Install Unified Manager on VMware vSphere systems

Active IQ Unified Manager

NetApp
November 11, 2026

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

Table of Contents

Install Unified Manager on VMware vSphere systems . . . 1
- Learn about Active IQ Unified Manager . . . 1
  - Learn about Active IQ Unified Manager . . . 1
  - Learn what the Active IQ Unified Manager server does . . . 1
  - Learn about the Active IQ Unified Manager installation sequence . . . 1
- Requirements for installing Unified Manager . . . 2
  - Ensure the server meets Active IQ Unified Manager installation requirements . . . 2
  - Learn about virtual infrastructure and hardware requirements for Active IQ Unified Manager . . . 2
  - Learn about VMware software and installation requirements for Active IQ Unified Manager . . . 3
  - Use supported browsers in Active IQ Unified Manager . . . 4
  - Learn about protocol and port requirements for Active IQ Unified Manager . . . 4
  - Complete the worksheet in Active IQ Unified Manager . . . 8
- Installation, upgrade, and removal of Unified Manager on VMware vSphere . . . 9
  - Learn about the Active IQ Unified Manager deployment process . . . 9
  - Unified Manager virtual appliance deployment workflow . . . 10
  - Unified Manager virtual appliance upgrade workflow . . . 14
  - Restart the Active IQ Unified Manager virtual machine . . . 16
  - Remove Active IQ Unified Manager . . . 17

Install Unified Manager on VMware vSphere systems

Learn about Active IQ Unified Manager

Learn about Active IQ Unified Manager

Active IQ Unified Manager (formerly OnCommand Unified Manager) enables you to monitor and manage the health and performance of your ONTAP storage systems from a single interface. You can deploy Unified Manager on a Linux server, on a Windows server, or as a virtual appliance on a VMware host.

After you have completed the installation and have added the clusters that you want to manage, Unified Manager provides a graphical interface that displays the capacity, availability, protection, and performance status of the monitored storage systems.

Related information

NetApp Interoperability Matrix Tool

Learn what the Active IQ Unified Manager server does

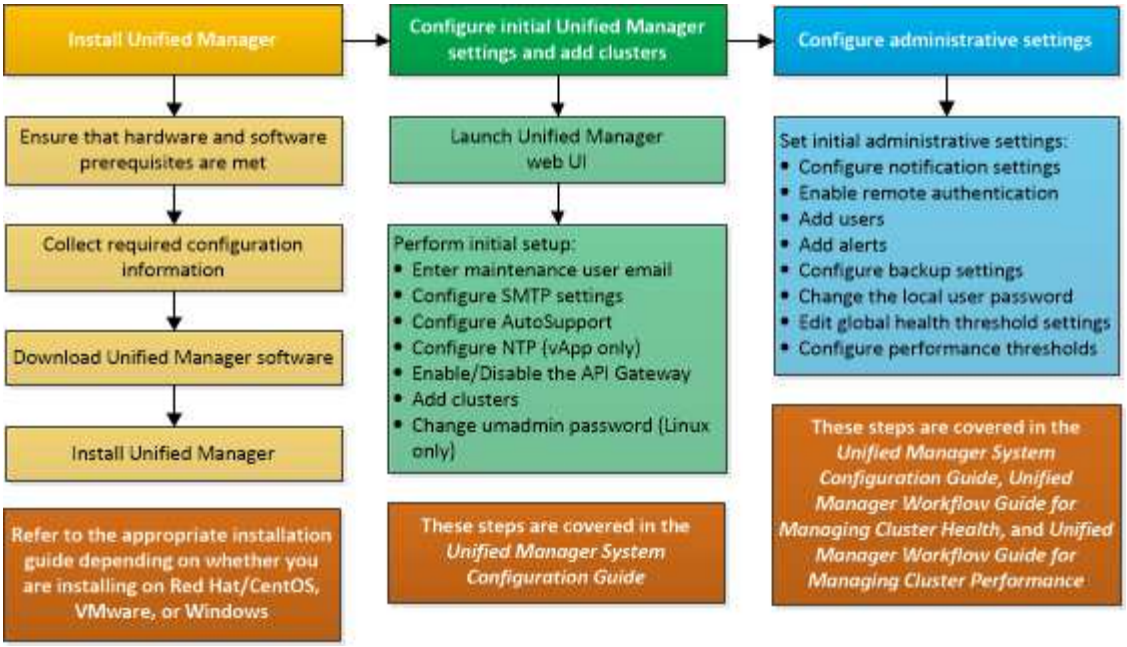
The Unified Manager server infrastructure consists of a data collection unit, a database, and an application server. It provides infrastructure services such as discovery, monitoring, role-based access control (RBAC), auditing, and logging.

Unified Manager collects cluster information, stores the data in the database, and analyzes the data to see if there are any cluster issues.

Learn about the Active IQ Unified Manager installation sequence

The installation workflow describes the tasks that you must perform before you can use Unified Manager.

These sections describe each of the items shown in the workflow below.



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

For more information, see NetApp Interoperability Matrix Tool

Learn about 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

Hardware configuration	Recommended settings
Processors	4 CPUs
CPU cycle capacity	9572 MHz total (minimum requirement 9572 MHz)
Free disk space	• 5 GB (thin provisioned) • 152 GB (thick provisioned)

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.

Learn about VMware software and installation requirements for Active IQ Unified Manager

The VMware vSphere system on which you install Unified Manager requires a specific

version of the operating system and specific versions of the supporting software.

Operating system software

The supported operating system is VMware ESXi 9.x or VMware ESXi 8.x.

> Unified Manager OVA on VMware vSphere systems runs Debian OS 13 (Trixie) internally. For information about the versions of the virtual machine hardware that the supported versions of ESXi servers can support, refer to the VMware documentation.

The following versions of vSphere are supported:

- VMware vCenter Server 7.0 and 8.0

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

mysupport.netapp.com/matrix

The VMware ESXi server time should be the same as the NTP server time for the virtual appliance to function correctly. Synchronizing the VMware ESXi server time with the NTP server time prevents a time failure.

Installation requirements

VMware High Availability for the Unified Manager virtual appliance is supported.

If you deploy an NFS datastore on a storage system that is running ONTAP software, use the NetApp NFS Plug-in for VMware VAAI to use thick provisioning.

If deployment fails using your High Availability-enabled environment because of insufficient resources, you might need to modify the Cluster Features Virtual Machine Options by disabling the VM Restart Priority, and leaving the Host Isolation Response powered on.

> While installing or upgrading Unified Manager, the required third-party software and security patches are automatically installed or upgraded on a VMware vSphere system. Because the Unified Manager installation and upgrade processes control these components, you should not attempt a standalone install or upgrade of any third-party component.

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.

Learn about 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.
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).

Interface	Protocol	Port	Description
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 VMware vSphere systems. 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 Maintenance console menus.

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. If you are using this port, or any other port to connect to the VMware vCenter Server or ESXi server, ensure that the port is available and can be connected in a secured site.
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)

Destination	Protocol	Port	Description
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.
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
ESXi server IP address	
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	
NTP server	
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

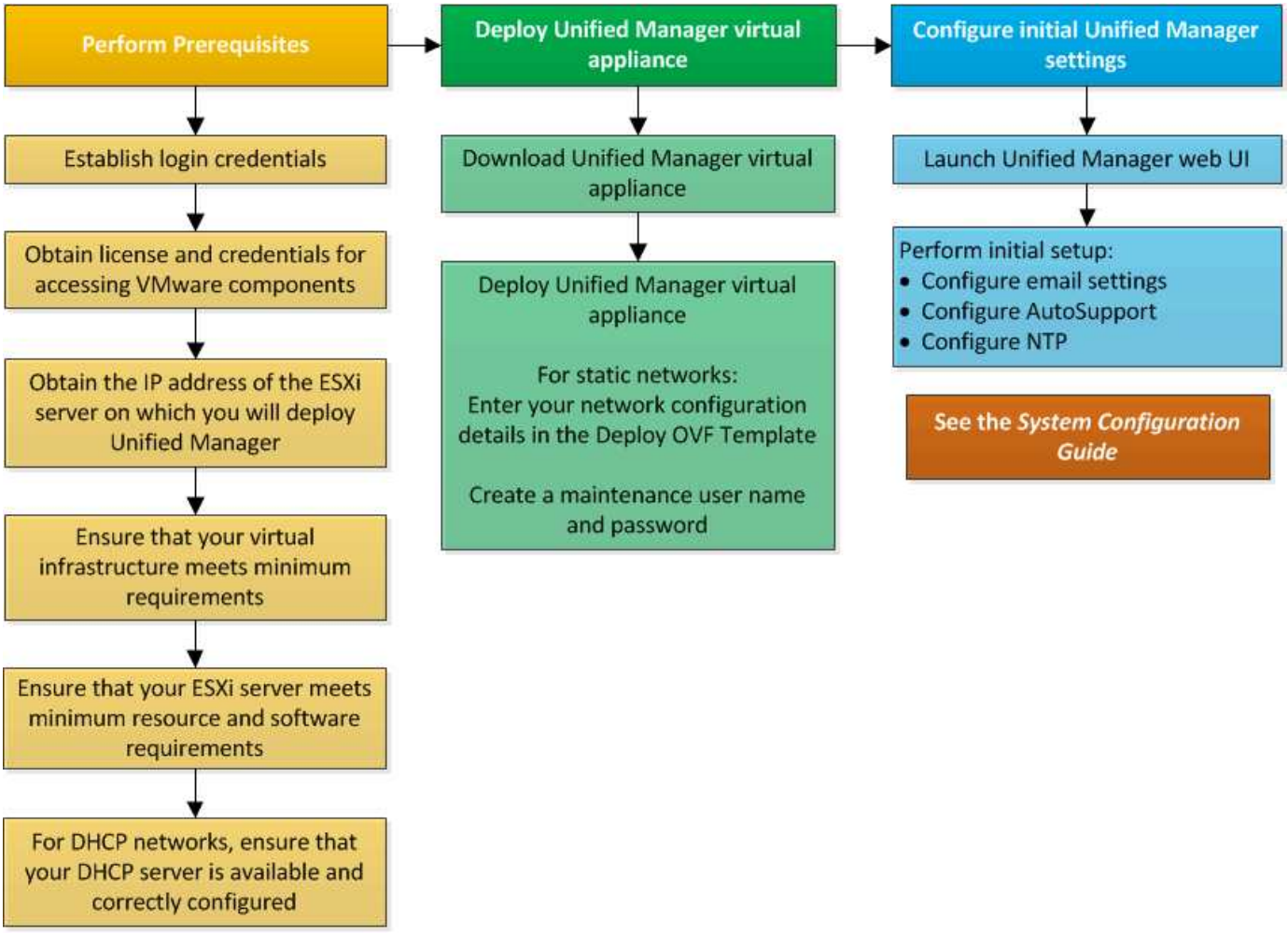
The details for the storage systems that you manage using Unified Manager.

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

Installation, upgrade, and removal of Unified Manager on VMware vSphere

Learn about the Active IQ Unified Manager deployment process

The deployment workflow describes the tasks that you must perform before you can use Unified Manager.



Unified Manager virtual appliance deployment workflow

Deploy Active IQ Unified Manager

Deploying Unified Manager includes downloading software, deploying the virtual appliance, creating a maintenance user name and password, and performing the initial setup in the web UI.

Before you begin

- You should verify and complete the system requirements for deployment.

  See System requirements.

- Ensure that you have the following information:
  - Login credentials for the NetApp Support Site
  - Credentials for accessing the VMware vCenter Server and vSphere Web Client
  - IP address of the ESXi server on which you are deploying the Unified Manager virtual appliance
  - Details about the data center, such as storage space in the datastore and memory requirements
  - IPv6 should be enabled on the host if you are planning to use IPv6 addressing.

You can deploy Unified Manager as a virtual appliance on a VMware ESXi server.

You should access the maintenance console by using the VMware console, and not by using SSH.

> Starting with Unified Manager 9.8, VMware Tools has been replaced with Open VM Tools (`open-vm-tools`). You no longer have to install VMware Tools as part of the installation because `open-vm-tools` is included with the Unified Manager installation package.

After finishing the deployment and initial setup, you can either add clusters, or configure additional network settings in the maintenance console, and then access the web UI.

Steps

1. Follow the steps in Download Unified Manager.
2. Additionally, follow the steps in Deploy the Unified Manager virtual appliance.

Download the Active IQ Unified Manager installation file

Download the Unified Manager installation file from the NetApp Support Site to deploy Unified Manager as a virtual appliance.

Before you begin

You should have the login credentials for the NetApp Support Site.

The installation file is a `.tar` file that contains a root certificate, a `README` file, and an `OVA` file containing Unified Manager software configured for a virtual appliance.

Steps

1. Log in to the NetApp Support Site, and navigate to the Download page for Unified Manager:

   NetApp Support Site

2. Select the required version of Unified Manager and accept the end-users license agreement (EULA).
3. Download and save the `.tar` file for VMware vSphere installation to a local directory or network directory that is accessible to your vSphere Client.
4. Verify the checksum to ensure that the software downloaded correctly.
5. Navigate to the directory where you downloaded the `.tar` file and enter the following command in your terminal window to expand the Unified Manager bundle:

   ```
   tar -xvzf ActiveIQUnifiedManager-<version>.tar.gz
   ```

   The required `OVA` file, a root certificate, and a `README` file for Unified Manager are unzipped to the target directory.

6. Verify the integrity of the `OVA` file by following the steps provided in the `README` file.

Deploy the Active IQ Unified Manager virtual appliance

After downloading the installation file, you deploy Unified Manager as a virtual appliance. Use the vSphere Web Client to deploy the virtual appliance on an ESXi server. When you deploy the virtual appliance, a virtual machine is created.

Before you begin

You should review the system requirements. Make the necessary changes before deploying the Unified Manager virtual appliance.

See Virtual infrastructure requirements.

See VMware software and installation requirements.

If you use Dynamic Host Configuration Protocol (DHCP), ensure that the DHCP server is available, and that the DHCP and virtual machine (VM) network adapter configurations are correct. DHCP is configured by default.

If you use a static networking configuration, ensure that the IP address is not duplicated in the same subnet, and that the appropriate DNS server entries have been configured.

Obtain the following information before deploying the virtual appliance:

- Credentials for accessing the VMware vCenter Server and vSphere Web Client
- IP address of the ESXi server on which you are deploying the Unified Manager virtual appliance
- Details about the data center, such as availability of storage space
- If you are not using DHCP, obtain the IPv4 or IPv6 addresses for the networking devices to which you are planning to connect:
  - Fully qualified domain name (FQDN) of the host
  - IP address of the host
  - Network mask
  - IP address of the default gateway
  - Primary and secondary DNS addresses
  - Search domains

Starting with Unified Manager 9.8, VMware Tools has been replaced with Open VM Tools (`open-vm-tools`). You do not have to install VMware Tools as part of the installation process because `open-vm-tools` is included with the Unified Manager installation package.

When the virtual appliance is deployed, a unique self-signed certificate for HTTPS access is generated. When accessing the Unified Manager web UI, you might see a browser warning about untrusted certificates.

VMware High Availability for the Unified Manager virtual appliance is supported.

Steps

1. In the vSphere Client, click **File** > **Deploy OVF Template**.
2. Complete the Deploy OVF Template wizard to deploy the Unified Manager virtual appliance.

   On the Review Details page:

   - Verify the details of the Publisher section. The message **Entrust Code Signing - OVCS2 (Trusted certificate)** confirms the integrity of the downloaded `OVA` file.
     If you see the message **Entrust Code Signing - OVCS2 (Invalid certificate)**, then upgrade the VMware vCenter Server to 7.0U3E or greater version.

     On the Customize Template page:

- Leave all the fields blank when using DHCP and IPv4 addressing.
- Check the “Enable Auto IPv6 addressing” box, and leave all the other fields blank when using DHCP and IPv6 addressing.
- If you want to use a static network configuration, you can complete the fields on this page and these settings are applied during deployment. Ensure that the IP address is unique to the host on which it is deployed, that it is not already in use, and that it has a valid DNS entry.

3. After the Unified Manager virtual appliance is deployed to the ESXi server, power on the VM by right-clicking the VM, and then selecting **Power On**.

   If the Power On operation fails because of insufficient resources, add resources and then retry the installation.

4. Click the **Console** tab.

   The initial boot process takes a few minutes to complete.

5. To configure your time zone, enter your geographic area and your city or region as prompted in the VM Console window.

   All the date information that is displayed uses the time zone that is configured for Unified Manager, regardless of the time zone setting on your managed devices. If your storage systems and the management server are configured with the same NTP server, they refer to the same instant in time, even if they appear differently. For example, if you create a Snapshot copy using a device that is configured using a different time zone than that of the management server, the time stamp is the management server time.

6. If no DHCP services are available, or if there is an error in the details for the static network configuration, select one of the following options:

If you use…	Then do this…
DHCP	Select **Retry DHCP**. If you plan to use DHCP, you should ensure that it is configured correctly. If you use a DHCP-enabled network, the FQDN and DNS server entries are given to the virtual appliance automatically. If DHCP is not properly configured with DNS, the host name “UnifiedManager” is automatically assigned and associated with the security certificate. If you have not set up a DHCP-enabled network, you should manually enter the networking configuration information.
A static network configuration	a. Select **Enter the details for static network configuration**. The configuration process takes a few minutes to complete. b. Confirm the values that you entered, and select **Y**.

7. At the prompt, enter a maintenance user name, and then click **Enter**.

The maintenance user name should start with a letter from a-z, followed by any combination of -, a-z, or 0-9.

8. At the prompt, enter a password, and then click **Enter**.

   The VM console displays the URL for the Unified Manager web UI.

You can access the web UI to perform the initial setup of Unified Manager, as described in the Configuring Active IQ Unified Manager.

Unified Manager virtual appliance upgrade workflow

Upgrade Active IQ Unified Manager

You can upgrade Active IQ Unified Manager to release 9.20 from release 9.16 or 9.18 only.

During the upgrade process, Unified Manager is unavailable. You should complete any running operations before upgrading Unified Manager.

If Unified Manager is paired with an instance of OnCommand Workflow Automation, and there are new versions of software available for both products, you must disconnect the two products and then set up a new Workflow Automation connection after performing the upgrades. If you are performing an upgrade to only one of the products, then you should log into Workflow Automation after the upgrade and verify that it is still acquiring data from Unified Manager.

> If you are upgrading from Unified Manager 9.7, you cannot upgrade directly from 9.14 to 9.20 because of file system changes in the Debian versions. If you are running a version that is earlier than the supported versions, your Unified Manager instance will need to be upgraded to one of the supported versions first, and then upgraded to the current version. Follow this recommended upgrade path: 9.14 → 9.16P2 → 9.20

Steps

1. Follow the steps in Download the Unified Manager ISO image.
2. Additionally, follow the steps described in Upgrade Unified Manager.

Use the supported upgrade path for versions of Active IQ Unified Manager

Active IQ Unified Manager supports a specific upgrade path for each version.

Not all versions of Unified Manager can perform an in-place upgrade to later versions. The Unified Manager upgrades are limited to an N-2 model. This means that you can only perform an upgrade to the next two releases on all platforms. For example, you can perform an upgrade to Unified Manager 9.20 from Unified Manager 9.16 and 9.18 only.

If you are running a version that is earlier than the supported versions, your Unified Manager instance will need to be upgraded to one of the supported versions first, and then upgraded to the current version.

For example, if your installed version is Unified Manager 9.11 and you want to upgrade to Unified Manager 9.20, you follow a sequence of upgrades.

Sample upgrade path:

1. Upgrade 9.11 → 9.13
2. Upgrade 9.13 → 9.14
3. Upgrade 9.13 → 9.16
4. Upgrade 9.14 or 9.16 → 9.18
5. Upgrade 9.16 or 9.18 → 9.20

For more information on the upgrade path matrix, see this knowledge base (KB) article.

Download the Active IQ Unified Manager upgrade file

Before upgrading Unified Manager, download the Unified Manager upgrade file from the NetApp Support Site.

Before you begin

You should have login credentials for the NetApp Support Site.

Steps

1. Log in to the NetApp Support Site:

   NetApp Support Site

2. Navigate to the Download page for upgrading Unified Manager on VMware vSphere.
3. Download the `.iso` image for upgrade, and save it to a local directory or network directory that is accessible to your vSphere Client.
4. Verify the checksum to ensure that the software has downloaded correctly.

Upgrade the Active IQ Unified Manager virtual appliance

You can upgrade the Active IQ Unified Manager virtual appliance from releases 9.16 or 9.18 to 9.20.

Before you begin

Ensure the following:

- You have downloaded the upgrade file and the ISO image from the NetApp Support Site.
- The system on which you are upgrading Unified Manager meets the system and software requirements.

  See Virtual infrastructure requirements.

  See VMware software and installation requirements.

- For vSphere 6.5 and later users, you have installed the VMware Remote Console (VMRC).
- During upgrade, you may be prompted to confirm on whether you want to keep the previous, default settings for retaining performance data for 13 months or to change it to 6 months. On confirming, the historical performance data is purged after 6 months.
- You have the following information:
  - Login credentials for the NetApp Support Site
  - Credentials for accessing the VMware vCenter Server and vSphere Web Client

- Credentials for the Unified Manager maintenance user

During the upgrade process, Unified Manager is unavailable. You should complete any running operations before upgrading Unified Manager.

If you have paired Workflow Automation and Unified Manager, you should manually update the host name in Workflow Automation.

Steps

1. In the vSphere Client, click **Home** > **Inventory** > **VMs and Templates**.
2. Select the virtual machine (VM) on which the Unified Manager virtual appliance is installed.
3. If the Unified Manager VM is running, navigate to **Summary** > **Commands** > **Shut Down Guest**.
4. Create a backup copy, such as a snapshot or a clone, of the Unified Manager VM to create an application-consistent backup.
5. From the vSphere Client, power on the Unified Manager VM.
6. Launch the VMware Remote Console.
7. Click the **CDROM** icon, and select **Connect to Disk Image File (.iso)**.
8. Select the `ActiveIQUnifiedManager-<version>-virtual-update.iso` file, and click **Open**.
9. Click the **Console** tab.
10. Log in to the Unified Manager maintenance console.
11. In the Main Menu, select **Upgrade**.

    A message is displayed that Unified Manager is to be unavailable during the upgrade process, and is to resume after completion.

12. Type `y` to continue.

    A warning is displayed, reminding you to back up the virtual machine on which the virtual appliance resides.

13. Type `y` to continue.

    The upgrade process and the restart of Unified Manager services can take several minutes to complete.

14. Press any key to continue.

    You are automatically logged out of the maintenance console.

15. **Optional:** Log in to the maintenance console, and verify the version of Unified Manager.

You can launch the web UI on a new window on a supported web browser and log in to use the upgraded version of Unified Manager. Note that you need to wait for the discovery process to finish before performing any task in the UI.

Restart the Active IQ Unified Manager virtual machine

You can restart the Unified Manager virtual machine (VM) from the maintenance console. You should restart the VM after generating a new security certificate, or if there is a problem with the VM.

Before you begin

- The virtual appliance should be powered on.
- You should be logged in to the Unified Manager maintenance console as the maintenance user.

You can also restart the virtual machine from vSphere by using the VMware **Restart Guest** option. Refer to the Restart-VMGuest cmdlet in Broadcom's VMware vSphere PowerCLI CMDLET reference.

Steps

1. In the maintenance console, select **System Configuration** > **Reboot Virtual Machine**.
2. Start the Unified Manager web UI from your browser, and log in.

Remove Active IQ Unified Manager

You can uninstall Unified Manager by removing the virtual machine (VM) on which the Unified Manager software is installed.

Before you begin

- You should have credentials for accessing VMware vCenter Server and vSphere Web Client.
- Any active connection of the Unified Manager server to a Workflow Automation server should be closed.
- All clusters (data sources) should be removed from the Unified Manager server before you remove the virtual machine (VM).

Steps

1. Use the Unified Manager maintenance console to verify that the Unified Manager server does not have an active connection to an external data provider.
2. In the vSphere Client, click **Home** > **Inventory** > **VMs and Templates**.
3. Select the VM that you want to remove, and click the **Summary** tab.
4. If the VM is running, click **Power** > **Shut Down Guest**.
5. Right-click the VM that you want to remove, and click **Delete from Disk**.

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.