Quest® Active Administrator® 8.6.3
Install Guide

Legend

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

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

Contents

1

Installation Considerations for Active Administrator

The following section outlines the installation considerations for Active Administrator.

Topics:

- System requirements
- Active Administrator module requirements
- Active Directory Health minimum permissions
- AFS service account minimum permissions
- Diagnostic Console minimum permissions

System requirements

The system requirements are the same for all components of Active Administrator. Before installing or upgrading

Active Administrator, ensure that your system meets the following minimum hardware and software requirements.

> **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.

Topics

- Server hardware requirements
- Server software requirements
- SQL Server requirements
- Console requirements
- Audit agents requirements
- Workstation logon audit agents requirements
- Web Console requirements
- System Center requirements
- Port requirements
- User privilege requirements
- Active Administrator module requirements
- Upgrade and compatibility
- Product licensing

Server hardware requirements

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

> **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.

The following table outlines the server hardware requirements.

Table 1. Server hardware requirements

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

Server software requirements

The following table outlines the server software requirements.

Table 2. Server software requirements

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

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

> **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 run the statement. The results list all sort and collation information for the database.

Console requirements

Topics:

- Console hardware requirements
- Console software requirements

Console hardware requirements

The following table outlines the console hardware requirements.

Table 3. Console hardware requirements

Requirement	Details
Processor	1 GHz
Memory	256 MB
Hard disk space	100 MB
Operating system	- Windows 8.1 - Windows 10 - Windows Server 2016 - Windows Server 2019 - Windows Server 2022 **NOTE:** Active Administrator does not support Microsoft Nano Server 2016. **NOTE:** If you are using the Certificate module, see Table 4 for information on support for SHA-2 certificates.

The following table outlines the 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 2016	supported	supported	supported
Windows Server 2019	supported	supported	supported
Windows 8.1	supported	supported	supported
Windows 10	supported	supported	supported

Console software requirements

The following software is required for the Active Administrator console.

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

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

Table 5. GPMC and DNS Server Tools install information

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

Audit agents requirements

The following table outlines the audit agents hardware requirements.

Table 6. Audit agents hardware requirements

Requirement	Details
Processor	1 GHz or higher
Hard disk	100 MB
Memory	256 MB
Operating systems	• Windows Server 2016 • Windows Server 2019 • Windows Server 2022

Workstation logon audit agents requirements

The following table outlines the 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	• Windows 8.1 • Windows 10 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022

Web Console requirements

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

- Microsoft Edge™ 98
- Google Chrome™ 98
- Mozilla® Firefox® 97

System Center requirements

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

- System Center 2016 Operations Manager

Port requirements

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

Active Administrator Console

- TCP 15600 for Active Administrator Foundation Service (AFS) communication with Active Administrator Server
- TCP 8080 for communication with Active Administrator Web Server through the Web Console (internal, http)
- TCP 9443 for communication with Active Administrator Web Server through the Web Console (external, https)
- TCP 389 for communication with Active Directory on domain controllers

Active Administrator Server

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

Active Administrator database server

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

Domain controller with no installed agents

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

Domain controller with auditing agent

- TCP 1433 for communication with SQL Server

Domain controller with Active Directory Health Analyzer agent

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

Domain controller with Azure Active Directory Connect agent

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

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

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

SMTP server

- TCP 25 for sending email notifications via SMTP

Workstation with logon agent

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

Figure 1. Port requirements example
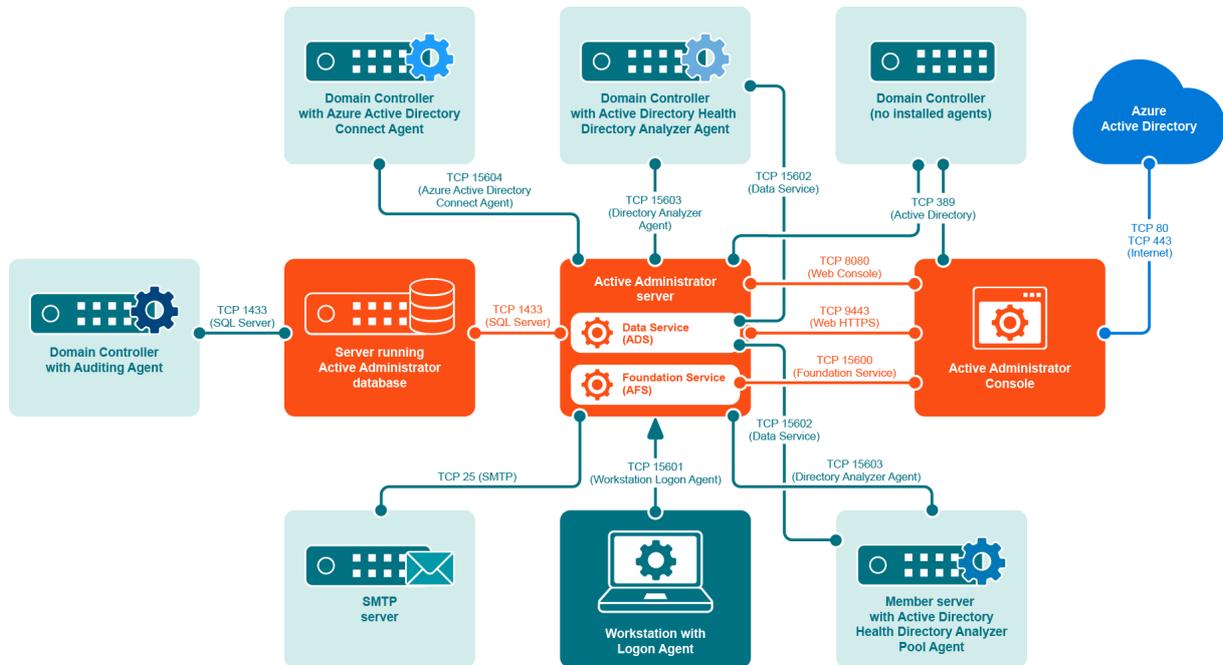
Additional requirements

- Remote Procedure Call (RPC) must be open between the AFS Server and the target.

- When installing the audit agent on a member server instead of a domain controller, the following inbound firewall exceptions for Windows Management Instrumentation must be enabled:

    - ASync-In

    - DCOM-In

    - WMI-In

- If you are using the Certificate Management feature, Remote Registry Service must be enabled on all Windows computers on which certificates are managed.

- If you want to access the DNS event logs in Active Administrator, the following inbound firewall exceptions are required on each DNS server:

    - COM+ Network Access (DCOM-In)

    - Remote Event Log Management (NP-In)

    - Remote Event Log Management (RPC)

    - Remote Event Log Management (RPC-EPMAP)

- HTTP Port 8080 must be open on the computer running the Web Server.

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.

User privilege requirements

- To install Active Administrator, a user must hold administrative rights on the local system and the SQL instance that will host the Active Administrator database.

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

Password recovery

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

Services

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

When choosing an account, keep these requirements in mind:

- Active Administrator Foundation service (AFS) requires an account that is a member of the Domain Admins group. For more detailed permission requirements, see Active Administrator module requirements.

- Active Administrator Data Services (ADS) requires an account that is a member of the AA_Users group, has read access to the enterprise, and has full access on the server where the Active Directory Health Analyzer agent is installed. For more detailed permission requirements, see Active Administrator Data Services (ADS) requirements.

- Active Administrator Advanced Auditing runs as the Local System account, regardless of the user account configured for the Active Administrator Agent service.

- Active Administrator Agent can run under a Domain User account provided it is a local administrator account, which gives it the rights to log on as a service, log on locally and manage auditing and security log. The user account should also be a member of the AA_Admin group, which by default is located in the Local groups of the server where the ActiveAdministrator database is located. If the group is not found in this location, the settings during the initial database creation were modified and it can be found under the Users container object of Active Directory.

- Active Administrator Agent can run under a non-domain admin user account if the following permissions are set.

    To set up a non-domain admin user account

    1 Create a Domain User account within Active Directory Users and Computers.

    2 Use Group Policy Management console (GPMC) to edit the Default Domain Controller Group Policy Object. Give the user account **User Rights** to **Manage auditing and security log**.

    3 On the target domain controllers, give the user account Read permission to the registry key: **HKLM\System\CurrentControlSet\Services\Eventlog\Security**.

4   After the agent is installed, verify the user account has Write permission on the folder:
     C:\Windows\SLAgent.

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

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

Audit database

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

•   AA_Admin group = users that need to be able to update the database

•   AA_User group = users that only need to run reports from the database

Active Administrator module requirements

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

Modules:

•   Home

•   Search

•   Certificates

•   Security and Delegation

•   Active Directory Health

•   Auditing & Alerts

•   Group Policy

•   Active Directory Recovery

•   DC Management

•   DNS Management

•   Active Administrator Module 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	Open to all users, but some items may not be available if the user does not have the required permission.
	
	Must have read access to the entire domain:
	    • Active Directory Search
	
	Must have the appropriate permissions on the target user account:
	    • Reset Password
	    • Unlock User Account
	    • Enable/Disable User Account
	
	Must have the appropriate permissions on the target group:
	    • Add a user to a group
	    • Remove a user from a group
	
	Must have the appropriate permissions on the target computer:
	    • 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.

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.
Certificate Authority (CA)	N/A	**NOTE:** Permissions apply to the AFS account or to the user account specified in the forest settings. Must be a member of the AA_Admins_Group and have Active Directory read access Must have read access to the CA server via remote registry to the registry key HKEY_LOCAL_MACHINE\SYSTEM\Current ControlSet\Services\CertSvc Must be a full administrator on the CA server to get the status of the CA service and to stop and start the service. Must be a full administrator on the CA server to back up the CA server
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 and 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.

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	Must have the Active Administrator Security role. 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.	To view the Active Templates applied to the object, must have permissions to the ActiveTemplate folder in the Active Administrator share.

Table 11. Required permissions for the Security & Delegation module

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

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.

> **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.
> - For details on the minimum permissions required for the Active Directory Health module, see Active Directory Health minimum permissions.
> - The Active Directory Health Analyzer agent must be upgraded to the current version.

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 12. Required permissions for the Active Directory Health module

Submodule	Console user account	AFS account
Active Directory Health Landing Page	Must have the Active Administrator Active Directory Health Analyzer role.	Must be a member of the AA_Users group.
Analyzer	Must have the Active Administrator Active Directory Health Analyzer role.	N/A
Alerts	Must have the Active Administrator Active Directory Health Analyzer role.	Must be a member of the AA_Users group.
	To manage notifications, must have the Active Administrator Active Directory Health Notification Management role.	Must have read/write access to the DACache folder in the Active Administrator share.
Agents	To manage agents, must have the Active Administrator Active Directory Health Agent Management role.	To install, edit, and remove agents, must be a member of the AA_Admins group and have full control access to the target server.
	To manage notifications, must have the Active Administrator Active Directory Health Notification Management role.	To update alerts and collectors, and to manage notifications, must have read/write access to the DACache folder in the Active Administrator share.
	to manage data collectors, must have the Active Administrator Active Directory Health Data Collector Management role.	**NOTE:** For the specific permissions required for each data collector, see *Appendix A* in the *Quest*® Active Administrator® User Guide or online help.
	To manage alerts, must have the Active Administrator Active Directory Health Alert Management role.	
	To manage agents, must have the Active Administrator Active Directory Health Agent Management role.	

Table 12. Required permissions for the Active Directory Health module

Submodule	Console user account	AFS account
Troubleshooter	Must have the Active Administrator Active Directory Health Troubleshooter role.	N/A
	To view reports or perform troubleshooting operations, must have WMI remote access enabled and be a member of the Distributed COM users group.	
	To run jobs, must have full control access to the target server.	
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 13. 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 *Appendix A* of the *Quest*® Active Administrator® *User Guide* or online help.
Agent Monitor and Recovery	Must have full access on the server where the Active Directory Health Analyzer agent is installed.

Data collectors requirements

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

To capture all data collectors accessible by the Active Directory Health Analyzer, the startup account for the Active Directory Health 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*.

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.

Table 14. 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.

Table 15. 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.
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.

Table 15. Required permissions for the Group Policy module

Submodule	Console user account	AFS account
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.

Table 16. 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. Must be a member of Domain Admins or Enterprise Admins group. 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.
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.

Table 16. Required permissions for the Active Directory Recovery module

Submodule	Console users account	AFS account
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.

Table 17. 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

Table 17. Required permissions for the DC Management module

Submodule	Console user account	AFS account
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.

Table 18. 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.
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

Active Administrator Module 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.

Table 19. Required permissions for the Configuration module

Subsystem	Console user	AFS account
Configuration Landing Page Tasks Role Based Access SMTP Settings Notification Settings Active Template Settings Agent Installation Settings Recovery Settings GPO History Settings GPO History Settings Certification Configuration Service Monitoring Policy	Must have the Active Administrator Full Control role.	Must be a member of the AA_Users group.
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
- 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 Active Directory Health Analyzer agent account needs to be a member of the Performance Monitor Users group in Active Directory.

Active Directory Health Module 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 20. Active Directory Health Analyzer agent management minimum permission requirements

Action	Minimum permission requirement
Install agents	• The AFS account must have local administrator rights to install a Windows service on the target system. • The Active Directory Health Analyzer agent service account must have the **run as a service** right on the target system.
Uninstall agents	• The AFS account must have local administrator rights to uninstall a Windows service on the target system.
View agent status	• Using a group policy, assign the Start, Stop, and Query status permissions to the AFS account for the Active Administrator Active Directory Health Analyzer Agent service. • The AFS account must have read access to the WINDIR\DAAgent\ folder on the target system.
Stop/Start/Restart agents	• Using a group policy assign the Start, Stop, and Query status permissions to the AFS account for the Active Administrator Active Directory Health Analyzer Agent service
Upgrade agents	• The AFS account must have local administrator rights to install a Windows service on the target system.
Set agent startup account	• The AFS account must have local administrator rights to set a Windows service startup account on the target system.
Set agent port number	• Using a group policy, assign the Start, Stop, and Query status permissions to the AFS account for the Active Administrator Active Directory Health Analyzer Agent service. • The AFS account must have read access to the WINDIR\DAAgent\ folder on the target system
Test connection	• Domain User rights required
View agent log	• Domain User rights required

Load-balanced agents

Table 21. 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 22. 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 Active Directory Health 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 Active Directory Health Analyzer Agent service.

Remediation (built-in only)

Table 23. 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 24. 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 25. Data point routing minimum permission requirements

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

Troubleshooter

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

Jobs

Table 26. 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.
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 27. 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*.

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). 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 28. 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.
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.
	The AFS account must have Enable Account and Remote Enable WMI Security permissions for the target servers.
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.

Table 28. Reports minimum permission requirements

Report	Minimum permission requirement
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.
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.

Table 28. Reports minimum permission requirements

Report	Minimum permission requirement
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.
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 29. Minimum permissions for the AFS service account submodules

AFS submodule	Minimum permissions
Account Expiration	• Read/Write database permission • Read Active Directory permission
Active Templates	• Read/Write Active Directory permission • Read/Write access to the Active Administrator share
Active Directory Health Reports	• Read Active Directory permission • Read registry permission • WMI execute permission • Read/Write database permission • Read/Write access to the Active Administrator share
Active Directory Infrastructure Reports	• Read Active Directory permission • Read/Write database permission • Read/Write access to the Active Administrator share
Alert History Report	• Read/Write database permission • Read/Write access to the Active Administrator share
Alerts	• Read/Write database permission
Archiving and Purging	• Read/Write database permission • Read/Write access to the Active Administrator share
Assessment Report	• Read Active Directory permission • Read/Write database permission
Audit Agent	• Read Active Directory permission • Read/Write database permission • WMI execute permission
Audit Reports	• Read/Write database permission • Read Active Directory permission
Auditing	• Read/Write access to the Active Administrator database • Read/Write access to the server working directory
Cache	• Read/Write access to the server working directory • Read/Write access to the Active Administrator registry key
Certificate Management	• Read Active Directory permission • Read/Write database permission • Read/Write Active Administrator registry permission • Read access to SOFTWARE\Microsoft\SystemCertificates\{StoreName}\Certificates
Certificate Repository	• Read/Write Certificate repository folder permission • Read database permission • Read registry permission
Certificate Search	• Read Certificate repository folder permission • Read/Write database permission • Read Active Administrator registry permission
Certification report	• Read Active Administrator registry permission • Read/Write database permission • Read access to the Active Administrator share

Table 29. Minimum permissions for the AFS service account submodules

AFS submodule	Minimum permissions
Conductors	• Read/Write access to the server working directory • Read access to the Active Administrator registry key • Windows Event Log Write access
Configuration	• 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	• Read Active Administrator registry permission • Read/Write database permission • WMI execute permission
Dashboard	• 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	• 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	• Active Directory Health reports permission • Remote registry access to SYSTEM\CurrentControlSet\Services\NTDS\RID Values
DFSR report	• Active Directory Health reports permission • Remote registry access to SYSTEM\CurrentControlSet\Services\lanmanserver\Shares
DNS Management DNS Analyzer DNS Event log DNS report	• Read Active Directory permission • Read\Write database permission • WMI execute permission • WMI execute permission
DNSConfiguration report	• Active Directory Health reports permission • Remote registry access to SYSTEM\CurrentControlSet\Services\DNS\Parameters
DSParameters report	• Active Directory Health reports permission • Remote registry access to SYSTEM\CurrentControlSet\Services\NTDS\Parameters
Event definition	• Read/Write database permission
Group Policy	• Read/Write Active Directory permission • Read/Write access to the Active Administrator share
Helpers	• 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

Table 29. Minimum permissions for the AFS service account submodules

AFS submodule	Minimum permissions
Inactive Accounts	• Read/Write database permission • Read/Write Active Administrator registry permission • Read/Write Active Directory permission
Licensing	• Read/Write access to the Active Administrator database • Read access to the Active Administrator registry key • Windows Event Log Write access
LockedOutAccounts	• Read/Write database permission • Read/Write Active Directory permission • Read/Write Active Administrator registry permission
LogLevels report WhiteSpace report	• Active Directory Health reports permissions • Remote registry access to SYSTEM\CurrentControlSet\Services\NTDS\Diagnostics
Password Reminder	• Read Active Directory permission • Read/Write database permission
Recovery	• Read/Write database permission • Read Active Directory permission • Read/Write access to the Active Administrator share
Replication Monitoring	• Read Active Directory permission • Read/Write database permission
SecConfig Report DiscSpace Report	• Active Directory Health reports permissions • 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	• Read Active Directory permission • Read/Write database permission
Service Monitoring	• Read/Write database permission
Site coverage report	• Active Directory Health reports permissions • Remote registry access to SYSTEM\CurrentControlSet\Services\Netlogon\Parameters
Tasks	• 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	• Active Directory Health reports permissions • Remote registry access to System\CurrentControlSet\Services\W32Time\Parameters
Trustees	• Read access to Active Directory domains • Read/Write access to the Active Administrator database • Read/Write access to the server working directory • Cache permissions

Table 29. Minimum permissions for the AFS service account submodules

AFS submodule	Minimum permissions
User Settings	• Read/Write access to the Active Administrator database • Read access to Active Directory domains • Read/Write access to the server working directory
Workstation Logon	• Read access to the Active Administrator registry key • Read/Write access to the server working directory • Read/Write access to the Active Administrator database

Diagnostic Console minimum permissions

To run the Diagnostic Console, the Domain Administrator permission is recommended.

The Performance Monitor Users and Performance Log Users permissions are the minimum permissions required to collect most, but not all, Active Directory performance data on the target domain controller.

The Domain Administrator permission is needed for the Diagnostic Console to collect data and display the following critical alarms on target domain controllers:

- Records and registration status for DNS entries

- Percentage of disk space consumed on the system disk

- Active Directory store database size, the amount of free space remaining, and the total size of the drive

- Physical RAM

- Domain controller configuration, such as Installed Software, Installed Hotfixes, and Network Adapters, on the target domain controller

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:

- Backing up your data
- Installing Active Administrator server
- Configuring the server
- Installing Active Administrator console
- Setting up the console
- Setting up workstation logon auditing
- Using Active Administrator

Backing up your data

> **i** | **IMPORTANT:** Prior to upgrading Active Administrator, it is highly recommended that you back up your Active Administrator database files and the folders in the Active Administrator share to avoid any loss of data. Quest Software will not be able to recover your data.

> **!** | **CAUTION:** It is very important to record the passphrase related to the backup files in a secure location where it can be retrieved when required. If the passphrase is lost, it will be impossible to restore and use Active Administrator backups.

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

- The Active Administrator share is located at the root on the computer where Active Administrator is installed (**C:\ActiveAdministrator**). The Active Administrator share contains several folders that contain information, such as settings, templates, repositories, backup files, and log files. Back up the entire Active Administrator share.

- The Active Administrator data files are located on the named data server. To identify the data server and database file, run the Active Administrator Server Configuration report from the Active Administrator Console (**Settings | Configuration Report**).

- The ActiveAdministrator.xml file is in the folder where Active Administrator server is installed. The default location is **C:\Program Files\Quest\Active Administrator\Server**.

- The registry key is located at **HKEY_LOCAL_MACHINE\SOFTWARE\Quest\Active Administrator**.

Installing Active Administrator server

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

To install Active Administrator server

1   Unzip the Active Administrator folder, browse to the Installation folder, and run the Active Administrator 8.6 Server.msi.

2   On the Welcome screen of the Install Wizard, click **Next**.

3   Click **View License Agreement**.

4   Scroll to the end of the license agreement.

5   Click **I accept these terms**, and click **OK**.

6   Click **Next**.

7   To change the location of the program files, click **Change**, or click **Next** to accept the default installation directory.

8   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**.

9   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*.

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.

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

- Applying a license file

- Creating a passphrase

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 Certificate Management features are not included.

The Certificate Management and Active Directory Health features each require a separate license. If you do not have a license file to apply, the module does not appear in Active Administrator. You will see the Certificate Management 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 Creating a passphrase.

Creating a passphrase

A passphrase is used to control access to Active Administrator data. A passphrase is similar to a password in usage, but is generally longer for added security. Active Administrator content will be secured using the passphrase and requires the passphrase for accessing the content or for changing the passphrase.

! | **CAUTION:** You must know the current passphrase to change or restore the passphrase. It is very important to record the passphrase in a secure location where it can be retrieved when required.

CAUTION: If the passphrase is lost, it will be impossible to access Active Administrator data. You will have to uninstall Active Administrator, remove all associated files, and start a new installation of Active Administrator. For more information, see Recovering from a lost passphrase **on page 56**.

> **NOTE:** You can manage the passphrase from the Active Administrator Server Manager. From the **Start** menu, open **AA Server Manager**, and click **Manage** in the Security Manager section.

To create a passphrase

1   Type a passphrase of 25 to 32 characters and then type it again to confirm.

2   Record the passphrase in a secure location.

> **CAUTION:** You must know the current passphrase to change or restore the passphrase. It is very important to record the passphrase in a secure location where it can be retrieved when required.

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; however, you must ensure that an existing database has been upgraded to the latest version before proceeding.

> **NOTE:** If you are upgrading Active Administrator, you have the option to upgrade your existing live database and all archive databases.

> **NOTE:** In a TLS 1.2 only environment, SQL 2012 Native Client must be installed on the Active Administrator server and agent servers, and the database server must be configured to use TLS 1.2.

To create a new database

1   Select **Create a new Active Administrator database**.

2   Click **Next**.

3   Type the target SQL Server or Azure SQL Managed instance.

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.

> **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   If using an Azure SQL Managed instance, select **SQL Server Authentication**, enter a SQL user ID that has login privilege for the SQL Managed instance, and enter the password for the SQL account.

The characters in the password will be hidden. Each character will be represented by a displayed dot. Select **Show Password** to display the password.

8   Click **Next**.

9   If necessary, adjust the database size or file paths.

10 Select the security group type for the SQL groups. Using the default group types is recommended.

11 Click **Next**. See Setting the Active Administrator database.

To use an existing database

1   Ensure the existing database has been upgraded to the latest version before proceeding.

2   Select **Use an existing Active Administrator database**.

3   Type the target SQL Server or Azure SQL Managed instance.

4   Type the database name or browse to select the database.

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   If using an Azure SQL Managed instance, select **SQL Server Authentication**, enter a SQL user ID that has login privilege for the SQL Managed instance, and enter the password for the SQL account.

8   The characters in the password will be hidden. Each character will be represented by a displayed dot. Select **Show Password** to display the password.

9   Click **Test Connection to validate the database**.

10 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**.

> **i** | **NOTE:** In a TLS 1.2 only environment, SQL 2012 Native Client must be installed on the Active Administrator server and agent servers, and the database server must be configured to use TLS 1.2.

To create a new archive database

1   Select **Create a new Active Administrator Archive database**.

2   Click **Next**.

3   Type the target SQL Server or Azure SQL Managed instance.

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   If using an Azure SQL Managed instance, select **SQL Server Authentication**, enter a SQL user ID that has login privilege for the SQL Managed instance, and enter the password for the SQL account.

8   The characters in the password will be hidden. Each character will be represented by a displayed dot. Select **Show Password** to display the password.

9   Type a name for the archive or use the default.

10 Click **Next**.

11 If necessary, adjust the database size or file paths.

12 Select the security group type for the SQL groups.

13   Using the default group types is recommended.

14 Click **Next**. See Configuring purge and archive settings.

To use an existing archive database

1   Select U**se an existing Active Administrator Archive database**.

2   Type the target SQL Server or Azure SQL Managed instance.

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   If using an Azure SQL Managed instance, select **SQL Server Authentication**, enter a SQL user ID that has login privilege for the SQL Managed instance, and enter the password for the SQL account.

7   The characters in the password will be hidden. Each character will be represented by a displayed dot. Select **Show Password** to display the password.

8   Click **Test Connection to validate the archive database**.

9   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*.

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. Set authenticated users full control on the share permissions. If you would like to restrict permissions further, you can change the NTFS permissions.

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.

> **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.

> **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 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, 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 during processing and stores the backup files when the backup is complete under the folder **C:\ActiveAdministrator\ADBackups\DOMAIN_*domainname*** (where *domainname* is the fully qualified name of the domain being backed up). You can specify the folder where the temporary files are processed and where the backup files are stored.

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**. See the *Quest*® Active Administrator® *User Guide*.

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 folder where temporary backup files are processed, if desired.

> *To change the folder where temporary backup files are processed*
>
> a Select the **Override the default temporary folder** check box.
>
> b Browse to locate or create a folder.
>
> c Click **OK**.

5 Change the folder where backup files are stored, if desired.

> **i** | **NOTE:** If there are existing backup files in the existing share, you must move them manually. Only newly created backup files are stored to the new share path.

> *To change the folder where backup files are stored*
>
> a Select the **Override AD Backup share path** check box.
>
> b Browse to locate or create a folder.
>
> c Click **OK**.

6 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.

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 and Enabling SNMP Notifications. Otherwise, see Reviewing selections.

Connecting to System Center Operations Manager and Enabling SNMP Notifications

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 Active Directory Health Analyzer agent to appear in the Operations Manager **Monitoring** pane under the **Quest Active Administrator** folder. You can also enable SNMP alert notifications.

> **¡** | **NOTE:** Only System Center 2016 Operations Manager is 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 and SNMP alert notifications in the Active Administrator console (**Configuration | SCOM and SNMP Settings**). See *Configuring SCOM and SNMP Settings* 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 and SNMP Notification** page.

> **NOTE:** After you complete the configuration wizard, you can edit the **System Center Operations Manager and SNMP Notification** to configure which Active Directory Health Analyzer alerts to push to SCOM and SNMP. See *Pushing alerts to the System Center Operations Manager and SNMP managers* in the *Active Administrator User Guide*.

To connect to Systems Center Operations Manager and enable SNMP notifications

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

> **¡** | **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.

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

4   Click **Test Settings** to test the connection.

5   Select **Send notifications via SNMP**.

6   Enter the IP address of the SNMP notification target computer.

> **¡** | **NOTE:** The SNMP notification target computer must be equipped with SNMP management software capable of TRAP v2 notifications processing.

7   Click **Test Settings** to test the connection.

8   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 [icon] and copy to a text file.

- ▪ To view individual detail, click [icon] to expand the detail.

- ▪ To collapse the detail, click [icon] .

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.

To install Active Administrator console

1 Unzip the Active Administrator folder, browse to the Installation folder, and run the **Active Administrator Console.msi**

2 On the Welcome screen of the Setup Wizard, click **Next**.

3 Click **View License Agreement**.

4 Scroll to the end of the license agreement.

5 Click **I accept these terms**, and click **OK**.

6 Click **Next**.

7 To change the location of the program files, click **Change**, or click **Next** to accept the default installation directory

8 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.

9 Click **Finish**.

The first time the Active Administrator console opens, you are asked to set the Active Administrator Server.

10 Type the name of the server where Active Administrator Server is installed, or browse to locate a server.

11 Click **OK**.

> ¡ | **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 polices 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.

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*.

> *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 run 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 runs when the alert condition is met.

The action is run 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 runs*

> a   Select **Enabled**. To disable an action, clear the check box.

> b   Type the full path to the .EXE file for the program or script or browse to locate the .EXE file.

> > **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 .EXE file 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. Enabling the default port adds these workstation events to the event definitions:

- User Locked Workstation

- User Logoff

- User Logon (interactive)

- User Logon (Remote Desktop)

- User Unlocked Workstation

See also:

- Deploying the workstation logon audit agent

- Enabling the default port

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.

 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).

   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 8.6.3 Workstation Audit Agent.msi** to a share where everyone has access.

3 Start **Active Administrator 8.6.3 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.

Appendix: Active Administrator Server Manager

The Active Administrator Server manager is a tool included with Quest Active Administrator for managing Active Administrator Foundation and Data Services, Active Administrator Notification Services, Active Administrator Licenses, and Active Administrator Security.

Topics

- Starting the Active Administrator Server Manager
- Active Administrator Foundation and Data Services
- Web Server Configuration
- Managing Security

Starting the Active Administrator Server Manager

To start the Active Administrator Server Manager from the Windows Start Menu

1 Click **Windows Start** | **Quest** | **AA Server Manager**.

Active Administrator Foundation and Data Services

This section of the Server Manager contains tools to manage Active Administrator Foundation and Data Services.

See also:

- SQL Full-Text Search

SQL Full-Text Search

Active Administrator audit reports use SQL Full-Text Search to filter event descriptions to help reports run faster. When the SQL Full-Text Search is enabled, the current index status is displayed and clicking on the status will update it.

To enable SQL Full-Text Search

1 Start the Active Administrator Server Manager. For more information, see Starting the Active Administrator Server Manager on page 52.

2 In the Active Administrator Foundation and Data Services section, locate SQL Full-Text Search and click **Enable**.

   The current index status is displayed and clicking on the status will update it.

To disable SQL Full-Text Search

1 Start the Active Administrator Server Manager. For more information, see Starting the Active Administrator Server Manager on page 52.

2 In the Active Administrator Foundation and Data Services section, locate SQL Full-Text Search and click **Disable**.

   The current index status is displayed and clicking on the status will update it.

Web Server Configuration

This section of the Server Manager can be used to configure the Web Server settings. To support Smart Card Authentication, you must enable Windows Authentication and use the Microsoft Edge browser when logging into the Active Administrator Web Console.

To configure the web server

1 Start the Active Administrator Server Manager. For more information, see Starting the Active Administrator Server Manager on page 52.

2 Locate Web server configuration and click **Configure**.

3 Type the server port number.

4 Optionally, **Enable HTTP logging** and set the **Number of logs to keep** in days.

5 Optionally, **Enable session timeouts** and set the **Session timeout** in minutes.

6 Optionally, **Enable Windows Authentication**.

   > **NOTE:** When enabled and using the Microsoft Edge browser, the web login page will prompt for Windows credentials or Smart Card PIN.

7 Optionally, set the **Authentication token expiration time** in minutes.

8 Optionally, set the **Authentication token refresh interval** in minutes.

9 Optionally, **Enable SSL** and set the **Certificate** and **SSL Port** number.

   Optionally, click **View HTTP Binding** to view the HTTP Binding Component.

   Optionally, click **View Certificate** to view the current certificate.

   Optionally, click **Clear Certificate** to remove the current certificate.

10 Click **OK**.

Managing Security

Active Administrator makes use of FIPS 140-2 compliant software to secure information and includes a security management tool in the Active Administrator Server Manager. For more information, see Starting the Active Administrator Server Manager on page 52. The Security Manager allows you to perform the following tasks related to the Active Administrator security.

- Managing the passphrase

- Managing file security

- Managing database security

To start the Security Manager

1 Start the Active Administrator Server Manager. For more information, see Starting the Active Administrator Server Manager on page 52.

2 In the Security Manager section, click **Manage**.

The current security status is displayed.

Topics

- Managing the passphrase

- Managing file security

- Managing database security

- Recovering from a lost passphrase

Managing the passphrase

A passphrase is used to control access to Active Administrator data. A passphrase is similar to a password in usage, but is generally longer for added security. Active Administrator content will be secured using the passphrase and requires the passphrase for accessing the content or for changing the passphrase.

> **!** **CAUTION:** You must know the current passphrase to change or restore the passphrase. It is very important to record the passphrase in a secure location where it can be retrieved when required.
>
> **CAUTION:** If the passphrase is lost, it will be impossible to access Active Administrator data. You will have to uninstall Active Administrator, remove all associated files, and start a new installation of Active Administrator. For more information, see Recovering from a lost passphrase **on page 56**.

To create a passphrase

1 Type a passphrase that is between 25 and 32 characters in length and then type it again to confirm.

2 Record the passphrase in a secure location.

> **!** **CAUTION:** You must know the current passphrase to change or restore the passphrase. It is very important to record the passphrase in a secure location where it can be retrieved when required.

3 Click **OK**.

The registry files and database will be secured using the passphrase.

To change a passphrase

1 In the Passphrase Management section, click **Change**.

2 Type the current passphrase.

3 Type a new passphrase that is between 25 and 32 characters in length and then type it again to confirm.

4 Record the passphrase in a secure location.

> **!** **CAUTION:** You must know the current passphrase to change or restore the passphrase. It is very important to record the passphrase in a secure location where it can be retrieved when required.

5 Click **OK**.

6 Review the informational message.

7 Click **Yes** to proceed.

The registry files and database will be secured using the new passphrase.

8 Review the reminder to create new backups.

9 Click **OK**.

Managing file security

The security of the Active Administrator files can be managed using this option.

To secure files

1 In the Files Security Management section, click **Secure Files**.

2 Type the current passphrase.

3 Click **OK.**

To clean the registry

1 In the Files Security Management section, click **Clean Registry**.

2 Review the informational message.

3 Click **Yes** to proceed.

Managing database security

The security of an Active Administrator database can be managed using this option.

To validate the security of a database

1 In the Database Security Management section, type the server name.

- OR -

Click the ellipsis to browse, select the server, and click **OK**.

2 Type the database name.

- OR -

Click the ellipsis to browse, select the database, and click **OK**.

3 Click **Validate** to verify that the security of the selected database is up to date.

To secure a database

1 In the Database Security Management section, type the server name.

- OR -

Click the ellipsis to browse, select the server, and click **OK**.

2 Type the database name.

- OR -

Click the ellipsis to browser, select the database, and click **OK**.

3 Optionally, click **Validate** to verify that the security of the selected database is up to date.

4 Click **Secure Database**.

5 Type the current passphrase.

6 Click **OK.**

Recovering from a lost passphrase

If the passphrase is lost, it will be impossible to access Active Administrator data. In this situation, the only option is to uninstall Active Administrator, remove all associated files, and start a new installation of Active Administrator.

To recover from a lost passphrase

1   Use the Active Administrator Security Manager to clean the registry. For more information, see Managing file security on page 55.

2   Use the Windows Add or Remove Programs option to uninstall Active Administrator.

3   Remove the contents of the Active Administrator share located at the root on the computer where Active Administrator is installed (**C:\ActiveAdministrator**).

4   Remove the Quest Active Administrator folder. The default location is **C:\Program Files\Quest\Active Administrator**.

5   Follow the steps to install Active Administrator, create a passphrase, and create a new database. For more information, see Installing and configuring Active Administrator on page 34.

About us

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

Technical support resources

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

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

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