Quest® Active Administrator® 8.4

Release Notes

December 2019

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

Topics:

About this release

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

Active Administrator 8.4 is a minor release, with new features and functionality. See New features.

New features

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

Additional Supported Platforms

The following platforms are now supported in Active Administrator.

- Windows Server® 2019
- SQL Server® 2019

License adjustments

The Active Administrator Domain Name System (DNS) module is now included with the base Active Administrator license and the Active Directory Health license instead of being separately licensed.

Active Directory Health enhancements

New Module Names

Some module names have been updated.

- Directory Analyzer has been updated to **Active Directory Health Analyzer**.
- Directory Troubleshooter has been updated to **Active Directory Health Troubleshooter**.

New Event Descriptions

- **Alert on GPO password complexity changes**

  Added two event descriptions — GPO Password Complexity Enabled and GPO Password Complexity Disabled — to use when creating alerts and reports on group policy changes.

New Alerts

- **Collect and alert on orphaned Group Policy Objects (GPOs)**

  Added a General Data Collector named *Orphaned group policy objects exist*. Select **Active Directory Health | Agents | Data Collectors | Domain Controllers | General**.

  Added support for orphaned Group Policy Object alerts. Select **Active Directory Health | Alerts.**

- **Monitor site link settings on domain controllers**

  Added a forest alert — Site link settings inconsistent with PDC — to indicate that some of the site link settings (Description, Assigned sites, Cost, Replication interval and Schedule) on domain controllers in the forest do not match the same settings on the primary domain controller (PDC).

- **Monitor site settings on domain controllers**

  Added a forest alert — Site settings inconsistent with PDC — to indicate that some of the site settings (name, description, cn, displayName, location, managedBy, objectCategory, Subnets, and Servers) on domain controllers in the forest do not match the same settings on the primary domain controller (PDC).

- **Monitor subnet settings on domain controllers**

Added a forest alert — Subnet settings inconsistent with PDC — to indicate that some of the subnet settings (Description, Assigned site, Prefix) on domain controllers in the forest do not match the same settings on the primary domain controller (PDC).

- **Collect and alert on domain controller components**

  Added data collectors — *Hard drive failed*, *Memory degrade,* and *Power supply failed*.

  Added domain controller alerts — *Hard disk drive*, *Physical memory*, and *Power supply* — to indicate when issues have been detected each component on the domain controller.

- **Monitor DFS replication service on domain controllers**

  Added domain controller alert — DFSRS unresponsive — to indicate that the DFS replication service is unresponsive on the domain controller.

New Options

- **Exclude domain controllers from Active Directory Health monitoring**

  A new menu option in the Active Directory Health module now makes it easier to exclude domain controllers from Active Directory Health monitoring. Select **Active Directory Health | Agents** | **Analyzer Agents** tab | **More | Excluded Domain Controllers**.

- **SNMP alert notification support**

  Added support for SNMP alert notification. Select **Active Directory Health | Alerts | Notifications | SNMP Alert Notification**.

- **Add grouping to alerts**

  Added the ability to group alerts from the Current Alerts list by Alert Name, Object Name, or Severity Level.

- **Add alert count**

  Added the total number of alerts to the header of the Alerts page.

- **Filter Active Directory Health Analyzer Agent log**

  Added the option to *Filter Log Entries* to the Analyzer Agent Log display. Select **Active Directory Health | Agents | Analyzer Agents | View Agent Log**.

- **Filter Active Directory Health Analyzer Applications and Updates displays**

  Added the option to *Filter Installed Applications by Name* to the Active Directory Health Analyzer Installed Applications display. Select **Active Directory Health | Analyzer | Monitored Domain Controllers | Applications** tab.

  Added the option to *Filter Installed Windows Updates by Name* to the Active Directory Health Analyzer Updates display. Select **Active Directory Health | Analyzer | Monitored Domain Controllers | Updates** tab.

- **Create and apply data collector templates for each type of Active Directory object**

  Added the option to create templates that hold the data collector settings and alert settings. Templates can be saved and applied for each type of Active Directory object. Select **Active Directory Health | Agents | Settings | Domain Controller, or Domain, or Forest, or Site | Save as Template**.

- **Set notification threshold for alerts that are cleared**

  Added the option to suppress notifications if an alert clears within a set length of time. Select **Active Directory Health | Alerts | Notifications| Add or Edit**.

- **Remove offline Azure Active Directory Connect Health agents**

  Added the option to remove an Azure Active Directory Connect Health agent when it is offline. Select **Active Directory Health | Azure AD Connect | Agents | Remove**.

- **Schedule the date and time to mute alerts for selected objects**

Added the option to schedule when alerts will be muted for selected objects. Select **Active Directory Health | Analyzer | Schedule Mute**. To display a schedule outlining when alerts will be muted for selected objects, select **Active Directory Health | Analyzer | Mute Schedule**.

Web console enhancements

New Options

- **Add new roles for Active Directory Health Check**

  Added following new roles for Active Directory Health Check. Permissions for these roles can be set in the **Configuration | Role Based Access** module.

  - Active Directory Health Check Management - full management control role
  - Active Directory Health Check Viewer - report viewer role that can view, stop, or cancel running health checks

- **Support adding Windows services and Windows Performance counters to Active Administrator Health**

  When viewing the data collectors on a domain controller in Active Administrator Health, you can now add Windows Performance counters or Windows services, depending on the tab selected.

- **Add export to CSV option to Active Directory Health**

  Added the ability to export the performance counter sample values from the trending details dialog into a CSV file stored on the local computer.

- **Add Update ID filter to Installed Updates report parameters**

  Added the ability to filter on Update ID when running the Installed Updates report. Select **Report | Active Directory Health | Installed Updates**.

- **Set notification threshold for alerts that are cleared**

  Added the option to suppress notifications if an alert clears within a set length of time. Select **Monitor | Active Directory Health | Notifications | Add or Edit**.

- **Support selecting multiple domain controllers for Event Log reports**

  Added the option to select more than one domain controller when running Event Log reports. Select **Report | Active Directory Health** and search for *event log*.

  The following reports have been enhanced:

  - Active Directory White Space
  - AD Diagnostic Event Logging Levels
  - AD Disk Space
  - Application Event Log
  - Authentication Methods
  - Connection Object Duplicates
  - Directory Service Event Log
  - DNS Configuration
  - DNS Event Log
  - DNS Zone Information
  - DNS Zones

- Domain Controller Advertising
- Domain Controller Environment Variables List
- Domain Controller Ping
- Domain Controller Process List
- Drivers List
- Event Log
- Event Log Errors
- IP Deny List
- Last Boot Up Time
- LDAP Policies
- Naming Context Topology Aliveness
- Net Logon
- Owner Information
- Replication Failures
- Replication Logon Privileges
- Replication Partner DNS Resolution
- Replication Partners
- Replication Queue Length
- RID Information
- Security Event Log
- System Event Log
- SYSVOL Attach
- Time Synchronization

- **Schedule the date and time to mute alerts for selected objects**

  Added the option to schedule when alerts will be muted for selected objects. Select **Monitor | Active Directory Health | Schedule Mute**. To display a schedule outlining when alerts will be muted for selected objects, select **Monitor | Active Directory Health | Mute Schedule**.

- **Add new threshold to the Active Administrator Domain Controller Response Time Report**

  Added the option to specify a threshold filter. Select **Report | Active Directory Health | Active Administrator Domain Controller Response Time Report**.

New Reports

- **Average DNS Interactions for TCP Report**

  The Average DNS Interactions for TCP Report displays DNS interactions for TCP per second for the selected period. You can choose a date range. Select **Report | Active Directory Health | Average DNS Interactions for TCP Report**.

- **Average DNS Interactions for UDP Report**

  The Average DNS Interactions for UDP Report displays DNS interactions for UDP per second for the selected period. You can choose a date range. Select **Report | Active Directory Health | Average DNS Interactions for UDP Report**.

- **Average Replication Time from PDC Report**

The Average Replication Time from PDC Report displays average replication time from PDC for each domain controller in selected domain(s). You can choose a date range. Select **Report | Active Directory Health | Average Replication Time from PDC Report**.

- **CPU Utilization Report**

  The CPU Utilization Report displays the domain controllers that have the highest CPU utilization in the specified period of time for the selected domain. You can set how many domain controllers to display. Select **Report | Active Directory Health | CPU Utilization Report**.

- **Domain Controller Response Time Report**

  The Domain Controller Response Time Report shows the average LDAP response time in the specified period of time for the selected domain controllers. You can choose a date range. Select **Report | Active Directory Health | Domain Controller Response Time Report**.

- **Domain Controller Service Status Alert Report**

  The Domain Controller Service Status Alert Report displays all the service status alerts that have occurred on the selected domain controllers over the specified period of time. You can choose a date range. Select **Report | Active Directory Health | Domain Controller Service Status Alert Report**.

- **Missing DNS Records Report**

  The Missing DNS Records Report displays all the DNS records that are missing from the DNS server over a selected period of time. Report information is displayed in Coordinated Universal Time (UTC). You can choose a domain, multiple domain controllers and a date range. Select **Report | Active Directory Health | Missing DNS Records Report**.

- **SMB Connections Report**

  The SMB Connections Report displays the Top N domain controllers that have the most SMB connections in the specified period of time. Report information is displayed in Coordinated Universal Time (UTC). Select **Report | Active Directory Health | SMB Connections Report**.

- **Time Synchronization - Top N DCs with Greatest Time Difference Report**

  The Time Synchronization - Top N DCs with Greatest Time Difference Report displays the top domain controllers with the greatest time difference with their W32Time Parent. Select **Report | Active Directory Health | Time Synchronization - Top N DCs with Greatest Time Difference Report**.

Other enhancements

Installation

Increased passphrase strength requirements

When upgrading from Active Administrator 8.2 or 8.3 to Active Administrator 8.4, or when installing Active Administrator 8.4 for the first time, the passphrase required for data encryption must be between 25 and 32 characters in length. The current passphrase can be changed using the previous passphrase value.

IMPORTANT: Active Administrator content may only be decrypted using this passphrase. It is very important to record the passphrase in a secure location where it can be retrieved when required.

NOTE: During upgrades and passphrase changes, larger amounts of data will take longer to re-encrypt.

Adding Active Administrator Application to Microsoft Azure

The process for adding the Active Administrator Application to the Microsoft Azure portal has been updated. Go to https://portal.azure.com, select **Azure Active Directory**. For more information, see Adding the Active Administrator App section in the Active Administrator User Guide.

Active Directory Infrastructure

Exclude specified domain controllers by name

Added the option to enter a computer name to add to the list of domain controllers excluded from Active Directory Replication Monitoring. Select **Active Directory Infrastructure | Replication Monitoring**.

Certificates

Read-only access

Added the Certificate Management Viewer role for read-only access to the Certificates module. If selected, the user can browse the Certificates module, and search and report on certificates, but not add, update, or delete certificates. The Certificate Management role must be disabled to limit the user to read-only access.

Select and delete multiple certificates

Added the ability to select and delete multiple certificates in the **Certificates | Certificate Management** console.

Configuration

Configurable e-mail notifications for certificate error messages

Added configurable e-mail notifications for certificate error messages to make it easier to know when a service is running or not. Select C**ertificates | Certificate Authority | Notifications options**.

You may opt to receive notifications when the following services are Up or Down:

- Server status
- NT Authentication Certificates
- Authority Information Access (AIA)
- Recovery Agent (KRA)
- Certificate Authority (CA)
- CRL Distribution Point (CDP)
- Enrollment

The frequency that certificate authority service states are checked can be configured using the **Configuration | Certificate Configuration | Certificate Authority** settings.

Configurable SNMP Notification Settings

You can enable and configure SNMP notifications for a target machine equipped with SNMP management software capable of processing TRAP v2 notifications. Select **Configuration | SCOM and SNMP Settings**.

Recovery

Select multiple objects to restore

When selecting Active Directory objects to recover, there is now an option to Select All objects, Clear All objects, or select multiple objects. Select **Recovery | Object Recovery**.

Security and Delegation

Manager notifications for password reminders

A manager notification is sent when a user receives a password reminder. The wording of the notification message and the subject line can be customized. Select **Security & Delegation | Password Reminder**.

New customization options for password reminders

The password reminders have some new and some improved customization options. Select **Security & Delegation | Password Reminder**.

- The greeting is separately configurable and defaults to %FIRSTNAME% %LASTNAME% or %LASTNAME% %FIRSTNAME% depending on the user's configuration.
- The user Info section is separately configurable.
- The manager Info section is separately configurable.
- Variables are supported in both the subject line and the body.
- The %USERNAME% variable is now supported for the user Info section.
- The Preview Message option displays a preview of the generated message that will be sent to the user.

See also:

- Resolved issues

Resolved issues

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

Table 1. Resolved issues

Resolved issue	Issue ID
Inactive Accounts: An error occurred while processing domain "". Index was out of range.	15358
Alert cleared notification incorrectly sent when an AD Health alert moves from pending to cleared state.	23051
Null reference error in scheduled security reports.	87155
Updated audit agent security.	107482
The Diagnostic Console does not open when clicking **Diagnose** after installing the upgrade to Active Administrator® 8.3.	108220
Issues with agents communicating with the server due to the DAAgent.xml file.	120168

Table 1. Resolved issues

Resolved issue	Issue ID
Azure® Active Directory® Connect error occurs when referencing the Get-ADSyncScheduler cmdlet with some Azure® Active Directory® Connect versions.	120877
ADS memory usage keeps growing.	122732
Active Directory® object backups made prior to Update 3 which exceed 2GB in size cannot be restored.	123259
Unable to push out Directory Analyzer agent to trusted forest. Receiving an error that, “No site information was provided.”	127319
Performance improvement for loading domain controller site information.	128049
Restore issue: Unable to find or browse to a number of Active Directory® user accounts	129880
Unable to restore deleted user.	153727
DNS alert incorrect.	154313
Reports fail for more than 20 days and FISMO roles are incorrectly shown.	154386
Workstation logon agent - only some machines are reporting logon events.	167302
Error occurred while attempting to load the Directory Analyzer tree.	175260
Active Directory Health Ineffective GPO’s report error - Disabled GPO links incorrect.	178156

System requirements

The system requirements are the same for all components of Quest® Active Administrator®. Before installing or upgrading Active Administrator® 8.4, ensure that your system meets the following minimum hardware and software requirements.

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

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

Server hardware requirements

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

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

Topics:

- Server hardware requirements
- Server software requirements
- SQL Server requirements

The following table outlines the server hardware requirements.

Table 2. Server hardware requirements

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

Server software requirements

The following table outlines the server software requirements.

Table 3. Server software requirements

Requirement	Details
.NET Framework v. 4.5.2 and 4.6	Install either the Full or Standalone version. Do not install just the Client Profile.
Group Policy Management Console (GPMC)	GPMC is included with Windows Server® 2008 R2 and later, but is not installed with the operating system. Use Server Manager to install GPMC. After installation, enable GPMC through the Server Manager **Add Features** Wizard. You can launch the Add Features Wizard through **Control Panel | Programs and Features | Turn Windows features on or off**. Alternatively, from the command line, use `ServerManagerCmd -install GPMC`.

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

SQL Server requirements

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

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

- SQL Server 2012
- SQL Server 2012 Express
- SQL Server 2014
- SQL Server 2014 Express
- SQL Server 2016
- SQL Server 2017
- SQL Server 2019

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

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

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

Console requirements

Topics:

Console hardware requirements

The following table outlines the console hardware requirements.

Table 4. Console hardware requirements

Requirement	Details
Processor	1 GHz
Memory	256 MB

Table 4. Console hardware requirements

Requirement	Details
Hard disk space	100 MB
Operating system	• Windows 8.1 • Windows 10 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 **NOTE:** Active AdministratorActive Administrator® does not support Microsoft® Nano Server 2016. **NOTE:** If you are using the Certificate module, see Table 5 for information on support for SHA-2 certificates.

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

Table 5. Support for SHA-2 certificates

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

Console software requirements

The following software is required for the Active Administrator console.

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

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

Table 6. GPMC and DNS Server Tools install information

Operating System	Download Links and Install Information
Windows 8.1 Windows 10	GPMC and DNS Server 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 GPMC and DNS Server 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, and select DNS Server Tools.
Windows Server 2012 Windows Server 2012 R2 Windows Server 2016 Windows Server 2019	***To active GMPC*** • The Group Policy Management Console, once installed, must be enabled through the Add Features Wizard in Server Manager. Alternatively, from the command line, use **ServerManagerCmd –install GPMC**. ***To install DNS Server Tools*** 1 Open the **Server Manager**. 2 Select **Manage | Add Features**. 3 Expand **Remote Server Administration Tools**. 4 Expand **Role Administration Tools**. 5 Select **DNS Server Tools**. 6 Advance through the wizard to **Confirmation**. 7 Click **Install**.

Audit agents requirements

The following table outlines the audit agents hardware requirements.

Table 7. Audit agents hardware requirements

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

Workstation logon audit agents requirements

The following table outlines the workstation logon audit agents requirements.

Table 8. Workstation logon audit agent hardware requirements

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

Web Console requirements

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

- Microsoft® Internet Explorer 11
- Microsoft Edge™ 42
- Google Chrome™ 77
- Mozilla® Firefox® 70

System Center requirements

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

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

Port requirements

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

Active Administrator Console

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

- TCP 8080 for communication with Active Administrator Web Server through the Web Console (internal, http)
- TCP 9443 for communication with Active Administrator Web Server through the Web Console (external, https)
- TCP 80 and 443 for communication via the Internet with Azure® Active Directory®
- TCP 389 for communication with Active Directory on domain controllers

Active Administrator Server

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

Active Administrator database server

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

Domain controller with no installed agents

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

Domain controller with auditing agent

- TCP 1433 for communication with SQL Server

Domain controller with Active Directory Health Analyzer agent

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

Domain controller with Azure Active Directory Connect agent

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

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

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

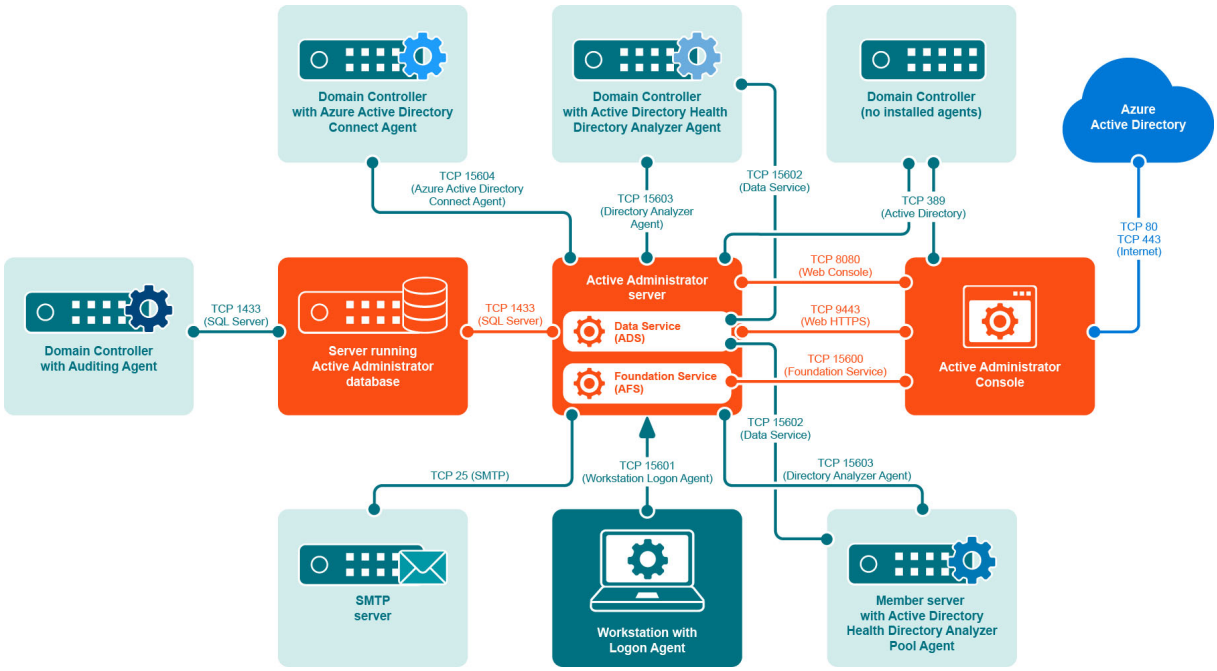
SMTP server

- TCP 25 for sending email notifications via SMTP

Workstation with logon agent

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

Figure 1. Port requirements example



Additional requirements

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

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

User privilege requirements

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

Password recovery

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

Services

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

When choosing an account, keep these requirements in mind:

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

  To set up a non-domain admin user account

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

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

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

Audit database

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

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

Active Administrator module requirements

For all Active Administrator® modules to operate properly, the Active Administrator Foundation service (AFS) requires an account that is a member of the Domain Admins group. However, you may want to customize access to each module for console users or the AFS account. See the *Quest® Active Administrator® 8.4 Install Guide* for the specific permissions required for operation of each module and submodule.

Upgrade and compatibility

Note the following when upgrading Active Administrator.

- Active Administrator® 8.4 only supports in-place upgrades from Active Administrator versions 8.2 or 8.3. Upgrades from previous editions are not supported. To perform an in-place upgrade to Active Administrator 8.4 from a version of Active Administrator that is earlier than 8.2, you must first upgrade to Active Administrator 8.2.
- Installing Active Administrator 8.4 onto an existing Active Administrator 8.2 or 8.3 installation will result in the removal of the earlier version. Active Administrator 8.2 or 8.3 databases, both live and archive databases, will be upgraded automatically to version 8.4.
- A database upgraded by Active Administrator 8.4 cannot be used by previous versions and the database upgrade cannot be rolled back.
- Data within the Active Administrator share can be used by Active Administrator 8.4.
- If you use group policy to deploy the Workstation Logon Auditing Agents (WLAA), the 8.4 installation process will not update the agent on the user workstations. You must replace the install package at the software distribution share with the 8.4 version. Computers will upgrade to the Active Administrator 8.4 WLAA the next time they are started.
- The Azure® Active Directory®, Certificate Management, and Active Directory Health features available in Active Administrator 8.4 each require a separate license. If you do not have a license file to apply, the module does not appear in Active Administrator. You will see the Azure Active Directory and Certificate Management features listed under the Configuration module, but when you select the feature, a warning displays that a license is required.

Product licensing

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

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

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

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

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

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

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

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

To update your license

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

Upgrade and installation instructions

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

Topics:

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

Backing up your data

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

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

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

Installing Active Administrator server

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

To install Active Administrator® server

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

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

Configuring the server

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

To run the AA Configuration Wizard

1. If you are installing Active Administrator, the configuration wizard opens automatically. Otherwise, open the **AA Configuration Wizard** from the **Start** menu.
2. On the Welcome page, click **Next**.
   - The first time you start the configuration wizard, you must apply a valid license file.
     a. Select the licenses to update, and click **Update License**.
     b. Locate the license file, and click **OK**.
3. Type the passphrase (8 character minimum), and then type it again to confirm.

   IMPORTANT: It is impossible to change or restore the passphrase. It is very important that you store the passphrase in a secure location.

4. Click **Next**.
5. If you are upgrading Active Administrator, you are asked if you want to upgrade your existing live database and all archive databases. If you select **Yes**, proceed to step 11. If you select **No**, continue to the next step.

   NOTE: The upgrade process may take longer than normal due to the re-encryption of existing data. Active Administrator uses Advanced Encryption Standard (AES) to allow for better data security.

6. Select **Use an existing Active Administrator database**.
7. Accept the displayed server and database or select a different server and database.
8. Click **Next**.
9. Select **Use an existing Active Administrator Archive database**.
10. Accept the displayed server and database or select a different server and database.
11. Click **Next**.
12. Select the purge and archive options to enable or disable.
13. Click **Next**.
14. Select the path to the Active Administrator share.
15. Click **Next**.
16. Accept the SMTP server setup or make any necessary changes.
17. Click **Next**.
18. Type a valid email address or accept the default.
19. Click **Next**.
20. Accept the active template settings or name any necessary changes.
21. Click **Next**.
22. Accept the group policy history settings or make any necessary changes.
23. Click **Next**.
24. Accept the Active Directory backup settings or make any necessary changes.
25. Click **Next**.
26. To add additional users, click **Add**, find and select users, click **OK**.

27 Click **Next**.

28 Type the account password for the Active Administrator Foundation Service account.

29 The default service port number is 15600. To change the port number, type a value.

30 To use the same account for the notification service, select the check box. Otherwise, type or browse for an account with Domain Admin rights, and type the password.

31 Click **Next**.

32 Click **Finish**.

33 Click **Finish**.

Installing Active Administrator console

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

IMPORTANT: Active Administrator includes the Diagnostic Console, which is also a feature in Spotlight® for Active Directory®. If you are currently using Spotlight for Active Directory, you must install the Active Administrator Console on a computer that does not have the Spotlight for Active Directory Console installed.

To install Active Administrator console

1 Launch the autorun.

2 On the Home page, click **Install**.

3 Click **Install** next to Active Administrator Console.

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

5 Click **View License Agreement**.

6 Scroll to the end of the license agreement.

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

8 Click **Next**.

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

10 Click **Install**.

11 By default, the option to start the Active Administrator Console is selected. If you do not want to start the console, clear the check box.

12 Click **Finish**.

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

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

14 Click **OK**.

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

Updating audit agents

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

To update audit agents

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

   –OR-

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

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

Switching to Active Directory Health

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

To switch gradually

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

To switch right away

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

More resources

Additional information is available from the following:

- Online product documentation (https://support.quest.com/active-administrator/8.4/release-notes-guides)
- The Active Administrator Community (https://www.quest.com/community/products/active-administrator)

Globalization

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

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

About us

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

Technical support resources

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

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

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

Third-party contributions

This product contains the following third-party components. For third-party license information, go to https://www.quest.com/legal/license-agreements.aspx. Source code for components marked with an asterisk (*) is available at https://opensource.quest.com.

Table 9. Third-party contributions

Component	License or acknowledgment
Angular.js 1.4.8	Copyright (c) 2010-2016 Google, Inc. http://angularjs.org
AngularJS Route 1.4.9	Copyright (c) 2010-2016 Google, Inc. http://angularjs.org
Blowfish 2	Copyright (c) 1999-2002 David Barton
Bootstrap 3.3.6	Copyright (c) 2011-2016 Twitter, Inc.
DevExpress WPF Subscription 16.2	jQuery JavaScript Library (Open Source - MIT License) Copyright Query Foundation and other contributors http://jquery.com/ jQueryUI JavaScript Library (Open Source - MIT License) Copyright jQuery Foundation and other contributors http://jqueryui.com/ Knockout JavaScript Library (Open Source - MIT License) Copyright Knockoutjs.com http://knockoutjs.com/ http://opensource.org/licenses/mit-license.php Globalize JavaScript Library (Open Source - MIT License) Copyright Software Freedom Conservancy, Inc. http://jquery.org/license Ace (Ajax.org Cloud9 Editor) (Open Source - BSD License) Copyright 2010, Ajax.org B.V. https://github.com/ajaxorg/ace/blob/master/LICENSE JS Beautifier (Open Source - MIT License) Copyright 2007-2013 Einar Lielmanis and contributors https://github.com/beautify-web/js-beautify/blob/master/LICENSE CodeMirror (Open Source - MIT License) Copyright 2015 Marijn Haverbeke https://codemirror.net/LICENSE
JQuery 1.9.1	Copyright 2016 The jQuery Foundation.
Json.NET 6.0.3	Copyright (c) 2007 James Newton-King

Table 9. Third-party contributions

Component	License or acknowledgment
Owin 1.0.0	Copyright 2012 OWIN contributors Apache License Version 2.0, January 2004 http://www.apache.org/licenses/ TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION 1. Definitions. "License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document. "Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License. "Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity. "You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License. "Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files. "Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types. "Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below). "Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

Table 9. Third-party contributions

Component	License or acknowledgment
Owin 1.0.0 (continued)	"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution." "Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work. 2. Grant of Copyright License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form. 3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed. 4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions: (a) You must give any other recipients of the Work or Derivative Works a copy of this License; and (b) You must cause any modified files to carry prominent notices stating that You changed the files; and (c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

Table 9. Third-party contributions

Component	License or acknowledgment
Owin 1.0.0 (continued)	(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License. You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License. 5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions. 6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file. 7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License. 8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

Table 9. Third-party contributions

Component	License or acknowledgment
Owin 1.0.0 (continued)	9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.
Toastr 2.1.2	Copyright © 2012-2015
Windows Installer XML Toolset (aka WIX) 3.11*	Copyright (c) .NET Foundation and contributors.

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

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

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

Patents

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

Trademarks

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

Legend

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

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

Active Administrator Release Notes
Updated - December 2019
Software Version - 8.4