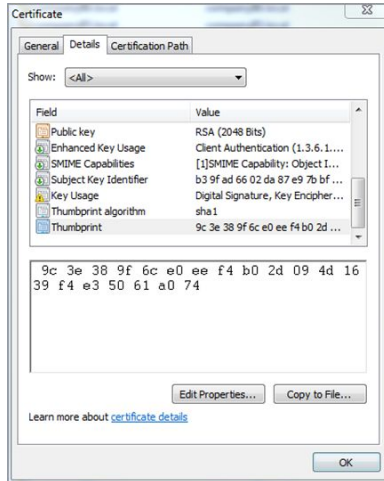
Export client certificate

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

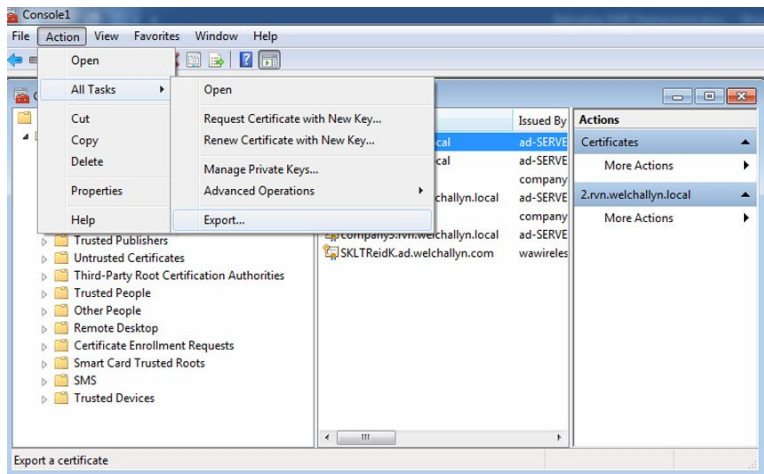
1. In the Console window, double-click on the certificate with an *Issued To* value that matches the value for the *Send Orders Certificate Common Name* from the EMR Deployment Portal.



- Verify that the certificate thumbprint in the Details tab for the Certificate window contains the same value as the *Send Orders Certificate Thumbprint* from the EMR Deployment Portal.

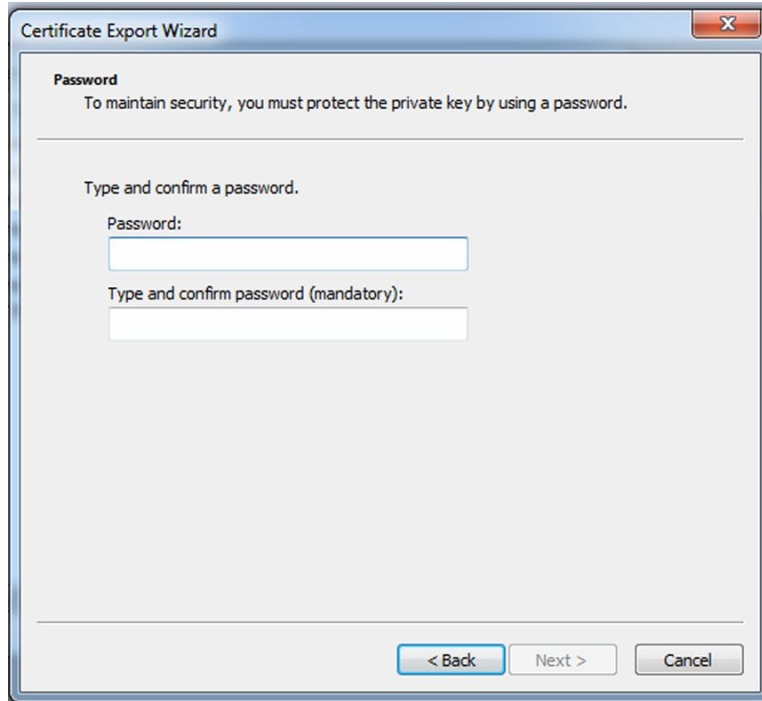


- Click **OK** to close the Certificate window.
- Highlight the correct certificate, and from the *Action* menu, select **All Tasks -> Export...**



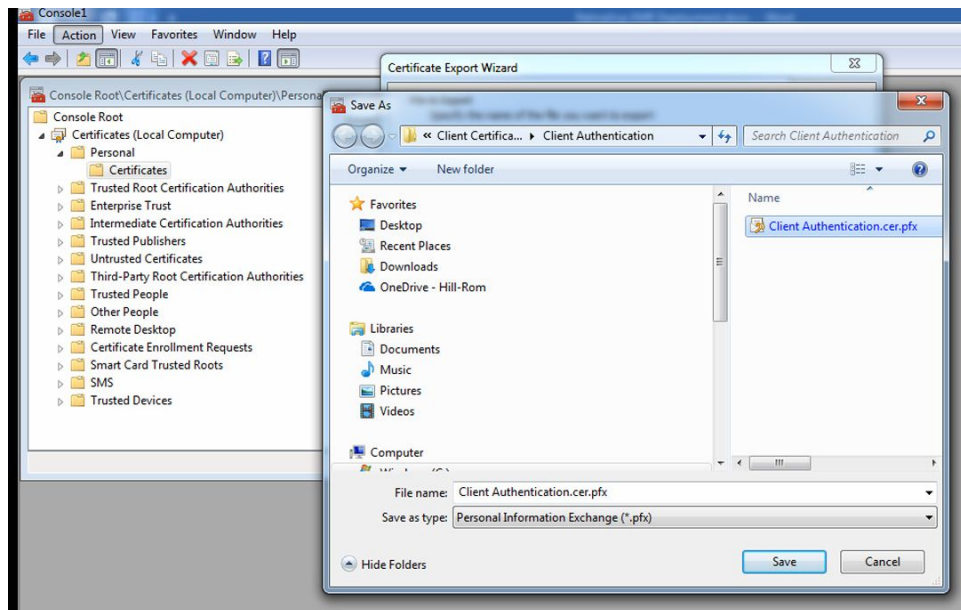
- From the Certificate Export Wizard window, click **Next >**.
- Select **Yes, export the private key** and then click **Next >**.

7. Select **Personal Information Exchange -PKCS #12 (>PFX)** , **Include all certificates in the certification path if possible**, and then click **Next >**.
8. Create your password and click **Next >**.



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

9. Click **Browse**, provide a file name, and click **Save**.



10. 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.

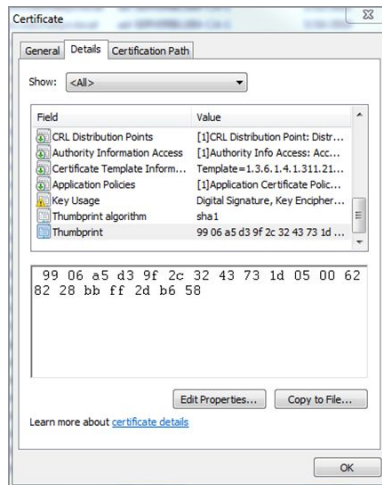


NOTE Not required for the Results Client configurations.

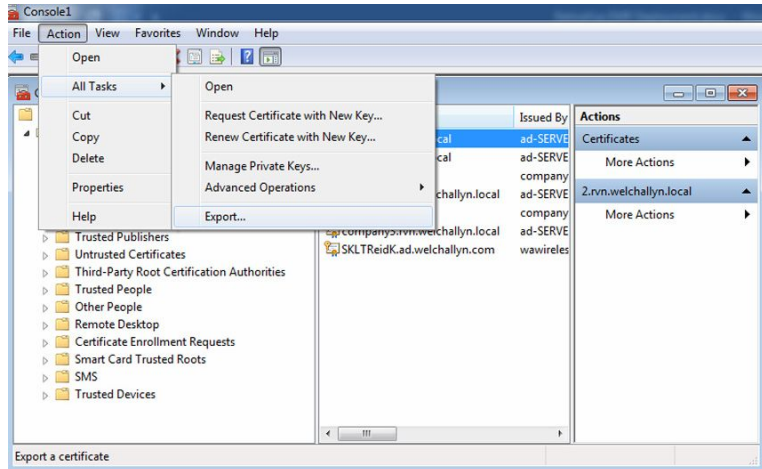
1. In the Console window, double-click on the certificate with an *Issued To* value that matches the value for the *Receive Results Certificate Common Name* from the EMR Deployment Portal.

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status
company502.rvn.welchallyn.local	HRC-RVN-CA	4/27/2022	Client Authentication	<None>	
company502.local	company502.local	11/5/2022	Client Authentication	<None>	
company50.rvn.welchallyn.local	ad-SERVERBLUE4-CA-1	2/21/2021	Client Authentication	<None>	1
company4.rvn.welchallyn.local	ad-SERVERBLUE4-CA-1	5/16/2019	Client Authentication	<None>	1
company37.rvn.welchallyn.local	ad-SERVERBLUE4-CA-1	6/3/2020	Client Authentication	<None>	1
company37.rvn.welchallyn.local	ad-SERVERBLUE4-CA-1	5/23/2020	Client Authentication	<None>	1
company37.rvn.welchallyn.local	ad-SERVERBLUE4-CA-1	1/2/2021	Client Authentication	<None>	1
company37.rvn.welchallyn.local	ad-SERVERBLUE4-CA-1	11/3/2019	Client Authentication	<None>	1
company37.rvn.welchallyn.local	ad-SERVERBLUE4-CA-1	9/11/2019	Client Authentication	<None>	1
company37.local	company37.local	9/11/2018	Client Authentication	<None>	
company37.local	company37.local	11/3/2018	Client Authentication	<None>	
company2.rvn.welchallyn.local	ad-SERVERBLUE4-CA-1	9/7/2019	Client Authentication	<None>	1
company2.rvn.welchallyn.local	ad-SERVERBLUE4-CA-1	9/7/2019	Client Authentication	<None>	1
company2.local	company2.local	9/7/2018	Client Authentication	<None>	
company2.local	company2.local	9/7/2018	Client Authentication	<None>	
company19.local	company19.local	3/14/2020	Client Authentication	<None>	
company19.local	company19.local	3/14/2021	Client Authentication	<None>	
company19.local	company19.local	3/14/2020	Client Authentication	<None>	
company1403.rvn.welchallyn.lo...	HRC-RVN-CA	4/27/2022	Client Authentication	<None>	R
company1403.rvn.welchallyn.lo...	HRC-RVN-CA	1/2/2021	Client Authentication	<None>	R
company1403.rvn.welchallyn.lo...	HRC-RVN-CA	1/2/2021	Client Authentication	<None>	R
86.rvn.welchallyn.local	ad-SERVERBLUE4-CA-1	4/12/2023	Server Authenticati...	<None>	1
85.rvn.welchallyn.local	ad-SERVERBLUE4-CA-1	3/25/2023	Server Authenticati...	<None>	1
85.rvn.welchallyn.local	ad-SERVERBLUE4-CA-1	3/25/2023	Server Authenticati...	<None>	1
85.rvn.welchallyn.local	ad-SERVERBLUE4-CA-1	4/16/2023	Server Authenticati...	<None>	1
85.rvn.welchallyn.local	ad-SERVERBLUE4-CA-1	4/19/2023	Server Authenticati...	<None>	1

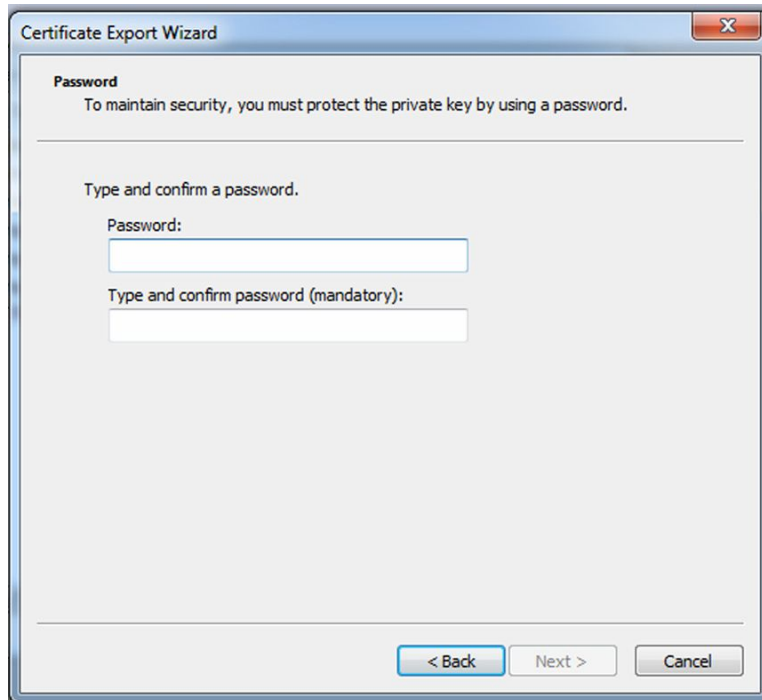
2. Verify that the certificate thumbprint in the Details tab for the Certificate window contains the same value as the *Receive Results Certificate Thumbprint* from the EMR Deployment Portal.



3. Click **OK** to close the Certificate window.
4. Highlight the correct certificate, and from the *Action* menu, select **All Tasks -> Export...**

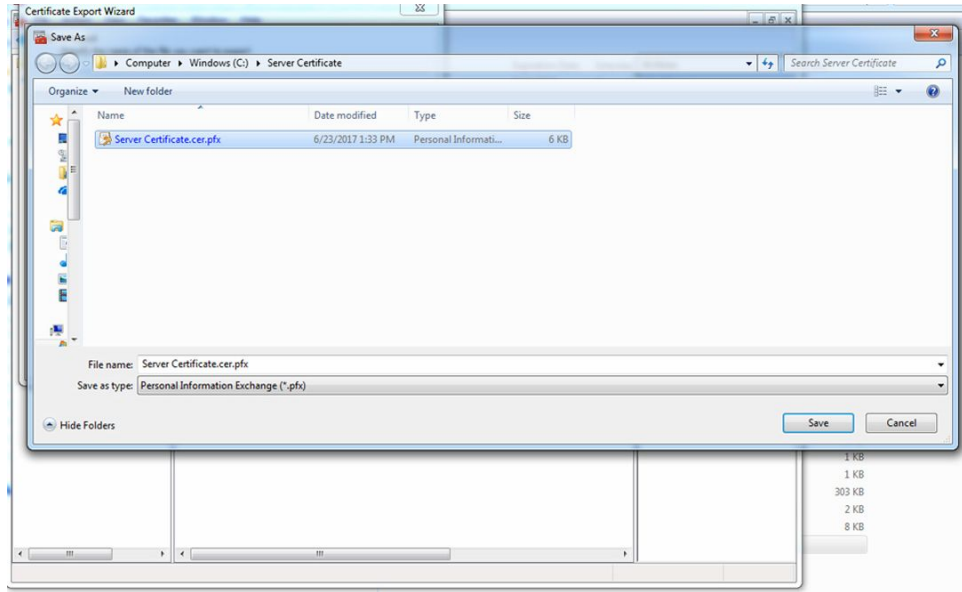


5. From the Certificate Export Wizard window, click **Next >**.
6. Select **Yes, export the private key** and then click **Next >**.
7. Select **Personal Information Exchange -PKCS #12 (>PFX)** , **Include all certificates in the certification path if possible**, and then click **Next >**.
8. Create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



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

9. Click **Browse**, provide a file name, and click **Save**.



10. 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.

