Agilent

GC/MS and LC/MS MassHunter Workstation and Networked Workstation

Requirements Guide

Notices

Manual Part Number

D0026036

October 2025 Revision A.01

Copyright

Agilent Technologies, Inc.
5301 Stevens Creek Blvd.
Santa Clara,
CA
95051
www.agilent.com

Software Revision

This guide is valid for MassHunter Acquisition for LC/TQ 12.0, MassHunter Acquisition for LC/TOF and LC/Q-TOF 11.0, MassHunter Acquisition for GC/MS 13.1, MassHunter Qualitative Analysis 10.0, and MassHunter Quantitative Analysis 12.0 and greater until superceded.

Trademark Acknowledgment

PCIe® is a US registered trademark and/or service mark of PCI-SIG.

Warranty

The material contained in this document is provided "as is," and is subject to being changed, without notice, in future editions. Further, to the maximum extent permitted by applicable law, Agilent disclaims all warranties, either express or implied, with regard to this manual and any information contained herein, including but not limited to the implied warranties of merchantability and fitness for a particular purpose. Agilent shall not be liable for errors or for incidental or consequential damages in connection with the furnishing, use, or performance of this document or of any information contained herein. Should Agilent and the user have a separate written agreement with warranty terms covering the material in this document that conflict with these terms, the warranty terms in the separate agreement shall control.

Technology Licenses

The hardware and/or software described in this document are furnished under a license and may be used or copied only in accordance with the terms of such license.

Restricted Rights Legend

U.S. Government Restricted Rights. Software and technical data rights granted to the federal government include only those rights customarily provided to end user customers. Agilent provides this customary commercial license in Software and technical data pursuant to FAR 12.211 (Technical Data) and 12.212 (Computer Software) and, for the Department of Defense, DFARS 252.227-7015 (Technical Data - Commercial Items) and DFARS 227.7202-3 (Rights in Commercial Computer Software or Computer Software Documentation).

Safety Notices

CAUTION

A **CAUTION** notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in damage to the product or loss of important data. Do not proceed beyond a **CAUTION** notice until the indicated conditions are fully understood and met.

WARNING

A WARNING notice denotes a hazard. It calls attention to an operating procedure, practice, or the like that, if not correctly performed or adhered to, could result in personal injury or death. Do not proceed beyond a WARNING notice until the indicated conditions are fully understood and met.

Contents

1 In This Book

This document details the minimum computer hardware, software, and network requirements as well as the minimum instrument firmware revisions required to run an Agilent MassHunter Workstation or Agilent MassHunter Networked Workstation. Also included are the supported instrument types and Windows operating system configurations.

Table 1. Terms and abbreviations used in this document

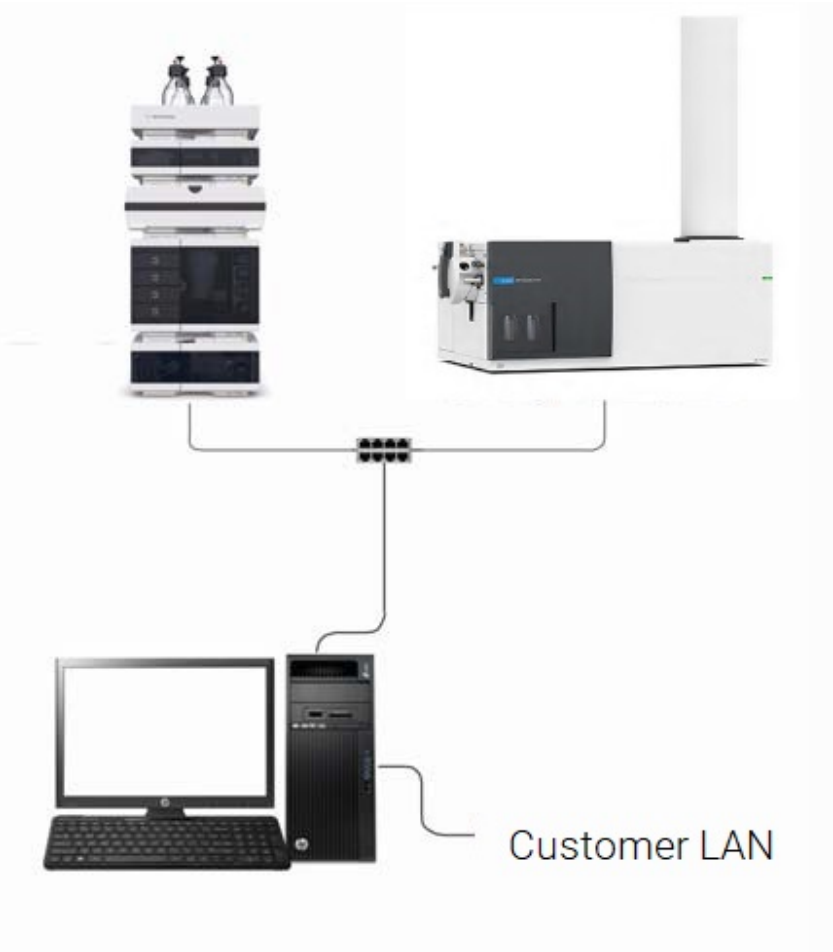
Term	Description
Content Management	Database to manage your analytical data. The database is provided as a component of OpenLab Server. Always used in Client/Server systems, optional for Workstations.
Control Panel	Control Panel for OpenLab Shared Services
Microsoft Control Panel	Part of the Microsoft Windows operating system

2 Hardware and Software Requirements

This chapter contains the hardware and software requirements for the different components of a MassHunter system.

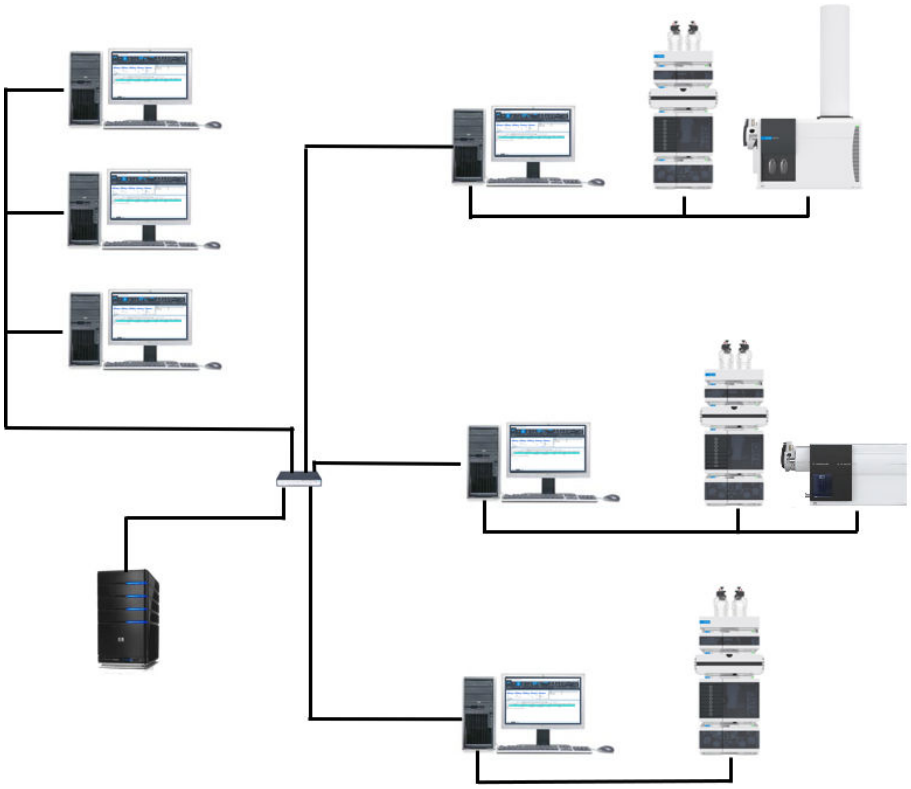
Depending on the type of installation, you may need different hardware components. The following graphics show the required components for each scenario.

Figure 1. MassHunter Workstation



All required components are installed on the workstation.

Figure 2. Networked Workstation system



The system includes both Networked Workstations and an OpenLab Server or OpenLab ECM XT server or ECM 3.x server.

Software

General Software Requirements

Component	Details
.NET framework	• NET 3.5.1 must be enabled on systems running on Windows 11 *and* • NET 4.7.2 or above (if needed, it will be installed automatically by the MassHunter Installer)
Web browser	• Google Chrome 40 or higher • Edge
Anti-virus software[1]	Microsoft Windows Defender

[1]The listed anti-virus software has been tested to be compatible with the MassHunter software described in this document. While other third-party AV solutions may also be compatible, they have not been tested, and compatibility cannot be guaranteed.

Windows Compatibility

Only these Windows operating systems are supported:

- Windows 11 Pro (or Pro for Workstations) General Availability Channel: 21H2 or newer.

Computer Hardware

Disk Space

Disk space requirements vary based on the number and type of instruments, archival frequency, and the method settings chosen for Acquisition. Agilent recommends providing enough disk space for one year of lab operation, in addition to the operating system and MassHunter Workstation requirements.

The MassHunter Workstation is available either with storage in the local file system (MassHunter Workstation) or on a remote OpenLab Server or OpenLab ECM XT server with built-in Content Management database (MassHunter Networked Workstation).

Note that on Networked Workstations, data is only temporarily stored in a secured location on the local computer until it is transferred to the OpenLab Server/ECM XT server.

PC Recommendation

Table 2 provides the recommended hardware configuration for MassHunter computers with a single LC/TOF or LC/Q-TOF instrument.

Table 2. Tested and recommended hardware configuration for Workstations and Networked Workstations for LC/TOF and LC/Q-TOF

Item	For all LC/Q-TOF except 6546 and 6575	For 6546 and 6575 only
Description	Standard MassHunter-ready Computer	High Capacity MassHunter-ready Computer
Processor speed (CPU)	Intel Xeon W-2123, 4 core, 3.6 GHz	Intel Xeon W-2235, 6 core, 3.8 GHz
Physical memory (RAM)	32 GB	64 GB
Hard disk	1 TB M.2 NVMe SSD - Primary (C:\) Boot. 4 TB × 2 RAID1 (4 TB) - Data (D:\)	1 TB M.2 NVMe SSD - Primary (C:\) Boot. 6 TB × 4 RAID10 (12 TB) - Data (D:\)
Graphic Resolution	1920 x 1080	1920 x 1080
USB port[1]	1 USB port required for installation	1 USB port required for installation
LAN card - House	Integrated Intel I217LM PCIe GbE Controller	1 Integrated Intel I217LM PCIe GbE Controller
LAN card - instrument[2]	Integrated Intel I217LM PCIe GbE Controller	1 Intel Ethernet 210-T1 PCIe

[1]If a USB port is not available, the installation media can be copied over the network or downloaded from https://agilent.subscribenet.com.

[2]A second LAN interface is required to isolate the instrument's data traffic from the local area network.

Table 3 provides the recommended hardware configuration for MassHunter computers with a single GC/SQ, GC/TQ, or GC/Q-TOF instrument.

Table 3. Tested and recommended hardware configuration for Workstations and Networked Workstations for GC/SQ, GC/TQ, and GC/Q-TOF

Item	For all GC/MS Single Quadrupole and Triple Quadrupole instruments	For all GC/MS Quadrupole Time of Flight instruments
Description	Standard MassHunter-ready Computer	High Capacity MassHunter-ready Computer
Processor speed (CPU)	Intel core i5-12500, 6 core, 3.0 GHz	Intel Xeon W-2423, 6 CORE, 4.2 GHz
Physical memory (RAM)	16 GB (nECC)	64 GB (ECC)
Hard disk	1 TB NVMe SSD (Partitioned between C:\ and D:\)	1 TB NVMe SSD - Primary C:\ Boot volume, 2 x 12 TB 7200 RPM SATA 6G HDD - Data D:\ volume
Graphic Resolution	1920 x 1080	1920 x 1080
USB port[1]	1 USB port required for installation	1 USB port required for installation
LAN card - House	Integrated 1 GbE LAN on mainboard	Integrated 1 GbE LAN on mainboard
LAN card - Instrument[2]	HP Flex 1 GbE NIC	1 GbE NIC for connection to GC and other networked instrument devices such as external sampler, 10 GbE network adapter for 7250 Q-TOF MS

[1]If a USB port is not available, the installation media can be copied over the network or downloaded from https://agilent.subscribenet.com.

[2]A second LAN interface is required to isolate the instrument's data traffic from the local area network.

Table 4. Minimum hardware configuration for Workstations

Item	For All TQ systems
Description	Hewlett-Packard Z4 G4 Minitower
Processor speed (CPU)	Intel Xeon W-2123 (3.6 GHz, 8.25 MB cache, 4 cores)
Physical memory (RAM)	16GB (2x8GB) DDR4 2666 DIMM ECC Registered Memory
Hard disk	2 x 500GB 7200 RPM SATA 6G Hard Drive (RAID 1)
Graphic Resolution	1920 x 1080
USB port[1]	1 USB port required for installation
LAN card[2]	2 × Integrated Intel I219 and I210 PCIe GbE

[1]If a USB port is not available, the installation media can be copied over the network or downloaded from https://agilent.subscribenet.com.

[2]A second LAN interface is required to isolate the instrument's data traffic from the local area network.

Windows 11 Configuration

This section describes how to configure Windows 11 Professional for MassHunter Workstation to prepare for MassHunter software installation.

Installations on computers and operating systems not supplied by Agilent are supported on a best-effort basis only.

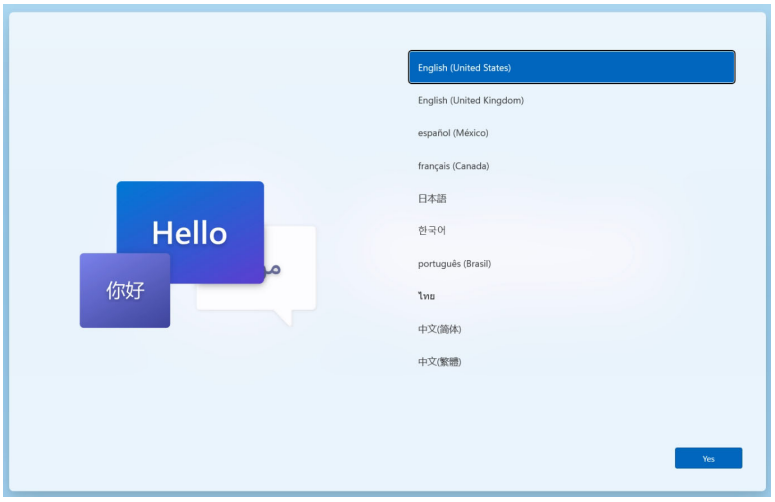
This guide assumes that the computer has been imaged using the Agilent branded PC Recovery Media produced specifically for and supplied with the bundled Hewlett-Packard computer. If using any other Windows 11 media, settings can differ from the settings that are optimal for Agilent MassHunter software.

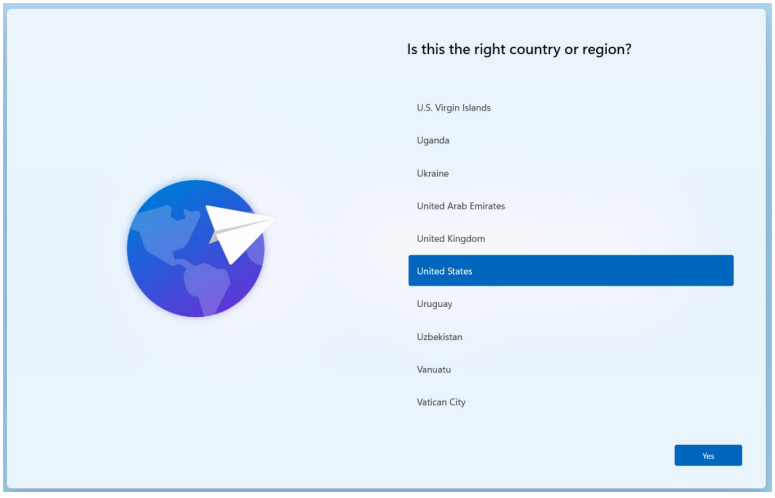
Step 1. Set up Windows 11

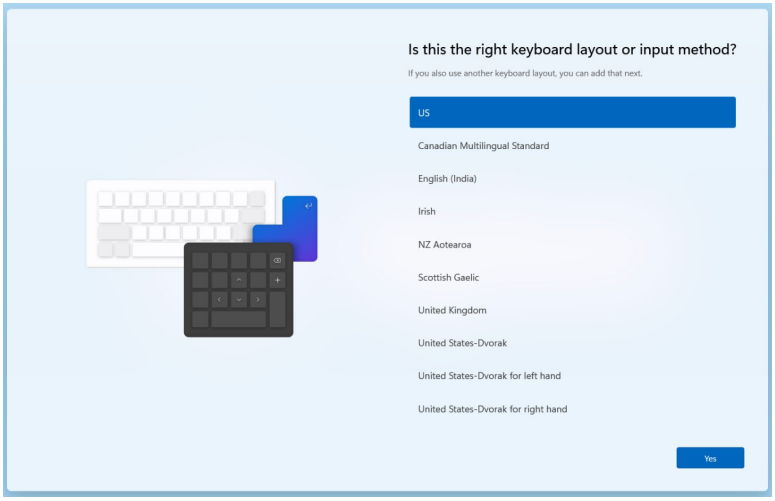
The first time that Windows 11 Professional starts after installation, a prompt for setup information displays.

NOTE The images in this guide may differ from what is shown on this screen.

1. When prompted, select a language, region, keyboard layout, and time zone.





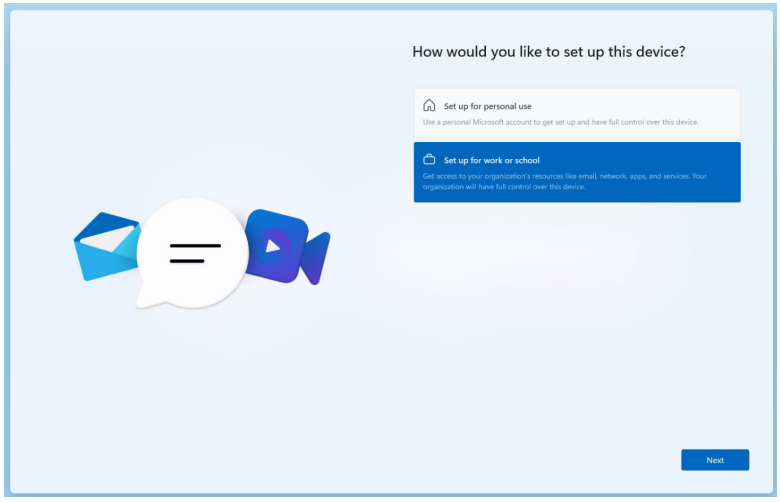


NOTE

MassHunter is supported only with the following localization/regionalization configurations:

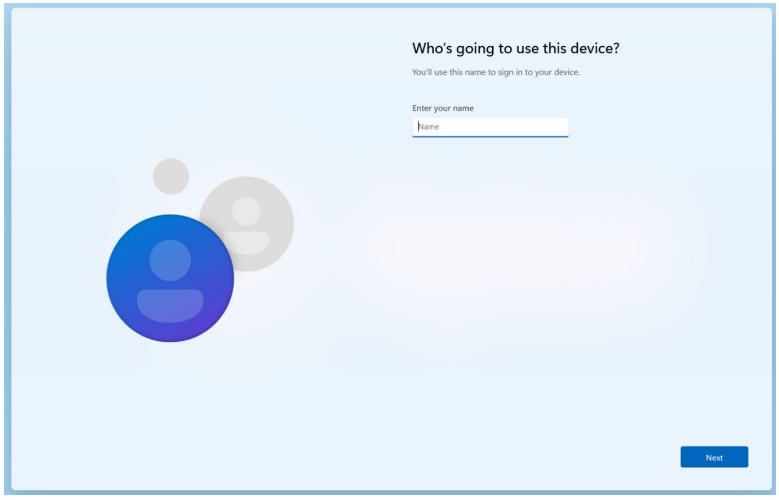
- en-US; US English
- zh-CN; Chinese (simplified)
- ja_JP; Japanese

2. Set up for work or school.



By default, Microsoft encourages users to log in with a Microsoft account. Bypass this requirement by disconnecting the PC from the Internet when prompted to sign in to a Microsoft account. Release the IP address using a command prompt (press **shift+f10** to open the command prompt, then run ipconfig/release). Alternatively, unplug the ethernet cable from the PC. Once disconnected, click the **Back** button to display a prompt to create a local account.

3. Create a username and password for a user that will be a member of the Administrators group.

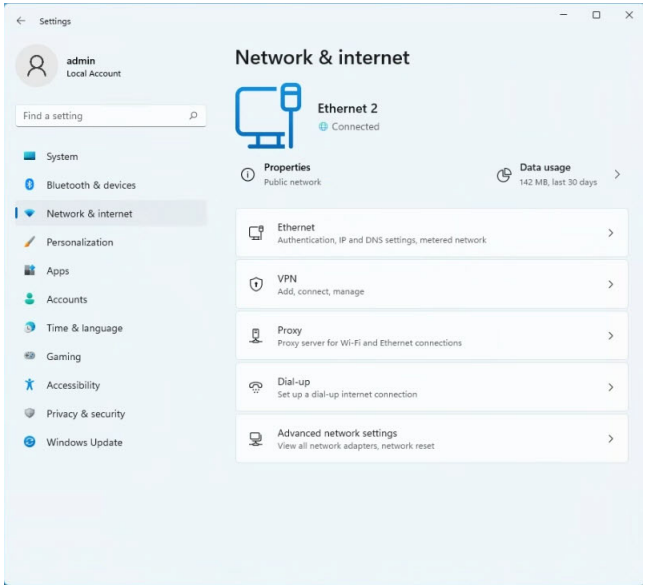


Step 2. Rename the network adapters

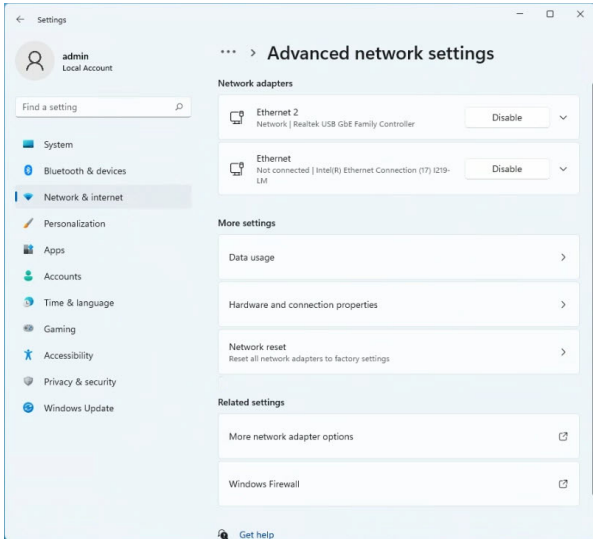
Renaming network adapters helps to keep track of them, especially with multiple network adapters (NICs). Before renaming, determine the purpose of each NIC.

CAUTION Real-time MS data acquisition requires stable, low-latency, high-bandwidth network communication. Be sure to confine instrument communication to a separate isolated network. Data acquisition can be interrupted if the instrument connects to the workstation over a shared network.

1. Select **Start** > **Settings** (⚙) > **Network & Internet**.



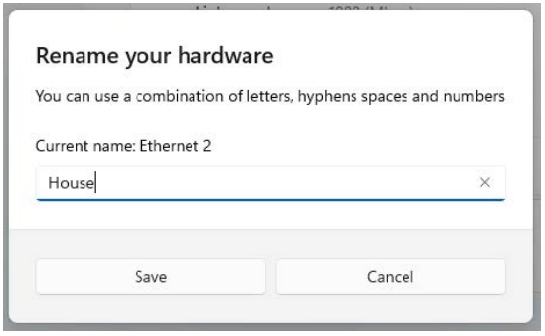
2. In the Network & Internet navigation pane, select **Advanced network settings**. Multiple network connections may be shown. Use this screen to determine which adapter connects to each device.



NOTE Some instruments require a third 10 Gbps network adapter. Contact Agilent for more information.

3. Disconnect all network cables from the computer.
4. (Optional) Connect the in-house network:
   a. Connect a network cable for the in-house network to the port labeled **House** on the back of the PC. The status of one adapter changes to Enabled.

b. Click the corresponding network adapter and select **Rename**. Enter the name *House connection* and click **Save**.



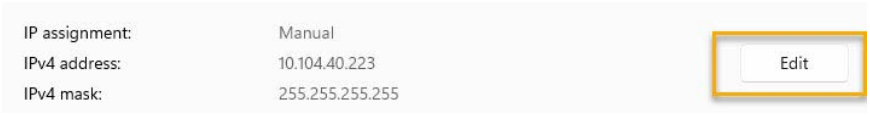
5. For 7250 GC/Q-TOF only:
   a. Connect a network cable from the LAN port of the MS to the **MS** network adapter on the back of the computer.
   b. Click the corresponding network adapter and select **Rename**. Enter the name *MS Instrument* and click **Save**.
6. Connect the Ethernet switch. Then, connect a CAT6A cable from the Ethernet switch to the network adapter on the back of the computer that is labeled **LC-MS** or **GCMS** for all GC/MS instruments except 7250 instruments.
   - For GC/Q-TOF instruments the connection is the GC NIC.
   - For 7250 GC/Q-TOF, 6546, and Revident, the connection is the 10 GbE NIC.
7. Click the name of the connected network adapter to display associated information. Click **Rename**.
   - For LC/MS instruments, enter the name *LC/MS Instrument*.
   - For GC/MS instruments, enter the name *GC/MS Instrument*.
   - For 7250 GC/MS Q-TOF only, change name to GC.
8. Click **Save**.
   See the installation guide for the GC/MS or LC/MS instrument to connect instruments and modules to the Ethernet switch.

NOTE For 6546 LC/Q-TOF only, use a Cat 6 or better network cable to connect the 6546 LC/Q-TOF to a 10 Gbps port on the Ethernet switch.

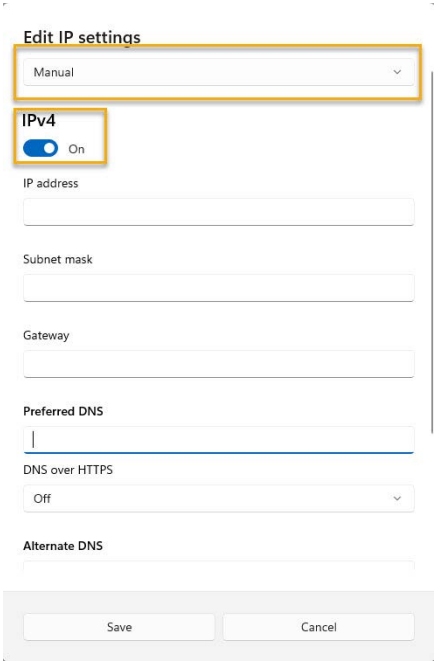
Step 3. Set the network adapter IP addresses

1. In Advanced Network Settings, under Network adapters, select the adapter associated with the instrument and click **View additional properties**.

2. Next to IP Assignment, click **Edit**.



3. Click the **Edit IP Settings** drop-down, and select **Manual**.



4. Switch on **IPv4**.

5. Enter an **IP Address** according to the table below.

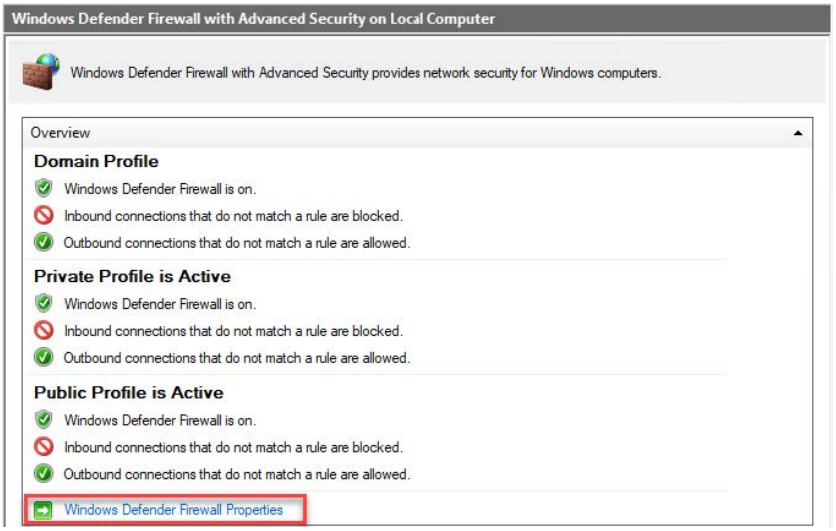
Table 5. Network Adapter IP Addresses

Instrument	LAN	GC LAN
7250 GC/Q-TOF	(MS LAN) 192.168.254.1	192.168.253.1
Other GC/MS or LC/MS	(GCMS or LCMS LAN) 192.168.254.1	n/a

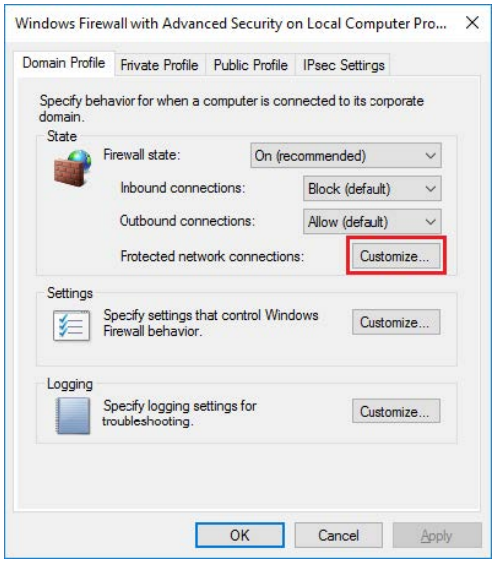
6. Enter the Subnet mask as *255.255.255.0*. Leave the Gateway and Preferred DNS Server lines empty.
7. Click **Save** to return to the Network Connections window.
8. Close the Network Connection window.

Step 4. Change firewall settings for the instrument network adapter

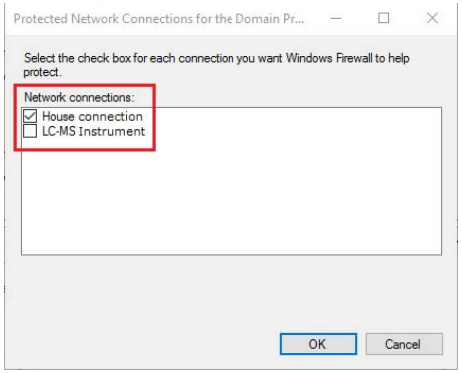
1. From the start menu, in the search field, type *Windows Security* and press **Enter**. The Security at a glance dialog box opens.
2. Click **Firewall & network protection**.
3. Click **Advanced Settings**.
4. Under **Overview**, click **Windows Defender Firewall Properties**.



5. In the **Domain Profile** tab, next to Protected network connections, click **Customize**.



6. Clear all check boxes except **House connection**, then click **OK**.

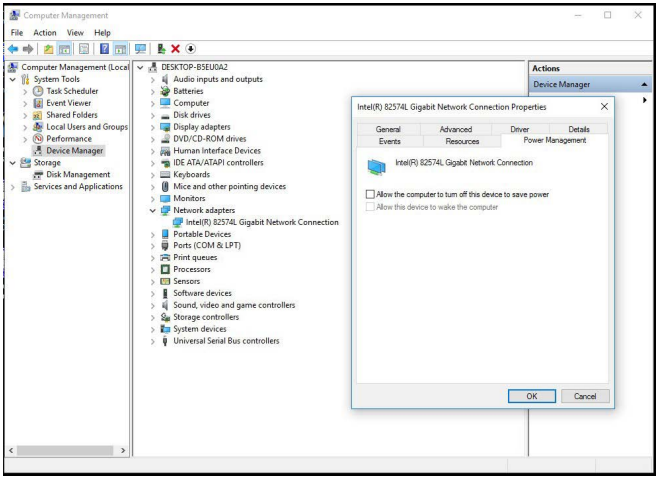


7. Repeat the two previous steps for the Private Profile and Public Profile tabs.
8. Click **OK** to close the Windows Firewall with Advanced Security on Local Computer Properties dialog box.
9. Close the Windows Firewall with Advanced Security window.

Step 5. Turn off Power Management for all Network Cards

1. Click the **Start menu** and type *Computer Management* in the Search field and press **Enter**.
2. Under **System Tools**, click **Device Manager**.
3. Expand **Network adapters**.
4. For each network adapter associated with the instruments:
   a. Right-click the adapter and select **Properties**.
   b. In the Power Management tab, **clear** the check box for **Allow the computer to turn off this device to save power**.
   c. Click **OK** and then close the Computer Management window.

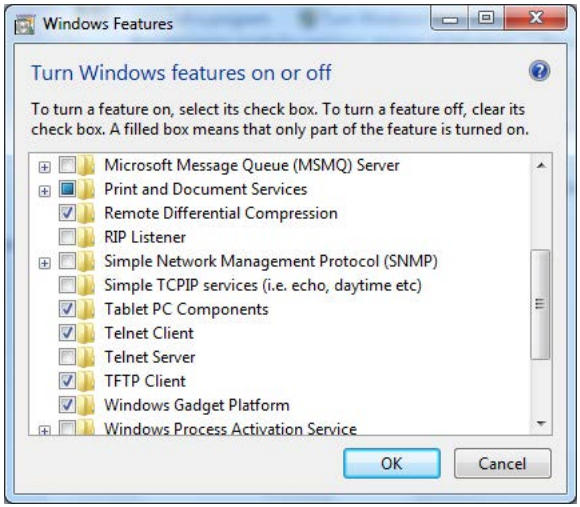
NOTE The figure that follows may differ from what is displayed depending on the version of the network interface driver installed. Disable any energy saving features that are associated with the Ethernet adapter. The names of these features vary by driver version.



Step 6. Confirm that Telnet Client and TFTP Client are enabled

The Telnet Client and TFTP Client features are used by the LC/MS Firmware Update Tool to allow Agilent-certified service professionals to collect diagnostic information from LC/MS and GC/MS instruments. These features are not required for normal use and can be disabled until they are needed.

1. Click **Start**, type *turn windows features on or off* in the search field, then press **Enter** or click **Turn Windows features on or off**.
2. Verify that the **Telnet Client** and **TFTP Client** check boxes are selected.



3. Click **OK** and close the Control Panel.

Step 7. Satisfy Requirements for Networked Workstation Systems

If you intend to use your system in the Networked Workstation configuration, please note these additional requirements:

- Your network must have a time synchronization service to make sure that all systems are using a consistent and valid time.
- It is important to synchronize the time on your system before installing the MassHunter software. Failure to do so may result in user lockout if the date and time of the system is earlier than the signing date of certificates required by the software.
- Changing the hostname after installation is not recommended. It is tedious and requires specific actions. Please contact your Agilent support representative if you need to change the hostname.

Step 8. Install MassHunter programs

Follow the appropriate installation or upgrade guide to install MassHunter programs. Make sure to install any help for the system.

Administrator rights are required to install MassHunter software and for some configuration steps, but are not required for routine operation of MassHunter programs. To ensure that users cannot change the time on a client system, users must not operate Networked Workstations using an administrator account after installing and configuring the MassHunter software. This is important as the client time is used during buffered activity logging during network outages.

To ensure availability of port 443, disable Microsoft's BranchCache feature before installing the MassHunter software.

Step 9. Set up exclusions in security program

See the Windows Defender or other security solution instructions to make these exclusions.

1. Exclude these processes.
   For LC/MS:
   - AgtMassHunterAcquisition.exe
   - AgtOptimizer.exe
   - AgtVoyAcqEng.exe
   - AgtVoyWklsEng.exe
   - AgtStudyEng.exe
   - AgtDAReprocessing.exe

   For GC/MS:
   - msinsctl.exe
2. Exclude the folder **D:\Masshunter** by default.
3. Exclude the folder **D:\Projects** by default.
4. Exclude the folder **C:\ProgramData\Agilent**.
5. For GC/MS, also exclude the folder **C:\GCMS**.
6. Exclude the file type **bin**.

Windows Defender

By default, the Windows Defender anti-malware service is enabled and must be updated regularly. No exclusions other than those listed in this topic are required for the Windows Defender service to operate with Agilent products.

Windows Firewall

By default, the Windows firewall is enabled for the House network connection. It is recommended to disable the firewall on any instrument network connections.

Third-party Software Security Programs Support

Agilent does exhaustive testing on software and hardware configurations to ensure that every configuration that Agilent sells works as designed.

However, Agilent is not able to test every combination of third party computer security (antivirus, anti-malware, and firewall) programs for compatibility.

The customer is responsible for determining the compatibility of any third party software that runs with an Agilent product.

If a third party computer security program causes problems for an Agilent product, Agilent can request that such program be disabled or removed before Agilent provides support.

Step 10. Update Windows 11 and run regularly

Run Windows Update regularly. Make sure to always install Windows Security Updates.

CAUTION Windows 11 offers the choice of when and how to get the latest updates to keep the device running smoothly and securely. To manage the options and view available updates, select **Check for Windows updates**, or from the **Start menu**, open **Settings** > **Update & Security** > **Windows Update**. Under **Advanced** options, view the value for feature and quality updates. Select **Pause updates** if critical tasks need to be performed when an automatic reboot must be delayed.

CAUTION Some Windows Feature Updates change the group policy setting on the computer to allow the computer to automatically download and install Windows Updates, or to automatically reboot.

For more information on how to control how and when Windows Updates are run, see the following:

https://learn.microsoft.com/en-us/windows/deployment/update/waas-restart

3 Network Requirements

This chapter describes the network requirements that must be met in order to support the environmental computing needs of a MassHunter system.

Introduction

MassHunter systems rely on network infrastructure in order to support the communication between Networked Workstations and the OpenLab Server/ECM XT server. This communication is based on standard TCP/IP protocols. In order to provide optimum performance and uptime, the network must meet design criteria for available bandwidth, IP address assignment, name resolution and appropriate isolation of the lab subnet from the corporate network.

Refer to the *Agilent OpenLab Server and OpenLab ECM XT Hardware and Software Requirements Guide* for more details about networking requirements.

LAN Connectivity

All MassHunter Networked Workstations include at least two 1 GB Ethernet network interfaces. One is reserved for PC-to-Instrument communication. The other is used to communicate with the OpenLab Server / ECM XT / ECM 3.x.

Note these LAN Connectivity requirements:

- For the 6546 LC/Q-TOF and 7250 GC/Q-TOF: a 10 GB Ethernet adapter is required for PC-to-instrument communication. In this configuration, high quality Cat 6 Ethernet over twisted-pair cables or better are required.
- NIC teaming[1]: LAN cards should not be teamed on workstations, instrument controllers, or clients.
- Communication between the Networked Workstation and OpenLab Server/ECM XT must be over Gigabit Ethernet (GbE) or faster.

[1]Network Interface Card (NIC) teaming is also known as Load Balancing and Failover (LBFO).

- For TOF/Q-TOF instruments only: The OpenLab Server/ECM XT server/ECM 3.x server must be located on the same physical premises as the Networked Workstation. Co-located or off-premise/cloud-based servers are not supported.
- USB network adapters are not supported

LAN Power Management

Avoid data capture or transfer interruptions in your data acquisition system by making LAN communication cards available for instrument and system component communications.

Windows may be configured to turn instruments/components off to save power while sleeping or hibernating. To change this setting:

1. In the Microsoft Control Panel, open the **Network and Sharing Center**.
2. Select **Change adapter settings**. Right-click **Local Area Connection**, and then click **Properties** > **Configure**.
3. Select the **Power Management** tab.
4. Clear the **Allow the computer to turn off this device to save power** check box.
5. Depending on the model of network adapter, the name of this option can also be **Energy efficient Ethernet**, **Power saving Ethernet mode**, or a similar name.

CAUTION While applying Windows Updates, LAN Power Management might become reactivated. Be sure to check the LAN Power Management settings after all Windows Updates.

Firewall and Network Port Settings

If you are using a third party firewall on the network where MassHunter is installed, open these firewall ports to allow communication between the system components of MassHunter. The following table applies to Networked Workstation systems.

Table 6. Inbound to Networked Workstation

Ports	Comment, required for
443	Reverse Proxy Service. Port 443 does not need to be opened in the Workstation configuration, but the port must be "available" for the reverse proxy service to run. Microsoft services such as BranchCache can occupy the port and disrupt operation of the reverse proxy service. To ensure availability of port 443, disable Microsoft's BranchCache feature before installing the MassHunter software.
6570	SubscribeNet: active retrieval and release of product licenses
8084	Agilent OpenLab Licensing support
8085-8089	Alternative to port 8084 if that port is in use by another page or process
8090	Hosts the viewing page of current license grants and consumption found in the OpenLab Control Panel administration interface
27000-27009	Communication of license availability
30101	Store and retrieve instrument data
53971	Activity log messages display notification

The following table applies to Workstation and Networked Workstation systems as component communications rely on these communication channels:

Table 7. Inbound to Workstation and Networked Workstation

Ports	Comment, required for
22	SSH used for Firmware installation
6002 / 6003	Instrument communications
8080	Tune/Calibration/Diagnostics Web Interface
30101	Store and retrieve instrument data

The MassHunter Workstation installer will automatically open required ports on an enabled Windows firewall during installation.

For MassHunter GC/MS Data Acquisition the table of ports enabled in Windows firewall during installation include:

Table 8. GC/MS Acquisition Services

Service name / Function	Application path (default installation path)	Protocol	Port
ICMPv4 (Ping)	N/A	ICMP	N/A
Agilent GCMS MassHunter httpdmsd tool	C:\Program Files (x86)\Agilent\MassHunter\GCMS\MSEXE\HTTPDMSD.EXE	TCP/UDP	Any
Agilent GCMS MassHunter Instrument Control and Calibration	C:\Program Files (x86)\Agilent\MassHunter\GCMS\MSEXE\MSINSCTL.EXE	TCP/UDP	Any
Agilent GCMS MassHunter MSD 5975 Firmware Update Tool	C:\Program Files (x86)\Agilent\MassHunter\GCMS\Firmware\5975\MSUPDATE2.EXE	TCP/UDP	Any

Service name / Function	Application path (default installation path)	Protocol	Port
Agilent GCMS MassHunter MSD 5977 Firmware Update Tool	C:\Program Files (x86)\Agilent\MassHunter\GCMS\Firmware\5977\MSUPDATE2.EXE	TCP/UDP	Any
Agilent GCMS MassHunter Optimizer for GC-TQ	C:\Program Files (x86)\Agilent\MassHunter\GCMS\MSEXE\GCMSOPTIMIZER.EXE	TCP/UDP	Any
Agilent GCMS MassHunter RpcInfo tool	C:\Program Files (x86)\Agilent\MassHunter\GCMS\MSEXE\RPCINFO.EXE	TCP/UDP	Any
Agilent GCMS MassHunter scqiolib tool	C:\Program Files (x86)\Agilent\MassHunter\GCMS\MSEXE\SCQIOLIB.EXE	TCP/UDP	Any
Agilent GCMS MassHunter scs tool	C:\Program Files (x86)\Agilent\MassHunter\GCMS\MSEXE\SCS.EXE	TCP/UDP	Any
Agilent GCMS MassHunter TQ Firmware Update Tool	C:\Program Files (x86)\Agilent\MassHunter\GCMS\Firmware\7000\MSUPDATE2.EXE	TCP/UDP	Any
Agilent GC Driver Port 10000-10020	Any	TCP	10000-10020
File Transfer Program	C:\Windows\System32\FTP.EXE	TCP	Any
Telnet	C:\Windows\System32\TELNET.EXE	TCP	Any

Service name / Function	Application path (default installation path)	Protocol	Port
Instrument communication		TCP	7890-7983 9001-9002 9100-9101 9110-9111 10000-10020 7972-7973

Table 9. OpenLab Components

OpenLab Component	Application path (default installation path)	Protocol	Port
Agilent CA Test Services Server port	C:\Program Files (x86)\Agilent Technologies\Test Services\Central Management Service\Agilent.TestServices.Server.Main.exe	TCP	52088
Agilent OpenLab Automation Services	Any	TCP	2886
Agilent OpenLab Certificate Service (HTTPS:52088)	Any	TCP	52088
Agilent OpenLab Data Collection Service (HTTP-Legacy)	C:\Program Files (x86)\Agilent Technologies\Data Collection Service\Bin\DataCollectionService.exe	TCP	6328
Agilent OpenLab Data Collection Service (HTTPS)	C:\Program Files (x86)\Agilent Technologies\Data Collection Service\Bin\DataCollectionService.exe	TCP	52088

OpenLab Component	Application path (default installation path)	Protocol	Port
Agilent OpenLab DataRepository Base (HTTP-Legacy)	C:\Program Files\Agilent Technologies\OpenLab Platform\Data Repository\Data Repository\Service\Agilent.OpenLab.DR.BaseService.exe	TCP	52080
Agilent OpenLab DataRepository Base (HTTPS)	C:\Program Files\Agilent Technologies\OpenLab Platform\Data Repository\Data Repository\Service\Agilent.OpenLab.DR.BaseService.exe	TCP	52088
Agilent OpenLab Diagnostics Tools	Any	TCP	3424
Agilent OpenLab License Server	C:\Program Files (x86)\Agilent Technologies\OpenLab Services\Licensing\Flexera\lmadmin.exe	Any	Any
Agilent OpenLab Licensing Support	Any	TCP	8084
Agilent OpenLab Licensing Support (Flexera)	Any	TCP	6570
Agilent OpenLab OpenSearch (HTTPS:9200)	Any	TCP	9200
Agilent OpenLab Platform - PostgreSQL 14.X	C:\Program Files\PostgreSQL\14\bin\postgres.exe	Any	Any
Agilent OpenLab RabbitMQ (Admin HTTPS:15671)	Any	TCP	15671
Agilent OpenLab RabbitMQ (Discovery 4369)	Any	TCP	4369

OpenLab Component	Application path (default installation path)	Protocol	Port
Agilent OpenLab RabbitMQ (HTTPS:5671)	Any	TCP	5671
Agilent OpenLab Remote Work Area	Any	TCP	6628
Agilent OpenLab REST API	Any	TCP	6624-6625
Agilent OpenLab Reverse Proxy (HTTP:80)	C:\Program Files\OpenLab Reverse Proxy\Apache24\bin\httpd.exe	TCP	80
Agilent OpenLab Reverse Proxy (HTTPS:443)	C:\Program Files\OpenLab Reverse Proxy\Apache24\bin\httpd.exe	TCP	443
Agilent OpenLab Shared Services	Any	TCP	6577

NOTE Windows Defender Firewall must be disabled before updating the firmware.

Domain Requirements

Domains support the flow of information and user access rights across machines in the network. This means that all machines and instruments within the MassHunter Networked Workstation system must reside within the same domain or have the appropriate cross domain trusts to allow name based communications between all components in the system. In the case of a workstation installation, domains are only relevant if you are using a Windows domain-based authentication model. In this case the workstation or client must always be able to communicate with domain components in order to function as expected.

Installing MassHunter Workstation will apply network exceptions to the Windows firewall under the domain profile to result in a functional system. The components necessary to support MassHunter on a domain are:

- Domain controller – broadcasts the domain name and negotiates access to machines.
- Domain name server (DNS) – maintains records of what host names belong to which IP on the network. This component is always required for effective components communications in networked systems.
- Active directory – maintains the list of users and their access rights on the domain.

NOTE The domain name server (DNS) must be able to resolve the IPv4 address of all instrument controllers and instruments. Any unresolved instrument controller or instrument will disrupt the functionality of MassHunter resulting in errors or delays. IPv6 is not supported and must be deactivated.

NOTE MassHunter Workstation components must not be installed on the same machine as the domain controller.

The domain components above host a variety of services and settings that must be configured appropriately to allow communication across machines. The following services and settings will need to be configured to fit your domain. Your internal IT group is responsible for proper configuration of any custom domain solutions. These include settings for:

- Lookup zones and hostnames
- Group and security policies
- Subnet masks and Virtual LANs
- IP reservation (static or DHCP)

Environments with Proxy Servers

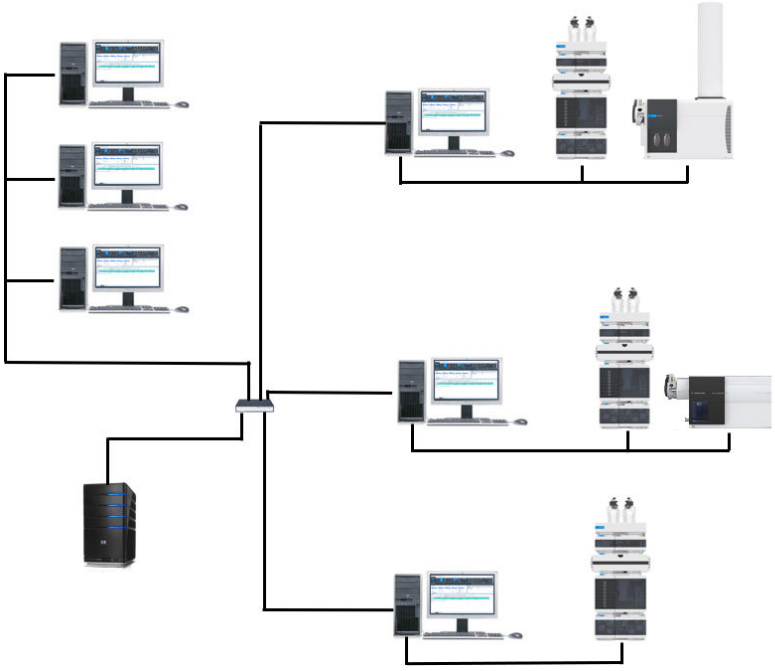
The OpenLab server must be accessible via http or https in the network. If you use proxy servers, verify that they can be accessed. If required, adjust the proxy settings.

Network Isolation

MassHunter Networked Workstations must be isolated from network environments that experience frequent failures due to faulty switching, viruses, or worms. If network isolation is not possible, the machines should be reconfigured and disconnected from the problematic network until these issues can be resolved. On an isolated network, name resolution services must be hosted by a separate machine to enable proper communications between system components by name.

An isolated network is completely physically isolated, so that no LAN switch connections on the network are shared with the corporate network infrastructure. Figure 3 shows a simple client/server topology.

Figure 3. Sample client/server topology: Network Isolation



4 Incompatible LC and LC/MS Modules

The following table lists selected instruments or modules that can not be controlled with the current revision of MassHunter Workstation.

Table 10. Incompatible LC and LC/MS Modules

Product Number	Module Name
G1361A	1260 Infinity Preparative Pump
G1362A	1100/1200 Refractive Index Detector
G1364A	1260 Infinity Preparative-Scale Fraction Collector
G1364B	1100 Fraction Collector
G1364C	1260 Infinity Analytical-Scale Fraction Collector
G1364D	1260 Infinity Micro-Scale Fraction Collector/Spotter
G1364E	1260 Infinity II Preparative-Scale Fraction Collector
G1364F	1260 Infinity II Analytical-Scale Fraction Collector
G1389A	1100 Micro-Scale Autosampler
G2258A	1260 Infinity Dual-Loop Autosampler
G2260A	1260 Infinity Preparative Autosampler
G4218A	1260 Infinity Evaporating Light-Scattering Detector
G4260A	380 Evaporative Light-Scattering Detector
G4260B	1260 Infinity Evaporative Light-Scattering Detector
G4261A	385 Evaporative Light-Scattering Detector
G4261B	1290 Infinity Evaporative Light-Scattering Detector

Product Number	Module Name
G5664A	1260 Infinity Bio-Inert Fraction Collector
G5664B	1260 II Infinity Bio-Inert Fraction Collector
G7102A	1290 Infinity II Evaporative Light-Scattering Detector
G7123B	1290 Infinity III Fluorescence Detector
G7157A	1260 Infinity II Preparative Autosampler
G7158B	1290 Infinity II Open-bed Sampler / Fraction Collector
G7159B	1290 Infinity II Preparative Open-Bed Fraction Collector
G7161A	1260 Infinity II Preparative Binary Pump
G7161B	1290 Infinity II Preparative Binary Pump
G7162A	1260 Infinity II Refractive Index Detector
G7162B	1290 Infinity II Refractive Index Detector
G7166A	1260 Infinity II Preparative Valve-Based Fraction Collector
G7169B	1290 Infinity II Open-bed Sampler / Fraction Collector
G7170B	1290 Infinity II MS Flow Modulator
G9322A	1260 Infinity II Clustering Valve

www.agilent.com

D0026036

October 2025 Revision A.01