



Quest[®] Active Administrator[®] 8.2

Install Guide



© 2017 Quest Software Inc.

ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

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, Spotlight, 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 Install Guide
Updated - October 2017
Software Version - 8.2

Contents

Installation Considerations for Active Administrator	5
Server requirements	5
Server hardware requirements	5
Server software requirements	6
SQL Server requirements	6
Console requirements	7
Console hardware requirements	7
Console software requirements	8
Audit agents requirements	9
Workstation logon audit agents requirements	9
Port requirements for Active Administrator	9
User privilege requirements	10
Password recovery	10
Services	11
Audit database	11
Active Administrator module requirements	11
Home	12
Search	13
Certificates	13
Security & Delegation	14
Azure Active Directory	15
Active Directory Health	16
Auditing & Alerts	18
Group Policy	19
Active Directory Recovery	20
DC Management	21
DNS Management	22
Configuration	23
Active Directory Health minimum permissions	24
Active Directory Health module	24
Configuration	24
Agents	25
Notifications	26
Troubleshooter	26
Web-based Active Directory Health reports	27
AFS service account minimum permissions	30
Installing and configuring Active Administrator	34
Installing Active Administrator server	34
Configuring the server	35
Applying a license file	35
Setting the Active Administrator database	35
Setting the Active Administrator archive database	36

Configuring purge and archive settings	37
Storing Active Administrator data	38
Setting up the email server	38
Setting up features and the owner	38
Configuring active template delegation enforcement	39
Configuring group policy history	39
Configuring Active Directory backups	40
Configuring Active Administrator users	41
Configuring service accounts	41
Connecting to System Center Operations Manager	42
Reviewing selections	42
Installing Active Administrator console	43
Setting up the console	43
Setting up auditing on domain controllers	44
Installing audit agents	44
Creating alerts	46
Setting up workstation logon auditing	48
Deploying the workstation logon audit agent	48
Enabling the default port	49
Using Active Administrator	49
About us	50
We are more than just a name	50
Our brand, our vision. Together.	50
Contacting Quest	50
Technical support resources	50
Index	51

Installation Considerations for Active Administrator

The system requirements are the same for all components of Quest® Active Administrator®. Ensure that the minimum requirements are met and all necessary software is installed before installing any of the components.

Topics:

- [Server requirements](#)
- [Console requirements](#)
- [Audit agents requirements](#)
- [Workstation logon audit agents requirements](#)
- [Port requirements for Active Administrator](#)
- [User privilege requirements](#)
- [Active Administrator module requirements](#)
- [Active Directory Health minimum permissions](#)
- [AFS service account minimum permissions](#)

Server requirements

i | **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®.

Server hardware requirements

Table 1. Server hardware requirements

Requirement	Details
Processor	1 GHz or higher
Memory	<ul style="list-style-type: none"> • For Windows Server® 2008 R2: 512 MB minimum, 2 GB recommended • 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

Table 1. Server hardware requirements

Requirement	Details
Hard disk space	100 MB
Operating system	<ul style="list-style-type: none">• Windows Server® 2008 R2• Windows Server 2012• Windows Server 2012 R2• Windows Server 2016

NOTE: Active Administrator® does not support Microsoft® Nano Server 2016.

Server software requirements

Table 2. Server software requirements

Requirement	Details
.NET Framework v. 4.5.2 and 4.6	Install either the Full or Standalone version. Do not install just the Client Profile.
Group Policy Management Console (GPMC)	<p>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.</p> <p>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 <code>ServerManagerCmd -install GPMC</code>.</p>

i | **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.

i | **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 2008
- SQL Server 2008 Express
- SQL Server 2008 R2
- SQL Server 2008 R2 Express
- SQL Server 2012
- SQL Server 2012 Express
- SQL Server 2014
- SQL Server 2014 Express
- SQL Server 2016

i **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 execute the statement. The results list all sort and collation information for the database.

Console requirements

Console hardware requirements

Table 3. Console hardware requirements

Requirement	Details
Processor	1 GHz
Memory	256 MB
Hard disk space	100 MB
Operating system	<ul style="list-style-type: none">• Windows® 7• Windows 8.1• Windows 10• Windows Server® 2008 R2• Windows Server 2012• Windows Server 2012 R2• Windows Server 2016

NOTE: Active AdministratorActive Administrator® does not support Microsoft® Nano Server 2016.

NOTE: When using Windows 7, you may experience problems when trying to perform some operations on Active Directory® objects, such as creating objects or viewing object properties. When the Microsoft® RSAT tools are installed on Windows 7, the adprop.dll.mui and dsadmin.dll.mui files are not installed and these files are needed by Active Administrator. Please see the Quest® Knowledge Base and Solution Center for instructions on how to locate and copy these files to the correct location.

NOTE: If you are using the Certificate module, see [Table 4](#) for information on support for SHA-2 certificates.

Table 4. 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 2008 R2	supported	KB3033929	KB3033929
Windows Server 2012	supported	supported	supported
Windows Server 2012 R2	supported	supported	supported

Table 4. 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 2016	supported	supported	supported
Windows 7	supported	KB3033929	KB3033929
Windows 8.1	supported	supported	supported
Windows 10	supported	supported	supported

Console software requirements

- .NET Framework v.4.5.2 or 4.6
- Group Policy Management Console (GPMC)
- DNS Server Tools

Table 5. GPMC and DNS Server Tools install information

Operating System	Download Links and Install Information
Windows® 7 Windows 8.1 Windows 10	<p>GPMC and DNS Server Tools are included in Remote Server Administration Tools (RSAT).</p> <ul style="list-style-type: none"> • Remote Server Administration Tools for Windows 7: https://www.microsoft.com/en-us/download/details.aspx?id=7887 • Remote Server Administration Tools for Windows 8.1: https://www.microsoft.com/en-us/download/details.aspx?id=39296 • Remote Server Administration Tools for Windows 10 https://www.microsoft.com/en-us/download/details.aspx?id=45520 <p>To activate GPMC and DNS Server Tools</p> <ol style="list-style-type: none"> 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, and select DNS Server Tools.
Windows Server 2008 R2 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016	<p>To active GPMC</p> <ul style="list-style-type: none"> • 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. <p>To install DNS Server Tools</p> <ol style="list-style-type: none"> 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

Table 6. Audit agents hardware requirements

Requirement	Details
Processor	1 GHz or higher
Hard disk	100 MB
Memory	256 MB
Operating systems	<ul style="list-style-type: none">• Windows Server® 2008 R2• Windows Server 2012• Windows Server 2012 R2• Windows Server 2016

Workstation logon audit agents requirements

Table 7. Workstation logon audit agent hardware requirements

Requirement	Details
Processor	1 GHz or higher
Hard disk	100 MB
Memory	256 MB
Operating systems	<ul style="list-style-type: none">• Windows® 7• Windows 8.1• Windows 10• Windows Server® 2008 R2• Windows Server 2012• Windows Server 2012 R2• Windows Server 2016

Port requirements for Active Administrator

i **NOTE:** The AFS Server is the computer on which the Active Administrator Server is installed and running the Active Administrator Foundation Service (AFS). The Console is the computer on which the Active Administrator Console is installed. The AFS Database Server is the computer on which the audit database resides.

- TCP Port 15600 must be open between Console and the AFS Server.
- TCP Port 15601 must be open between the computer running the workstation logon audit agent and the AFS Server.

- TCP Port 389 must be open between domain controllers and the AFS Server and Console.
- TCP Port 1433 must be open between the AFS Server and the AFS Database Server.
- 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 are using the Azure[®] Active Directory[®] feature, TCP Ports 80 and 443 must be open on the Internet-facing firewall.
- If you are using the Active Directory Health feature:
 - TCP Port 15602 must be open on the Active Administrator server for the Active Administrator Data Service (ADS).
 - TCP Port 15603 must be open on the computer running the Directory Analyzer agent.
- 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.

i **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. See [Configuring the web server](#) in the *Web Console User Guide*.

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 Directory 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>.

- 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. This section details the permissions required for operation of each module and submodule.

Modules:

- [Home](#)
- [Search](#)
- [Certificates](#)
- [Security & Delegation](#)
- [Azure Active Directory](#)
- [Active Directory Health](#)
- [Auditing & Alerts](#)
- [Group Policy](#)
- [Active Directory Recovery](#)
- [DC Management](#)
- [DNS Management](#)
- [Configuration](#)

Home

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. The following table lists the specific permission requirements for the Home module.

Table 8. Required permissions for the Home module

Submodule	Console user account	AFS account
Home page	<p>Open to all users, but some items may not be available if the user does not have the required permission.</p> <p>Must have read access to the entire domain:</p> <ul style="list-style-type: none"> • Active Directory Search <p>Must have the appropriate permissions on the target user account:</p> <ul style="list-style-type: none"> • Reset Password • Unlock User Account • Enable/Disable User Account <p>Must have the appropriate permissions on the target group:</p> <ul style="list-style-type: none"> • Add a user to a group • Remove a user from a group <p>Must have the appropriate permissions on the target computer:</p> <ul style="list-style-type: none"> • Reset Computer Account 	N/A
Dashboard	Open to all users.	Must be a member of the AA_User group and have read access to the domains being managed.

Search

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. The following table lists the specific permission requirements for the Search module.

Table 9. Required permissions for the Search module

Submodule	Console user account	AFS account
Search	Open to all users. Requires Read access to the Active Directory® domains being searched. Active Directory object commands, such as move or rename, require the appropriate permissions on the target objects.	N/A

Certificates

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. The following table lists the specific permission requirements for the Certificates module.

i | **NOTE:** To assign roles in Active Administrator, select **Configuration | Role Based Access | New**. See [Defining role-based access in the Quest® Active Administrator® User Guide](#) for detailed information. See [Defining role-based access in the Quest® Active Administrator® User Guide](#).

Table 10. Required permissions for the Certificates module

Submodule	Console user account	AFS account
Certificate Landing Page	Must have the Active Administrator Certificate Management role.	Must be a member of the AA_Users group.
Certificate Management	Must have the Active Administrator Certificate Management role.	Must be a member of the AA_Admins group and the Administrators group on the target server.
Certificate Search	Must have read access to the Certificate Repository in the Active Administrator share.	Must have read and remote registry access to the target computer. Must be a member of the AA_Users_Group.

Table 10. Required permissions for the Certificates module

Submodule	Console user account	AFS account
Certificate Authority (CA)	N/A	<p>NOTE: Permissions apply to the AFS account or to the user account specified in the forest settings.</p> <p>Must be a member of the AA_Admins_Group and have Active Directory read access</p> <p>Must have read access to the CA server via remote registry to the registry key HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\CertSvc</p> <p>Must be a full administrator on the CA server to get the status of the CA service and to stop and start the service.</p> <p>Must be a full administrator on the CA server to back up the CA server</p>
Certificate Repository	Must have the Active Administrator Certificate Management role.	Must have read and write access to the CertificateRepository folder in the Active Administrator Share.

Security & Delegation

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. The following table lists the specific permission requirements for the Security & Delegation module.

i | **NOTE:** To assign roles in Active Administrator, select **Configuration | Role Based Access | New**. See [Defining role-based access in the Quest® Active Administrator® User Guide](#) for detailed information. See [Defining role-based access in the Quest® Active Administrator® User Guide](#).

Table 11. Required permissions for the Security & Delegation module

Submodule	Console user account	AFS account
Security Landing Page	Must have any of these Active Administrator roles: Security, Active Templates, or Password Policies.	Must be a member of the AA_Users group and have read access to all domains being managed.
Security	<p>Must have the Active Administrator Security role.</p> <p>Must have read access to view all objects in the selected domain and must have the appropriate permissions on the target Active Directory® object to perform actions.</p>	To view the Active Templates applied to the object, must have permissions to the ActiveTemplate folder in the Active Administrator share.
User Logon Activity	Must have the Active Administrator Security role.	<p>Must be a member of the AA_Admins group.</p> <p>The workstation logon audit agent must run under the local system account.</p>
Locked Out Accounts	Must have the Active Administrator Security role.	Must be a member of the AA_Admins group and have read access to all user objects in the selected domains.

Table 11. Required permissions for the Security & Delegation module

Submodule	Console user account	AFS account
Password Policies	<p>Must have the Active Administrator Password Policy role.</p> <p>To view all of the password policies, the must have read access to the policies in the selected domain.</p> <p>To create, edit, or delete the password policies, must have the appropriate permissions on the selected policy.</p>	N/A
Delegation Status	<p>Must have the Active Administrator Active Templates role.</p> <p>To create new, edit, or delete delegations on objects, must have full control access on the target object.</p>	<p>Must have read/write access to the ActiveTemplates folder in the Active Administrator share.</p> <p>To maintain permissions for delegations, must have full control access on the target objects.</p>
Active Templates	<p>Must have the Active Administrator Active Templates role.</p> <p>To create new, edit, or delete delegations on objects, must have full control access on the target object.</p>	<p>To create new, edit, or delete Active Templates, must have read/write access to the ActiveTemplates folder in the Active Administrator share.</p> <p>To maintain permissions for delegations, must have full control access on the target object.</p>
Inactive Accounts	<p>Must have the Active Administrator Security role.</p>	<p>Must be a member of the AA_Admins group.</p> <p>Must have read access to all users in the selected domains.</p> <p>To perform actions, must have the appropriate permissions on the target object.</p> <p>To move an object, must have the appropriate permissions on the target object and the target location.</p>
Password Reminder	<p>Must have the Active Administrator Security role.</p>	<p>Must be a member of the AA_Admins group.</p> <p>Must have read access to all users in the selected domains.</p>
Account Expiration	<p>Must have the Active Administrator Security role.</p>	<p>Must be a member of the AA_Admins group and have read access to all user objects in the selected domains.</p>
Purge Account History	<p>Must have the Active Administrator Full Control role.</p>	<p>Must be a member of the AA_Admins group.</p>

Azure Active Directory

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. The following table lists the specific permission requirements for the Azure[®] Active Directory[®] module.

i | **NOTE:** To assign roles in Active Administrator, select **Configuration | Role Based Access | New**. See [Defining role-based access](#) in the *Quest[®] Active Administrator[®] User Guide* for detailed information. See [Defining role-based access](#) in the *Quest[®] Active Administrator[®] User Guide*.

Table 12. Required permissions for the Azure Active Directory module

Subsystem	Console user account	AFS account
Azure Active Directory Landing Page	Must have the Active Administrator Azure Active Directory role.	Must be a member of the AA_Users group.
Azure Active Directory Search		Must have the appropriate settings to access the directory.
Azure Active Directory Users		
Azure Active Directory Groups		
Azure Active Directory Change Notifications	Must have the Active Administrator Azure Active Directory role.	Must have read/write access to the AzureAD folder in the Active Administrator share. Must be a member of the AA_Users group. Must have the appropriate settings to access the directory.

Active Directory Health

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.

- NOTE:** To assign roles in Active Administrator, select **Configuration | Role Based Access | New**. See [Defining role-based access in the Quest® Active Administrator® User Guide](#) for detailed information. See [Defining role-based access in the Quest® Active Administrator® User Guide](#).
- NOTE:** For details on the minimum permissions required for the Active Directory Health module, see [Active Directory Health minimum permissions](#).

Topics:

- [Required permissions for Active Directory Health](#)
- [Active Administrator Data Services \(ADS\) requirements](#)
- [Data collectors requirements](#)

Required permissions for Active Directory Health

The following table lists the specific permission requirements for the Active Directory Health module.

Table 13. Required permissions for the Active Directory Health module

Submodule	Console user account	AFS account
Active Directory Health Landing Page	Must have the Active Administrator Directory Analyzer role.	Must be a member of the AA_Users group.
Analyzer	Must have the Active Administrator Directory Analyzer role.	N/A
Alerts	Must have the Active Administrator Directory Analyzer role. to manage notifications, must have the Active Administrator Directory Analyzer Notification Management role.	Must be a member of the AA_Users group. Must have read/write access to the DACache folder in the Active Administrator share.

Table 13. Required permissions for the Active Directory Health module

Submodule	Console user account	AFS account
Agents	<p>To manage agents, must have the Active Administrator Directory Analyzer Agent Management role.</p> <p>To manage notifications, must have the Active Administrator Directory Analyzer Notification Management role.</p> <p>to manage data collectors, must have the Active Administrator Directory Analyzer Data Collector Management role.</p> <p>To manage alerts, must have the Active Administrator Directory Analyzer Alert Management role.</p> <p>To manage agents, must have the Active Administrator Directory Analyzer Agent Management role.</p>	<p>To install, edit, and remove agents, must be a member of the AA_Admins group and have full control access to the target server.</p> <p>To update alerts and collectors, and to manage notifications, must have read/write access to the DACache folder in the Active Administrator share.</p> <p>NOTE: For the specific permissions required for each data collector, see <i>Appendix A</i> in the <i>Quest® Active Administrator® User Guide</i> or online help.</p>
Troubleshooter	<p>Must have the Active Administrator Directory Analyzer Troubleshooter role.</p> <p>To view reports or perform troubleshooting operations, must have WMI remote access enabled and be a member of the Distributed COM users group.</p> <p>To execute jobs, must have full control access to the target server.</p>	N/A
Diagnostic Console	To collect performance counter values, must be a member of the local administrator group on the target domain controller.	N/A

Active Administrator Data Services (ADS) requirements

Table 14. Required permissions for Active Administrator Data Services (ADS)

Subsystem	ADS account
Loader	Must be a member of the AA_Users group and have read access to the enterprise.
Data Collectors	See the data collector permissions for forests, domains, and sites in <i>Appendix A</i> of the <i>Quest® Active Administrator® User Guide</i> or online help.
Agent Monitor and Recovery	Must have full access on the server where the Directory Analyzer agent is installed.

Data collectors requirements

The Active Directory Health module uses the Directory Analyzer to monitor domain controllers and presents data for you to troubleshoot issues. For the Directory Analyzer to acquire the necessary data, certain permissions and access are required for the Directory Analyzer agent startup account. See the *Quest® Active Administrator® User Guide* for more information on the Directory Analyzer agent. See [Installing Directory Analyzer agents](#) in the *Quest® Active Administrator® User Guide*.

To capture all data collectors accessible by the Directory Analyzer:

- The startup account for the Directory Analyzer agent must:

- have Domain User and domain administrative privileges;
- be a member of the Distributed COM Users group; and
- be a member of the Performance Logs Users group.
- The target server must have WMI remote access enabled.

To see the specific requirements for each data collector, see *Appendix A* in the *Quest® Active Administrator® User Guide*. To see the specific requirements for each data collector, see the [Alerts Appendix](#) in the *Quest® Active Administrator® User Guide*.

Auditing & Alerts

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. The following table lists the specific permission requirements for the Auditing & Alerts module.

i | **NOTE:** To assign roles in Active Administrator, select **Configuration | Role Based Access | New**. See [Defining role-based access](#) in the *Quest® Active Administrator® User Guide* for detailed information. See [Defining role-based access](#) in the *Quest® Active Administrator® User Guide*.

Table 15. Required permissions for the Auditing & Alerts module

Submodule	Console user account	AFS account
Auditing & Alert Landing Page	Must have any of these Active Administrator roles: Audit Report Management, Audit Report Viewer, Alert Editor or Alert Viewer.	Must be a member of the AA_Users group.
Audit Reports	Must have the Active Administrator Report Viewer role to view reports. Must have the Active Administrator Report Management role to manage reports.	Must be a member of the AA_Admins group.
Archives	Must have the Active Administrator Report Viewer role to view reports. Must have the Active Administrator Report Management role to manage reports.	Must be a member of the AA_Admins group.
Agents	Must have the Active Administrator Full Control role.	Must be a member of the AA_Admins group and have full access to the target server. The agent account must have read access to the security log on the target domain controller and be a member of the AA_Admins group.
Auditing Alerts	Must have the Active Administrator Report Viewer role to view alerts and alert history. Must have the Active Administrator Alert Editor role to manage alerts.	Must be a member of the AA_Admins group.
Event Definitions	Must have the Active Administrator Full Control role.	Must be a member of the AA_Admins group.
Archive & Purging	Must have the Active Administrator Full Control role.	Must be a member of the AA_Admins group.

Group Policy

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. The following table lists the specific permission requirements for the Group Policy module.

i | **NOTE:** To assign roles in Active Administrator, select **Configuration | Role Based Access | New**. See [Defining role-based access](#) in the *Quest[®] Active Administrator[®] User Guide* for detailed information. See [Defining role-based access](#) in the *Quest[®] Active Administrator[®] User Guide*.

Table 16. Required permissions for the Group Policy module

Submodule	Console user account	AFS account
Group Policy Landing Page	Must have one of these Active Administrator roles: Group Policy Object Management, Group Policy History, or Group Policy Repository. Must have read access to all group policies objects in the selected domains.	Must have read access to the GPORepository, GPOBackups, and RSOPPlanning folders in the Active Administrator share.
Group Policy Objects	Must have the Active Administrator Group Policy Management role. To view GPOs, must have read access to all GPO objects in the selected domain. To create, edit, or delete GPOs, must have the appropriate permissions on the selected GPO. To link or unlink a GPO, must have the appropriate permissions on the target.	To backup GPOs, must have read access to the selected GPO and read/write access to the GPOBackup folder in the Active Administrator share. To add to the repository, must have full control access to the selected GPO, including SysVol and the System/Policies in Active Directory [®] . Must also have read/write access to the GPORepository folder in the Active Administrator share.
Group Policy by Container	Must have the Active Administrator Group Policy Management role. To view GPOs and GPO modeling, must have read access to all GPO objects in the selected domain. To create, edit, delete, block, and unblock GPOs, must have the appropriate permissions on the selected GPO. To link, unlink, or change link order, must have the appropriate permissions on the target. To create a new OU, must have the appropriate permissions in the selected OU.	N/A
GPO Settings Search	Must have the Active Administrator Group Policy Management role.	Must have read access to the GPOBackup, GPOCache, GPORepository, and GPOHistory folders in the Active Administrator share. Must have read access to the all of the GPOs in the managed domains.
GPO History	Must have the Active Administrator Group Policy History role.	Must have read/write access to the GPOHistory folder in the Active Administrator share and read access to all GPOs in the managed domains. To rollback GPOs, must have full control on the selected GPO.

Table 16. Required permissions for the Group Policy module

Submodule	Console user account	AFS account
GPO Repository	Must have the Active Administrator Group Policy Repository role.	To add, edit, remove, check out, check in, or discard, must have full control access to the selected GPO including the SysVol and the System/Policies in Active Directory®. Must have read/write access to the GPORepository folder in the Active Administrator share.
GPO Modeling	Must have the Active Administrator Group Policy Management role. Must have read access to the entire directory to run the simulation.	Must have read/write access to the RSOPPlanning folder in the Active Administrator share.
GPO Backup	Must have the Active Administrator Group Policy Management role.	Must have read/write access to the GPOBackup folder in the Active Administrator share. Must have read access to the selected GPO.
Client-side troubleshooting	Must have the Active Administrator Group Policy Management role. Must have full access to the target computer.	N/A
Purge GPO History	Must have the Active Administrator Full Control role.	Must have read/write access to the GPOHistory folder in the Active Administrator share.

Active Directory Recovery

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. The following table lists the specific permission requirements for the Active Directory Recovery module.

- i** | **NOTE:** To assign roles in Active Administrator, select **Configuration | Role Based Access | New**. See [Defining role-based access in the Quest® Active Administrator® User Guide](#) for detailed information. See [Defining role-based access in the Quest® Active Administrator® User Guide](#).

Table 17. Required permissions for the Active Directory Recovery module

Submodule	Console users account	AFS account
Recovery Landing Pages	Must have the Active Administrator Recovery role.	Must be a member of the AA_Users group.
Object Recovery	Must have the Active Administrator Recovery role. To perform a restore, must have full access to the target and read access to the ADBackups folder in the Active Administrator share.	Must have read/write access to the ADBackups folder. Must have read access to the entire domain.

Table 17. Required permissions for the Active Directory Recovery module

Submodule	Console users account	AFS account
Purge AD Backups	Must have the Active Administrator Recovery role.	Must be a member of the AA_Users group. Must have read/write access to the ADBackups folder in the Active Administrator share.
Active Directory Infrastructure Landing Page	Must have any of these Active Administrator roles: Site Management or Trust Management. User must have read access to the entire forest.	Must be a member of the AA_Users group.
Active Directory Sites	Must have the Active Administrator Site Management role. Must have read access to view all sites, subnets and site links in the forest. To create, edit or delete sites, subnets and site links, must have enterprise access.	N/A
Replication Monitoring	Must have the Active Administrator Site Management role.	Must be a member of the AA_Admins group. Must have read access to the entire forest.
Replication Analyzer	Must have the Active Administrator Site Management role. Must have read access to the entire forest.	N/A
Active Directory Trust	Must have the Active Administrator Trust Management role. To view trusts, must have read access to the entire forest. To add, edit, or delete trusts, must have the appropriate permissions in the target domain.	N/A

DC Management

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. The following table lists the specific permission requirements for the DC Management module.

- i** | **NOTE:** To assign roles in Active Administrator, select **Configuration | Role Based Access | New**. See [Defining role-based access](#) in the *Quest[®] Active Administrator[®] User Guide* for detailed information. See [Defining role-based access](#) in the *Quest[®] Active Administrator[®] User Guide*.

Table 18. Required permissions for the DC Management module

Submodule	Console user account	AFS account
DC Management Landing Page	Must have the Active Administrator Domain Controller Management role. Must have read access to the selected domain controller.	N/A
DC Status	Must have the Active Administrator Domain Controller Management role. Must have read access to the selected domain controller, have WMI remote access enabled, and must be a member of the Distributed COM users group.	N/A
DC Services	Must have the Active Administrator Domain Controller Management role. Must have full control on the selected domain controller.	N/A
DC Performance	Must have the Active Administrator Domain Controller Management role. Must have read access to the selected domain controller and be a member of the Performance Log Users group.	N/A
DC Event Logs	Must have the Active Administrator Domain Controller Management role. Must have read access to the selected event log on the selected domain controller.	N/A

DNS Management

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. The following table lists the specific permission requirements for the DNS Management module.

- i** | **NOTE:** To assign roles in Active Administrator, select **Configuration | Role Based Access | New**. See [Defining role-based access in the Quest® Active Administrator® User Guide](#) for detailed information. See [Defining role-based access in the Quest® Active Administrator® User Guide](#).

Table 19. Required permissions for the DNS Management module

Submodule	Console user account	AFS account
DNS Landing Page	Must have the Active Administrator DNS Management role. Must have full control on the selected DNS server	Must be a member of the AA_Users group.
DNS Management	Must have the Active Administrator DNS Management role. To view, create, edit, or delete DNS records, must have full control on the selected DNS server.	N/A
DNS Monitoring	Must have the Active Administrator DNS Management role.	Must be a member of the AA_Users group.

Table 19. Required permissions for the DNS Management module

Submodule	Console user account	AFS account
DNS Analyzer	Must have the Active Administrator DNS Management role.	N/A
DNS Event Log	Must have the Active Administrator DNS Management role. Must have read access to the DNS event log on the selected DNS server.	N/A
DNS Search	Must have the Active Administrator DNS Management role. Must have full control access on the selected DNS servers.	N/A

Configuration

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. The following table lists the specific permission requirements for the Configuration module

i | **NOTE:** To assign roles in Active Administrator, select **Configuration | Role Based Access | New**. See [Defining role-based access in the Quest® Active Administrator® User Guide](#) for detailed information. See [Defining role-based access in the Quest® Active Administrator® User Guide](#).

Table 20. Required permissions for the Configuration module

Subsystem	Console user	AFS account
Configuration Landing Page	Must have the Active Administrator Full Control role.	Must be a member of the AA_Users group.
Tasks		
Role Based Access		
SMTP Settings		
Azure Configuration		
Notification Settings		
Active Template Settings		
Agent Installation Settings		
Recovery Settings		
GPO History Settings		
GPO History Settings		
Certification Configuration		
Service Monitoring Policy		
Archive Databases	Must have the Active Administrator Full Control role.	Must have permission on the target database server to create databases.
User Logon Agent Settings	Must have the Active Administrator Full Control role.	Must be a member of the AA_Admins group.

Active Directory Health minimum permissions

For the Active Directory Health module to operate properly, the Active Administrator Foundation service (AFS) requires an account that is a member of the Domain Admins group. See [Active Directory Health](#). You may want to customize access to each Active Directory Health subsystem for console users or the AFS account. This section details the minimum permission requirements for the Active Directory Health module and its subsystems.

Topics:

- [Active Directory Health module](#)
- [Configuration](#)
- [Agents](#)
- [Notifications](#)
- [Troubleshooter](#)

Active Directory Health module

- The AFS account requires local administrator rights on the Active Administrator server.
- The AFS account requires read, write, and modify access to the Logging directory in the Active Administrator server installation folder.
- The Directory Analyzer agent account needs to be a member of the Performance Monitor Users group in Active Directory.

Configuration

- The AFS account must have read/write access to the:
 - Active Administrator share (default: C:\ActiveAdministrator\)
 - HKLM\SOFTWARE\WOW6432Node\Quest\Active Administrator\ registry key
 - Active Administrator server installation directory (default: C:\Program Files\Quest\Active Administrator\Server\)
- The AFS account must have read, write, and modify permissions to the Logging directory (default: C:\Program Files\Quest\Active \Server\LOGGING\).
- The AFS account must be a member of the AA_Admins group either in the domain or on the database server, depending on the configuration selected during setup.

Agents

Table 21. Directory Analyzer agent management minimum permission requirements

Action	Minimum permission requirement
Install agents	<ul style="list-style-type: none">The AFS account must have local administrator rights to install a Windows service on the target system.The DA agent service account must have the run as a service right on the target system.
Uninstall agents	<ul style="list-style-type: none">The AFS account must have local administrator rights to uninstall a Windows service on the target system.
View agent status	<ul style="list-style-type: none">Using a group policy, assign the Start, Stop, and Query status permissions to the AFS account for the Active Administrator Directory Analyzer Agent service.The AFS account must have read access to the WINDIR\DAAgent\ folder on the target system.
Stop/Start/Restart agents	<ul style="list-style-type: none">Using a group policy assign the Start, Stop, and Query status permissions to the AFS account for the Active Administrator Directory Analyzer Agent service
Upgrade agents	<ul style="list-style-type: none">The AFS account must have local administrator rights to install a Windows service on the target system.
Set agent startup account	<ul style="list-style-type: none">The AFS account must have local administrator rights to set a Windows service startup account on the target system.
Set agent port number	<ul style="list-style-type: none">Using a group policy, assign the Start, Stop, and Query status permissions to the AFS account for the Active Administrator Directory Analyzer Agent service.The AFS account must have read access to the WINDIR\DAAgent\ folder on the target system
Test connection	<ul style="list-style-type: none">Domain User rights required
View agent log	<ul style="list-style-type: none">Domain User rights required

Load-balanced agents

Table 22. Load-balanced agents minimum permission requirements

Action	Minimum permission requirement
Agent online verification	Domain User rights required.
Agent workload deployment	Domain User rights required.

Agent watcher

Table 23. Agent watcher minimum permission requirements

Action	Minimum permissions requirement
Check agent service status	Using a group policy, assign the Start, Stop, and Query status permissions to the AFS account for the Active Administrator Directory Analyzer Agent service.
Restart agent service	Using a group policy, assign the Start, Stop, and Query status permissions to the AFS account for the Active Administrator Directory Analyzer Agent service.

Remediation (built-in only)

Table 24. Remediation (built-in only) minimum permission requirements

Action	Minimum permission requirement
Stop/start process	The AFS account must have local administrator rights to stop or start a process on the target system.
Stop/start/restart service	Using a group policy, assign the Start, Stop, and Query status permissions to the AFS account for the target service.
Reboot server	The AFS account must be assigned the Force shutdown from a remote system right on the target system which can be applied from a Group Policy: Computer Configuration Policies Windows Settings Security Settings Local Policies User Rights Assignment Force shutdown from a remote system .

Notifications

Table 25. Notifications minimum permission requirements

Action	Minimum permission requirement
Send alert notifications	Domain User rights required
Mute notifications	Domain User rights required
Limit notifications	Domain User rights required

Data point routing

Table 26. Data point routing minimum permission requirements

Action	Minimum permission requirement
Routing	Domain User rights required
Alert processing	Domain User rights required

Troubleshooter

The Directory Analyzer Troubleshooter minimum permissions outlined below are required for the logged on user account running the Active Administrator Console.

Jobs

Table 27. Jobs minimum permission requirements

Action	Minimum permission requirement
Directory Service Replication Troubleshooter	The Console user must have rights to perform replication. The Console user must have directory synchronization rights at the configuration root. See the article at: https://social.technet.microsoft.com/wiki/contents/articles/21565.active-directory-delegate-replication-rights-to-non-admins.aspx
Enable or disable domain controller replication	The Console user must have read/write access to LDAP://CN=NTDS Settings,CN={DCName},CN=Servers,CN={Site Name},CN=Sites,CN=Configuration,DC={Domain Name} Active Directory object.

Table 27. Jobs minimum permission requirements

Action	Minimum permission requirement
Set directory service log levels	The Console user must have read/write access to the following registry key on the remote system: HKLM\System\CurrentControlSet\Services\NTDS\Diagnostics
Set Netlogon Parameters	The Console user must have read/write access to the following registry key on the remote system: HKLM\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters
Set startup and recovery options	The Console user must have read/write access to the following registry key on the remote system: HKLM\SYSTEM\CurrentControlSet\Control\CrashControl\
Start metadata cleanup	The Console user must have Domain Administrator rights.
Start online defrag	The Console user must have Domain Administrator rights.

Troubleshooting

Table 28. Troubleshooting minimum permission requirements

Action	Minimum permission requirement
Replication View	The Console user must have Domain User rights.

Web-based Active Directory Health reports

The reports listed in this section are available only in the Web-based application of Active Directory Health. For more information on these reports, see the *Quest® Active Administrator® Web Console User Guide*. For more information on these reports, see [Reports](#) in the *Quest® Active Administrator® Web Console User Guide*.

Active Administrator Web-based application

- The Active Administrator Foundation service (AFS) user account must be a member of the Distributed COM Users group in Active Directory.
- The AFS user account must have **Enable Account** and **Remote Enable WMI Security** permissions for the target servers. See **Authorize WMI users and set permissions** ([https://technet.microsoft.com/en-us/library/cc771551\(v=ws.11\).aspx](https://technet.microsoft.com/en-us/library/cc771551(v=ws.11).aspx)). Be sure the permission entry you create for the AFS account applies to **This namespace and subnamespaces** so the permissions inherit down the tree.
- The AFS user account should be a member of the Event Log Readers group in Active Directory to run event log reports.

The following table details the minimum permissions required for each individual report in Active Directory Health web-based application.

Table 29. Reports minimum permission requirements

Report	Minimum permission requirement
Active Directory White Space	The AFS account must have read access to HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics\ registry key on the remote system or the AFS account should be a member of the Server Operators group in Active Directory.
AD Diagnostic Event Logging Levels	The AFS account must have read access to HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics\ registry key on the remote system or the AFS account should be a member of the Server Operators group in Active Directory.

Table 29. Reports minimum permission requirements

Report	Minimum permission requirement
AD Disk Space	The AFS account must have read access to HKLM\SYSTEM\CurrentControlSet\Services\NTDS\Parameters registry key on the remote system. The AFS account must have read access to the SYSVOL directory. The AFS account must have read access to the folder where the Active Directory databases are located.
Application Event Log	The AFS account must be a member of the Event Log Readers group in Active Directory.
Authentication Methods	Domain User rights required.
Bind with RID Master	Domain User rights required.
Conflicting Objects	Domain User rights required.
Connection Object Duplicates	Domain User rights required.
Cross-Domain Linked GPO	Domain User rights required.
DC Adapter Information	Domain User rights required.
DC Advertising	Domain User rights required.
DC Connection Objects	Domain User rights required.
DC Consistency	Domain User rights required.
DC Information	Domain User rights required.
DC Operating System Information	Domain User rights required. The AFS account must have Enable Account and Remote Enable WMI Security permissions for the target servers.
DC Replica State	Domain User rights required.
DC Roles	Domain User rights required.
DC RootDSE	Domain User rights required.
DC Security Configuration	Domain user rights, WMI rights, and File System rights required.
DC Services	Domain Administrator rights required.
DC Site Coverage	Domain User rights required.
DC Sites	Domain User rights required.
DC SPNs	Domain User rights required.
Directory Health Alerts	Domain User rights required. The AFS account must be a member of the AA_Admins group either in the domain or on the database server, depending on the configuration selected during setup.
Directory Objects	Domain User rights required The AFS account must be a member of the AA_Admins group either in the domain or on the database server, depending on the configuration selected during setup.
Directory Service Event Log	The AFS account must be a member of the Event Log Readers group in Active Directory.
Directory Service Parameters	The AFS account must have read access to HKLM\CurrentControlSet\Services\NTDS\Parameters registry key on the remote system or the AFS account should be a member of the Server Operators group in Active Directory.

Table 29. Reports minimum permission requirements

Report	Minimum permission requirement
Disk Drives	The AFS account must have read access to HKLM\CurrentControlSet\Services\NTDS\Parameters\ registry key on the remote system, or be a member of the Server Operators group in Active Directory.
Distributed File System (DFS) Shares	Domain User rights required.
Distributed File System Replication	Domain User rights required and the AFS account must have Enable Account and Remote Enable WMI Security permissions for the target servers.
DNS Configuration	Domain User rights required and the AFS account must have Enable Account and Remote Enable WMI Security permissions for the target servers.
DNS Event Log	Domain Administrator rights required.
DNS Zone Information	The AFS account must have read access rights to all DNS zones on the target DNS servers, and Enable Account and Remote Enable WMI Security permissions for the target servers.
DNS Zones	The AFS account must have read access rights to all DNS zones on the target DNS servers and Enable Account and Remote Enable WMI Security permissions for the target servers.
Domain Advertising	Domain User rights required.
Domain Configuration	Domain User rights required.
Domain Controllers	Domain User rights required.
Domain Controllers without Replication Links	Domain User rights required.
Domain Naming Masters	Domain User rights required.
Domain Role Holders	Domain User rights required.
Domains	Domain User rights required.
Drivers List	Domain Administrator rights required.
Duplicate SIDS	Domain User rights required.
Event Log	The AFS account must be a member of the Event Log Readers group in Active Directory. NOTE: If selecting the DNS Event Log the AFS account must also have Domain Administrator rights.
Event Log Errors	The AFS account must member of the Event Log Readers group in Active Directory. NOTE: If selecting the DNS Event Log the AFS account must also have Domain Administrator rights.
Forest Configuration	Domain User rights required.
Forest Inventory	Domain User rights required. The AFS account must have read and write access to the Active Administrator share.
Global Catalogs	Domain User rights required.
GPO Consistency	Domain User rights required.
Ineffective GPO	Domain User rights required.
Infrastructure Master	Domain User rights required.
Installed Updates	Domain Administrator rights required.
Inter-site Topology Generators	Domain User rights required.
Lost and Found Items	Domain User rights required.

Table 29. Reports minimum permission requirements

Report	Minimum permission requirement
Naming Context Metadata	Domain user rights required.
Naming Context Topology	Domain user rights required.
Naming Context Topology Aliveness	Domain User rights required.
Naming Context Up-to-Dateness	Domain User rights required.
Owner Information	Domain User rights required.
PDC Emulators	Domain User rights required.
Ping Global Catalog	Domain User rights required.
Remote Access Information	Domain Administrator rights required.
Replication Failures	Domain User rights required.
Replication Logon Privileges	Domain User rights required.
Replication Partners	Domain User rights required.
Replication Partner DNS Resolution	Domain User and WMI rights required.
Replication Queue Length	Domain Administrator rights required.
RID Information	Domain User rights required.
RID Masters	Domain User rights required.
RIDs	Domain User rights required.
Schema Master	Domain User rights required.
Security Event Log	The AFS account must be a member of the Event Log Readers group in Active Directory.
System Event Log	The AFS account must be a member of the Event Log Readers group in Active Directory.
SYSVOL Consistency	Domain User, WMI, and File System Access rights required.
Time Synchronization	Domain User and WMI rights required.
Unlinked GPO	Domain User rights required.

AFS service account minimum permissions

The following table details the minimum permissions required for proper functionality of the Active Administrator Foundation Service (AFS) service account.

Table 30. Minimum permissions for the AFS service account submodules

AFS submodule	Minimum permissions
Account Expiration	<ul style="list-style-type: none"> • Read/Write database permission • Read Active Directory permission
Active Templates	<ul style="list-style-type: none"> • Read/Write Active Directory permission • Read/Write access to the Active Administrator share
Active Directory Health Reports	<ul style="list-style-type: none"> • Read Active Directory permission • Read registry permission • WMI execute permission • Read/Write database permission • Read/Write access to the Active Administrator share

Table 30. Minimum permissions for the AFS service account submodules

AFS submodule	Minimum permissions
Active Directory Infrastructure Reports	<ul style="list-style-type: none"> • Read Active Directory permission • Read/Write database permission • Read/Write access to the Active Administrator share
Alert History Report	<ul style="list-style-type: none"> • Read/Write database permission • Read/Write access to the Active Administrator share
Alerts	<ul style="list-style-type: none"> • Read/Write database permission
Archiving and Purging	<ul style="list-style-type: none"> • Read/Write database permission • Read/Write access to the Active Administrator share
Assessment Report	<ul style="list-style-type: none"> • Read Active Directory permission • Read/Write database permission
Audit Agent	<ul style="list-style-type: none"> • Read Active Directory permission • Read/Write database permission • WMI execute permission
Audit Reports	<ul style="list-style-type: none"> • Read/Write database permission • Read Active Directory permission
Auditing	<ul style="list-style-type: none"> • Read/Write access to the Active Administrator database • Read/Write access to the server working directory
Azure Active Directory	<ul style="list-style-type: none"> • Read/Write database permission
Cache	<ul style="list-style-type: none"> • Read/Write access to the server working directory • Read/Write access to the Active Administrator registry key
Certificate Management	<ul style="list-style-type: none"> • Read Active Directory permission • Read/Write database permission • Read/Write Active Administrator registry permission • Read access to SOFTWARE\Microsoft\SystemCertificates\{StoreName}\Certificates
Certificate Repository	<ul style="list-style-type: none"> • Read/Write Certificate repository folder permission • Read database permission • Read registry permission
Certificate Search	<ul style="list-style-type: none"> • Read Certificate repository folder permission • Read/Write database permission • Read Active Administrator registry permission
Certification report	<ul style="list-style-type: none"> • Read Active Administrator registry permission • Read/Write database permission • Read access to the Active Administrator share
Conductors	<ul style="list-style-type: none"> • Read/Write access to the server working directory • Read access to the Active Administrator registry key • Windows Event Log Write access
Configuration	<ul style="list-style-type: none"> • Read/Write access to the server working directory • Read/Write access to the credentials directory • Read/Write access to the Active Administrator database • Permission to send emails • Read access to Active Directory domains
Configuration report	<ul style="list-style-type: none"> • Read Active Administrator registry permission • Read/Write database permission • WMI execute permission

Table 30. Minimum permissions for the AFS service account submodules

AFS submodule	Minimum permissions
Dashboard	<ul style="list-style-type: none"> • Read access to the Active Administrator database • Windows Event Log Write access • Read access to the Active Administrator registry key • Read access to Active Directory domains • Read/Write access to the server working directory
DC consistency report	<ul style="list-style-type: none"> • Active Directory health reports permission • Remote registry access to SYSTEM\CurrentControlSet\Control\FileSystem • Remote registry access to SYSTEM\CurrentControlSet\Control\Lsa • Remote registry access to Software\Microsoft\Windows\NT\CurrentVersion\Winlogon
DCRIDInfoReport	<ul style="list-style-type: none"> • Active Directory Health reports permission • Remote registry access to SYSTEM\CurrentControlSet\Services\NTDS\IRID Values
DFSR report	<ul style="list-style-type: none"> • Active Directory Health reports permission • Remote registry access to SYSTEM\CurrentControlSet\Services\lanmanserver\Shares
DNS Management	<ul style="list-style-type: none"> • Read Active Directory permission
DNS Analyzer	<ul style="list-style-type: none"> • Read/Write database permission
DNS Event log	<ul style="list-style-type: none"> • WMI execute permission
DNS report	<ul style="list-style-type: none"> • WMI execute permission
DNSConfiguration report	<ul style="list-style-type: none"> • Active Directory Health reports permission • Remote registry access to SYSTEM\CurrentControlSet\Services\DNS\Parameters
DSParameters report	<ul style="list-style-type: none"> • Active Directory Health reports permission • Remote registry access to SYSTEM\CurrentControlSet\Services\NTDS\Parameters
Event definition	<ul style="list-style-type: none"> • Read/Write database permission
Group Policy	<ul style="list-style-type: none"> • Read/Write Active Directory permission • Read/Write access to the Active Administrator share
Helpers	<ul style="list-style-type: none"> • Read access to Active Directory domains • Read access to the Active Administrator database • Windows Event Log Write access • Read/Write access to the server working directory • Permission to send emails • Tasks permission
Inactive Accounts	<ul style="list-style-type: none"> • Read/Write database permission • Read/Write Active Administrator registry permission • Read/Write Active Directory permission
Licensing	<ul style="list-style-type: none"> • Read/Write access to the Active Administrator database • Read access to the Active Administrator registry key • Windows Event Log Write access
LockedOutAccounts	<ul style="list-style-type: none"> • Read/Write database permission • Read/Write Active Directory permission • Read/Write Active Administrator registry permission

Table 30. Minimum permissions for the AFS service account submodules

AFS submodule	Minimum permissions
LogLevels report	<ul style="list-style-type: none"> Active Directory Health reports permissions
WhiteSpace report	<ul style="list-style-type: none"> Remote registry access to SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics
Password Reminder	<ul style="list-style-type: none"> Read Active Directory permission Read/Write database permission
Recovery	<ul style="list-style-type: none"> Read/Write database permission Read Active Directory permission Read/Write access to the Active Administrator share
Replication Monitoring	<ul style="list-style-type: none"> Read Active Directory permission Read/Write database permission
SecConfig Report	<ul style="list-style-type: none"> Active Directory Health reports permissions
DiscSpace Report	<ul style="list-style-type: none"> Remote registry access to SYSTEM\CurrentControlSet\Services\NTDS\Parameters Remote registry access to SOFTWARE\Microsoft\Windows NT\CurrentVersion Remote registry access to SYSTEM\CurrentControlSet\Services\lanmanserver\Shares
Security (All objects) reports	<ul style="list-style-type: none"> Read Active Directory permission Read/Write database permission
Service Monitoring	<ul style="list-style-type: none"> Read/Write database permission
Site coverage report	<ul style="list-style-type: none"> Active Directory Health reports permissions Remote registry access to SYSTEM\CurrentControlSet\Services\Netlogon\Parameters
Tasks	<ul style="list-style-type: none"> Read/Write access to the server working directory Read/Write access to the Active Administrator database Read access to the Active Administrator registry key Windows Event Log Write access
TimeSync report	<ul style="list-style-type: none"> Active Directory Health reports permissions Remote registry access to System\CurrentControlSet\Services\W32Time\Parameters
Trustees	<ul style="list-style-type: none"> Read access to Active Directory domains Read/Write access to the Active Administrator database Read/Write access to the server working directory Cache permissions
User Settings	<ul style="list-style-type: none"> Read/Write access to the Active Administrator database Read access to Active Directory domains Read/Write access to the server working directory
Workstation Logon	<ul style="list-style-type: none"> Read access to the Active Administrator registry key Read/Write access to the server working directory Read/Write access to the Active Administrator database

Installing and configuring Active Administrator

Quest® Active Administrator® has two main components: Server and Console. Install the Console component on any computer that requires it. The Server component needs to be installed on only one computer. Both the Console and Server components can be installed on the same server.

To install and configure Active Administrator, follow the steps in these sections:

- [Installing Active Administrator server](#)
- [Configuring the server](#)
- [Installing Active Administrator console](#)
- [Setting up the console](#)
- [Setting up workstation logon auditing](#)
- [Using Active Administrator](#)

Installing Active Administrator server

i | **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

The AA Configuration Wizard guides you through configuring the various services that are required to run Active Administrator. After this initial configuration, you can modify the server configuration within the Active Administrator console under the Configuration module. See the Configuration chapter in the *Quest® Active Administrator® User Guide*. See [Configuration](#) in the *Quest® Active Administrator® User Guide*.

If you are upgrading Active Administrator or have already run the configuration wizard, 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.

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. See [Applying a license file](#).
 - 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 [Configuring purge and archive settings](#). If you select **No**, see [Setting the Active Administrator database](#).

Applying a license file

i | **NOTE:** The full and evaluation versions of Active Administrator® are identical. The license file is the sole determinant of program functionality.

During the free 30-day trial period, there is unlimited auditing of domain controllers. The Azure Active Directory, Certificate Management, and DNS Management features are not included.

The Azure Active Directory, Certificate Management, DNS 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 Azure Active Directory and Certificate Management features listed under the Configuration module, but when you select the feature, a warning displays that a license is required.

To apply the license file

- 1 Select the licenses to update, and click **Update License**.
 - i** | **NOTE:** You also can update licenses from the Active Administrator Server Manager. From the **Start** menu, open **AA Server Manager**, and click **Update License**.
- 2 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**.
 - To view details of a license, select the license, and click **Details**.
- 3 Click **Next**. See [Setting the Active Administrator database](#).

Setting the Active Administrator database

You can either create a new Active Administrator® database or use an existing database.

To create a new database

- 1 Select **Create a new Active Administrator database**.
- 2 Click **Next**.
- 3 Type the target SQL Server® instance or browse to select a server.
- 4 Type a name for the database or use the default.
- 5 By default, Secure Sockets Layer (SSL) encryption is used for all data sent from the named server to the Active Administrator archive database. To remove encryption, clear the **Encrypt Connection** check box.
- 6 By default, the server certificate is trusted. To remove the trust, clear the check box.
 - i | **NOTE:** If the **Trust Server Certificate** check box is not selected, Active Administrator will walk the validation chain until it finds a valid authority.
- 7 Click **Next**.
- 8 If necessary, adjust the database size or file paths.
- 9 Select the security group type for the SQL groups. Using the default group types is recommended.
- 10 Click **Next**. See [Setting the Active Administrator archive database](#).

To use an existing database

- 1 Select **Use an existing Active Administrator database**.
- 2 Type the target SQL Server instance or browse to select a server.
- 3 Type the database name or browse to select the database.
- 4 By default, Secure Sockets Layer (SSL) encryption is used for all data sent from the named server to the Active Administrator archive database. To remove encryption, clear the **Encrypt Connection** check box.
- 5 By default, the server certificate is trusted. To remove the trust, clear the check box.
 - i | **NOTE:** If the **Trust Server Certificate** check box is not selected, Active Administrator will walk the validation chain until it finds a valid authority.
- 6 Click **Test Connection to validate the database**.
- 7 Click **Next**. See [Setting the Active Administrator archive database](#).

Setting the Active Administrator archive database

Next, set the Active Administrator® archive database, which is used to store events. By default, events older than 60 days are archived. You can either create a new archive database or use an existing archive database.

- i | **NOTE:** After you complete the configuration wizard, you can use the Active Administrator Console to manage archive databases by selecting **Configuration | Archive Databases**.

To create a new archive database

- 1 Select **Create a new Active Administrator Archive database**.
- 2 Click **Next**.
- 3 Type the target SQL Server® instance or browse to select a server.
- 4 Type a name for the database or use the default.
- 5 By default, Secure Sockets Layer (SSL) encryption is used for all data sent from the named server to the Active Administrator archive database. To remove encryption, clear the **Encrypt Connection** check box.

- 6 By default, the server certificate is trusted. To remove the trust, clear the check box.
 - i** | **NOTE:** If the **Trust Server Certificate** check box is not selected, Active Administrator will walk the validation chain until it finds a valid authority.
- 7 Type a name for the archive or use the default.
- 8 Click **Next**.
- 9 If necessary, adjust the database size or file paths.
- 10 Select the security group type for the SQL groups.
- 11 Using the default group types is recommended.
- 12 Click **Next**. See [Configuring purge and archive settings](#).

To use an existing archive database

- 1 Select **Use an existing Active Administrator Archive database**.
- 2 Type the target SQL Server instance or browse to select a server.
- 3 Type the database name or browse to select the archive database.
- 4 By default, Secure Sockets Layer (SSL) encryption is used for all data sent from the named server to the Active Administrator archive database. To remove encryption, clear the **Encrypt Connection** check box.
- 5 By default, the server certificate is trusted. To remove the trust, clear the check box.
 - i** | **NOTE:** If the **Trust Server Certificate** check box is not selected, Active Administrator will walk the validation chain until it finds a valid authority.
- 6 Click **Test Connection to validate the archive database**.
- 7 Click **Next**. See [Configuring purge and archive settings](#).

Configuring purge and archive settings

- i** | **NOTE:** You can set more options to purge events, GPO history, and Active Directory® backups, and to archive events in the Active Administrator Console. See the *Quest® Active Administrator® User Guide*. See [Archiving & purging audit events](#), [Purging GPO history](#), and [Purging Active Directory backups](#) in the *Quest® Active Administrator® User Guide*.

To configure purging and archiving

- 1 Select the purge and archive options to enable or disable.

Table 1. Purge and archive options

Option	Description
Event Archiving	By default, events older than 60 days are archived to the Active Directory archive database. To keep all events in the Active Administrator database, clear the check box.
Group Policy History Purging	By default, the GPO History backups are purged after 90 days. To keep all GPO History backups, clear the check box.
Active Directory Backup Purging	By default, Active Directory backups are purged after 90 days. To keep all Active Directory backups, clear the check box.
Inactive User and Computer History Purging	By default, inactive user accounts and computer history are purged after 30 days. To keep all inactive accounts and computer history, clear the check box.

- 2 Click **Next**. See [Storing Active Administrator data](#).

Storing Active Administrator data

The **Active Administrator Path Selection** page displays the default path to the folder where the Active Administrator data is stored.

The install process creates the ActiveAdministrator share, which contains five subfolders in which Active Administrator data is stored: **ActiveTemplates**, **ADBackups**, **Config**, **GPOHistory**, and **GPORepository**. You can create your own share as long as it resides on a server that is accessible by all Active Administrator users. Make sure the share has sufficient hard drive capacity. You can estimate that each GPO initially takes 2MB to back up. Each version saved thereafter is significantly smaller, about 10k on average. If you have a large Active Directory® database, you should have 10GB available.

i | **IMPORTANT:** If you create a share manually, you must use the name **ActiveAdministrator** for that share.

To create the Active Administrator share

- 1 Type a path to the folder where you want Active Administrator to create the share, or browse to locate a folder.
i | **NOTE:** You should have at least 2GB of free space available on the drive you select. If you have a large Active Directory database, ideally, you should have 10GB free.
- 2 Click **Next**. If the folder you entered does not exist, you receive a confirmation message.
- 3 To create the folder, click **Yes**. See [Setting up the email server](#).

Setting up the email server

The Active Administrator notification service sends automatic emails to specified recipients. On this page, identify the email server to use.

i | **NOTE:** After you complete the configuration wizard, you can use the Active Administrator Console to modify the email server settings by selecting **Configuration | SMTP Settings**.

To set up the email server

- 1 Type the name of the SMTP server that sends the alert emails.
- 2 Type the number of the TCP/IP port on which the SMTP server is listening.
- 3 If your SMTP server requires authentication, type the username and password in the **SMTP User Name** and **SMTP Password** boxes.
- 4 Select to use secure socket layer (SSL), if desired.
- 5 Type the email address that to appear in the **From** box of the alert email. By entering something meaningful, you can use the **From** box to filter your email.
- 6 Choose a format for the email.
- 7 Click **Test Settings**.
- 8 Click **Next**. See [Setting up features and the owner](#).

Setting up features and the owner

On many tasks, an email is sent automatically to the Administrator's email address. You also have the opportunity to enable or disable key features of Active Administrator®. If you disable a feature, you can enable it within the Active Administrator console.

To enable Active Administrator features and set the owner

- 1 Type a valid email address or accept the default.

- 2 By default, the listed Active Administrator features are enabled. To see an explanation of each feature, hover the cursor over the icon. Disable any feature you do not want.

i | **NOTE:** The first time you run the configuration wizard, the check boxes are enabled. The next time you run the configuration wizard, the check boxes are disabled, so you need to use Active Administrator Console to enable/disable the features.

- **Inactive Users and Computers**
To modify the feature, finish the wizard, start Active Administrator Console, and select **Security & Delegation | Inactive Accounts**.
- **Change Your Password Reminder Policy**
To modify the feature, finish the wizard, start Active Administrator Console, and select **Security & Delegation | Password Policy**.
- **Enable Account Expiration Notification**
To modify the feature, finish the wizard, start Active Administrator Console, and select **Security & Delegation | Account Expiration**.
- **Active Directory Replication Monitoring**
To modify the feature, finish the wizard, start Active Administrator Console, and select **AD Infrastructure | Replication Monitoring**.
- **Active Directory Health Assessment Reports**
To modify the feature, finish the wizard, start Active Administrator Console, and select **Settings | Assessment Report**.

- 3 Click **Next**. See [Configuring active template delegation enforcement](#).

Configuring active template delegation enforcement

Active Templates, which are used to grant specific sets of Active Directory® rights to an object, can be configured so that they are automatically reapplied if any of their permissions within the template are accidentally removed. Additionally, you can alert administrators automatically by email when an Active Template is repaired.

i | **NOTE:** After you complete the configuration wizard, you can use the Active Administrator® Console to manage active template delegation enforcement by selecting **Configuration | Active Template Settings**.

To configure active template delegation enforcement

- 1 By default, Active Administrator checks Active Template delegations every 30 seconds.
- 2 To disable the enforcement of Active Template delegations, clear the check box.
- 3 To send reports of broken templates to selected users by email, click **Add** to add email addresses to the list. To suppress the reports, clear the list of email addresses.

i | **NOTE:** You must have configured the Email server to continue. If necessary, click **Back** to return to the **Email Server Settings** page. See [Setting up the email server](#).

- 4 Click **Next**. See [Configuring group policy history](#).

Configuring group policy history

You can set how often selected domain controllers are polled for Group Policy Object (GPO) changes. The polling interval is set to 60 seconds by default. We recommend a polling interval of 60 seconds as this gives administrators enough time to make a few changes to the GPO without creating new versions for every change.

i | **NOTE:** After you complete the configuration wizard, you can use the Active Administrator Console to manage group policy history by selecting **Configuration | GPO History Settings**.

To configure group policy history

- 1 Specify the polling interval.
- 2 To add additional domains, click **Add Domain**, select a domain from the list, and click **OK**.
If the list of domains is long, you can filter the list by typing in the box.
- 3 Click **Next**. See [Configuring Active Directory backups](#).

Configuring Active Directory backups

Administrators can select a domain that contains Windows Server® 2008 (or later) domain controllers and back up Active Directory® user and group objects in that domain. When a situation occurs that requires a user or group object to be restored, administrators can select the object from a list and restore either the object with all the attributes it possessed when it was backed up, or only attributes the administrator selects. In the case of an organizational unit object, administrators have the option of either restoring all objects it contains or all objects it contains of a particular type.

i | **IMPORTANT:** Active Administrator® restores only selected user, group, and organizational unit (OU) objects, and their attributes from the backup file. If you require a backup file that restores Active Directory in its entirety, we recommend that you use an Active Directory disaster recovery product.

The Active Administrator AD Object Backup Service backs up the listed domains based on the settings in the Run backup boxes. If you are using Windows Server 2008 or later, Yes displays in the **Supports Password Recovery** column.

i | **IMPORTANT:** If you choose to disable Password Recovery, passwords are not backed up. If you restore a backup that does not contain passwords, you must unjoin, and then rejoin computer accounts.

By default, an Active Directory backup creates temporary files in the Active Administrator share, under the folder C:\ActiveAdministrator\ADBackups\DOMAIN_*domainname* (where *domainname* is the fully qualified name of the domain being backed up).

i | **NOTE:** After you complete the configuration wizard, you can use the Active Administrator Console to manage Active Directory backups by selecting **Configuration | Recovery Settings**.

To configure Active Directory backups

- 1 Add any additional domains.

To add domains

- a Click **Add Domain**.
 - b In the **Domain** box, type a domain name, or browse to locate a domain.
 - c Specify the domain controller to perform the backup. By default, Active Administrator uses a domain controller automatically selected by Active Directory. You can browse to choose a different domain controller.
 - d Click **OK**.
- 2 Password recovery is enabled by default. If you disable password recovery, passwords will not be backed up. When you restore the backup, you will need to unjoin, and then rejoin the computer accounts.

To disable password recovery

- a Select the domain controller.
 - b Click **Password Recovery**.
 - c Click **Yes**.
- 3 By default, backups occur twice a day at 6:00 A.M. and 6:00 P.M.

To change the frequency

- a Select to run the backup **Every Day**, **Twice a Day**, or **Weekly** in the **Run backup** box.
 - b Select the day of the week or time(s) from the lists.
- 4 Change the temporary folder, if desired.

To change the temporary folder

- a Select the check box.
 - b Browse to locate or create a folder.
 - c Click **OK**.
- 5 Click **Next**. See [Configuring Active Administrator users](#).

Configuring Active Administrator users

Active Administrator® users have unrestricted access to the Active Administrator Console. By default, the user installing and running the configuration wizard is automatically considered an Active Administrator user.

- i** | **NOTE:** Upon initial installation, the Domain Admins group is added automatically to the list. If you remove the Domain Admins group from the list and do not add any groups or users, the Domain Admins group is added automatically the next time you start the configuration wizard.
- After you complete the configuration wizard, you can use the Active Administrator Console to manage users by selecting **Configuration | Role Based Access**.

To configure Active Administrator users

- 1 To add additional users, click **Add**, find and select users, click **OK**.
- 2 Click **Next**. See [Configuring service accounts](#).

Configuring service accounts

The Domain Administrator account provides the necessary permissions for the Active Administrator® foundation and notification services to operate properly.

- i** | **NOTE:** After you complete the configuration wizard, use the AA Server Manager to manage service account logons. See the *Quest® Active Administrator® User Guide* for more information about the AA Server Manager. See [Managing the Active Directory server](#) in the *Quest® Active Administrator® User Guide*.

To configure service accounts

- 1 Type a name for a group/user with domain administrator rights, or browse to locate a group/user.
- 2 Type the account password.
- 3 The default service port number is 15600. To change the port number, type a value.
- 4 To use the same account for the notification service, select the check box. Otherwise, type or browse for an account with domain administrator rights, and type the password.
- 5 Click **Next**.

If you have a license for the Active Directory Health module, see [Connecting to System Center Operations Manager](#). Otherwise, see [Reviewing selections](#).

Connecting to System Center Operations Manager

If you have a license for the Active Directory Health module and are using Microsoft® System Center Operations Manager (SCOM), you can choose to deploy the Quest® Active Administrator® management pack, which establishes a connection to SCOM and enables Active Directory Health alerts from the Directory Analyzer agent to appear in the Operations Manager **Monitoring** pane under the **Quest Active Administrator** folder.

i | **NOTE:** Only System Center 2016 Operations Manager, System Center 2012 R2 Operations Manager, and System Center 2012 SP1 Operations Manager are supported.

NOTE: After you complete the configuration wizard, if you need to make any changes or if you skip this page, you can configure the SCOM connection in the Active Administrator console (**Configuration | SCOM Integration Settings**). See [Configuring SCOM integration](#) in the Active Administrator User Guide. See *Configuring SCOM integration* in the *Active Administrator User Guide*. You also can restart the configuration wizard (**Start | AA Configuration Wizard**). Page through the wizard until you reach the **System Center Operations Manager** page.

NOTE: After you complete the configuration wizard, you can edit the **System Center Operations Manager Notification** to configure which Directory Analyzer alerts to push to SCOM. See [Pushing alerts to System Center Operations Manager](#) in the *Active Administrator User Guide*. See *Pushing alerts to the System Center Operations Manager* in the *Active Administrator User Guide*.

To connect to Systems Center Operations Manager

- 1 Select to forward alert events and to deploy the Quest Active Administrator management pack to the specified SCOM management server.

i | **NOTE:** If the check box is not selected, the **Remove management pack** check box is visible. Use this check box to remove the management pack.

- 2 Type the name of the SCOM management server.
- 3 Type or browse for an account with SCOM administrator rights, and type the password.

i | **NOTE:** The account must be a member of the SCOM Administrator group.

- 4 To test the connection, click **Test Settings**.
- 5 Click **Next**. See [Reviewing selections](#).

Reviewing selections




The **Summary** page displays the choices that you made.

To review your selections and complete the setup

- 1 To modify any selection, click **go back**.
- 2 Click **Finish**.

The **Finish** box shows the progress of the installation. Upon completion, you can click **View Full Log** to examine details of the process.

The **ServerInstallLog.log** is located in the **Quest\Active Administrator\Server\Logging** folder.

- To copy individual items to a text file, click  and copy to a text file.
- To view individual detail, click  to expand the detail.
- To collapse the detail, click .

- 3 Click **Finish**. See [Installing Active Administrator console](#).

Installing Active Administrator console

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

i | **IMPORTANT:** Active Administrator includes the Diagnostic Console, which is also a feature in Quest® Spotlight® for Active Directory®. If you are currently using Spotlight for Active Directory, you must install the Active Administrator 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**.
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.
- 11 Click **Finish**.
The first time the Active Administrator console opens, you are asked to set the Active Administrator Server.
- 12 Type the name of the server where Active Administrator Server is installed, or browse to locate a server.
- 13 Click **OK**.

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

Setting up the console

The Active Administrator® Console has a vast number of tasks that you can perform to manage Active Directory® and the servers in your system. To get started, there are a few necessary tasks to complete. Once you complete these setup tasks, you can start using the full capacity of Active Administrator.

Topics:

- [Setting up auditing on domain controllers](#)
- [Installing audit agents](#)
- [Creating alerts](#)

Setting up auditing on domain controllers

To gather the proper information from the security event logs, the information must first be audited. You need to modify the **Default Domain Controllers Policy** to enable auditing.

i | **NOTE:** If you have not installed the Active Administrator® console, you also can use the Active Directory® Users and Computers MMC snap-in.

To set up auditing on a domain controller

- 1 Start Active Administrator Console.
- 2 Select **Group Policy | Group Policy Objects**.
- 3 Select **Default Domain Controllers Policy**, and click **Edit**.
- 4 Expand **Computer Configuration | Windows Settings | Security Settings | Local Policies**, and select **Audit Policy**.
- 5 Verify that the following policies are defined. If not, double-click the following policies to edit their Success and Failure settings.
 - Audit logon events [Success, Failure]
 - Audit account logon [Success]
 - Audit account management [Success]
 - Audit directory service access [Success]
 - Audit policy change [Success]
 - Audit system events [Success]
- 6 Close the **Group Policy** window.
- 7 At the command prompt, type `gpupdate /force`.

i | **NOTE:** Auditing policy changes may take a long time to take effect.

Installing 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.

i | **IMPORTANT:** Please review the minimum and port requirements for installing the audit agent before you begin the wizard. See [Audit agents requirements](#) and [Port requirements for Active Administrator](#).

To install an audit agent

- 1 Select **Auditing & Alerting | Agents**.
- 2 Click **Install**.
- 3 Click **Next**.
- 4 Type the domain name, or browse to locate a domain.
- 5 If necessary, click **Find Domain Controllers**.
 - To select all listed domain controllers, click **Select all**.
 - To clear all the check boxes, click **Clear all**.
- 6 Select the domain controllers from which you want to audit activity.
- 7 Click **Next**.
- 8 Select the options for the install process.

You can install the audit agent on the selected domain controllers themselves or on another computer in the current domain. A single audit agent should be able to monitor activity on up to five domain controllers, depending on the type and frequency of activities being audited.

i **IMPORTANT:** 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

Table 2. Install options for the audit agent

Option	Description
Install on target Domain Controller(s)	By default, the audit agent is installed on the domain controllers you selected on the previous page.
Audit from an agent on the following computer	Select to install the audit agent on a computer in the domain. Type a computer's fully qualified domain name in the box, or browse to locate a computer. NOTE: If you choose to do remote monitoring, the Advanced Agent is not installed on the selected domain controllers.
Start collecting events immediately after installation of the agent	By default, the audit agent is activated and collection begins immediately upon completion of the installation process. Clear the check box if you want to activate the audit agents manually.
Enable agent monitoring and recovery	By default, Active Administrator monitors the status of the audit agent.

9 Click **Next**.

10 In the **Run as** box, type an account with domain administrator rights, or browse to locate an account, and enter the password.

i **NOTE:** The Active Administrator Agent service can also run under a domain user account provided it is either a local administrator account, which gives it the rights to log on as a service and log on locally, or these two privileges can be granted individually. This user or service 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 initially database creation were modified and it can be found under the Users container object of Active Directory®.

11 To verify the account, click **Test Audit Agent Account**.

12 Click **Next**.

13 Review the summary.

14 Click **Next**.

15 Click **Finish**.

The **Audit Agent** page lists the domain controllers you selected, the time and date of the last event collected, the status of the audit agent and the advanced audit agent, the name of the server on which Active Administrator is installed, and the version number of the audit agent installed on the domain controller.

i **NOTE:** By default, the audit agent is activated upon installation. To change the default setting, select **Configuration | Agent Installation Settings**.

You can view details about the install in the **AuditAgentInstall*.log** file, which is located here: **Program Files\Quest\Active Administrator\Server\Logging**.

Creating alerts

A wizard guides you through creating a new Active Administrator® alert. Alerts provide you the opportunity to combine different conditions into one alert that is sent to specified email recipients. You also can add a filter to the alert to further isolate audit events for the recipient.

To create a new alert

- 1 Select **Auditing & Alerting | Alerts**.
- 2 Click **New**.
- 3 On the **Welcome** page, click **Next**.
- 4 Type a name and optional description for the alert.
- 5 Select the priority of the alert: normal, low, or high.
- 6 Click **Next**.
- 7 Set up the email list of the recipients of the alert notification.

To manage the email list

- To add a new email address, click **Add** and type the email address.
 - To edit a selected email address, click **Edit**.
 - To remove a selected email address from the list, click **Remove**.
- 8 Click **Next**.
 - 9 Select the Event Definitions to include in the alert.
 - To filter the list, type text in the **Filter** box. The list changes as you type characters. The definitions displayed contain the characters you type. For example, if you type **com**, the definitions displayed may contain the words **Completed** or **Computer**.
 - To clear the filter and restore the list, click **X**.
 - To show only selected definitions, open the **Show** box, and choose **Selected**.
 - To show only unselected definitions, open the **Show** box, and choose **Unselected**.
 - 10 Click **Next**.
 - 11 Add alert filters.

Use this feature to help limit the number of emails sent to the specified email list. Alert filters are optional and applied to the details section of the event. Only the events that match the filter will be included in the notification email. For example, if the alert filter is **Contains OU=Sales**, only the events where **OU=Sales** appears in the details section are included in the notification email.

To define an alert filter

- a Click **Add** to add a new alert filter.
- OR–
- Click **Edit** to edit a selected alert filter.
- b Select if the email **Contains** or **Does not contain** the condition text.
 - c Type the text to find in the details section of the alert.
 - d By default the filter conditions are combined using the **OR** operator. If you want to connect with the **AND** operator, select **AND all conditions**.
- 12 Click **Next**.

- 13 Define the quiet time during which no notifications are sent. Alerts that are triggered during the quiet time are still logged to the Alert History. Setting an Alert Quiet Time is optional.

i | **NOTE:** There is also a global quiet time that you can set. The quiet times set here are in addition to any global quiet times. See *Setting global quiet time* in the *Quest® Active Administrator® User Guide*. See *Setting global quiet time* in the *Quest® Active Administrator® User Guide*.

To define a quiet time

- a Click **Add** to add a new quiet time.
–OR–
Click **Edit** to edit a selected quiet time.
 - b Select **Enabled**. To disable a quiet time, clear the check box.
 - c Select **All Days** or specify a specific day.
 - d Set the start and end time.
 - e By default, actions associated with the alert are stopped during quiet time. To execute actions during quiet time, select the check box.
- 14 Click **Next**.
 - 15 Set the alert threshold. The alert threshold sets limits that must be met before alerts are sent out.

To add a new threshold

- a Click **Add** to add a new threshold.
–OR–
Click **Edit** to edit a selected threshold.
 - b Select **Enabled**. To disable a threshold, clear the check box.
 - c Select the event definition from the list.
 - d Select the number of events and minutes to define the threshold.
- 19 Click **Next**.
 - 19 Define the action that this alert executes when the alert condition is met.

The action is executed using the Notification service account. Please make sure the Notification Service account has sufficient rights to all of the resources needed by the action.

To define the action the alert executes

- a Select **Enabled**. To disable an action, clear the check box.
 - b Type the full path to the executable for the program or script or browse to locate the executable.
i | **NOTE:** The script must reside in a share on the Active Administrator server. That share must be accessible to the Active Administrator Foundation Server (AFS) service and the operator of the remote Active Administrator console. The path to the script must be entered using Uniform Naming Convention (UNC).
 - c For the argument, browse to open the list of Alert Action Variables.
 - d Select a variable in the top box, and then click **Insert**.
 - e Click **OK**.
 - f Optionally, type the path to a folder that contains the executable or browse to locate the folder.
- 16 Click **Next**.
 - 17 Review the summary.
 - 18 Click **Finish**.

Setting up workstation logon auditing

With workstation logon auditing, you can audit user logon and logoff events including lock and unlock. [Deploying the workstation logon audit agent](#) adds these workstation events to the event definitions:

- User Locked Workstation
- User Logoff
- User Logon (interactive)
- User Logon (Remote Desktop)
- User Unlocked Workstation

Deploying the workstation logon audit agent

To audit user logon events, you must enable workstation logon auditing and deploy the workstation logon audit agent to workstations and member servers. Once enabled, the workstation logon auditing service will send messages to the Active Administrator® server.

i | **NOTE:** The workstation logon auditing service must run under context of the local system account.

To enable workstation logon auditing

- 1 Select **Configuration | User Logon Agent Settings**.
- 2 Enable workstation logon auditing and verify the port number. By default the port number is 15601, which is the port for Active Administrator Foundation Service (AFS).

i | **NOTE:** If Windows® Firewall is enabled on the workstation where the Active Administrator Workstation Logon Auditing Agent is installed, you need to create an exception to allow communication with Active Administrator Foundation Service (AFS) through port 15601. See [Enabling the default port](#).

- 3 Click **Save**.

To deploy the workstation logon agent

- 1 Open Windows Explorer.
- 2 Navigate to C:\Program Files\Quest\Active Administrator\Server\WorkstationLogonAuditAgent.
 - Copy **ActiveAdministrator.admx** to C:\Windows\PolicyDefinitions on the domain controller.
 - Copy **ActiveAdministrator.adml** to C:\Windows\PolicyDefinitions\en-US on the domain controller.
 - Copy **Active Administrator 8.2 Workstation Audit Agent.msi** to a share where everyone has access.
- 3 Start **Active Administrator 8.2 Workstation Audit Agent.msi**.
- 4 On the welcome page, click **Next**.
- 5 Accept the license agreement and click **Next**.
- 6 Click **Install**.
- 7 Click **Finish**.

Enabling the default port

If Windows® Firewall is enabled on the workstation where the workstation logon auditing agent is installed, you need to create an exception to allow communication with Active Administrator® Foundation Service (AFS) through port 15601.

To enable the default port

- 1 On the workstation where the workstation logon auditing agent is installed, start the **Windows Firewall with Advanced Security** snap-in, right-click on **Outbound Rules**, and choose **New Rule**.
- 2 Select **Port**.
- 3 Click **Next**.
- 4 Select **Specific local ports**, and type **15601**.
- 5 Click **Next**.
- 6 Select **Allow the connection**.
- 7 Click **Next**.
- 8 Click **Next**.
- 9 Type a name for the rule, and (optionally) a description.
- 10 Click **Finish**.

Using Active Administrator

For more information on using Active Administrator® Console, see the *Quest® Active Administrator® User Guide* or access the help contents within the Active Administrator Console application.

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece—you—to the community, to the new Quest.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

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.

Symbols

.NET Framework, 6, 8

A

AA Configuration Wizard, 35

AA_Admin, 11

AA_User, 11

account expiration

permissions, 15

Active Administrator

configure users, 41

create share, 38

enable features, 38

install server, 34

set owner, 38

Active Administrator Advanced Auditing, 11

Active Administrator Agent, 11

Active Administrator Data Services, 11

permissions, 17

Active Administrator Foundation Service

default port, 49

Active Administrator Foundation service, 11, 12

Active Administrator Notification service, 11

Active Administrator server

configure, 35

Active Directory

configure backups, 40

Active Directory Health

permissions, 16, 24

report permissions, 27

Active Directory recovery

permissions, 20

Active Directory trust

permissions, 21

active template

delegation enforcement, 39

permissions, 15

ActiveAdministrator database, 11

add

alert, 46

ADS, 11

AFS, 11, 12

AFS service

permissions, 30

agent

permissions, 17

workstation logon, 48

alert

create, 46

alerts

permissions, 16, 18

analyzer

permissions, 16

archive

configure, 37

permissions, 18

archive database

create, 36

ASync-In, 10

audit agent

install, 44

permission, 18

audit reports

permissions, 18

AuditAgentInstall*.log, 45

auditing

set up, 44

auditing and alerts

permissions, 18

Azure Active Directory

permissions, 16

C

certificate authority

permissions, 14

certificate landing page

permissions, 13

certificate management

permissions, 13

certificate repository

permissions, 14

certificate search

permissions, 13

COM+ Network Access, 10

configuration

permissions, 23

- configure
 - Active Administrator server, 35
 - Active Directory backups, 40
 - archiving, 37
 - email server, 38
 - purging, 37
 - service accounts, 41
 - users, 41
 - connect
 - SCOM, 42
 - console
 - install, 43
 - create
 - Active Administrator share, 38
 - archive database, 36
 - database, 36
- D**
- dashboard
 - permissions, 12
 - data collector
 - permissions, 17
 - requirements, 17
 - database
 - create, 36
 - DC management
 - permissions, 22
 - DCOM-In, 10
 - delegation status
 - permissions, 15
 - Diagnostic Console
 - permissions, 17
 - DNS management
 - permissions, 22
 - DNS Server Tools, 8
 - install, 8
 - Domain Admins, 11
- E**
- email server
 - configure, 38
 - enable
 - Active Administrator features, 38
 - password recovery, 10
 - event definition
 - permissions, 18
- G**
- gpo history
 - configure, 40
 - group policy
 - permissions, 19
 - Group Policy Management Console, 6, 8
 - activate, 8
- H**
- Home page
 - permissions, 12
 - HTTP Port, 10
 - HTTPS, 10
- I**
- inactive accounts
 - permissions, 15
 - install
 - Active Administrator server, 34
 - audit agent, 44
 - console, 43
 - DNS Server Tools, 8
 - workstation logon agent, 48
- L**
- license
 - apply, 35
 - locked out accounts
 - permissions, 14
 - log
 - AuditAgentInstall*.log, 45
 - serverinstalllog.log, 42
- M**
- Microsoft Nano Server 2016, 6, 7
 - Microsoft® System Center Operations Manager, 42
- N**
- non-domain admin user account, 11
- P**
- password policies
 - permissions, 15
 - password recovery
 - enable, 10
 - password reminder
 - permissions, 15
 - permission
 - account expiration, 15
 - Active Administrator Data Services, 17
 - Active Directory Health, 16, 24
 - Active Directory Health reports, 27
 - Active Directory recovery, 20
 - Active Directory trust, 21
 - AFS service, 30

- agent, 17
- alerts, 16
- analyzer, 16
- archive, 18
- audit reports, 18
- auditing alerts, 18
- auditing and alerts, 18
- Azure Active Directory, 16
- certificate authority, 14
- certificate search, 13
- configuration, 23
- data collectors, 17
- DC management, 22
- DNS management, 22
- event definition, 18
- group policy, 19
- inactive accounts, 15
- password reminder, 15
- purge, 18
- purge account history, 15
- replication monitoring, 21
- troubleshooter, 17
- permissions
 - active template, 15
 - audit agent, 18
 - certificate landing page, 13
 - certificate management, 13, 14
 - dashboard, 12
 - delegation status, 15
 - diagnostic console, 17
 - Home page, 12
 - locked out accounts, 14
 - password policies, 15
 - search, 13
 - security, 14
 - security landing page, 14
 - user logon activity, 14
- port
 - Active Administrator Foundation Service, 49
- purge
 - configure, 37
 - permissions, 18
- purge account history
 - permissions, 15

Q

QL Server 2016, 6

R

Remote Event Log Management, 10
 Remote Procedure Call, 10

Remote Registry Service, 10
 Remote Server Administration Tools, 8
 replication monitoring

- permissions, 21

S

SCOM

- connect, 42

 search

- permissions, 13

 security

- permissions, 14

 security landing page

- permissions, 14

 ServerInstallLog.log, 42
 service

- Active Administrator Advanced Auditing, 11
- Active Administrator Agent, 11
- Active Administrator Data, 11
- Active Administrator Foundation, 11
- Active Administrator Notification, 11

 service accounts

- configure, 41

 set owner, 38
 SHA-2 certificates, 7
 SQL Server 2008, 6
 SQL Server 2012, 6
 SQL Server 2014, 6
 SSL, 10

T

TCP Port, 9
 troubleshooter

- permissions, 17

U

update

- license, 35

 user

- configure, 41

 User Locked Workstation, 48
 User Logoff, 48
 User Logon, 48
 user logon activity

- permissions, 14

 user privilege requirements, 10
 User Unlocked Workstation, 48

W

Windows 10, 7, 8, 9
 Windows 7, 7, 8, 9

- Windows 8, 8
- Windows 8.1, 7, 8, 9
- Windows Server 2008 R2, 7, 8, 9
- Windows Server 2012, 7, 8, 9
- Windows Server 2012 R2, 7, 8, 9
- Windows Server 2016, 7, 8, 9
- WMI-In, 10
- workstation logon agent
 - deploy, 48
- workstation logon auditing, 48