All Information provided in this document and in the accompanying software is subject to change without notice and does not represent a commitment on the part of RamSoft. RamSoft assumes no responsibility for any errors or consequential damages that may result from the use or misinterpretation of any information in this document. No part of this document may be reproduced in any form or by any means, electronic or mechanical, including photocopying and recording, for any purpose without the express written permission of RamSoft.

MANUFACTURER
RamSoft Incorporated
700 – 60, Adelaide St E
Toronto, ON M5C 3E4
CANADA
Toll Free: (888) 343-9146
Phone: (416) 674-1347
Fax: (416) 674-7147
Email: support@ramsoft.com
Web Site: http://www.ramsoft.com

RamSoft®, RamSoft PACS™ are registered trademark of RamSoft Inc.
PowerServer™, PowerReader™, PowerCache™ and Gateway™ are registered trademarks of RamSoft Inc.
Microsoft® and Windows® are registered trademarks of Microsoft Corporation.
M*Modal Speech Understanding™ is a registered trademark of MModal IP LLC.
Dragon Medical® is a registered trademark of Nuance Communications, Inc.
RamSoft Gateway Router 6.0 Quick Start Guide

Contents

1 EXECUTIVE SUMMARY ........................................................................................................ 4
2 RECOMMENDED SYSTEM REQUIREMENTS ........................................................................ 4
   2.1 Less than 30,000 studies per year ................................................................................ 4
   2.2 More than 30,000 studies per year ............................................................................... 5
3 STEPS TO A QUICK START .................................................................................................. 6
   3.1 Installation ..................................................................................................................... 6
   3.2 Maintenance Settings ..................................................................................................... 6
   3.3 Gateway Router Configuration .................................................................................... 8
   3.4 Configuring Other DICOM Stations ............................................................................. 10
   3.5 Simple Routing Rule Trigger Setup & Example .......................................................... 10
4 SETTING UP A SECURE DICOM COMMUNICATION ....................................................... 12
1 EXECUTIVE SUMMARY

This guide is meant to help the users with setting up and starting a RamSoft Gateway Router 6.0.

2 RECOMMENDED SYSTEM REQUIREMENTS

2.1 Less than 30,000 studies per year

**Required**

<table>
<thead>
<tr>
<th>Hardware Requirements</th>
<th>Recommended Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Microsoft Windows 10 Pro (64-Bit)</td>
</tr>
<tr>
<td>CPU</td>
<td>Recent CPU (less than 5 years old) with at least 4 Cores</td>
</tr>
<tr>
<td>RAM</td>
<td>8 GB</td>
</tr>
<tr>
<td>Hard Drive(s)/Primary Storage</td>
<td>RAID1, 2 x 500 GB Hybrid HDD, Database and Image storage sized appropriately</td>
</tr>
<tr>
<td>Network Bandwidth (LAN)</td>
<td>1,000 Mbps</td>
</tr>
</tbody>
</table>

**Software Requirements**

<table>
<thead>
<tr>
<th>Software</th>
<th>Recommended Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus</td>
<td>Windows Defender</td>
</tr>
<tr>
<td></td>
<td>AVG Antivirus Business Edition</td>
</tr>
<tr>
<td></td>
<td>AVG CloudCare</td>
</tr>
<tr>
<td>Remote Access</td>
<td>LogMeIn will be supplied by RamSoft for the exclusive use of RamSoft Support.</td>
</tr>
</tbody>
</table>

**Optional**

<table>
<thead>
<tr>
<th>Software</th>
<th>Recommended Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard Drive Imaging</td>
<td>Windows Backup</td>
</tr>
<tr>
<td>Server Monitoring</td>
<td>LogMeIn Pro</td>
</tr>
</tbody>
</table>
2.2 More than 30,000 studies per year

## Required

<table>
<thead>
<tr>
<th>Hardware Requirements</th>
<th>Recommended Hardware</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>Windows Server 2016 Standard with Hyper-V</td>
</tr>
<tr>
<td>CPU</td>
<td>Recent CPU (less than 5 years old) with at least 4 Cores</td>
</tr>
<tr>
<td>RAM</td>
<td>8 GB</td>
</tr>
<tr>
<td>Hard Drive(s)/Primary Storage</td>
<td>RAID1, 2 x 500 GB Hybrid HDD, Database and Image storage sized appropriately</td>
</tr>
<tr>
<td>Network Bandwidth (LAN)</td>
<td>1,000 Mbps</td>
</tr>
</tbody>
</table>

## Software Requirements

<table>
<thead>
<tr>
<th>Software</th>
<th>Recommended Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Antivirus</td>
<td>AVG Antivirus Business Edition</td>
</tr>
<tr>
<td></td>
<td>AVG CloudCare</td>
</tr>
<tr>
<td>Remote Access</td>
<td>LogMeIn will be supplied by RamSoft for the exclusive use of RamSoft Support.</td>
</tr>
</tbody>
</table>

## Optional

<table>
<thead>
<tr>
<th>Software</th>
<th>Recommended Software</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hard Drive Imaging</td>
<td>Windows Backup, Veeam Backup &amp; Replication (for Hyper-V)</td>
</tr>
<tr>
<td>Server Monitoring</td>
<td>LogMeIn Pro</td>
</tr>
</tbody>
</table>
3 STEPS TO A QUICK START

Increase productivity and maximize your resources in your fast paced medical imaging facility. RamSoft Gateway Router offers the features required to meet the present and future demands of an increasingly demanding operating environment.

3.1 Installation

2. At the Install Shield Wizard welcome screen, click Next.
3. Click the radio button “I accept the terms in the license agreement.” Click Next.
4. Type in the User Name and Organization. Click Next.
5. For the Database, Image, and Destination folders, use the default folder and click Next.
6. Click Install to begin the installation.
7. When the Install Shield Wizard has completed, click Finish.
8. When prompted to restart, click Yes.

3.2 Maintenance Settings

1. Launch the RamSoft PACS Maintenance application.

3. If you are on the evaluation version, a popup is displayed requesting you to either Purchase, Activate or use the Evaluation version. Make your selection.
4. When prompted for the Password, type in “@admin4M@int”.
5. Go to Communication > DICOM > DICOM Configuration.
6. Type in the appropriate Local Station Name and Local AE Title.
7. If you do not wish to accept DICOM connections with all stations, uncheck the Allow receiving without verifying AE Title credentials (Promiscuous Receiving) option.
8. The RamSoft Software requires the AE title and Station Name to communicate with other DICOM stations. However, if you do not wish to define the Station Name and AE Title, then the Promiscuous Receiving option should be enabled. Enabling this option allows the RamSoft software to communicate with all DICOM devices.

**Warning:** It is not recommended to enable Promiscuous mode for DICOM communication with other devices for a prolonged period of time. This mode should be only used for testing purposes.

9. Go to **Services > Local Services > Restart**.
10. After the services have been restarted, click **OK**.
11. Close the **Maintenance** module.

### 3.3 Gateway Router Configuration

1. Double-click the **Gateway Router 6.0** shortcut on the desktop.
2. A form will be displayed requesting you to either purchase, activate or use the evaluation version. Make your selection.

![Gateway Router 6.0 Form](image)

3. When prompted for the **User Name** and **Password**, type in “**ADMIN**” and “@dmIn4PS”.
4. Go to **Settings > Password**.
5. Type in the **Old Password** “@dmIn4PS” and type in the desired custom password and confirmation. Click **OK** to commit changes.
6. Go to **Settings > Server Settings > Station List**.
7. In the Station List window, click **New Station**.
8. Type in the Station, IP Address, Port, and AE Title of the station you are going to connect with. This will be known as the **Second Station**.

9. Click Test Connection to test the connection.
10. Click Apply to commit changes and click OK again to close the window.
3.4 Configuring Other DICOM Stations

1. Launch the other DICOM station to which the Gateway router is to be connected.
2. Enter the Station, IP Address, Port, and AE Title of the Gateway Router.
3. Click the Test Connection button to ensure the DICOM connection succeeded.
4. Click OK to close the pop-up and click OK to close the window.

3.5 Simple Routing Rule Trigger Setup & Example

1. Go to Settings > Server Settings > Workflow.
2. By default, the Triggers tab appears.
4. Select the appropriate Rule Name, Status (after COMPLETED), Modality, and Body Part from the drop-down lists. The % symbol represents all selections.
5. Type in the appropriate Facility, Reading Physician, Referring Physician, and Origin AE Title. Click Save to commit changes.
7. Under the Destinations tab, click New.
8. Under Type, select Dicom/Replication Station.
9. Under Destination, select name of the second station. Click Save to commit changes.
10. Click OK to close the window.
11. Launch the other DICOM station (the one you wish to connect the Gateway Router with).
12. Create or modify a patient (e.g. Last name: GATEWAY, First name: ROUTER).
13. Enter the **Facility, Reading Physician, and Referring Physician** as entered in Step 5.
14. Modify the study **Modality and Body Part** to the ones in Step 4.
15. Send the study to the **Gateway Router**.
16. Go to the **Gateway Router. Search for the patient study and open the Study Information form**. Verify that the study information is the same (the Status may be different).
17. Change the Status to the Status in Step 4. Click **OK** to commit changes and close the window.
18. Go to **Settings > Logs > Communication**. Under the Transmit Log tab, under Pending, verify that the study has been placed in the queue.
19. Once transmission has been completed, go to the other DICOM Station. Search for the patient study and double-click to open the study. Verify that the patient, study information and the images are correct.
20. Close the study.
4 SETTING UP A SECURE DICOM COMMUNICATION

Gateway Router allows encrypted DICOM communication using TLS encryption. DICOM communication encryption and authentication is done through SSL keys and certificates. By providing each machine with a copy of the public certificate, the need for using a third party Certificate Authority is eliminated, making this a fully secure authentication system where the only concerned parties are the two machines performing a DICOM transaction.

**Note:** TLS communication should only be set up if DICOM communication is taking place across an unsecured channel, such as the Internet. If the DICOM machines are all enclosed within a secure Local Area Network or a VPN, TLS does not need to be setup as it is not necessary.

The following procedure describes the setup of a secure DICOM communication:

1. Go to `%\RamSoft\GatewayRouter\Tools`.
2. Execute Makecert.bat in Command Prompt.
3. Enter the prompted information.
4. The utility will create a private key (pacs.key) and a public certificate (pacs.crt); both are placed in the tools directory.
5. Place the certificate (pacs.crt) in the `%\RamSoft\GatewayRouter\Certificates` folder on every machine that will be involved in the DICOM communication. This eliminates the need for a Local Certificate Authority.
7. Go to **Communication > Dicom > Dicom Configuration**.
8. Point the certificate field to the pacs.crt file that was created.
9. Point the key field to the pacs.key file that was created.
10. Point the Peer Certificates field to the Certificates folder.
11. Click OK.
12. DICOM Services should be restarted at this point at Services > Local Services > Restart
14. Go to Settings > Server Settings > Station List.
15. Change the default unencrypted port 104 to the TLS encrypted port 2762 for the station you wish to connect to.

**Note:** For each station in the list, the default unencrypted port is 104 and the default TLS encrypted port is 2762.

15. Select the DICOM tab.
16. For each station using encryption, enable the Encrypt Data (TLS) option.
17. Click on the Test Connection button.
18. If the steps above have been followed properly, the communication should be successful.