COMPULINK

advantage™

Software Installation, Configuration, and Performance Guide for Windows®

compulink

Sales: 800.456.4522 | Support: 805.716.8677

Contents

PREFACE

This document contains networking, hardware, security and configuration information for running Compulink Advantage products in a Client/Server environment. IT Administrators should review and refer to this document to ensure effective performance of Compulink Advantage software. This document may be updated as information is updated, please visit our IT Support site for this document's Revision Date to ensure you have the latest version.

PRE-REQUISITES

A Certified Network Professional, if not provided by **Compulink**, must install, be readily available and administer your network prior to, during and following your **Compulink** training. Installation and operability must include the following:

• Recommended minimum network hardware resources, e.g., servers, workstations, network appliances (routers and switches), scanners, printers, etc.

• Operational TCP/IP configured network, configured network user accounts for access to shared resources, workstations connected to shared resources on file server.

HARDWARE MINIMUM REQUIREMENTS

NOTE: The Charts below are only minimum system requirements, enhancements to these requirements will boost performance depending on the number of workstations, overall system and network configuration. If in doubt, check with your IT consultant or **Compulink** IT support staff at (800) 888-8075.

Minimum Requirements: 1 to 9 users

SERVER		
	Minimum	**Recommended**
Processor	Intel Dual Core or higher	Intel Core i3 or higher
(Processor speed will vary based on availability and office needs)		
Storage	80 GB SATA – 7200 RPM	250 GB SATA – 7200 RPM+ RAID 1 or 5 *
(Storage needs are based on office requirements. Contact IT Support for assistance)		
Memory	8 GB RAM	16 GB RAM
(Amount of RAM or memory varies based on number of workstations and other server tasks – This amount may increase with added EHR functions)		
Operating System	• Windows 8 Pro, 8.1 Pro • Windows 10 Pro, 11 Pro	• Windows 2012/R2 Foundation • Windows 2012/R2, 2016, 2019, 2022

Minimum Requirements: 10 to 25 users

SERVER		
	Minimum	**Recommended**
Processor	Intel Dual Core or higher	Intel Core i5 or higher
(Processor speed will vary based on availability and office needs)		
Storage	250 GB SATA – 7200 RPM	500 GB SATA – 7200 RPM+ RAID 5 or 10[1] *
(Storage needs are based on office requirements. Contact IT Support for assistance)		
Memory	16 GB RAM	24 GB RAM
(Amount of RAM or memory varies based on number of workstations and other server tasks – This amount may increase with added EHR functions)		
Operating System	• Windows 2012/R2, 2016, 2019, 2022	• Windows 2012/R2, 2016, 2019, 2022

Minimum Requirements: 25 to 50 users

SERVER		
	Minimum	**Recommended**
Processor	Intel Core i3 or higher	Intel Xeon or Dual Xeon
(Processor speed will vary based on availability and office needs)		
Storage	500 GB SATA – 7200 RPM	1TB SATA - 7200 RPM+ - RAID 5 or 10[1] *
(Storage needs are based on office requirements. Contact IT Support for assistance)		
Memory	24 GB RAM	32 GB RAM or higher
(Amount of RAM or memory varies based on number of workstations and other server tasks – This amount may increase with added EHR functions)		
Operating System	• Windows 2012/R2, 2016, 2019, 2022	• Windows 2012/R2, 2016, 2019, 2022 • *A Redundant/Test Server*

Minimum Requirements: 50 to 100 users

SERVER		
	Minimum	**Recommended**
Processor	Intel Xeon	Intel Dual Xeon
(Processor speed will vary based on availability and office needs)		
Storage	1000 GB SATA – 7200 RPM+	2000 GB SATA - 7200 RPM - RAID 5 or 10[1] *
(Storage needs are based on office requirements. Contact IT Support for assistance)		
Memory	32 GB RAM	48 GB RAM+
(Amount of RAM or memory varies based on number of workstations and other server tasks – This amount may increase with added EHR functions)		
Operating System	• Windows 2012/R2, 2016, 2019, 2022	• Windows 2012/R2, 2016, 2019, 2022 • *A Redundant/Test Server*

Minimum Requirements: +100 users

SERVER		
	Minimum	**Recommended**
Processor	Intel Dual Core or higher	Intel Xeon Dual/Quad Core or higher
(Processor speed will vary based on availability and office needs)		
Storage	2000 GB EIDE – 7200 RPM	3000 GB SATA – 7200 RPM – RAID 10 *
(Storage needs are based on office requirements. Contact IT Support for assistance)		
Memory	48 GB RAM	64 GB RAM
(Amount of RAM or memory varies based on number of workstations and other server tasks – This amount may increase with added EHR functions)		
Operating System	• Windows 2012/R2, 2016, 2019, 2022	• Windows 2012/R2, 2016, 2019, 2022 • *A Redundant/Test Server*

Minimum Requirements: Server and Workstation

WORKSTATION		
	Minimum	**Recommended**
Processor	Intel Dual Core or higher	Intel Core Duo or higher
(Processor speed will vary based on availability and office needs)		
Storage	40 GB SATA	*120+ GB SSD
(Storage needs are based on current market availability and office needs)		
Memory	4 GB of SDRAM	8 GB of SDRAM
(RAM or memory requirements may vary based on number of tasks and applications)		
Operating System	Windows 8 Professional *(non-professional versions may be used in peer-to-peer networks)*.	• Windows 8 Pro, 8.1 Pro, 10 Pro, 11 Pro
SERVER and WORKSTATION Components		
Display	WSXGA Adapter or 1600 x 1024 or higher with minimum 16 bit Colors	WSXGA Adapter or 1600 x 1024 or higher with minimum 16 bit Colors
Network	100 Mbps Ethernet Network Interface Card (NIC) – Small Workgroups ONLY	1000 Mbps Ethernet Network Interface Card (NIC) (Link aggregation and NIC teaming is recommended for large networks)
Supported Peripherals		
For a list of recommended peripherals, please visit our Recommended Peripherals page. If asked for login credentials, ask your COMPULINK representative for access.		

SSD drives are recommended for performance enhancements, although more costly

[1]RAID 10 is the best option for critical databases, although more costly

NOTE FOR LARGER SYSTEMS: For high availability, virtualization technology and Storage Area Networks are highly recommended by **Compulink**. It is also recommended that clients with a **large number of users** install and maintain a **redundant/test server** in their environment. The redundant server can be utilized for beta testing software upgrades prior to installation on the production server and serve as a redundant server in case the main production server is unavailable.

NETWORK APPLIANCE

Compulink recommends SonicWall or Sophos routers for Internet, VPN and Remote Desktop services connections.

MOBILE DEVICES AND SUGGESTED WIRELESS SOLUTION

Compulink Advantage software has been tested and proven compatible with Tablets, Notebooks and Desktops using wireless connectivity while utilizing Terminal Services or Remote Desktop technology **ONLY**.

Wireless connections with direct connectivity to the Wireless Local Area Network (WLAN) are not supported. Clients can implement such solution at their own risk. Implementing a wireless connection from the station hosting the databases and another station on the network could cause delay in packet delivery and result in performance issues, database disconnections and data corruption. The use of Windows Terminal Services, and similar products available from proprietary vendors, such as Thinstuff, are necessary with low bandwidth environments.

Apple iPad - **Compulink Advantage** software supports the use of Apple devices such as iPad in RDP or Terminal Services mode **ONLY**. The use of proprietary applications such as Microsoft RDP client for iOS may be necessary to provide certain Windows functionalities such as 'right-click' in this type of environment.

Android Devices - **Compulink Advantage** software supports the use of Android devices in RDP or Terminal Services mode **ONLY**. The use of proprietary applications such as Microsoft RDP client for Android may be necessary to provide certain Windows functionalities such as 'right-click' in this type of environment.

NETWORK OPERATING SYSTEMS

Compulink Advantage has proven compatibility with the following 32 and 64 bit Network Operating Systems:

Windows 8 and 8.1 Pro and Enterprise
Windows 10 Pro and Enterprise
Windows 11 Pro and Enterprise
Windows 2012 R2, Windows 2016,
Windows 2019, Windows 2022

- **Compulink Advantage** software has been tested and is compatible with **Citrix Metaframe** using Windows Server environments.
- Using the compatible Operating Systems listed above is required on all workstations. Installation of Windows NT SERVER, Windows 2000, Windows Millennium (ME) or Windows 98, Windows XP, Windows 7, and Windows Server 2003 is NOT supported on any server or workstation. Clients with existing **Windows Home** versions may use these operating systems only as a workstation and not in an Active Directory domain environment.

COMPULINK does **NOT** install, recommend or support any versions of **Novell Netware**, **Linux** or **MAC OS** on the server or workstations and does not guarantee compatibility or reliability with any of **Compulink Advantage** products in these environments.

MAC OS
Compulink Advantage software only runs in a Windows environment. MACs can be used only by accessing a Windows Operating System through Terminal Services or Virtual Windows PC. Customer support is only available for troubleshooting the Terminal Services session environment. Compulink recommends using Microsoft RDP Client for MAC for accessing your terminal server(s).

INSTALLATION OF COMPULINK ADVANTAGE SOFTWARE (GENERAL)

Compulink Advantage software for Windows is installed using the Internet and **Compulink**'s remote connection/assistance software. Your Implementation Coordinator will deliver the necessary files electronically, install and test the product on your server or any available station.

In some cases, the software may be installed in the root of the "C" drive by your Implementation Coordinator. This may be due to time constraints or lack of access to an IT professional. Sharing the C: drive, operating system and program files, and other sensitive documents is not recommended. It is important that our clients designate an exclusive partition or directory ***other than the Boot Partition*** for the **Compulink** files and folders. The contents of this partition/directory are shared and will be available to all **Compulink Advantage** users with read/write access.

Once the installation has been completed, a shortcut will be created on the desktop to launch the **Compulink Advantage** software. Please see **SETUP INSTRUCTIONS FOR COMPULINK ADVANTAGE SOFTWARE** for details.

To confirm the successful installation and operation of **Compulink Advantage** software, log into the software with the username and password (provided by Compulink staff) and run diagnostics using the Utility menu. In most cases your Implementation Coordinator will assist you with this process.
NOTE: Compulink Advantage software database directory (i.e. EYECARE, EYEMD, CHIRO, PT, CBSMAIL, etc.) does not edit the Windows registry and can be moved/copied without the need for reinstallation. **Compulink**'s database management software by **SAP** DOES edit the Windows registry and has to be reinstalled with assistance from **Compulink**'s support staff or instructions available online.
Instructions for downloading, installing and configuring the **Advantage DataBase Server** can be found on page 3 of the Server Migration and Advantage Database installation document.

DRIVE SHARING

In a Peer-to-Peer or client/server environment, one computer will act as the file server. This will be the computer where your **Compulink Advantage** software files and databases will be installed.
The hard drive, partition or folder that contains the **Compulink Advantage** software on this machine must have Read/Write permissions for EVERYONE (or any designated group using the software). We recommend giving FULL Control permission for EVERYONE initially for testing. When full functionality is confirmed, permissions can be reduced to Read/Write. SYSTEM must also be given "Full Control" in the security properties of the folder.
Do not share the folder that contains the **Compulink Advantage** files, i.e. EYECARE or EYEMD, PT, PSYCH, etc. Share only the root of the directory or partition where these folders reside. Multiple copies or copies saved on workstation local hard drives can possibly cause system errors. DO NOT Place the product folder in a directory with the same name (e.g. C:\eyecare\eyecare\eyecare.exe).

COMPUTER NAMES and SHARE NAMES

SERVER NAMES **CANNOT** contain spaces, (i.e., COMPULINK SERVER). The proper naming would be "COMPULINKSERVER" or "SERVER".

DIRECTORY SHARED NAMES

SHARED NAMES **CANNOT** contain spaces or hyphens (-), (i.e. COMPULINK SHARE or COMPULINK-SHARE). The proper naming would be, "COMPULINK" or "COMPULINK_SHARE". For ease of support, Compulink recommends using "COMPULINK" as the shared name. The use of hidden shares (e.g. COMPULINK$) is also recommended to help protect against malware that may spread through network shares.

SETUP INSTRUCTIONS FOR COMPULINK ADVANTAGE SOFTWARE

WINDOWS SERVER ENVIRONMENT SETUP

For Multi-User environments and after the initial electronic installation, Compulink recommends moving the product directory (i.e. EYECARE, EYEMD, CHIRO, PT, etc.) to a directory named "**COMPULINK**".
CAUTION: Do not use the product name (i.e. EYECARE, EYEMD, CHIRO, PT, Psych, etc.) for the root directory name. For supporting the product, Compulink recommends using **COMPULINK** as the root directory name.
Root Directory or **COMPULINK** directory can be created on any available local drive with sufficient storage space. ***Using the boot partition is not recommended***. Share this directory as **"COMPULINK"** (or **"COMPULINK$"** for hidden shares) for easy identification. The **COMPULINK** share must have Read/Write permissions for EVERYONE or a designated group using the Compulink Advantage software (e.g. Domain Users or Compulink Group). SYSTEM must also be given Full Control of this share in the Security properties of the folder. Once the proper share has been created, all stations, including the server, will launch the software utilizing this share.
CAUTION: Do not share the product folder. Only the root folder should be shared. The incorrect path will prohibit the launch of the software.

HIDDEN SHARE RECOMMENDED

Due to the wide spread of advanced malware, Compulink recommends using a hidden share. Utilizing a hidden share may offer some protection against malware, such as the CryptoLocker.

WINDOWS WORKSTATION ENVIRONMENT SETUP

On all workstations' desktops, create a shortcut using UNC (Universal Naming Convention) to the product's Executable file.
PLEASE NOTE: **Compulink Advantage** software is launched by running an Executable file through UNC. When creating a shortcut, the **Target** and **Start in** should be through the IP address UNC. This also applies to all users utlizing Remote Desktop sessions on a Windows Server.

Example: **Target:** \\SERVER_IP\sharename\eyecare\eyecare.exe
Start in: \\SERVER_IP\sharename\eyecare\
Hidden share: **Target:** \\SERVER_IP\sharename$\eyecare\eyecare.exe
Start in: \\SERVER_IP\sharename$\eyecare\

THIRD PARTY SOFTWARE REQUIREMENTS AND OPTIONS

Required:
Crystal Reports Runtime: Required - installation file: CR11SETUP.EXE included in the product folder.
Copy the file to the local workstations and run it to install Crystal Reports Runtime.
Adobe Reader: required for creating and printing PDF reports

Optional:

Open Office Writer: Required for merging ODT documents and templates
Also required for Signature Pad interface and other functions.
Libre Office Writer: Required for merging ODT documents and templates
Also required for Signature Pad interface and other functions.
Microsoft XPS Writer print driver: Optional for testing and printing to XPS documents.
***Microsoft WORD versions:** Due to legal issues, Microsoft disabled XML integration features from WORD 2007 and later products. **Compulink** now recommends **OpenOffice Writer or Libre Office Writer**, free and available for download from http://download.openoffice.org/, or https://www.libreoffice.org/download/download/ for all Advantage software data merge processes.

ENVIRONMENT VARIABLE SETTING (AKA SET STATEMENT)

Compulink Advantage software utilizes the Environmental Variables settings in the System Properties to add a unique environment/ID for each user accessing the software. These are also referred to as "**SET STATEMENTS**." Create a new variable using "CBS" as the Variable Name (without the quotation marks). For Variable Value type "X" (without the quotation marks). "X" represents a sequential alphabetical ID based on the number of Compulink licenses purchased Alternatively, clients on version 12.1 or higher can use the variable "COMPULINK" with a number as the value. In this case, instead of CBS=A, you'd use COMPULINK=1. (i.e., five licenses will allow the use of IDs ranging from A-E. or 1-5 using the COMPULINK variable)

Windows 8/2012 and Windows 10/11/2012R2/2016/2019/2022
To access the Environment Variables, navigate to the control panel, double click the system icon (classic/small icons view), choose the Advanced System Settings in the menu and click on the Environment Variable button under the Advanced tab. To add a Global environment variable, use the SYSTEM Variable (recommended on workstations). To add a User environment variable, use the USER variable. (recommended in terminal server environments.)

GENERAL ENVIRONMENTAL SETTING
THE VARIABLES MUST BE TYPED IN CAPITAL LETTERS. Should your network exceed 26 workstations, use sequential double alpha IDs, beginning with AA for the 27th workstation, AB for the 28th, etc. It is important to assign the double alpha IDs in consecutive order within the range "AA to RZ".

For assistance with assigning variables in environments with a large number of clients, **Compulink**'s IT department has designed scripts that will generate and assign variables based on workstation/client names, locally and remotely. Please contact **Compulink**'s IT department at (800) 888-8075 for additional information regarding this solution.

CONCURRENT (DYNAMIC) LICENSING
CAUTION: It is **extremely important** that the proper licensing model is determined and implemented by the network administrator prior to the client's go-live date or access to the **Compulink Advantage** software on all stations may not be possible.

Starting with **Compulink**'s version 9.5, license verification has been updated and can be determined by the number of active network users rather than number of terminals and workstations. Clients with mobile staff members and more workstations than staff members can purchase licenses according to the number of active Compulink users. With concurrent (dynamic) licensing, workstations no longer need to be identified by a unique CBS environmental variable (see exception list below). A dynamic license will be assigned once the **Compulink Advantage** software is launched.

Stations with any of the following items must be assigned a unique "CBS" or "Compulink" environment variable and use Static licensing for proper operation.

- Cash Drawer
- Local or remote Twain Interface devices such as cameras and scanners
- Workstation Name identified for Patient Tracking
- Any equipment interface/hand-off to 3rd party software requiring workstation setup
- DYMO LabelWriters that print Chart Labels from Compulink
- Compulink Cloud

Note: Static licenses assigned to workstations due to the above requirements will NOT be available in the concurrent licensing pool. Such environments must use the hybrid (static and dynamic) licensing model. Refer to Licensing Setup and Troubleshooting (PDF) on Compulink's support site.

HARDWARE INFORMATION - MISCELLANEOUS

SYSTEM AND HARDWARE REQUIREMENTS

Compulink Advantage software does not require specific hardware or computer systems and will function over most current versions of Windows-based operating systems (see Network Operating Systems) and Windows-based compatible hardware.

RECOMMENDED COMPUTER ROOM TEMPERATURE AND HUMIDITY

Monitoring the environment in a computer room or data center is vital to ensuring uptime and system reliability. Maintaining recommended temperature and humidity levels in the area where computer systems are placed can increase uptime.
Maintaining an ambient temperature range of 68° to 75°F (20° to 24°C) is optimal for system reliability. This temperature range provides a safe environment for equipment to operate in the event of air conditioning or HVAC equipment failure.

Relative humidity (RH) is a term used to describe the amount of water vapor that exists in a gaseous mixture of air and water vapor. In a data center or computer room, maintaining ambient relative humidity levels between 45% and 55% is recommended for optimal performance and reliability.

CABLING

Minimum of Category 5 or 5e Balanced 100 Ω cable and associated connecting hardware whose transmission characteristics are specified up to 100 MHz.
For best performance, 1000 Mbps (1GB) bandwidth from the file server to the switch is recommended. **Compulink** does not supply, install or contract with any network cable installers. It is necessary that a professional and capable cable installer install your network cable prior to the arrival of your computer systems and your **Compulink** Trainer.

ELECTRICAL

Power fluctuation and outages are common; **Compulink** recommends the use of UPS (Uninterruptible Power Supply) on file servers and systems that store your data. Surge protectors are recommended for workstations.
Standard Electrical Requirements: 2 standard electrical duplex receptacles (1 circuit per 2 workstations) - maximum of (24) receptacles per circuit

BATTERY BACKUP (Uninterruptible Power Supply)

Uninterruptible power supply units are important for equipment that could be damaged in a power failure. In any business environments with a network application such as **Compulink Advantage** software, networking equipment could also benefit from being on an uninterruptible power supply, as a lack of power to network equipment could prevent communication.
An uninterruptible power supply can ensure that electronic equipment remains operational even if external power was unavailable. It also reduces the chance that a power outage could corrupt data on a server. An appropriate backup power solution is highly recommended for use with **Compulink Advantage** software.

PERMISSIONS

Whether you are using Windows built-in groups or a new group created by the administrator, users of **Compulink Advantage** software must be granted **Read/Write** access to the share where the application resides. It is recommended to grant **FULL Control** to user initially for testing. If there are no issues with functionality, FULL control may be restricted. If security is an issue, the network administrator can place restriction on all other shares on the network while granting **Compulink Advantage** users Read/Write access to the product's parent share (the COMPULINK folder). The share can be hidden ($) to enhance the security, if desired.

PRINTERS

Compulink Advantage software utilizes printers that are properly setup in the Windows environment. A Test Page should be printed from within the Properties Sheet for that printer to confirm the printer's functionality prior to printing from **Compulink Advantage** software.
Some all-in-one (multi-function) INKJET printers/scanners are not compatible with **Compulink Advantage** software. **Compulink Advantage** software has been tested successfully with the HP LaserJet and Dell Laser Black and White business printer line. It is recommended that basic printer driver language, such as PCL5 drivers are used. Postscript and PCL6 drivers may cause printing issues in **Compulink Advantage** software. For generating labels, **Compulink Advantage** software has proven compatibility with Dymo Labelwriter series.

WIDE-AREA-NETWORK CLIENTS: Not all printers are compatible with Terminal Services and RDP protocol. Please consult the printer manufacturer's documentation (see Remote Printing).

SCANNING AND IMAGES - TWAIN LAN AND WAN DEVICES

Compulink Advantage software utilizes TWAIN compliant devices to capture and transfer images/data to the various sections of the patient's demographic screen or medical records. In most cases, the devices with a TWAIN data source file or ".ds" extension located in Windows "TWAIN_32" directory will enable **Compulink Advantage** software to acquire images from a TWAIN compliant device.

Due to the wide variety of devices and their associated drivers available on the market, it is impossible to guarantee which devices/peripherals will successfully work with Advantage software. **Compulink** recommends the use of peripherals that are tested and researched by our IT lab. Visit Recommended Peripherals for details.

Wide-Area-Network: Third-party remote scan solution such as TS SCAN from TerminalWorks is recommended for WAN environments. Multi-page scanning is ONLY supported in wide-area-network environments with the use of third-party remote scanning solutions, regardless of operating system. Clients may also utilize various third-party solutions such as Paperport to export images as Multi-Page TIFF or PDF and use the import function in the Patient Demographic screen. Contact **Compulink**'s IT department for any additional details.

TIME SYNCHRONIZATION

Time is critical for transactions across computer networks. Synchronizing a network time is performed using the Windows Time Service, also known as W32Time. The Windows Time Service was implemented in compliance with the Kerberos authentication protocol and with system clock synchronization following (RFC) 1305 Network Time Protocol Version 3 (NTPv3) or RFC 5905 Network Time Protocol Version 4 (NTPv4). Advantage software utilizes Windows time synchronization through W32Time that has been synchronized with Network Time Protocol technology to time stamp all records.

Compulink recommends SonicWall or Sophos routers for Internet, VPN and Remote Desktop services connections.

WIRELESS AND REMOTE ACCESS (Wide-Area-Network)

To access Compulink Advantage software over the public INTERNET lines, wireless networks and/or a remote location, a VPN (virtual private network) is highly recommended.

Compulink Advantage software utilizes **Remote Desktop Protocol** to provide access to remote and wireless stations. Public Internet lines or wireless networks do not provide sufficient bandwidth to access the **Compulink Advantage** software. Virtual Private Networks such as Microsoft's L2TP/IPSec VPN Client and IPSec tunnels may be mandatory in the future for the security of patient health data.
Compulink recommends SonicWall or Sophos routers for Internet, VPN and Remote Desktop services connections.

Microsoft's L2TP/IPSec VPN Client: The combination of L2TP and IPSec, known as L2TP/IPSec, is a highly secure technology for making remote access virtual private network (VPN) connections across public networks such as the Internet. L2TP/IPSec connections use the Data Encryption Standard (DES) algorithm, which uses either a 56-bit key for DES or three 56-bit keys for Triple DES (3DES).

Internet Protocol Security (IPSec): Internet Protocol security (IPSec) is a framework of open standards for helping to ensure private, secure communications over Internet Protocol (IP) networks through the use of cryptographic security services. IPSec uses packet filtering and cryptography. Cryptography provides user authentication, ensures data confidentiality and integrity, and enforces trusted communication.

Compulink recommends the following site to site communication settings over open networks:

Tunnel 1 IKE Proposal settings	
DH Group	Group2
Encryption algorithm	3DES
Authorization algorithm	SHA1
Life Time	28800

Tunnel 1 IPSec Proposal settings	
DH Group	Group2
Protocol	ESP
Encryption algorithm	3DES
Authorization algorithm	SHA-1
Life Time	28800

REMOTE DESKTOP PROTOCOL / WINDOWS TERMINAL SERVICES CONFIGURATION

Adding the **Compulink Advantage** Remote Desktop users is similar to adding users to the Local workstations with the exception of environmental variables. Terminal Server session variables must be added using the **USER VARIABLE SECTION ONLY**. A unique variable must be set for each session. **DO NOT ADD THE "CBS" VARIABLE TO THE SYSTEM VARIABLE OF THE SERVER**. Once each variable is set, in each user profile/session, map a network drive to the share where the **Compulink Advantage** software resides and create a shortcut on the remote user's desktop to launch the software through the mapped drive. In some cases, Remote Desktop users can launch the software through the UNC Path, however, the Start in path should still be through the mapped drive., please see **WORKSTATION SETUP**. It is recommended that all shortcuts have "read only" attributes so they do not resolve to the absolute root in case the network path and/or the mapped drive are temporarily unavailable.

Remote Location Identification
If your office utilizes multiple locations, use the variable **"CBSWAN"** along with the correct variable value assigned to each location by **Compulink**. Adding CBSWAN will allow the users to set their respective location prior to the launch of the software. If all terminal server users are from the same location, it is possible to use the **SYSTEM VARIABLE** and set the **CBSWAN** variable globally. If the terminal server users use different locations codes, use the **USER VARIABLE** section. (Example CBSWAN=001 for main location, and CBSWAN=002 for the remote location.)
The **CBSMOBILE** variable has been created for clients with staff members that move between offices and locations. This variable will allow users to enter the correct location code prior to the full launch of the **Compulink Advantage** software. When **CBSMOBILE=Y** is in the environmental settings, the software will prompt the user to enter the appropriate preferred location code upon every launch of the **Compulink Advantage** software.
PLEASE NOTE: It is **very important** that each workstation (remote sessions or local) utilizes a unique environment variable. Duplicating variables will cause interruption in the software operation and serious data corruption.
Open Office and/or **Microsoft Word *must be installed*** on the server to allow Terminal Server users to merge patient data with their preferred word processor. Adobe **Acrobat Reader** is also required for viewing and printing reports. See Third Party Software Requirements.

WIDE AREA NETWORK GENERAL INFORMATION - REMOTE PRINTING
All remote printers, including the Dymo label printers, must have an exact matching printer driver on the server and be registered as a known printer in the NTPRINT.INF file. In most cases, only printers created by the session will successfully print to **Compulink Advantage** software unless a third-party application is used to create and redirect the printer. In Windows 2012 R2 and beyond, the Remote Desktop Easy Print driver could eliminate the need for installing matching print drivers in certain environments. Easy Print driver has to be disabled when redirecting and using the Dymo Label printers to print labels in **Compulink Advantage** software. **Compulink** recommends using simplest language printer drivers such as PCL5 for all printing.

RECOMMENDED NETWORK APPLIANCES
As more health care providers make patient information available over the Web and on wireless devices, security and patient privacy are a big concern. The Data Protection Act 1998 (DPA) requires "appropriate technical and organizational measures" to prevent "unauthorized or unlawful processing of personal data." **Compulink** recommends the use of advanced network appliances to assist in protecting this information. Aside from the security software (see **SECURITY INFORMATION** section), Internet connectivity devices and firewalls play a big role in securing a network from external threats.

Compulink recommends SonicWall or Sophos routers for Internet, VPN and Remote Desktop services connections.

WIDE AREA NETWORK ADDITIONAL INFORMATION
Accessing **Compulink Advantage** software from a remote location is only possible if **Windows Remote Desktop Protocol** (Terminal Services) is utilized. System Administrators may have to login as each individual user during the initial setup to configure and test the environment for accessing **Compulink Advantage** software.

Recommended bandwidth per user: 64 kbps upload and download (note: up to 80/90 kbps or higher may be required if the remote scanning solution is implemented or there is a high volume of printing). The general memory recommendation for servers running terminal services is a minimum of 50MB of memory per session. This requirement does not include any other application or the operating system's general RAM requirements. Implementing **Electronic Health Records (EHR)** may require additional RAM for each **EHR** user.

For questions regarding Wide-Area-Networks, please contact **Compulink**'s IT department at (800) 888-8075 or consult@compulinkadvantage.com

SECURITY INFORMATION

SECURITY AND ANTI-VIRUS SOLUTION
Compulink recommends Security and Anti-Virus solutions developed for business/corporate environments. Solutions made for home/home office users are not designed for network applications such as **Compulink Advantage** software. It is imperative that your security solution provides an interface for proper configuration and unfiltered network packet delivery on the local area network to the COMPULINK share. All security applications must be configured by a network professional to permit full access to **Compulink Advantage** software and all of its associated TCP/UDP ports.

NOTE: Anti-Virus software alone cannot prevent virus and Trojans from attacking a network. Staff training is the best practice and defense against malicious attacks. Train your staff to refrain from visiting non-business related sites and opening unsolicited and unrecognized emails. Also using a hidden share will greatly increase protection against auto-spreading malware from infecting your product folder and patient information in the case a PC in your office is infected. Compulink recommends Cisco's OpenDNS and Umbrella solution for content filtering and DNS filtering.

Network scanning option **MUST** be disabled for all available Security and Anti-Virus programs. The content of the local drives are scanned and protected. Enabling the network drive scanning will only cause latency and create lag time for users of **Compulink Advantage** software. Scanning system for malware should also be scheduled during off peak hours or when system is not in use to avoid performance issues.

SECURITY AND ANTI-VIRUS SOLUTION – RECOMMENDATION
Many proprietary software companies provide threat prevention and defense against malware. Enterprise grade solutions, such as Sophos Endpoint Protection, are recommended for use with **Compulink Advantage** software. **Compulink** Users can deploy enterprise grade security solutions on their networks to protect against attacks.

NOTE: Compulink Healthcare Solutions utilizes Sophos Intercept X Advanced with EDR, XDR and other major solutions, as well as Windows Server Update Services (WSUS), to certify all communication between Compulink and Compulink Advantage clients are free of malware.

WIDE AREA NETWORK - *See Wireless and Remote Access*

DATA INFORMATION AND PROTECTION – BACKUPS

The following is provided for **Compulink** clients to ensure data integrity and maximizing system up time.
How much is your data worth?
Compulink cannot stress enough the importance of performing daily backup. Many businesses fail to appreciate the importance of backing up vital data on a daily basis until it is too late. Valuable equipment is usually insured against fire, theft or other disasters. A current on and off-site backup is the only insurance policy on your patient data. HIPAA Security Regulations dictate specific details as to how the electronic information used by the healthcare industry should be stored, transferred, and used to ensure the privacy of individually identifiable data related to a patient's healthcare. Your backup strategy is your first defense against the loss of patient data.

Different types of backup
Different types of backups are available with most backup software. A FULL backup of **Compulink's Advantage** product folder (e.g. EYEMD, EYECARE, PT, PSYCH) must be performed daily**.**
IMPORTANT: Differential or Incremental backups are not supported.

A Full backup will store all files and system data to the backup media. The **Compulink Advantage** product folder includes all application data, Security credentials and all transactional details. No other folder or directory needs to be backed up to successfully restore the **Compulink Advantage** software.

BACKUP STRATEGY

Each day, back up the product folder (e.g. EYEMD, EYECARE, PT, PSYCH, etc.) onto removable media to keep in the office. Keep at least 5 days' worth of backup on hand. ***Automatic Backups are recommended.***

Once a week, make a backup copy of the Advantage product folder on a different removable media and store off-premises. Perform a weekly exchange of this media for a new copy to take off-site.

When should backups take place?

Backups should be scheduled outside of business hours, when network traffic is at a minimum and ***Compulink Advantage software is NOT IN USE***. Scheduling the backup at some time during the night (e.g. Midnight) is a suitable tactic. Backing up data once a day (after each working day) provides good coverage against data disaster.

What storage medium should I use?

There are several factors to consider when selecting a place where your files will be stored:

- Time you want to spend on backups
- Convenience of restoring files
- Device reliability
- Total size of files to backup

The following backup media are to be taken into account when choosing where to backup:

Disk Storage, NAS, DAS or SAN: ideal for backing up large amounts of data

USB drive: for small backup jobs and keeping your important files always at hand

DVD: suitable for storing small sets of files (4.7GB per layer)

Tape: Tape backups are far more reliable than DVDs, but tape drives and their associated media are much more expensive.

Miscellaneous Backup Information

- CHECK THE BACKUP LOG AND REPORTS OFTEN TO ENSURE YOUR DAILY BACKUP IS RUNNING ERROR FREE.
- It is imperative that **Compulink Advantage** software is not in use while the backup is being performed. Contact **Compulink**'s IT department to obtain information on how to close all connections to the software prior to your backup. Instructions are included in the Autodiagnostics setup document.
- Hard Drive Redundancy (RAID) on the file server is recommended. However, RAID will not protect against physical damage due to fire, floods, etc. An external backup is required.
- Virtualization and virtual hard disks are highly recommended. A separate virtual disk for data can be dismounted and backed up for redundancy. This virtual disk may also be restored to another VM for easy access in case disaster recovery becomes necessary.
- Internet based and online backup solutions generally do not provide full nightly backups due to bandwidth limitations. These backup solutions can only perform incremental backups and are not recommended methods of file and disaster recovery for **Compulink Advantage** software.
- Do not use the COPY or XCOPY command to make a backup while **Compulink** software is in use.

BACKUP SOFTWARE

There is a myriad of options available for performing data backups. **Compulink** does not recommend any specific brand of Backup and Recovery software to backup and restore data. Clients must consult their IT administrator regarding **Compulink**'s backup requirements and provide this documentation for their review.

STORED DATA PROTECTION AND ENCRYPTION

Health Insurance Portability and Accountability Act (HIPAA) requires medical service providers to provide security measures for all stored patient health information. The compliance efforts are sometimes threatened by the ease with which sensitive information could reside unprotected on USB flash drives, external hard drivers, backup tapes and other portable devices and media. There are many solutions that secure mobile data and ensure that sensitive data remains private through encryption and password protection.

Password protecting the data is one of the most common used data protection means today. Backup applications generally offer an option to password protect the data during the backup operation. Compulink also recommends the workstations do not include writeable drives such as CD/DVD writers. Group Policies can be implemented in a domain to make flash drives "read only".
If you are using portable devices, a program such as Winzip or 7-zip can compress and encrypt any file or folder that resides on a local or portable device. Such archiving programs utilize AES encryption and password policy to protect stored data. There are many other solutions such as TrueCrypt that can provide the same level of security. BitLocker to Go Drive Encryption is a data protection feature available in some Windows versions. It extends data protection to USB storage devices, enabling them to be restricted with a passphrase. BitLocker uses the AES encryption algorithm in CBC mode with a 128 bit key and an optional 256 bit key, combined with the Elephant diffuser for additional disk encryption specific security not provided by AES. Consult your IT Professional for options.

RESTORE
In order to restore all application data, Security credentials and all transactional details, restore a full copy of **Compulink Advantage** software's folder (i.e. EYEMD, EYECARE, PT, PSYCH, etc.).

STANDBY FAILOVER SERVER (Available with Compulink Advantage version 9.0 and higher)
Standby Failover servers can be implemented by installing **Compulink Advantage** software in an environment where the software is running on a Storage Area Network (SAN) and connected to a server. In case the server fails, another server can be connected to the Storage Area Network (SAN) that is on standby with the same name and database management engine running. **Compulink Advantage** clients will not automatically reconnect in the case of a failure. Clients will have to refresh the network drive and restart their applications.

DISK REDUNDANCY AND CRASH
Compulink Advantage software can be installed on a system with disks that utilize RAID "Redundant Array of Independent (or Inexpensive) Disks" for fault tolerance. RAID allows data to be stored redundantly on an array of disks for additional protection. NOTE: RAID is not a backup solution replacement.

REDUNDANCY AND VIRTUALIZATION

Compulink utilizes **SAP's Advantage Database Server** management software to manage all connections and the integrity of databases. If a client connection is unexpectedly broken during the table update operation, data loss and corruptions are minimized due to the "write all/write nothing" nature of this database management software. **Compulink** highly recommends the use of virtualization and virtual hard disks for redundancy. Redundant virtual servers and hosts, connected to iSCSI SANs hosting the data, can greatly enhance redundancy and disaster recovery options. Typically, virtualization and such affordable iSCSI SANs can offer scalability, high-availability and in some cases easy replication. Virtualization and virtual hard disks are highly recommended. A separate virtual disk for data can be dismounted and backed up for redundancy. This virtual disk may also be restored to another Virtual Machine for easy access in case disaster recovery becomes necessary.

IMPORTANT NOTES

OPERATING SYSTEM UPDATES AND PATCHES
In addition to malware protection software, Windows Updates are the easiest, most reliable and cost efficient way to help protect your computer from the latest Internet threats. Installing the most current Windows Service Packs, Critical Updates and Patches are highly recommended.
To check for available or missing Windows Updates, visit the following Microsoft Web site:
http://windowsupdate.microsoft.com.

All current and supported Microsoft operating systems will have the ability to check for missing updates by viewing, downloading and installing the available Windows Service Packs, Critical Updates and Patches free of charge.

INTERNET EXPLORER ENHANCED SECURITY CONFIGURATION

Compulink recommends adding the server's path to the Local Intranet zone. Enhanced Security Configuration restricts access to scripts, executable files, and other potentially unsafe files on a UNC path unless it is added to the Local intranet zone explicitly. For example, if you want to access *server**share**setup.exe*, you must add *server* to the Local intranet zone.

MISCELLANEOUS

- In some cases Windows new enhanced security, such as User Account Control (UAC), may block some functionalities of the **Compulink Advantage** software including Compulink's legacy TWAINWAN process.
- It is **REQUIRED** that the NTFS File Allocation Table be used on the server if any of the workstations are utilizing NTFS. **Note:** FAT and FAT32 file systems have storage limitations.
- Some EMC and NEIC carriers may still require an external modem connected to a 9 pin serial COM1 and/or COM2 Port.
- **Compulink** has experienced difficulties with Keytronics brand keyboards. If you encounter abnormal behavior related to keyboard input with your copy of **Compulink Advantage** software, please consult with your systems' supplier.

Much more information, including Configuration and Troubleshooting Guides, Recommended Peripherals, Advantage Database Server Error Codes, and more, please visit the Compulink Advantage IT Support **pages.**

(You may require Login credentials to access Compulink Support pages. Please contact your Compulink representative for access to online resources)

For any questions or comments, please contact **Compulink IT Support** at **805.716.8677** or consult@compulinkadvantage.com

SOLUTIONS FOR SECURITY AND DATA PROTECTION

WIRELESS DATA PROTECTION AND ENCRYPTION

The "open air" nature of wireless radio signals poses challenges for securing wireless computer networks. Wireless radio signals broadcast through the air and are naturally easier to intercept. Signals from most wireless LANs pass through exterior walls and into nearby streets or parking lots. Strong encryption and wireless security is absolutely necessary to protect patient data. **Compulink** requires the following safeguards for implementing wireless security:

1. Change default administrator passwords and usernames (if available)

At the core of your wireless network is the access point or router. Hackers can discover the initial default settings of your device via the Internet. Change the administrator password immediately after installing the access point or router.

2. Turn on WPA encryption and implement a VPN

Encryption is a means of protecting transmitted data from being read by anyone but the intended recipient. WEP is not a secure protocol and has proven to have many flaws. Only implement wireless equipment that supports the **Wi-Fi Protected Access (WPA**) encryption technology or stronger. Wireless LAN users access the network just as remote dial-in or Internet users would. Access points and routers without VPN capabilities are viewed as a security risk. A hacker with an IEEE 802.11b network interface card who is in the transmission range can connect and access the wireless network. Place the access point behind the firewall, requiring that wireless clients authenticate to the VPN or firewall using third-party software or hardware. Utilizing L2TP VPN tunneling and IPSec encryption and authentication (see Wireless and Remote Access) adds another layer of encryption to secure the data. Hackers can easily penetrate and gain access to the data traversing unsecure access points but data secured by a firewall and VPN will be harder to decrypt and adds another layer of protection to protect patient data.

3. Change the default network name
Known as the Service Set Identifier (SSID), the name of the wireless local area network (WLAN) must be the same for all your network's wireless devices for them to communicate with each other. Manufacturers of access points and routers normally ship their products with the same SSID set. While knowing just the SSID does not enable anyone to break into your network, using a default SSID is a sign of a poorly configured network and is easy prey for hackers. So, when configuring your WLAN, change the default SSID as soon as possible.
4. Activate address filtering
Every piece of wireless hardware possesses a unique identifier called a Media Access Control (MAC) address. Access points and routers keep track of the MAC addresses of all wireless devices that connect to them. Your device should be configured to allow only MAC addresses that have been registered with the wireless access point or router. You can usually locate the MAC address of your network card on the device itself.
5. Disable SSID broadcast
In wireless networking, the access point or router typically broadcasts the Service Set Identifier (SSID) over the air at regular intervals. This feature of Wi-Fi network protocols is intended to allow clients to dynamically discover and roam between WLANs. After the implementation of your WLAN, this feature is unnecessary and makes your network more accessible to hackers.
6. Assign static Internet Protocol addresses to devices
Potential attackers of your network can easily obtain valid Internet Protocol (IP) addresses from your network's Dynamic Host Configuration Protocol (DHCP). To remedy this, disable DHCP on the router or access point and set a fixed IP address range.
7. Refrain from using the default IP subnet
Many routers and access points use the default IP subnet (e.g. 192.168.1.1 and 192.168.0.1). Change the IP subnet on your device during initial installation.

WIRELESS LOCAL AREA NETWORKS (WLAN)

Compulink Advantage software has been tested and proven compatible with Tablets, Notebooks and Desktops using wireless connectivity.

Please note: Due to the limitations of certain wireless environments, using a wireless connection as a direct means of communication between the station hosting the databases and another device on the network could cause disruption in packet delivery. Packet delivery disruptions may result in performance issues, database disconnections and data corruption. Compulink highly recommends utilizing Remote Desktop technology in wireless environments.

RELIABILITY
Like any radio frequency transmission, wireless networking signals are subject to a wide variety of interference.

SPEED
The speed of a wireless network depends on several factors. Wireless standards, typically advertised at 1-108 Mbps, will transmit data at a fraction of a wired network (typically at 1000 Mbps and up to several Gigabits per second). There are also performance issues caused by TCP and its built-in congestion avoidance.

SECURITY
The "open air" nature of wireless radio signals poses challenges for securing improperly configured wireless computer networks. Wireless radio signals broadcast through the air and are naturally easier to intercept. Signals from most wireless LANs pass through exterior walls and into nearby streets or parking lots. Strong encryption and wireless security is absolutely necessary to protect patient data.

The use of Windows Terminal Services and similar products, available from proprietary vendors such as Thinstuff's XP/VS Terminal Server, are necessary with low bandwidth environments.

Requirements for setting up wireless environments utilizing Remote Desktop are similar to the Wide Area Network, which is outlined in the **Wireless and remote access** and **Wireless Data Protection and Encryption** sections of this guide. For additional details regarding wireless networking, contact **Compulink**'s IT department.

Wireless Acknowledgement:
I have read and understand the Installation and Configuration Guide for **Compulink Advantage** software in a Wireless Area Network. A copy of this guide has also been provided to my Network Professional. These instructions have been followed to the best of my knowledge and ability. I hereby release **Compulink** from any configurations implemented by this office other than what is stated here or recommended by **Compulink**:

Client's Signature: _____ Date: _____/_____/_____

Print Your Name _____

CLIENT'S ACKNOWLEDGEMENT
Compulink provides these instructions as a guide to help insure a hassle free installation and operation. The support staff is available to assist with any questions and/or issues not covered in this guide.

I have read and understand the Installation, Configuration and Performance Guide for **Compulink Advantage** software (18 pages). A copy of this guide has also been provided to my Network Professional. These instructions have been followed to the best of my knowledge and ability. I hereby release **Compulink** from any configurations implemented by this office other than what is stated here or recommended by **Compulink**:

Date: _____ / _____ / _____

Account Number: _____

Client's Signature: _____

Print Your Name _____

IT Professional's Signature: _____

Print Your Name _____