Quest® Active Administrator® 8.2

Release Notes

November 2017

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 8.2 is a minor release, with new features and functionality. See New features and Enhancements.

New features

New features in Active Administrator® 8.2:

- **Exclude domain controllers from replication monitoring and analysis** - When you add or edit a forest in **Replication Monitoring**, you now have the opportunity to select domain controllers to exclude.

  When you start a test in the **Replication Analyzer**, you can exclude domain controllers from the test. By default, all domain controllers are included. To exclude a domain controller, clear the check box.

- **Exclude organizational units and accounts when checking for inactive accounts** - In a selected domain, you can choose to exclude selected organizational units or to exclude selected users and groups. You also can choose to specify a condition to select user and computer accounts to exclude (**Security & Delegation | Inactive Accounts | Exclusion**).
- **Create temporary group memberships** - When managing group memberships, you can now set the Time-to-Live (TTL) value for selected group members. You can set the TTL value in the **Security & Delegation | Security** submodule when modifying user properties, when viewing group members, and when adding an account to a group. A new Groups with Temporary Members report lists the groups with members that have a set TTL value.

  > **NOTE:** To set the TTL value, the Forest functional level must be Windows Server® 2016 and the Privileged Access Management Feature must be enabled for the forest.

- **Select account to install and manage audit agents** - When installing the audit agent and the Directory Analyzer agent, you now have the opportunity to select the account to use for installation. Also, when performing actions, such as Remove, Start, Stop, Restart, Move, Set Startup Account, and Set Port Number, you can select the account to use to perform those actions. You can choose the Active Administrator Foundation Service (AFS) account or a specified user account. The selected account must be a full Administrator on the target server.

  The specified user name is stored in the configuration file and used as the default until another user name is selected. The account password is saved until you exit Active Administrator.
- **Customize the list of users** - In **Security & Delegation | Security | View | All Users**, you can now create a filter to display only those users who meet the selected criteria. Click **Filter**, select the criteria, and click **OK**. The applied filter affects the users list display, the report list, and the export file.

  You also can select the columns to display or export. Click **Columns**, clear the check boxes of the columns to exclude, and click **OK**.
- **Schedule reports on Active Directory objects by type** - You can now not only generate reports for all Active Directory® objects of a specific type within a container and its subcontainers (**Security & Delegation | View | All Users, All Groups, All Organizational Units, All Computers | Report List**); you also can schedule a report to send through email or to save to a file (**Security & Delegation | View | All Users, All Groups, All Organizational Units, All Computers | Schedule**).
- **Manage password expiration reminders** - If enabled, the Password Change Reminder service runs daily at the time you specify. If the service finds accounts about to expire, notifications are sent. The list of accounts with passwords about to expire (administrator password summary notification) is sent daily to the email addresses you specify, but you now can schedule the notifications sent to users when their passwords are about to expire. You can set up to three levels of password reminders. For example, you could set up the first reminder at 14 days, the second at 7 days, and the final notification at 3 days before the password expires. You can then choose to repeat the final notification daily until the user changes their password. Select **Security & Delegation | Password Reminder** and set up the schedule.

  To help manage the email password reminder notifications, in addition to the custom schedule, you can create a custom email list of select user accounts. When previewing the list of user accounts about to expire, you can select only the accounts you want to receive the email password reminder notification. You can send a notification on demand, or let your custom schedule handle the delivery.

  Daily, the email addresses you specify receive the administrator summary notification, which is a list of users with passwords about to expire. You now can sort the results by User Name, Expiration Date, Domain, or nested by Domain/Expiration Date/User Name or Domain/User Name/Expiration Date. You also can choose to exclude accounts with expired passwords in the notification. The administrator summary notification indicates if the user was notified.
- **Send password notifications for fine-grained password policies** - If you are using fine-grained password policies, you can now run expiration reports and send email notifications. Select **Security & Delegation | Password Policies | Preview | Preview**. When previewing the list of user accounts about to expire, you can select only the accounts you want to receive the email password reminder notification. Click **Send Notification** to send a notification on demand. You also can export the list of user accounts to send in an email, save to a file, or print.
- **View expiring and expired accounts** - You can now look at a list of expiring and expired accounts in a domain. Select **Security & Delegation | Account Expiration**. You can look at live data or the Active

Administrator database. The **Pending** column indicates **True** if the account is about to expire. If the **Pending** column is **False**, the account has expired. The **Notification dates** column indicates when the account was discovered and the notification was sent. The **Expires On** column displays the date and time when the account will expire.

The **Security & Delegation | Purge Account History** feature now includes expired accounts in addition to the inactive user and computer accounts.

- **Encrypt the SQL Server connection** - When creating and editing the Active Administrator® and Active Administrator Archive databases, you now can choose to encrypt the connection with the computer running SQL Server®. You also can choose to trust the server certificate. If the **Trust Server Certificate** check box is not selected, Active Administrator will walk the validation chain until it finds a valid authority.

  This feature is available in the installation wizard, in the AA configuration wizard, and though the console (**Configuration | Archive Databases**).

New features in Active Directory Health:

- **Monitor Directory Analyzer agent performance** - You can monitor the memory and CPU usage of Directory Analyzer agents. In addition, performance monitoring displays properties about the selected agent to help you maintain agent health. First, set up the thresholds for memory and CPU usage and indicate how long to keep performance history (**Active Directory Health | Agents | Analyzer Agents | More | Agent Performance Settings**). Next, select an agent and look for instances when the agent exceeded the thresholds you set for memory and CPU usage (**Active Directory Health | Agents | Analyzer Agents | More | Agent Performance**). In addition, use the details and the agent log to help you monitor the health of the agent. For example, you can quickly see how many domain controllers the agent is monitoring and if there are any active alerts.
- **Connect to System Center Operations Manager** - If you have a license for the Active Directory Health module and are using Microsoft® System Center Operations Manager (SCOM), you can choose to deploy the Quest® Active Administrator® management pack, which establishes a connection to SCOM and enables Active Directory Health alerts from the Directory Analyzer agent to appear in the Operations Manager **Monitoring** pane under the Quest Active Administrator folder.

  You can install or remove the management pack using the AA Configuration Wizard.

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

New features in Certificate Management:

- **Certificate Protection** - On a specified interval, the new Certificate Protection feature validates that the certificate details stored by Active Administrator match the details of the certificates installed on the computer. When this feature is enabled (**Configuration | Certificate configuration**), any differences found are reported as broken certificates and email notifications are sent to the recipients on the certificate email list.

  Broken certificate notifications display in a pane at the bottom of the Certificate Management window (**Certificate | Certificate Management)**. You can attempt to repair the broken certificate or override the broken certificate notification, which replaces the certificate details stored in Active Administrator with the details of the broken certificate. An email notification is sent to a list of recipients when a broken certificate is repaired, fails repair, or is accepted. To see the history of repairs and accepts, select **More | Broken Certificate History**.
- **Monitor organizational units for certificate management** - When adding computers in the Certificate Management window, you can now select organizational units (OUs) to help you add computers for certificate management (**Certificate | Certificate Management | Computers | Add**). When selecting OUs, you can also add those OUs to the list of monitored OUs, which enables Active Administrator to automatically add newly discovered computers for certificate management. If enabled, Active Administrator can also automatically remove a computer from certificate management if that computer is removed from the OU.

  Once an organizational unit is being monitored by Active Administrator, you can further manage that OU by choosing to enable/disable monitoring, to include/exclude nested OUs, to enable/disable automatic removal of computers, or to change the credentials used to monitor OUs (**Certificate | Certificate Management** | **More | Monitored Organizational Units | Edit**).

- **Search for certificates** - The Certificate Search feature enables you to search for certificates based on a variety of search criteria (**Certificates | Certificate Search**). Search by name, subject, issued to and by, effective date, expiration date, expired, key usage, revoked, serial number, thumbprint, store, and signature algorithm. You can create multiple search definitions that search for certificates on managed computers, in certificate stores on selected computers, and in the Certificate Repository. From the search results, you can install, export, or add to the repository.
- **Exclude selected certificate stores** - Now when adding a computer, you can choose to exclude selected stores (**Certificate | Certificate Management | Computers | Add**). You also can manage excluded stores when managing the list of managed computers (**Certificate | Certificate Management | Computers | Stores**).
- **Add computers from OUs when managing certificates** - When adding computers to Certificate Management, you now can choose to add computers from selected organizational units (OUs). Select **Certificate | Certificate Management** | **Computers** | **Add**, and choose between adding computers individually and adding computers from OUs to populate the list of available computers. You can choose multiple OUs and include nested OUs as well.
- **Schedule certificate reports** - In the Certificate Management module, you can now schedule certificate reports to be sent daily, weekly, or monthly. In the Certificate Management Report wizard (**Certificate Management | More | Report**), you can set the schedule when setting up delivery options. Once created, you can view and manage all the schedules by selecting **Certificate Management | More | Report schedules**. You can edit existing schedules, disable or enable schedules as needed, and delete schedules.
- **Manage certificate expiration reminders** - If enabled, certificates are checked daily at the time you specify. If Active Administrator finds certificates about to expire, notifications are sent to the email addresses you specify, but you now can select to send notifications to users on a specified schedule. You can set up to three levels of notifications. For example, you could set up the first reminder at 14 days, the second at 7 days, and the final notification at 3 days before the certificate expires. You can then choose to repeat the final notification daily until the user updates the certificate. Select **Configuration | Certificate configuration**, and set up the schedule.
- **Expanded notification of certificates using cryptographic hash algorithms** - The email notification feature for certificates using cryptographic hash algorithms is expanded to include SHA1RSA, SHA2RSA, SHA224RSA, SHA256RSA, SHA384RSA, SHA512RSA, SHA512DSA, MD2RSA, MD3RSA, MD4RSA, MD5RSA, AND MD6RSA, in signatures, PFX files, and in the certificate repository (**Configuration | Certificate Configuration** | **General** tab).

  If the notification feature is enabled, you can still exclude a selected certificate from the email notification (**Certificates | Certificate Management | More | Notifications | Exclude from notification** or **Certificates | Certificate Repository | Edit Certificate** | **Exclude from notification**).
- **Add a certificate to the repository from a URL** - When adding a certificate to the repository, you can now choose to download a certificate from a URL (**Certificate | Certificate Repository** | **Add Certificate | Add Certificate from URL**). In addition to providing the URL, you need to include the port number of the resource where the certificate is located and authentication if the resource requires it.
- **Manage Certificate Authority certificates and servers** - With the Certificate Authority feature, you can manage the Certificate Authority (CA) servers, the Active Directory Certificate Service (certsvc), and CA certificates within a selected forest. Quickly see the status of the certsvc, and associated Active Directory objects. Back up CA servers, view processing events, view certificate templates, and search for CA certificates and templates. Select **Certificate | Certificate Authority**, and add your forests. Use the tabs to view details about the CA certificates and servers.

New features in Active Administrator Web Console

- **Automatic Directory Analyzer agent deployment** - Automatic deployment of the Directory Analyzer is available only for domain controllers that were not discovered when you ran the wizard to install the Directory Analyzer agent. Once you run the wizard, any new domain controllers that are brought online can be deployed automatically into the agent pool or the Directory Analyzer agent can be installed automatically onto that domain controller. By default, only a list of the new domain controllers are sent to a specified email list. You can specify a delay between discovery and deployment, and exclude specific domains from the process. Finally, you can view and manage pending deployments. You can cancel a pending deployment or initiate the deployment immediately. Select **Active Directory Health | Agents** | **Analyzer Agents** | **More | Automatic Agent Deployment**.

- **Schedule Active Directory Health Checks** - In previous versions of Active Administrator, you could choose to run a health check now or at a later date and time. You now can choose to repeat the health check on specified days at a specified time. For example, you could schedule the health check to run every Sunday at 1 AM.
- **View domain controller details** - When using the Topology Viewer, you can now select a domain controller and view details (**Monitor | Active Directory Topology | Run | Info)**. Details include general information about the domain controller, operating system details, memory size and available space, disk size and available space, network adapters, and alerts.
- **New Web Console reports** - The following tables list the new Active Directory Heath, security, and certificates reports. In addition, there is a new Server Configuration report that displays information about the Active Administrator configuration settings. Information includes server names, port numbers, and database names.

Table 1. New Web Console Active Directory Health reports

Report	Description
Domain Controller Ping	Pings the specified domain controller and displays the ping times. Times that are less than 10 milliseconds are shown as **< 10 milliseconds**. **Minimum required permission:** Domain User rights.
Domain Controller Processes List	Displays the list of processes on a domain controller. The results include the following properties for each process: Process Name, Process ID, Handle Count, Page File Bytes, Page File Bytes Peak, Pool Paged Bytes, Pool Nonpaged Bytes and Thread Count. **Minimum required permission:** WMI rights.
Domain Controller Processors List	Displays all of the processors on a domain controller. **Minimum required permission:** WMI rights.
Domain Security	Displays the following security information for the specified domain: • Indicates if the Authenticated Users group has Read access to the AdminSDHolder object. • Indicates if the Guest account is disabled • Lists Administrator and Guest account names and description status • Lists users from other domains/forests that are members of the Administrators group. • Lists external trusts and indicated if these trusts are quarantined. • Lists Administrator membership • Lists Administrator Groups members **Minimum required permission:** Domain user rights.
Environment Variables	Displays all the environment settings, including both system and individual user settings, on a domain controller. The results include the following details: Variable Name, User Name, System Variable (true/false), and Variable Value. **Minimum required permission:** Domain user rights and WMI rights.
Group Membership Consistency	Checks the group membership consistency between two or more domain controllers in a domain. **Minimum required permission:** Domain user rights.

Table 1. New Web Console Active Directory Health reports

Report	Description
IP Deny List	Displays the list of IP addresses in the IP Deny List (Configuration/services/ windows nt/Directory Service/Query-Policies/Default QueryPolicy/ldapdenylist/ IDAPIPDenyList) for the specified server. **Minimum required permission:** Domain user rights.
Last Boot Up Time	Displays the last time a domain controller was booted and how long the domain controller has been running. **Minimum required permission:** WMI rights.
LDAP Policies	Displays the Lightweight Directory Access Protocol (LDAP) protocol policies of the specified domain controller. The results display the attributes and values for LDAP Administration limits and lists LDAP Admin limits that could not be found. **Minimum required permission:** Domain user rights.
NetLogon	Verifies that NetLogon is running on the specified domain controller and retrieves information about the NetLogon service on the specified domain controller using WMI. **Minimum required permission:** WMI and Registry Read rights.
SYSVOL Attach	Tests attaching to the SYSVOL of the specified domain controller. Results show the path for which the attempt was made, as well as the actual path after connecting. **Minimum required permission:** WMI rights.
Time Synchronization - Domain Controllers with Time Difference greater than threshold	Displays the domain controllers that have time differences greater than the specified threshold. Report information is displayed in Coordinated Universal Time (UTC). **Minimum required permission:** Domain User and WMI rights.
Tombstoned Items	Enumerates tombstoned items, which are objects that have been marked for deletion by Active Directory, but whose tombstone lifetime has not expired. Tombstone lifetime is the number of days before a deleted item is removed from Active Directory (default is 60 days). **Minimum required permission:** Domain user rights.
User Consistency	Checks the consistency of user objects between two or more domain controllers in a domain. Verifies that each user object exists and that its group member list and other attributes are the same on each domain controller. **Minimum required permission:** Domain user rights.

Table 2. New Web Console security report

Report	Description
Active Templates Delegation Details	Lists the delegated permissions provided by the active templates for the selected object and the current delegation status of each permission.
Active Template Delegations	Lists the active templates for the selected object and the delegation status of each active template.
Inactive Accounts Report	Lists all inactive user or computer accounts in the specified database and domain.

Table 3. New Web Console certificates reports

Report	Description
Certificate Management Report	Displays information about the certificates installed on monitored computers. You can customize the report to show only certificates of interest. Select the computers, specify the status of certificates, and then select the certificates.
Certificate Repository Report	Displays information about the certificates added to the repository. You can customize the report to show only certificates of interest. Select the computers, specify the status of certificates, and then select the certificates.

See also:

- Enhancements
- Resolved issues

Enhancements

The following is a list of enhancements implemented in Active Administrator® 8.2.

Table 4. General enhancements

Enhancement	Issue ID
Added event definitions for 627 **Change Password Attempt** and 4723 A**n attempt was made to change an account's password**.	4401
Added the ability to open the Web Console from the Active Administrator Console.	4612
Added the OU column to the User account(s) set to expire notification summary to indicate where the user account resides.	4617
When creating or editing an alert, you can now specify a time delay before the alert action initiates (**Auditing & Alerting | Alerts | New |** Alert Action page or **Auditing & Alerting | Alerts | Edit | Action**).	4730
Added a column for account expiration dates when viewing, exporting, or reporting on all users in the selected domain (**Security & Delegation | Security | View | All Users**).	4868
Added ability to exclude accounts with expired passwords from the administrator password summary notification (**Security & Delegation | Password Reminder**).	5192
Added the ability to choose how to display the name in the email message for password reminders (**Security & Delegation | Password Reminder | Message**).	5228
Added new event definitions to enable auditing when the Active Administrator Foundation Server (AFS) service is started or stopped.	5261
Added the ability to move inactive user and computer accounts to any sub-OU in Active Directory.	5266
Added the ability to modify the date and time formats in audit reports (**Settings | User Options | Audit Reports**).	9025
Tool tips were added to certificate management and the certificate repository to display a description of the state of the certificate when the cursor is hovered over the state icon.	9069
Updated the Azure Active Directory chapter in the user guide and help with instructions for setting up the new Azure portal to work with Active Administrator.	11188
Added the ability to install updates using UpdateAAcmd.exe.	11635
Added the ability to create a schedule that backs up all the GPOs in specified domains (**Group Policy | Schedule**).	14298

Table 5. Active Directory Health enhancements

Enhancement	Issue ID
Failed tests now display at the top of all Active Directory Health Check reports.	5814
Added a new process to the Active Directory Health Remediation Library that clears the Conflict And Deleted folder in the SYSVOL directory	6308
Added the ability to view information on a domain controller selected in the Topology Viewer in the web-based Active Directory Health module. Details include general information about the domain controller, operating system details, memory size and available space, disk size and available space, network adapters, and alerts.	7420

Resolved issues

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

Table 6. General resolved issues

Resolved issue	Issue ID
Password notifications with Fine Grained Password Policies are not working as expected after upgrading to 8.1.	7635
Saving Password Reminder settings from a remote console cause a critical error.	7849
The audit agent sometime fails on domain controllers that are running Windows Server® 2016.	9358
Unable to restore backed up GPOs due to a space in the AFS account user name (aa admin).	9400
An error occurred when attempting to obtain unmonitored domain controllers.	10023
An error occurred while attempting to get the unmonitored domain controllers from remote computers.	10023
Unable to get a report on Active Directory for All Users or All Computers.	10216
Custom report filters were not working.	10919
High CPU utilization occurs when selecting monitored domain controllers within the Analyzer page.	11373
Role based access does not work on remote computers.	12534
The Group Policy module displayed the GPO modified date as local and UTC in different nodes.	15153
The Locked Out Accounts tab did not display the selected monitored domain.	15354

Table 7. Active Directory Health resolved issues

Resolved issue	Issue ID
Improved Directory Analyzer agent memory usage.	5387
The Active Directory Health agent causes event ID 1035 to be logged constantly on the domain controller.	5491
An error occurs in Active Directory forest after running the Active Directory Health Check replication tests.	5929
Inconsistencies in the Forest Report.	6682
Failed to archive the Directory Analyzer data points from storage.	9024
The Directory Analyzer agent is consuming a lot of memory.	9271
The DFSR Conflict Files Generated collector indicates Wrong Count.	9659
Error for one child domain when selected to install the Active Directory Health agents.	11519
Directory Analyzer Agent memory and health monitoring improvements.	14281

Known issues

The following is a list of issues, including those issues attributed to third-party products, known to exist at the time of release.

Table 8. General known issues

Known issue	Issue ID
The Diagnostic Console does not work when trying to create a Connection to a domain controller using a UNC path.	13377
Changing the Active Administrator Foundation Service (AFS) account when upgrading Active Administrator using the Configuration Wizard causes an error when setting the owner on the Certificate Repository. **Workaround:** Add Full Control permissions to the Certificates Repository folder for the new AFS account you want to use, and then run the Configuration Wizard again.	15500

System requirements

Before installing or upgrading Active Administrator® 8.2, 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 Agent requirements
- Workstation logon audit agent requirements
- Web Console requirements
- System Center requirements
- Port requirements
- User privilege requirements

Server hardware requirements

Table 9. Server hardware requirements

Requirement	Details
Processor	1 GHz or higher
Memory	• For Windows Server® 2008 R2: 512 MB minimum, 2 GB recommended • For Windows Server 2012: 1 GB minimum, 2 GB recommended • For Windows Server 2012 R2: 1 GB minimum, 2 GB recommended • For Windows Server 2016: 1 GB minimum, 2 GB recommended
Hard disk space	100 MB
Operating system	• Windows Server 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 **NOTE:** Active Administrator® does not support Microsoft® Nano Server 2016.

Server software requirements

Table 10. 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`.

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 2008
- SQL Server 2008 Express
- SQL Server 2008 R2
- SQL Server 2008 R2 Express
- SQL Server 2012

- SQL Server 2012 Express
- SQL Server 2014
- SQL Server 2014 Express
- SQL Server 2016

> **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.

Console hardware requirements

Table 11. Console hardware requirements

Requirement	Details
Processor	1 GHz
Memory	256 MB
Hard disk space	100 MB
Operating system	• Windows® 7 • Windows 8.1 • Windows 10 • Windows Server® 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 **NOTE:** Active Administrator® does not support Microsoft® Nano Server 2016. **NOTE:** When using Windows 7, you may experience problems when trying to perform some operations on Active Directory® objects, such as creating objects or viewing object properties. When the Microsoft® RSAT tools are installed on Windows 7, the adprop.dll.mui and dsadmin.dll.mui files are not installed and these files are needed by Active Administrator. Please see the Quest® Knowledge Base and Solution Center for instructions on how to locate and copy these files to the correct location. **NOTE:** If you are using the Certificate module, see Table 12 for information on support for SHA-2 certificates.

Table 12. Support for SHA-2 certificates

Operating system	Support SHA-2 certificates	Verify SHA-2 certificates (user mode)	Verify SHA-2 certificates (kernel mode)
Windows Server 2008 R2	supported	KB3033929	KB3033929
Windows Server 2012	supported	supported	supported
Windows Server 2012 R2	supported	supported	supported
Windows Server 2016	supported	supported	supported
Windows 7	supported	KB3033929	KB3033929

Table 12. Support for SHA-2 certificates

Operating system	Support SHA-2 certificates	Verify SHA-2 certificates (user mode)	Verify SHA-2 certificates (kernel mode)
Windows 8.1	supported	supported	supported
Windows 10	supported	supported	supported

Console software requirements

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

Table 13. GPMC and DNS Server Tools install information

Operating system	Download links and install information
Windows® 7 Windows 8.1 Windows 10	GPMC and DNS Server Tools are included in Remote Server Administration Tools (RSAT). • Remote Server Administration Tools for Windows 7: http://www.microsoft.com/en-us/download/details.aspx?id=7887 • Remote Server Administration Tools for Windows 8.1: http://www.microsoft.com/en-us/download/details.aspx?id=39296 • Remote Server Administration Tools for Windows 10 https://www.microsoft.com/en-us/download/details.aspx?id=45520 ***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 2008 R2 Windows Server 2012 Windows Server 2012 R2 Windows Server 2016	***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 Agent requirements

Table 14. Audit agents hardware requirements

Requirement	Details
Processor	1 GHz or higher
Hard disk	100 MB
Memory	256 MB
Operating systems	• Windows Server® 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016

Workstation logon audit agent requirements

Table 15. Workstation logon audit agent hardware requirements

Requirement	Details
Processor	1 GHz or higher
Hard disk	100 MB
Memory	256 MB
Operating systems	• Windows® 7 • Windows 8.1 • Windows 10 • Windows Server® 2008 R2 • Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016

Web Console requirements

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

- Microsoft® Internet Explorer 12
- Microsoft Edge™
- Google Chrome™ 55
- Mozilla® Firefox® 52

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

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

- TCP Port 15600 must be open between Console and the AFS Server.
- TCP Port 15601 must be open between the computer running the workstation logon audit agent and the AFS Server.
- TCP Port 389 must be open between domain controllers and the AFS Server and Console.
- TCP Port 1433 must be open between the AFS Server and the AFS Database Server.
- Remote Procedure Call (RPC) must be open between the AFS Server and the target.
- When installing the audit agent on a member server instead of a domain controller, the following inbound firewall exceptions for Windows® Management Instrumentation must be enabled:
  - ASync-In
  - DCOM-In
  - WMI-In
- If you are using the Certificate Management feature, Remote Registry Service must be enabled on all Windows computers on which certificates are managed.
- If you are using the Azure® Active Directory® feature, TCP Ports 80 and 443 must be open on the Internet-facing firewall.
- If you are using the Active Directory Health feature:
  - TCP Port 15602 must be open on the Active Administrator server for the Active Administrator Data Service (ADS).
  - TCP Port 15603 must be open on the computer running the Directory Analyzer agent.
- If you want to access the DNS event logs in Active Administrator, the following inbound firewall exceptions are required on each DNS server:
  - COM+ Network Access (DCOM-In)
  - Remote Event Log Management (NP-In)
  - Remote Event Log Management (RPC)
  - Remote Event Log Management (RPC-EPMAP)
- If you are using the Web Console, 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 See the *Quest®* Active Administrator® *8.2 Install Guide* for the specific permissions required for operation of each module and submodule.
- Active Administrator Data Services (ADS) requires an account that is a member of the AA_Users group, has read access to the enterprise, and has full access on the server where the Directory Analyzer agent is installed. For more detailed permission requirements, see the *Quest®* Active Administrator® *8.2 Install Guide* for the specific permissions required for ADS and data collectors.
- 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 also can 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, log on locally and manage auditing and security log, or these 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 initial database creation were modified and it can be found under the Users container object of Active Directory®.
- 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® *8.2 Install Guide* for the specific permissions required for operation of each module and submodule.

Upgrade and compatibility

- Active Administrator® 8.2 only supports in-place upgrades from Active Administrator versions 7.5, 8.0, or 8.1. Upgrades from previous editions are not supported. To perform an in-place upgrade to Active Administrator 8.2 from a version of Active Administrator that is earlier that v7.5, the user must first upgrade to Active Administrator 7.5.
- Installing Active Administrator 8.2 onto an existing Active Administrator 7.5, 8.0, or 8.1 installation will result in the removal of the earlier version. Active Administrator 7.5, 8.0, or 8.1 databases, both live and archive databases, will be automatically upgraded to version 8.2.
- A database upgraded by Active Administrator 8.2 cannot be used by previous version and the database upgrade cannot be rolled back.
- Data within the Active Administrator share can be used by Active Administrator 8.2.
- Active Administrator 8.2 Auditing Agents cannot be installed on Windows 2000 hosts.
- If you use group policy to deploy the Workstation Logon Auditing Agents (WLAA), the v8.2 installation process will update the agent on the user workstations. If the Workstation Logon Auditing Agents are installed manually, you must replace the install package at the software distribution share with the 8.2 version. Computers will upgrade to the Active Administrator 8.2 WLAA the next time they are started.
- The Azure® Active Directory®, Certificate Management, DNS Management, and Active Directory Health features available in Active Administrator 8.2 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, DNS Management, and Active Directory Health are not included.
>
> The Azure Active Directory, Certificate Management, DNS Management, and Active Directory Health features each require a separate license. If you do not have a license file to apply, the module does not appear in Active Administrator. You will see the Azure Active Directory and Certificate Management features listed under the Configuration module, but when you select the feature, a warning displays that a license is required.

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

- Installing Active Administrator server
- Configuring the server
- Installing Active Administrator console
- Updating audit agents
- Switching to Active Directory Health

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

Installing Active Administrator server

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

To install Active Administrator® server

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

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

Configuring the server

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**.
    - 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 9. If you select **No**, continue to the next step.
3. Select **Use an existing Active Administrator database**.
4. Accept the displayed server and database or select a different server and database.
5. Click **Next**.
6. Select **Use an existing Active Administrator Archive database**.

7. Accept the displayed server and database or select a different server and database.
8. Click **Next**.
9. Select the purge and archive options to enable or disable.
10. Click **Next**.
11. Select the path to the Active Administrator share.
12. Click **Next**.
13. Accept the SMTP server setup or make any necessary changes.
14. Click **Next**.
15. Type a valid email address or accept the default.
16. Click **Next**.
17. Accept the active template settings or name any necessary changes.
18. Click **Next**.
19. Accept the group policy history settings or make any necessary changes.
20. Click **Next**.
21. Accept the Active Directory backup settings or make any necessary changes.
22. Click **Next**.
23. To add additional users, click **Add**, find and select users, click **OK**.
24. Click **Next**.
25. Type the account password for the Active Administrator Foundation Service account.
26. The default service port number is 15600. To change the port number, type a value.
27. 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.
28. Click **Next**.
29. Click **Finish**.
30. Click **Finish**.

Installing Active Administrator console

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

> i **IMPORTANT:** Active Administrator includes the Diagnostic Console, which is also a feature in 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/8.2/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

We are more than just a name

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

Our brand, our vision. Together.

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

Contacting Quest

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

Technical support resources

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

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

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

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 16. 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.
JQuery 1.9.1	Copyright 2016 The jQuery Foundation.
Json.NET 6.0.3	Copyright (c) 2007 James Newton-King

Table 16. Third-party contributions

Component	License or acknowledgment
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

Table 16. 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 16. 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 16. 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 16. 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) 3.10	Windows Installer XML Toolset version 3.10.2.2516. Copyright(c) Outercurve Foundation. All rights reserved. Microsoft Reciprocal License (MS-RL)
ZLib 1.1.4	Copyright (C) 1995-2005 Jean-loup Gailly and Mark Adler This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software. Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions: 1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required. 2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software. 3. This notice may not be removed or altered from any source distribution. Jean-loup Gailly jloup@gzip.org Mark Adler madler@alumni.caltech.edu

© 2017 Quest Software Inc.

ALL RIGHTS RESERVED.

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

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

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

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

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

Patents

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

Trademarks

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

Legend

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

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