Quest® Active Administrator® 8.2

What's New

November 2017

Quest® Active Administrator® 8.2 is the latest release of Quest Software's complete solution for managing Microsoft® Active Directory® health, delegation, accounts, GPOs, recovery and security auditing, and certificate and DNS management. This document provides a highlight of these improvements.

NOTE: The Certificate Management, Azure Active Directory, DNS Management, and Active Directory Health modules each require a license in addition to the license for Active Administrator.

This document highlights key features new in this release. For more information about these or any features, see the *Quest Active Administrator 8.2 User Guide*.

- Automatic Directory Analyzer agent deployment
- Schedule Active Directory Health Checks
- View domain controller details
- New Active Directory Health reports
- New Security reports
- New Certificates reports
- New Server Configuration report

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**).

What's new in Active Directory Health

- Monitor Directory Analyzer agent performance
- Connect to System Center Operations Manager

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 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.

What's new in Certificate Management

- Certificate Protection
- Monitor organizational units for certificate management

- Search for certificates
- Exclude selected certificate stores
- Add computers from OUs when managing certificates
- Schedule certificate reports
- Manage certificate expiration reminders
- Expanded notification of certificates using cryptographic hash algorithms
- Add a certificate to the repository from a URL

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 overridden. To see the history of repairs and overrides, 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 load 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

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.

- The **Summary** tab lists all the CA servers found in the selected forest along with status of the Active Directory Certificate Service, and required Active Directory objects. Double-click a certificate to view details and to install the certificate.
- On the **Search** tab, you can search for users, computers, users and computers with a template name, users or computers with an issuer name, users and computers by key usage, and objects without certificates. From the search results, you can view certificate details and install a certificate.
- Use the **Servers** tab to view and manage each CA server found in the selected forest. You can stop, start, and restart the Active Directory Certificate service (certsvc), back up the selected server, and open the Microsoft Management Console (MMC) for the selected server.
- On the **Templates** tab, you can view all the certificate templates found in the selected forest.
- The **Events** tab displays events for a selected CA server. Events are separated into processing events and all server events.
- The **Backups** tab lists the backups for each CA server. Backup files are saved for 30 days. Use certutil.exe to restore the backup.

What's New 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 Active Directory Health reports

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.

New Security reports

Table 2. New Security reports

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 History Report	Lists all inactive user or computer accounts in the specified database and domain.

New Certificates reports

Table 3. New 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.

New Server Configuration report

Displays information about the Active Administrator configuration settings. Information includes server names, port numbers, and database names.

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.

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.