Requirements for installing Unified Manager

Active IQ Unified Manager

NetApp
November 11, 2026

This PDF was generated from https://docs.netapp.com/us-en/active-iq-unified-manager/install-windows/concept_requirements_for_installing_unified_manager.html on November 11, 2026. Always check docs.netapp.com for the latest.

Table of Contents

Requirements for installing Unified Manager . . . 1
- Ensure the server meets Active IQ Unified Manager installation requirements . . . 1
- Understand virtual infrastructure and hardware requirements for Active IQ Unified Manager . . . 1
  - Requirement for dedicated use . . . 2
  - Space requirements for backups . . . 2
  - Requirements for host connectivity . . . 2
- Understand Windows software and installation requirements for Active IQ Unified Manager . . . 2
  - Operating system software . . . 2
  - Third-party software . . . 3
  - Installation requirements . . . 3
- Use supported browsers in Active IQ Unified Manager . . . 4
- Understand protocol and port requirements for Active IQ Unified Manager . . . 4
  - Connections to the Unified Manager server . . . 4
  - Connections from the Unified Manager server . . . 6
- Complete the worksheet in Active IQ Unified Manager . . . 7
  - Unified Manager installation information . . . 7
  - Unified Manager configuration information . . . 7
  - Cluster information . . . 8

Requirements for installing Unified Manager

Ensure the server meets Active IQ Unified Manager installation requirements

Before you begin the installation process, ensure that the server on which you want to install Unified Manager meets the specific software, hardware, CPU, and memory requirements.

NetApp does not support any modification of the Unified Manager application code. If you need to apply any security measures to the Unified Manager server, you should make those changes to the operating system on which Unified Manager is installed.

For more details about applying security measures to the Unified Manager server, see the Knowledge Base article.

Supportability for Security Measures applied to Active IQ Unified Manager for Clustered Data ONTAP

Related information

NetApp Interoperability Matrix Tool

Understand virtual infrastructure and hardware requirements for Active IQ Unified Manager

Installing Unified Manager on virtual infrastructure or a physical system should meet the minimum requirements for memory, CPU, and disk space.

The following table displays the values that are recommended for memory, CPU, and disk space resources. These values have been qualified so that Unified Manager meets acceptable performance levels.

Hardware configuration	Recommended settings
RAM	12 GB
Processors	4 CPUs
CPU cycle capacity	9572 MHz total (minimum requirement 9572 MHz)
Free disk space	150 GB, where the capacity is allocated as follows: • 100 GB of disk space for the installation directory • 50 GB of disk space for the MySQL data directory

Unified Manager can be installed on systems with a small amount of memory, but the recommended 12 GB of RAM ensures that enough memory is available for optimal performance, and so that the system can accommodate additional clusters and storage objects as your configuration grows. You should not set any memory limits on the VM where Unified Manager is deployed, and should not enable any features (for example, ballooning) that hinder the software from utilizing the allocated memory on the system.

Additionally, there is a limit to the number of nodes that a single instance of Unified Manager can monitor before you install a second instance of Unified Manager. For node limits, CPU, and memory recommendations,

see the Unified Manager Best Practices Guide.

Memory-page swapping negatively impacts the performance of the system and the management application. Competing for CPU resources that are unavailable because of overall host utilization can degrade performance.

Requirement for dedicated use

The physical or virtual system on which you install Unified Manager should be used exclusively for Unified Manager and should not be shared with other applications. Other applications might consume system resources and can drastically reduce the performance of Unified Manager.

Space requirements for backups

If you plan to use the Unified Manager backup and restore feature, allocate additional capacity so that the "data" directory or disk has 150 GB of space. A backup can be written to a local destination or to a remote destination. The best practice is to identify a remote location that is external to the Unified Manager host system that has a minimum of 150 GB of space.

Requirements for host connectivity

The physical system or virtual system on which you install Unified Manager should be configured in such a way that you can successfully `ping` the host name from the host itself. In case of IPv6 configuration, you should verify that `ping6` to the host name is successful to ensure that the Unified Manager installation succeeds.

You can use the host name (or the host IP address) to access the product web UI. If you configured a static IP address for your network during deployment, then you designated a name for the network host. If you configured the network using DHCP, you should obtain the host name from the DNS.

If you plan to allow users to access Unified Manager by using the short name instead of using the fully qualified domain name (FQDN) or IP address, then your network configuration has to resolve this short name to a valid FQDN.

Understand Windows software and installation requirements for Active IQ Unified Manager

For the successful installation of Unified Manager on Windows, you should ensure that the system on which Unified Manager is being installed meets the software requirements.

Operating system software

You can install Unified Manager on the following Windows editions:

- Microsoft Windows Server 2019 Standard and Datacenter Edition
- Microsoft Windows Server 2022 Standard and Datacenter Edition

Unified Manager is supported on 64-bit Windows operating system for the following languages:

- English
- Japanese

- Simplified Chinese

See the Interoperability Matrix for the complete and most current list of supported Windows versions.

mysupport.netapp.com/matrix

NetApp does not support installation of Unified Manager by using third-party tools, such as Microsoft System Center Configuration Manager (SCCM).

The server should be dedicated to running Unified Manager. No other applications should be installed on the server. It is possible that an active anti-virus software is installed on your Windows system because of company regulations. You should disable the anti-virus software before installing Unified Manager to prevent the installation from failing.

Third-party software

The following third-party packages are bundled with Unified Manager. If these third-party packages are not installed on your system, Unified Manager installs them as a part of the installation.

- Microsoft Visual C++ Redistributable Packages for Visual Studio 2015 version 14.29.30133.0
- MySQL Community Edition version 8.4.10
- Python 3.14.10
- OpenJDK version 17.0.15+6
- 7-zip version 25.01 or later

Starting with Unified Manager 9.5, OpenJDK is provided in the Unified Manager installation package and installed automatically. Oracle Java is not supported starting with Unified Manager 9.5.

If MySQL is pre-installed, you should ensure that:

- It is using the default port.
- The sample databases are not installed.
- The service name is “MYSQL84”.

Unified Manager is deployed on a WildFly web server. WildFly 27.0.1.Final is bundled and configured with Unified Manager.

You should shut down a running instance of Unified Manager before upgrading any third-party software. After the third-party software installation is complete, you can restart Unified Manager.

Installation requirements

- Microsoft .NET 4.5.2, or greater, should be installed.
- The `temp` directory should be configured with 2 GB of disk space for extracting the installation files. To verify whether the directory is created, run the following command on the command-line interface: `echo %temp%`
- You should reserve 2 GB of disk space in the Windows drive for caching the Unified Manager MSI files.

- The Microsoft Windows Server on which you want to install Unified Manager should be configured with a fully qualified domain name (FQDN) such that `ping` responses to the host name and FQDN are successful.
- You should disable Microsoft IIS worldwide web publishing service and ensure that ports 80 and 443 are free.
- You should make sure that the Remote Desktop Session Host setting for “Windows Installer RDS Compatibility” is disabled during the installation.
- UDP port 514 should be free, and should not be used by any other service.
- You should disable all anti-virus software on your system before installing Unified Manager. After your installation is complete, make sure to manually exclude the following paths from anti-virus scan:
  - Unified Manager data directory, for example, `C:\ProgramData\NetApp\OnCommandAppData\`
  - Unified Manager installation directory, for example, `\C:\Program Files\NetApp\`
  - MySQL data directory, for example, `C:\ProgramData\MySQL\MySQLServerData`

Use supported browsers in Active IQ Unified Manager

To access the Unified Manager web UI, use a supported browser.

The Interoperability Matrix has the list of supported browser versions.

mysupport.netapp.com/matrix

For all browsers, disabling pop-up blockers ensures that software features are displayed properly.

If you plan to configure Unified Manager for SAML authentication, so that an identity provider (IdP) can authenticate users, you should check the list of browsers supported by the IdP as well.

Understand protocol and port requirements for Active IQ Unified Manager

The required ports and protocols enable communication between the Unified Manager server and the managed storage systems, servers, and other components.

Connections to the Unified Manager server

In typical installations you do not have to specify port numbers when connecting to the Unified Manager web UI, because default ports are always used. For example, because Unified Manager always attempts to run on its default port, you can enter `https://<host>` instead of `https://<host>:443`.

The Unified Manager server uses specific protocols to access the following interfaces:

Interface	Protocol	Port	Description
Unified Manager web UI	HTTP	80	Used to access the Unified Manager web UI; automatically redirects to the secure port 443.

Interface	Protocol	Port	Description
Unified Manager web UI and programs using APIs	HTTPS	443	Used to securely access the Unified Manager web UI or to make API calls; API calls can only be made using HTTPS.
Maintenance console	SSH/SFTP	22	Used to access the maintenance console and retrieve support bundles.
Linux command line	SSH/SFTP	22	Used to access the Red Hat Enterprise Linux command line and retrieve support bundles.
Syslog	UDP	514	Used to access subscription-based EMS messages from ONTAP systems and to create events based on the messages.
REST	HTTPS	9443	Used to access realtime REST API-based EMS events from authenticated ONTAP systems.
MySQL database	MySQL	3306	Used to enable OnCommand Workflow Automation and OnCommand API Services access to Unified Manager.
AMQP QPID broker	TCP/IP	56072	Used for internal message communication.
AMQP QPID broker	WebSocket over TCP	56080	Used to listen on this port for messages received from ONTAP (cloud agent).
AMQP QPID broker	WebSocket over TCP	56443	Used to listen on this port for messages received from ONTAP (cloud agent).The communication over this port supports encryption provided by TLS or SSL.

The default port for MySQL, 3306, is restricted only to localhost while installing Unified Manager on Windows systems. Enable the firewall to restrict access for the port MySQL, 3306, once the installation is complete. This does not impact any upgrade scenario, where the previous configuration is maintained. This configuration can be modified, and the connection can be made available to other hosts by using the `Control access to MySQL port 3306` option on the maintenance console. For information, see Additional menu options. The ports used for

HTTP and HTTPS communication (ports 80 and 443) can be changed using the Unified Manager maintenance console. For more information, see Configuring Active IQ Unified Manager.

Connections from the Unified Manager server

You should configure your firewall to open ports that enable communication between the Unified Manager server and managed storage systems, servers, and other components. If a port is not open, communication fails.

Depending on your environment, you can choose to modify the ports and protocols used by the Unified Manager server to connect to specific destinations.

The Unified Manager server connects using the following protocols and ports to the managed storage systems, servers, and other components:

Destination	Protocol	Port	Description
Storage system	HTTPS	443/TCP	Used to monitor and manage storage systems.
Storage system	NDMP	10000/TCP	Used for certain Snapshot restore operations.
AutoSupport server	HTTPS	443	Used to send AutoSupport information. Requires the internet access to perform this function.
Authentication server	LDAP	389	Used to make authentication requests, and user and group lookup requests.
	LDAPS	636	Used for secure LDAP communication.
Mail server	SMTP	25	Used to send alert notification emails.
SNMP trap sender	SNMPv1 or SNMPv3	162/UDP	Used to send alert notification SNMP traps.
External data provider server	TCP	2003	Used to send performance data to an external data provider, such as Graphite.
NTP server	NTP	123/UDP	Used to synchronize the time on the Unified Manager server with an external NTP time server. (VMware systems only)
AMQP QPID broker	TCP/IP	56072	Used for internal message communication.

Destination	Protocol	Port	Description
AMQP QPID broker	WebSocket over TCP	56080	Used to listen on this port for messages received from ONTAP (cloud agent).
AMQP QPID broker	WebSocket over TCP	56443	Used to listen on this port for messages received from ONTAP (cloud agent). The communication through this port supports encryption provided by TLS or SSL.
Syslog	UDP	514	Used by Unified Manager to send audit logs to a remote syslog server.

Complete the worksheet in Active IQ Unified Manager

Before you install and configure Unified Manager, you should have specific information about your environment readily available. You can record the information in the worksheet.

Unified Manager installation information

The details required to install Unified Manager.

System on which software is deployed	Your value
Host fully qualified domain name	
Host IP address	
Network mask	
Gateway IP address	
Primary DNS address	
Secondary DNS address	
Search domains	
Maintenance user name	
Maintenance user password	

Unified Manager configuration information

The details to configure Unified Manager after installation. Some values are optional depending on your configuration.

Setting	Your value
Maintenance user email address	

Setting	Your value
SMTP server host name or IP address	
SMTP user name	
SMTP password	
SMTP port	25 (Default value)
Email from which alert notifications are sent	
Authentication server host name or IP address	
Active Directory administrator name or LDAP bind distinguished name	
Active Directory password or LDAP bind password	
Authentication server base distinguished name	
Identity provider (IdP) URL	
Identity provider (IdP) metadata	
SNMP trap destination host IP addresses	
SNMP port	

Cluster information

The details for the storage systems that you manage using Unified Manager.

Cluster 1 of N	Your value
Host name or cluster-management IP address	
ONTAP administrator user name The administrator must have been assigned the “admin” role.	
ONTAP administrator password	
Protocol	HTTPS

Copyright information

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.