Quest® Active Administrator® 8.6

Release Notes

May 2022

These release notes provide information about this Quest® Active Administrator® release.

Topics

About this release

Active Administrator is a complete, integrated, and proactive Microsoft® Active Directory® administration solution that fills the management gaps system-provided tools leave behind. From a single console, the solution addresses the most important areas of Active Directory including security and delegation, auditing and alerting, backup and recovery, Group Policy, health and replication, and accounts and configurations. Active Administrator makes it easier and faster than system-provided tools to meet auditing requirements, tighten security, maintain business continuity, and increase IT efficiency.

Active Administrator 8.6 is a minor release, with new features and functionality. See New features.

New features

As a result of ongoing research and development, and in response to customer feedback, the following enhancements have been made in this release of Active Administrator:

Topics

Additional Supported Platforms

The following platforms are now supported in Active Administrator.

- Azure SQL Managed instance
- Windows Server 2022

User Provisioning

With the rise of data breaches within organizations, it has become increasingly important to ensure users are created with proper access as they join an organization as well providing an easy way to remove that access when they leave. Ensuring user's access is up-to-date through provisioning is a time consuming process that typically needs to be done immediately and has the potential for human error.

Active Administrator is extending its user management capabilities by providing the ability to automate provisioning and de-provisioning of users accounts.

When you begin the provisioning or deprovisioning process, a log file that tracks your provisioning actions is created, stored on the server until purged, and available to view in the client for troubleshooting purposes.

NOTE: The provisioning feature is enabled through role-based access.

- By default, all users are granted the User Provisioning read-only access role.
- Users who hold the Full Access role are automatically granted the User Provisioning role.

Active Directory Health enhancements

- Ability to review the selected alerts included in a notification before completing the configuration.

Auditing and alerting enhancements

- Ability to search for accounts to exclude by name, group, or OU.
- Ability to select the time zone for scheduled reports.

Installation and upgrade enhancements

- Ability for a non-administrator to run Active Administrator without User Account Control (UAC).
- Ability to use Azure SQL Managed Instance for live and archive databases.

The New Active Administrator Database and New Active Administrator Archive Database dialogs have been extended to allow you to connect to an Azure SQL Managed Instance using the required Azure Active Directory or SQL Server authentication.

Certificate updates

- The Certificate Management window has been updated to include a tree view that, by default, displays the computers being managed with the Certificate module in your organization and all the associated certificates. From here, you can also select to create a virtual folder structure to help visually organize those certificates to facilitate their management.

Security and delegation updates

- Ability to copy text from objects in Active Directory Security & Delegation's security dialog.
- Ability to sort the contents in the inactive users preview and history panes by selecting the column header.
- Ability to set the number of days before a user and computer account is disabled after it has been deemed inactive.
- Ability to select to include either both inactive user and computer accounts or just one type in email notifications.
- Ability to set a schedule for sending inactive account email notifications.

See also:

- Resolved issues

Resolved issues

The following is a list of issues addressed in this release.

Table 1. Resolved issues

Resolved issue	Issue ID
The Active Directory Domain Test under the DNS Modeling feature is showing a false failure when querying for domain root.	325402
Domain Users built in group members are not displaying in the Security and Delegation module.	264262
AD Health inaccurate disk space warning issued when the domain controller cannot be contacted through WMI.	242624
Unable to select source and target domain controllers when creating a replication tests in Active Directory Health Troubleshooter.	242635
Updated jQuery used by the web console to the latest version 3.6.	244970
TCP Port Exhaustion occurring on the ADS service host computer in large environments with many AD Health agents.	245229
"AD version" column on regular auditing agent displays the incorrect version.	246523
Unable to purge computer accounts if bitlocker is enabled on the computer.	256716

Table 1. Resolved issues

Resolved issue	Issue ID
Restore failing on non-English operating systems.	257823
AD Health frequent NULL HeartBeat values in the database (Null DC, Site, Domain, Forest).	261523
AD Health unable to apply templates to domain controllers unless they contain the same alert settings.	264643
Logout now forcefully ends user session in web console.	268883
Issue with AD health custom remediation action for deleting conflict folder contents.	268887
Unable to changes to the Dashboard view in the web console.	293297
AD Health unable to monitor domain controllers named using DC-Name format.	329067

Known issues

The following is a list of known issues to exist at the time of release.

Table 2. Known issues

Known issues	
Unable to add a large number of certificates (50+) to a repository when running Azure Active Directory Connect on monitored computers.	227571
AD Health: An object reference error is generated when attempting to delete a custom event log item that was not deployed to all DCs.	227629
Unable to create a new archive database using "SQL, port" format in the Configuration | Archive Databases | New | Database Server option.	229028

System requirements

The system requirements are the same for all components of Active Administrator. Before installing or upgrading Active Administrator, ensure that your system meets the following minimum hardware and software requirements.

IMPORTANT: You must be an administrator for the computer on which you are installing Active Administrator Server. You must have the credentials of an account that can be used to create a database on the server running SQL Server.

Topics

- Server hardware requirements
- Server software requirements
- SQL Server requirements
- Console requirements
- Audit agents requirements
- Workstation logon audit agents requirements
- Web Console requirements
- System Center requirements

- Port requirements
- User privilege requirements
- Active Administrator module requirements
- Upgrade and compatibility
- Product licensing

Server hardware requirements

The server is the computer where you install the server component of Active Administrator.

IMPORTANT: You must be an administrator for the computer on which you are installing Active Administrator Server. You must have the credentials of an account that can be used to create a database on the server running SQL Server.

The following table outlines the server hardware requirements.

Table 3. Server hardware requirements

Requirement	Details
Processor	1 GHz or higher
Memory	• For Windows Server 2012: 1 GB minimum, 2 GB recommended • For Windows Server 2012 R2: 1 GB minimum, 2 GB recommended • For Windows Server 2016: 1 GB minimum, 2 GB recommended • For Windows Server 2019: 1 GB minimum, 2 GB recommended
Hard disk space	100 MB
Operating system	• Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022 **NOTE:** Active Administrator does not support Microsoft Nano Server 2016.

Server software requirements

The following table outlines the server software requirements.

Table 4. Server software requirements

Requirement	Details
.NET Framework 4.7.2	Install either the Full or Standalone version. Do not install just the Client Profile. Visit https://privacy.microsoft.com/en-us/privacystatement to view Microsoft's privacy policy related to the data being collected and shared with Microsoft. Visit http://go.microsoft.com/fwlink/?LinkId=825925 to see Microsoft's explanation of their data collection practices.
Group Policy Management Console (GPMC)	GPMC is included with Windows Server 2008 R2 and later, but is not installed with the operating system. Use Server Manager to install GPMC. After installation, enable GPMC through the Server Manager **Add Features** Wizard. You can launch the Add Features Wizard through **Control Panel | Programs and Features | Turn Windows features on or off**. Alternatively, from the command line, use `ServerManagerCmd -install GPMC`.

IMPORTANT: You must be an administrator for the computer on which you are installing Active Administrator Server. You must have the credentials of an account that can be used to create a database on the server running SQL Server.

SQL Server requirements

The following versions of Microsoft SQL Server are supported. See the Microsoft web site for the hardware and software requirements for your version of SQL Server.

IMPORTANT: You must have the credentials of an account that can be used to create a database on the server running SQL Server.

- SQL Server 2014
- SQL Server 2014 Express
- SQL Server 2016
- SQL Server 2017
- SQL Server 2019

IMPORTANT: On the server running SQL Server, you must enable Named Pipes communication, which is off by default.

Active Administrator requires the default collation for the audit database. In SQL Server, collation refers to a set of rules that determine how data is sorted and compared. Active Administrator supports only the default collation and sort order configurations for the audit database.

If you are unsure of the collation assigned to the audit database, use the Microsoft ISQL_w or Query Analyzer tools, connect to the database, enter **sp_helpsort**, and run the statement. The results list all sort and collation information for the database.

Console requirements

Topics:

- Console hardware requirements
- Console software requirements

Console hardware requirements

The following table outlines the console hardware requirements.

Table 5. Console hardware requirements

Requirement	Details
Processor	1 GHz
Memory	256 MB
Hard disk space	100 MB
Operating system	• Windows 8.1 • Windows 10 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 **NOTE:** Active Administrator does not support Microsoft Nano Server 2016. **NOTE:** If you are using the Certificate module, see Table 6 for information on support for SHA-2 certificates.

The following table outlines the support for SHA-2 certificates.

Table 6. Support for SHA-2 certificates

Operating system	Support SHA-2 certificates	Verify SHA-2 certificates (user mode)	Verify SHA-2 certificates (kernel mode)
Windows Server 2012	supported	supported	supported
Windows Server 2012 R2	supported	supported	supported
Windows Server 2016	supported	supported	supported
Windows Server 2019	supported	supported	supported
Windows 8.1	supported	supported	supported
Windows 10	supported	supported	supported

Console software requirements

The following software is required for the Active Administrator console.

- .NET Framework 4.7.2
- Group Policy Management Console (GPMC)
- DNS Server Tools

The following table outlines the GPMC and DNS Server Tools install information.

Table 7. GPMC and DNS Server Tools install information

Operating System	Download Links and Install Information
Windows 8.1 Windows 10	GPMC, DNS Server, and AD DS and AD LDS Tools are included in Remote Server Administration Tools (RSAT). For downloads, see https://support.microsoft.com/en-us/help/2693643/remote-server-administration-tools-rsat-for-windows-operating-systems. ***To activate the required tools*** 1 Open the Control Panel, click **Programs and Features**, and click **Turn Windows features on or off**. 2 Expand Remote Server Administration Tools. 3 Expand Feature Administration Tools, and select Group Policy Management Tools. 4 Expand Role Administration Tools, select DNS Server Tools and AD DS and AD LDS Tools.
Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019	***To active GMPC*** • The Group Policy Management Console, once installed, must be enabled through the Add Features Wizard in Server Manager. Alternatively, from the command line, use **ServerManagerCmd –install GPMC**. ***To install DNS Server Tools*** 1 Open the **Server Manager**. 2 Select **Manage | Add Features**. 3 Expand **Remote Server Administration Tools**. 4 Expand **Role Administration Tools**. 5 Select **DNS Server Tools**. 6 Advance through the wizard to **Confirmation**. 7 Click **Install**.

Audit agents requirements

The following table outlines the audit agents hardware requirements.

Table 8. Audit agents hardware requirements

Requirement	Details
Processor	1 GHz or higher
Hard disk	100 MB
Memory	256 MB
Operating systems	• Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019

Workstation logon audit agents requirements

The following table outlines the workstation logon audit agents requirements.

Table 9. Workstation logon audit agent hardware requirements

Requirement	Details
Processor	1 GHz or higher
Hard disk	100 MB
Memory	256 MB
Operating systems	• Windows 8.1 • Windows 10 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019

Web Console requirements

You can open Active Administrator Web Console on a variety of devices in the following browsers:

- Microsoft® Internet Explorer 11
- Microsoft Edge™ 98
- Google Chrome™ 98
- Mozilla® Firefox® 97

System Center requirements

The following versions of Microsoft® System Center Operations Manager are supported.

- System Center 2016 Operations Manager
- System Center 2012 R2 Operations Manager
- System Center 2012 SP1 Operations Manager

Port requirements

NOTE: All ports need to be open (incoming/outgoing) with the exception of the Workstation Logon agent which only needs to be outgoing on the workstation's firewall and incoming on the Active Administrator Server. Figure 1 displays an example of how communication is achieved through the specified ports.

Active Administrator Console

- TCP 15600 for Active Administrator Foundation Service (AFS) communication with Active Administrator Server

- TCP 8080 for communication with Active Administrator Web Server through the Web Console (internal, http)
- TCP 9443 for communication with Active Administrator Web Server through the Web Console (external, https)
- TCP 389 for communication with Active Directory on domain controllers

Active Administrator Server

- TCP 15600 for communication with Active Administrator Foundation Service (AFS)
- TCP 15601 incoming only communication from Workstation Logon agents
- TCP 15602 for communication with Active Administrator Data Service (ADS)
- TCP 15603 for communication with Active Directory Health Analyzer agents
- TCP 15604 for communication with Azure Active Directory Connect agents
- TCP 1433 for communication with SQL Server
- TCP 8080 for communication as a Web Server for Active Administrator Web Consoles (internal, http)
- TCP 9443 for communication as a Web Server for Active Administrator Web Consoles (external, https)
- TCP 389 for communication with Active Directory on domain controllers

Active Administrator database server

- TCP 1433 for SQL communication with Active Administrator Server and domain controllers with auditing agents

Domain controller with no installed agents

- TCP 389 for communication with Active Administrator Server and Active Administrator Consoles

Domain controller with auditing agent

- TCP 1433 for communication with SQL Server

Domain controller with Active Directory Health Analyzer agent

- TCP 15602 for communication with Active Administrator Data Service (ADS)
- TCP 15603 for communication through the Active Directory Health Analyzer agent

Domain controller with Azure Active Directory Connect agent

- TCP 15604 for communication through the Azure Active Directory Connect agent

Member server with Active Directory Health Analyzer agent (pool agent)

- TCP 15602 for communication with Active Administrator Data Service (ADS)
- TCP 15603 for communication through the Active Directory Health Analyzer Agent

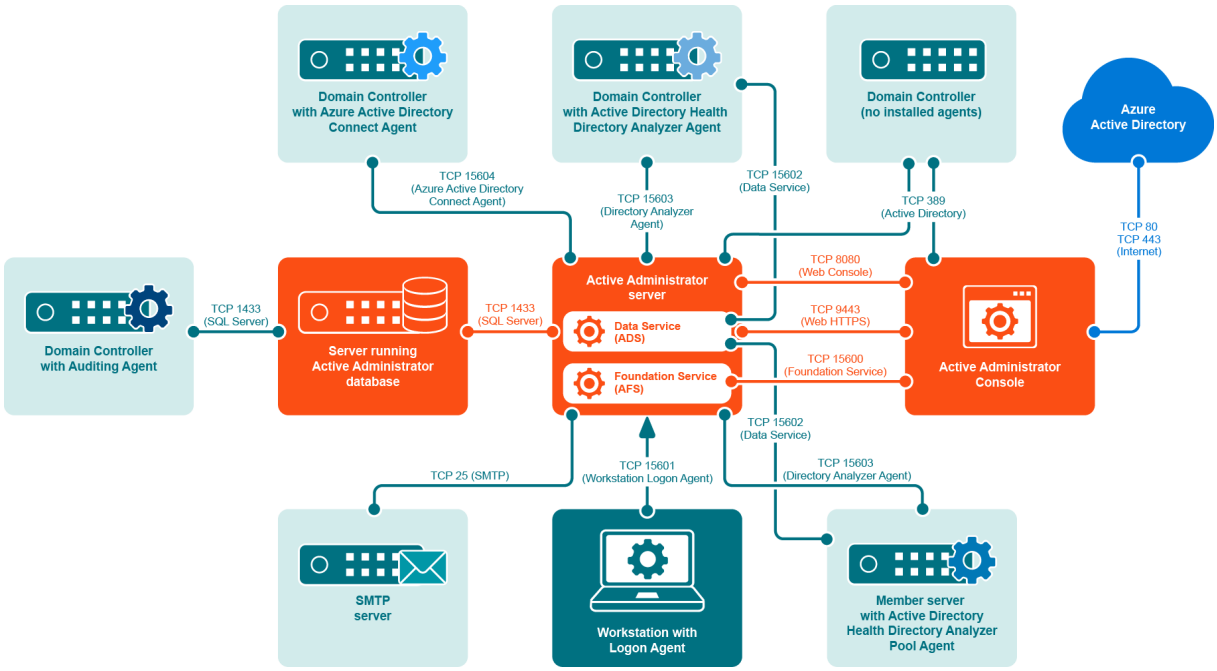
SMTP server

- TCP 25 for sending email notifications via SMTP

Workstation with logon agent

- TCP 15601 outgoing only for communication to Active Administrator Server through Workstation Logon agent

Figure 1. Port requirements example



Additional requirements

- Remote Procedure Call (RPC) must be open between the AFS Server and the target.
- When installing the audit agent on a member server instead of a domain controller, the following inbound firewall exceptions for Windows Management Instrumentation must be enabled:
  - ASync-In
  - DCOM-In
  - WMI-In
- If you are using the Certificate Management feature, Remote Registry Service must be enabled on all Windows computers on which certificates are managed.
- If you want to access the DNS event logs in Active Administrator, the following inbound firewall exceptions are required on each DNS server:
  - COM+ Network Access (DCOM-In)
  - Remote Event Log Management (NP-In)
  - Remote Event Log Management (RPC)
  - Remote Event Log Management (RPC-EPMAP)
- HTTP Port 8080 must be open on the computer running the Web Server.

IMPORTANT: It is recommended that you only use the Web Console internal to the network. If you want to use the Web Console externally, use HyperText Transfer Protocol Secure (HTTPS) by enabling Secure Sockets Layer (SSL). You need to select a certificate, which must be installed in the Personal or My store on the local computer. The default port is 9443. See the *Web Console User Guide* for more instructions on configuring the Web Server.

User privilege requirements

- To install Active Administrator, a user must hold administrative rights on the local system and the SQL instance that will host the Active Administrator database.
- To use Active Administrator, a user must hold administrative rights on both the local system and the domain, and be a member of the AA_Admin database access group, which is created during the installation process.

Password recovery

Active Administrator can restore passwords when you restore accounts that were deleted. To enable password recovery, a minor modification is made to the Schema. To be able to modify the Schema, you must use an account that is a member of the Schema Admins group.

Services

The Domain Administrator account provides the necessary permissions for the various Active Administrator services to operate properly.

When choosing an account, keep these requirements in mind:

- Active Administrator Foundation service (AFS) requires an account that is a member of the Domain Admins group. For more detailed permission requirements, see Active Administrator module requirements.
- Active Administrator Data Services (ADS) requires an account that is a member of the AA_Users group, has read access to the enterprise, and has full access on the server where the Active Directory Health Analyzer agent is installed. For more detailed permission requirements, see Active Administrator Data Services (ADS) requirements.
- Active Administrator Advanced Auditing runs as the Local System account, regardless of the user account configured for the Active Administrator Agent service.
- Active Administrator Agent can run under a Domain User account provided it is a local administrator account, which gives it the rights to log on as a service, log on locally and manage auditing and security log. The user account should also be a member of the AA_Admin group, which by default is located in the Local groups of the server where the ActiveAdministrator database is located. If the group is not found in this location, the settings during the initial database creation were modified and it can be found under the Users container object of Active Directory.
- Active Administrator Agent can run under a non-domain admin user account if the following permissions are set.

  To set up a non-domain admin user account

  1. Create a Domain User account within Active Directory Users and Computers.
  2. Use Group Policy Management console (GPMC) to edit the Default Domain Controller Group Policy Object. Give the user account **User Rights** to **Manage auditing and security log**.
  3. On the target domain controllers, give the user account Read permission to the registry key: **HKLM\System\CurrentControlSet\Services\Eventlog\Security**.
  4. After the agent is installed, verify the user account has Write permission on the folder: **C:\Windows\SLAgent**.

  NOTE: For more detailed instructions, see https://support.quest.com/active-administrator/kb/209446/how-to-configure-a-non-domain-admin-audit-agent-service-account.

- Active Administrator Notification service needs to have access to the database.

Audit database

On the database server, the database installation creates two local groups that control access to the audit database.

- AA_Admin group = users that need to be able to update the database
- AA_User group = users that only need to run reports from the database

Active Administrator module requirements

For all Active Administrator® modules to operate properly, the Active Administrator Foundation service (AFS) requires an account that is a member of the Domain Admins group. However, you may want to customize access to each module for console users or the AFS account. See the *Quest® Active Administrator® 8.6 Install Guide* for the specific permissions required for operation of each module and submodule.

Upgrade and compatibility

Note the following when upgrading Active Administrator.

- Active Administrator 8.6 supports in-place upgrades from Active Administrator versions 8.4 or 8.5. Upgrades from previous editions are not supported. To perform an in-place upgrade to Active Administrator 8.6 from a version of Active Administrator that is earlier than 8.4, you must first upgrade to Active Administrator 8.4.
- Installing Active Administrator 8.6 onto an existing Active Administrator installation will result in the removal of the earlier version. Active Administrator databases, both live and archive databases, will be upgraded automatically to version 8.6.
- A database upgraded by Active Administrator 8.6 cannot be used by previous versions and the database upgrade cannot be rolled back.
- Data within the Active Administrator share can be used by Active Administrator 8.6.
- If you use group policy to deploy the Workstation Logon Auditing Agents (WLAA), the 8.6 installation process will not update the agent on the user workstations. You must replace the install package at the software distribution share with the 8.6 version. Computers will upgrade to the Active Administrator 8.6 WLAA the next time they are started.
- The Active Directory Health features available in Active Administrator 8.6 each require a separate license. If you do not have a license file to apply, the module does not appear in Active Administrator. You will see the Certificate Management feature listed under the Configuration module, but when you select the feature, a warning displays that a license is required.
- The Active Directory Health Analyzer agent must be upgraded to the current version.

Product licensing

You need either a trial or full license to use Active Administrator. If you have questions about your license, contact your sales representative.

NOTE: The full and evaluation versions of Active Administrator are identical. The license file is the sole determinant of program functionality. Limitations during the free 30-day trial period include:

- Unlimited auditing of domain controllers.
- Certificate Management and Active Directory Health are not included.

The Certificate Management and Active Directory Health features each require a separate license. If you do not have a license file to apply, the module does not appear in Active Administrator. You will see the Certificate Management feature listed under the Configuration module, but when you select the feature, a warning displays that a license is required.

You apply the license the first time you launch the AA Configuration Wizard following the installation of the server component. You must have your license available prior to beginning the install process.

To apply the license file when you first start the configuration wizard

1. If you are installing Active Administrator, the configuration wizard opens automatically. Otherwise, open the AA Configuration Wizard from the **Start** menu.

   The first time you start the configuration wizard, you must apply a valid license file.
2. Select Active Administrator, and click **Update License**.
3. Locate the license file(s). A license file is approximately 1 KB in size and has a .dlv file extension. Once applied, the **License Status** should indicate **Installed** or **Trial** depending on the type of license.
4. Click **OK** to continue with the configuration wizard.

To update your license

1. From the **Start** menu, open **AA Server Manager**.
2. To view details about the current license, click **Details**.
3. To update the license, click **Updated License**.
4. Locate the license file (*.dlv), and click **Open**.

Upgrade and installation instructions

For detailed instructions, see the *Quest*® Active Administrator® *Install Guide* and the *Quest*® Active Administrator® *User Guide*.

Topics

- Backing up your data
- Installing Active Administrator server
- Configuring the server
- Installing Active Administrator console
- Updating audit agents
- Switching to Active Directory Health

Backing up your data

IMPORTANT: Prior to upgrading Active Administrator, it is highly recommended that you back up your Active Administrator database files and the folders in the Active Administrator share to avoid any loss of data. Quest Software will not be able to recover your data.This includes the ActiveAdministrator.xml file and the Active Administrator registry key.

Prior to upgrading Active Administrator ensure you back up the Active Administrator share, any data files, ActiveAdministratror.xml, and export the HKEY_LOCAL_MACHINE\SOFTWARE\Quest\Active Administrator registry key.

- The Active Administrator share is located at the root on the computer where Active Administrator is installed (**C:\ActiveAdministrator**). The Active Administrator share contains several folders that contain information, such as settings, templates, repositories, backup files, and log files. Back up the entire Active Administrator share.
- The Active Administrator data files are located on the named data server. To identify the data server and database file, run the Active Administrator Server Configuration report from the Active Administrator Console (**Settings | Configuration Report**).
- The ActiveAdministrator.xml file is in the folder where Active Administrator server is installed. The default location is **C:\Program Files\Quest\Active Administrator\Server**.
- The registry key is located at **HKEY_LOCAL_MACHINE\SOFTWARE\Quest\Active Administrator**.

Installing Active Administrator server

NOTE: The server needs to be installed on only one computer.

To install Active Administrator server

1. Launch the autorun.
2. On the Home page, click **Install**.
3. Click **Install** next to Active Administrator Server.
4. On the Welcome screen of the Install Wizard, click **Next**.
5. Click **View License Agreement**.
6. Scroll to the end of the license agreement.
7. Click **I accept these terms**, and click **OK**.
8. Click **Next**.
9. To change the location of the program files, click **Change**, or click **Next** to accept the default installation directory.
10. Click **Install**.
    - If you receive a message that some files are currently in use, click **OK** to close the applications automatically.
    - If you receive a message that setup was unable to close the applications, close the applications manually, and then click **OK**.
11. Click **Finish**.

    Launch Configuration Wizard is selected by default. When you click **Finish**, you continue to the configuration wizard. See Configuring the server.

Configuring the server

If you are upgrading Active Administrator, your previous settings appear on each page. You can quickly page through the wizard accepting the current settings or take the opportunity to make changes to your setup. For detailed instructions on the configuration wizard, see the *Quest*® Active Administrator® *Install Guide*.

To run the AA Configuration Wizard

1. If you are installing Active Administrator, the configuration wizard opens automatically. Otherwise, open the **AA Configuration Wizard** from the **Start** menu.
2. On the Welcome page, click **Next**.
   - The first time you start the configuration wizard, you must apply a valid license file.
     a. Select the licenses to update, and click **Update License**.
     b. Locate the license file, and click **OK**.
3. Type the passphrase (25 character minimum), and then type it again to confirm.

   IMPORTANT: You must know the current passphrase to to change or restore the passphrase. It is very important that you store the current passphrase in a secure location.
4. Click **Next**.
5. If you are upgrading Active Administrator, you are asked if you want to upgrade your existing live database and all archive databases. If you select **Yes**, proceed to step 11. If you select **No**, continue to the next step.

   NOTE: The upgrade process may take longer than normal due to the re-encryption of existing data. Active Administrator uses Advanced Encryption Standard (AES) to allow for better data security.
6. Select **Use an existing Active Administrator database**.
7. Accept the displayed server and database or select a different server and database, and click **Next**.
8. Select **Use an existing Active Administrator Archive database**.
9. Accept the displayed server and database or select a different server and database and click **Next**.
10. Select the purge and archive options to enable or disable and click **Next**.
11. Select the path to the Active Administrator share, and click **Next**.
12. Accept the SMTP server setup or make any necessary changes, and click **Next**.
13. Type a valid email address or accept the default and click **Next**.
14. Accept the active template settings or name any necessary changes and click **Next**.
15. Accept the group policy history settings or make any necessary changes and click **Next**.
16. Accept the Active Directory backup settings or make any necessary changes and click **Next**.
17. To add additional users, click **Add**, find and select users, click **OK**.
18. Click **Next**.
19. Type the account password for the Active Administrator Foundation Service account.
20. The default service port number is 15600. To change the port number, type a value.
21. To use the same account for the notification service, select the check box. Otherwise, type or browse for an account with Domain Admin rights, and type the password.
22. Click **Next**.
23. Click **Finish**.
24. Click **Finish**.

Installing Active Administrator console

Install the Active Administrator console on any workstation that requires the use of Active Administrator.

IMPORTANT: If you are currently using Spotlight® for Active Directory® and plan to install the Diagnostic Console, you must install the Active Directory console on a computer that does not have the Spotlight for Active Directory Console installed.

To install Active Administrator console

1. Launch the autorun.
2. On the Home page, click **Install**.
3. Click **Install** next to Active Administrator Console.
4. On the Welcome screen of the Setup Wizard, click **Next**.
5. Click **View License Agreement**.
6. Scroll to the end of the license agreement.
7. Click **I accept these terms**, and click **OK**.
8. Click **Next**.
9. To change the location of the program files, click **Change**, or click **Next** to accept the default installation directory
10. Click **Install**.
11. By default, the option to start the Active Administrator Console is selected. If you do not want to start the console, clear the check box.
12. Click **Finish**.

    The first time the Active Administrator console opens, you are asked to set the Active Administrator Server.
13. Type the name of the server where Active Administrator Server is installed, or browse to locate a server.
14. Click **OK**.

NOTE: If you want to change the server, select **Settings | Set Active Administrator Server**.

Updating audit agents

To collect data on a computer, you must install and activate the audit agent. A wizard guides you through installing the audit agent.

To update audit agents

1. Select **Auditing & Alerting | Agents**.
2. To update selected domain controller(s), select **More | Update**.

   –OR-

   To update all listed domain controllers, select **More | Update All**.

NOTE: You may need to refresh the audit agents to correct the display. Click **Refresh** or select domain controllers, and click **Refresh Selected**.

Switching to Active Directory Health

The Active Directory® Health module incorporates key features from Quest® Directory Analyzer and Directory Troubleshooter. If you are a current user of Directory Analyzer and Directory Troubleshooter, you can switch over to Active Directory Health gradually, or right away. See the *Quest*® Active Administrator® *User Guide* for detailed instructions.

To switch gradually

1. Deploy at least two agents into the Active Directory Health agent pool and add a few domain controllers to monitor.
2. Stop, but do not uninstall yet, the old Directory Analyzer agent running on the domain controllers you just added.
3. Test these domain controllers in Active Directory Health.
4. If everything looks good, uninstall the old Directory Analyzer agents on the monitored domain controllers.
5. Add a few more domain controllers to the list of monitored domain controllers.
6. Test these domain controllers in Active Directory Health.
7. If everything looks good, uninstall the old Directory Analyzer agents on the monitored domain controllers.
8. Repeat steps 5 through 7 until all of your domain controllers are monitored by the Active Directory Health Agent pool.

To switch right away

1. Deploy the number of required agents and add the domain controllers.
2. Shut down the old Directory Analyzer agents.
3. Test Active Directory Health for a period of time.
4. Remove the old Directory Analyzer agents.

More resources

Additional information is available from the following:

- Online product documentation (https://support.quest.com/active-administrator/8.6/technical-documents)
- The Active Administrator Community (https://www.quest.com/community/products/active-administrator)

Globalization

This section contains information about installing and operating this product in non-English configurations, such as those needed by customers outside of North America. This section does not replace the materials about supported platforms and configurations found elsewhere in the product documentation.

This release is Unicode-enabled and supports any character set. In this release, all product components should be configured to use the same or compatible character encodings and should be installed to use the same locale and regional options. This release is targeted to support operations in the following regions: North America, Western Europe and Latin America, Central and Eastern Europe, Far-East Asia, Japan.

About us

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request.
- View Knowledge Base articles.
- Sign up for product notifications.
- Download software and technical documentation.
- View how-to-videos.
- Engage in community discussions.
- Chat with support engineers online.
- View services to assist you with your product.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.
Attn: LEGAL Dept.
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our website (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, Active Administrator, and the Quest logo are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT NOTE, **NOTE**, **TIP**, **MOBILE**, or **VIDEO:** An information icon indicates supporting information.

Active Administrator Release Notes
Updated - May 2022
Software Version - 8.6