HIS/RIS Link Field Guide for AMX™ Navigate

gehealthcare.com

Effortless Workflow

HIS/RIS Link

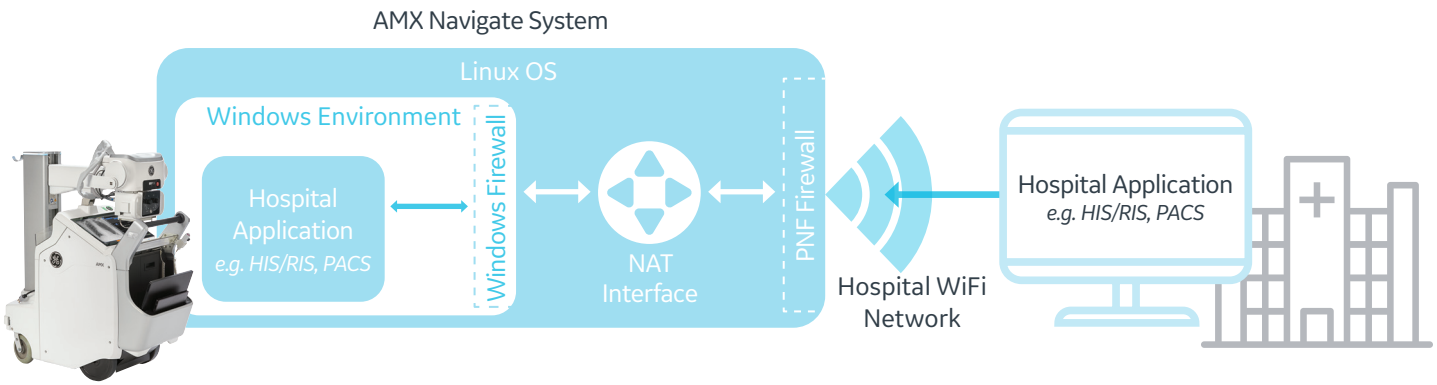
The HIS/RIS Link feature provides a Windows® environment via a virtual machine on the AMX Navigate operating system. Hospitals can install software in the Windows environment or open an internet browser to enable user access to HIS/RIS, EMR, and/or PACS directly from the X-ray system.

Sites are free to configure the Windows environment within the virtual machine, as long as the validated major Windows version, Windows 10, supports the configuration.

Feature Overview

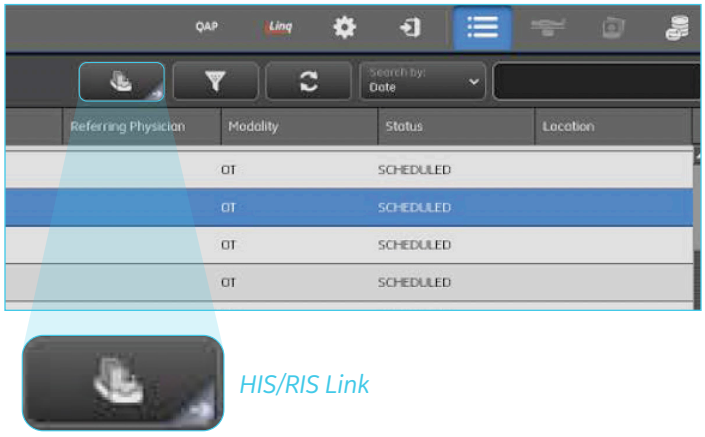
The HIS/RIS Link feature provides access to a facility's HIS/RIS, EMR, and/or PACS software directly from the AMX Navigate user interface. This feature enables a technologist to complete actions in those hospital applications, such as remotely start, close, and complete HIS/RIS exams from the portable.

System Architecture: Linux-based OS provides added security



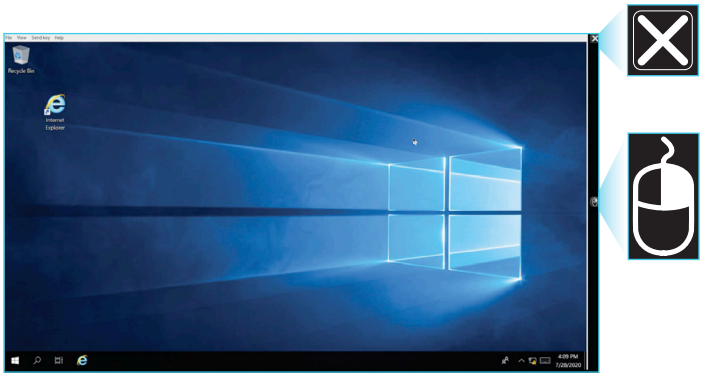
Steps to Launch and Close the Virtual Machine on AMX Navigation

1. Select the HIS/RIS Link button from the Worklist screen. The Windows Virtual Machine application will open, followed by the Windows desktop which will have a link to the HIS/RIS server (depending on site configuration).



HIS/RIS Link

2. While in the VM, if right click function is needed select the right click button as shown below.



3. To Close the HIS/RIS Windows desktop application and return to the mobile X-ray system application, select the “X” in the upper right corner.

Software Installation

After the service engineer has completed installation of the HIS/RIS Link feature, Site IT may configure the Windows environment and install site-specific HIS/RIS and/or PACS software. Software can be installed from a USB media or a network location such as a shared network drive or file sharing service

System and VM Configuration

System Components	Details
Touch Screen	
Aspect Ratio	16.9
Resolution	1920 x 1080
Size	21.5 inch
Function	Capacitive touch
System Storage	Solid State Drive (SSD)
Memory	32 GB
Linux Host	30 GB
VM	2 GB
Virtual Machine (VM) Load Time	
First time load after start-up	25 sec.
Subsequent Re-open	1 sec.
Windows 10 Operating system License	Windows 10 IoT LTSC enterprise 2019
Windows 10 Operating System Build	1809
Network Configuration	NAT
MAC Address	Virtual. Different from Physical Interface
AV Security	Windows Defender – Enabled, Automatic Updates – Enabled
Required AV Exceptions	None
ActiveDirectory Support	Allowed
Remote Management	Allowed but not tested by GE

Product Network Filter (PNF) Configuration

The PNF configuration can be accessed through the X-ray system service user interface. After modifying any PNF options, select **Restart Firewall** to apply the changes. The following PNF information is an excerpt from the PNF user interface control area.

The PNF user interface control area, near the top of the screen, contains these options:

Option	Action
Filter Settings	Configure filter settings that allow access through the firewall by adding allowed services and IP addresses, and removing filters.
Backup/Restore	Options: **Backup Current Filters:** Create a backup of the current filters. **Restore from Backup Filters:** Restore the filters to a previously backed up set. **Restore to Factory Defaults:** Reset all filter settings to those originally installed. **Remove Backup Filters**
Network Tools	Show the firewall rules that are currently in effect on this system. Select **Refresh** to refresh the list of rules.
Configure PNF	Select which red interfaces the filter settings should be applied to. Select **Update Red Interfaces** to apply the changes.

The following parameters are available in tabs of the PNF user interface:

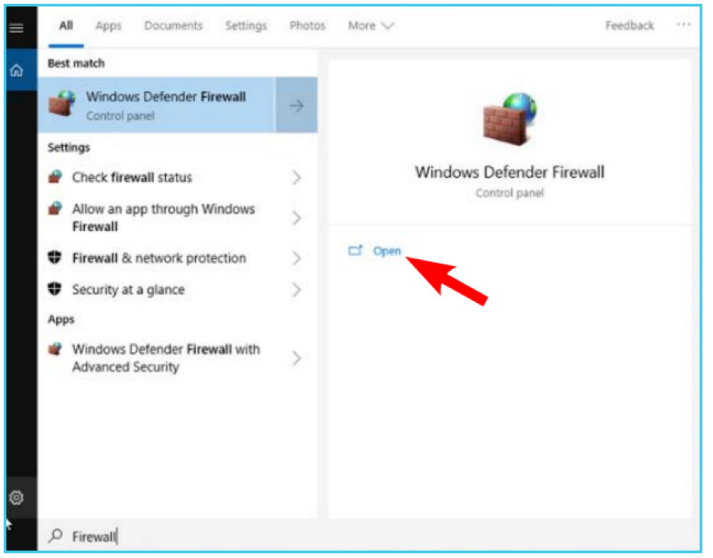
Option	Action
Named Services Tab Used to set up filters to allow traffic to common network services (such as telnet or ftp) by name, without needing to know the port and protocol.	
Services/Allowed IPs	Lists current filters by name and IP.
Remove Existing Filters	Select the Delete box checkbox next to the filter to delete, then select **Delete Existing Filters**.
Add New Filter	From the Service Name drop-down list, select the service to be allowed (such as telnet, ssh, ftp). In the Allowed IPs field, specify a particular IP address, a range of IP addresses, or a masked subnet. Select **Add Filter** to apply your changes.
Allowed Nodes Tab Used to set up filters to allow all traffic from specified nodes. You can specify a particular IP address, a range of IP addresses, or a masked subnet.	
Allowed IPs	Lists current filters by IP.
Remove Existing Filters	Select the Delete box checkbox next to the filter to delete, then select **Delete Existing Filters**.
Add New Filter	In the Allowed IPs field, specify a particular IP address, a range of IP addresses, or a masked subnet. Select **Add Filter** to apply your changes.

Option	Action
DICOM® tab Used to add DICOM port numbers (all IP addresses are allowed DICOM access; the DICOM application may limit access by IP). You can add multiple DICOM ports.	
Allowed DICOM Ports	Lists current DICOM ports by number.
Remove Existing Filters	Select the Delete box checkbox next to the port to delete, then select **Delete Existing Filters**.
Add New Filter	In the Allowed Port field, specify a particular DICOM port. Select **Add Filter** to apply your changes.
Expert Tab Used to set up detailed filters by port, protocol, and node-lock (source). Used only by advanced IT users.	
Name/Port/Protocol	Lists current filters by name, port number, protocol, and IP.
Remove Existing Filters	Select the Delete box checkbox next to the filter to delete, then select **Delete Existing Filters**.
Add New Filter	In the Name field, specify the filter name. In the Allowed IPs field, specify a particular IP address, a range of IP addresses, or a masked subnet. In the Allowed Port field, specify a particular port. From the Protocol drop-down list, select the protocol to be allowed (TCP, UDP, Any). Select **Add Filter** to apply your changes.
NAT Tab Used to define NAT (Network Address Translation) rules.	
Name/Source IP/Dest. IP	Lists current filters by name, source IP, destination IP, destination port, and protocol.
Remove Existing Filters	Select the Delete box checkbox next to the filter to delete, then select **Delete Existing Filters**.
Add New Filter	In the Name field, specify the filter name. In the Source IP field, specify the source IP. In the Destination IP field, specify the destination IP. In the Destination Port field, specify the destination port. From the Protocol drop-down list, select the protocol to be allowed (TCP, UDP, Any). Select **Add Filter** to apply your changes.

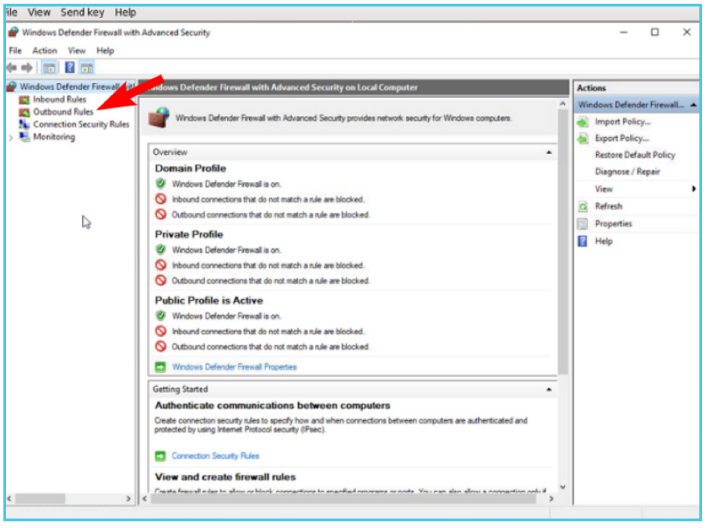
Enable outgoing communication for a port through the Windows Firewall

Complete the following steps using the siteadmin account inside the Windows environment.

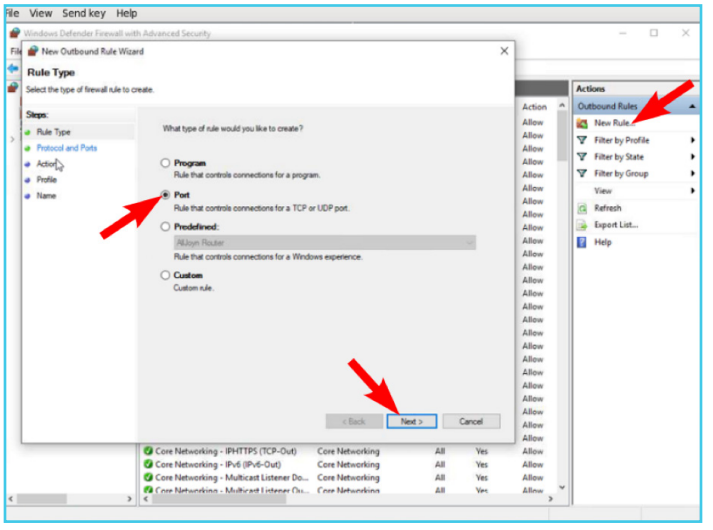
1. Open Search box, type **Firewall**.
2. Select **Open** to launch Windows Defender Firewall Popup.



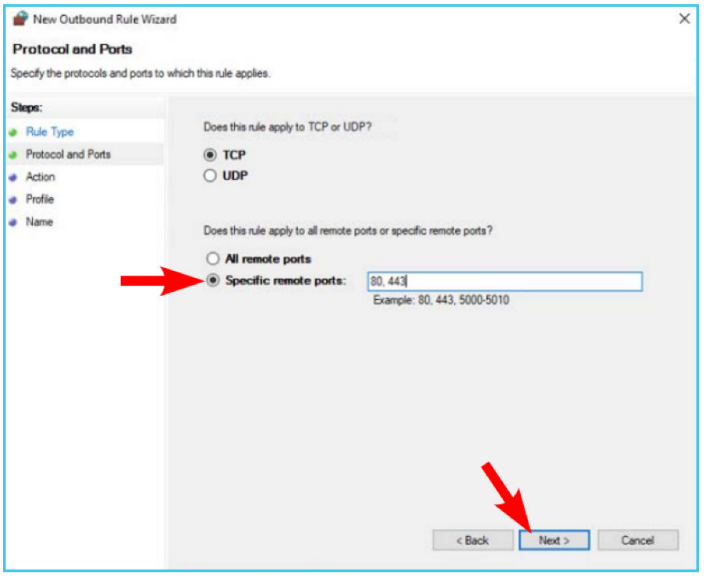
3. Select Advanced Settings > Outboard Rules in the left hand pane



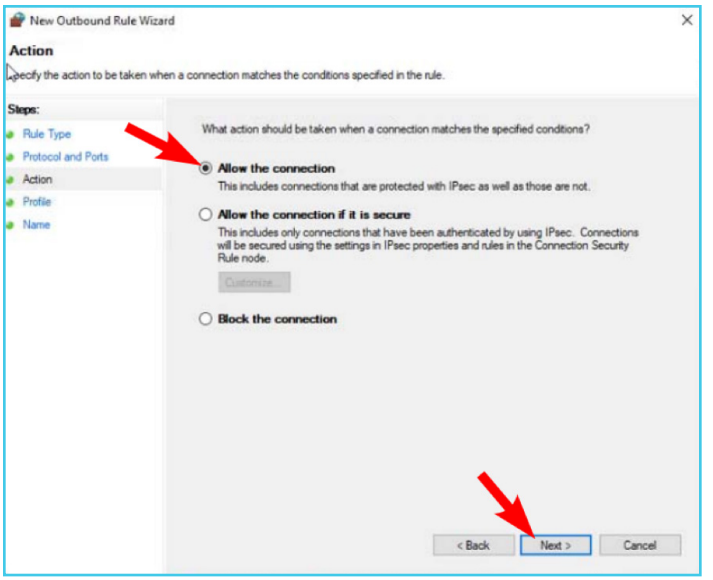
4. Select **New Rule** in the right-hand pane
5. Select **Port**, then click **Next**



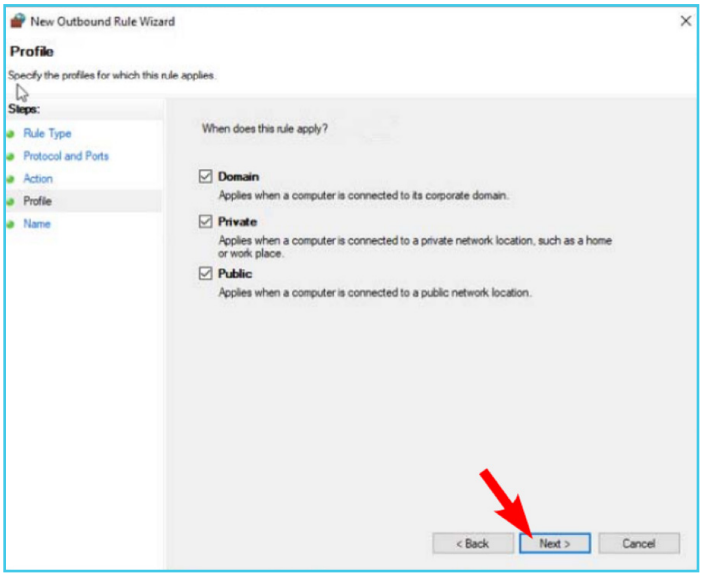
6. At **Specific remote ports**, type the port number to be opened in the text box. Click **Next**



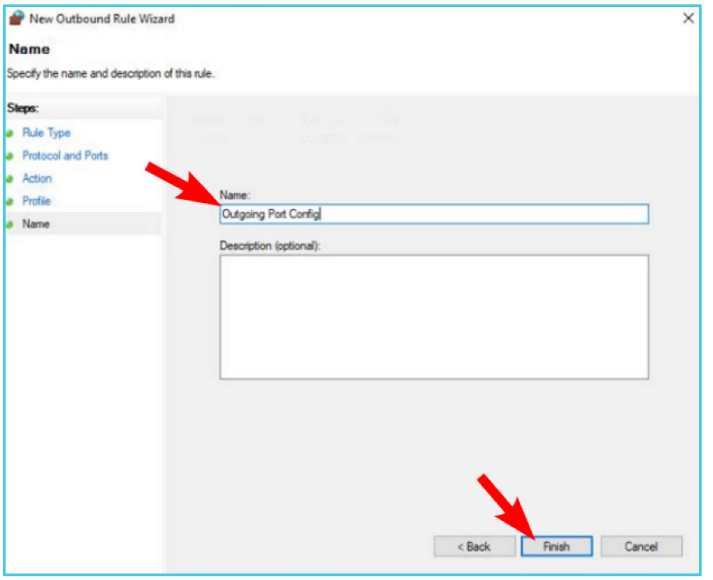
7. Select **Allow the Connection**, then click **Next.**



8. Make no changes to the **When does this rule apply** screen. Click **Next.**



9. Add a descriptive name to the **Name:** text box. Click **Finish**



10. Verify the Port name created appears in the **Outboard Rules** list.
11. Close all popups and return to the desktop.
12. Select the Windows Start icon, select shutdown.
13. Windows will automatically close and return to worklist.

Troubleshooting Guide

CAN'T CONNECT TO NETWORK FROM WINDOWS

Can the X-ray system connect to the network using C-Echo or worklist queries?

- **NO** → Troubleshoot X-ray system connectivity
- **YES** → Does the site require a proxy to be configured?

Configure the proxy in Internet Explorer.

Internet Options > Connections > LAN Settings.

If the proxy uses a port other than 80 or 443, this will need to be allowed through the firewall. Some sites will also require proxy exceptions for local addresses. These can be added in the advanced menu.

YES ←

Can you ping an internal IP address from the windows command line?

NO ←

- **NO** → Test the same ping command in the X-ray system command line to determine if it can be accessed from there.

  If not, troubleshoot X-ray system connectivity to that IP.
- **YES** → Can you ping an internal URL from the command line?

Check application configuration. Windows is able to access the internal network

YES ←

Configure the DNS server in Windows

Control Panel > Network and Internet > Network and Sharing Center > Change adapter settings

NO ←

CAN'T CONNECT TO HIS/RIS OR PACS

Is your HIS/RIS or PACS on the same network as the system?

- **NO** → Determine if there is a network which can access both. The X-ray system can only connect to one network.
- **YES** → Is your HIS/RIS or PACS on the same network as the system?

Can you load websites in Internet Explorer that you would expect to be able to access?

YES ←

- **NO** → Attempt troubleshooting in "Can't connect to network from Windows" flow.
- **YES** → Try connecting with Windows and X-ray system firewalls disabled. If this resolves the issue, you will need to open additional ports in the firewall. For instance, Centricity Universal Viewer Zero Footprint requires port 28818 to be opened.

  If you have a computer check its firewall configuration to determine which ports these should be.

November 2021
JB18311XX
DOC2645980