Quest

Quest® Active Administrator® 8.8

User Guide

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

Quest Software Inc.
Attn: LEGAL Dept.
20 Enterprise, Suite 100, Aliso Viejo, CA 92656

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

Patents

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

Trademarks

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

Legend

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

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

Active Administrator User Guide
Updated - January 2025
Software Version - 8.8

Contents

Active Administrator Overview 14
Starting Active Administrator console 14
Using quick tasks 14
Using the dashboard 15
Managing domain controllers 15
Adding a managed domain controller 16
Removing a managed domain controller 16
Accessing a domain controller remotely 17
Searching Active Directory 17
Opening the Web Console 18

User Provisioning 19
Using the Provisioning landing page 19
Provisioning Users 19
Editing the Provisioning Template 20
Deprovisioning Users 22
Viewing the provisioning and deprovisioning logs 23
Purging the logs 23

Certificates 24
Using the Certificates landing page 25
Managing computers 25
Adding computers 26
Excluding stores 28
Removing computers 28
Disabling certificate management 28
Managing monitored objects 29
Managing certificates 30
Updating the list of certificates 31
Sorting and filtering the list of certificates 32
Grouping the list of certificates 32
Viewing certificate details 32
Viewing the validation chain 32
Sending email notifications 33
Excluding certificates that support cryptography 33
Excluding revoked certificates 33
Reporting on certificates 34
Sending a report 34
Managing report schedules 35
Exporting certificates 36
Installing certificates 36
Deleting certificates 37
Managing Certificate Authority 37

Viewing a Certificate Authority summary . . . 38
Adding a forest . . . 38
Searching Certificate Authority . . . 39
Managing Certificate Authority servers . . . 40
Viewing certificate templates . . . 40
Viewing events . . . 40
Configuring Certificate Authority notifications . . . 41
Viewing Certificate Authority backups . . . 41
Purging Certificate Authority backups . . . 42
Managing Purge History . . . 42
Using the Certificate Repository . . . 42
Adding a certificate to the repository . . . 43
Viewing certificate details from the repository . . . 43
Installing certificates from the repository . . . 44
Updating certificates in the repository . . . 44
Reporting on certificates in the repository . . . 45
Exporting certificates from the repository . . . 46
Deleting certificates from the repository . . . 46
Searching certificates . . . 47
Searching for certificates . . . 47
Creating a new certificate search definition . . . 47
Editing a certificate search definition . . . 48
Deleting a certificate search definition . . . 48

Security & Delegation . . . 50
Using the Security & Delegation landing page . . . 50
Managing security . . . 51
Managing Active Directory objects . . . 51
Viewing Active Directory objects by type . . . 52
Reporting on Active Directory objects by type . . . 53
Viewing native permissions . . . 54
Viewing Active Template delegations . . . 56
Resetting passwords . . . 57
Resetting computers . . . 57
Moving Active Directory objects . . . 58
Managing group memberships . . . 58
Reporting on Active Directory objects . . . 60
Monitoring user logon activity . . . 60
Managing locked out accounts . . . 61
Adding domains to monitor . . . 61
Resolving a locked out account . . . 62
Managing password policies . . . 63
Creating a new fine-grained password policy . . . 63
Linking a password policy . . . 64
Sending password notifications . . . 64
Checking delegation status . . . 65
Adding a delegation . . . 65
Managing Active Templates . . . 66

Creating an Active Template . . . 67
Copying an Active Template . . . 68
Categorizing Active Templates . . . 68
Adding a delegation link . . . 69
Reporting on Active Templates . . . 69
Managing inactive accounts . . . 70
Configuring inactive users and computers . . . 70
Checking for inactive users and computers . . . 74
Viewing inactive users and computers history . . . 74
Reporting on inactive accounts . . . 75
Purging stale accounts . . . 75
Sending password reminders . . . 76
Sending account expiration notifications . . . 79
Viewing expired accounts . . . 80
Purging account history . . . 80
Archiving account history on demand . . . 81
Purging account history on demand . . . 81
Scheduling an account history purge and archive . . . 81

Active Directory Health . . . 83
Switching to Active Directory Health . . . 84
Using the Active Directory Health landing page . . . 84
Installing Active Directory Health Analyzer agents . . . 86
Installing Active Directory Health Analyzer agents into a pool . . . 87
Installing Active Directory Health Analyzer agents onto domain controllers . . . 88
Installing Active Directory Health Analyzer agents manually . . . 90
Setting up automatic Active Directory Health Analyzer agent deployment . . . 90
Using the Active Directory Health Analyzer agent configuration utility . . . 91
Setting network settings . . . 92
Enable logging . . . 92
Excluding domain controllers . . . 92
Managing the Remediation Library . . . 93
Adding custom remediations . . . 93
Deleting custom remediations . . . 94
Analyzing Active Directory health . . . 95
Managing the Active Directory Health Analyzer tree . . . 95
Using the analyzer pages . . . 96
Analyzing health of all domain controllers . . . 97
Analyzing health of a selected domain controller . . . 97
Analyzing health of all domains . . . 99
Analyzing health of a selected domain . . . 99
Analyzing health of all sites . . . 100
Analyzing health of a selected site . . . 101
Analyzing the health of a forest . . . 102
Analyzing Microsoft Entra ID . . . 103
Installing the Microsoft Entra Connect Health Monitoring Agent . . . 104
Setting up the Microsoft Entra Connect application . . . 105

Viewing Microsoft Entra Connect status . . . 105
Viewing Microsoft Entra Connect alerts . . . 107
Monitoring Microsoft Entra Connect operations . . . 108
Viewing Microsoft Entra Connect events . . . 109
Searching the Metaverse . . . 109
Viewing Microsoft Entra Connect connectors . . . 110
Managing the Microsoft Entra Connect Health Monitoring Agent . . . 110
Managing Active Directory Health Analyzer alerts . . . 113
Setting alerts . . . 113
Purging and archiving alert history . . . 114
Viewing alerts and alert history . . . 115
Filtering alert history . . . 116
Generating an alert history report . . . 117
Muting alerts . . . 118
Clearing mutes . . . 119
Viewing mute history . . . 120
Managing alert notifications . . . 120
Creating alert notifications . . . 120
Editing alert notifications . . . 122
Removing alert notifications . . . 122
Pushing alerts to System Center Operations Manager and SNMP managers . . . 123
Limiting alert notifications . . . 123
Managing monitored domain controllers . . . 124
Adding monitored domain controllers . . . 125
Managing data collectors . . . 126
Setting permissions for data collectors . . . 126
Setting data collectors . . . 126
Adding performance counter data collectors . . . 127
Adding Windows Services data collectors . . . 128
Adding Event Log data collectors . . . 129
Setting an authoritative RODC . . . 129
Purging and archiving Active Directory Health Analyzer data . . . 130
Active Directory Health Templates . . . 130
Creating and Applying Active Directory Health Templates . . . 130
Managing Active Directory Health Templates . . . 132
Managing Active Directory Health Analyzer agents . . . 134
Managing agent workload . . . 136
Sending agent notifications . . . 137
Monitoring agent performance . . . 137
Using the Troubleshooter . . . 139
Managing the DFSR service . . . 139
Running the Directory Service Replication Troubleshooter . . . 140
Enabling or disabling domain controller replication . . . 141
Setting directory service log levels . . . 141
Setting Netlogon parameters . . . 142
Setting startup and recovery options . . . 142
Cleaning up metadata . . . 143

Running online defrag . . . 143
Replicating Active Directory . . . 144
Recovering Active Directory Health data . . . 145
Preparing for data recovery . . . 145
Restoring the Active Directory Health module and data . . . 146

Auditing & Alerting . . . 147
Using the Auditing & Alerting landing page . . . 147
Managing audit reports . . . 148
Creating a new audit report . . . 149
Creating a new audit report by copying a report . . . 151
Running an audit report . . . 151
Scheduling audit reports . . . 152
Changing ownership of scheduled reports . . . 153
Categorizing audit reports . . . 153
Using tags to mark events . . . 154
Adding a comment to an event . . . 155
Grouping events . . . 155
Viewing event details . . . 156
Managing archive reports . . . 156
Managing audit agents . . . 157
Excluding domain controllers . . . 158
Setting up auditing on domain controllers . . . 158
Installing audit agents . . . 159
Modifying the audit agent startup account . . . 160
Modifying the audit agent test account . . . 161
Updating audit agents . . . 161
Moving an audit agent . . . 161
Automating audit agent deployment . . . 162
Canceling pending automated deployments . . . 163
Managing alerts . . . 164
Creating an alert . . . 165
Managing existing alerts . . . 167
Changing the alert notification policy . . . 167
Setting global quiet time . . . 168
Managing alert history . . . 168
Managing event definitions . . . 170
Importing new event definitions . . . 170
Excluding account events from auditing . . . 171
Archiving & purging audit events . . . 172
Archiving events on demand . . . 173
Purging events on demand . . . 173
Setting purge and archive options . . . 173
Scheduling an event log purge and archive . . . 174
Managing the history log . . . 175
Running database maintenance . . . 175

Group Policy . . . 176

Using the Group Policy landing page . . . 176
Managing Group Policy objects . . . 177
Creating a new Group Policy object . . . 178
Copying Group Policy objects . . . 178
Copying Group Policy objects between domains . . . 179
Comparing Group Policy objects . . . 179
Reporting on Group Policy objects . . . 180
Managing links . . . 181
Managing GPOs by container . . . 181
Creating containers . . . 182
Linking Group Policy objects . . . 183
Blocking inheritance . . . 183
Managing linked GPOs . . . 184
Reporting on Group Policy objects . . . 185
Searching for GPO settings . . . 185
Managing GPO history . . . 185
Rolling back Group Policy . . . 186
Using the GPO repository . . . 187
Adding a GPO to the repository . . . 188
Editing a GPO offline . . . 188
Modeling GPO changes . . . 189
Creating a simulation . . . 189
Managing GPO backups . . . 190
Backing up Group Policy objects . . . 191
Scheduling a GPO backup . . . 191
Scheduling a purge of GPO backups . . . 192
Comparing Group Policy backups . . . 192
Restoring a Group Policy object . . . 192
Troubleshooting . . . 193
Enabling logging . . . 193
Updating Group Policy . . . 194
Purging GPO history . . . 194
Purging GPO history on demand . . . 195
Scheduling a GPO history purge . . . 195

Active Directory Recovery . . . 196
Using the Active Directory Recovery landing page . . . 196
Managing Active Directory backups . . . 196
Restoring from a backup . . . 197
Purging Active Directory backups . . . 199
Purging Active Directory backups on demand . . . 199
Scheduling an Active Directory backup purge . . . 200

Active Directory Infrastructure . . . 201
Using the Active Directory Infrastructure landing page . . . 201
Managing Active Directory sites . . . 201
Browsing Active Directory . . . 202

Building Active Directory structure . . . 202
Reporting on Active Directory . . . 205
Monitoring replication . . . 206
Adding a forest . . . 206
Using the replication analyzer . . . 207
Managing Active Directory trusts . . . 208
Adding a forest trust . . . 208
Adding a domain trust . . . 209

DC Management . . . 211
Using the DC Management landing page . . . 211
Checking domain controller status . . . 211
Managing services . . . 212
Monitoring domain controller performance . . . 212
Managing event logs . . . 213

DNS Management . . . 215
Using the DNS Management landing page . . . 215
Managing DNS servers . . . 216
Adding managed DNS servers . . . 216
Adding records . . . 217
Editing records . . . 217
Deleting records . . . 217
Running reports . . . 217
Editing DNS server properties . . . 218
Editing zone properties . . . 219
Editing zone permissions . . . 219
Scavenging records . . . 220
Monitoring DNS servers . . . 220
Setting testing options . . . 220
Creating tests . . . 220
Running tests . . . 221
Editing a test . . . 221
Deleting a test . . . 222
Using the DNS analyzer . . . 222
Viewing the DNS event log . . . 223
Using custom filters . . . 223
Setting display options . . . 224
Searching for DNS records . . . 225

Configuration . . . 226
Using the Configuration landing page . . . 226
Managing tasks . . . 227
Defining role-based access . . . 227
Adding a new user or group to Active Administrator . . . 231
Setting email server options . . . 232
Configuring SCOM and SNMP Settings . . . 232

Setting notification options 233
Setting Active Template options 233
Setting agent installation options 234
Setting recovery options 235
Adding a domain 236
Enabling or disabling password recovery 236
Setting GPO history options 236
Setting certificate configuration 237
Setting certificate notifications 237
Setting up certificate email notifications 238
Configuring certification authority 239
Setting security on the repository 239
Setting service monitoring policy 240
Managing archive databases 240
Creating an archive database 241
Modifying archive database settings 242
Migrating data to another database 242
Setting a preferred domain controller 243
Setting up workstation logon auditing 243
Deploying the workstation logon audit agent 244
Enabling the default port for the workstation logon auditing agent 245
Managing configuration settings 245
Setting the Active Administrator server 246
Viewing license details 246
Running an assessment report 246
Scheduling an assessment report 247
Running a configuration report 248
Managing email addresses 249
Scheduling a configuration report 250
Checking status of the AFS server 251
Setting user options 251
Setting general user options 252
Setting options for audit reports 252
Setting user log on activity 253
Setting Active Directory Health Analyzer options 253
Enabling console logging 254
Managing the Active Directory server 254
Stopping and starting AFS and ADS services 254
Setting the services startup accounts 255
Managing logging for services 255
Clearing the AFS cache 255
Setting port numbers for services 255
Enabling Full-Text Search 256
Updating Active Administrator licenses 256
Managing Security 256
Managing Notification Services 258
Configuring the Web server 258

Diagnostic Console 260
Opening the Diagnostic Console 261
Using components 261
Network components 261
Dataflow components 262
LSASS components 263
File Replication components 264
AD Store components 264
Active Directory components 264
Operating System components 265
Using indicators 265
Using drilldowns 266
Performance drilldown 267
Replication drilldown 268
Configuration drilldown 270
DNS drilldown 271
LSASS drilldown 272
LDAP drilldown 272
FSMO Roles drilldown 272

Alerts Appendix 274
Domain controller alerts 274
Active Directory Certificate Services service is not running 276
Active Directory Domain Services is not running 276
Active Directory Web Services service is not running 276
Consecutive replication failures 277
DC cache hits 277
DC DIT disk space 278
DC DIT log file disk space 279
DC LDAP load 280
DC LDAP response too slow 280
DC Memory Usage 281
DC properties dropped 282
DC RID pool low 282
DC SMB connections 283
DC SYSVOL disk space 284
DC time sync lost 284
Detected NO_CLIENT_SITE record 285
DFS Replication service not running 286
DFS service is not running 286
DFSR conflict area disk space 287
DFSR conflict files generated 287
DFSR RDC not enabled 288
DFSR sharing violation 288
DFSR staged file age 289
DFSR staging area disk space 289
DFSR USN records accepted 290
DFSRS CPU load 290

DFSRS unresponsive . . . 291
DFSRS virtual memory . . . 291
DFSRS working set . . . 292
DNS Client Service is not running . . . 292
Domain controller CPU load . . . 293
Domain controller page faults . . . 293
Domain controller unresponsive . . . 294
File Replication Service is not running . . . 295
File replication (NTFRS) staging space free in kilobytes . . . 295
GC response too slow . . . 296
Group policy object inconsistent . . . 297
Hard disk drive . . . 298
Intersite Messaging Service is not running . . . 298
Invalid primary DNS domain controller address . . . 298
Invalid secondary DNS domain controller address . . . 299
KDC service is not running . . . 300
LSASS CPU load . . . 300
LSASS virtual memory . . . 301
LSASS working set . . . 301
Missing SRV DNS record for either the primary or secondary DNS server . . . 302
NETLOGON not shared . . . 303
NetLogon service is not running . . . 304
Orphaned group policy objects exist . . . 305
Physical memory . . . 305
Power supply . . . 306
Primary DNS resolver is not responding . . . 306
Secondary DNS resolver is not responding . . . 307
Security Accounts Manager Service is not running . . . 307
SRV record is not registered in DNS . . . 307
SYSVOL not shared . . . 308
W32Time service is not running . . . 309
Workstation Service is not running . . . 310
Domain alerts . . . 310
Conflict encountered during replication . . . 311
DNS server missing domain SRV records . . . 311
Domain FSMO role placement . . . 312
Global catalog server replication latency . . . 312
Infrastructure operations master hosts a global catalog server . . . 313
Infrastructure operations master inconsistent . . . 313
Infrastructure operations master not responding . . . 314
Missing root PDC time source . . . 315
Objects exist in the Lost and Found container . . . 315
PDC operations master inconsistent . . . 316
PDC operations master not responding . . . 317
Replication latency . . . 317
RID operations master inconsistent . . . 318
RID operations master not responding . . . 319
RODC allowed password replication policy inconsistent . . . 320

RODC denied password replication policy inconsistent . . . 320
Site alerts . . . 321
Inter-site replication manager . . . 321
Inter-site replication topology generation disabled . . . 322
Intra-site replication topology generation disabled . . . 322
Morphed directories exist in site . . . 323
No authority in site to resolve universal group memberships . . . 323
Too few global catalog servers in site . . . 324
Forest alerts . . . 324
Domain naming and schema operations masters differ . . . 325
Domain naming operations master inconsistent . . . 325
Domain naming operations master is not a GC . . . 326
Naming operations master not responding . . . 326
Schema operations master inconsistent . . . 327
Schema operations master not responding . . . 328
Schema version inconsistent . . . 328
Site link settings inconsistent with PDC . . . 329
Site settings inconsistent with PDC . . . 329
Subnet settings inconsistent with PDC . . . 330
Microsoft Entra Connect alerts . . . 330
Windows Services alerts . . . 330
Connectivity alerts . . . 331
Event ID alerts . . . 331

Event Definitions . . . 332

PowerShell cmdlets . . . 337
What are cmdlets? . . . 337
Using Active Administrator cmdlets . . . 338
Using cmdlets to get information about the Active Administrator server . . . 339
Using cmdlets to manage the Active Administrator server . . . 343
Using cmdlets to manage Active Administrator tasks . . . 347
Active Templates and Delegations Cmdlets . . . 348

Appendix: Registering Active Administrator for Office 365 Exchange Online . . . 350

About us . . . 351
Technical support resources . . . 351

1

Active Administrator Overview

Quest® Active Administrator® extends the functionality of the built-in Windows® management tools for Active Directory® by allowing administrators to view and manage security in a much more extensible interface. Active Administrator gives administrators the ability to control permissions inheritance on objects as well as change inherited permissions to explicit permissions.

Topics

- Starting Active Administrator console
- Using quick tasks
- Using the dashboard
- Managing domain controllers
- Searching Active Directory
- Opening the Web Console

Starting Active Administrator console

To start Active Administrator console

1 Select **Start | Active Administrator Console**.

> **NOTE:** The first time you open the Active Administrator® console, you may be asked to set the Active Administrator server.
>
> Do one of the following:
>
> - Select a connection point from the list.
> - Type the name of the Active Administrator server in the **Server** box.
> - Browse to locate a server.
>
> If a connection point is not listed, you must type the server name in the **Server** box. If you do not want to use connection points, you can disable the feature. See Setting general user options.

2 The Active Administrator console opens to the **Home** page, which is divided into two areas.

- The menu structure on the left provides access to Active Administrator modules. You can expand or collapse the menu structure as needed.
- The **Active Administrator Quick Tasks** area presents links to options in the menu structure that are frequently used, as well as basic tasks that you can perform directly on the **Home** page. See Using quick tasks.

Using quick tasks

The **Home** page lists quick tasks that take you to specific areas in Active Administrator®. In addition, you can perform some quick tasks directly on the **Home** page.

- To hide or show the quick tasks, click the chevron.

Table 1. Quick tasks

Quick task	Description
Search Active Directory	For a more complex search, see Searching Active Directory.
Enable/Disable User Account	Enable or disable an account from search results. See Searching Active Directory. You also can enable/disable a user account from the Security & Delegation module. See Monitoring user logon activity.
Reset Password	Reset the password from search results. See Searching Active Directory. You also can reset the password on an account from the Security & Delegation module. See Resetting passwords.
Add a User to or Remove a User from a Group	Add a user to a group from search results. See Searching Active Directory. You also can add a user to a group from the Security & Delegation module. See Managing security.
Unlock User Account	Unlock a user account from search results. See Searching Active Directory. You also can unlock a user account from the Security & Delegation module. See Managing locked out accounts.
Reset Computer Account	You can reset a computer account from search results. See Searching Active Directory. You also can reset a computer account from the Security & Delegation module. See Managing security.

Using the dashboard

The dashboard provides a quick look into Active Directory® activity.

To view a chart

1. Click **Dashboard**.
2. Select the type of chart: **Domains**, **Auditing**, **Alerting**, or **Logon Activity**.
3. Choose the options for the chart, and click **Go**.
   - By default, the legend displays on the chart. To hide the legend, clear the check box.
   - To print a chart, click **Print Chart**.

Managing domain controllers

Some modules within Active Administrator®, such as Group Policy and DNS, are specific to a selected domain controller. You can add or remove domain controllers from the list, reboot a domain controller, access a domain controller using Remote Desktop Connection, and launch the Diagnostic Console.

Topics

- Adding a managed domain controller
- Removing a managed domain controller
- Accessing a domain controller remotely

To manage domain controllers

1 Open an Active Administrator module.

2 In the **Domain Controller** box, select a domain controller.

3 Use the icons to manage the selected managed domain controller.

Table 2. Domain controller icons

Icon	Description
	Add or remove a managed domain controller. See Adding a managed domain controller and Removing a managed domain controller.
	Refresh the domain controller.
	Access the domain controller using Remote Desktop Connection. See Accessing a domain controller remotely.
	Reboot the domain controller.
	Launch the Diagnostic Console for the domain controller. See Diagnostic Console.

Adding a managed domain controller

The list of managed domain controllers is limited to those you add from the list of available domain controllers.

To add a managed domain controller

1 Click  .

2 Type a domain name or browse to locate a domain.

3 Click **Find Domain Controllers**.

4 From the list of available domain controllers, select a domain controller.

- To filter the list of available domain controllers, type in the **Filter Domain Controllers** box. The list filters as you type. To remove the filter, click **X**.
- To view details about a selected domain controller, click **Details**.

5 To add the domain controller to the list of managed domain controllers, click **Add**.

- To filter the list of managed domain controllers, type in the **Filter Domain Controllers** box. The list filters as you type. To remove the filter, click **X**.
- To view details about a selected domain controller, click **Details**.

6 Click **OK**.

Removing a managed domain controller

Removing a managed domain controller only removes it from the list. You can quickly add it back to the list when you need it.

To remove a managed domain controller

1 Click  .

2 Select a managed domain controller.

- To filter the list of managed domain controllers, type in the **Filter Domain Controllers** box. The list filters as you type. To remove the filter, click **X**.
- To view details about a selected domain controller, click **Details**.

3 Click **Remove**.

4 Click **OK**.

Accessing a domain controller remotely

You can access a domain controller using Remote Desktop Connection.

To access a domain controller using Remote Desktop Connection

1 Click  .

2 Type the password for the account.

3 Select the resolution.

4 To set advanced options, click **Advanced**.

You can select to auto reconnect, to display the connection bar in full screen mode, and to use smart sizing.

5 Click **Connect**.

Searching Active Directory

Use the Search module to find Active Directory® objects quickly and to perform basic tasks.

NOTE: You can perform a quick search on the **Home** page. See Using quick tasks.

To search Active Directory

1 Click **Search**.

2 Select a domain controller, if necessary.

NOTE: Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3 If you are looking for a specific object or know part of the object name, type a string in the **Search for users, computers, groups, etc.** box. You can use the * wildcard character in your search string.

4 Choose the type of object to search for. If you choose **All**, every object in the domain is returned. If you want to match the string exactly, select **Exact Match**.

5 To start the search, click **Start**.

- If the search is taking too long, click **Stop**.

  The results of the search display in the left column. If you do not see any results, alter the search string or deselect **Exact Match**.

- To filter the list, start typing in the box. The list filters as you type.

6 Select an item to view the details in the right pane.

7 Use the menu to perform tasks on the object.

Table 3. Active Directory menu

Option	Description
Move	Move the selected object to a different container.
Rename	Rename the selected organizational unit, group, contact, or user.
Add to Group	Add the selected computer, contact, group, or user to a group.
Edit	Edit the selected object.
Reset Computer	Reset the selected computer.
Enable	Enable the selected account.
Disable	Disable the selected computer, contact, or user.
Unlock	Unlock the selected user.
Change Photo	Change the photo for the selected user or contact.
Delete Photo	Delete the photo for the selected user or contact.
Reset Password	Reset the password for the selected user.
Delete	Delete the selected object.

Opening the Web Console

Active Administrator® Web Console extends the functionality of the built-in Windows® management tools for Active Directory® by allowing administrators to view and manage security in a much more extensible interface. You can open Active Administrator Web Console on a variety of devices in the following browsers:

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

The Active Directory Health dashboard is where you can monitor the overall health of your organization. From the dashboard, you can view Alerts, set up Notifications, run Health checks, and generate Reports. The Active Directory Topology viewer lets you monitor alerts while viewing a customizable topology diagram of your organization. For more information on the Web Console, see the *Active Administrator Web Console User Guide*.

NOTE: You must configure the web server before you open the web console. See *Configuring the web server* in the *Active Administrator Web Console User Guide*.

To open the Web Console

- Click **Web Console**.

  The Web Console opens in the default browser.

2

User Provisioning

With the rise of data breaches within organizations, it has become increasingly important to ensure users are created with proper access as they join an organization as well as providing an easy way to remove that access when they leave. Ensuring user's access is up-to-date through provisioning is a time consuming process that typically needs to be done immediately and has the potential for human error.

Active Administrator is extending its user management capabilities by providing the ability to automate provisioning and de-provisioning of users accounts. Automating this process:

- Eases administration and increases efficiency by allowing you to bulk import user account data in a form that is specific to your organization.
- Improves security by ensuring users have access only to the resources they need and quickly and efficiently removing access as required.

NOTE: The provisioning feature is enabled through role-based access. See Defining role-based access for details on managing access through roles.

- By default, all users are granted the User Provisioning read-only access role.
- Users who hold the Full Access role are automatically granted the User Provisioning role.

Topics

- Using the Provisioning landing page
- Provisioning Users
- Editing the Provisioning Template
- Editing the Provisioning Template
- Viewing the provisioning and deprovisioning logs
- Purging the logs

Using the Provisioning landing page

User provisioning and deprovisioning involves creating accounts as people join an organization; updating access as they change responsibilities within it; and disabling or deleting accounts as people leave.

Active Administrator's automated user provisioning is accomplished through a provisioning template that contains the user attributes and a csv file that contains the user data. You can easily bulk import user data from an existing system, such as an HR database, and preview the entries before committing the changes to Active Directory.

A default template is included that contains basic user account attributes. You can, however, edit the template to suit your organization. If you update the template or csv file, you can simply refresh the template to preview the updates.

Provisioning Users

Provisioning involves creating user accounts, giving permissions, and changing accounts or privileges as necessary.

To provision users:

1 Click **Provisioning | Provision Users**.

2 Click **Provision Users** to configure your provisioning settings.

3 On the Choose template screen, select the template that defines the columns in the user data file, and click **Next**.

You can use the default template provided by Active Administrator that contains basic user account attributes or select a previously created custom template

If there is an issue with the template file you will be prompted to either load the default file or edit the template and try again. See Editing the Provisioning Template for file details.

4 On the **Import data** screen, browse to the .csv file that contains the user account data, select whether the source user data is separated by a comma, colon, semi-colon, pipe, or tab, and enter the number of header rows to be removed from the file.

The imported data will display in the preview pane. If the format meets your requirement, click **Next** to select the provisioning option. If not, edit the template or the csv file, re-import the csv file and review the data again.

5 On the **Select options page**, define how you want to provision users, then click **Next** to commit the changes.

- Select to create new users, update existing users, or both.
  - If selecting to create new users, select to have new users enabled (if required), and choose the domain and container where the users will be located.

NOTE: Passwords are required to provision users as enabled.

  - If updating existing users, you can choose to update their passwords.

6 On the **Provision users screen**, preview the changes that will be made to the Active Directory once the updates are committed. Select **Stop Preview** to stop loading user data once you are satisfied with the settings.

7 Select **Back** to edit the user provisioning settings if required or click **Commit** to apply the updates in Active Directory.

Once you commit the changes, the Active Directory Users container is searched to locate the specified SAMAccountName attribute specified in the template. If an associated user is not found, a new user is created; if the user is found, it is updated with the attributes in the imported csv file.

8 The preview pane will be updated with the progress as users are provisioned.

Editing the Provisioning Template

The provisioning template contains the user attributes that you want to manipulate. A default template is installed with Active Administrator that contains the following user attributes: Login Name, Display name, First name, Last name, and Initial password. However, if required, you can create a copy of this file and update as required to meet your specific needs.

NOTE: The following fields are required in the template:

- SAMAccountName
- Common name
- Display name
- Temporary password (to create new users in the enabled state only)

NOTE: The template only supports single-value strings.

To edit the template

1. Locate the **UserProvisioningTemplate.json** file found under **MyDocuments\Quest Active Administrator\Provisioning\Templates**.
2. This file is read-only. To edit the file, you must make a copy of it and update as needed. You can then select this file in the provisioning wizard.

   By default, the file contain fields for:

   - name: The name of the template.
   - description: A description of the template.
   - properties: An array of properties used for user provisioning.

   Each property will consist of:

   - name: The name of the property, corresponding to an Active Directory property for a user object.
   - displayName: The name that will display on the top of the list view columns.
   - inclusion: One of the following values:
     - Mandatory: This column is shown in the list view and *must* have a value.
     - Optional: This column is shown in the list view and its value may be null.
     - Ignore: This column is not shown in the list view, nor used for provisioning.
3. Re-import the csv file, and click **Refresh Template** to review the data again. Once you are satisfied with the preview, commit the updates.

Example template file structure

```
{
  "name": "User provisioning template",
  "description": "The template for provisioning users.",
  "properties": [
{
      "name": "saMAccountName",
      "displayName": "Login Name",
      "inclusion": "mandatory"
    },
{
      "id": "cn",
      "displayName": "Common Name",
     "adPropertyName": "cn"
     "inclusion": "mandatory"
    },
    {
      "name": "displayName",
      "displayName": "Display Name",
      "inclusion": "mandatory"
    },
```

```
    {
      "name": "givenName",
      "displayName": "First Name",
      "inclusion": "optional"
    },
    {
      "name": "sn",
      "displayName": "Last Name",
      "inclusion": "optional"
    },
     {
      "name": "initialPassword",
      "displayName": "Initial Password",
      "inclusion": "optional"
    }
  ]
}
```

Deprovisioning Users

Deprovisioning users removes privileges or access from an account or deletes an account that is no longer required as a result of employee leaving a company or changing responsibilities within the organization. The ability to automate this process helps to quickly ensure these accounts are not left exposed to attacks and potentially inappropriate data access.

To deprovision a user account:

1. Click **Provisioning | Deprovision Users**.
2. Click **Deprovision Users** to configure your provisioning settings.
3. Select the users to deprovision. Begin by selecting the required domain, then specify the required users using one of the following methods:

   Search through Active Directory or type a specific user and add and remove as required.

   Import a list of users from a .csv file. Browse to the .csv file that contains the user account data, select whether the source user data is separated by a comma, colon, semi-colon, pipe, or tab, enter the number of header rows to be removed from the file, and identify which column contains the required SAM account.

   Use the list of users that have been deemed inactive through the settings that have been configured through Active Administrator. See Managing inactive accounts.
4. Once you have selected the users, choose whether you want to **Disable accounts** or **Delete accounts**, and click **Next**.
5. On the **Deprovision users screen**, preview the changes that will be made to the Active Directory once the updates are committed. Select **Stop Preview** to stop loading user data once you are satisfied with the settings.
6. Select **Back** to edit the user deprovisioning settings if required or click **Commit** to apply the updates in Active Directory.
7. The preview pane will be updated with the progress as users are deprovisioned.

Viewing the provisioning and deprovisioning logs

When you begin the provisioning or deprovisioning process, a log file that tracks your provisioning actions is created, stored on the server until purged, and available to view in the client for troubleshooting purposes. For ease of management, the name of each log file is prefaced with the type of action (provisioning or deprovisioning), a date and time stamp, and a unique ID.

Once the existing log file reaches the maximum size of 16MB, a new log file is created.

To view the stored log entries

1. Click **Provisioning | View logs**.
2. Expand **Provisioning** or **Deprovisioning** to view the associated logs.
3. Select the required log to view the log message details.

Purging the logs

Once the log files are no longer required, you can manually purge them from the server. The log files are stored in the Active Administrator server logging folder (c:\ProgramData\Quest\Active Administrator\Provisioning\Logs). Each file is prefaced with the type of provisioning, date, time stamp, and a unique identifier. For example, Provisioning 1/12/2022 5:09:20 AM (ID: 3aectj6h-89b0-4456-V57F-840246184h8h6)

To purge the logs

- Browse to the logging folder in File Explorer, sort the file based on the name, and remove as needed.

3

Certificates

With the Certificates module, you can monitor and manage the certificates in your organization. This module enable you to view the certificates on a single computer, view all the certificates in your organization, and organize certificates into a virtual folder structure to ease management. Regardless of the view you choose, you can view, update, export, install, and remove certificates.

Using Certificate Management, you can organize certificates into a virtual folder structure, identify certificates that are about to expire and set up automatic email notifications. You can also see if certificates were deleted by system-provided tools, and you easily can reinstall the deleted certificate.

Using Certificate Authority, you can manage the Certificate Authority (CA) servers, the Active Directory Certificate Service (certsvc), and CA certificates within a selected forest. You can 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.

Using Certificate Repository, you can manage all the certificates you choose to add to the repository. You can sort the list to find the certificates that are about to expire, update the certificate, and install it on selected computers.

Using Certificate Search you can search for certificates based on a variety of search criteria. 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.

NOTE:

- The Certificates module is included with your Active Administrator base license.
- Users must have the Certificate Management and the Certificate Management Viewer roles enabled to manage certificates. For read-only access to the Certificate module, users require only the Certificate Management Viewer role. See Defining role-based access.

Topics

- Using the Certificates landing page
- Managing computers
- Updating the list of certificates
- Managing certificates
- Viewing certificate details
- Viewing the validation chain
- Sending email notifications
- Sending email notifications
- Reporting on certificates
- Exporting certificates
- Installing certificates
- Deleting certificates
- Managing Certificate Authority
- Using the Certificate Repository
- Searching certificates

Using the Certificates landing page

The landing page displays the active tiles for each computer in the section. The active tiles automatically update every 30 minutes, but you can use the icons to refresh the tiles at any time. You also can pause and resume the refresh of data. To customize the active tile refresh, see Setting general user options.

NOTE: After initial installation, the Certificates Management landing page is empty. You must add at least one computer to activate the landing page. See Adding computers.

To use the Certificates landing page

1 Click **Certificates**.

Active tiles indicate the number of certificates in each state.

Table 1. Certificate states

State	Description
Valid	Certificate is within the validate date ranges, has not expired, and has not been revoked.
Expires Soon	Certificate will expire soon.
Expired	Certificate has reached or surpassed its expiration date.
Revoked	Certificate has been revoked by the authority.
Parent Revoked	Certificate parent has been revoked by the authority.
Deleted	Certificate was deleted from the target computer.

2 Click an active tile to open the Certification Management window for the computer.

Managing computers

To view certificates on a computer, you must add the computer. When you first add a computer, it is synced when you choose to display the certificates. Only those computers that are managed by the Certificate module are monitored for certificates. Managed computers are monitored based on the schedule set on the **Certificate Configuration** page (see Setting certificate configuration). You can turn off the dynamic monitoring of managed computers and sync them manually.

Topics

- Adding computers
- Excluding stores
- Removing computers
- Disabling certificate management

To manage computers

1 Select **Certificate | Certificate Management**.

2 Click **Computers**.

3 Use the buttons to manage the list of computers.

Table 2. Computers to Manage Certificates options

Button	Description
Add	Add a computer to the list of managed computers. See Adding computers.
Remove	Remove the selected computers from the list of managed computers. See Removing computers.
Edit	Enable/disable the selected computer or edit the credentials on the selected computer. See Disabling certificate management and Adding computers.
Stores	Exclude selected stores on a specified computer from monitoring. See Excluding stores.
Test	Validate the connection to the selected computer.
Enable	Enable certificate management on the selected computers.
Disable	Disable certificate management on the selected computers. See Disabling certificate management.

Adding computers

To manage certificates on a computer, you must first add the computer. Only the computers listed in the **Available computers** list are monitored for certificate management.

To add computers to view certificates

1. Select **Certificate | Certificate Management**.
2. Click **Computers**.
3. Click **Add** to add new computers to the list.
4. To populate the **Available computers** list, choose between adding selected computers, loading computers from selected OUs or loading computers from selected groups. You can use a combination of these options to populate the list of computers.

   To add selected computers

   a. Select **Select Computers**.

   b. Type the fully qualified domain name (FQDN) of each computer you want to add, separated by semi colons.

   -OR-

   Browse and select one or more computers.

   c. Click **Add** to add the computers to the list of **Available computers**.

   d. Repeat as necessary to add the computers you need.

   To add computers in OUs

   a. Select **Select Organizational Units**.

   b. Type the name of each OU, separated by semicolons.

   -OR-

   Browse and select one or more OUs.

   NOTE: The OUs you select are added to the list of monitored OUs. You can add or remove OUs from the list of Monitored Objects once you complete this task. See Updating the list of certificates.

   NOTE: To reload the list of objects, click **Refresh**. All selections are cleared and any newly added OUs appear in the list.

c By default, nested OUs are included. To exclude nested OUs, clear the check box.

d By default, the OUs you selected are monitored for computers that are added or removed. To disable monitoring, clear the check box.

> **NOTE:** By default, OUs are monitored every 30 minutes to check for computers that are added or removed. To change the monitoring time, to add or remove OUs from monitoring, or to disable/enable monitoring, see Updating the list of certificates.

e Click **Add** to add the computers from the selected OUs to the list of **Available Computers**.

f Repeat as necessary to add the computers you need.

To add computers in Groups

a Select **Select Groups**.

b Type the name of each group, separated by semicolons.

-OR-

Browse and select one or more groups.

> **NOTE:** The groups you select are added to the list of Monitored Objects. You can add or remove groups from the list of Monitored Objects once you complete this task. See Updating the list of certificates.
>
> **NOTE:** To reload the list of objects, click **Refresh**. All selections are cleared and any newly added groups appear in the list.

c By default, nested groups are included. To exclude nested groups, clear the check box.

d By default, the groups you selected are monitored for computers that are added or removed. To disable monitoring, clear the check box.

> **NOTE:** By default, groups are monitored every 30 minutes to check for computers that are added or removed. To change the monitoring time, to add or remove groups from monitoring, or to disable/enable monitoring, see Updating the list of certificates.

e Click **Add** to add the computers from the selected groups to the list of **Available Computers**.

f Repeat as necessary to add the computers you need.

5 To manage the **Available computers** list, you can filter the list and remove computers you no longer need to monitor.

- To filter the list, start typing in the **Filter Computers** box. The list filters as you type.
- To remove selected computers from the list, click **Remove**.

6 By default, all stores in a selected computer are included. You can exclude selected stores from monitoring.

To exclude selected stores

a Select a computer.

b Click **Stores**.

You can filter the list of stores or use **Select all**/**Clear all** to manage the list.

c Clear the check boxes of the stores to exclude.

d Click **OK**.

e Click **Yes** to confirm the excluded stores.

7 By default, the Active Administrator® Foundation Service Credentials are used to retrieve certificates from the selected computers. If you want to specify a different account, clear the check box, and enter the username, or browse to select an account, and enter the password.

8 Click **OK**.

> **NOTE:** Active Administrator validates each computer, in the order they appear in the **Available computers** list. If you selected several computers and the process is taking too long or you are getting errors, you can cancel the process. Click **Cancel** in the progress bar, and click **Yes** to confirm. If you want to repeat the test, click **Test**.

9 Click **Close**.

10 To view the certificates, select the computer from the treeview. You can now select to create virtual folders to organize the certificates to ease their management. See Managing certificates.

Excluding stores

You can exclude selected stores on a specified computer from certificate monitoring.

To exclude stores

1 Select **Certificate | Certificate Management**.

2 Click **Computers**.

Filter the list, if necessary. Start typing in the **Filter computers** box. The list filters as you type.

3 Select a computer.

4 Click **Stores**.

Filter the list, if necessary. Start typing in the **Filter stores** box. The list filters as you type.

5 Clear the check boxes of the stores to exclude.

6 Use **Select all**/**Clear all** to manage the list.

7 Click **OK**.

8 Click **Yes** to confirm the excluded stores.

Removing computers

Removing a computer only removes it from Certificate Management. You can add it back at any time.

To remove computers

1 Select **Certificate | Certificate Management**.

2 Click **Computers**.

3 Filter the list, if necessary. Start typing in the **Filter computers** box. The list filters as you type.

4 Select the computers to remove.

5 Click **Remove**.

6 Click **Close**.

Disabling certificate management

You can disable or enable dynamic monitoring of certificates on selected computers. To disable or enable dynamic monitoring of certificate management entirely, see Setting certificate configuration.

If you disable dynamic monitoring of certificates, you can update the Active Administrator® database manually at any time by clicking **Sync** for a selected managed computer.

To disable certificate management on selected computers

1. Select **Certificate | Certificate Management**.
2. Click **Computers**.
3. Select the computers to disable.
4. Click **Disable**.
5. Click **Yes**.

   The icon next to the computers dims indicating that dynamic monitoring is disabled.

   NOTE: You also can disable a selected computer by clicking **Edit**, clearing the **Enabled** check box, and clicking **OK**.

6. Click **Close**.

   The computer remains in the selection list and the last synced display of certificates remains.

   - To sync the display manually, click **Sync**.

Managing monitored objects

You can monitor objects to check for computers that are added or removed. If monitoring is enabled, Active Administrator automatically adds newly discovered computers in the monitored OUs or groups to the Certificate Management window. If a computer is removed, it is automatically removed from the Certificate Management window, if computer removal is enabled.

When editing a monitored object, you can choose to enable/disable monitoring, include/exclude nested OUs or groups, enable/disable automatic removal of computers, or change the credentials used to monitor objects.

NOTE: Removing an OU or group from the list of Monitored Objects, does not automatically remove the computers in that OU or group from the Certificate Management window. Removing an OU or group only removes that OU or group from monitoring. To remove computers, see Removing computers.

To manage monitored objects

1. Select **Certificate | Certificate Management**.
2. Select **More | Monitored Objects**.
3. Use the buttons to manage the list of Monitored Objects.

   Table 3. Manage monitored objects

Option	Description
Add OU	Add OUs to the list of Monitored Objects. **NOTE:** To reload the list of objects, click **Refresh**. All selections are cleared and any newly added OUs appear in the list.
Add Group	Add groups to the list of Monitored Objects. **NOTE:** To reload the list of objects, click **Refresh**. All selections are cleared and any newly added groups appear in the list.
Edit	Edit a selected object. You can enable/disable monitoring, include nested OUs or groups, allow computers to be removed automatically, and change the credentials.
Remove	Remove selected objects from the list of Monitored Objects.
Refresh	Refresh the list of Monitored Objects from the Active Administrator database.

4. Change the monitoring interval, if desired. The default value is 30 minutes.

Click **Apply** to apply the changes and keep the dialog box open, or **OK** to save the changes and close the dialog box.

Managing certificates

The **Certificate Management** window displays the computers being managed by the Certificate module, the associated certificates and their state.

The menu at the top of this view enumerates and displays the number of valid, soon to expire, expired, revoked, parent revoked, and deleted certificates. The tree view, by default, displays the computers being managed with the Certificate module in your organization and all the associated certificates. From here, you can also select to create a virtual folder structure to help visually organize those certificates to facilitate their management.

The pane at the bottom of this view displays certificates that have been deleted using system-provided tools. You can restore the deleted certificate from the Active Administrator database or install the certificate on another computer.

NOTE:

- To manage certificates on a computer, you must first add the computer. See Adding computers.
- For full access to virtual folders you must have the Certificate Management role; for read only access, the Certificate Management Viewer role is required. See Defining role-based access.
- The virtual structure that you create will also be available for selection in your reports. See Reporting on certificates.
- You cannot move certificates from one computer's virtual folder to another computer's virtual folder.
- Deactivated computers are identified with a grayed out icon in the treeview.

To create a virtual folder structure

1. Select **Certificate | Certificate Management**.
2. Right-click **All Certificates** and select **Add Folder** to create a container that can include certificates from any computer in your organization that is being managed by the Certificated module.
3. Once you have the desired structure in place, you can begin the drag and drop the certificates in the required folder.

   The number of certificates in each folder will be displayed and updated as certificates are added.

   You can sort based on the Computer column to quickly see the computer associated with the certificates in the folder.
4. If required, right-click the virtual folder and select **Rename Folder** to edit the name of the folder.
5. If required, right-click the virtual folder and select **Remove Folder** to delete the folder when it is no longer required

To manage certificates

1. Select **Certificate | Certificate Management**.
2. Select the computer or virtual folder to view the certificates.
3. Select the certificate to be managed.

   - OR -

   Select multiple certificates to be managed by holding the Shift or Ctrl keys during selection.
4. Use the tool bar to manage the selected certificates. You also can right-click a certificate and select an option from the shortcut menu.

Table 4. Certificate Management tool bar

Option	Description
Computers	Manage the computers on which certificates are monitored. See Updating the list of certificates.
Sync	Refresh the Active Administrator database and the display with the certificates on a selected computer. See Updating the list of certificates.
Delete	Delete a certificate from a selected computer. Deleting certificates.
Install on	Install selected certificates on one or more computers. See Installing certificates.
Refresh	Refresh the display by pulling the contents of the Active Administrator database. See Updating the list of certificates.
More | Export	Export a selected certificate to a selected location, either from the list of certificates or a selected computer. See Exporting certificates.
More | Details	View the details of the selected certificate. You also can install the certificate on a computer, export the certificate, and view the validation chain. See Viewing certificate details.
More | Add to Repository	Add a selected certificate to the Certificate Repository. See Adding a certificate to the repository.
More | Validation Chain	View the validation chain of the selected certificate. See Viewing the validation chain.
More | Report	Create a certificates report to display in a report editor, to send in an email, or to save to a file. See Sending a report.
More | Report schedules	Edit, disable, or remove report certificate report schedules. See Managing report schedules.
More | Notifications	Exclude a selected certificate from being included in the certificates that support cryptography notification email. See Excluding certificates that support cryptography.
More | Revoke Notifications	Exclude a selected certificate from being included in the revoked certificate notification email. See Excluding revoked certificates
More | Monitored Objects	View the list of objects that are being monitored for computers that are added or removed. See Updating the list of certificates.
Group by	Group the list of certificates by stores or by the state of the certificate. See Grouping the list of certificates.

Updating the list of certificates

The displayed certificates are a reflection of the contents of the Active Administrator® database. The display updates automatically based on the synchronization schedule set in certificate configuration. See Setting certificate configuration.

- To refresh the display by pulling the contents of the Active Administrator database, click **Refresh**.
- To refresh the Active Administrator database and the display with the certificates on a selected computer, click **Sync**.

Sorting and filtering the list of certificates

- To sort the list of certificates, click in a column heading to toggle between ascending and descending order.
- To filter the list of certificates, start typing in the **Filter Certificates by Name** box. The display updates as you type.
- To remove the filter, click **X**.

Grouping the list of certificates

While viewing certificates for a selected computer, you can group the list of certificates by stores or by the state of the certificate.

- To group certificates, click **Group by | Store** or **Group by |State**.
- To remove the grouping, click **Group by | Remove Grouping**.

Viewing certificate details

While viewing the details of a certificate, you can install the certificate on a computer, export the certificate, and view the validation chain. You also can view details on certificates in the repository. See Viewing certificate details from the repository.

To view certificate details while viewing a selected computer

1. Select **Certificates | Certificate Management**
2. Select the computer or virtual folder to view the certificates.
3. Select a certificate, and select **More | Details**.

To manage the certificate

- To install the certificate on a selected computer, click **Install Certificate**. A wizard guides you through installing the certificate.
- To export the certificate, open the **Details** tab, and click **Copy to File**. A wizard guides you through exporting the certificate.
- To view the validation chain, open the **Certification Path** tab.

Viewing the validation chain

To view the validation chain while viewing a selected computer

1. Select **Certificates | Certificate Management**.
2. Select the computer or virtual folder to view the certificates.
3. Select a certificate, and select **More | Validation chain.**

To view the validation chain in certificate details

- See Viewing certificate details.

Sending email notifications

You can send email notifications when a certificate is about to expire, added, or deleted. You also can check for certificates that use a cryptographic hash algorithm. Some notifications apply only to Certificate Management, while others also apply to the Certificate Repository. See Setting certificate configuration.

Topics

- Excluding certificates that support cryptography
- Excluding revoked certificates

Excluding certificates that support cryptography

If notifications are enabled and a certificate supports the selected cryptographic hash algorithm, an email notification is sent. See Setting certificate configuration. You can exclude a selected certificate from being included in the notification.

To exclude a certificate from notification

1. Select **Certificates | Certificate Management**.
2. Select the computer or virtual folder to view the certificates.
3. Select a certificate, and select **More | Notifications.**
4. Select **Exclude from notification**.
5. Click **OK**.

To exclude a certificate in the repository from notification

1. Select **Certificates | Certificate Repository**.
2. Select a certificate, and click **Edit Certificate.**
3. Select **Exclude from notification**.
4. Click **OK**.

Excluding revoked certificates

By default, if a certificate is revoked, an email notification is sent. You can exclude a selected certificate from being included in the notification.

To exclude a certificate from revoked notification

1. Select **Certificates | Certificate Management**.
2. Select the computer or virtual folder to view the certificates.
3. Select a certificate, and select **More | Revoke notifications.**
4. Select the check box to exclude the certificate.
5. Click **OK**.

To exclude a certificate in the repository from revoked notification

1. Select **Certificates | Certificate Repository**.

2 Select a certificate, and click **Edit Certificate.**

3 Select **Exclude from revoke notification**.

4 Click **OK**.

Reporting on certificates

You can choose to create a certificates report to display in a report editor, to send in an email, or to save to a file. You also can report on certificates in the repository. See Reporting on certificates in the repository.

Topics

- Sending a report
- Managing report schedules

Sending a report

To send a certificates report by email or save to a file

1 Select **Certificates | Certificate Management**.

2 Select the computer or virtual folder to view the certificates.

3 Select **More | Report.**

4 Click **Next**.

5 Select the data to include in the report.

Table 5. Certificate report options

Option	Description
All Certificates	Select to include all certificates in the report.
Certificates that should be replaced	Select to include only the certificates that should be replaced.
Specified Certificates	Select to include only the specified certificates. • Valid • Expired • Will expire in • x days • Parent Revoked • Revoked • You can filter the certificates by hash. By default, all certificates that support the cryptographic hash algorithm are included. To include only a specific cryptographic hash algorithm, select the filter from the list.
Filter by computer	Select the computers to include in the report. To unselect all computers, clear the check box in the column heading. The computers available for selection must be included in the list of computers being managed for certificates. See Updating the list of certificates.
Filter by folder	Select the virtual folders to include in the report. See To create a virtual folder structure for details on creating the structure.

6 Click **Next**.

7 Click **Next**.

8 Choose to create a **Delivery report** that you can print or email, or to open an **Interactive** report in a report editor.

If you choose **Interactive**, go to step 13.

9 Create a schedule for the report if desired.

a Select **Enable Schedule**.

b Click **Update**.

c Set the schedule.

d Click **OK**.

NOTE: You can modify this schedule or disable its execution. See Managing report schedules.

10 Change the default report name if desired.

11 By default, the date and time are appended to the end of the file name. Clear the check box if you do not want the date and time appended to the file name.

12 By default, a PDF file is created. You can choose a different format.

13 You can send the report by email and save it to a file.

To send an email

a Click **Email**, if necessary.

b By default, the logged in account displays in the **Email Addresses** list. To add more recipients, click **Add**, type the email addresses, and click **OK**.

c Modify the default subject line if desired.

d Set the priority of the email.

To save the file to a folder

a Click **Save to Folder**.

b Click **Add**.

c Add a path to the location where you want to store the report file.

d Click **OK**.

14 Click **Next**.

15 Review the choices you made.

16 Click **Finish**.

If you chose Interactive, a report editor opens to display the report.

Managing report schedules

You can edit, disable, or remove report certificate report schedules. Disabling a report schedule retains the definition of the report schedule, so you can enable it when you need it.

1 Select **Certificates | Certificate Management**.

2 Select the computer or virtual folder to view the certificates.

3 Select **More | Report Schedules.**

4 Manage the list of schedules.

Table 6. Manage schedule options

Option	Description
Edit	Modify the selected schedule.
Disable	Disable the selected schedule.
Enable	Enable the selected schedule.
Remove	Delete the selected schedule.

5 Click **OK**.

Exporting certificates

You can export a certificate to a selected location. You also can export a certificate when viewing certificate details or from the repository. See Viewing certificate details and Exporting certificates from the repository.

To export a certificate while viewing a selected computer

1 Select **Certificate | Certificate Management**.

2 Select the computer or virtual folder to view the certificates.

3 Select certificate, and choose **More | Export**.

4 Select the location and type a name for the CER file.

5 Click **Save**.

Installing certificates

You can add a certificate to a selected computer, or select certificates to install on one or more computers. You can choose certificates from the list of the computer you are viewing or from the Certificate Repository. You also can install a certificate when viewing certificate details and from the Certificate Repository. See Viewing certificate details and Installing certificates from the repository.

To add a certificate to the computer you are viewing

1 Select **Certificate | Certificate Repository**.

2 Import a certificate into the Certificate Repository.

3 Select **Add Certificate t**o install a repository certificate on a computer.

4 Select the store in which to place the certificate.

5 If you selected to install a PFX (PKCS12) file, type the password.

6 Click **OK**.

7 Click **Refresh**.

To install certificates to one or more computers

1 Select **Certificate | Certificate Management**.

2 Select the computer or virtual folder to view the certificates, if necessary.

3 Select one or more certificate files, and click **Install on**.

4 Browse to locate a computer.

5 Click **Get Certificate Stores**.

6 Select the store in which to place the certificate.

7 If you selected to install a PFX (PKCS12) file, type the password.

8 To add the certificate(s) to an additional computer, click **Add**, and select a computer. Repeat for each computer you want to add to the list.

> **NOTE:** The selected certificate store must exist on all the additional computers you add. If the store is missing on a selected computer, you receive an error message during the validation process. You can cancel the validation process and click **Remove** to remove the selected computer from the list.

9 Click **OK**.

10 Click **Yes** to verify.

> **NOTE:** Active Administrator validates each computer and certificate before installing it. If you selected several computers and the process is taking too long or you are getting errors, you can cancel the process. Click **Cancel** in the progress bar, and click **Yes** to confirm.

Deleting certificates

Deleting a certificate from a selected computer removes the certificate from the selected computer only, and not from the repository. You also can delete certificates from the repository. See Deleting certificates from the repository.

To delete a certificate

1 Select **Certificate | Certificate Management**.

2 Select the computer or virtual folder to view the certificates.

3 Select a certificate, and click **Delete**.

4 Click **Yes**.

Managing 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.

Topics

- Viewing a Certificate Authority summary
- Adding a forest
- Searching Certificate Authority
- Managing Certificate Authority servers
- Viewing certificate templates
- Viewing events
- Configuring Certificate Authority notifications
- Viewing Certificate Authority backups
- Purging Certificate Authority backups

- Managing Purge History

Viewing a Certificate Authority summary

The **Summary** tab lists all the Certificate Authority servers found in the selected forest along with status of the Active Directory Certificate Service, and required Active Directory objects.

To view Certificate Authority servers and objects

1 Select **Certificate | Certificate Authority**.

2 Select a forest from the list in the tool bar. If you do not see a forest, click **Add forest**. See Adding a forest.

Table 7. Summary tab

Detail	Description
CA Servers	Lists the CA servers in the selected forest. Details include the FQDN of the CA server name, the CA type, time and date of the last backup, and the overall status. The icons indicate the status of the Active Directory Certificate Service (certsvc) and required Active Directory objects (CA, AIA, CDP, KRA, and Enrollment). Open the **Servers** tab for details. See Managing Certificate Authority servers.
NT Authentication Certificates Certificate Authorities (CA)	Displays the path and lists the certificates, including the expiration date, and key usages. Click a certificate to view details and to install the certificate.
Enrollment Services	Displays the name, path, number of templates, and lists the certificates, including the expiration date, and key usages. Click a certificate to view details and to install the certificate.
Authority Information Access (AIA)	Displays the path and lists the certificates, including the expiration date, and key usages. Click a certificate to view details and to install the certificate.
CLR Distribution Point (CDP)	Displays the name and path of the CLR Distribution Points.
Recovery Agents (KRA)	Displays the name and path of the Key Recovery Agents.

Adding a forest

Active Administrator® manages all Certificate Authority (CA) certificates in a forest.

To add a forest

1 Select **Certificate | Certificate Authority**.

2 Click **Add Forest**.

3 The CA management for the forest is enabled by default.

> **NOTE:** Once you add a forest, you can disable the forest to remove it temporarily from CA management. Click **Edit forest** and clear the check box. To remove the forest permanently, click **Remove forest**.

4 Search caching is enabled by default. If enabled, Active Administrator searches the cache based on the configuration selected in **Configuration | Certificate Authority**. See Configuring certification authority.

> **NOTE:** The search caching feature must be enabled in **Configuration | Certificate Authority**.

To override the cache setting and always search Active Directory for this forest, clear the check box.

5 Set the maximum number of events in hours to return in the search results. The default value is 48 hours of events.

6 By default, server backup is enabled for the forest. Enter the password for the account used to perform the backup. To disable backups, clear the check box.

7 By default the Active Administrator Foundation service (AFS) account is used to access the forest. To use a different account, select **Specify account** and enter the user name and password for the account.

> **NOTE:** The specified account must have the rights to read the server configuration settings from the registry and to run backups.

8 Click **OK**.

Searching Certificate Authority

The Active Administrator® Certificate Authority Search feature finds users and computers that have certificates issued by Active Directory® Certificate Authority and published into Active Directory. From the search results, you can view certificate details.

To search certificate authority

1 Select **Certificate | Certificate Authority**.

2 Select a forest from the list in the tool bar. If you do not see a forest, click **Add forest**. See Adding a forest.

3 Open the **Search** tab.

4 Select a search type.

Search type	Description
User	Search for users who have certificates issued by Active Directory Certificate Authority.
Computer	Search for computers that have certificates issued by Active Directory Certificate Authority.
Templates	Search the Template field of certificates issued by Active Directory Certificate Authority for both users and computers.
Issuer	Search the Issuer field of certificates issued by Active Directory Certificate Authority for both users and computers.
Key Usage	Search the Key Usage field of certificates issued by Active Directory Certificate Authority for both users and computers.
Objects without certificates	Search for all users or computers that do not have certificates issued by Active Directory Certificate Authority.

5 By default, the cache is searched. To search Active Directory, clear the **Use search cache** check box.

> **NOTE:** The search cache is not available when the **Objects without certificates** search type is selected. To configure the search cache, see Configuring certification authority.

6 Select the domain to search. Searching **All Domains** is the default.

7 Select a filter from the list.

8 Depending on which search type you chose, browse to locate the user, computer, template, issuer, or key usage to search.

If you selected the **Objects without certificates** search type, select either users or computers to search.

9 Click **Search**.

The search results display the number of certificates found.

10 Double-click a result to view the certificates. Select a certificate, and click **View Certificate** to see details and to install the certificate.

Managing Certificate Authority servers

You can view and manage each Certificate Authority server found in the selected forest. In this tab, 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.

To manage a Certificate Authority server

1 Select **Certificate | Certificate Authority**.

2 Select a forest from the list in the tool bar. If you do not see a forest, click **Add forest**. See Adding a forest.

3 Open the **Servers** tab.

- For each server, you can **Start**/**Stop**/**Restart** the Active Directory Certificate Service.
- To open the Microsoft Management Console (MMC) for a server, click **Manage**.
- To back up the selected server, click **Backup**. See Viewing Certificate Authority backups.

Viewing certificate templates

You can view all the certificate templates found in the selected forest.

To view certificate templates

1 Select **Certificate | Certificate Authority**.

2 Select a forest from the list in the tool bar. If you do not see a forest, click **Add forest**. See Adding a forest.

3 Open the **Templates** tab.

- To view details, double-click a template.
- To search for templates, start typing in the **Search template names** box. The list filters as you type.
- To sort the templates, click in a column header.

Viewing events

The **Events** tab displays events for a selected Certificate Authority (CA) server. Events are separated into processing events and all server events.

To view Certificate Authority events

1 Select **Certificate | Certificate Authority**.

2 Select a forest from the list in the tool bar. If you do not see a forest, click **Add forest**. See Adding a forest.

3 Open the **Events** tab.

4 Select a Certificate Authority server.

- The first scrollable list displays events related to Active Directory Certificate Services Request (Enrollment) Processing where the request was denied and other request processing issues.
- The second scrollable list displays all CA server events.
- To view details, double-click an event.
- The number of hours returned is set in the forest settings dialog. See Adding a forest.

- To sort the list, click a column header.

Configuring Certificate Authority notifications

Various services make use of certificate authority. You can configure Active Administrator to monitor those services and email notifications when particular services are running or stopped.

NOTE: By default, services are monitored every 10 minutes to check for state changes. To change the monitoring time, use Configuration | Certificate Configuration | Certificate Authority. For more information, see Configuring certification authority.

To configure Certificate Authority notifications

1. Select **Certificate | Certificate Authority**.
2. Select a forest from the list in the tool bar. If you do not see a forest, click **Add forest**. See Adding a forest.
3. Click **Notification Options**.
4. Select a notification preference.
   - Do not send notifications
   - Send notification when the service has entered into a running state
   - Send notification when the service has entered into a stopped state
   - Send notification when the service enters into either a stopped or running state
5. Select the services to monitor.
6. Optionally, click **Add** to add an email address to receive notifications, enter the email address, and click **OK** to save the recipient.

   - OR -

   Optionally, select an email address, click **Edit** to change the address, and click **OK** to accept the changes.

   - OR -

   Optionally, select an email address and click **Remove** to remove the recipient.
7. Click **OK**.

Viewing Certificate Authority backups

The Certificate Authority servers are backed up every 24 hours. You also can manually backup a server. See Managing Certificate Authority servers. Backup files are saved for 30 days. Use certutil.exe to restore the backup.

To view Certificate Authority backups

1. Select **Certificate | Certificate Authority**.
2. Select a forest from the list in the tool bar. If you do not see a forest, click **Add forest**. See Adding a forest.
3. Open the **Backups** tab.

   The backups are organized by Certificate Authority server. Double-click a backup to obtain the path to and name of the backup file. Use certutil.exe to restore the backup.

Purging Certificate Authority backups

The Certificate Authority backup files are saved for 30 days. See Viewing Certificate Authority backups. If the files need to be deleted more frequently, a purge of backup files can be scheduled or performed manually.

To schedule a purge of Certificate Authority backups

1. Select **Certificate | Certificate Authority**.
2. Click **Backup Purging**.
3. Select **Purge Schedule**.
4. Optionally, select **Enable scheduled purging**.
5. Optionally, change the number of days of Certificate Authority backups to keep.
6. Optionally, click **Update** to change the displayed schedule.
7. Click **Save**.

To manually purge Certificate Authority backups

1. Select **Certificate | Certificate Authority**.
2. Click **Backup Purging**.
3. Select **Purge Schedule**.
4. Optionally, change the number of days of Certificate Authority backups to keep.
5. Click **Purge Now.**
6. Click **Yes** to confirm the purge.

Managing Purge History

When Certificate Authority backups are purged on a schedule or manually, the purge history is stored and displayed on the Purge History tab. See Purging Certificate Authority backups. The purge history can be cleared.

To manage Purge History

1. Select **Certificate | Certificate Authority**.
2. Select a forest from the list in the tool bar. If you do not see a forest, click **Add forest**. See Adding a forest.
3. Open the **Purge History** tab to display the details related to purged Certificate Authority backups.
4. Optionally click **Clear History** to remove the purge history.

Using the Certificate Repository

The Certificate Repository provides a central location to store certificates. From the repository, you easily can install selected certificates on computers in your organization. In the repository, certificates (.CER files) and PFX (PKCS12) files (.PFX) are separated on different tabs.

Topics

- Adding a certificate to the repository
- Viewing certificate details from the repository
- Installing certificates from the repository
- Updating certificates in the repository
- Reporting on certificates in the repository
- Exporting certificates from the repository
- Deleting certificates from the repository

Adding a certificate to the repository

You can add a certificate directly to the repository, or while you are viewing the certificates on a selected computer.

To add a certificate directly to the repository

1. Select **Certificate | Certificate Repository**.
2. Open the **Certificates** tab for .CER files.

   -OR-

   Open the **PFX** tab for .PFX files.
3. You can add a certificate from a file or from a URL.

   To add a certificate from a file:

   a. To add a .CER file, select **Add Certificate | Add Certificate from File**.

      -OR-

      To add a .PFX file, click **Add PFX**.

   b. Locate the certificate.

   c. Click **Open**.

   To add a certificate from a URL:

   a. Select **Add Certificate | Add Certificate from URL**.

   b. Enter the HTTPS URL and the number of the port of the resource from where to import the certificate. Example: https://address.com with port 443.

   c. If the resource requires authentication, select the check box, and enter the username and password.

   d. Click **OK**.

To add a certificate while you are viewing a selected computer

1. Select **Certificate | Certificate Management**.
2. Select a computer.
3. Select a certificate, and click **More | Add to Repository**.

Viewing certificate details from the repository

While viewing the details of a certificate in the repository, you can install the certificate on a computer, export the certificate, and view the validation chain.

To view certificate details from the repository

1. Select **Certificates | Certificate Repository**.
2. Open the **Certificates** tab for .CER files.

   -OR-

   Open the **PFX** tab for .PFX files.
3. Select a certificate, and click **Details**.

To manage the certificate

- To install the certificate on a selected computer, click **Install Certificate**. A wizard guides you through installing the certificate.

- To export the certificate, open the **Details** tab, and click **Copy to File**. A wizard guides you through exporting the certificate.
- To view the validation chain, open the **Certification Path** tab.

Installing certificates from the repository

To install certificates to selected computers

1. Select **Certificate | Certificate Repository**.
2. Open the **Certificates** tab for .CER files.

   -OR-

   Open the **PFX** tab for .PFX files.
3. Select one or more certificate files, and click **Install on**.
4. Browse to locate a computer.
5. Click **Get Certificate Stores**.
6. Select the store in which to place the certificate.
7. If you selected to install a PFX (PKCS12) file, type the password.
8. To add the certificate(s) to an additional computer, click **Add**, and select a computer. Repeat for each computer you want to add to the list.

   NOTE: The selected certificate store must exist on all the additional computers you add. If the store is missing on a selected computer, you receive an error message during the validation process. You can cancel the validation process and click **Remove** to remove the selected computer from the list.
9. Click **OK**.
10. Click **Yes** to verify.

    NOTE: Active Administrator® validates each computer and certificate before installing it. If you selected several computers and the process is taking too long or you are getting errors, you can cancel the process. Click **Cancel** in the progress bar, and click **Yes** to confirm.

Updating certificates in the repository

Certificates in the repository are not updated automatically.

To update a certificate in the repository

1. Select **Certificate | Certificate Repository**.
2. Open the **Certificates** tab for .CER files.

   -OR-

   Open the **PFX** tab for .PFX files.
3. Select a certificate, and click **Edit Certificate**.
4. To update the certificate, click **Update**.
5. Locate the file, and click **Open**.
   - You can edit the **Installed On**, **Location**, **Contact Number**, and **Comments** fields.
   - To exclude the certificate from notification, select the appropriate check box.
6. Click **OK**.

Reporting on certificates in the repository

You can choose to create a certificates report to display in a report editor, to send in an email, or to save to a file.

To send a certificates report by email or save to a file

1 Select **Certificates | Certificate Repository**.

2 Click **Report.**

3 Select the data to include in the report.

Table 8. Certificate Repository report options

Option	Description
All Certificates	Select to include all certificates in the report.
Certificates that should be replaced	Select to include only the certificates that should be replaced.
Specified Certificates	Select to include only the specified certificates. • Valid • Expired • Will expire in • x days • Parent Revoked • Revoked • You can filter the certificates by hash. By default, all certificates that support the cryptographic hash algorithm are included. To include only a specific cryptographic hash algorithm, select the filter from the list.

4 Change the default report name if desired.

5 By default, the date and time are appended to the end of the file name. Clear the check box if you do not want the date and time appended to the file name.

6 By default, a PDF file is created. You can choose a different format.

7 You can send the report by email and save it to a file.

To send an email

a Click **Email**, if necessary.

b By default, the logged in account displays in the Email Addresses list. To add more recipients, click **Add**, type the email addresses, and click **OK**.

c Modify the default subject line if desired.

d Set the priority of the email.

To save the file to a folder

a Click **Save to Folder**.

b Click **Add**.

c Add a path to the location where you want to store the report file.

d Click **OK**.

8 Click **OK**.

To generate a certificates report and display in a report editor

1. Select **Certificates | Certificate Repository**.
2. Click **Report.**
3. Select **Interactive**.
4. Click **OK**.

Exporting certificates from the repository

You can export a certificate to a selected location from the Certificate Repository. You also can export a certificate when viewing certificate details. See Viewing certificate details from the repository.

To export a certificate from the repository

1. Select **Certificate | Certificate Repository**.
2. Open the **Certificates** tab for .CER files.

   -OR-

   Open the **PFX** tab for .PFX files.
3. Select a certificate.
4. Click **Export**.
5. Select the location and type a name for the file.
6. Click **Save**.

Deleting certificates from the repository

Deleting a certificate from the repository removes the certificate from the repository only and not from the computers on which it is installed.

To delete a certificate

1. Click **Certificate | Certificate Repository**.
2. Open the **Certificates** tab for .CER files.

   -OR-

   Open the **PFX** tab for .PFX files.
3. Select a certificate, and click **Delete**.
4. Click **Yes**.

Searching certificates

The Certificate Search feature enables you to search for certificates in three different sources: computers managed by Active Administrator, certificate stores in selected computers, and the Certificate Repository. The New Certificate Search wizard helps you easily create a search based on multiple search values and criteria. You can save, edit, and delete certificate search definitions.

Topics

- Searching for certificates

- Creating a new certificate search definition
- Editing a certificate search definition
- Deleting a certificate search definition

Searching for certificates

To search for certificates

1 Select **Certificate | Certificate Search**.

2 Select a search from the list.

If you do not see a search that fits your needs, create a new search definition. See Creating a new certificate search definition.

3 Click **Search**. The search results display.

- To filter the list by certificate name, start typing in the **Filter Certificates Names** box. The list filters as you type.
- To sort a column, click the column header.

4 Use the tool bar to manage certificates. You also can right-click a certificate and select an option from the shortcut menu.

Table 9. Certificate search results tool bar

Option	Description
Add to Repository	Add a selected certificate to the Certificate Repository. **NOTE:** Not available when the source of the search is the Certificate Repository.
View Details	View the details of the selected certificate. You also can install the certificate on a computer, export the certificate, and view the validation chain. See Viewing certificate details.
Export	Export a selected certificate to a selected location, either from the list of certificates or a selected computer. See Exporting certificates.
Validation Chain	View the validation chain of the selected certificate.
Install on	Install selected certificates on one or more computers. See Installing certificates.

Creating a new certificate search definition

You also can use an existing certificate search definition to create a new certificate search definition. See Editing a certificate search definition

To create a new search definition

1 Select **Certificate | Certificate Search**.

2 Click **New**.

3 Click **Next** on the welcome screen.

4 Choose the source to search for certificates. You can search managed computers, certificate stores on selected computers, or the Active Administrator certificate repository.

5 Click **Next**.

- If you search managed computers, select the managed computers to search. By default all managed computers are selected.

- If you search certificate stores, click **Add** and add computers to the list. See Adding computers.

6 Create the certificate search filter by selecting the values to search on and the criteria. Search by name, subject, issued to and by, effective date, expiration date, expired, key usage, revoked, serial number, thumbprint, store, and signature algorithm.

> **NOTE:** Multiple search filter values are evaluated using the OR condition. Wildcards, such as * and ?, are not supported.

7 Click **Next**.

8 Review the selections you made. You can select to save the search for future use. Enter a name for the search.

> **NOTE:** If you do not save the search, the search is saved anyway as **Temp-*n* (unsaved)** until you restart the Active Administrator Console or delete the search. If you choose to save the temporary search definition, click **Edit**, and advance the wizard to the page where you can enter a name for the search definition.

9 Click **Next**.

10 Click **Finish**.

The search proceeds automatically and the results display. See Searching for certificates.

Editing a certificate search definition

You can edit a certificate search definition to change the search criteria or add/remove computers from the list. You also can use an existing certificate search definition to create a new certificate search definition.

To edit a certificate search definition

1 Select **Certificate | Certificate Search**.

2 Select a search from the list.

3 Click **Edit**.

4 Make desired changes to the search definition.

On the **Summary and Save** page, you can change the name of the search definition to create a new search definition.

5 When you click **Finish**, click **Yes** to refresh the results with the new search definition.

Deleting a certificate search definition

Temporary certificate search definitions are deleted automatically when you exit the Active Administrator Console.

To delete a certificate search definition

1 Select **Certificate | Certificate Search**.

2 Select a search from the list.

3 Click **Delete**.

4 Click **Yes** to confirm.

4

Security & Delegation

Manage Active Directory® security and delegation. Create Active Templates to apply permissions easily to users, groups, and organizational units. Manage dormant user and computer accounts. Set up reminders to send when passwords are about to expire and notifications to send when accounts are set to expire.

Topics

- Using the Security & Delegation landing page
- Managing security
- Monitoring user logon activity
- Managing locked out accounts
- Managing password policies
- Checking delegation status
- Managing Active Templates
- Managing inactive accounts
- Sending password reminders
- Sending account expiration notifications
- Viewing expired accounts
- Purging account history

Using the Security & Delegation landing page

The landing page displays the active tiles for each feature in the module. The active tiles automatically update every 30 minutes, but you can use the icons to refresh the tiles at any time. You also can pause and resume the refresh of data. To customize the active tile refresh, see Setting general user options.

To use the Security & Delegation landing page

1. Click **Security & Delegation**.
2. To access the features in this section, click an active tile or choose from the tree.
   - **Security** (See Managing security.)
   - **User logon activity** (See Monitoring user logon activity.)
   - **Locked out accounts** (See Managing locked out accounts.)
   - **Active Templates** (See Managing Active Templates.)
   - **Password policies** (See Managing password policies.)
   - **Delegation status** (See Checking delegation status.)

- **Inactive accounts** (See Managing inactive accounts.)
- **Change password reminders** (See Sending password reminders.)
- **Account expiration notifications** (See Sending account expiration notifications.)
- **Purge inactive accounts** (See Purging account history.)

Managing security

The main permissions display in Active Administrator® provides extended information in addition to the general rights that are visible in the built-in tools. You also can enable/disable accounts and reset passwords.

Topics

- Managing Active Directory objects
- Viewing Active Directory objects by type
- Reporting on Active Directory objects by type
- Viewing native permissions
- Viewing Active Template delegations
- Resetting passwords
- Resetting computers
- Moving Active Directory objects
- Managing group memberships
- Reporting on Active Directory objects

Managing Active Directory objects

The Active Directory® containers and objects are listed in a tree in the left pane. You can drill down in the tree and view details in the top right pane.

To drill down and view details

1 Click **Security & Delegation | Security**.

2 Select a domain controller, if necessary.

> **NOTE:** Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3 Use the tool bar to manage Active Directory objects. The options on the tool bar change depending on the object selected.

> **NOTE:** You can perform some options on multiple selected items. Options that cannot be performed on multiple selected items are unavailable. If different types of items are selected, only options that can be performed to all selected types are available.

Table 10. Security tool bar

Option	Description
Refresh	Refresh the display.
Refresh Container	Refresh the selected container.

Table 10. Security tool bar

Option	Description
Properties	Edit the properties of the selected container.
View	View and report on all users, groups, organization units, or computers. See Viewing Active Directory objects by type and Reporting on Active Directory objects by type.
New	Add a new computer, contact, group, organizational unit, printer, shared folder, or user.
Delete	Delete the selected objects.
Permissions	Manage native permissions. See Viewing native permissions.
Delegations	Manage Active Template delegations. See Viewing Active Template delegations.
More | Rename	Rename the selected object.
More | Add to Group	Add selected accounts to a group. See Managing group memberships.
More | Unlock	Unlock the selected accounts. See Resetting passwords.
More | Reset Password	Reset the password on the selected account. See Resetting passwords.
More | Reset Computer	Reset the password on selected computers. See Resetting computers.
More | Manage Computer	Opens the Microsoft® Computer Management Console.
More | Move	Move selected Active Directory objects to another container. See Moving Active Directory objects. **NOTE:** To test the move, you might want to run a simulation. See Modeling GPO changes.
More | Disable More | Enable	Disable or enable the selected accounts. The icon for an enabled account is blue. If an account is disabled, the icon is gray. **NOTE:** There is no confirmation for the process.
More | Group Members	Manage the list of users in the selected group. See Managing group memberships. **NOTE:** If the Forest functional level is Windows Server® 2016 or Windows Server 2019, and the Privileged Access Management Feature is enabled for the forest, you can change the Time-to-Live (TTL) value for selected group members.
More | Group Membership Wizard	Opens the Group Membership Wizard where you can add multiple members to selected groups. See Managing group memberships.

Viewing Active Directory objects by type

You can view all Active Directory® objects of a specific type within a container and its subcontainers. You can choose to view all users, groups, organizational units, or computers. Within each view, you can customize the display by selecting the columns of interest to you. When viewing users, you can filter the list by entering criteria for selected columns. You can display the list as a report that you can view or print, or you can schedule a report to run at the time of your choosing.

To view Active Directory objects by type

1 Click **Security & Delegation | Security**.

2 Select a domain controller, if necessary.

> **NOTE:** Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3 Select a container, click **View**, and choose a type to view.

4 Use the tool bar to manage the list that displays.

Table 11. View objects tool bar

Option	Description
Back	Return to the previous display.
Refresh	Refresh the display.
Stop	Stop loading of objects if the process is taking too long.
Report List	Display the list as a report that you can view or print. **NOTE:** Any applied filters to the user list will affect the report.
Export	Export the list to a .csv or .txt file. **NOTE:** Any applied filters to the user list will affect the export file. **NOTE:** To export only selected columns, click **Column**, select the columns to exclude from the export, and click **OK**.
LDAP Path	Display the path to the selected object.
	Move the selected object to a different container. See Moving Active Directory objects.
Columns	Select the columns you want to display or export. By default, all columns are selected.
Filter	Filter the list of users. There is a filter for each column. • To clear a filter, click **Filter**, click **Clear**, and click **OK**.
Schedule	Schedule a report for the selected object. See Reporting on Active Directory objects by type.

Reporting on Active Directory objects by type

You can generate and schedule reports for all Active Directory® objects of a specific type within a container and its subcontainers. When viewing users, you can filter the list by entering criteria for selected columns. You can display the list as a report that you can view or print, or you can schedule a report to run at the time of your choosing.

To generate a report and display in a report editor

1 Click **Security & Delegation | Security**.

2 Select a domain controller, if necessary.

> **NOTE:** Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3 Select a container, click **View**, and choose a type to view.

When viewing users, you can filter the list by entering criteria for selected columns.

4 Click **Report List**.

To schedule a report to send by email or to save to a file

1 Click **Security & Delegation | Security**.

2 Select a domain controller, if necessary.

> **NOTE:** Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3 Select a container, click **View**, and choose a type to view.

4 Click **Schedule.**

5 By default, the report schedule is enabled. To disable the schedule, clear the check box.

6 By default, selected filters are not applied to the report. To override the selected filters, select the check box.

7 Change the default report name if desired.

8 By default, the date and time are appended to the end of the file name. Clear the check box if you do not want the date and time appended to the file name.

9 By default, a PDF file is created. You can choose a different format.

10 You can send the report by email and save it to a file.

To send an email

a Click **Email**, if necessary.

b By default, the logged in account displays in the Email Addresses list. To add more recipients, click **Add**, type the email addresses, and click **OK**.

c Modify the default subject line if desired.

d Set the priority of the email.

To save the file to a folder

a Click **Save to Folder**.

b Click **Add**.

c Add a path to the location where you want to store the report file.

d Click **OK**.

11 Click **Set Schedule**, set the schedule for the report, and click **OK**.

12 Click **OK**.

The scheduled report is added to the list of scheduled reports.

- To edit a selected report schedule, click **Edit**.
- To delete selected report schedules, click **Remove**.

Viewing native permissions

The **Native Permissions** area displays the permissions for the selected user, computer, or organization unit. You can sort the columns in ascending or descending order.

Topics

- Setting the owner
- Managing native permissions
- Removing propagation

To view native permissions

1 Click **Security & Delegation | Security**.

2 Select a domain controller, if necessary.

> **NOTE:** Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3 Select a container or object.

4 Drill down to the desired object to view the permissions in the **Native Permissions** area.

You can set the owner, manage the displayed permissions, and disallow propagation.

Setting the owner

To set the owner

1 Click **Security & Delegation | Security**.

2 Select a domain controller, if necessary.

> **NOTE:** Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3 Select a container or object.

4 Drill down to the desired object to view the permissions in the **Native Permissions** area.

5 Click **Set Owner**.

6 Browse to select a new owner.

7 Choose to recurse across subfolders, if desired.

8 Click **OK**.

Managing native permissions

You can show or hide inherited and default permissions on the display, view properties on a selected account, modify permissions, or delete permissions.

To manage native permissions

1 Click **Security & Delegation | Security**.

2 Select a domain controller, if necessary.

> **NOTE:** Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3 Select a container or object.

4 Drill down to the desired object to view the permissions in the **Native Permissions** area.

5 Use the **Permissions** menu to manage native permissions.

Table 12. Native permissions menu

Option	Description
Hide Inherited Show Inherited	Hide or show inherited permissions in the list.
Hide Defaults Show Defaults	Hide or show default permissions in the list.
View Account Properties	Open the properties for the selected account.
Modify Permissions	Open the security tab of the properties for the selected account.

Table 12. Native permissions menu

Option	Description
Delete Permissions	Delete the selected permissions.
Create Active Template	Create a new Active Template. See Creating an Active Template.

See Viewing native permissions.

Removing propagation

IMPORTANT: Removing the inherited permissions from an object may also remove permissions from child objects.

To remove inheritable permission propagation

1. Click **Security & Delegation | Security**.
2. Select a domain controller, if necessary.

   NOTE: Use the icons to manage the selected managed domain controller. See Managing domain controllers.
3. Select a container or object.
4. Drill down to the desired object to view the permissions in the **Native Permissions** area.
5. In the **Native Permissions** area, clear the **Allow inheritable permissions from parent to propagate to this object** check box.
6. Choose an option.
   - To copy previously inherited permissions to the object, click **Copy**.
   - To remove the inherited permissions and keep only the explicit permissions on the object, click **Remove**.

To re-establish propagation

- In the **Native Permissions** area, select the **Allow inheritable permissions from parent to propagate to this object** check box.

Viewing Active Template delegations

For more information on Active Templates, see Managing Active Templates.

To view Active Template delegations

1. Click **Security & Delegation | Security**.
2. Select a domain controller, if necessary.

   NOTE: Use the icons to manage the selected managed domain controller. See Managing domain controllers.
3. Click **Active Template Permissions**.
4. Select a container or object to view delegations in the **Active Template Permissions** area.
5. Use the **Delegations** menu to manage Active Template permissions.

Table 13. Delegations menu

Option	Description
New Delegation	Create a new delegation. See Adding a delegation link. You also can right-click an object in the tree and choose **Add Delegation**. **NOTE:** Delegation in the Configuration partition in the tree is disabled by default. To enable delegation in the Configuration partition, you must enable it in User Settings. See Setting general user options.
Edit Delegation	Edit the selected delegation.
Copy Delegation	Copy the selected delegation to create a new delegation.
Remove Delegation	Remove the selected delegation.
View Account Properties	Open the properties for the selected account.
View Container Properties	Open the properties for the container for the selected account.

Resetting passwords

You can reset the password on a user account. When resetting the password, you can choose to unlock the account. You also can unlock the account without resetting the password by selecting **More | Unlock**.

To reset the password on a user accounts

1. Click **Security & Delegation | Security**.
2. Select a domain controller, if necessary.

   NOTE: Use the icons to manage the selected managed domain controller. See Managing domain controllers.
3. Drill down to locate the user account.
4. Select the user account, and click **More | Reset Password**.
5. Type the new password.
6. By default, the user must change their password at the next logon.
7. To unlock the account, select the check box.
8. Click **OK**.

Resetting computers

You can reset the account password on computers locally. The change is written to the computer account object on the domain controller that resides in the same domain. Active Directory replication is initiated so that other domain controllers receive the change.

To reset the password on a computer

1. Click **Security & Delegation | Security**.
2. Select a domain controller, if necessary.
3. Drill down to locate the computers.
4. Select one or more computers, and click **More | Reset Computer**.
5. Click **Yes** to reset the computers.

Moving Active Directory objects

You can move a selected Active Directory® object to another container.

To move Active Directory objects

1. Click **Security & Delegation | Security**.
2. Select a domain controller, if necessary.

   NOTE: Use the icons to manage the selected managed domain controller. See Managing domain controllers.
3. Select objects.
4. Select **More | Move**.
5. Select the container.
6. Click **OK**.

Managing group memberships

You have a variety of methods to manage group memberships. You can add members to a selected group, add a selected account to a group, or use a wizard to add multiple accounts to multiple selected groups.

NOTE: If the Forest functional level is Windows Server® 2016 or Windows Server 2019, and the Privileged Access Management Feature is enabled for the forest, you can set the Time-to-Live (TTL) value for selected group members.

Topics

- Adding members to a selected group
- Adding selected accounts to a group
- Adding multiple accounts to selected groups

Adding members to a selected group

To add members to a selected group

1. Click **Security & Delegation | Security**.
2. Select a domain controller, if necessary.

   NOTE: Use the icons to manage the selected managed domain controller. See Managing domain controllers.
3. Select a group.
4. Select **More | Group Members**.
5. Use the tool bar to manage the group membership.

   Table 14. Group Members options

Option	Description
Add	Add accounts to the group.
Remove	Remove accounts from the group.

Table 14. Group Members options

Option	Description
Change TTL	Change the Time-to-Live (TTL) value of a selected group member. **NOTE:** The Forest functional level must be Windows Server® 2016 or Windows Server 2019, and the Privileged Access Management Feature must be enabled for the forest. **NOTE:** You also can change the TTL value on the **Member of** tab when modifying user properties.
Refresh TTL	Refresh the TTL of the listed group members.

6 Click **OK**.

Adding selected accounts to a group

To add selected accounts to group

1 Click **Security & Delegation | Security**.

2 Select a domain controller, if necessary.

> **NOTE:** Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3 Select accounts.

4 Select **More | Add to group**.

5 Select a group.

6 Click **OK**.

Adding multiple accounts to selected groups

To add multiple members to selected groups

1 Click **Security & Delegation | Security**.

2 Select a domain controller, if necessary.

> **NOTE:** Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3 Select **More | Group Membership Wizard**.

4 Click **Next**.

5 On the **Groups** page, select one or more groups. To add a group to the list, click **Add**.

6 Click **Next**.

7 On the **Members** page, select one or more accounts.

- To add an account, click **Add**.
- To change the TTL of a selected account, click **Change TTL**.

8 Click **Next**.

9 Review the selections, and click **Finish**.

Reporting on Active Directory objects

There are four reports from which to choose. You can export any report to a PDF, HTML, MHT, RTF, Excel, CSV, Text, or Image file.

To run a report on Active Directory® objects

1 Click **Security & Delegation | Security**.

2 Select a domain controller, if necessary.

> **NOTE:** Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3 Right-click an object or container, point to **Reports**, and choose a report.

Table 15. Active Directory reports

Report	Description
Object Class Summary	Lists the number of objects in a particular class in the selected container and all subcontainers.
Groups with Temporary Members	Lists the groups with users who are assigned a Time-to-Live (TTL) value. The temporary members are listed with the assigned TTL value. **NOTE:** The Forest functional level must be Windows Server® 2016 or Windows Server 2019, and the Privileged Access Management Feature must be enabled for the forest.
Delegated Permissions	Lists delegated permissions for the object and all child objects.
Active Templates Delegated Permissions	Lists the Active Template applied to the selected object.
Active Templates Delegated Permissions with Details	Lists the Active Templates, with permissions and accounts, applied to the selected object.

Monitoring user logon activity

To see user logon activity, you must set up workstation logon auditing and set the options for what type of activity to capture. See Setting up workstation logon auditing and Setting user log on activity.

To monitor user logon activity

1 Click **Security & Delegation | User Logon Activity**.

The display is based on the chosen settings. See Setting user log on activity.

You can sort the columns or filter the list.

- To sort the columns, click the column heading to toggle between ascending and descending.
- To filter the list, start typing in the box.

2 Use the tool bar to manage the user logon activity.

Table 16. User Logon Activity tool bar

Option	Description
Refresh	Refresh the display.
Logon Details	View details about a selected logon event.
Find User	Find a specific user.

Table 16. User Logon Activity tool bar

Option	Description
Disable Account Enable Account	Disable or enable a user account.
Enable Auto Updates Disable Auto Updates	Disable or enable automatic updates to the display. If you disable auto updates, click **Refresh** to update the display.

Managing locked out accounts

For domains you choose to monitor, you can view, research, and resolve locked out accounts. You can view the reason that account is locked and locate the locked out account in Active Directory®. Based on your research, you can decide to unlock the account or disable it.

Topics

- Adding domains to monitor
- Resolving a locked out account

To managed locked out accounts

1. Click **Security & Delegation | Locked Out Accounts**.
2. Add the domains to monitor. See Adding domains to monitor.
3. Use the tool bar to manage the locked out accounts.

Table 17.

Option	Description
Refresh	Refresh the display.
Unlock Account	Unlock selected accounts.
Disable Account	Disable or enable selected accounts. A disabled account has a gray icon. An enabled account has a blue icon.
Find User	Locate a user account. See Searching Active Directory.
Locked Out Reason	Research why an account is locked before you decide to unlock it or disable it. See Resolving a locked out account.
Monitored Domains	Add domains to monitor for locked out accounts. See Adding domains to monitor.

Adding domains to monitor

You must add the domains you want to monitor for locked out accounts.

Adding domains to monitor

1. Click **Security & Delegation | Locked Out Accounts**.
2. Click **Monitored Domains**.
3. Click **Add**.
4. Select the domains to manage.

   The domains are added to the list and are enabled by default.

- To disable selected domains, click **Disable**.
- To remove selected domains from the list, click **Remove**.
- To enable selected domains, click **Enable**.

5 Click **Close**.

6 Click **Refresh**.

The top pane displays any locked out accounts. You can unlock selected accounts, disable accounts, locate accounts in Active Directory®, and view the reason that accounts are locked.

The bottom pane displays the status of the managed domains. If a domain displays an error, you can copy the error to a text editor.

To copy the error to a text editor

a Right-click the domain, and choose **Copy Error**.

b Open a text editor, such as Notepad, and paste the error from the clipboard.

Resolving a locked out account

You may want to research why an account is locked before you decide to unlock it or disable it. You can view details about the event and locate the user in Active Directory®.

To research and resolve a locked out account

1 Click **Security & Delegation | Locked Out Accounts**.

2 Select the locked out account.

3 To view the reason why an account is locked, click **Locked Out Reason**.

Details about the event display. You can add a comment and a tag.

To add a comment

a Click **Add Comment**.

b Type the comment, and click **OK**.

To tag the event

a Click **Add Tag**.

b Click **Select Tag**.

c Select the tag. If you do not see a suitable tag, click **New Tag** to add a tag. See Using tags to mark events.

d Click **OK**. You can use the tag to filter the events list. See Managing audit reports.

4 Click **OK**.

5 To view the selected account in Active Directory, click **Find User**.

A search window opens with the selected account.

6 Select the account to view the account details.

7 To return to the locked out account, click **Security & Delegation | Locked Out Accounts**.

Based on your research, you can unlock the account, or disable it.

To unlock the account

a Click **Unlock Account**.

b Select **Reset Password**.

c Enter and confirm the new password.

d By default the user must change the password at their next logon.

e Click **Unlock**.

To disable the account

a Click **Disable Account**.

b Click **Yes**.

Managing password policies

You can manage Fine Grained Password Policy (FGPP) by linking password policies to users or groups.

NOTE: Fine-grained password policies always take precedence over domain password policy.

Topics

- Creating a new fine-grained password policy
- Linking a password policy
- Sending password notifications

To manage password policies

1 Click **Security & Delegation | Password Policies**.

2 Browse to select a domain.

The **General** tab is divided into three areas. The top area lists the current password policies. Select a policy in the top area to view the groups and users linked to the selected policy. Select a group or user in the middle area to view the password policies linked to that selected group or user.

The **Report** tab provides a list of user accounts with expired passwords and password about to expire. You can choose to send email notifications to selected accounts. See Sending password notifications.

3 Use the tool bar options to manage password policies. You also can right-click a policy, user, or group and choose from a shortcut menu.

Table 18. Password policies tool bar

Option	Description
Refresh Policies	Refresh the display.
Create Policy	Create a new password policy. See Creating a new fine-grained password policy.
Edit Policy	Modify the selected password policy.
Delete Policy	Delete the selected password policy.
Refresh Policy Links	Refresh the links to the password policies.
Link Policy	Link groups and users to the selected password policy. See Linking a password policy.
Unlink Policy	Unlink the selected groups or users from the password policy.
Unlink All	Unlink all groups and users from the selected password policy.

Creating a new fine-grained password policy

Password policies for the selected domain display in the top area of the window. To see what users and groups are linked to a policy, select the policy. The linked users and groups display in the center area.

To create a new fine-grained password policy

1. Click **Security & Delegation | Password Policies**.
2. Browse to locate a domain.
3. Click **Create Policy**.
4. Type a name for the password policy.
5. Type a description for the password policy.
6. Determine the precedence of the policy.
7. By default, the password is protected from accidental deletion. To remove the protection, clear the check box.
8. Select the settings for the password.
9. Select the maximum number of days until the password expires.
10. Select the settings for locking out the account.
11. Click **OK**.

    To link users and groups to the policy, see Linking a password policy.

Linking a password policy

Users and groups linked to a selected password policy display in the center area of the window. To see if the user or group is linked to another policy, select the user or group. The other links display in the bottom area.

To link a user or group to a password policy

1. Click **Security & Delegation | Password Policies**.
2. Browse to locate a domain.
3. Select a policy, and click **Link Policy**.
4. Choose the users or groups to link to the password policy.
5. Click **OK**.

Sending password notifications

You can preview a list of user accounts with passwords about to expire. You also can choose user accounts to receive notifications.

To send password notifications

1. Click **Security & Delegation | Password Policies**.
2. Browse to locate a domain.
3. Open the **Preview** tab.
4. Click **Preview**.
5. Enter the number of days before passwords expire. The default is 30 days.
6. The list displays user accounts with passwords that are about to expire. To include accounts with expired passwords, select the check box.
7. To create a custom email list, select the users to receive the email password reminder notification. You can filter the list of user accounts, and use **Select All** and **Clear All** to help with the selection.

8 To send the email password reminder notifications immediately to the selected user accounts, click **Send Notification**.

9 Click **Yes** to accept the confirmation message.

Checking delegation status

Active Templates can easily be broken by someone modifying the permissions of an object through the Microsoft® system-provided tools. With Active Administrator®, you quickly can repair a broken Active Template or delete it from the object. For more information on Active Templates, see Managing Active Templates.

NOTE: The administrator can set up Active Administrator to fix broken Active Templates automatically. See Setting Active Template options.

Topics

- Adding a delegation

To check delegation status

1 Click **Security & Delegation | Delegation Status**.

The **Active Template Delegation Status** page lists the current delegations and indicates how many are enforced and how many are broken.

2 Use the tool bar to repair broken templates or manage delegations.

Table 19. Delegation status tool bar

Option	Description
Refresh	Refresh all delegations.
Refresh Selected	Refresh all selected delegations.
Repair	Repair selected broken delegations.
Repair All	Repair all broken delegations.
New	Add a new delegation or copy a selected delegation to create a new delegation. See Adding a delegation.
Edit	Edit the selected delegation.
Remove	Remove a delegation.
Security Properties	View container or account properties.
Group by	Group the list of delegations by status, template name, or user.

Adding a delegation

A wizard guides you through selecting the users or groups and specifying how to delegate the selected Active Template. You also can add a delegation link in the Active Templates module.See Adding a delegation link.

To add a delegation link

1 Click **Security & Delegation | Delegation Status | New | New Delegation.**

2 On the welcome page, click **Next**.

3 Select the Active Templates.

4 Click **Next**.

5 Click **Add**.

6 Select the users or groups to include in the delegation.

7 Click **Next**.

8 Select the paths or objects to apply the delegation.

> **NOTE:** To reload the list of OUs, click **Refresh**. All selections are cleared and any newly added OUs appear in the list.

9 Click **Next**.

10 Select to make the delegation effective immediately or on a specific date.

11 Select for the delegation to never expire or to be deleted on a specific date.

12 Add an optional description.

13 Click **Next**.

14 Review the summary, and click **Finish**.

15 Click **Finish**.

Managing Active Templates

Active Templates in Active Administrator® allow administrators to quickly create and manage sets of permissions to apply to objects in Active Directory®. Any changes made to security using active templates can be repaired or removed. Custom templates can be made and standardized easily. Active Templates can also be copied as a starting point for a new template in the same category or in a different category.

To check the status on any applied Active Templates, see Checking delegation status.

Topics

- Creating an Active Template
- Copying an Active Template
- Categorizing Active Templates
- Adding a delegation link
- Reporting on Active Templates

To manage Active Templates

1 Click **Security & Delegation | Active Templates.**

The Active Templates tab is divided into three areas.

- **Active Templates** area lists the standard Active Templates, which are grouped into categories, and any custom Active Templates that you create.
- **Permissions** area lists the permissions associated with the selected Active Template.
- **Delegation Links** area lists the delegations associated with the selected Active Template.

2 Use the tool bar to manage Active Templates.

Table 20. Active Templates tool bar

Option	Description
Refresh	Refresh the display.
New	Create a new Active Template. See Creating an Active Template.
Edit	Modify a selected Active Template.
Copy	Copy a selected Active Template.

Table 20. Active Templates tool bar

Option	Description
Delete	Delete selected Active Templates.
Delegations | Add Delegation	Add a delegation to an Active Template. See Adding a delegation link.
Delegations | Edit Delegation	Edit a selected delegation.
Delegations | Copy Delegation	Copy a delegation to create a new delegation by making minimal changes.
Delegations | Remove Delegation	Remove a delegation.
Delegations | View Account Properties	View properties on the selected account.
Delegations | View Container Properties	View properties on the selected container.
Categories	Use categories to organize Active Templates. See Categorizing Active Templates.

Creating an Active Template

A wizard guides you through creating an Active Template.

To create an Active Template

1. Click **Security & Delegation | Active Templates**.
2. Click **New**.

   NOTE: Delegation in the configuration partition in the tree is disabled by default. To enable delegation in the configuration partition, see Setting general user options.
3. On the welcome page, click **Next**.
4. Type a name and description for the new Active Template.
5. From the **Category** list, choose a category to classify the Active Template. See Categorizing Active Templates.
6. Click **Next**.
7. From the **Forest** list, choose a domain.
8. From the **Applies to** list, choose how apply the template security. You can select common object types, all object types on the system, or an inheritance level.

   When selecting an inheritance level such as **This object and all child objects**, **This object only**, or **Child objects only**, you can select the permissions available to domains, organizational units, containers, and sites, which are the common objects that truly utilize the Active Directory® inheritance model for permissions.
9. From the **Classes** list, select the object.

   The **Classes** list shows common object types or all object types. If you are adding an access right based on the Active Directory inheritance model, this list is disabled.

   To filter the Classes list, type a full or partial class name in the box.
10. From the **Permissions** list, select the security to apply to the selected object.

    The **Permissions** list displays all permissions specific to the object type you selected in the Applies to list. In the case of **This object and all child objects**, **This object only**, or **Child objects only**, the list reflects all permissions available to domains, organizational units, containers, and sites. This list includes all generic rights, extended rights, property rights and the ability to create and/or delete child objects of these classes.

To filter the **Permissions** list, type a full or partial class name in the box.

11 In the **Effective Template Permissions** area, click a button to apply the permission.

12 Click **Next**.

13 Click **Finish**.

14 Click **Finish**.

Copying an Active Template

The permissions and delegations of an Active Template can be duplicated by copying the template. The category for the resulting template can be set during the process.

To copy an Active Template

1 Click **Security & Delegation | Active Templates**.

2 Select an Active Template.

3 Click **Copy**.

4 Type a unique name for the resulting Active Template.

5 From the **Category** list, choose a category to classify the resulting Active Template. See Categorizing Active Templates.

6 Optionally, select **Copy Delegations** to copy the delegation information into the resulting Active Template.

7 Click **Copy**.

Categorizing Active Templates

Active Templates are organized into categories. You can create more categories and move Active Templates to other categories.

To add a category

1 Select **Security & Delegation | Active Templates**.

2 Select **Categories | New Category**.

3 Type a name and description for the category.

4 Click **OK**.

To move Active Templates to a different category

1 Select **Security & Delegation | Active Templates**.

2 Select an Active Template.

3 Click **Categories | Move to Category**.

4 Choose a category from the list.

5 Click **OK**.

To delete a category

1 Select **Security & Delegation | Active Templates**.

2 Select a category.

3 Select **Categories | Remove Category**.

NOTE: The Active Templates in the category are not deleted.

Adding a delegation link

A wizard guides you through selecting the users or groups and specifying how to delegate the selected Active Template. You also can add a delegation link when checking the status of a delegation. See Adding a delegation link.

To add a delegation link

1 Select **Security & Delegation | Active Templates**.

2 Select an Active Template, and select **Delegations | New Delegation**.

3 On the welcome page, click **Next**.

4 Click **Add**.

5 Select the users or groups to include in the delegation.

6 Click **Next**.

7 Select the paths or objects to apply the delegation.

8 Click **Next**.

9 Select to make the delegation effective immediately or on a specific date.

10 Select for the delegation to never expire or to be deleted on a specific date.

11 Add an optional description.

12 Click **Next**.

13 Review the summary and click **Finish**.

14 Click **Finish**.

Reporting on Active Templates

NOTE: You also can run a report showing all delegations on a selected Active Template from the Security module. See Reporting on Active Directory objects.

To run an Active Template report

1 Select **Security & Delegation | Active Templates**.

2 Right-click an Active Template, point to **Reports** and choose a report. You can export any report to a PDF, HTML, MHT, RTF, Excel, CSV, Text, or Image file.

Table 21. Active Template reports

Report	Description
Active Templates Summary	Lists the accounts and associated permissions for each template.
Active Templates Category Summary	Lists the accounts and associated permissions for each template within the selected category.
Active Templates Delegation Links	Lists the delegation links for the current domain.
Active Templates Category Delegation Links	Lists the delegation links for the current domain within the selected category.

Managing inactive accounts

You can manage inactive users and computers by configuring tasks to run after a specified number of days. You also can send out an email notification to specified users.

Topics

- Configuring inactive users and computers
- Checking for inactive users and computers
- Viewing inactive users and computers history
- Reporting on inactive accounts
- Purging stale accounts

To manage inactive accounts

1. Select **Security & Delegation | Inactive Accounts**.
2. Configure the tasks to perform on inactive accounts. See Configuring inactive users and computers.
3. Use the tool bar to manage inactive accounts.

Table 22. Inactive accounts tool bar

Option	Description
Run	Run the current configuration to check for inactive users and computers. See Configuring inactive users and computers and Checking for inactive users and computers.
Save	Save changes to the current configuration.
Refresh	Refresh the display.
History Source	Select a source for the inactive account history.
Go	Go to the selected source for inactive account history.
Refresh History	Refresh the inactive account history.
Filter	Filter the list of inactive account history archives.
Clear Filter	Clear the filter and restore all archives to the list.
Report	Run an Inactive Accounts History Report. See Reporting on inactive accounts.

Configuring inactive users and computers

You can configure Active Administrator® to perform tasks based on how long a user account or computer has been inactive. Next, select the domains to monitor, configure organizational units or criteria to exclude areas from being monitored, and add email recipients to receive notifications of inactive accounts.

To configure inactive users and computers

1. Select **Security & Delegation | Inactive Accounts**.
2. Select **Users & Computers**, if necessary.
3. Configure inactive users.
    a. By default, inactive user accounts are managed. To disable, clear the **Manage Inactive Users** check box.
    b. By default, a user is considered inactive if the user has not logged in after 60 days. To change the value, type a number in the box. The value must be greater than 13 days.

c To create a report of inactive users, select **Identify Inactive Users Only**. You can select to exclude accounts with passwords set to never expire from the report. No other tasks are performed on the inactive accounts.

-OR-

Select **Perform the Following Actions** to perform the selected tasks on the inactive accounts.

Table 23. Actions for inactive accounts

Option	Description
Leave User in Place	Select to leave the user account in its original location.
Move User to	By default, inactive user accounts are moved to the InactiveUsers OU, which is created at the root of the domain. To change the value, type in the box. **NOTE:** If you enter the name of an OU or a sub-OU, such as VK/InactiveUsers, and that OU or sub-OU is not present on the managed domain, the OU or sub-OU is created when you click **Save**.
Purge stale users	By default, inactive accounts are purged after 30 days of inactivity. You can set up a schedule, send notifications, and prevent specific users from being deleted. See Purging stale accounts.
Disable User -Days until disabled	By default, the user account is disabled once it has met the inactive user account requirement. If required, you can also set the number of days before the user account is disabled after it has been deemed inactive. To leave the user account enabled, clear the check box.
Reset Password to a Random Password	By default, the user's password is set to a random password. To leave the password as is, clear the check box.
Exclude accounts that have passwords set to not expire	By default, user accounts with passwords set to not expire are excluded from the selected tasks. To include those accounts in the selected tasks, clear the check box.
Execute this program or script	Select to run a program or script. Type a path or browse to locate the program or script to run. **NOTE:** The script must be a local path on the Active Administrator server.
Script arguments (optional)	Type arguments, or browse to build arguments by selecting parameters from a list. ***To build arguments*** 1 Click the browse button. 2 Build the argument in the lower pane by typing switches and inserting parameters from the list. To insert a selected parameter from the list, double-click the parameter or click **Insert**. The parameter is inserted at the location of the cursor. **EXAMPLE** Type **/dom:**, double-click **%DOMAIN%**; or select **%DOMAIN%**, and click **Insert**. Repeat for additional parameters. `/dom:%DOMAIN% /t:%TYPE% /sid:%SID%` 3 Click **OK**.
Execute program or script in this folder (optional)	Browse to locate a working folder in which to run the selected program or script. If you leave this box blank, the working folder is the System directory on the Active Administrator server. **NOTE:** The working folder must be a local path on the Active Administrator server.

4 Set up inactive computers.

a By default, the selected tasks are performed on inactive computers. To disable the feature, clear the **Managed Inactive Computers** check box.

b By default, computers are considered inactive after 200 days. To change the value, type a number in the box. The value must be greater than 29 days.

c Select **Identify Inactive Computers Only** to include inactive computers on the preview report only. No other tasks are performed on the inactive account.

-OR-

Select **Perform the Following Actions** to perform the selected tasks on the inactive account.

Table 24. Actions for inactive computers

Options	Description
Leave Computer in Place	Select to leave the user account in its original location.
Move the Computer to	By default, inactive computer accounts are moved to the InactiveComputers OU, which is created at the root of the domain. To change the value, type in the box. **NOTE:** If you enter the name of an OU or a sub-OU, such as VK/InactiveUsers, and that OU or sub-OU is not present on the managed domain, the OU or sub-OU is created when you click **Save**.
Purge stale computers	By default, inactive accounts are purged after 30 days of inactivity. You can set up a schedule, send notifications, and prevent specific computers from being deleted. See Purging stale accounts.
Disable Computer - Days until disabled	By default, the computer account is disabled once it has met the inactive account requirement. If required, you can set the number of days before the computer account is disabled after it has been deemed inactive. To leave the computer account enabled, clear the check box.
Execute this program or script	Select to run a program or script. Type a path or browse to locate a program or script to run. **NOTE:** The script must be a local path on the Active Administrator server.
Script arguments (optional)	Type arguments, or browse to build arguments by selecting parameters from a list. ***To build arguments*** 1 Click the browse button. 2 Build the argument in the lower pane by typing switches and inserting parameters from the list. To insert a selected parameter from the list, double-click the parameter or click **Insert**. The parameter is inserted at the location of the cursor. **EXAMPLE** Type **`/dom:`**, double-click **%DOMAIN%**; or select **%DOMAIN%**, and click **Insert**. Repeat for additional parameters. `/dom:%DOMAIN% /t:%TYPE% /sid:%SID%` 3 Click **OK**.
Execute program or script in this folder (optional)	Type a path or browse to locate a working folder in which to run the selected program or script. If you leave this box blank, the working folder is the System directory on the Active Administrator server. **NOTE:** The working folder must be a local path on the Active Administrator server.

5 Select a time of day to check for inactive accounts.

6 Select domains to monitor.

   a Click **Domains**.

   b Click **Add**, select a domain to monitor for inactive accounts, and click **OK**.

   c By default, all domain controllers are included in checking for inactive accounts. To exclude a domain controller, clear the check box.

   > **NOTE:** You must have at least one domain controller that is not excluded in order to check for inactive users and computers.

7 By default, all organizational units, users, and groups are included in checking for inactive accounts. To save time, you can select organizational units, or users and groups to exclude when checking for inactive accounts.

   a Click **Exclusions**.

   b Click **Add**.

   c Choose the domain.

   d You can choose to exclude selected organizational units, to exclude selected users and groups, or to use a condition to identify exclusions (for user and computer objects only).

   > **NOTE:** To reload the list of OUs, click **Refresh**. All selections are cleared and any newly added OUs appear in the list.

   To exclude organizational units

      a Select **Exclude Organizational Unit**.

      b Click **Add**.

      c Select one or more organizational units to exclude. If you select an OU, all the OUs below it are also selected, but you can clear the check box to remove it from the selection.

      d Click **OK**.

   To exclude users or groups

      a Select **Exclude Users and Groups**.

      b Click **Add**.

      c Select one or more users and groups to exclude.

      d Click **OK**.

   To use a condition

      a Select to either **Start with** or **End with** a condition (user and computer objects only).

      b Type the condition.

   e Click **OK**.

8 Set up notifications.

> **NOTE:** The email server must be configured to send notifications. See Setting email server options.

   a Click **Notifications**.

   By default, the Active Administrator owner email address that was added during installation automatically receives email notifications for both inactive users and computers.

   > **NOTE:** The Active Administrator owner was identified in the AA Configuration Wizard. To change the AA Owner email address, see Managing email addresses.

   b To add more email recipients, click **Add**, type an email address, and click **OK**.

c Select to include either both inactive user and computer accounts or just one type by clearing or enabling the **Users** and **Computers** check box.

9 To preview the list of inactive users and computers, click **Preview**.

To sort the contents by a column, click the column header.

> **NOTE:** To manage the Inactive Accounts email address list, see Managing email addresses.

10 To setup a schedule for email notifications, select **Users and Computers**, click **Set Schedule,** select how often to send the email, the time zone, and start time, and click **OK**.

11 Click **Save**.

Checking for inactive users and computers

You also can create a schedule to check for inactive users and computers. See Configuring inactive users and computers.

To check for inactive users and computers

1 Select **Security & Delegation | Inactive Accounts**.

2 If necessary, make any changes to the configuration. See Configuring inactive users and computers.

3 Click **Run Now**.

4 Click **Yes**.

5 To view the progress of the task, select **Configuration | Tasks**. See Managing tasks.

Viewing inactive users and computers history

To view inactive users and computers history

1 Select **Security & Delegation | Inactive Accounts**.

2 Click **History**.

3 From the **History Source** list, select the live database or an archive database.

4 Click **Go**.

5 Select the domain to examine.

> **NOTE:** If you do not see the domain you need, the domain was not added to the configuration. See Configuring inactive users and computers.

The **Archives** column lists all the past occurrences when the selected domain was checked for inactive users and computers.

- To filter the list of archives, click **Filter**, enable the filter, select the date, and click **Filter**.
- To remove the filter, click **Clear Filter**.

6 Select an archive to view. To sort the contents by a column, click the column header.

- The **Users** area lists the inactive users discovered during the selected archive run.
- The **Computers** area lists the inactive computers discovered during the selected archive run.

Reporting on inactive accounts

You can choose to create a report to display in a report editor, to send in an email, or to save to a file.

NOTE: The email server must be configured to send notifications. See Setting email server options.

To send an inactive report by email or save to a file

1. Select **Security & Delegation | Inactive Accounts**.
2. Click **Reports.**
3. Select **Delivery report**, if necessary.
4. Change the default report name if desired.
5. By default, the date and time are appended to the end of the file name. Clear the check box if you do not want the date and time appended to the file name.
6. By default, a PDF file is created. You can choose a different format.
7. You can send the report by email and save it to a file.

   To send an email

   a. Click **Email**, if necessary.

   b. By default, the logged in account displays in the Email Addresses list. To add more recipients, click **Add**, type the email addresses, and click **OK**.

   c. Modify the default subject line if desired.

   d. Set the priority of the email.

   To save the file to a folder

   a. Click **Save to Folder**.

   b. Click **Add**.

   c. Add a path to the location where you want to store the report file.

   d. Click **OK**.
8. Click **OK**.

To generate an inactive accounts report and display in a report editor

1. Select **Security & Delegation | Inactive Accounts**.
2. Click **Reports**.
3. Select **Interactive**.
4. Click **OK**.

Purging stale accounts

By default, inactive accounts are purged after 30 days of inactivity. You can set up a schedule, send notifications, and prevent specific users from being deleted.

To set up stale account purging

1. Select **Security & Delegation | Inactive Accounts**.
2. Click **Set up** next to **Purge stale users** or **Purge stale computers**.
3. Set the schedule for Active Administrator to check for stale accounts.
4. Set the number of days after which an inactive account is purged. The default is 30 days.

5 Select to send notifications. You can send a notice when the account is about to deleted and/or when the account is deleted.

6 To prevent specific accounts from being deleted, click Add, select the account, and click **OK**.

7 Click **Save**.

Sending password reminders

If enabled, the Password Change Reminder service runs every day at the time you specify. If user accounts are about to expire, email notifications are sent to the users according to the schedule you set up. You can set up to three levels of password reminder notifications. For example, you could set up the first reminder at 14 days, the second at 7 days, and the final notification at 1 day before the password expires. You can then choose to repeat the final notification until the user changes their password. You can also send the manager a notification when a user is sent a password reminder.

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 expired passwords and users with passwords about to expire. You can choose to exclude accounts with less than or more than a configurable number of days before their password expires. You can also exclude organization units, users and groups, accounts that start or end with specific criteria, and enabled or disabled accounts. The administrator summary notification indicates if the user was notified.

NOTE: The email server must be configured to send notifications. See Setting email server options.

To send password reminders

1 Select **Security & Delegation | Password Reminder**.

2 Click **General**, if necessary.

3 By default, the password reminder feature is enabled. To disable the feature, clear the check box.

4 Select a time for Active Administrator to run the Password Change Reminder service.

NOTE: You can run the Password Change Reminder service at any time by clicking **Run Now**.

5 Set the number of days prior to a password expiring that signals Active Administrator to begin sending email password reminder notifications. The maximum value is 90 days.

6 Select to send additional levels of notification, if desired.

7 Select to repeat the notifications after the final notification, if desired. Once the password expires, the user will receive a notification daily until the password is changed.

8 By default, accounts with expired passwords are included in the administrator password summary notification. To exclude accounts with expired passwords, clear the check box.

9 Optionally, set **Send manager notifications** to notify the manager when a user receives a password reminder.

NOTE: The user must be linked to a manager in Active Directory.

10 Choose to sort the results by User Name, Expiration Date, Domain, or nested by Domain/Expiration Date/User Name or by Domain/User Name/Expiration Date.

11 By default, the email address of the Active Administrator owner that was added during installation automatically receives the administrator password summary notification. To add additional email recipients, click **Add**.

NOTE: The Active Administrator owner was identified in the AA Configuration Wizard. To change the AA Owner email address, see Managing email addresses.

NOTE: To manage the Password Reminder Settings email address list, see Managing email addresses.

12 Choose the domains to monitor for password expiration.

a Click **Domains**.

b To add additional domains, click **Add**, select a domain, and click **OK**.

13 Optionally, configure exclusions.

a Click **Exclusions**.

b To add exclusions, click **Add**, set the Password Reminder Filters, and click **OK** to save the settings.

Table 25. Password Reminder Filters

Filter	Usage
Apply to Domain	Set a domain to which the filters will be applied.
Exclude Organization Unit	Add organization units to be excluded.
Exclude Users and Groups	Add users and groups to be excluded.
Starts with <condition>	Type a “starts with” condition that will be used to exclude user or computer objects.
Ends with <condition>	Type an “ends with” condition that will be used to exclude user or computer objects.
Exclude user accounts with less than X days before their password expires	Type the number of days to consider. Any accounts with less than this many days before the pass word expires will be excluded.
Exclude user accounts with more than X days before their password expires	Type the number of days to consider. Any accounts with more than this many days before the password expires will be excluded.
Exclude user if account is enabled or disabled	Set whether a user account is excluded when it is enabled or disabled.

c Optionally, click **Edit** to change a selected exclusion.

d Optionally, click **Remove** to remove a selected exclusion.

14 Customize the message to send. A default message is provided, but you can edit parts of the message to fit your needs.

a Click **Message**.

A default message is included. To view the default message, click **Preview Message**.

b To change the default Subject Line or Manager Subject Line of the email notification, click in the box and edit the default text.

There are variables you can use to customize the subject line or the body of the message.

Table 26. Variables to customize subject line or body of password reminder message

Variable	Description
%FIRSTNAME%	First name of the user
%LASTNAME%	Last name of the user
%DISPLAYNAME%	Display name of the user

Table 26. Variables to customize subject line or body of password reminder message

Variable	Description
%DATE%	Expiration date
%LASTCHANGEDATE%	Date of last change to the password
%DAYSLEFT%	Number of days left before the password expires
%USERNAME%	Username of the user

c Choose how to display the name of the recipient in the message greeting.

d The email message has the following sections: **Greeting**, **Message, Info, Instructions**, **Requirements**, **Helpful Advice**, and **Help Desk**. The manager notification has the following sections: **Message** and **Info**. You can enable or disable a section, edit the default text, and add an image, such as a company logo.

- To disable a section, clear the check box.
- To change the text or include an image in the message:
  - Click **Edit** next to the section you want to change.
  - Make changes in the text editor that opens, optionally making use of the variables in Table 26.
  - Click **Save**.
- To restore the text to the default, click **Default**.

e To preview the message, click **Preview Message**.

15 Preview the list of user accounts with passwords about to expire. You also can choose user accounts to receive notifications.

a Click **Preview and Notify**.

b Click **Preview**.

c By default, the list of user accounts is based on the settings on the **General** tab. To override the settings on the **General** tab, select the check box, and enter the number of days before passwords expire.

d By default, accounts with expired passwords do not display. To show accounts with expired passwords, select the check box.

e To export the list of user accounts to a .csv or .txt file, click **Export**.

f To create a custom email list, select the users to receive the email password reminder notification. You can filter the list of user accounts, and use **Select All** and **Clear All** to help with the selection.

g To send the email password reminder notifications immediately to the selected user accounts, click **Send Notification**. Otherwise, the email password reminder notifications are sent according to the schedule you set up.

h Click **Yes** to accept the confirmation message.

16 Click **Save**.

17 If you want to run the Password Reminder Service now, click **Run Now**. Otherwise, the task runs according to the schedule designated on the **General** tab.

Sending account expiration notifications

You can manage account expirations by configuring an email message to send when user accounts are about to expire.

NOTE: The email server must be configured to send notifications. See Setting email server options.

To send account expiration notifications

1. Select **Security & Delegation | Account Expiration**.
2. Click **General**, if necessary.
3. By default, the account expiration notification feature is enabled. To disable the feature, clear the check box.
4. Select a time at which Active Administrator checks for accounts about to expire.

   NOTE: You can check for expired accounts at any time by clicking **Run Now**.

5. Select the number of days prior to an account expiring that signals Active Administrator® to begin sending email notifications.
6. Select to send the notification to the user and/or the manager of the user.

   NOTE: The user must be linked to the manager in Active Directory®.

7. By default, the administrator email address added during installation automatically receives the account expiration notification message. To add additional email recipients, click **Add**.

   NOTE: The Active Administrator owner was identified in the AA Configuration Wizard. To change the AA Owner email address, see Managing email addresses.

   NOTE: To manage the Account Expiration email address list, see Managing email addresses.

8. Click **Domains**.
9. To add additional domains, click **Add**, select a domain, and click **OK**.
10. Click **Message**.

    There are two messages: user and manager. Use the variables in the table below to construct your subject line and message.

    Table 27. Account expiration message variables

Variable	Description
`%username%`	User name
`%displayname%`	Display name of the user
`%date%`	Date account is set to expire

11. To change the default subject line, click in the box and edit the default text.
12. To change the text in the message, click **Edit**, make changes in the text editor that opens, and click **Save**.
    - To restore the text to the default, click **Default**.
13. Click **Preview**.
14. To preview the list of accounts about to expire, click **Preview**.
15. Click **Save**.

16 If you want to check for expired accounts now, click **Run Now**. Otherwise, the task runs at the time designated on the **General** tab.

Viewing expired accounts

You can view a list of all expiring and expired accounts in the selected domain.

To view expiring and expired accounts

1 Select **Security & Delegation | Account Expiration**.

2 Select the source of the account expiration history. You can look at live data or the Active Administrator database.

3 Click **Go**. To refresh the list, click **Refresh History**.

- If the **Pending** column is **True**, the account is about to expire. 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.
- If the **Pending** column is **False**, the account has expired.

Purging account history

You can archive or purge account history on demand or schedule an archive or purge. Purged expired and inactive accounts are deleted from the live audit database. Archived expired and inactive accounts are first copied to the archive database and then deleted from the live audit database.

Topics

- Archiving account history on demand
- Purging account history on demand
- Scheduling an account history purge and archive

To purge account history

1 Select **Security & Delegation | Purge Account History**.

- The top pane displays the history of archiving and purging account history.
- The bottom pane displays the maintenance tasks specific to archiving and purging account history.

2 Use the options on the tool bar to manage purging and archiving inactive account history.

Table 28. Purging inactive account history tool bar

Option	Description
Archive Now	Archive expired and inactive account history from the live audit database. See Archiving account history on demand.
Purge Now	Purge expired and inactive account history from the live audit database. See Purging account history on demand.
Schedule	Schedule the archive or purge process. Scheduling an account history purge and archive.
Refresh	Refresh the display.
Export History	Export the account history to a .csv file.

Table 28. Purging inactive account history tool bar

Option	Description
Clear History	Clear the account history.
Tasks	Refresh the tasks list, view task properties, send a selected task to email recipients, and group the list of tasks by status. See Managing tasks.

Archiving account history on demand

Copies expired and inactive user and computer history from the live audit database to the active archive database, and then deletes the history from the live audit database.

NOTE: To schedule the archive process, see Scheduling an account history purge and archive.

To archive account history on demand

1. Select **Security & Delegation | Purge Account History**.
2. Click **Archive Now**.
3. Type a date or select a date from the calendar.
4. Click **Archive Now**.

Purging account history on demand

Deletes event entries and alert history items permanently from the live audit database based on the selected purge options.

NOTE: To schedule the purge process, see Scheduling an account history purge and archive.

To purge account history on demand

1. Select **Security & Delegation | Purge Account History**.
2. Click **Purge Now**.
3. Type a date or select a date from the calendar.
4. Click **Purge Now**.

Scheduling an account history purge and archive

You can choose to purge only, archive only, or purge then archive. You can select different events to purge or archive. Purged events are deleted from the live database. Archived events are copied to the Archive database, and then deleted from the live database.

To schedule an account history purge and archive

1. Select **Security & Delegation | Purge Account History**.
2. Click **Schedule**.
3. By default, scheduling is enabled. You can create a schedule and then disable it until you need it.
4. Select to archive or purge.

Table 29. Archive and purge options

Option	Description
Archive inactive user and computer history and account expiration history	Select to copy account history items from the live database to the active archive database, and then delete the history from the live database.
Purge inactive user and computer history and account expiration history	Select to delete account history items permanently from the live database.

5 By default, selected event entries and alert history items older than 30 days are deleted.

6 To change the default schedule, click **Update**.

7 Set the schedule.

8 Click **Save**.

5

Active Directory Health

Active Directory Health proactively monitors and troubleshoots Active Directory so that you can deploy Windows Server with confidence.

IMPORTANT:

- The Active Directory Health license is required for the Active Directory Health module. If you do not have a license applied to your installation, the Active Directory Health module will not appear in Active Administrator.
- Users must have the appropriate user roles selected to use the various features of the Active Directory Health Analyzer. See Defining role-based access.
- The first time you open the **Agents** option, the **Managed Domain Controllers** page display is empty. The first task is to install an Active Directory Health Analyzer agent. See Installing Active Directory Health Analyzer agents. Once an agent is installed the **Managed Domain Controllers** page lists the domain controllers monitored by Active Directory Health Analyzer agents. See Managing monitored domain controllers.
- If you are a current user of Quest® Directory Analyzer® and Directory Troubleshooter, you have the option of switching over to Active Directory Health gradually or all at once. See Switching to Active Directory Health.
- The Active Directory Health Analyzer agent must be upgraded to the current version.

Topics

- Switching to Active Directory Health
- Using the Active Directory Health landing page
- Installing Active Directory Health Analyzer agents
- Using the Active Directory Health Analyzer agent configuration utility
- Excluding domain controllers
- Managing the Remediation Library
- Analyzing Active Directory health
- Analyzing Microsoft Entra ID
- Managing Active Directory Health Analyzer alerts
- Managing alert notifications
- Pushing alerts to System Center Operations Manager and SNMP managers
- Managing monitored domain controllers
- Managing data collectors
- Active Directory Health Templates
- Managing Active Directory Health Analyzer agents
- Using the Troubleshooter
- Recovering Active Directory Health data

Switching to Active Directory Health

Active Directory Health 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.

To switch gradually

1. Deploy at least two agents into the Active Directory Health agent pool and add a few domain controllers to monitor. See Installing Active Directory Health Analyzer agents into a pool.

   NOTE: When adding the agents into the pool, make sure that you make the agent available to all domain controllers or at least to all of the domain controllers that you plan to monitor with the pool of agents.

2. Stop, but do not uninstall, 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. See Adding 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. See Installing Active Directory Health Analyzer agents into a pool.
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.

Using the Active Directory Health landing page

The first time you open the **Active Directory Health** module, a message displays that you need to configure Active Directory forests. Click **Manage Agents** and install at least one Active Directory Health Analyzer agent. See Installing Active Directory Health Analyzer agents.

Once you have installed at least one Active Directory Health Analyzer agent, the **Active Directory Health** landing page displays summary information for about forests, domains, sites, domain controllers, and alerts. Active tiles display summary information for each domain that is configured in Active Administrator®.

Summary area

The **Summary** area displays a summary of the forests, domains, sites, and domain controllers.

Table 30. Summary area

Object	Description
Forest	Number of forests being monitored.
Domains	Number of domains in the forest, including domains not being monitored.
Domain controllers	Number of domain controllers in the forest, including domain controllers not being monitored.
Agents	Number of installed agents.
Global catalog servers	Number of global catalog servers in all domains.
Read only domain controllers	Number of read-only domain controllers (RODCs) in all domains.
Sites	Number of sites in all forests.
Bridgehead servers	Number of bridgehead servers in all sites.
Monitored domain controllers	Number of monitored domain controllers.
Unmonitored domain controllers	Number of unmonitored domain controllers.
All agents running All schema versions consistent All schema masters consistent All naming masters consistent All PDC masters consistent All infrastructure masters consistent All RID masters consistent All functional levels consistent	Indicates the status of the object in all forests and domains. If one object has a problem, the status becomes No.

Alerts area

The **Alerts** area indicates the total number of critical, and warning alerts for the forest. The chart shows alert history over the past 12 hours. If you pause the cursor over the graph, you can view the number of critical, and warning alerts that were triggered or created during the hour, and the number of active alerts that occurred during the hour.

Active tiles

An active tile displays for each domain being monitored by Active Administrator®. The active tiles automatically update every 30 minutes, but you can use the icons to refresh the tiles at any time. You also can pause and resume the refresh of data. To customize the active tile refresh, see Setting general user options.

To use the Active Directory Health landing page

1. Select **Active Directory Health**.
2. Click the item to open a window so you can examine details.
   - Click the **Summary** area to open the Analyzer window for the forest. See Analyzing the health of a forest.
   - Click the **Alert Summary** area to open the Alerts window. See Viewing alerts and alert history.
   - Click an active tile to open the Analyzer window for the domain. See Analyzing health of a selected domain.

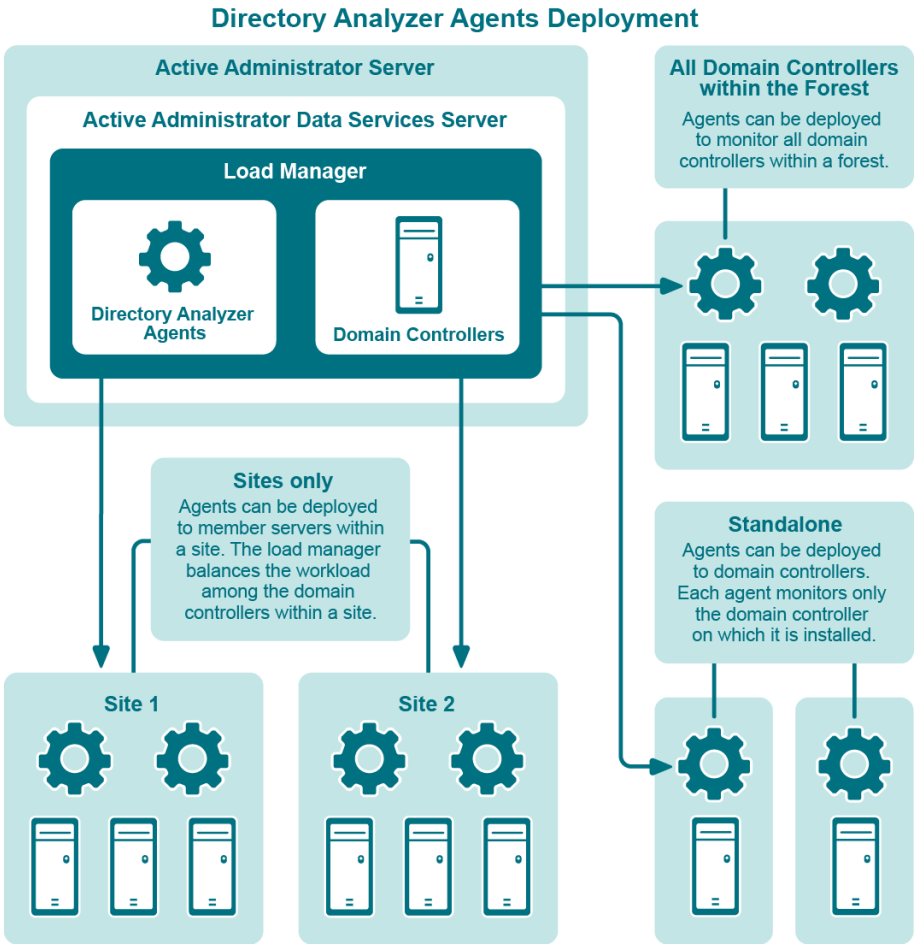
Installing Active Directory Health Analyzer agents

To monitor Active Directory domains, an agent is required. You can install the agent on each domain controller that you want to monitor, which is called standalone mode. You also have the option to install the agents on servers in a pool that are used to monitor selected domain controllers. Installing the agents into a pool helps to distribute the workload. Finally, once you run the wizard, you can set up automatic deployment, which deploys either the agent to newly discovered domain controllers or adds the domain controller to the pool of agents.

IMPORTANT:

- For the Active Directory Health Analyzer agent to deploy successfully, .NET Framework 4.8 must be installed.
- There must be one Active Directory Health Analyzer agent for every 25 monitored domain controllers. For example, if you need to monitor 100 domain controllers, you must have at least 4 Active Directory Health Analyzer agents in the pool.

Figure 1. Active Directory Health Analyzer agent deployment options



Topics

- Installing Active Directory Health Analyzer agents into a pool
- Installing Active Directory Health Analyzer agents onto domain controllers
- Installing Active Directory Health Analyzer agents manually

- Setting up automatic Active Directory Health Analyzer agent deployment

Installing Active Directory Health Analyzer agents into a pool

Active Administrator recommends installing Active Directory Health Analyzer agents into a pool to balance the workload among the servers in the pool. As domain controllers are added, removed, stopped, or started, the servers automatically adjust the workload every 24 hours. You also can initiate a workload evaluation manually at any time.

When installing the agents into a pool of servers, you can choose to have the pool monitor domain controllers in selected sites or all domain controllers.

NOTE: The number of pooled agents required will differ depending on the number of (and the activity generated by) the domain controllers that are being monitored, as well as the number and types of data collectors selected to run for each particular domain controller. The more data that is monitored, the busier the agent will be, and the more memory and computing resources it will consume. Users are encouraged to find the balance between the number of monitored data points and the number of required agent host machines needed to keep agent load and responsiveness at an acceptable level.

To install Active Directory Health Analyzer agents into a pool

1. Select **Active Directory Health | Agents**.
2. Open the **Monitored Domain Controllers** tab, and click **Add**.

   -OR-

   Open the **Analyzer Agents** tab, and click **Install**.
3. On the welcome page, click **Next**.
4. Select **Manage the Active Directory Health agent pool**.
5. Click **Next**.

   NOTE: If you selected **Managed Domain Controllers | Add**, the first time you open this page, you see a warning that no Active Directory Health Analyzer agents are deployed. You can close the warning message.
6. Use the **Add**, **Edit**, and **Remove** buttons to manage the list of servers in the pool.

   Table 31. Active Directory Health Analyzer agent pool options

Option	Description
Add	Add a server to the pool. ***To add a server to the pool*** 1 Click **Add**. 2 Browse to select the server on which to install the agent. 3 Select to make the agent available to all domain controllers or select specific sites from the list. Use **Select All** and **Clear All** to help with the selection Regardless of the option you select, you will have the opportunity to select the actual domain controllers that the agent will monitor. 4 Click **OK**. Repeat for each server you want to add to the pool.
Edit	Edit the selected server. You can change the sites for which the agent is available.
Remove	Remove the selected servers from the pool.

7. Click **Next**.

8 In the **Domain** box, type a domain, or browse to locate a domain.

9 Click **Find Domain Controllers**.

If you want to load all the domain controllers for the forest, select the check box. Keep in mind that the load time depends on the size of the forest. If the forest is large, the load time may take a while.

10 Select the domain controllers that the servers in the pool will monitor. If you selected specific sites, only the unmonitored domain controllers in the selected sites are listed.

- To filter the list of domain controllers, start typing in the **Filter Domain Controller** box. The list filters as you type. You also can sort the list by clicking a column heading.
- To select all the listed domain controllers, click **Select all**.
- To clear the selections, click **Clear all**.

11 Click **Next**.

12 In the **Run as** box, type an account, or browse for an account.

IMPORTANT: For optimal monitoring of domain controllers, an account with domain administrative privileges is recommended.

If you cannot use an account with domain administrative privileges, choose an account that is a member of the Performance Log Users and Distributed COM Users groups in the monitored domain. You also must enable Remote Access for WMI on remotely monitored domain controllers. Some monitoring features will not be available.

NOTE: To analyze replication, the startup account must have the rights to monitor performance data and to create objects in Active Directory.

NOTE: A service account that is a member of the "Protected Users" security group cannot be used for AD health agents.

13 Type the password for the account.

14 Click **Next**.

15 To configure Windows Firewall to allow the Active Directory Health Analyzer agent to communicate with the Active Administrator Data Service (ADS), select the check box.

16 Select the account to use to install the agent. You can use the Active Administrator Foundation Service (AFS) account, or indicate a specific user account.

NOTE: The selected account must be a full Administrator on the target server.

17 Click **Next**.

18 On the **Summary** page, check the settings, and click **Finish**.

19 Click **Finish** again to begin installation.

When installation is complete, the **Monitors** column indicates the agent is available for all domain controllers or indicates which site it is monitoring.

- To view the domain controllers monitored by the agent pool, click **Monitored Domain Controllers**. The **Monitored by** column indicates which server in the agent pool is monitoring each domain controller. You also can click **Properties** for a selected domain controller. See Managing the Remediation Library.

Installing Active Directory Health Analyzer agents onto domain controllers

Active Administrator recommends installing Active Directory Health Analyzer agents into a pool to balance the workload among the servers in the pool. For more information, see Installing Active Directory Health Analyzer

agents into a pool on page 87. It is also possible to install an Active Directory Health Analyzer agent directly onto a domain controller where the agent monitors only that domain controller.

To install Active Directory Health Analyzer Agents onto domain controllers

1 Select **Active Directory Health | Agents**.

2 Open the **Monitored Domain Controllers** tab, and click **Add**.

-OR-

Open the **Analyzer Agents** tab, and click **Install**.

3 On the welcome page, click **Next**.

4 Select **Install the Active Directory Health Analyzer agents directly onto domain controllers**.

5 Click **Next**.

6 In the **Domain** box, type a domain, or browse to locate a domain.

7 Click **Find Domain Controllers**.

If you want to load all the domain controllers for the forest, select the check box. Keep in mind that the load time depends on the size of the forest. If the forest is large, the load time may take a while.

8 Select the domain controllers on which to install the agents.

- To filter the list of domain controllers, start typing in the **Filter Domain Controller** box. The list filters as you type. You also can sort the list by clicking a column heading.
- To select all the listed domain controllers, click **Select all**.
- To clear the selections, click **Clear all**.

9 Click **Next**.

10 In the **Run as** box, type an account, or browse for an account.

> **IMPORTANT:** For optimal monitoring of domain controllers, an account with domain administrative privileges is recommended.
>
> If you cannot use an account with domain administrative privileges, choose an account that is a member of the Performance Log Users and Distributed COM Users groups in the monitored domain. You also must enable Remote Access for WMI on remotely monitored domain controllers. Some monitoring features will not be available.

11 Type the password for the account.

12 Click **Next**.

13 To configure Windows® Firewall to allow the Active Directory Health Analyzer agent to communicate with the Active Administrator Data Service (ADS), select the check box.

14 Select the account to use to install the agent. You can use the Active Administrator Foundation Service (AFS) account, or indicate a specific user account.

> **NOTE:** The selected account must be a full Administrator on the target server.

15 Click **Next**.

16 On the **Summary** page, check the settings, and click **Finish**.

17 Click **Finish** again to begin installation.

When installation is complete, the **Monitors** column indicates the agent is monitoring the domain controller on which it is installed.

Installing Active Directory Health Analyzer agents manually

Active Administrator recommends installing Active Directory Health Analyzer agents into a pool to balance the workload among the servers in the pool. For more information, see Installing Active Directory Health Analyzer agents into a pool on page 87. It is also possible to install an Active Directory Health Analyzer agent directly onto a domain controller where the agent monitors only that domain controller. For more information, see Installing Active Directory Health Analyzer agents onto domain controllers on page 88.

You can also install an Active Directory Health Analyzer agent into a pool or onto domain controllers manually. Pooled agents can monitor multiple domain controllers in a forest. Load balanced agents must be installed directly onto the domain controller to be monitored.

Before you begin installation, you need the following information:

- The FQDN or IP address of the ADS Server.
- The SAM Account name of the user used to run the DAAgent service.
- The password of the user used to run the DAAgent service.

To deploy the Active Directory Health Analyzer agent

1. Locate **C:\Program Files\Quest\ActiveAdministrator\Server\SLAgent\DAAgent**.
2. Copy the **DAAgent** folder and its contents.
3. Paste the folder and its contents into **C:\Windows** on the target server to create **C:\Windows\DAAgent**.

   The Windows service will be installed in this location and the Active Directory Health Analyzer Agent will run out of this location.
4. Select **Start | Command Prompt (Admin)**, navigate to the folder where you copied the files, type **Setup.exe -help**, and press **Enter** to see the usage details for all of the available parameters.

After the installation is complete, use the **Agents** tab in the Active Administrator console or **Setup.exe** from the command line to manage the Active Directory Health Analyzer Agent.

Setting up automatic Active Directory Health Analyzer agent deployment

Automatic deployment of the Active Directory Health Analyzer is available only for domain controllers that were not discovered when you ran the wizard to install the Active Directory Health Analyzer agent. See Installing Active Directory Health Analyzer agents into a pool and Installing Active Directory Health Analyzer agents onto domain controllers. Once you run the wizard, any new domain controllers that are brought online can be deployed automatically into the agent pool or the Active Directory Health 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.

> **NOTE:** Once a domain controller is discovered during the Install Active Directory Health Analyzer Agents wizard, the automatic Active Directory Health Analyzer agent deployment will not recognize those domain controllers. You can, however, view a list of unmonitored domain controllers and add selected domain controllers to the list of monitored domain controllers. See Adding monitored domain controllers.

To set up automatic Active Directory Health Analyzer agent deployment

1. Select **Active Directory Health | Agents**.
2. Open the **Analyzer Agents** tab.
3. Select **More | Automatic Agent Deployment**.
4. Open the **General** tab, if necessary.

5 By default, the automatic agent deployment feature is disabled. If you want to enable the feature, select the **Enabled** check box.

6 By default, only a list of newly discovered domain controllers is sent to the list of email addresses. The Active Administrator owner is added automatically to the list of email addresses. To add more email addresses to the list, click **Add**.

> **NOTE:** The Active Administrator owner was identified in the AA Configuration Wizard. To change the email address of the AA Owner, see Managing email addresses.
>
> **NOTE:** To manage the DA Agent Auto Deploy email address list, see Managing email addresses.

7 To set up automatic agent deployment, select **Deploy agent or domain controller**.

- If you select to deploy the Active Directory Health Analyzer agent to the domain controller, browse to locate the startup account, and enter the password.
- If you choose to deploy the domain controller into the agent pool, you can choose to deploy it immediately, or wait for the specified number of hours.

8 Enter the number of hours to wait before automatically deploying the agent or the domain controller. The default value is 24 hours. You can set the delay for 1 to 48 hours.

9 If you want to exclude any domains from automatic deployment, open the **Excluded Domains** tab, and click **Add**.

10 Click **OK**.

11 To check for pending deployments, open the **Pending Deployments** tab. You can cancel a deployment or initiate the deployment immediately.

Using the Active Directory Health Analyzer agent configuration utility

While you can manage the Active Directory Health Analyzer agent within Active Administrator® (see Managing Active Directory Health Analyzer agents), there may be an occasion when you need to manage the agent outside of Active Administrator. A configuration utility for the Active Directory Health Analyzer agent and Active Administrator Data Service (ADS) server is available to help you diagnose issues. Once you install a Active Directory Health Analyzer agent, you can find the utility at C:\Windows\DAAgent\DAAgentConfig.exe.

> **NOTE:** You cannot use the Active Directory Health Analyzer Agent Configuration utility on a Server Core installation of Windows Server.

Topics

- Setting network settings
- Enable logging

To use the Active Directory Health Analyzer agent configuration utility

- Launch **DAAgentConfig.exe**, which is located at **C:\Windows\DAAgent**.

  The utility displays the Directory Agent ID and indicates if the Active Directory Health Analyzer agent is running. You can stop, start, and restart the Active Directory Health Analyzer agent.

  You can also configure the Network settings and Logging settings.

Setting network settings

You can set the address and port number for the Active Administrator Data Service (ADS) server and the port number for the Active Directory Health Analyzer agent.

IMPORTANT: The default values for the ports are 15602 for the ADS Server and 15603 for the Active Directory Health Analyzer agent. If you change the value, verify that the port is open in Windows Firewall on the computer where the Active Directory Health Analyzer agent is installed.

To change a network setting

1. Launch **DAAgentConfig.exe**, which is located at **C:\Windows\DAAgent**.
2. Optionally, type the ADS Server Address and click **Set**.

   - AND -

   Optionally, type the ADS Server Port Number and click **Set**.

   - AND -

   Optionally, type the Active Directory Health Agent Port Number and click **Set**.

   A message warns that the Active Directory Health Analyzer agent may become disabled.
3. Click **Yes** to continue.
4. Click **Yes** to restart the agent.
   - To test the connection with the ADS server, click **Test Connection with Server**.
   - To test the connection with the Active Directory Health Analyzer agent, click **Test Connection with Agent**.

Enable logging

In Active Administrator, you can view recent log entries that are stored in memory. See Managing Active Directory Health Analyzer agents. If you require a log file for troubleshooting purposes, you can enable logging in the utility, which writes the log entries to a file.

Logging for the Active Directory Health Analyzer agent is disabled by default. Enable logging only if you need a log file for troubleshooting as the process may affect performance. The maximum size for the log file is 500 MB. Once the log file reaches its maximum size, it will automatically roll over. The log file is located at C:\Windows\DAAgent\DAAgent.log.

NOTE: When you enable logging, system performance may be affected. Use the utility for troubleshooting purposes only.

- Launch **DAAgentConfig.exe**, which is located at C:\Windows\DAAgent.
  - To enable logging, click **Enable**, and click **Yes** to confirm.
  - To view the log file, click **View Log File**.
  - To delete the log file, navigate to C:\Windows\DAAgent\, and delete the DAAgent.log file.

Excluding domain controllers

You can exclude specified domain controllers when analyzing forests, domains, and sites, and from matching Active Directory Health Check tests. Excluded domain controllers will also be removed from the Agent Configuration wizard.

To exclude domain controllers

1 Select **Active Directory Health | Agents**.

2 Open the **Analyzer Agents** tab.

3 Select **More | Excluded Domain Controllers**.

1 Click **Add**, and browse for the domain controllers to exclude.

2 Click **OK**.

Use **Remove** to remove selected domain controllers from the list.

Managing the Remediation Library

IMPORTANT: You must restart the ADS Service to load the ExcludedDomainControllers.xml file.

Remediations are actions that run when an alert reaches its critical threshold. Several built-in remediation actions are included, but you also can create custom remediations, which can be a PowerShell® script, VBS script, batch file, or .cmd file. Once you have populated the library with the remediations you need, you attach the remediations to alerts. See Setting alerts.

Topics

- Adding custom remediations
- Deleting custom remediations

To manage the Remediation Library

1 Select **Active Directory Health | Agents**.

2 Open the **Monitored Domain Controllers** tab, and click **Remediations**.

The Remediation Library displays custom remediations in the top pane and built-in remediations in the bottom pane. You can add, edit, or delete custom remediations. See Adding custom remediations. See Deleting custom remediations.You cannot edit or delete built-in remediations.

Table 32. Built-in remediations

Remediation action	Description
Reboot Computer	Reboots the specified computer
Restart Windows Service	Restarts the specified Windows service
Start Windows Service	Starts the specified Windows service
Stop Windows Service	Stops the specified Windows service
Stop Process	Stops the specified process.
Start Process	Starts the specified process.
Perform Active Directory Replications	Performs Active Directory replication for all servers in the forest.
Start Conflict and Deleted Folder Cleanup	Performs DFSR SYSVOL replicated folder conflict cleanup.

Adding custom remediations

If the built-in remediations do not provide what you need, you can create a custom remediation, which can be a PowerShell® script, VBS script, batch file, or .cmd file. After you create the custom remediation, you need to attach it to an alert. See Setting alerts.

NOTE: Custom remediation definitions are stored in \\AAServer\ActiveAdministrator\DACache\Remediations.xml.

To add a custom remediation

1. Select **Active Directory Health | Agents**.
2. Open the **Monitored Domain Controllers** tab, and click **Remediations**.
3. Click **Add** to create a new custom remediation.

   -OR-

   Click **Edit** to modify a selected custom remediation.
4. Enter a name for the remediation action.
5. Enter a description for the action.
6. Browse to locate the script to run.

   IMPORTANT: The script must be accessible from the Active Administrator® server.
7. If arguments are required, select the check box and enter a description of the arguments to use.

   NOTE: Arguments are supplied when you attach a remediation action to an alert. The description will help another user provide the necessary arguments. See Setting alerts.
8. Select the Active Directory® objects on which the script is supported.

   NOTE: Built-in remediation actions can run on any Active Directory® object.
9. Click **OK**.

Deleting custom remediations

To delete a custom remediation

1. Select **Active Directory Health | Agents**.
2. Open the **Monitored Domain Controllers** tab, and click **Remediations**.
3. Select the remediations to delete.
4. Click **Delete**.

Analyzing Active Directory health

The Active Directory Health Analyzer displays read-only real-time data about forests, sites, domains and domain controllers so you can monitor the health of your organization. The data on the screen you are viewing is refreshed automatically every minute by default. You also can refresh the data manually by clicking **Refresh**.

NOTE:

- The Active Directory Health Analyzer agent must be monitoring at least one domain controller to view objects in the Active Directory Health Analyzer tree. See Managing monitored domain controllers and Installing Active Directory Health Analyzer agents.
- The Active Directory Health Analyzer agent sends data every five minutes to the Active Administrator® database. When a data collector falls out of range, data is sent every 30 seconds to the database. You can adjust the automatic refresh rate from 30 to 3600 seconds or turn off the automatic refresh. If you turn off the automatic refresh, you can refresh the screens manually. See Setting Active Directory Health Analyzer options.
- By default, the Active Directory Health Analyzer screens are cached. As you view more and more screens on multiple domain controllers, more memory is consumed. To clear the cache, you must restart Active Administrator. You can turn off the cache, but the screens are not saved as you navigate from screen to screen. See Setting Active Directory Health Analyzer options.

Topics

- Managing the Active Directory Health Analyzer tree
- Using the analyzer pages
- Analyzing health of all domain controllers
- Analyzing health of a selected domain controller
- Analyzing health of all domains
- Analyzing health of a selected domain
- Analyzing health of all sites
- Analyzing health of a selected site
- Analyzing the health of a forest

Managing the Active Directory Health Analyzer tree

The Active Directory Health Analyzer tree displays forests, domains, sites, and domain controllers. By default, unmonitored domain controllers display beneath a selected domain. If you want to see only monitored domain controllers beneath a selected domain, clear the **Display unmonitored domain controllers in the tree view** check box in **Settings | User Options**. See Setting Active Directory Health Analyzer options.

NOTE: You receive a message if there are no Active Directory Health Analyzer agents installed or if the selected domain controller is not in a monitored site if site agents are being used. The domain controller is added, but you need to install the Active Directory Health Analyzer agent. See Installing Active Directory Health Analyzer agents.

- To quickly add a selected unmonitored domain controller to the list of monitored domain controllers, click **Add Domain Controller**, and click **Refresh**. See Adding monitored domain controllers.
- To filter the tree, type in the **Filter objects** box. The list filters as you type.
- To refresh the tree, click **Refresh**.

Using the analyzer pages

All the analyzer pages have a similar tool bar and shortcut links that help you with analyzing the health of Active Directory.

Tool bar

Table 33. Analyzer tool bar

Option	Description
Refresh	Refresh the tree.
Refresh View	Refresh the data on the page.
Alert Details	View the details of a selected alert.
Copy Alert	Copy a selected alert to the clipboard.
Diagnose	Open the Diagnostic Console. See Diagnostic Console. **NOTE:** Not available for all objects.
Mute	Mute alerts. See Muting alerts. **NOTE:** Not available for all objects.
Mute History	View the history of mutes. See Viewing mute history.
Schedule Mute	Schedule muting alerts. See To schedule muting alerts.
Mute Schedule	View or modify the schedule of mutes. See To view and modify a scheduled mute..

Shortcut Links

Table 34. Analyzer shortcut links

Option	Description
Details	View the details of a selected alert.
Copy	Copy a selected alert to the clipboard.
Create Notification	Create a notification in which the selected alert should be included. See Creating alert notifications.
Add To Notification	Set the notifications in which the selected alert should be included.

Page heading

The top pane on each analyzer page displays the names and numbers of objects and remains in the display when you change tabs. A count of the current alerts, critical and warnings, displays in the upper right-hand corner.

- To refresh the data on the page, click **Refresh**.
- To open the Diagnostic Console, click **Diagnose**. See Diagnostic Console.

Alerts tab

The **Current Alerts** tab lists the alerts for the object. A count of the current alerts, critical and warnings, displays in the upper right-hand corner.

- Alerts are enabled by default. Both alerts and data collectors can be enabled and disabled. See Setting alerts and Setting data collectors.
- To view details about an alert, click **Alert Details** or double-click an alert.

You see the alert severity; the alert value; and details about the alert such as domain, the object name, forest name, when the alert started, and the values observed during the alert. Click **Copy** to copy the alert to the clipboard and click **Notifications** to see who received the listed notifications.

Analyzing health of all domain controllers

You can view information on all monitored domain controllers or a selected monitored domain controller. To view information on a selected domain controller, see Analyzing health of a selected domain controller.

To analyze the health of all monitored domain controllers

1. Select **Active Directory Health | Analyzer**.
2. Expand the tree, and select **Monitored Domain Controllers**.
3. Use the tool bar and the tabs to view and manage domain controller health. See Using the analyzer pages.

   The **Summary** tab lists all the domain controllers and indicates the number of critical alerts and warnings for each. A vertical bar next to each domain controller indicates its status. A red bar indicates the domain controller has alerts.

   - To group the list by domain, select **Group by domain**.
   - To filter the list of monitored domain controllers, type in the **Filter domain controller** box. The list filters as you type.
   - To display the analyzer window for a selected domain controller, double-click a domain controller. See Analyzing health of a selected domain controller.

   The **Current Alerts** tab lists the alerts for all the domain controllers. See Using the analyzer pages.

Analyzing health of a selected domain controller

You can view information on all monitored domain controllers or a selected monitored domain controller. To view information on all domain controllers, see Analyzing health of all domain controllers.

To analyze health on a selected domain controller

1. Select **Active Directory Health | Analyzer**.
2. Expand the tree, and expand **Monitored domain controllers**.
3. Select a domain controller.
4. Use the tool bar, page heading, and the tabs to view and manage domain controller health. See Using the analyzer pages.

   The page heading displays general information about the selected site.

   Table 35. Domain controller general information

Field	Description
Domain	Name of the domain in which the domain controller resides
Site	Name of the site in which the domain controller resides
Forest	Name of the forest in which the domain resides
OS version	Version of the operating system
System up time	Duration of time the domain controller has been running
Read only DC	Indicates if the domain controller is a read-only domain controller (RODC)

Table 35. Domain controller general information

Field	Description
Global catalog	Indicates if the domain controller is a global catalog server
Monitored by	Name of the domain controller on which the agent is installed that is monitoring the selected domain controller
Last updated	Date and time the domain controller was last updated

The bottom pane changes depending on the tab you select. The following table lists the tabs and the information displayed.

NOTE: A message displays if there is no data to display. There may be a pending workload evaluation or the system is waiting on data from the Active Directory Health Analyzer agent. Check to see if the Active Directory Health Analyzer agent is running. If there is no data because the domain controller is not being monitored, you need to install the agent. See Installing Active Directory Health Analyzer agents.

Data collectors provide the input to the various tabs. Some data collectors can be enabled or disabled. See Managing data collectors. If you do not see the corresponding data, make sure the data collector is enabled and the necessary permissions are set. To check the required minimum permissions, see the dialog box for the individual data collector or the Alerts Appendix.

The remaining data collectors used to provide information to the tabs are not available for management and are provided to Active Administrator® through Windows® Management Instrumentation (WMI).

Table 36. Domain controller tabs

Tab	Description	Data Collectors
Summary	Displays the data collected in the indicated time frame for the enabled Performance Counters for the selected forest, domain, site, or monitored domain controller. • To view more detail, select **View Trends**. • To view the full chart for a selected Performance Counter, click **View Details**.	Performance Counters data collectors
Services	Displays the status of Windows services. If a service is running, but has stopped at a point in time, that stoppage is indicated with red.	Windows Services data collectors
Server	Displays information about the server, the server time, memory details, disk details, and network adapters.	General data collectors: Domain controller time synchronization Logic disk details
Active Directory	Displays Active Directory® database and SYSVOL disk usage and LDAP response time.	Validation data collectors General data collectors: Active Directory database details Domain controller relative identifier (RID) LDAP response time SysVol details
Current Alerts	Displays the current alerts for the selected item in the tree. See Using the analyzer pages.	Alerts are enabled by default and correspond to data controllers. Both alerts and data collectors can be enabled and disabled. See Setting alerts and Setting data collectors.

Table 36. Domain controller tabs

Tab	Description	Data Collectors
Applications	Displays installed applications on the selected monitored domain controller. Applications installed or removed in the last 24 hours are listed in a separate pane. • Use the **Filter Installed Applications by Name** option to search for specific applications.	Not available for management
Updates	Displays installed updates on the selected monitored domain controller. Updates installed or removed in the last 24 hours are listed in a separate pane. To view information about the update in the default web browser, double-click the update. • Use the **Filter Installed Windows Updates by Name** option to search for specific updates.	Not available for management

Analyzing health of all domains

You can view information on all domains or a selected domain. To view information on a selected domain, see Analyzing health of a selected domain.

NOTE: There must be at least one monitored domain controller in a domain for the domain to appear in the tree.

To analyze health of all domains

1. Select **Active Directory Health | Analyzer**.
2. Expand the tree, and select **Domains**.
3. Use the tool bar, the page heading, and the tabs to view and manage domain health. See Using the analyzer pages.
   - The **Summary** tab lists all the domains and indicates the number of critical alerts and warnings for each domain. A vertical bar next to each domain indicates its status. A red bar indicates the site has alerts.
   - The **Current Alerts** tab lists the alerts for all the domains. See Using the analyzer pages.

Analyzing health of a selected domain

You can view information on all domains or a selected domain. To view information on all domains, see Analyzing health of all domains.

To view information on a selected domain

1. Select **Active Directory Health | Analyzer**.
2. Expand the tree, and expand **Domains**.
3. Select a domain.
4. Use the tool bar, the page heading, and the tabs to view and manage domain health. See Using the analyzer pages.

The page heading displays general information about the selected domain. Table 37 lists the fields that display.

Table 37. Domain general information

Field	Description
Domain	Name of the selected domain.
Domain controllers	Number of domain controllers.
GC servers	Number of global catalog (GC) servers
RODC servers	Number of read-only domain controllers (RODCs)
Functional level	Functional level of the forest, domain, or site
PDC owner	Owner of the primary domain controller (PDC) Flexible Single Master Operation (FSMO) role
RID master	Owner of the relative identifier (RID) FSMO role
Infrastructure master	Owner of the infrastructure FSMO role
Operations master consistent	Indicates if all the domain controllers report the same operation masters
Functional level consistent	Indicates if all the domain controllers report the same functional level

The bottom pane changes depending on the tab you select. Table 38 lists the tabs and the information displayed.

Table 38. Domain tabs

Tab	Description
Summary	Lists all the domain controllers in the selected domain, the domain and site in which the domain controller resides, and the number of alerts for each domain controller. • To filter the list of domain controllers, type in the **Filter domain controllers** box. The list filters as you type. • To group the list of domain controllers by site, select **Group by site**.
Replication Latency	Lists the replication latency times for a domain controller and its replication partners. **NOTE:** The Replication latency data collector is disabled by default. If you want to monitor replication latency, enable this data collector. See Setting data collectors and Replication latency.
GC Replication Latency	Lists the replication latency times for the domain controller and servers hosting the global catalog. **NOTE:** The Global catalog server replication latency data collector is disabled by default. If you want to monitor global catalog replication latency, enable this data collector. See Setting data collectors and Global catalog server replication latency.
Current Alerts	Displays the current alerts for the selected item in the tree. See Using the analyzer pages.

Analyzing health of all sites

You can view information on all sites or a selected site. To view information on a selected site, see Analyzing health of a selected site.

NOTE: There must be at least one monitored domain controller in a site for the site to appear in the tree.

To analyze health on all sites

1 Select **Active Directory Health | Analyzer**.

2 Expand the tree, and select **Sites**.

3 Use the tool bar, the page heading, and the tabs to view and manage site health. See Using the analyzer pages.

The page heading displays general information about the selected site. Table 39 lists the fields that display.

Table 39. Site general information

Field	Description
Forest	Name of the forest.
Domains	Number of domains.
Domain controllers	Number of domain controllers.
Sites	Number of sites.
Empty sites	Number of empty sites.
GC servers	Number of global catalog (GC) servers.
RODC servers	Number of read-only domain controllers (RODCs).
Application partitions	Number of application partitions.
Bridgehead servers	Number of bridgehead servers.
Functional level	Functional level of the site.
Domain naming master	Name of the domain controller with the domain naming master role.
Schema master	Name of the domain controller with the schema master role.
Operations master consistent	Indicates if all the domain controllers report the same operation masters.
Schema master consistent	Indicates if all the domain controllers report the same operation masters.
Functional level consistent	Indicates if all the domain controllers report the same functional level.

The **Summary** tab lists all the sites and indicates the number of critical alerts and warnings for each site. A vertical bar next to each site indicates its status. A red bar indicates the site has alerts.\

- To filter the list of sites, type in the **Filter sites** box. The list filters as you type.
- To refresh the list, click **Refresh**.

The **Current Alerts** tab lists the alerts for all the sites. See Using the analyzer pages.

Analyzing health of a selected site

You can view information on all sites or a selected site. To view information on all sites, see Analyzing health of all sites.

To analyze health on a selected site

1 Select **Active Directory Health | Analyzer**.

2 Expand the tree, and expand **Sites**.

3 Select a site.

4 Use the tool bar, the page heading, and the tabs to view and manage site health. See Using the analyzer pages.

The page heading displays general information about the selected site. Table 39 lists the fields that display.

Table 40. Site general information

Field	Description
Group caching enabled	Indicates if group caching is enabled or disabled.
Intersite topology generation	Indicates if intersite topology generation is enabled or disabled.
Intrasite topology generation	Indicates if intrasite topology generation is enabled or disabled.
Intersite topology generator	Name of the intersite topology generator.

The bottom pane changes depending on the tab you select. The following table lists the tabs and the information displayed.

Table 41. Site tabs

Tab	Description
Summary	Lists all the domain controllers in the selected domain and indicates if the domain controller is: • a global catalog (GC} • a read-only domain controller (RODC) • a bridgehead server • a primary domain controller (PDC) • an infrastructure master • a relative identifier (RID) master • Schema master • Naming master
Site Links	Lists the site link name, the site to which the selected site is linked, the relative cost of using the link, as defined by the administrator. The **Schedule** column indicates how the inter-site link is connected. • **Permanent** indicates the link is connected all of the time as a schedule is not assigned. • **Scheduled** indicates the link is connected occasionally on a schedule. • **Disabled** indicates the link is never connected. A schedule is assigned to the connection, but there is no scheduled time when the link is connected.
Current Alerts	Displays the current alerts for the selected item in the tree. See Using the analyzer pages.

Analyzing the health of a forest

To analyze health of the forest

1 Select **Active Directory Health | Analyzer**.

2 Select the forest.

3 Use the tool bar, the page heading, and the tabs to view and manage site health. See Using the analyzer pages.

The page heading displays general information about the forest. Table 42 lists the fields that display.

Table 42. Forest general information

Field	Description
Forest	Name of the forest.
Domains	Number of domains.

Table 42. Forest general information

Field	Description
Domain controllers	Number of domain controllers.
Sites	Number of sites.
Empty sites	Number of empty sites.
GC servers	Number of global catalog (GC) servers.
RODC servers	Number of read-only domain controllers (RODCs).
Application partitions	Number of application partitions.
Bridgehead servers	Number of bridgehead servers.
Functional level	Functional level of the site.
Domain naming master	Name of the domain controller with the domain naming master role.
Schema master	Name of the domain controller with the schema master role.
Operations master consistent	Indicates if all the domain controllers report the same operation masters.
Schema master consistent	Indicates if all the domain controllers report the same operation masters.
Functional level consistent	Indicates if all the domain controllers report the same functional level.

The **Summary** tab lists all the monitored domains and indicates the number of critical alerts and warnings for each domain. A vertical bar next to each domain indicates its status. A red bar indicates the domain has alerts.

- To filter the list of domains, type in the **Filter domains** box. The list filters as you type.
- To refresh the list, click **Refresh**.

The **Current Alerts** tab lists the alerts for the forest. See Using the analyzer pages.

Analyzing Microsoft Entra ID

Once you install the Microsoft Entra Connect Health Monitoring Agent on a computer where Microsoft Entra Connect is installed, you can view a summary of the output of the Synchronization Service Manager and manage the Microsoft Entra Connect Scheduler; view the output of the Synchronization Service Manager; view warnings, errors, and events that occurred over the last 24 hours; and view a list of the installed connectors, and properties, partitions, and run profiles of selected connectors.

NOTE:

- Azure Active Directory is now Microsoft Entra ID.
- Users must have Microsoft Entra Connect enabled to use the Microsoft Entra Connect submodule. See Defining role-based access.

Topics

- Installing the Microsoft Entra Connect Health Monitoring Agent
- Setting up the Microsoft Entra Connect application
- Viewing Microsoft Entra Connect status
- Viewing Microsoft Entra Connect alerts
- Monitoring Microsoft Entra Connect operations
- Viewing Microsoft Entra Connect events
- Monitoring Microsoft Entra Connect operations

- Viewing Microsoft Entra Connect events
- Searching the Metaverse
- Viewing Microsoft Entra Connect connectors
- Managing the Microsoft Entra Connect Health Monitoring Agent

Installing the Microsoft Entra Connect Health Monitoring Agent

You must install the Microsoft Entra Connect Health Monitoring Agent on each computer that you want to monitor. Microsoft Entra Connect must also be installed on that computer.

Before you begin installation, you need the following information:

- The path from where you want to run the Microsoft Entra Connect Health Monitoring Agent.
- The name of the Active Administrator server. To see the server name, select **Settings | AA Server**.
- The name of the database server where the Microsoft Entra Connect database is installed and the name of the Microsoft Entra Connect database (ADSync is the default database). Only required if you choose not to use the default database, which is limited to 50,000 objects.

To deploy the Microsoft Entra agent

1. Locate **C:\Program Files\Quest\ActiveAdministrator\Server\SLAgent\AADCAgent**.
2. Copy all the files in the **AADCAgent** folder.
3. Locate a folder on the target server where you want to place the files. For example: **C:\Data\AADCAgent**.

   The Windows service will be installed in this location and the Microsoft Entra Connect Health Monitoring Agent will run out of this location.
4. Copy the files to the folder on the target server.
5. Right-click **Setup.exe**, and select **Run as Administrator**.

   -OR-

   Select **Start | Command Prompt (Admin)**, navigate to the folder where you copied the files, type **Setup**, and press **Enter**.
6. Type **Y** and press **Enter** to install the Microsoft Entra Connect Health Monitoring Agent.
7. Type a name for the agent, and press **Enter**.

   If you press **Enter** without entering a name, the default is the computer name, which displays next to **Agent name** in the prompt.
8. Type the name of the Active Administrator server, and press **Enter**.
9. For the Microsoft Entra Connect database, you have two options.
   - To use the default database, which is limited to 50,000 objects, type **Y**, and press **Enter**.
   - To use another database, type **N**, and press **Enter**.
     a. Type the name of the database server where the Microsoft Entra Connect database is installed, and press **Enter**.
     b. Type the name of the Microsoft Entra Connect database (default is ADSync), and press **Enter**.

   After the installation is complete, use the **Agents** tab or Setup.exe from the command line to manage the Microsoft Entra Connect Health Monitoring Agent. See Managing the Microsoft Entra Connect Health Monitoring Agent.

Setting up the Microsoft Entra Connect application

Setting up the Microsoft Entra Connect application is a two-step process. First create the Microsoft Entra Connect application through the Microsoft Entra admin center, and then configure settings in Active Administrator.

The default port to use for Microsoft Entra Connect is 15604. The AADCAgentPortNumber property is set in the AADCSettings.xml file located in ProgramData\Quest\ActiveAdministrator\AADCAgent folder.

Topics

- Adding the Microsoft Entra Connect application
- Configuring Microsoft Entra Connect application settings

Adding the Microsoft Entra Connect application

Refer to Microsoft documentation for details on how to create a Microsoft Entra application.

For Active Administrator, ensure that you enable the following permissions for the application:

- Application: **Read directory data**
- Delegated: **Access the directory as the signed-in user**
- Delegated: **Sign in and read user profile**

The next step is to configure the Microsoft Entra Connect app settings in Active Administrator. See Configuring Microsoft Entra Connect application settings.

Configuring Microsoft Entra Connect application settings

To configure Microsoft Entra Connect application settings

1. Select **Active Directory Health | Microsoft Entra Connect**.
2. Select the domain.
3. Open the **Agents** tab.
4. Click **Microsoft Entra App Settings**.
5. In the **Tenant** box, enter the fully qualified name of the Microsoft Entra domain.
6. In the **Application Name** box, enter **AAADConnectApp** as the display name.
7. In the **Application ID** box, enter the Application ID that you recorded from the Microsoft Entra admin center.
8. In the **Security Key** box, enter the Security key that you copied from the Microsoft Entra admin center.
9. Click **OK**.

Viewing Microsoft Entra Connect status

On the **Summary** tab you can view a summary of the output of the Synchronization Service Manager and manage the Microsoft Entra Connect Scheduler on each computer where you installed the Microsoft Entra Connect Health Monitoring Agent. See Installing the Microsoft Entra Connect Health Monitoring Agent.

To view Microsoft Entra Connect status

1. Select **Active Directory Health | Microsoft Entra Connect**.

2 Select an agent.

3 Open the **Summary** tab, if necessary.

The date and time of the last sync and the results of the sync display, as well as the date and time the display was last updated.

The **Summary** tab is divided into six sections:

- Microsoft Entra Connect Environment
- Running Connectors
- Synchronization Status
- Service Status
- Connector Statistics
- Microsoft Entra Connect events

Microsoft Entra Connect Environment

Table 43. Microsoft Entra Connet Environment indicators

Indicator	Description
Computer name	Name of the computer where the Microsoft Entra Connect agent is installed.
Operating system	Operating system on the computer where the Microsoft Entra Connect agent is installed
Microsoft Entra Connect version	Version of Microsoft Entra Connect that is running.
SQL server name	Name of the database server where the Microsoft Entra Connect database is installed
Database name	Name of the Microsoft Entra database
Database size	Size of the Microsoft Entra Connect database.
Last connectivity test completed	Indicates if the last connectivity test was successful or failed at the time and date shown. The connectivity test runs automatically every 15 minutes. • To view details about the test, click **Test Details**. You can copy the information to a text file. • To run the test, click **Test Now**. • To view the history of the past 30 tests, click **History**.

Running Connectors

Indicates the date and time when the connectors last ran and if any connectors are currently running. To rerun the connectors, click **Refresh**.

Synchronization Status

Table 44. Synchronization status indicators

Indicator	Description
Last sync	Indicates the date and time of the last synchronization.
Next sync	Indicates the date and time of the next synchronization. **NOTE:** To start a synchronization manually, click **Start Synchronization**.
Allowed sync cycle interval	Displays the minimum amount of time (30 minutes) between synchronization cycles allowed by Microsoft Entra ID.
Effective sync cycle interval	Displays the synchronization cycle schedule currently in effect.

Table 44. Synchronization status indicators

Indicator	Description
Sync cycle enabled	Indicates if the synchronization cycle is enabled. To disable or enable the synchronization cycle, click **Synchronization Settings**.
Customized sync cycle interval	Displays the amount of time between synchronization cycles. To set the time interval, click **Synchronization Settings**.
Next sync cycle policy type	Indicates if the next run will process delta changes (Delta), or run a full import and sync (Initial).
Purge run history interval	Displays the amount of time that operation logs are kept. The default is to keep these logs for 7 days. To set the amount of time to keep the logs, click **Maintenance Settings**.
Maintenance enabled	Indicates if the maintenance process is enabled. The maintenance process updates the certificates/keys and purges the operations log. To disable or enable maintenance, click **Maintenance Settings**.
Staging mode enabled	Indicates if staging mode is enabled. If enabled, suppresses exports from running, but import and synchronization still run.
Scheduler suspended	Indicates if the scheduler is blocked from running, which may happen during an upgrade.
Sync cycle in progress	Indicates if the scheduler is running the import, sync, and export processes.

Table 45. Synchronization status options

Option	Description
Start Synchronization	Start the synchronization process.
Synchronization Settings	Enable/disable synchronization. Set the time interval between synchronization cycles.
Maintenance Settings	Enable/disable maintenance. Set the amount of time to keep the operation logs,
View Configuration	View the Microsoft Entra Connect agent configuration. Click **Copy** to copy the list to the clipboard.

Service Status

Indicates the status of the services that run for Microsoft Entra Connect. You can restart, start, and stop the services. If you restart or start a service, you are asked for credentials.

Connector Statistics

Indicates the number of exports added, updated, and deleted, and the total number of connectors.

Microsoft Entra Connect events

Lists the last five Microsoft Entra Connect warnings and errors and the last five events. To view the events over the last 24 hours, open the **Events** tab. See Viewing Microsoft Entra Connect events.

- To view details about the warning, error, or event, double-click the entry.
- To sort the list, click in a column header.

Viewing Microsoft Entra Connect alerts

On the Alerts tab, you can view current alerts, view alert history, clear alerts, and manage alert notification. To see a list of alerts, see Microsoft Entra Connect alerts.

To view alerts

1 Select **Active Directory Health | Microsoft Entra Connect**.

2 Select an agent.

3 Open the **Alerts** tab.

The current active alerts display.

4 Use the menu options to view and manage the alerts.

Table 46. Alerts options

Option	Description
Refresh	Refresh the list of alerts.
Properties	View details about a selected alert, such as the last time it was checked, which server is involved, a description of the alert, and the alert history. You also can clear an alert, except for Windows® Services alerts.
Clear	Clear the selected alert. **NOTE:** You cannot clear Windows Services alerts. If the alert does not clear itself, you can start and stop the service. See Stopping and starting AFS and ADS services.
Alert History	View a list of the last 100 alerts. Click **Load More** to view more alerts. You also can double-click a selected alert to view details.
Alert Notification	Enable/disable alert notifications and manage the Microsoft Entra Connect Notifications email list. **NOTE:** To manage the Microsoft Entra Connect Notifications email address list, see Managing email addresses.

Monitoring Microsoft Entra Connect operations

On the **Operations** tab you can view the output of the Synchronization Service Manager on each computer where you installed the Microsoft Entra Connect Health Monitoring Agent. See Installing the Microsoft Entra Connect Health Monitoring Agent.

To monitor operations

1 Select **Active Directory Health | Microsoft Entra Connect**.

2 Select an agent.

3 Open the **Operations** tab.

4 The top pane displays the first 50 operations for the selected agent. The **Sync statistics** area displays a summary of the list of operations.

- To load more operations, click **Load Next Page**.
- To sort the columns, click a column header.
- To filter the list, click **Filter**. You can filter by date or date range. To remove the filter, click **Remove Filter**.
- To refresh the list, click **Refresh**.
- To clear the log, click **Purge Log**.

5 Select an operation to view details in the lower panes.

The **Export Statistics** pane lists all the details for the selected operation.

- To see a list of the objects affected by the operation, click **Affected Objects**. You can sort the list by clicking in a column header.

If the selected operation is an export, the **Connection Status** pane shows which server was used for the connection and any errors that occurred.

Viewing Microsoft Entra Connect events

On the **Events** tab you can view warnings, errors, and events that occurred over the last 24 hours on each computer where you installed the Microsoft Entra Connect Health Monitoring Agent. See Installing the Microsoft Entra Connect Health Monitoring Agent.

NOTE: You can view the last five warnings, errors, and events on the **Summary** tab. See Viewing Microsoft Entra Connect events.

To view events

1. Select **Active Directory Health | Microsoft Entra Connect**.
2. Select an agent.
3. Open the **Events** tab.

   The top pane lists the warnings and errors that occurred over the last 24 hours. The bottom pane lists the events that occurred over the last 24 hours.

   - To view details about the warning, error, or event, double-click the entry or click **Details**.
   - To sort the list, click in a column header.

Searching the Metaverse

The Metaverse database maintains data that is synced between the Microsoft Entra Connect database and the Active Administrator database. Searching the Metaverse helps in troubleshooting data-related problems that may occur during synchronization.

NOTE: To compare the Metaverse data to the Microsoft Entra Connect database, you must select the attributes to sync in Microsoft Entra Connect.

1. Open Microsoft Entra Connect.
2. Select **Sync | Optional Features**.
3. Select **Directory extension attribute sync**.
4. Click **Next**.
5. Select the attributes to sync. Only selected attributes are included when comparing the Metaverse data with Microsoft Entra Connect.

To search the Metaverse

1. Select **Active Directory Health | Microsoft Entra Connect**.
2. Select an agent.
3. Open the **Metaverse Search** tab.
4. There are two ways to search the Metaverse.
   - To display all data in the Metaverse, click **Find All**.
   - To search for specific data in the Metaverse, click **Search Filter**.
     a. Select the scope.
     b. Select the attribute.
     c. Select the operator and enter a value.
     d. Click **Add**.

e Repeat for each search value you want to use.

All search values are ANDed, so all must be true to produce a result.

f Click **OK**.

5 Double-click an item to view details.

-OR-

Select an item and click **Properties**.

6 You can compare the attributes in the Metaverse to Active Directory or Microsoft Entra . Any mismatches are indicated in red.

Table 47. Metaverse compare options

Option	Description
Compare with Active Directory	Attributes in the Metaverse are compared to attributes in the Active Directory database. **NOTE:** You must provide credentials for the server where Active Administrator is installed.
Compare with Microsoft Entra ID	Attributes in the Metaverse are compared to attributes in the Active Directory Connect database. **NOTE:** Only attributes that are selected in Microsoft Entra Connect are available for matching.

Viewing Microsoft Entra Connect connectors

On the **Connectors** tab, you can view a list of the installed connectors, and properties, partitions, and run profiles of selected connectors.

To view connectors

1 Select **Active Directory Health | Microsoft Entra Connect**.

2 Select an agent.

3 Open the **Connectors** tab.

4 Use the menu to view details about a selected connector. You can view **Properties**, **Partitions**, and **Run Profiles**.

Managing the Microsoft Entra Connect Health Monitoring Agent

After the installation is complete, you can use the **Agents** tab or **Setup.exe** at a command line prompt to manage the Microsoft Entra Connect Health Monitoring Agent.

NOTE: Installing the Microsoft Entra Connect Health Monitoring Agent must be initiated from a command line prompt. See Installing the Microsoft Entra Connect Health Monitoring Agent.

Topics

- Managing the agent from the Agents tab
- Managing the agent from the command line

Managing the agent from the Agents tab

NOTE: If the target server is not in a trusted forest or domain, controlling the agent service status is not possible from the **Agents** tab. To start, stop, and restart the Microsoft Entra Connect Health Monitoring Agent, log on to the target server and run the setup command with /start, /stop, or /restart. See Managing the agent from the command line.

To manage the agent from the Agents tab

1. Select **Active Directory Health | Microsoft Entra Connect**.
2. Select an agent.
3. Open the **Agents** tab.
4. Use the menu to manage the agent.

Table 48. Microsoft Entra Connect agent menu options

Option	Description
Refresh	Refresh the display. The display is refreshed automatically every 30 seconds.
Properties	View properties of the selected agent. Properties include the name of the computer where the agent is installed; the agent ID; the status of the agent; version of the agent; date and time when the agent was installed and registered, returned a heartbeat, and was set online; last attempt of the heartbeat; last attempt at setting the agent online; and the description of the error that occurred. **NOTE:** The date and time of the last attempted heartbeat and the error description display only if the heartbeat fails. The system retries every 30 seconds. **NOTE:** The date and time of the last attempt at setting the agent online and the error description display only if setting the agent online fails. The system retries every 30 seconds.
Microsoft Entra App Settings	Configure the Microsoft Entra Connect application. See Setting up the Microsoft Entra Connect application.
Start	Start the selected agent (trusted forest and domains only).
Stop	Stop the selected agent (trusted forest and domains only).
Restart	Restart the selected agent (trusted forest and domains only).
Remove	Remove an offline agent from the list of Microsoft Entra Connect Health agents. **NOTE:** The agent must be uninstalled and re-installed to resume monitoring the server. See Managing the agent from the command line.
Agent Log	View the log of the selected agent.

Managing the agent from the command line

To manage the Microsoft Entra Connect Health Monitoring Agent from the command line

1. Select **Start | Command Prompt (Admin).**
2. Navigate to the folder where you copied the files.
3. Type **Setup** <option>. See Table 49 Options for Setup.exe.
4. Press **Enter**.

Setup.exe

Setup.exe is located at **C:\Program Files\Quest\ActiveAdministrator\Server\SLAgent\AADCAgent**.

Usage

```
Setup <option>
```

NOTE: If you do not supply an option, running Setup installs the Microsoft Entra Connect Health Monitoring Agent.

Table 49. Options for Setup.exe

Option	Description
`/i`	Installs the Microsoft Entra Connect Health Monitoring Agent.
`/i /setFWRules`	Installs the Microsoft Entra Connect Health Monitoring Agent and configures Windows Firewall to allow the agent to communicate with the Active Administrator Data Service (ADS).
`/u`	Uninstalls the Microsoft Entra Connect Health Monitoring Agent.
`/u -q`	Uninstalls the Microsoft Entra Connect Health Monitoring Agent quietly.
`/start`	Starts the Microsoft Entra Connect Health Monitoring Agent.
`/stop`	Stops the Microsoft Entra Connect Health Monitoring Agent.
`/restart`	Restarts the Microsoft Entra Connect Health Monitoring Agent.
`/status`	Gets the status of the Microsoft Entra Connect Health Monitoring Agent.
`/setDBservername`	Sets the name of the computer running SQL Server. Optional to use `/name=[server name]`.
`/setDBname`	Sets the name of the database. Optional to use `/name=[database name]`.
`/setDBuser`	Sets the username and password of the account running SQL Server. Optional to use `/user=[user]` and `/password=[password]`.
`/setFWrules`	Sets the firewall rules to allow the Microsoft Entra Connect Health Monitoring Agent to communicate with the Active Administrator Data Service (ADS).
`/clearFWrules`	Clears the firewall rules for the Microsoft Entra Connect Health Monitoring Agent.
`/clearDBuser`	Clears the account running SQL Server and reverts to integrated security.
`/config`	Dumps the configuration of the Microsoft Entra Connect Health Monitoring Agent.
`/testaaserver`	Validates the connection to the Active Administrator server.
`/taas`	Validates the connection to the Active Administrator server.
`/tac`	Validates the connection to the Microsoft Entra Connect Health Monitoring Agent.
`/testagentconn`	Validates the connection to the Microsoft Entra Connect Health Monitoring Agent.
`/enablelogging`	Enables logging to the AADCAgentlog file.
`/disablelogging`	Disable logging to the AADCAgentlog file.
`/printlog`	Prints the agent logs
`/printlog /last`	Prints the last 10 log entries.
`/pl`	Prints the agent logs
`/pl /last`	Prints the last 10 log entries.
`/h[elp]`	Shows this screen.
`/?`	Shows this screen.

Managing Active Directory Health Analyzer alerts

Active Directory Health Analyzer alerts have two levels of severity: warning and critical. As a situation escalates, a warning alert is generated, indicating that a lower priority threshold has been violated. As the severity of the error increases, a critical alert is generated, indicating that the higher priority threshold has been exceeded.

A number of attributes can be customized for each of these levels, including the threshold value, duration before an alert occurs, duration before an alert clears. If a remediation is attached to the alert, specified actions can run when the alert reaches the critical state. A lightning bolt indicates a remediation is attached to an alert.

There are two ways to view alerts. You can view current alerts for selected forests, domains, sites, and domain controllers while using the Analyzer feature. The Alerts feature displays all the current alerts and alert history. You also can generate an alert history report to send to recipients through email or save the report to a file.

If you know about an upcoming maintenance to the system or some other event that may cause a lot of unnecessary alerts, you can mute the collection of alerts. During the mute period, no alerts are collected into the Active Administrator® database and no alert notifications are sent. If you forget to remove the mute, the mute is cleared automatically after one hour.

NOTE: If you have a license for the Active Directory Health module, you can forward the Active Directory Health alerts generated by Active Directory Health Analyzer agents to Microsoft® System Center Operations Manager (SCOM) and SNMP managers. These alerts will appear in the **Quest Alert Events** view, under the **Quest Active Administrator** folder in the **Operations Manager Monitoring** pane and in the **SNMP Manager**. See the *Active Administrator Install Guide* for instructions on connecting to SCOM and enabling SNMP notifications.

Topics

- Setting alerts
- Purging and archiving alert history
- Viewing alerts and alert history
- Filtering alert history
- Generating an alert history report
- Muting alerts
- Clearing mutes
- Viewing mute history

Setting alerts

You can enable, disable, and edit alerts for a selected monitored domain controller, domain, forest, or site, or for all monitored domain controllers, domains, forests or sites. To see a list of the alerts that you can manage and the corresponding data collector that captures the data for the alert, see the Alerts Appendix.

NOTE: For the alert to appear, the data collector for the specified alert must be enabled. See Managing data collectors and Setting data collectors.

You also can attach a remediation action to an alert. Remediations are actions that run when an alert reaches its critical threshold. There are several built-in remediation actions that you can choose or you can create custom remediations. All remediations are stored in the Remediation Library. See Managing the Remediation Library.

To set alerts

1. Select **Active Directory Health | Agents**.
2. Open the **Monitored Domain Controllers tab**, if necessary.

3 Select a domain controller, and select **Settings | Domain Controllers**, **Domain**, **Forest**, or **Site**.

4 Click **Alerts**.

5 All the alerts for the selected object are displayed. Disabled alerts are indicated by a gray icon.

- To filter the list, start typing in the **Filter alerts** box. The list filters as you type.

6 Double-click an alert.

7 Modify the alert general settings.

- All the alerts are system alerts, so you cannot change the data or the type. You can change the name, description, operator, and threshold values for warning (⚠) and critical (⛔).

  NOTE: For the Boolean type, you can select only the **Equal To** or **Not Equal To** operators.

  IMPORTANT: For the RODC allowed/denied password alerts, you must set at least one authoritative Read-only domain controller (RODC). See Setting an authoritative RODC.

- To reset the alert to the original default settings, click **Reset.**

8 To attach a remediation, open the **Remediation** tab.

a Click **Add**.

b Select a remediation, and click **OK**.

a The remediation is enabled by default. If at a later time you want to disable the remediation for a period of time, clear the check box.

b Enter the target computer, if required. Only built-in remediation actions request a target computer.

c If arguments are required, browse to select and insert arguments. The user who created the custom remediation may have added a description as to which arguments are to be used.

d Click **OK**.

e The remediations run in the order they appear in the list. You can move a selected remediation up or down the list.

IMPORTANT: Any reboot remediation must be last on the list.

9 You can apply the changes to the selected domain controller, domain, forest or site; or to all domain controllers, domains, forests, or sites.

To apply the changes only to the selected object, click **Apply**.

-OR-

To apply the changes to all objects, click **Apply to All.**

10 Click **Yes** to confirm.

A lightning bolt indicates that a remediation is attached to the alert.

11 Optionally, click **Save as Template** to save all of the alert settings and data collector settings for this domain controller, domain, forest, or site as a template that can be applied to other Active Directory objects. For more information, see Active Directory Health Templates on page 130.

Purging and archiving alert history

You can choose to purge and/or archive the alerts added to the Active Administrator® database by Active Directory Health. If you choose to purge, records are removed from the database. If you choose to archive, the alerts are also added to the Active Administrator archive database.

To purge and archive Active Directory Health Analyzer alert history

1 Select **Active Directory Health | Agents**.

2 Open the **Monitored Domain Controllers tab**, if necessary.

3 Select any domain controller, and select **Settings | Purging and Archiving.**

4 Select to enable purging and archiving, then choose to either purge or archive.

5 Change the default number of days to keep data, if desired. The default is to keep 30 days of Active Directory Health Analyzer data.

6 You can set a schedule or choose to run the purge or archive now.

To set a schedule

a Click **Schedule**.

b Create the schedule.

c Click **OK**.

To purge or archive now

a Click **Run Now**.

b Choose to archive or purge data.

c Choose a date.

d Click **OK**.

7 Click **OK**.

Viewing alerts and alert history

The **Active Directory Health Analyzer Alerts** page is divided into two areas. The top pane displays current alerts and the bottom pane displays alert history.

NOTE: To manage Active Directory Health Analyzer alerts, the user must have the Active Directory Health and the Active Directory Health Alert Management roles. If you want a user to only view the alerts, the user needs the Active Directory Health and the Active Directory Health Alert Viewer roles. See Defining role-based access.

TIP: If you know of a maintenance event or some other known event that may generate unnecessary alerts, you can mute alerts.

To view alerts and alert history

1 Select **Active Directory Health | Alerts**.

The **Current Alerts** area displays the current alerts for the monitored domain controllers and domains with the total number of alters indicated next to the **Alerts Count** in the header. By default, the list of active alerts automatically refreshes every 30 seconds. A lightning bolt indicates a remediation is attached to the alert.

- To disable automatic refresh, clear the **Auto refresh active alerts** check box.

The **Alert History** area displays the 50 newest current and cleared alerts, filtered by date range for the previous day.

- By default, the Alert History displays alerts from the **Live** Active Administrator database. To view alerts from the Active Administrator® archive database, choose the source of the Alert History.
- To load another 50 alerts, click **Load 50 More**.
- To hide the **Alert History** pane, click . To show the **Alert History** area, click .

2 Double-click an alert to view details about the alert.

Table 50. Alert details menu options

Option	Description
Alert Settings	Edit alert settings. See Setting alerts.
Notifications	View the recipients of the listed notifications.
Copy	Copy a selected alert to the clipboard.

3 Use the menu to manage the list of alerts.

Table 51. Alerts menu options

Option	Description
Refresh	Refresh the list of active alerts.
Copy Active Alert	Copy a selected alert to the clipboard.
Copy Alert History	Copy a selected alert history item to the clipboard.
Filter History	Filter the list of alert history. See Filtering alert history.
Alert History Report	Generate an alert history report. See Generating an alert history report.
Notifications	Add, edit, or remove notifications. See Managing alert notifications.
Limiter	Limit the number of notifications. See Limiting alert notifications.
Grouping	Add or remove grouping the alerts by severity, alert name, or object name.

4 Use the shortcut links to manage the list of current alerts.

Table 52. Alerts shortcut links options

Option	Description
Details	View the details of the selected alert.
Copy	Copy the selected alert to the clipboard.
Create Notification	Create a notification in which the selected alert should be included. See Creating alert notifications.
Add To Notification	Set the notifications in which the selected alert should be included.

- OR -

Use the shortcut links to manage the list of historical alerts.

Table 53. Alerts shortcut links options

Option	Description
Details	View the details of the selected alert.
Copy	Copy the selected alert to the clipboard.

Filtering alert history

You can display all alerts or filter the list to display only those alerts for a specific date, date range, domain, or domain controller. You also can filter the list for specific alerts and by severity.

To filter alert history

1 Select **Active Directory Health | Alerts**.

2 Select the source of the alert history.

3 Click **Filter History**.

4 By default, all dates are included. You can select a specific date or date range.

5 To filter the list of alerts, select **Filter by alerts**. Use **Select All** and **Clear All** to help you select the alerts to display in the Alert History area.

6 To filter the list by severity, select **Filter by severity**, and choose the levels of alerts to display in the Alert History pane.

7 To filter by a domain or domain controller, type the Fully Qualified Domain Name (FQDN) in the **Object name** box.

8 Click **OK**. A banner displays the filters that are in effect for the Alert History area.

Generating an alert history report

You can generate a report of the alert history and display it in a report editor, send the report in an email, or save the report to a file.

To generate an alert history report

1 Select **Active Directory Health | Alerts**.

2 Select the source of the alert history.

3 Click **Alert History Report**.

4 By default, all dates are included. You can select a specific date or date range.

5 To filter the list of alerts, select **Filter by alerts**. Use **Select All** and **Clear All** to help you select the alerts to display in the Alert History area.

6 To filter the list by severity, select **Filter by severity**, and choose the levels of alerts to display in the Alert History pane.

7 Select how to deliver the report. You can display the report in a report editor, where you can make additional formatting changes, or you can send the report in an email and save it to a folder.

To display the report in a report editor

a Select **Interactive**.

b Click **OK**.

To send the report in an email

a Select **Delivery report**, if necessary.

b Change the default report name if desired.

c By default, the date and time are appended to the end of the file name. Clear the check box if you do not want the date and time appended to the file name.

d By default, a PDF file is created. You can choose a different format.

e Open the **Email tab**, if necessary.

f By default, the logged in account displays in the list. To add more recipients, click **Add**, type the email addresses, and click **OK**.

g Modify the default subject line if desired.

h Set the priority of the email.

NOTE: If you also want to save the report to a folder, do so before you click **OK**.

i Click **OK**.

To save the report to a file

a Select **Delivery report**, if necessary.

b Change the default report name if desired.

c By default, the date and time are appended to the end of the file name. Clear the check box if you do not want the date and time appended to the file name.

d By default, a PDF file is created. You can choose a different format.

e Open the **Save to Folder** tab.

f Click **Add**.

g Add a path to the location where you want to store the report file, and click **OK**.

h Click **OK**.

Muting alerts

If you know about an upcoming maintenance to the system or some other event that may cause a lot of unnecessary alerts, you can mute the collection of alerts or set a schedule to mute the alerts. During the mute period, no alerts are collected into the Active Administrator® database and no alert notifications are sent. If you forget to remove the mute, the mute is cleared automatically after one hour.

You can mute all alerts or just alerts for a specific forest, domain, domain controller, or site. The Mute button displays on each window in the Active Directory Health Analyzer. If you are viewing health for a specific object, the Mute button will mute the alerts for that object. For example, if you are viewing a specific site and you click **Mute**, only the alerts for that site are muted.

Table 54. Muting alerts

Mute type	Forest alerts	Domain alerts	DC alerts	Site alerts
All	Muted	Muted	Muted	Muted
Forest	Muted	Alerts sent	Alerts sent	Alerts sent
Forest + domain controllers + sites **NOTE:** Applies to only one forest.	Muted	Muted	Muted	Muted
Domain	Alerts sent	Muted	Alerts sent	Alerts sent
Domain + domain controllers	Alerts sent	Muted	Muted	Alerts sent
Domain controller	Alerts sent	Alerts sent	Muted	Alerts sent
Site	Alerts sent	Alerts sent	Alerts sent	Muted

To mute alerts

1 Select **Active Directory Health | Alerts**.

2 Select an object in the tree. The Mute button is not active for Domains, Sites, and Monitored Domain Controllers. See Table 54 to see what alerts are muted for each object.

3 Click **Mute**.

- To mute the entire system, including all forests, domains, sites, and domain controllers, click **Mute All**.
- To mute the selected object only, click **Mute**.
  - When muting a forest, you can also choose to include the sites, domains, and domain controllers.
  - When muting a domain, you can also choose to include domain controllers.

4 Click **Yes** to confirm the mute.

A heading displays on every analyzer page to indicate what object is muted, the time it was muted, and by whom it was muted. If more than one object is muted, only the number of muted objects displays. The mute automatically clears after one hour.

- To clear all mutes, click **Clear All**.
- To open the Mute dialog, click **Details**. You can mute the object again if the mute is about to expire or clear a selected mute or all mutes. See Clearing mutes.

To schedule muting alerts

1. Select **Active Directory Health | Analyzer**.
2. Select an object in the tree.
3. Click **Schedule Mute**.
4. If scheduling a mute for a forest object, optionally select **Include sites, domains and domain controllers** to also mute their alerts.

   - OR -

   If scheduling a mute for a domain object, optionally select **Include all domain controllers** to also mute their alerts.
5. Optionally, enter the **Reason** the alerts are being muted.
6. Set the **Start** and **End** dates and times for the alerts to be muted.
7. Optionally, select **Override manual mutes** to override existing mutes during the scheduled mute.
8. Optionally, select **Do not save observed values** to suppress saving details of the alerts that occur during the scheduled mute in the database.
9. Click **Schedule** to create the scheduled mute.

To view and modify a scheduled mute

1. Select **Active Directory Health | Analyzer**.
2. Click **Mute Schedule**.
3. Optionally, select a schedule and click **Edit** to change the schedule details.
4. Optionally, select a schedule and click **Remove** to delete the schedule.

Clearing mutes

A heading displays on every analyzer page to indicate what object is muted, the time it was muted, and by whom it was muted. If more than one object is muted, only the number of muted objects displays. A mute automatically clears after one hour. You can quickly clear all mutes from the heading. You also can clear just a selected mute.

To clear all mutes

- Click **Clear All** in the heading, and click **Yes** to confirm.
- Click **Details** in the heading, click **Clear All**, and click **Yes** to confirm.

To clear a selected mute

1. Click **Details** in the heading.
2. Select a mute from the list.
3. Click **Clear Mute**.
4. Click **Yes** to confirm.

Viewing mute history

A history of mutes is kept so you can see the object that was muted, who set the mute and at what time, and who cleared the mute and at what time.

To view mute history

- Click **Mute History** on any analyzer page.
    - To sort the columns, click in the heading.

Managing alert notifications

Active Directory Health Analyzer generates alerts when problems with Active Directory are detected. You can create notifications to send to specified email recipients. The wizard helps you create multiple types of notifications to address varied audiences and their specific needs. For more information on the types of alerts you can include in the notifications, see the Alerts Appendix.

For example, you might send only site alerts on a selected site to a certain user. You would exclude all forests, all domains, and all domain controllers from the notification. On the **Site Selection** page, you would choose the selected site.

Assign names and add descriptions to your alert notifications so you can easily manage the list. You can edit and remove alert notifications as your needs change.

Once you create alert notifications, you can see who alerts were sent to and when by displaying the details of an alert. See Viewing alerts and alert history.

IMPORTANT: To view, add, and edit alert notifications, the user must have:

- the Active Directory Health Notification Management permission (See Defining role-based access.);
- the Active Directory Health Alert Management permission (See Defining role-based access.); and
- membership in the Administrators group on the computer where Active Administrator Foundation Service (AFS) is installed.

Topics

- Creating alert notifications
- Editing alert notifications
- Removing alert notifications

Creating alert notifications

NOTE: To create an alert notification successfully, you must:

- Add at least one email address.
- Select at least one Active Directory object (forest, domain, domain controller, or site).
- Select alerts to match the selected Active Directory object.

  For example, if you select only domain alerts, and select only domain controllers, you receive a warning.

To create an alert notification

1. Select **Active Directory Health | Agents**.
2. Open the **Monitored Domain Controllers tab**, if necessary.
3. Click **Notifications**.

> **NOTE:** You also can manage notifications from **Alerts | Notifications**. See Viewing alerts and alert history.

4 Click **Add**.

5 Click **Next**.

6 Type a name and description for the alert notification.

By default, notifications for all alerts are enabled and notifications for all cleared alerts are enabled.

7 If notifications for an alert are enabled, optionally set whether to send or suppress notifications when an alert has cleared.

8 If notifications for cleared alerts is enabled, optionally, set whether to send or suppress cleared notifications if the alert clears within 15 minutes. You can adjust the time limit.

9 Click **Next**.

10 By default, all alerts are included in the notification. To send notifications for selected alerts, clear the check box, and select the alerts to include.

11 Click **Next**.

12 Review the alerts included in the notification. Click **Next** to complete the notification configuration or **Back** to make changes.

For more information on the alerts, see the Alerts Appendix.

13 Click **Next**.

14 By default all forests are included in the notification. You can choose to exclude all forests or include only selected forests.

To filter the list, start typing in the **Filter by forest name** box. The list filters as you type. You also can click the header to sort the list in ascending or descending order.

> **NOTE:** If you select a forest, only forest alerts are included in the notification. The domains, domain controllers, and sites associated with the forest are not automatically included in the notification. You must select domains, domain controllers, and sites separately.
>
> If you select a forest, you must select at least one forest alert. If you receive a warning, go back and select a forest alert.

15 Click **Next**.

16 By default all domains are included in the notification. You can choose to exclude all domains or include only selected domains.

To filter the list, start typing in the **Filter by domain name** box. The list filters as you type. You also can click the header to sort the list in ascending or descending order.

> **NOTE:** If you select a domain, only domain alerts are included in the notification. The domain controllers and sites associated with the domain are not automatically included in the notification. You must select domain controllers and sites separately.
>
> If you select a domain, you must select at least one domain alert. If you receive a warning, go back and select a domain alert.

17 Click **Next**.

18 By default all domain controllers are included in the notification. You can choose to exclude all domain controllers or include only selected domain controllers.

To filter the list, start typing in the **Filter by domain controller name** box. The list filters as you type. You also can click the header to sort the list in ascending or descending order.

> **NOTE:** If you select a domain controller, you must select at least one domain controller alert. If you receive a warning, go back and select a domain controller alert.

19 Click **Next**.

20 By default all sites are included in the notification. You can choose to exclude all sites or include only selected sites.

   To filter the list, start typing in the **Filter by site name** box. The list filters as you type. You also can click the header to sort the list in ascending or descending order.

   > **NOTE:** If you select a site, only site alerts are included in the notification. The domain controllers associated with the site are not automatically included in the notification. You must select domain controllers separately.
   >
   > If you select a site, you must select at least one site alert. If you receive a warning, go back and select a site alert.

21 Click **Next**.

22 Add, edit, or remove email addresses of the recipients of the notification.

   > **NOTE:** To manage email address list, you can edit the notification (see Editing alert notifications) or select the notification under All DA Notifications in Active Administrator Email Configuration (see Managing email addresses).

23 Click **Next**.

24 Review the selections, and click **Finish**.

25 Click **Finish**.

   The alert notification is enabled automatically. If you want to disable the notification, see Editing alert notifications.

Editing alert notifications

You can edit the alert notification as your needs change. You also can disable the notification for a period of time, and then enable it again when you need it.

To edit an alert notification

1 Select **Active Directory Health | Agents**.

2 Open the **Monitored Domain Controllers tab**, if necessary.

3 Click **Notifications**.

4 Select a notification, and click **Edit**.

5 Select the area you want to edit from the menu.

6 Make the necessary changes.

7 Click **OK**.

Removing alert notifications

To remove an alert notification

1 Select **Active Directory Health | Agents**.

2 Open the **Monitored Domain Controllers tab**, if necessary.

3 Click **Notifications**.

4 Select a notification, and click **Remove**.

5 Click **Yes**.

Pushing alerts to System Center Operations Manager and SNMP managers

If you have a license for the Active Directory Health module, you can forward the Active Directory Health alerts generated by Active Directory Health Analyzer agents to Microsoft® System Center Operations Manager (SCOM) and SNMP managers. These alerts will appear in the **Quest Alert Events** view, under the **Quest Active Administrator** folder in the Operations Manager Monitoring pane and in the SNMP Manager.

NOTE: Only System Center 2016 Operations Manager is supported. See Configuring SCOM and SNMP Settings.

NOTE: Only SNMP management software capable of TRAP v2 notifications processing is supported. See Configuring SCOM and SNMP Settings.

Topics

- Limiting alert notifications

To configure the System Center Operations Manager Alert Notification and SNMP Alert Notification

1. Select **Active Directory Health | Agents**.
2. Open the **Monitored Domain Controllers tab**.
3. Click **Notifications**.
4. Select **System Center Operations Manager Alert Notification**.

   - OR -

   Select **SNMP Alert Notification**.
5. Click **Edit**.
6. For SCOM and SNMP alerts, alert notification is enabled by default. To disable the alert notification, clear the check box.
7. To choose which Active Directory Health alerts to push, click **Alert Selection**.

   By default, all Active Directory Health alerts are included in the notification. If you want to send notifications for selected alerts, clear the check box, and select the alerts to include. For more information on the alerts, see the Alerts Appendix.
8. By default, alerts detected by the Active Directory Health Analyzer agents are sent to the SCOM server or the SNMP manager, unless you specify otherwise in the **Forest Selection**, **Domain Selection**, **Domain Controller Selection**, and **Site Selection** tabs. See Creating alert notifications.

   NOTE: The SCOM server and the SNMP manager are identified during the configuration wizard.
9. Click **OK**.

Limiting alert notifications

To prevent being overwhelmed with notifications, you set up the notification limiter to govern the number of notifications sent within a specified time period. For example, you set the notification limit to 100 notifications within 20 minutes with a 10 minute reset time, which is the default. Once 100 notifications are sent within the 20 minute time period, notifications are suspended for 10 minutes, which is the reset time.

The **Notification Limiter** dialog indicates if notifications are being sent or suspended and the countdown for the reset. Once the **Current Count** reaches the limit, the **Reset Duration** starts to increment. The **Missed Notification** indicates the number of notifications that were not sent. Click **Refresh** to renew the display information.Once the **Reset Duration** reaches the limit, all counts return to zero. You can manually reset the counter when notifications are suspended by clicking **Reset**.

NOTE: The notification limit applies collectively to all email notifications sent from Active Directory Health Analyzer. Any email notification from Active Administrator Health, including Active Directory Health Analyzer agent notifications, increases the notification count in the notification limiter count by one.

To limit notifications

1. Select **Active Directory Health | Agents**.
2. Open the **Monitored Domain Controllers tab**, if necessary.
3. Click **Limiter**.
4. By default, the notification limiter feature is enabled. If you want unlimited notifications sent, clear the **Enabled** check box.
5. By default, an email is sent to the administrator when the limit is reached. To suppress the email, clear the check box.
6. Set the number of notifications to send within a specified time period. Once the limit is met, notifications are suspended until the reset time period is met.
7. Set the reset time period, which is the period of time to wait after the limit is met before automatically resetting the count.
   - To renew the counter display, click **Refresh**.
   - To reset the counters manually, click **Reset**.
     NOTE: Notifications must be in the Suspended state to reset the counters manually.
8. Click **OK**.

Managing monitored domain controllers

The first time you open the **Agents** option, the **Monitored Domain Controllers** page display is empty. The first task is to install a Active Directory Health Analyzer agent. See Installing Active Directory Health Analyzer agents. Once an agent is installed the **Monitored Domain Controllers** page lists the domain controllers monitored by Active Directory Health Analyzer agents. The name of the server monitoring each domain controller is listed in the **Monitored by** column.

NOTE: To help you assess the health of the monitored domain controllers, use the **Summary** tab in the **Active Directory Health | Analyzer**. See Analyzing Active Directory health.

Topics

- Adding monitored domain controllers

To manage monitored domain controllers

1. Select **Active Directory Health | Agents**.
2. Select the **Monitored Domain Controllers** tab.
3. Use the toolbar to manage domain controllers.

Table 55. Monitored domain controllers tool bar

Option	Description
Refresh	Refresh the list of monitored domain controllers.
Add	Install the Active Directory Health Analyzer agent. See Installing Active Directory Health Analyzer agents. If you want to add more monitored domain controllers, see Adding monitored domain controllers.
Properties	View details about the selected domain controller, including which server in the agent pool is monitoring the selected domain controller.
Remediations	Add, edit, or delete remediation actions.
Settings	Enable, disable, and edit data collectors and alerts for a one or all monitored domain controllers, domains, forests or sites. See Managing data collectors, Setting data collectors, Setting an authoritative RODC, and see Setting alerts. Manage Active Directory Health templates. See Active Directory Health Templates. Enable or disable purging and archiving of the alerts collected by the Active Directory Health Analyzer. See Purging and archiving alert history. Enable or disable purging and archiving of data collected by the Active Directory Health Analyzer. See Purging and archiving Active Directory Health Analyzer data.
Notifications	Add, edit, or remove Active Directory Health Analyzer notifications.
Limiter	Enable, disable, and edit time thresholds for notifications.
Remove	Remove the Active Directory Health Analyzer agent from selected domain controllers or remove the domain controller from being monitored by the agent pool.
Tasks	Manage the tasks that pertain to the monitored domain controllers. See Managing tasks.

Adding monitored domain controllers

If you want to add more domain controllers, you can use the Add Agent wizard where you can add a standalone agent to monitor a single domain controller. See Installing Active Directory Health Analyzer agents.

If you have a pool of agents, you can easily add more unmonitored domain controllers to be monitored by the agent pool.

NOTE: To see the list of unmonitored domain controllers, you must select the **Display unmonitored domain controllers in the tree view** check box in user options. See Setting Active Directory Health Analyzer options.

To add more monitored domain controllers

1. Select **Active Directory Health | Analyze**.
2. Expand **Domains** in the tree.
3. Expand the domain the holds the domain controllers you want to add.
4. Expand **Unmonitored**.
5. Select the domain controller to add.
6. Click **Add Domain Controller**.
7. Click **Yes**.
8. Click **Refresh**.

Managing data collectors

The Active Directory Health Analyzer module monitors domain controllers and presents data for you to troubleshoot issues. The data collectors are used to display information on the **Details** tabs and to trigger alerts.

Topics

- Setting permissions for data collectors
- Setting data collectors
- Adding performance counter data collectors
- Adding Windows Services data collectors
- Adding Event Log data collectors
- Setting an authoritative RODC
- Purging and archiving Active Directory Health Analyzer data

Setting permissions for data collectors

For the Active Directory Health Analyzer to acquire the necessary data, certain permissions and access are required. To capture all data collectors accessible by the Active Directory Health Analyzer:

- The startup account for the Active Directory Health Analyzer agent must:
  - have domain user and domain administrative privileges;
  - be a member of the Distributed COM Users group; and
  - be a member of the Performance Logs user group.
  - The target server must have WMI remote access enabled.

To see the specific requirements for each individual data collector, see the Alerts Appendix.

Setting data collectors

By default, all data collectors are enabled. You can customize the scope of data collection to suit your environment. You can:

- Enable/disable individual data collectors
- Enable/disable debugging for troubleshooting purposes
- Enable/disable trending for those data collectors that support trending
- Adjust the duration and/or sample rates

You can save the data collector settings for a domain controller, domain, forest, or site as a template that can be applied to other domain controllers, domains, forests, or sites.

To set data collectors

1. Select **Active Directory Health | Agents**.
2. Select the **Monitored Domain Controllers tab**.
3. Select a domain controller.
4. Select **Settings | Domain Controllers, Domain, Forest, or Site**.
5. Select **Data Collectors**.
6. Select the data collector category to modify.

7 If there is more than one data collector listed, double-click the data collector.

You can filter the list by typing in the **Filter data collector** box. The list filters as you type.

8 Modify the settings.

- Only enable debugging if you need to troubleshoot the data collector.
- If the data collector does not support trending, the option is disabled.
- To reset the alert to the original default settings, click **Reset.**

> **IMPORTANT:** For the RODC allowed password data collectors, you must set at least one authoritative Read-only domain controller (RODC). See Setting an authoritative RODC.
>
> For the Domain FSMO role placement data collector, you must select at least one FSMO role validation option to enable the data collector.

9 To apply the changes only to the selected domain controller, click **Apply**.

-OR-

To apply the changes to all managed domain controllers, click **Apply to All**.

10 Click **Yes** to confirm.

> **NOTE:** If you changed the interval, duration, or sample rate to a value outside the recommended settings, you see a warning message. Click **Yes** to continue.

11 Optionally, click **Save as Template** to save all of the data collector settings and alert settings for this domain controller, domain, forest, or site as a template that can be applied to other Active Directory objects. For more information, see Active Directory Health Templates on page 130.

Adding performance counter data collectors

Performance counter data collectors collect data using the Windows Performance Counters. You can add customized performance counter data collectors.

To add a performance counter data collector

1 Select the **Active Directory Health | Agents**.

2 Select the **Monitored Domain Controllers** tab.

3 Select one of the monitored domain controllers that needs a new performance counter data collector.

4 Select **Settings | Domain Controllers**.

5 Select the **Performance Counters** tab.

6 Click **Add**.

7 Click the ellipses (...) next to the category name to search for a performance counter.

8 Select the Category Name of the performance counter.

9 Select the Counter Name.

10 Optionally, select the Instance Name.

11 Click **OK** to populate the performance counter configuration information. For more information, see To configure a performance counter data collector.

To configure a performance counter data collector

1 Follow the steps To add a performance counter data collector.

2 Optionally, enter a **Display Name**.

3 Optionally, enable **Add this new performance counter to all domain controllers**.

NOTE: This is the only opportunity to add this performance counter to all domain controllers.

4 Optionally, set the operating systems that support this performance counter.

5 Select a **Data Type** to be monitored by this performance counter.

6 Select an **Operator** to be used to compare the data type to the threshold values to determine if an alert condition is true.

7 Configure the Threshold settings to be used to determine if an alert condition is true.

Table 56. Performance Counter Data Collector Threshold Settings

Setting	Description
Warning Threshold	The value for which a warning alert is monitored. For example, if file size is being monitored, the data type may be set to GB and this value could be set to 100 GB.
• Before Alert	The length of time in seconds that the value must be above the Warning Threshold before an alert is triggered.
• After Alert	The length of time in seconds that the value must be below the Warning Threshold before an alert is cleared.
Error Threshold	The value for which an error alert is monitored. For example, if file size is being monitored, the data type may be set to GB and this value could be set to 100 GB.
• Before Alert	The length of time in seconds that the value must be above the Error Threshold before an alert is triggered.
• After Alert	The length of time in seconds that the value must be below the Error Threshold before an alert is cleared.

8 Click **OK** to save the settings, update the listing of Performance Counter Data Collectors, and trigger the collection of data for this performance counter.

Adding Windows Services data collectors

Windows services data collectors monitor the status of Active Directory Windows services. You can add customized Windows services data collectors.

To add a Windows service data collector

1 Select the **Active Directory Health | Agents**.

2 Select the **Monitored Domain Controllers** tab.

3 Select one of the monitored domain controllers that needs a new Windows service data collector.

4 Select **Settings | Domain Controllers**.

5 Select the **Windows Services** tab.

6 Click **Add**.

7 Enter a **Service name**.

8 Enter a **Display name**.

9 Optionally, enable **Add this new Windows service data collector to all monitored domain controllers**.

10 Optionally, set the operating systems that support this Windows Services data collector counter.

11 Click **OK** to save the settings, update the listing of Windows Services Data Collectors, and trigger the collection of data for this Windows Service.

Adding Event Log data collectors

Event Log data collectors monitor the status of Windows events. You can add customized Event Log data collectors. A corresponding alert is created.

To add an Event Log data collector

1. Select the **Active Directory Health | Agents**.
2. Select the **Monitored Domain Controllers** tab.
3. Select one of the monitored domain controllers that needs a new Event Log data collector.
4. Select **Settings | Domain Controllers**.
5. Select the **Event Log** tab.
6. Click **Add**.
7. Enter a **Log Name** (such as System).
8. Optionally, enter a **Source** (such as NETLOGON) to filter the results.
9. Enter the numeric **Event Id** to collect.
10. Optionally, enable **Add this new Event Log data collector to all monitored domain controllers**.
11. Optionally, set the operating systems that support this Event Log data collector.
12. Click **OK** to save the settings, update the listing of Event Log Data Collectors, and trigger the collection of data for this Event Id.

To view the alert created by the Event Log data collector

1. Select the **Active Directory Health | Agents**.
2. Select the **Monitored Domain Controllers** tab.
3. Select one of the monitored domain controllers that needs a new Event Log data collector.
4. Select **Settings | Domain Controllers**.
5. Click **Alerts**.
6. Type **LogName** to display only Error Log alerts.

   - OR -

   Type a specific Event Id to display only alerts for that Event Id.

   - OR -

   Scroll through the alphabetic list of alerts to display those starting with LogName.

Setting an authoritative RODC

To enable the RODC allowed/denied password replication policy inconsistent data collector, you must set at least one authoritative Read-only Domain Controller (RODC) in the domain.

To set an authoritative RODC

1. Select **Active Directory Health | Agents**.
2. Open the **Monitored Domain Controllers tab**, if necessary.
3. Select any domain controller, and select **Settings | Set Authoritative RODC**.
4. Browse to locate an RODC.
5. Click **OK**.

Purging and archiving Active Directory Health Analyzer data

You can choose to purge and/or archive the data points added to the Active Administrator database by Active Directory Health. If you choose to purge, records are removed from the database. If you choose to archive, data points are also added to the Active Administrator archive database.

To purge and archive Active Directory Health Analyzer data

1. Select **Active Directory Health | Agents**.
2. Open the **Monitored Domain Controllers tab**, if necessary.
3. Select any domain controller, and select **Settings | Data Purging and Archiving.**
4. Select to enable purging and archiving, then choose to either purge or archive.
5. Change the default number of days to keep data, if desired. The default is to keep 30 days of Active Directory Health Analyzer data.
6. You can set a schedule or choose to run the purge or archive now.

   To set a schedule

   a. Click **Schedule**.

   b. Create the schedule.

   c. Click **OK**.

   To purge or archive now

   a. Click **Run Now**.

   b. Choose to archive or purge data.

   c. Choose a date.

   d. Click **OK**.
7. Click **OK**.

Active Directory Health Templates

The settings for the data collectors and alerts within a domain controller, a domain, a forest, or a site can be saved as a template. These templates can later be applied to other domain controllers, domains, forests, or sites to keep settings consistent between objects and to save configuration time.

Topics

- Creating and Applying Active Directory Health Templates
- Managing Active Directory Health Templates

Creating and Applying Active Directory Health Templates

The settings for the data collectors and alerts within a domain controller, a domain, a forest, or a site can be saved as a template. These templates can later be applied to other domain controllers, domains, forests, or sites. Templates can be applied with the data collector settings locked or unlocked.

When a template is applied to an object as locked, the data collector and alert settings for an object may only be modified by removing the applied template or by updating the template. When a template is applied to an object as unlocked, the data collector and alert settings are applied to the object but the object can be modified and may subsequently be saved as a new template. When a template is updated, only objects with the template applied as locked will be updated with the changes to that template.

To create an Active Directory Health template

1. Select **Active Directory Health | Agents**.
2. Select the **Monitored Domain Controllers tab**.
3. Select a domain controller.
4. Select **Settings | Domain Controllers, Domain, Forest, or Site**.
5. Modify the all data collectors and alerts until they contain the settings you want to save as a template that can later be applied to other domain controllers, domains, forests, or sites. For more information, see To apply an Active Directory Health template on page 131.
6. To apply the changes only to the selected domain controller, click **Apply**.

   -OR-

   To apply the changes to all managed domain controllers, click **Apply to All**.
7. Click **Yes** to confirm.

   NOTE: If you changed the interval, duration, or sample rate to a value outside the recommended settings, a warning message will be displayed. Click **Yes** to continue.
8. Click **Save as Template**.

   NOTE: When you save this template, all existing data collector settings and all existing alert settings will be stored in the template. To view or modify any of the template properties, you can edit the template. For more information see, To edit Active Directory Health templates on page 133.
9. Enter a unique template name to create a new template.

   - OR -

   Enter the name of an existing template to overwrite it.
10. Optionally, enter a description.
11. Click **OK**.
12. If prompted, click **Yes** to overwrite the existing template.

To apply an Active Directory Health template

1. Select **Active Directory Health | Agents**.
2. Select the **Monitored Domain Controllers tab**.
3. Select one or more domain controllers.
4. Right-click to select **Apply Templates | Domain Controllers, Domain, Forest, or Site**.
5. Select the template to be applied.
6. Click **OK**.
7. Select **Apply as a locked template.**

   NOTE: When a template is applied as locked, the data collector or alert settings may only be modified by removing the applied template or by updating the template.

   - OR -

Select **Apply as an unlocked template** and select the sections of the template to be applied.

> **NOTE:** When a template is applied as unlocked, the data collector or alert settings can be modified and can be subsequently saved as a new template.

8 Click **Yes** to continue and apply the template.

To remove the application of an Active Directory Health template

> **NOTE:** Active Directory Health templates may also be removed by managing the template. For more information, see To edit Active Directory Health templates on page 133.

1 Select **Active Directory Health | Agents**.

2 Select the **Monitored Domain Controllers tab**.

3 Select a domain controller.

4 Select **Settings | Domain Controllers, Domain, Forest, or Site**.

5 Select **Data Collectors**.

- OR -

Select **Alerts**.

If a template is applied, an information note containing the name of the applied template is displayed at the top of the window. Optionally, click **View Details** to see a description of the applied template.

6 Optionally, click **Template Details** to see a who applied the template and what date it was applied.

7 Click **Remove Template**.

8 Click **Yes** to accept and continue.

> **NOTE:** The template is no longer applied. The settings are retained for each data collector or alert and may now be changed.

Managing Active Directory Health Templates

Active Directory Health templates can be viewed, modified, removed from an object, and deleted. Templates can also be imported or exported.

When viewing templates, the number of objects locked to that template are displayed to the right of the template name. When viewing the properties of a template, details such as the template ID, template name, description, object type, created dates, creator, updated dates, who updated the template, and the objects that are using the template are displayed. The collector settings and alert settings can also be viewed.

When a template is modified, all objects locked to that template will be updated to reflect the changes.

When a template is deleted, all objects locked to that template will be unlinked. The settings for the objects will remain unchanged.

Topics

- Managing agent workload
- Sending agent notifications
- Monitoring agent performance

To view Active Directory Health templates

1 Select **Active Directory Health | Agents**.

2 Select the **Monitored Domain Controllers tab**.

3 Select **Settings | Templates**.

4 Select a template.

5 Click **Properties** to display the template details.

6 Click **Settings**.

7 Optionally, click **Data Collectors** to view all of the data collector settings for this template.

8 Optionally, click **Alerts** to view all of the alert settings for this template.

9 Click **Close** to exit.

To edit Active Directory Health templates

1 Select **Active Directory Health | Agents**.

2 Select the **Monitored Domain Controllers tab**.

3 Select **Settings | Templates**.

4 Select a template.

5 Click **Properties** to display and edit the template details.

6 Click **Settings**.

7 Optionally, click **Data Collectors** and double-click any data collector to edit its settings. Click **Apply** to save the changes for all objects locked to this template.

8 Optionally, click **Alerts** and double-click any alert to edit its settings. Click **Apply** to save the changes for all objects locked to this template.

9 Optionally, select Active Directory objects that have the template applied and click **Remove Template** to remove the application of the template. Click **Yes** to accept and continue..

> **NOTE:** The template is no longer applied to the object. The data collector and alert settings are retained and may now be changed.

10 Click **Update** to save the modified template details.

11 Click **Close** to exit.

To delete Active Directory Health templates

1 Select **Active Directory Health | Agents**.

2 Select the **Monitored Domain Controllers tab**.

3 Select **Settings | Templates**.

4 Select the templates to be deleted.

5 Click **Delete**.

> **NOTE:** The templates are no longer applied to the data collectors. The settings are retained for each data collector and may now be changed.

6 Click **Close** to exit.

To export Active Directory Health templates to a file

1 Select **Active Directory Health | Agents**.

2 Select the **Monitored Domain Controllers tab**.

3 Select **Settings | Templates**.

4 Select the templates to be exported.

5 Click **Export**.

6 Navigate to the location to save the file.

7 Enter a meaningful file name.

8 Click **Save**.

To import Active Directory Health templates from a file

1 Select **Active Directory Health | Agents**.

2 Select the **Monitored Domain Controllers tab**.

3 Select **Settings | Templates**.

4 Click **Import**.

5 Navigate to the file containing exported templates and select it.

6 Click **Open**.

The templates contained in the file will be displayed.

7 Select the templates to import.

8 Click **OK**.

9 Click **Yes** to overwrite any existing templates that have the same name as a template being imported.

- OR -

Click **No** to skip importing any templates with the same name as an existing template.

10 Click **Close** to exit.

Managing Active Directory Health Analyzer agents

You can install agents directly to a domain controller in standalone mode. The standalone agent monitors only the domain controller on which it is installed. Installing agents into a pool maximizes the efficiency by balancing the workload among the pool of load-balancing agents.

NOTE: The DAAgentConfig.exe utility is available for managing the Active Directory Health Analyzer agent if you are experiencing problems. The DAAgentConfig.exe utility is located at C:\Program Files\Quest\Active Administrator\Server\SLAgent\DAAgent. The utility is launched outside of Active Administrator® to help you troubleshoot issues.

If a Active Directory Health Analyzer agent is experiencing problems, an alert is triggered and displays in the **Current Alert** list. See Viewing alerts and alert history. For Active Directory Health Analyzer agents in a pool, the domain controllers it monitors move to another agent, and the domain controller hosting the agent is removed from the pool and no longer monitored until it come back online.

To manage Active Directory Health Analyzer Agents

1 Select **Active Directory Health | Agents**.

2 Open the **Analyzer Agents** tab.

3 Use the tool bar to manage audit agents.

NOTE: When you select **Remove**, **Start**, **Stop**, **Restart**, **Set Agent Startup Account**, or **Set Port Number**, you are asked to select the account to use to manage the agent. You can use the Active Administrator Foundation Service (AFS) account, or indicate a specific user account.

Table 57. Audit agent tool bar

Option	Description
Refresh	Refresh the Active Directory Health Analyzer agent on all listed domain controllers.
Refresh Selected	Refresh the Active Directory Health Analyzer agent on selected domain controllers.

Table 57. Audit agent tool bar

Option	Description
Install	Install the Active Directory Health Analyzer agent. See Installing Active Directory Health Analyzer agents.
Properties	Display properties for the selected Active Directory Health Analyzer agent. You also can view properties when monitoring agent performance. See Monitoring agent performance.
Limiter	Enable, disable, and edit time thresholds for notifications.
Remove	Uninstall the selected Active Directory Health Analyzer agent. **NOTE:** If for some reason, the Active Directory Health Analyzer agent cannot be removed, use the **Remove Orphaned Agent** option. **NOTE:** You must select the account to use to remove the agent.
Start	Start collecting events on the selected domain controller(s). **NOTE:** You must select the account to use to start the agent.
Stop	Stop collecting events on the selected domain controller. **NOTE:** You must select the account to use to stop the agent.
Restart	Restart selected Active Directory Health Analyzer agents. **NOTE:** Agents can be restarted only if they are started. If an agent is stopped, click **Start**. **NOTE:** You must select the account to use to restart the agent.
Workload Details	Manage workload distribution by the agent pool. See Managing agent workload. Manage email notifications for the status of load-balancing agents. See Sending agent notifications.
More | Agent Notifications	Manage email notifications for the status of standalone and load-balancing agents. See Sending agent notifications.
More | Automatic Agent Deployment	Set up automatic deployment of the Active Directory Health Analyzer agent. Manage pending deployments. You can cancel or initiate the deployment immediately. See Setting up automatic Active Directory Health Analyzer agent deployment.
More | Agent Performance Settings	Set up performance monitoring of a selected Active Directory Health Analyzer agent. See Monitoring agent performance.
More | Agent Performance	View properties and statistics to help monitor memory and CPU usage on a selected Active Directory Health Analyzer agent. See Monitoring agent performance.
More | Set Agent Startup Account	Change the Active Directory Health Analyzer agent startup account. **NOTE:** For optimal monitoring of domain controllers, an account with domain administrative privileges is recommended. If you cannot use an account with domain administrative privileges, use an account that is a member of the Performance Log Users and Distributed COM Users groups in the monitored domain. You also must enable Remote Access for WMI on the remotely monitored domain controllers. Some monitoring features will not be available. **NOTE:** You must select the account to use to set the agent startup account.

Table 57. Audit agent tool bar

Option	Description
More | Set Agent Port Number	Specify the port that the Active Administrator Foundation Server uses to communicate with the Active Directory Health Analyzer agent on the domain controller. **NOTE:** TCP Port 15603 is the default value. If you change the agent port number from the default, make sure the port is open in Windows® Firewall on the computer hosting the Active Directory Health Analyzer agent. **NOTE:** You must elect the account to use to set the agent port number.
More | Remove Orphaned Agents	Removes the Active Directory Health Analyzer agents from the selected computers. **NOTE:** If the Remove option does not uninstall the agent, use this option.
More | View Agent Log	View the Active Directory Health Analyzer agent log. **NOTE:** The log entries exist in memory. You can use the **Filter Log Entries** option to search for specific log entries. You can right-click and copy a selection of log entries to the clipboard. If you require a log file for troubleshooting, use the Active Directory Health Analyzer agent configuration utility. See Using the Active Directory Health Analyzer agent configuration utility.
More | Test Agent Status	Test the Active Directory Health Analyzer agent connection.
More | Configure Firewall Rules	Configures Windows Firewall to allow the Active Directory Health Analyzer agent to communicate with the Active Administrator Data Service (ADS).
More | Upgrade	Upgrade the selected Active Directory Health Analyzer agent.
More| Upgrade All	Upgrade all listed Active Directory Health Analyzer agents.
More | Group by Status	Group the list of agents by status.
More | Remove Grouping	Remove the grouping.
More | Excluded Domain Controllers	Manage the list of domain controllers that are excluded from monitoring. See Excluding domain controllers.
Tasks	Manage the tasks that pertain to the Active Directory Health Analyzer Agent. See Managing tasks.

Managing agent workload

As domain controllers are added, removed, started, or stopped, the agent pool automatically redistributes the workload. A workload evaluation is run every 24 hours automatically, but you can trigger it manually as well. You may find you need to add more agents to the pool to help with the workload. See Installing Active Directory Health Analyzer agents into a pool.

To run a workload evaluation

1. Select **Active Directory Health | Agents**.
2. Open the **Analyzer Agents** tab.
3. Click **Workload Details**.

   The agents and the number of domain controllers monitored by the agent display along with their status and time stamp of the last evaluation.

   - If you want to send notifications when a load evaluation occurs, click **Agent Notifications**.
   - To view the domain controllers that an agent is monitoring, click **Agent Details**.

4 Click **Evaluate Agent Load**.

A message displays stating an evaluation will begin in one minute.

Sending agent notifications

By default, an email notification is sent when an agent goes into a critical state, a stopped state, and when the agent has recovered. You also can select to send an email notification when the agent goes into a warning state or when an agent workload evaluation is performed, which occurs if a load-balancing agent cannot recover.

To manage agent notification

1 Select **Active Directory Health | Agents**.

2 Open the **Analyzer Agents** tab.

3 Select **More | Agent Notifications**.

> **NOTE:** For load-balancing agents, you also can set agent notifications by selecting **Workload Details | Agent Notifications**.

4 By default, agent notifications are enabled. Clear the check box to disable notifications.

5 Select the status of the agent to trigger the email notification.

> **NOTE:** For stand-alone agents, if the **Load Evaluation** check box is selected, a notification is not sent because load balancing does not occur.

6 Click **Add** to add an email address to the list of recipients for the email notifications. You can edit a selected address or remove selected addresses from the list.

> **NOTE:** You also can manage the DA Agent Notification Settings email address list from the **Settings** menu. See Managing email addresses.

7 Click **OK**.

Monitoring agent performance

You can monitor the memory and CPU usage of Active Directory Health Analyzer agents. In addition, performance monitoring displays properties about the selected agent to help you maintain agent health.

Topics:

- Viewing agent performance
- Viewing agent performance

Setting up performance monitoring

To set up agent performance monitoring

1 Select **Active Directory Health | Agents**.

2 Open the **Analyzer Agents** tab.

3 Select **More | Agent Performance Settings**.

4 By default, monitoring is enabled. To disable monitoring, clear the check box.

5 Set the limit for average memory usage. The default setting is 800 MB. The lowest value is 200 MB.

6 Set the limit for average CPU usages. The default is 80 percent. The lowest value is 20%.

7 By default, the agent is restarted automatically if a performance issue is detected. To disable automatic restart, clear the check box.

8 By default, performance history is saved to a file in C:\ActiveAdministrator\DACache\AgentPerformance. To disable performance history, clear the check box. You also can change the number of days performance history is kept.

9 By default, a daily performance report is sent to the Active Administrator owner. The report contains the average values for CPU usage, memory usage, data points, errors, warnings, restarts, and work load; and indicates if an update is required. To disable the report, clear the check box. You can add more email addresses and set the start time for data collection.

> **NOTE:** To manage the DA Agent Daily Performance email address list, see Managing email addresses.

10 Click **OK**.

Viewing agent performance

To view agent performance

1 Select **Active Directory Health | Agents**.

2 Open the **Analyzer Agents** tab.

3 Select **More | Agent Performance**.

The newest 100 performance history records displays.

- To load another 100 records, click **More**.
- To refresh the display, click **Refresh**.
- To clear the log, click **Clear Log**.
- To view the log, click **Agent Log**.

The trending graph shows minute-by-minute usage. Drag the cursor across the graph to view details of occurrence.

Use the performance details to help you monitor the agent.

Table 58. Active Directory Health Analyzer agent performance details

Detail	Description
Date & Time	Date and time of the log entry.
Agent health	Overall state of the agent.
Computer name	Name of the computer where the agent is installed.
Agent memory usage	Average amount of memory the agent is using.
Average CPU usage	Average amount of CPU usages the agent is using.
Average working set	Size of the average memory working set.
Peak working set	Size of the peak memory working set.
Average data points sent	Average number of data points sent to the Active Administrator server.
Managed active alerts	Number of collectors that are above the alert threshold.
Active collectors	Number of collectors running on the selected agent.
Workload	Number of domain controllers being monitored by the selected agent.
Recovered data points	Number of data points recovered because the agent could not connect to the Active Administrator server.
Forest	Forest where the domain controllers that the agent is monitoring reside.
Status	Status of the agent. Indicates if the agent is Running or Stopped.

Table 58. Active Directory Health Analyzer agent performance details

Detail	Description
Monitoring mode	Indicates if the agent is monitoring a site only or is available for all domain controllers.
Agent type	Indicates if the agent monitors all domain controllers or a single domain controller.
Agent ID	ID of the selected agent.
Agent version	Version of the agent.
Update required	Indicates if the agent needs to be upgraded.
Failed load evaluation	Indicates if the agent failed during load evaluation, which means the domain controllers were not deployed to the agent.
Last heard from	Last time the agent was heard from.
Last error count	Last error count observed.
OS version	Version of the operating system that is running on the agent.
Connection pool size	Size of the server connection pool.
Active connections	Number of connections in use in the connection pool.
Disconnected connections	Number of connections that are disconnected in the connection pool.
Description	Current agent health state.
Domain controllers	List of domain controllers the agent is monitoring.

Using the Troubleshooter

Use the Troubleshooter to run jobs on managed forests and domains.

Topics

- Managing the DFSR service
- Running the Directory Service Replication Troubleshooter
- Enabling or disabling domain controller replication
- Setting directory service log levels
- Setting Netlogon parameters
- Setting startup and recovery options
- Cleaning up metadata
- Running online defrag
- Replicating Active Directory

Managing the DFSR service

You can start or stop the Distributed File System Replication (DFSR) service, start replication, poll Active Directory® for configuration updates, and enable/disable SYSVOL subscription.

To run the DFSR jobs

1. Select **Active Directory Health | Troubleshooter**.
2. Open the **Jobs** tab.

3 Expand the DFSR jobs folder.

4 Select a DFSR job.

Table 59.

DFSR job	Description
DFSR Poll AD	Forces Distributed File System (DFS) to poll Active Directory for configuration updates.
Start Replication	Starts replication from all replication partners for the specified domain controllers.
Start/Stop DFSR service	Start or stop the DFSR service on the specified domain controllers.
SYSVOL Subscription	Enable or disable SYSVOL Subscription on the specified domain controllers.

5 Double-click the target to add it to the lower pane.

- Select a forest to run the job on all domain controllers in the forest.
- Select a domain to run the job on all domain controllers in the domain.

6 Click **Next**.

7 Select the options for the test.

8 Click **Next**.

9 Click **Finish**.

Running the Directory Service Replication Troubleshooter

Run a replica consistency check against the selected domain controller and attempt to force a replication with any partners that failed. The replica consistency check mimics the functionality of `Repadmin /kcc`. The Knowledge Consistency Checker (KCC) generates its replication topology if required.

To run the Directory Service Replication Troubleshooter

1 Select **Active Directory Health | Troubleshooter**.

2 Open the **Jobs** tab.

3 Double-click **Directory Service Replication Troubleshooter.**

4 Double-click the target to add it to the lower pane.

- Select a forest to run the job on all domain controllers in the forest.
- Select a domain to run the job on all domain controllers in the domain.

5 Click **Next**.

6 By default, a replica consistency check is run against the domain controllers in the selected forest or domain and failed replications are retried. To disable one of the options, clear the check box.

7 Click **Next**.

8 Click **Finish**.

Enabling or disabling domain controller replication

Enables or disables inbound and outbound domain controller replication on all domain controllers in a selected forest or domain.

To enable or disable domain controller replication

1. Select **Active Directory Health | Troubleshooter**.
2. Open the **Jobs** tab.
3. Double-click **Enable or disable domain controller replication.**
4. Double-click the target to add it to the lower pane.
   - Select a forest to run the job on all domain controllers in the forest.
   - Select a domain to run the job on all domain controllers in the domain.
5. Click **Next**.
6. Select to enable or disable inbound and outbound replication.
7. Click **Next**.
8. Click **Finish**.

   The job results are listed in the **Result History** area. Select a job result to view details in the **Result Details** area.

Setting directory service log levels

Active Directory records events in the directory service log in Event Viewer. In Active Administrator, you can run the **Set directory service log levels** job to set the log level in Active Directory. By default, Active Directory only records critical and error events (log level 0). As you increase the setting, more events are recorded for the event type, with log level 5 recording all events. If you select **No Change**, the current setting in Active Directory remains.

To set directory service log levels

1. Select **Active Directory Health | Troubleshooter**.
2. Open the **Jobs** tab.
3. Double-click **Set directory service log levels**.
4. Double-click the target to add it to the lower pane.
   - Select a forest to run the job on all domain controllers in the forest.
   - Select a domain to run the job on all domain controllers in the domain.
5. Click **Next**.
6. Select the log level to change.

Table 60. Directory service log levels

Setting	Description
No Change	No change is made to the setting in Active Directory. If another application was used to set the logging level, that setting is unchanged.
0 (None)	Includes critical events and error events only (default setting in Active Directory).
1 (Minimal)	Includes very high-level events.
2 (Basic)	Includes events with a logging level of 2 or lower.

Table 60. Directory service log levels

Setting	Description
3 (Extensive)	Includes events with a logging level of 3 or lower.
4 (Verbose)	Includes events with a logging level of 4 or lower.
5 (Internal)	Includes all events.

7 Click **Next**.

8 Review the settings.

9 Click **Finish**.

Setting Netlogon parameters

View and/or modify the current settings for the parameters set for the following registry key:

HKEY_LOCAL_MACHINES\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters

To modify Netlogon parameters

1 Select **Active Directory Health | Troubleshooter**.

2 Open the **Jobs** tab.

3 Double-click

4 **Set Netlogon parameters**.

5 Double-click the target to add it to the lower pane.

- Select a forest to run the job on all domain controllers in the forest.
- Select a domain to run the job on all domain controllers in the domain.

6 Click **Next**.

7 Select a parameter, and click **Edit**.

8 Modify the current value, or click

9 **Default** to restore the value to the default setting.

10 Click **OK**.

The changed value displays.

- To clear the value and restore the previous setting for the selected parameter, click **Clear**.
- To set the value as the default for the selected parameter, click **Set Default**.

Setting startup and recovery options

A wizard guides you through modifying the boot configuration for the selected managed domain controller.

To set startup and recovery options

1 Select **Active Directory Health | Troubleshooter**.

2 Open the **Jobs** tab.

3 Double-click **Set startup and recovery options**.

4 On the Welcome page, click **Next**.

5 Select a domain controller, and click **Next**.

6 Select the default operating system and system failure options.

> **NOTE:** The settings for system failure apply to the registry of the current operating system for the selected domain controller. If you change the default operating system, the settings for system failure will not apply to the new operating system.

7 Click **Next**.

8 Select optional settings to configure the server startup for the operating system that you selected on the previous page. The switches are analogous to those used by the BCDEDIT command-line application.

> **NOTE:** If the operating system is not correct, click **Back** and select the correct operating system. The pages in this wizard are specific to the operating system you selected.

9 Click **Next**.

10 Choose to enable or disable debugging for the selected operating system.

11 If you enable debugging, choose the type of debugger connection.

12 Click **Next**.

13 Select options for memory, processors, and virtual address space for the selected operating system.

14 Click **Next**.

15 Review the current boot configuration to the new boot configuration.

16 Click **Finish**.

Cleaning up metadata

When a server is promoted to a domain controller, configuration data is added to Active Directory. When the domain controller is demoted successfully to a member server, the configuration data is removed. If the demotion is unsuccessful, the configuration data remains. Run this job to remove the configuration data.

To clean up metadata

1 Select **Active Directory Health | Troubleshooter**.

2 Open the **Jobs** tab.

3 Double-click **Start metadata cleanup**.

4 Click **Next** on the information page.

5 Type the name of the server to clean up.

6 Optionally, type the distinguished name of the server.

Depending on the state of the objects in the directory, the cleanup job may not be able to determine the correct path to the object it will clean up. Entering the distinguished name of the server will increase the success of the cleanup job.

7 Click **Next**.

8 Review the settings.

9 Click **Finish**.

Running online defrag

To optimize the Active Directory database, periodically run online defragmentation to redistribute data and free disk space for the database to use. The size of the database does not shrink. Optionally, you can run garbage collection prior to online defragmentation to remove tombstones, which are remains of objects that were deleted, and to delete unnecessary log files.

To start online defrag

1 Select **Active Directory Health | Troubleshooter**.

2 Open the **Jobs** tab.

3 Double-click **Start online defrag**.

4 Double-click the target to add it to the lower pane.

- Select a forest to run the job on all domain controllers in the forest.
- Select a domain to run the job on all domain controllers in the domain.

5 Click **Next**.

6 Select to run online defragmentation with or without garbage collection.

7 Click **Next**.

8 Review the settings.

9 Click **Finish**.

Replicating Active Directory

The Replication View provides valuable information about the two domain controllers selected for data replication. The information consists of the immediate replication partners for the target server and the recommended replication path between the two servers. From the Replication View, you can also initiate an end-to-end data replication for these domain controllers.

To replicate Active Directory

1 Select **Active Directory Health | Troubleshooter**.

2 Open the **Troubleshooting** tab.

3 Double-click

4 **Replication view**.

5 Type a name and an optional description for the replication.

The name you enter displays in the tree under Replication View so you can rerun the replication. If you have several replications created, the name helps you select the desired replication.

6 Click **Browse** to locate the source domain controller.

7 Click **Browse** to locate the target domain controller.

8 Click **OK**.

9 Expand **Replication view**, and select the replication.

The **Replication view** displays the source and target domain controllers, the shared naming contexts for the two servers, and the target's immediate replication partners.

10 Select the naming contexts.

For a path to exist between two servers, you must select at least one shared naming context. All of the shared naming context(s) are selected by default.

The **Recommended Replication Path** list displays the source and target servers for each naming context. Selecting/unselecting naming contexts show/hide pairs in the **Recommended replication path** list.

11 To replicate a pair, right-click the pair, and select **Replicate now**.

The status changes to **Replicated**.

12 To view details on the replications, click  .

This list shows the immediate replication partners for the target server grouped by naming context. Each server in the list will have an entry for the selected naming context, containing the following information for each partner:

- **Last attempt**: date and time when the last replication was attempted
- **Last result**: results of the last replication process
- **Last success**: date and time of the last successful replication
- **Consecutive failures**: number of consecutive failures encountered during the last replication session
- **Current USN**: current Update Sequence Number (USN)

13 To return to the replication pairs, click  .

14 To view objects and attributes that were not replicated, right-click the replication pair, and select

15 **Show unreplicated changes**.

The **Unreplicated changes** window displays the source and target servers, the selected naming context, unreplicated objects, and unreplicated attributes for the selected object.

- To filter the list of unreplicated objects, start typing in the **Filter objects** box. The display updates as you type.
- To view attribute values for a selected object, click **Show values**.

16 Click **OK** to return to the main display.

Recovering Active Directory Health data

In the event that you may need to recover the Active Directory Health module set up and data, we recommend that you follow these steps to collect the necessary information to restore the Active Directory Health module.

Topics

- Preparing for data recovery
- Restoring the Active Directory Health module and data

Preparing for data recovery

To prepare for the possibility of data recovery, record information about the Active Administrator installation and back up the necessary folders and files.

1 Document the following information:

- Active Administrator version and update number
- Name of the Active Administrator server
- Name of the database server where the Active Administrator live database is located
- Name of the database servers where the Active Administrator archive databases are located.
- Names of the Active Administrator live database, the active archive database, and all other archive databases
- Names of all servers that have an installed Active Administrator Active Directory Health Analyzer agent

- All permissions on the Active Administrator databases
- All permissions on the **ActiveAdministrator** folder share

2 Back up the following at least once a day:

- All Active Administrator databases
- Contents of the **ActiveAdministrator** folder share

Restoring the Active Directory Health module and data

These steps assume that you are recovering both the Active Administrator server and the Active Administrator databases. To make the recovery faster it is recommended, if possible, to use the same Active Administrator server name.

To restore the Active Directory Health module and data

1 Restore the Active Administrator folder share. Make sure the Active Administrator folder is shared as **ActiveAdministrator**. Restore any custom NTFS or share permissions.

2 Restore all of the Active Administrator databases and any permissions.

3 Install the Active Administrator server.

4 Apply the Active Administrator update (if applicable).

5 Using the Active Administrator Server Configuration Wizard, configure the Active Administrator server. On the database selection screen select the Active Administrator database server and the live database name from step 2. Repeat these steps for the archive database and select the active archive database.

6 Recover the Active Directory Health Analyzer agent.

- If you used the same Active Administrator server then there are no additional steps needed.
- If you used a different Active Administrator server, select one the following options.

  Option 1: Remove and install all Active Directory Health Analyzer agents using the Active Administrator Console. See Installing Active Directory Health Analyzer agents.

  Option 2: Use the Active Directory Health Agent Configuration utility, which you can find at **C:\Windows\DAAgent\DAAgentConfig.exe**. See Using the Active Directory Health Analyzer agent configuration utility.

  a Log on to each server and open the DA Agent Configuration utility.

  b Type the name of the new Active Administrator server in the **ADS Server Address** box.

  c Click **Set**.

  d Click **Yes** to confirm.

  e Click **Yes** to restart the agent.

  - To test the connection with the ADS server, click **Test Connection with Server**.
  - To test the connection with the Active Directory Health Analyzer agent, click **Test Connection with Agent**.

6

Auditing & Alerting

The Auditing & Alerting module helps you manage auditing and alerting needs. The audit agent collects and stores the events that you identify to the audit database. You can run reports on the collected information and send alert notifications to specified recipients. To manage the audit database, you can archive or purge selected data.

Topics

- Using the Auditing & Alerting landing page
- Managing audit reports
- Managing archive reports
- Managing audit agents
- Managing alerts
- Managing event definitions
- Archiving & purging audit events

Using the Auditing & Alerting landing page

The Auditing & Alerting landing page displays the active tiles for each feature in the section. The active tiles automatically update every 30 minutes, but you can use the icons to refresh the tiles at any time. You also can pause and resume the refresh of data. To customize the active tile refresh, see Setting general user options.

To use the auditing & alerting landing page

1. Select **Auditing & Alerting**.
2. To access the features in this section, click an active tile or choose from the tree.
   - Audit Reports (See Managing audit reports.)
   - Archives (See Managing archive reports.)
   - Alerts & History (See Managing alerts.)
   - Audit Agents (See Managing audit agents.)
   - Event Definitions (See Managing event definitions.)
   - Archive & Purging (See Archiving & purging audit events.)

Managing audit reports

Reports provide a means to filter the data in the audit database. Active Administrator® has default reports that display under **User Reports**. You also can create reports. All reports are stored in the Active Administrator database and are available to all users.

Topics

- Creating a new audit report
- Creating a new audit report by copying a report
- Running an audit report
- Scheduling audit reports
- Changing ownership of scheduled reports
- Categorizing audit reports
- Using tags to mark events
- Adding a comment to an event
- Grouping events
- Viewing event details

To manage audit reports

1 Select **Auditing & Alerting | Audit Reports**.

The left pane displays the list of auditing reports that are grouped by categories. You also can designate reports to be listed under **Favorites**.

All Events (Last 24 Hours) is a snapshot of the audit database. The **Applied Filters** area displays the last 1000 events collected based on the applied filters and selected report.

2 Use the tool bar to manage the audit reports.

Table 61. Audit reports tool bar

Option	Description
Refresh All	Refresh the report list.
Refresh Selected	Refresh selected reports.
New	Create a new report. See Creating a new audit report.
Edit audit report	Edit the selected report.
Delete	Delete the selected report(s).
View	Generate a report to send as an email, to save to a file, or to open in a report editor. See Running an audit report.
Schedules	Schedule a report. See Scheduling audit reports. Change ownership of scheduled reports. See Changing ownership of scheduled reports
More | Copy As	Copy an existing report to create a new report. See Creating a new audit report by copying a report.
Categories	Manage report categories. See Categorizing audit reports.
Tags	Manage audit tags. See Using tags to mark events.
Grouping	Group events to organize the display. See Grouping events.

Creating a new audit report

A wizard guides you through creating an audit report. You also can copy an existing report and make changes to create a new report. See Creating a new audit report by copying a report.

NOTE: If you want a report that identifies the user account that modified or deleted any audit reports, include the **Active Administrator Audit Report Updated** or **Active Administrator Audit Report Deleted** events.

To create a new report

1. Select **Auditing & Alerting | Audit Reports**.
2. Click **New**.
3. On the **Welcome** page, click **Next**.
4. Type a name and description for the report.
5. Click **Next**.
6. To display the report under **Favorites**, select the check box.
7. To display the results in a table format, select **Export View**. Otherwise, leave the check box unselected to generate a formatted report.
8. To categorize the report, browse to choose a category. See Categorizing audit reports.
9. By default, all comments attached to an event are included. You can choose to exclude all comments or include only a set number of the most recent comments.
10. Click **Next**.
11. By default, the report is filtered by today's date. You can add additional filters to the report.

    To add filters

    a. Click **Add Filter**.

    b. Select a filter from the list.

    The **Edit Report Filter** page lists all the possible filters, but opens to the filter that you selected. You can continue to define the filter you selected and add additional filters.

    c. Select a filter to add a definition.

Table 62. Audit report filters

Filter	Description
Date/Time Range	By default, the Date/Time Span filter is set to 1 day. You can change this filter and add other filters by selecting a filter in the list. On each filter, all items are selected by default. You can choose to include or exclude selected items.
Acting Users	By default, all users are included in the report results. You can include or exclude selected users.
Events	By default, all events are included in the report results. You can include or exclude selected events.
Domain Controllers	By default, all servers are included in the report results. You can include or exclude selected servers.

Table 62. Audit report filters

Filter	Description
Event Description Filters	You can filter the report results by text that displays either in the **Action Text** column of the **Report Results Preview** area or in the **Event Details** area. ***To add a search value*** 1 Click **Add**. 2 Type a search value. 3 Choose whether to filter the **Action Text** column or the **Event Details** area. 4 Click **OK**. 5 Choose to include only events that include the search value or do not include the search value in their descriptions. 6 Choose to include all or any of the lines shown in the **Search Values** area. **NOTE:** If you want to use Full-Text Search to filter the event descriptions, you must first install Full-Text Search, and then enable Full-Text Search in Active Administrator. For more information on installing Full-Text Search, refer to the documentation for SQL Server® Database Engine. To enable Full-Text Search in Active Administrator, use the AA Server Manager tool. See Managing the Active Directory server.
Event Log ID's	By default, all Event IDs are included in the report results. You can include or exclude specific Event IDs.
Affected Object Locations	By default, all Object Locations are included in the report results. You can include or exclude specific Object Locations.
Affected Object Types	By default, all Object Types are included in the report results. You can include or exclude specific Object Types.
Failure/Success	By default, all Event Types are included in the report results. You can include or exclude specific Event Types.
Event Tags	By default, all Tags are included in the report results. You can include or exclude specific Tags. See Using tags to mark events.
Comments Mask	You can filter the report results by text that displays in the **Comments** area of the **Event Details**. See Adding a comment to an event and Viewing event details.
Attributes	You can filter the report results by changes in their attributes. You can search for the value before the change or after the change. ***To add an attribute*** 1 Click **Add**. 2 Type an Attribute. 3 Choose whether a Value is before the change occurred or after the change occurred. 4 Click **OK**.

12 Click **Next**.

13 Review the summary, and click **Finish**.

14 Click **Finish**.

Creating a new audit report by copying a report

Instead of creating an entirely new report, you can copy an existing report and make minor changes to create a new report.

To create a new report by copying a report

1. Select **Auditing & Alerting | Audit Reports**.
2. Select a report, and select **More | Copy As**.
3. Type a new name for the report.
4. Select the report, and click **Edit**.
5. Make the desired changes to the report. See Creating a new audit report.
6. Click **OK**.

Running an audit report

By default the report is generated and sent by email to the listed recipients and/or copied to a file in a specified location. You can choose to generate a report and display in a report editor where you can save, print, export, and email the document from the **Preview** window. You also can display the report in a basic table format.

NOTE: The email server must be configured to send notifications. See Setting email server options.

To send an audit report by email or save to a file

1. Select **Auditing & Alerting | Audit Reports**.
2. Select a report, and click **View.**
3. Select **Delivery report**.
4. Change the default report file name, if desired.
5. By default, the date and time are appended to the end of the file name. Clear the check box if you do not want the date and time appended to the file name.
6. Choose a format for the report. By default, a PDF file is created.
7. By default the report is generated and sent by email to the listed recipients. By default, the logged in account displays in the **Email Addresses** list. You can add more addresses to receive the report by email. A default subject line is included. Set the priority of the email.
8. You also can save the report to a specified location on the **Save to Folder** tab. Add a path to the location where you want to store the report file.
9. Click **OK**.

To display an audit report in a report editor

1. Select **Auditing & Alerting | Audit Reports**.
2. Select a report, and click **View.**
3. Select **Interactive**.
4. Click **OK**.

To display results in a table format

1. Select **Auditing & Alerting | Audit Reports**.
2. Select a report, and click **View.**
3. Select **Export View**.

4 Click **OK**.

Scheduling audit reports

Except for the All Events (last 24 hours) report, you can schedule auditing reports to send to specified email recipients or to a file.

There are two ways to schedule an audit report. You can select a report from the list of reports and manage the schedules for that selected report. You also can view the list of reports separated into unscheduled and scheduled categories and manage schedules from there. In either location, you can add, edit, and remove schedules.

NOTE: The email server must be configured to send notifications. See Setting email server options.

To schedule an audit report

1 Select **Auditing & Alerting | Audit Reports**.

2 Select a report, and select **Scheduling | Schedules**.

-OR-

Select **Scheduling | Scheduled Reports**, and select a report from the list of unscheduled and scheduled reports.

The schedules for the selected report display. Using the buttons, you can add, edit, or remove a schedule for the selected report.

NOTE: By default, only the schedules that you create are listed. If you want to see the schedules that all other users create, you can select the **Show scheduled reports for all users** check box in User Options. See Setting options for audit reports.

3 To add a new schedule for the selected report, click **Add**.

–OR-

To edit a selected schedule for the selected report, click **Edit**.

4 By default the report is generated and sent by email to the listed recipients and/or copied to a file in the specified location on the **Save to Folder** tab. To disable the schedule, clear the check box.

5 To change the default schedule, click **Update**, set the new schedule, and click **OK**.

6 Change the default report name if desired.

7 By default, the date and time are appended to the end of the file name. Clear the check box if you do not want the date and time appended to the file name.

8 By default, a PDF file is created. You can choose a different format.

9 You can send the report by email and save it to a file.

To send an email

a Click **Email**, if necessary.

b By default, the logged in account displays in the Email Addresses list. To add more recipients, click **Add**, type the email addresses, and click **OK**.

c Modify the default subject line if desired.

d Set the priority of the email.

To save the file to a folder

a Click **Save to Folder**.

b Click **Add**.

c Add a path to the location where you want to store the report file.

d Click **OK**.

10 Click **OK**.

11 Click **Close**.

Changing ownership of scheduled reports

When a user creates a scheduled audit report, that user owns the report schedule and only that user can see the schedule. In the event a user leaves the company, another user with Full Control permissions for Active Administrator can take over the ownership of the scheduled reports.

To change ownership of scheduled reports

1 Select **Settings | User Options | Audit Reports**, and select **Show scheduled reports for all users**. See Setting options for audit reports.

2 Select **Auditing & Alerting | Audit Reports | Scheduling | Scheduled Reports**. See Scheduling audit reports.

   If you own the schedule, your account does not display next to the schedule. If another user owns the schedule, their account displays in brackets next to the schedule.

   NOTE: You must have Full Control permissions for Active Administrator to complete the next steps.

3 Select a scheduled report.

4 Select a schedule.

   If you own the schedule, you can transfer ownership to another account.

   If another user owns the schedule, you can take ownership of this schedule or transfer ownership to another account.

   To transfer ownership

   a Click **Add** to create a new schedule or **Edit**/**View** to modify the existing schedule.

   b Click **Transfer Ownership**, and browse for an account.

   c Click **OK**.

   To take ownership

   a Click **Add** to create a new schedule or **View** to modify the existing schedule.

   b Click **Take Ownership**, and browse for an account.

   c Click **OK**.

5 Click **OK**.

Categorizing audit reports

Reports can be grouped into categories or added to Favorites.

To add a report category

1 Select **Auditing & Alerting | Audit Reports**.

2 Click **Categories**.

3 Click **Add**.

4 Type a name and description.

5 To create a subcategory, type a report category name in the box, or browse to locate a report category.

6 Click **OK**.

To move a report to a category

1. Select **Auditing & Alerting | Audit Reports**.
2. Right-click a report, and select **More | Move to Category**.
3. Choose a category from the list.
4. Click **OK**.

To add a report to Favorites

1. Select **Auditing & Alerting | Audit Reports**.
2. Right-click a report, and select **More | Add to Favorites**.

To remove a report from Favorites

1. Select **Auditing & Alerting | Audit Reports**.
2. Right-click a report, and select **More | Remove from Favorites**. Since the report was a copy, the report is still in its original location

Using tags to mark events

In the **Applied Filters** area, you can apply a tag to a result, and then filter the results by that tag. One application would be to tag events that you would later research.

To add tags

1. Select **Auditing & Alerting | Audit Reports**.
2. Click **Tags**.
3. Click **Add**.
4. Type the name of the tag.
5. Click **OK**.

To delete tags

1. Select **Auditing & Alerting | Audit Reports**.
2. Click **Tags**.
3. To filter the list of tags, starting typing in the **Filter tags** box.
4. Select one or more tags, and click **Delete**.
5. Click **OK**.

To tag an event

1. Select **Auditing & Alerting | Audit Reports**.
2. Right-click an event in the **Applied Filters** area, and choose **Add Tag**.
3. Select a tag from the **Select Tag** list.
4. Click **OK**. The tag appears in the **Tags** column.
    - You can filter an audit report based on tags. See Creating a new audit report.
    - You also can manage tags through event details. See Viewing event details.

To remove a tag from an event

1. Select **Auditing & Alerting | Audit Reports**.

2 Right-click the event in the **Applied Filters** area, and choose **Event Details**.

3 Click **Tags**.

4 Click **Select Tags**.

5 Clear the check box next to the tag you want to remove.

6 Click **OK**.

7 Click **Close**.

Adding a comment to an event

In the **Applied Filters** area, you can add a comment to a result, and then filter the results by text in that comment.

To add a comment to an event

1 Select **Auditing & Alerting | Audit Reports**.

2 Right-click the event in the **Applied Filters** area, and choose **Add Comment**.

3 Type the comment.

4 Click **OK**. The comment displays in the **Last Comment** column.

- You can filter an audit report based on comments. See Creating a new audit report.
- You also can manage comments through event details. See Viewing event details.

To remove a comment from an event

1 Select **Auditing & Alerting | Audit Reports.**

2 Right-click the event in the **Applied Filters** area, and choose **Event Details**.

3 Click **Comments**.

4 Click **X** next to the comment you want to delete.

5 Click **Yes**.

6 Click **Close**.

Grouping events

The **Applied Filters** area lists the last 1000 events in the auditing database based on the filters you added to the report. Use the navigation keys to page through the results. Click on the column headings to sort the events. You can also group the results by the various column headings.

To group events

1 Select **Auditing & Alerting | Audit Reports**.

2 Click **Grouping,** and select to group by computer name, user account, or action text.

To ungroup events

1 Select **Auditing & Alerting | Audit Reports**.

2 Click **Grouping**, and select **Remove Grouping**.

Viewing event details

In addition to viewing the event details, you can send the event in an email to specified recipients.

NOTE: The email server must be configured to send notifications. See Setting email server options.

To view event details

1. Select **Auditing & Alerting | Audit Reports**.
2. Double-click an event in the **Applied Filters** area.

   You can scroll through the list of events by clicking the arrows.

   - To view the details of the event, click the various sections: **Action Text**, **Event Details**, **Comments**, **Tags**, and **Applied Filters**.
   - On the **Comments** page, you can add a comment. See Adding a comment to an event.
   - On the **Tags** page, you can add tags to the event. See Using tags to mark events.
   - To send the event as an email, click **Send Email**, edit the subject line, add recipients, and click **Send**.

Managing archive reports

You can create and run reports on the data in the archive audit database.

To manage archive reports

1. Select **Auditing & Alerting | Archives**.
2. Select the archive to use.

   The left pane displays the list of auditing reports that are grouped by categories. You also can designate reports to be listed under Favorites.

   All Events (Last 24 Hours) is a snapshot of the archive audit database. The Applied Filters area displays displays the last 1000 events collected based on the applied filters and selected report.
3. Use the tool bar to manage the archive reports.

Table 63. Audit reports tool bar

Option	Description
Refresh All	Refresh the report list.
Refresh Selected	Refresh selected reports.
New	Create a new report. See Creating a new audit report.
Edit	Edit the selected report.
Delete	Delete the selected report(s).
View	Generate a report to send as an email, to save to a file, or to open in a report editor. See Running an audit report.
Schedules	Schedule a report. See Scheduling audit reports.
More	Copy an existing report to create a new report. See Creating a new audit report by copying a report.
Categories	Manage report categories. See Categorizing audit reports.
Tags	Manage Audit tags. See Using tags to mark events.
Grouping	Group events. See Grouping events.

Managing audit agents

You can manage audit agents from the **Audit Agent** page. Initially the display is blank. You must install and activate the audit agent to begin collection of audit events.

NOTE: A warning may appear at the bottom of the page that indicates domain controllers are present without installed audit agents. You can suppress this warning by selecting the check box. If you want to reinstate this warning, select **Configuration | Agent Installation Options**. See Setting agent installation options.

The bottom half of the display shows the tasks that pertain to audit agents. To manage all tasks in Active Administrator, see Managing tasks. Click the chevron to hide the **Tasks** area.

A warning message displays to inform that domain controllers do not have audit agents installed. To suppress this display, click the check box. You can manage the display of the message using **Configuration | Agent Installation Settings**. See Setting agent installation options. Alternatively, you can exclude selected domain controllers to suppress this message. See Excluding domain controllers.

Topics

- Excluding domain controllers
- Setting up auditing on domain controllers
- Installing audit agents
- Modifying the audit agent startup account
- Modifying the audit agent test account
- Updating audit agents
- Moving an audit agent
- Automating audit agent deployment
- Canceling pending automated deployments

To manage audit agents

1. Select **Auditing & Alerting | Agents**.
2. Use the tool bar to manage audit agents.

NOTE: When you select **Remove**, **Start**, **Stop**, or **Move**, you are asked to select the account to use to manage the agent. You can use the Active Administrator Foundation Service (AFS) account, or indicate a specific user account.

Table 64. Audit agent tool bar

Option	Description
Refresh	Refresh the audit agent on all listed domain controllers.
Refresh Selected	Refresh the audit agent on selected domain controllers.
Install	Install the audit agent on the selected domain controller. See Installing audit agents.
Properties	Display properties, change the start-up account, or SQL Authentication for the selected domain controller.
Remove	Remove the audit agent from the selected domain controller. **NOTE:** You must select the account to use to remove the audit agent.
Start	Start collecting events on the selected domain controller(s). **NOTE:** You must select the account to use to start the audit agent.

Table 64. Audit agent tool bar

Option	Description
Stop	Stop collecting events on the selected domain controller. **NOTE:** You must select the account to use to stop the audit agent.
More | Test Agent Account	Set the test agent account. See Modifying the audit agent startup account.
More | Set Startup Account	Set the startup account. See Modifying the audit agent test account.
More | Move	Move the audit agent to another computer. See Moving an audit agent. **NOTE:** You must select the account to use to move the audit agent.
More | Update	Update the audit agent on the selected domain controller(s) to the version installed on the server. See Updating audit agents.
More | Update All	Update the audit agent on all listed domain controllers to the version installed on the server. See Updating audit agents.
More | Excluded Domain Controllers	Exclude domain controllers from Active Administrator. See Excluding domain controllers.
More| Group by	Group the list of domain controllers by Domain, Status, or Agent Computer.
Tasks	Manage the tasks that pertain to the audit agent. See Managing tasks.
Autodeployment	Set up Active Administrator so the audit agent is installed on newly discovered domain controllers. See Automating audit agent deployment.

Excluding domain controllers

You can exclude domain controllers from Active Administrator so you do not see the information banner at the bottom of the display that indicates a domain controller does not have an audit agent installed.

To exclude domain controllers from Active Administrator

1. Select **Auditing & Alerting | Agents**.
2. Select **More | Excluded Domain Controllers**.
3. Select a domain controller, and click **Exclude**.
4. Click **OK**.

NOTE: If at a later time you want to install an audit agent on an excluded domain controller, repeat this process and choose to include the domain controller.

Setting up auditing on domain controllers

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

To set up auditing on a domain controller

1. Start Active Administrator Console.
2. Select **Group Policy | Group Policy Objects**.
3. Select **Default Domain Controllers Policy**, and click **Edit**.

4 Expand **Computer Configuration | Windows Settings | Security Settings | Local Policies**, and select **Audit Policy**.

5 Verify that the following polices are defined. If not, double-click the following policies to edit their Success and Failure settings.

Table 65. Default domain controller policy settings

Policy	Setting
Audit logon events	[Success, Failure]
Audit account logon	[Success]
Audit account management	[Success]
Audit directory service access	[Success]
Audit policy change	[Success]
Audit system events	[Success]

6 Close the **Group Policy** window.

7 From the command prompt, refresh the Group Policies by typing **gpupdate /force**.

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

NOTE: If there are issues detecting audit events when monitoring domain controllers, manually set the above audit policies for each type of object using the Microsoft auditpol system utility.

Installing audit agents

To collect data on a computer, you must install and activate the audit agent.

IMPORTANT: For Active Administrator Server agents to audit Active Directory events, auditing must be enabled in all domains that will be monitored. Make sure that Windows auditing is enabled on the Default Domain Controller policy. See Setting up auditing on domain controllers.

To install an audit agent

1 Select **Auditing & Alerting | Agents**.

2 Click **Install**.

The **Welcome** page reminds you to enable auditing in Active Directory®. See Setting up auditing on domain controllers.

3 Click **Next**.

4 In the **Domain** box, type the domain name; or browse to locate a domain.

5 If necessary, click **Find Domain Controllers**.

- To select all listed domain controllers, click **Select all**.
- To clear all the check boxes, click **Clear all**.

6 Select the domain controllers from which you want to audit activity.

7 Click **Next**.

8 Select the options for the install process.

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

Table 66. Options for the install process

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

9 Click **Next**.

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

> **NOTE:** The Active Administrator Agent service can also run under a domain user account provided it is a local administrative 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.

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

12 Click **Next**.

13 Review the summary.

14 Click **Next**.

15 Click **Finish**.

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

> **NOTE:** By default, the audit agent is activated upon installation. To change the default setting, click **Configuration | Agent Installation Settings**. See Setting agent installation options.
>
> You can view details about the install in the **AuditAgentInstall*.log** file, which is located in C:\ProgramData\Quest\Active Administrator\Logs.
>
> **NOTE:** If you experience deactivated audit agents after installing agents in a new domain on a Windows Server 2016, Windows 2019, or Windows 2022 domain controller, clear the security event log and restart the audit agent.

Modifying the audit agent startup account

> **IMPORTANT:** The agent startup account must have the privilege to manage auditing and security logs. Domain administrators have this privilege by default.

To modify the audit agent startup account

1. Select **Auditing & Alerting | Agents**.
2. Select a domain controller, and select **More | Set Startup Account**.
3. Change the account used to start the audit agent.

   NOTE: A domain administrator account is recommended. The Active Administrator audit agent service can run under a domain user account if it is a local administrative account, which gives it the rights to log on as a service and log on locally, or an account with these two privileges granted individually. This account should also be a member of the AA_Admin group, which by default is located in the Local groups of the server where the ActiveAdministrator database is located. If the group is not found in this location, the settings during the initially database creation were modified and the group can be found under the Users container object of Active Directory.

4. Type the password.
5. Click **OK**.

Modifying the audit agent test account

By default, Active Administrator monitors the status of the audit agent.

To modify the audit agent test account

1. Select **Auditing & Alerting | Agents**.
2. Select a domain controller, and select **More | Test Startup Account**.
3. Change the account used to monitor the status of the audit agent.
4. Type the password.
5. Click **OK**.

Updating audit agents

If you receive an update to the audit agent, use this option to install the update.

To update audit agents

1. Select **Auditing & Alerting | Agents**.
2. To update selected domain controllers, 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**.

Moving an audit agent

You can move the audit agent from one computer to another.

To move an audit agent

1. Select **Auditing & Alerting | Agents**.

2 Select a domain controller, and select **More | Move**.

> **IMPORTANT:** Auditing must be enabled in all domains that will be monitored. Make sure auditing is enabled on the Default Domain Controller policy. See the *Quest*® Active Administrator®*Install Guide*.

3 Select the account to use to move the agent. You can use the Active Administrator Foundation Service (AFS) account, or indicate a specific user account.

> **NOTE:** The selected account must be a full Administrator on the target server.

4 Click **Next**.

5 Type the target computer name or browse to locate a computer.

6 Type the user name and password of the account with domain administrative rights on the selected target computer.

> **NOTE:** The Active Administrator Agent service can run under a domain user account provided it is a local administrative account, which gives it the rights to **log on as a service**, **log on locally**, and **manage auditing and security log**, or an account with these privileges granted individually. This 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 the group can be found under the Users container object of Active Directory®.

7 Choose options for the install process.

Table 67. Install options

Option	Description
Start collecting events immediately after installation of the agent	By default, the audit agent is activated and collection begins immediately upon completion of the installation process. Clear the check box if you want to activate the audit agents manually.
Enable agent monitoring and recovery	By default, Active Administrator monitors the status of the audit agent.

8 Click **OK**.

> **NOTE:** You can view details about the move agent process in the **MoveAgentInstall*.log** file, which is located in C:\ProgramData\Quest\Active Administrator\Logs.

Automating audit agent deployment

Once you have installed an agent into a domain, Active Administrator can monitor the domain for new domain controllers. When a new domain controller is discovered, the agent can be automatically installed on that domain controller. You also have the option to just notify users of a new domain controller so they can install the agent manually.

- Deploy audit agent automatically
- Notify users only

Deploy audit agent automatically

To deploy the audit agent automatically

1 Select **Auditing & Alerting | Agents**.

2 Click **Auto Deployment**.

3 On the **General** tab, select **Enable automated agent deployment and notification**.

4 Select whether to install the audit agent on the newly discovered domain controller or to audit the newly discovered domain controller using an agent on a different computer.

Table 68. Install options

Option	Description
Install on target Domain Controller(s)	By default, the audit agent is installed on the newly discovered domain controllers.
Audit from an agent on the following computer	Select to install the audit agent on a computer in the domain. Type a computer name in the box, or browse to locate a computer. **NOTE:** If you choose to do remote monitoring, the Advanced Agent is not installed on the selected domain controllers.

5 Type an account with domain administrative rights, or browse to locate an account, and enter the password.

> **NOTE:** The Active Administrator Agent service can also run under a domain user account provided it is a local administrative account, which gives it the rights to log on as a service, log on locally, and **manage auditing and security log**, or an account with these privileges granted individually. This 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 the group can be found under the Users container object of Active Directory.

6 By default, Active Administrator waits 24 hours after discovering a domain controller before installing the audit agent. Change the wait time if necessary.

> **NOTE:** During the wait time, you can cancel the pending installation. See Canceling pending automated deployments.

7 By default, Active Administrator monitors the status of the audit agent. To disable service monitoring and recovery, clear the check box.

8 Click **OK**.

Notify users only

To only notify users of newly discovered domain controllers

1 Select **Auditing & Alerting | Agents**.

2 Click **Auto Deployment**.

3 On the **General** tab, select **Enable automated agent deployment and notification**.

4 Select **Only notify users**.

5 Use the buttons to add, edit, or remove email addresses from the list.

> **NOTE:** You also can manage the Agent Auto Deploy Configuration email list from the **Settings** menu. See Managing email addresses.

6 Click **OK**.

Canceling pending automated deployments

When you set up Auto Deployment, you set a wait time between discovering domain controllers and installing the agent. During that wait time you can cancel the installation.

Topics

- Creating an alert
- Managing existing alerts
- Changing the alert notification policy
- Setting global quiet time
- Managing alert history

To cancel pending automated deployments

1 Select **Auditing & Alerting | Agents**.

2 Click **Auto Deployment**.

3 Click **Pending Installations**.

4 Select a pending installation, and click **Cancel automated agent installation**.

5 Click **OK**.

Managing alerts

Alerts give you the opportunity to combine different alert conditions into a set that is sent to specified individuals. You can also add a filter to the condition set to further isolate audit events for the email recipient.

NOTE: The email server must be configured to send notifications. See Setting email server options.

TIP: You can configure the notification service to send emails in batches. See Setting notification options.

NOTE: The Active Directory Health module also uses alerts to help you manage Active Directory®. See Setting alerts.

TIP: Each alert has a separate email address list for notification. To manage the email list, you can edit the individual alert or you can manage the email address lists in one location. See Managing email addresses.

The **Alert** page shows the alerts in the top pane and the alert history for a selected alert in the bottom pane. You can size the panes by dragging the horizontal split bar up or down.

To manage alerts

1 Select **Auditing & Alerting | Alerts**.

2 Use the tool bar to manage alerts.

Table 69. Alerts tool bar

Option	Description
Refresh	Refresh all alerts.
Refresh Selected	Refresh selected alerts.
New	Add a new alert. See Creating an alert.
Edit	Edit an existing alert.
Delete	Delete a selected alert.
More	Enable or disable alerts. Suspend or resume email notifications. See Managing alerts.
Notification Policy	Set the policy for alert notification emails. See Changing the alert notification policy.

Table 69. Alerts tool bar

Option	Description
Global Quiet Times	Set global alert quiet times for all alerts. See Setting global quiet time.
Alert History	Filter the alert history, view details on an alert history item, resend an alert in an email, or run a report. See Setting global quiet time.

Creating an alert

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

To create a new alert

1. Select **Auditing & Alerting | Alerts**.
2. Click **New**.
3. On the **Welcome** page, click **Next**.
4. Type a name and optional description for the alert.
5. Select the priority of the alert: normal, low, or high.
6. Click **Next**.
7. Click **Add** and type the email address to receive notification of the alert.
   - To edit a selected email address, click **Edit**.
   - To remove a selected email address from the list, click **Remove**.

   NOTE: To manage the Auditing and Alerting Alerts email address list, see Managing email addresses.
8. Click **Next**.
9. Select the Event Definitions to include in the alert.
   - To filter the list, type **text** in the **Filter** box. The list changes as you type characters. The definitions displayed contain the characters you type. For example, if you type **com**, the definitions displayed may contain the words **Com**pleted or **Com**puter.
   - To clear the filter and restore the list, click **X**.
   - To show only selected definitions, open the Show box, and choose **Selected**.
   - To show only unselected definitions, open the Show box, and choose **Unselected**.
10. Click **Next**.
11. Add alert filters.

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

    a. To add a new alert filter, click **Add**.

    –OR-

    To edit a selected alert filter, click **Edit**.

    b. Select if the email **Contains** or **Does not contain** the condition text.

    c. Type the text to find in the details section of the alert.

d By default the filter conditions are combined using the **OR** operator. If you want to connect with the AND operator, select **AND all conditions**.

12 Click **Next**.

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

> **NOTE:** There is also a global quiet time that you can set. The quiet times set here are in addition to any global quiet times. See Setting global quiet time.

a To add a new quiet time, click **Add**.

–OR-

To edit a selected quiet time, click **Edit**.

b Select **Enabled**. To disable a quiet time, clear the check box.

c Select All Days or specify a specific day.

d Set the start and end time.

e By default, actions associated with the alert are stopped during quiet time. To run actions during quiet time, select the check box.

14 Click **Next**.

15 Set the alert threshold. The alert threshold sets limits that must be met before alerts are sent out.

a To add a new threshold, click **Add**.

–OR-

To edit a selected threshold, click **Edit**.

b Select **Enabled**. To disable a threshold, clear the check box.

c Select the event definition from the list.

d Select the number of events and minutes to define the threshold.

16 Click **Next**.

17 Define the action that this alert runs when the alert condition is met.

> **NOTE:** The action is run using the Notification service account. Please make sure the Notification Service account has sufficient rights to all of the resources needed by the action.

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

b Type the full path to the executable for the program or script or browse to locate the executable.

> **NOTE:** The script must reside in a share on the Active Administrator server. That share must be accessible to the Active Administrator Foundation Server (AFS) service and the operator of the remote Active Administrator console. The path to the script must be entered using Uniform Naming Convention (UNC).

c For the argument, browse to open the list of **Alert Action Variables**.

a Select a variable in the top box.

b Click **Insert**.

c Click **OK**.

d Optionally, type the path to a folder that contains the executable or browse to locate the folder.

e If you want to delay the action that the alert will run, enter a time delay in minutes.

18 Click **Next**.

19 Review the summary.

20 Click **Finish**.

Managing existing alerts

You can enable and disable alerts, either individually or all at once. A disabled alert is not triggered, therefore no email is sent regardless of the status of the notification policy.

You also can suspend email notifications, either individually or all at once. To suspend the email notification globally, see Changing the alert notification policy.

NOTE: Suspended alerts will not send emails when the alert is triggered. The suspended alert is still logged into alert history.

To enable or disable selected alerts

1. Select **Auditing & Alerting | Alerts**.
2. Right-click one or more alerts, and choose **Disable** or **Enable**.

To enable or disable all alerts

1. Select **Auditing & Alerting | Alerts**.
2. Select **More | Disable All** or **More |Enable All**.

To suspend or resume email notification on selected alerts

1. Select **Auditing & Alerting | Alerts**.
2. Right-click one or more alerts, and select **Suspend** or **Resume.**

To suspend or resume email notification on all alerts

1. Select **Auditing & Alerting | Alerts**.
2. Select **More | Suspend All** or **More |Resume All**.

Changing the alert notification policy

You can view the status and past history of the alert notification policy. The alert notification policy determines how many notifications are sent within a specified time period and if an email is sent to the administrator when alerts are suspended. You also can disable the notification of alerts altogether.

To change the notification policy

1. Select **Auditing & Alerting | Alerts**.
2. Click **Notification Policy**.

   The **Status** and **History** pages display information about the current status of the alert notification policy.
3. Click **Settings**.
4. By default, the alert notification policy is enabled. To disable the policy, clear the check box.
5. Set the maximum number of alerts to send and the period of time to include. By default, a maximum of 100 alerts are sent in a 20 minute period and the counter resets after 10 minutes.
6. By default, a notification is sent to the administrator when alerts are suspended. To not send notifications, clear the check box.
7. Click **OK**.

Setting global quiet time

Define the quiet time during which no notifications are sent. Alerts that are triggered during the quiet time are still logged to the alert history. You also can set a global quiet time for each individual alert. See Creating an alert.

To set global quiet time

1. Select **Auditing & Alerting | Alerts**.
2. Click **Global Quiet Times**.
3. To add a new quiet time, click **Add**.

   –OR-

   To edit a selected quiet time, click **Edit**.
4. Select **Enabled**. To disable a quiet time, clear the check box.
5. Select **All Days** or specify a specific day.
6. Set the start and end time.
7. By default, actions associated with the alert are stopped during quiet time. To run actions during quiet time, select the check box.
8. Click **OK**.

Managing alert history

The bottom pane on the **Active Administrator Alerts & Alert History** page displays the history for the selected alert. By default, all event definitions for the selected alert display. In addition to filtering the list, you can limit the display by selecting individual events to display.

You can resend the alert to selected email addresses. You also can create an alert history report to send to specified email recipients or to save to a file.

Topics

- Filtering alert history
- Viewing alert history details
- Resending an alert notification
- Creating an alert history report

To manage alert history

1. Select **Auditing & Alerting | Alerts**.
2. Use the Alert History menu to manage the alert history in the bottom pane.

Table 70. Alert history menu options

Option	Description
Refresh	Refresh the display.
Details	View details about the selected event. See Viewing alert history details.
Resend	Resend an alert notification. See Resending an alert notification.
Filter	Filter the list of alert history. See Filtering alert history.
Clear Filter	Clear filters from the list of alert history.
Report	Create a report. See Creating an alert history report.

Filtering alert history

To filter alert history

1. Select **Auditing & Alerting | Alerts**.
2. Select an alert in the top pane.
3. Select **Alert History | Filter**.
4. By default, only the alert history for the current day displays in the left pane. You can select a different day from the calendar drop-down or specify a range of dates.
5. Click **OK**.

Viewing alert history details

To view alert history details

1. Select **Auditing & Alerting | Alerts**.
2. Select an alert.
3. Select an event in the **Alert History** pane, and select **Alert History | Details**.
   - To scroll through the list of events in the **Alert History** pane by clicking **Next** or **Back**.
   - To resend an alert for the selected event, click **Resend**.

Resending an alert notification

NOTE: You also can resend an alert from the details page. See Viewing alert history details.

To resend an alert

1. Select **Auditing & Alerting | Alerts**.
2. Select an alert.
3. Select an event in the **Alert History** pane, and select **More | Resend**.
4. In the **Comments** area, type a message about the email.
5. Select the email addresses you want to receive the email notification. To add additional email addresses to the list, click **Add**.
6. Click **Send**.

Creating an alert history report

To create an alert history report

1. Select **Auditing & Alerting | Alerts**.
2. Select **Alert History | Report**.
3. By default, all dates are included in the report.
   - To specify a specific day for the report, select **Date**, and type a date or select from the calendar.
   - To specify a range of dates, select **Date Range**, and type the dates or select from the calendar.
4. By default, all alerts are included in the report. To filter the report, select **Filter by Alerts**, and select specific alerts to include in the report.

5 Type a name for the report.

6 Choose a format for the report. By default, a PDF file is created.

7 By default the report is generated and sent by email to the listed recipients. By default, the logged in account displays in the **Email Addresse**s list. You can add more addresses to receive the report by email. A default subject line is included. Set the priority of the email.

8 You also can save the report to a specified location on the **Save to Folder** tab. Add a path to the location where you want to store the report file.

> **NOTE:** If you want to generate the report in a report editor where you can preview the report, select **Interactive**. You can save, print, export, and email the document from the **Preview** window.

9 Click **OK**.

Managing event definitions

The **Event Definitions** page lists the events definitions, and for a selected event, the details for that definition and the alert attached to the definition.

Topics

- Importing new event definitions
- Excluding account events from auditing

To manage event definitions

1 Select **Auditing & Alerting | Event Definitions**.

2 Use the tool bar to manage event definitions.

Table 71. Event definitions tool bar

Option	Description
Refresh	Refresh the list.
Import	Import new event definitions into the audit database. See Importing new event definitions.
Enable	Enable selected event definitions.
Disable	Disable selected event definitions.
Remove Alert	Remove a selected alert from a selected event definition.
Exclude Accounts	Exclude accounts and all of their related events from auditing. See Excluding account events from auditing.

Importing new event definitions

The event definitions file, EventDefinitions.edx, is located in the Active Administrator\Server folder. Occasionally new event definition files are made available. You can import these new event definitions into your auditing database.

> **IMPORTANT:** When event definitions are imported, existing definitions with the same name are overwritten.

To import new event definitions

1 Select **Auditing & Alerting | Event Definitions**.

2 Click **Import**.

3 Locate the event definitions file (*.edx), and click **Open**.

> **NOTE:** New event definitions are added and existing definitions are updated. No event definitions are deleted.

4 Click **Import**.

Excluding account events from auditing

The events for specific accounts can be excluded from auditing. Accounts can be removed from the Excluded Accounts list to reinstate auditing of events for those accounts.

To exclude account events from auditing

1 Select **Auditing & Alerting | Event Definitions**.

You can select to search for accounts to exclude accounts by name, group, or OU.

To exclude accounts by name, select **Exclude Accounts by Name.**

a Select a domain, type the account name to be excluded, and click **Search**.

b Navigate through the search results selecting one or more accounts to be excluded and click the arrow button to add them to the list of Excluded Accounts.

- OR -

Click the plus sign button to add objects to be excluded by SID.

Type the Account SID and click **Load details**.

Click **Exclude**.

To exclude accounts by group, select **Exclude Accounts by Group.**

a Select a domain, type the group name that includes the accounts to be excluded, and click **Search**.

b Navigate through the search results selecting one or more accounts to be excluded and click the arrow button to add them to the list of Excluded Accounts.

To exclude accounts by organizational usint select **Exclude Accounts by OU.**

a Select a domain, type the OU name that includes the accounts to be excluded, and click **Search**.

b Navigate through the search results selecting one or more accounts to be excluded and click the arrow button to add them to the list of Excluded Accounts.

2 Optionally, click **Refresh** to update the list of Excluded Accounts with changes made by other administrators.

3 Click **Exclude**.

To remove accounts from the Excluded Accounts list

1 Select **Auditing & Alerting | Event Definitions**.

2 Click **Exclude Accounts**.

3 Select one or more accounts in the Excluded Accounts list.

4 Click the recycle bin button to remove the selected accounts from the Excluded Accounts list.

5 Optionally, click **Refresh** to update the list of Excluded Accounts with changes made by other administrators.

6 Click **Exclude**.

Archiving & purging audit events

The audit database can become quite large over time. You should routinely purge and archive events to keep the audit database at a manageable size. If you choose to archive, the data is moved into the archive database.

Purged events are deleted from the live audit database. Archived events are first copied to the archive database and then deleted from the live audit database. You can select different events to purge or archive.

Topics

- Archiving events on demand
- Purging events on demand
- Setting purge and archive options
- Scheduling an event log purge and archive
- Managing the history log
- Running database maintenance

To archive and purge audit events

1 Select **Auditing & Alerting | Archiving and Purging**.

The top pane displays the defined audit event archiving and purging schedules.

- To switch to the **Archive and Purge History** page, click **History**.
- To switch back to the **Scheduled Audit Event Archiving and Purging** page, click **Schedule**.

The bottom pane displays the maintenance tasks specific to the Purging and Archiving Events feature. See Managing tasks.

2 Use the options on the tool bar to manage purging and archiving.

Table 72. Archive and purge tool bar

Option	Description
Archive Now	Archive event entries and alert history items from the live audit database. See Archiving events on demand.
Purge Now	Purge event entries and alert history items from the live audit database. See Purging events on demand.
Refresh	Refresh the display.
Run	Immediately runs the purge and archive based on the properties for the selected schedule. See Scheduling an event log purge and archive. You can monitor the progress in the **Tasks** area.
Add	Add a new event log purge and archive schedule. See Scheduling an event log purge and archive.
Edit	Edit a selected event log purge and archive schedule. See Scheduling an event log purge and archive.
Delete	Delete selected event log purge and archive schedules.
History	Refresh the history log display, export the history log to a file, or clear the history log display. See Managing the history log.
Tasks	Refresh the task display, view task properties, send a task to email recipients, and group the task display by status. See Managing tasks.
DB Maintenance	Run database maintenance on the audit database. See Running database maintenance.

Archiving events on demand

Copies event entries and alert history items from the live audit database to the active archive database, and then deletes the event entries and alert history from the live audit database. To schedule the archive process, see Scheduling an event log purge and archive.

To archive events on demand

1. Select **Auditing & Alerting | Archiving & Purging**.
2. Click **Archive Now**.
3. Type a date or select a date from the calendar.
4. Set options for the archive process, such as choosing to shrink the database, and include or exclude specific events. See Setting purge and archive options.
5. Click **Archive Now**.

Purging events on demand

Deletes event entries and alert history items permanently from the live audit database based on the selected purge options. To schedule the purge process, see Scheduling an event log purge and archive.

To purge events on demand

1. Select **Auditing & Alerting | Archiving & Purging**.
2. Click **Purge Now**.
3. Type a date or select a date from the calendar.
4. Set options for the purge process, such as choosing to shrink the database, and include or exclude specific events. See Setting purge and archive options.
5. Click **Purge Now**.

Setting purge and archive options

To select specific events to purge or archive, click **Purge Options** or **Archive Options**. By default, the database shrinks after the database is purged or archived and the list of event definitions is not filtered. You can choose to include or exclude selected event definitions.

You can access the purge and archive options from the **Purge Now**, **Archive Now**, **New**, or **Edit** options on the tool bar.

To set options for the event purge archive process

1. Click **Purge Options** or **Archive Options** depending on the type you selected.
2. By default, the database shrinks after purging or archiving. Clear the check box if you do not want the database to shrink.
3. You can filter the list of events by typing text in the
4. Filter box. Once you have selected events, you can choose to show **All**, **Selected** or **Unselected**. Active only if **Include** or **Exclude the selected event definitions** check boxes are selected.

> **IMPORTANT:** Events selected in **Purge Options** are deleted first. If the same events are selected in **Archive Options**, those events are not archived because they were deleted in the purge.

Table 73. Event purge/archive options

Option	Description
Do not filter event definitions	By default, all events are purged or archived based on the selected date range.
Include the selected event definitions	Select to specify specific events to purge or archive based on the selected range. Events that are not selected are not purged or archived.
Exclude the selected event definitions	Select to specify specific events to exclude from the database purge or archive. Events that are not selected are purged or archived.

5 Select the events to include or exclude from the purge or archive process.

6 Click **OK**.

Scheduling an event log purge and archive

You can choose to purge only, archive only, or purge then archive. You can select different events to purge or archive. Purged events are deleted from the live database. Archived events are copied to the archive database and then deleted from the live database.

IMPORTANT: If you select **Purge then Archive**, the events selected in **Purge Options** are deleted first. If the same events are selected in **Archive Options**, those events are not archived because they were deleted during the purge, which occurred first.

To schedule an event log purge or archive

1 Select **Auditing & Alerting | Archiving & Purging**.

2 Click **New**.

3 By default, scheduling is enabled. You can create a schedule and then disable it until you need it.

4 Type a description of the schedule.

5 Select the type of purge and/or archive.

Table 74. Type of purge and/or archive

Option	Description
Purge Only	Select to delete event entries and alert history items permanently from the live database based on the selected purge options.
Archive Only	Select to copy event entries and alert history items from the live database to the active archive database, and then delete the event entries and alert history from the live database.
Purge then Archive	Select to permanently delete event entries and alert history items from the live database based on the selected purge options, copy the event entries and alert history items from the live database to the active archive database and then delete the event entries and alert history items from the live database.

6 By default, selected event entries and alert history items older than 60 days are deleted.

7 Set options for the process, such as choosing to shrink the database, and include or exclude specific events. See Setting purge and archive options.

8 To change the default schedule, click **Update**, set the schedule, and click **OK**.

9 Click **OK**.

Managing the history log

You can refresh the event archive and purge history, export it, and/or clear it.

To export the history log

1. Select **Auditing & Alerting | Archiving & Purging**.
2. Click **History** in the top pane.
3. Select **History | Export**.
4. Select a destination for the .csv file.
5. Click **Save**.

To clear the history log

1. Select **Auditing & Alerting | Archiving & Purging**.
2. Click **History** in the top pane.
3. Select **History | Clear History**.
4. Click **Yes**.

Running database maintenance

Routinely run maintenance on the Active Administrator® database. Database Maintenance runs an SQL script that reorganizes and rebuilds indexes on the Active Administrator audit database. If an index is fragmented less than 30%, the process reorganizes the index; if an index is fragmented 30% or more, the process rebuilds the index.

To run database maintenance

1. Select **Auditing & Alerting | Archiving & Purging**.
2. Click **DB Maintenance**.
3. Click **Run Now**.

To schedule database maintenance

1. Select **Auditing & Alerting | Archiving & Purging**.
2. Click **DB Maintenance**.
3. By default, scheduling is enabled. To disable the schedule, clear the check box.
4. To change the schedule, click **Update, s**et the occurrence of the database maintenance, and click **OK**.
5. Click **Save**.

7

Group Policy

Quest® Active Administrator® provides unparalleled functionality in the area of Group Policy object management. Many familiar functions can be performed through the intuitive interface. Administrators can create, delete, and rename Group Policy objects, and add and remove links. Administrators also can copy a Group Policy object from one domain to another and explore the exact location on the network where the object is stored.

Topics

- Using the Group Policy landing page
- Managing Group Policy objects
- Managing GPOs by container
- Searching for GPO settings
- Managing GPO history
- Using the GPO repository
- Modeling GPO changes
- Managing GPO backups
- Troubleshooting
- Purging GPO history

Using the Group Policy landing page

The landing page displays the active tiles for each feature in the section. The active tiles automatically update every 30 minutes, but you can use the icons to refresh the tiles at any time. You also can pause and resume the refresh of data. To customize the active tile refresh, see Setting general user options.

To use the Group Policy landing page

1. Click **Group Policy**.
2. To access the features in this section, you can either click an active tile or choose from the tree.
   - **Group Policy Objects** (See Managing Group Policy objects.)
   - **GPO by Container** (See Managing GPOs by container.)
   - **GPO History** (See Managing GPO history.)
   - **GPO Repository** (See Using the GPO repository.)
   - **GPO Modeling** (See Modeling GPO changes.)
   - **GPO Backups** (See Managing GPO backups.)
   - **Troubleshooting** (See Troubleshooting.)
   - **Purge GPO history** (See Purging GPO history.)
   - **GPO Settings Search** (See Searching for GPO settings.)

Managing Group Policy objects

The Group Policy Objects page displays all the group policies for a selected domain controller. You can create new Group Policy objects or edit existing Group Policy objects. You can view details about the Group Policy object, manage links, and generate reports.

Topics

- Creating a new Group Policy object
- Copying Group Policy objects
- Copying Group Policy objects between domains
- Comparing Group Policy objects
- Reporting on Group Policy objects
- Managing links

To manage Group Policy object

1 Select **Group Policy | Group Policy Objects**.

2 Select a domain controller, if necessary.

> **NOTE:** Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3 Select a Group Policy to view details, security group filters, and Group Policy links.

You can sort the list of group policies alphabetically in ascending or descending order by clicking the Group Policies heading. You also can filter the list by typing in the **Filter Group Policies** box.

4 Use the tool bar to manage Group Policy objects. You also can right-click a GPO and select an option from the shortcut menu.

Table 75. Group policy objects tool bar

Option	Description
Refresh	Refresh the display.
Add	Create a new Group Policy object. See Creating a new Group Policy object.
Edit	Modify the selected Group Policy. **NOTE:** If you modify a GPO online and it is in use, changes you make may not be applied to the object using that GPO. To control the GPO change process, edit the GPO offline. Select the Group Policy, and select **More | Add to Repository**. See Using the GPO repository.
Properties	Open the properties for the selected Group Policy.
Delete	Delete a selected Group Policy.
More | Copy GPO	Copy a selected GPO. See Copying Group Policy objects.
More | Paste GPO	Paste a copied GPO. See Copying Group Policy objects.
More | Copy GPOs to Domain	Copy a selected GPO to a different domain. See Copying Group Policy objects between domains.
More | Add to Repository	Add the selected Group Policy to the repository. See Using the GPO repository.
More | Backup GPO	Back up the selected Group Policy. See Backing up Group Policy objects.
More | Rename GPO	Rename the selected Group Policy.

Table 75. Group policy objects tool bar

Option	Description
More | Compare	Compare two or more group policies to examine the differences. See Comparing Group Policy objects.
More | Explore	Locate a Group Policy object in Windows® Explorer.
Reports	Generate reports on selected group policies. See Reporting on Group Policy objects.
Links	Add, remove, and refresh Group Policy links. See Managing links.
Security Filters | Modify Security Filters	Modify the security for the selected Group Policy.
Security Filters | Account Properties	Modify the properties for the selected account in the **Security Group Filters** area.

Creating a new Group Policy object

To create a new Group Policy object

1. Select **Group Policy | Group Policy Objects**.
2. Select a domain controller.
3. Click **Add**.
4. Type a name for the GPO.

   NOTE: By default, the Group Policy Management Editor opens when you click **OK**. If you choose to clear the check box, you can edit the Group Policy at a later time by clicking **Edit**.

5. Click **OK**. The Group Policy Management Editor opens where you can add the Group Policy object settings.

Copying Group Policy objects

Instead of creating a new Group Policy object, you can copy an existing Group Policy object and then make modifications. To copy a Group Policy object to a different domain, see Copying Group Policy objects between domains.

To copy a Group Policy object to the same domain

1. Select **Group Policy | Group Policy Objects**.
2. Select a domain controller.
3. Select a Group Policy, and select **More | Copy GPO**.
4. Select **More | Paste GPO**.
5. Type a new name for the copied GPO.
6. Click **OK**.
7. Click **Refresh**, if necessary.
8. Select the Group Policy, and click **Edit**.
9. Make the necessary modifications.

Copying Group Policy objects between domains

One of the truly unique features of Active Administrator® is the ability to copy Group Policy objects between domains.

NOTE: Each GPO has a Globally Unique Identifier (GUID). If these are the same between domains, the current GPO is overwritten. The GUID displays in the details for the selected GPO.

To copy a Group Policy object to another domain

1. Select **Group Policy | Group Policy Objects**.
2. Select a domain controller.
3. Select a Group Policy.
4. Select **More | Copy GPOS to domain**.
5. To add additional GPOs to the list to be copied, click **Add GPO**, select a GPO, and click **OK**.
6. Click **Add Domain**.
7. Select the domain to receive the copy of the GPOs.
8. To copy security group filters, select the check box.
9. Click **OK**.

Comparing Group Policy objects

You can compare selected Group Policy objects to determine the differences. You can see what settings were changed, removed, or added.

To compare one or more group polices

1. Select **Group Policy | Group Policy Objects**.
2. Select a domain controller.
3. Select one or more group policies, and select
4. **More | Compare**.

   The **Summary** tab lists the source GPO and all the targets used in the comparison. Each target GPO is listed on a separate tab compared to the source GPO.

   To change the source GPO

   a. Click **Select Source GPO**.

   b. Click **Yes** to acknowledge that all comparisons will be removed.

   c. Select the new source GPO.

   d. Click **OK**.

   To add target GPOs

   a. Click **Add Target GPO**.

   b. Select one or more GPOs to compare to the source GPO.

   c. Click **Add**.

   d. Click **OK**.

   To remove a target GPO

a Open the Summary tab.

b Select a GPO.

c Click **Remove Target GPO**.

5 When the comparison process is complete, a full report displays with the differences color-coded. Use the tool bar to examine the data.

Table 76. GPO comparison tool bar

Option	Description
Next	Go to the next difference.
Previous	Go to the previous difference.
Show	Filter the display to show **All**, **Differences only**, **Changes only**, **Added only**, **Removed only**, or **Similarities only**.
Find	Type characters in the **Find** box and the cursor automatically goes to the first occurrence.
Next	Go to the next line.
Color Options	Change the colors on the display. Default colors are yellow for changed, green for added, and red for removed.
View Printable	View and print the comparison.
Save	Save the comparison as a compare file (*.compare).

6 Close the window to exit the comparison.

Reporting on Group Policy objects

Active Administrator can generate reports for administrators that provide relevant and useful information about Group Policy objects. The reports are available in a wide variety of formats and can be exported to popular formats for portability.

To run a report on a selected Group Policy objects

1 Select **Group Policy | Group Policy Objects**.

2 Select a domain controller.

3 Select a Group Policy, click **Reports**, and choose a report from the list.

Table 77. Group policy reports

Report	Description
Selected GPO Settings	Shows the Unique ID, number of revisions, created date, modified date, status of computer and user settings, Group Policy filters and Group Policy links for the selected Group Policy object in the selected domain.
Domain GPO Summary	Shows the Unique ID, number of revisions, created date, modified date, status of computer and user settings, Group Policy filters and Group Policy links for all Group Policy objects in the selected domain.
Selected GPO Affected Registry Keys	Shows the registry keys affected by the selected Group Policy object in the selected domain.

Managing links

The Group Policy tree indicates which GPOs are linked and which are not. If the GPO is linked, the number of links displays next to the GPO.

NOTE: You also can manage links in the GPO by Container module. See Managing linked GPOs.

Topics

- Adding a link

To manage links

1. Select **Group Policy | Group Policy Objects**.
2. Select a domain controller.
3. Select a Group Policy with links.
4. Use the **Links** menu to manage the Group Policy links.

Table 78. Links menu

Option	Description
Add Link	Add a link to the selected Group Policy. See Adding a link.
Remove Link	Remove selected Group Policy links.
Refresh Links	Refresh the Group Policy links.
Link Properties	Open the properties for the selected Group Policy link.
Change No Override	Toggle the value in the **No Override** column. By default, Group Policy Objects at a lower level can override policy set at a higher level (**No** displays in the **No Override** column). To prevent other Group Policy Objects at a lower level from overriding the policy set in a Group Policy Object, change the **No Override** value to **Yes**.
Change Disabled	Toggle the value in the **Disabled** column. By default, links are enabled (**No** displays in the **Disabled** column). If you want to disable the Group Policy Link from being applied to the selected container, change the **Disabled** value to **Yes**.

Adding a link

To link a Group Policy object to a container

1. Select **Group Policy | Group Policy Objects**.
2. Select a domain controller.
3. Select a Group Policy object, and select **Links | Add Link**.
4. Select the container to link to the Group Policy object.
5. Click **OK**.
6. Click **Refresh**, if necessary.

Managing GPOs by container

Active Administrator® includes the ability to view Group Policy objects (GPOs) by the containers to which they are linked, which allows administrators to quickly view and manage Group Policy objects for a specific container. After

locating a desired container object, applied GPOs are displayed, and a Resultant Set of Policies calculation can be provided immediately.

Topics

- Creating containers
- Linking Group Policy objects
- Blocking inheritance
- Managing linked GPOs
- Reporting on Group Policy objects

To manage GPOs by container

1 Select **Group Policy | GPO by Container**.

2 Select a domain controller.

> **NOTE:** Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3 Use the tool bar to manage GPOs.

Table 79. GPO by container tool bar

Option	Description
Refresh	Refresh the display.
New GPO	Create a new GPO. See Creating a new Group Policy object.
Link Existing	Link an existing GPO to a container. See Linking Group Policy objects.
New OU	Create a new container. See Creating containers.
Block	Block inheritance of GPOs from the parent. See Blocking inheritance.
Unblock	Unblock inheritance of GPOs from the parent. See Blocking inheritance.
Delete	Delete a selected container.
Properties	Open the properties for the selected container.
Links	Manage linked GPOs. See Managing linked GPOs.
Reports	Generate reports on selected containers. See Reporting on Group Policy objects.

Creating containers

To create a container

1 Select **Group Policy | GPO by Container**.

2 Select a domain controller.

3 Select a container in the tree, and click **New OU**.

4 Type the name of the organizational unit.

5 By default, the container is protected from accidental deletion. A warning message displays if a user attempts to delete the container. To remove the protection, clear the check box.

6 Click **OK**.

Linking Group Policy objects

There are two methods to link Group Policy objects. You can create a new Group Policy object to link to a selected container, or you can link an existing Group Policy object to a selected container.

To create and link a new Group Policy object

1. Select **Group Policy | GPO by Container**.
2. Select a domain controller.
3. Right-click a container, and choose **Create a GPO, and Link it here**.
4. Type a name for the GPO.
5. By default the Group Policy Object Editor opens when you click OK. If you do not want to edit the GPO at this time, clear the check box. To modify the GPO at a later time, see Managing Group Policy objects.
6. Click **OK**.

To link existing Group Policy objects

1. Select **Group Policy | GPO by Container**.
2. Select a domain controller.
3. Select a container, and click **Link Existing**.
4. Select a domain to view existing Group Policy objects.

   NOTE: If you do not see the domain you need, click **Add Forest**, type the forest name or browse to locate the name, select the account with access to the forest, and click **OK**.

5. Select a Group Policy object and click **Add**. Repeat for additional Group Policy objects.
6. Click **OK**.

Blocking inheritance

By default, child-level containers inherit GPOs from the parent container. You can link GPOs to a child container and block the inheritance from the parent.

The folder icon next to the container indicates if it is blocked ( ) or unblocked( ).

To block inheritance

1. Select **Group Policy | GPO by Container**.
2. Select a domain controller.
3. Select a container, and click **Block**.

To unblock inheritance

1. Select **Group Policy | GPO by Container**.
2. Select a domain controller.
3. Select a blocked container, and click **Unblock**.

Managing linked GPOs

Topics

- Comparing linked GPOs

To manage linked GPOs

1 Select **Group Policy | GPO by Container**.

2 Select a domain controller.

3 Select a container to view the current GPO links.

4 Use the **Links** menu to manage the linked GPOs.

Table 80. Links menu

Option	Description
Move GPO Link Up	Move the selected link up one position. Group Policy is applied based on the order the links display in the **Current GPO Links** area.
Move GPO Link Down	Move the selected link down one position. Group Policy is applied based on the order the links display in the **Current GPO Links** area.
Edit GPO	Open the **Group Policy Management Editor** for the linked GPO.
Explore GPO	Locate a linked GPO in Windows® Explorer.
Compare	Compare multiple GPOs side-by-side with differences color-coded. See Comparing linked GPOs.
Change No Override	Toggle the value in the **No Override** column. By default, Group Policy objects at a lower level can override policy set at a higher level (**No** displays in the **No Override** column). To prevent other Group Policy objects at a lower level from overriding the policy set in a Group Policy object, change the **No Override** value to **Yes**.
Change Disabled	Toggle the value in the **Disabled** column. By default, links are enabled (**No** displays in the **Disabled** column). If you want to disable the Group Policy link from being applied to the selected container, change the **Disabled** value to **Yes**.
Remove Link(s)	Remove selected GPO links.
Linked Container Properties	Open the properties for the container linked to the selected GPO.

Comparing linked GPOs

You can compare Group Policies being used in production, or compare those in production against Group Policies in the offline Group Policy repository.

To compare multiple linked GPOs

1 Select **Group Policy | GPO by Container**.

2 Select a domain controller.

3 Select a container to view the current linked GPOs.

4 Select a linked GPO that you want to compare to other GPOs, and select **Links | Compare**.

You also can select multiple linked GPOs. The first selected GPO is used as the source GPO. Each subsequent linked GPO is considered a target GPO.

The **Summary** tab lists the source GPO and all the targets used in the comparison. Each target GPO is listed on a separate tab compared to the source GPO.

For more information on the comparison results, see Comparing Group Policy objects.

Reporting on Group Policy objects

To report on Group Policy objects

1. Select **Group Policy | GPO by Container**.
2. Select a container with GPO Links.
3. Click **Reports** and select a report.

Table 81. GPO by container reports

Report	Description
Report Container GPO Links	Shows the Group Policy links and their settings for the selected container.
Selected GPO Settings	Shows the unique ID, number of revisions, created date, modified date, status of computer and user settings, Group Policy filters and Group Policy links for the selected Group Policy object in the selected domain.
Selected GPO Affected Registry Keys	Shows the registry keys affected by the selected Group Policy object in the selected domain.

Searching for GPO settings

To help you manage GPOs in your domains, you can search for specific GPO settings to verify the correctness of the setting or to check for changes that may have been made. You can search for settings in the Live GPO, in the repository, in GPO history, and in GPO backups.

To search for GPO settings

1. Select **Group Policy | GPO Settings Search**.
2. Select the GPO setting on which to search.
3. If available, select the specific parameter on which to search. Not every GPO setting has specific parameters.
4. Select the area in which to search. You can search for settings in the Live GPO, in the repository, in GPO history, and in GPO backups.
5. If you do not see the domain you need, click **Add Domain**, select the domain, and click **OK**.
6. Click **Search**.

Managing GPO history

History is kept for all Group Policy objects (GPOs) in your domains. The Group Policy history service automatically checks for changes and saves the changes to a file share on your network. The default folder created during installation is GPOHistory.

In GPO history, you can see exactly who made changes to the group policies and what they changed. If you do not like a change that someone made, you can roll back to a previous version of the GPO.

Topics

- Rolling back Group Policy

To manage GPO history

1 Select **Group Policy | GPO History**.

2 Select a domain controller.

3 Select a Group Policy.

The right pane displays the history versions, which are ordered by date of when the changes were made. You can view the revisions of the GPO, who made the changes, and on which domain controller the change was made.

4 Use the tool bar to manage the GPO history.

Table 82. GPO history tool bar

Option	Description
Refresh	Refresh the Group Policy History list.
Edit GPO	Open the Group Policy Management Editor for the linked GPO.
Edit Comments	View basic information about a GPO history item, and add or edit comments.
Remove	Remove the selected GPO history item.
Remove GPO	Remove the selected GPO.
Roll Back	Rollback the GPO to the selected GPO history item. See Rolling back Group Policy.
More | GPO Settings	View detailed settings of the selected GPO history item.
More | Show Changes	View changes made to a selected GPO history item. You can export the report to a PDF, HTML, MHT, RTF, Excel, CSV, Text, or Image file.

Rolling back Group Policy

If you notice changes that were not supposed to occur, you can roll back to a previous version of the Group Policy object (GPO). Rolling back causes the GPO to be set back in time to the exact settings as they were at a previous date.

To roll back Group Policy

1 Click **Group Policy | GPO History**.

2 Select a domain controller.

3 Select the GPO to roll back.

- To filter the list, start typing in the **Filter Group Policies** box.
- To make changes to the GPO, click **Edit GPO**.

4 In the right pane, select a version to roll back to, and click **Roll Back**.

5 Select if you want to roll back the **GPO Security Filters** and/or **GPO Links.**

6 Type a reason and comment to explain the rollback for auditing purposes, and then click **OK**.

7 Click **Yes**.

NOTE: If the default domain policy is included in the version, a warning message displays. To overwrite the default, click **Yes**.

Upon completion of the rollback, the list of GPO revisions increase by one to ensure that the GPO is applied the next time polices are refreshed.

Using the GPO repository

Active Administrator® provides an offline repository for editing Group Polices. The offline repository makes a copy of the Group Policy object (GPO) that you can edit without interfering with the normal operation of Active Directory®. When editing is complete, you can publish the changed GPO to Active Directory in a single operation.

The offline repository uses a system of checking in and out to maintain the integrity of the GPOs in the repository. When a GPO is added to the repository, it is actually a copy of the GPO that gets added; the actual GPO is not affected. The copy in the repository can then be checked out and changed, and then checked in and applied when needed. When a GPO is published from the repository, a copy of the GPO is then copied over the online GPO, thus effectively making any changes to that GPO live.

Topics

- Adding a GPO to the repository
- Editing a GPO offline

To use the GPO repository

1 Select **Group Policy | GPO Repository**.

2 Select a domain.

> **NOTE:** If you do not see a domain listed, you must first add a copy of the Active Directory GPO to the repository. See Adding a GPO to the repository.

Group policy objects that in the repository display in the upper pane. These GPOs are copies of the GPOs in Active Directory. You can edit these GPOs without affecting the live GPOs.

The bottom pane displays the check in/out history for the selected GPO. To view the history of publishing the GPO to Active Directory, click **Publish to Active Directory History**.

3 Use the options on the tool bar to edit Group Policy objects offline.

Table 83. GPO repository tool bar

Option	Description
Refresh	Refresh the **GPO's in Offline Repository** list.
Publish	Write over the GPO in Active Directory with the selected GPO in the offline repository. See Editing a GPO offline.
Add	Add a copy of the Active Directory GPO to the repository. See Adding a GPO to the repository.
Remove	Remove the selected GPOs from the repository. **NOTE:** Removing a GPO from the repository does not remove the GPO from the system. The GPO in the repository is a read-only copy of the GPO that resides in Active Directory.
Edit GPO	Edit a checked-out offline GPO. See Editing a GPO offline.
Check In/Out	Check out a GPO for offline editing. When you are finished editing, check the GPO back into the repository. See Editing a GPO offline.
More | Offline GPO Settings	Show the unique id, number of revisions, created date, modified date, status of computer and user settings, Group Policy filters and Group Policy links for the selected Group Policy object in the selected domain.
More | Compare Offline GPO to Live GPO	Prior to publishing an offline GPO to Active Directory, you can compare the offline GPO to the live GPO. See Comparing Group Policy objects.

Adding a GPO to the repository

During installation, Active Administrator® creates the GPORepository folder, which is located in the Active Administrator folder. When you check in a GPO into the repository, a copy of the GPO is placed in this folder. All changes you make to the GPO are stored in this folder until you choose to publish the GPO or discard the changes.

NOTE: You also can select **Group Policy | Group Policy Objects**, select a Group Policy object, and select **More | Add to Repository**. See Managing Group Policy objects.

To add a GPO to the repository

1. Select **Group Policy | GPO Repository**.
2. Click **Add**.
3. Select a domain.

   If you do not see the desired domain, click **Add Forest** and locate the forest with the desired domain.
4. Select a Group Policy, and click **Add**.
5. Repeat for additional group policies.
6. Click **OK**.
7. Click **Refresh**, if necessary.

   When the checkout is complete, you can edit the GPO offline. See Editing a GPO offline.

Editing a GPO offline

Once GPO is in the repository, you can check it out for editing offline. When you are done editing offline, check the GPO in, and publish it to Active Directory®.

To edit a GPO offline

1. Select **Group Policy | GPO Repository**.
2. Select a domain.
3. Select a GPO, and select **Check In/Out | Check Out**.
4. Select the checked out GPO, and click **Edit GPO**.
5. Modify the GPO in the Group Policy Management Editor, and then close the window.

   NOTE: To cancel the checkout without applying the changes, select the GPO, and then select **Check In/Out | Check In (discard)**.
6. To check in the selected GPO, select **Check In/Out | Check In**.
7. Type a comment that describes the changes you made to the GPO.
8. Click **Check In**.

   The GPO is read-only in the repository. The change is not applied to the live GPO until you publish it to Active Directory.

   NOTE: Before publishing the GPO, you may want to compare the settings of the GPO in the repository to those in Active Directory by running the **Compare Offline GPO to Live GPO** report.
9. To publish the edited GPO to Active Directory, select the GPO, and click **Publish**.

Modeling GPO changes

Active Administrator® provides increased levels of manageability by way of GPO modeling, which allows you to select a user and computer and view or report on the Group Policy objects that affect those accounts. To get an exact picture of how your actions will affect Group Policy application, you can perform several calculations of what if scenarios, including the addition or removal of these objects from OUs, sites, or security groups, which allows you to quickly view Group Policy object application and errors on remote computers. Recent calculations are automatically saved for easy retrieval at a later time.

Reporting on GPO Modeling allow administrators to see exactly how objects are affected by Group Policy objects and to quickly troubleshoot where application of Group Policies were not handled correctly. Active Administrator provides clear and concise reports that not only show what Group Policy objects are applied, but the effective settings of such policies.

Topics

- Creating a simulation

To model GPO changes

1 Select **Group Policy | GPO Modeling**.

Existing simulations display in a list. You can sort each column in ascending or descending order by clicking on the column heading.

2 Use the tool bar to manage GPO modeling simulations.

Table 84. GPO modeling tool bar

Option	Description
Refresh	Refresh the display.
New	Create and run a new simulation. See Creating a simulation.
Run Again	Run a selected simulation.
Copy Simulation	Copy a selected simulation to make changes to create a new simulation. See Creating a simulation.
View Report	View the report for the selected simulation.
Save Report	Save the selected simulation report to an HTML file.
Delete	Delete selected simulations.

Creating a simulation

To create a simulation

1 Select **Group Policy | GPO Modeling**.

2 Click **New**.

NOTE: You also can select an existing simulation, and click **Copy Simulation** to create a new simulation by making minor changes.

3 On the **Welcome** page, click **Next**.

4 Browse to select a domain.

5 Browse to select a domain controller.

6 Choose a site for the simulation from the list.

7 Click **Next**.

8 Select the simulation.

NOTE: The user or computer does not have to be a direct member of a listed group. If the user or computer belongs to a group that is a member of another group, that user or computer is a member of the parent group as well and is listed.

NOTE: To reload the list of OUs, click **Refresh**. All selections are cleared and any newly added OUs appear in the list.

- To simulate user policy settings, choose either user or container, and browse to find the user or container.
- To simulate computer policy settings, choose either computer or container, and browse to find the computer or container.

9 Select to simulate slow network connection, if desired.

10 Select to perform loop-back process if desired. Choose to merge or replace.

11 Click **Next**.

12 Optionally, browse to locate the network location to simulate the policy settings for users or computers.

13 Click **Next**.

14 Select group memberships.

The everyone and authenticated users groups are automatically added to the simulation and cannot be removed. You can add additional groups to simulate group membership changes.

15 Optionally, click **Add** for user or computer security groups, select groups, and click **OK**.

16 Click **Next**.

17 Click **Finish.**

The simulation displays in a report.

- To print the simulation report, right-click in the window and choose **Print**.

18 Close the report window.

- To view the report again, select the simulation, and click **View Report**.
- To save a selected simulation to an HTML file, click **Save Report**.
- To run a selected simulation again, click **Run Again**.
- To delete a selected simulation, click **Delete**.

Managing GPO backups

Another feature unique to Active Administrator® is the ability to back up an entire Group Policy object (GPO) to a folder structure from where it can be restored if needed. This feature provides a high level of fault tolerance and recoverability that was never before possible with any other tool.

Topics

- Backing up Group Policy objects
- Scheduling a GPO backup
- Scheduling a purge of GPO backups
- Comparing Group Policy backups
- Restoring a Group Policy object

To manage GPO backups

1 Select **Group Policy | GPO Backup**.

2 Use the tool bar to manage GPO backups.

Table 85. GPO backup tool bar

Option	Description
Refresh	Refresh the display.
Backup Group Policy	Back up group policies. See Backing up Group Policy objects.
Restore Group Policy	Restore selected group policies. See Restoring a Group Policy object.
Remove	Delete a selected backup.
Show Settings	Display a selected backed up Group Policy in a report. To print the report, right-click in the window, and choose **Print**.
Compare	Compare two or more selected Group Policy backups. See Comparing Group Policy backups.
Schedule	Schedule a GPO backup. See Scheduling a GPO backup,
Schedule Purge	Schedule a purge of GPO backups. See .

Backing up Group Policy objects

Back up your Group Policy objects before making any changes. You can restore the backup if a problem arises. You also can create a schedule to back up all the GPOs in selected domains. See Scheduling a GPO backup.

To back up Group Policy objects

1 Select **Group Policy | GPO Backup**.

2 Click **Backup Group Policy**.

3 Click **Add GPOs**.

4 Select a domain.

5 If you do not see the desired domain, click **Add Forest** and locate the forest with the desired domain.

6 Select the Group Policy to back up, and click **Add**.

7 Repeat for additional group policies in the selected domain.

8 Click **OK**.

9 Select the Group Policy, and click **Backup**.

Scheduling a GPO backup

You can create a schedule to back up all the GPOs in selected domains.

To schedule a GPO backup

1 Select **Group Policy | GPO Backup**.

2 Click **Schedule**.

3 To enable scheduling, select the check box.

4 To create the schedule, click **Set Schedule**, select the schedule type, and click **OK**.

5 To add domains to the backup schedule, click **Add**, select the domains, and click **OK**.

NOTE: All the GPOs in the domain are backed up.

6 Click **OK**.

Scheduling a purge of GPO backups

You can create a schedule to purge GPO backups older than N days.

To schedule a purge of GPO backups

1 Select **Group Policy | GPO Backup | Schedule Purge**.

2 Optionally, select **Enable scheduling for purging GPO backups**.

3 Enter the number of days of backups to keep.

4 Optionally, click **Update** to make changes to the default schedule.

5 Select the schedule type, set the related date and time for the schedule, and click **OK**.

6 Click **Save**.

Comparing Group Policy backups

To compare two or more GPO backups

1 Select **Group Policy | GPO Backup**.

2 Select two or more backups.

3 Click **Compare**.

4 When the comparison process is complete, a full report displays with the differences color-coded. Use the tool bar to examine the data.

Table 86. GPO comparison tool bar

Option	Description
Next	Go to the next difference.
Previous	Go to the previous difference.
Show	Filter the display to show **All**, **Differences only**, **Changes only**, **Added only**, **Removed only**, or **Similarities only**.
Find	Type characters in the Find box and the cursor automatically goes to the first occurrence.
Next	Go to the next line.
Color Options	Change the colors on the display. Default colors are Yellow for Changed, Green for Added, and Red for Removed.
View Printable	View and print the comparison.
Save	Save the comparison as a Compare file (*.compare).

Restoring a Group Policy object

With Active Administrator, you can easily restore backed up GPOs to repair damaged GPOs or those that were accidentally deleted.

To restore a selected Group Policy object

1. Select **Group Policy | GPO Backup**.
2. Click **Restore Group Policy**.
3. Select the Group Policy backup to restore.
4. To restore the backup to a different domain:
    a. Select **Restore to Domain**.
    b. Click **Add Domain**.
    c. Select the domain.
    d. Click **OK**.
5. Select to restore links, if available.
6. Click **OK**.

Troubleshooting

Active Administrator® includes the ability to view event log entries on Windows® 2000 and later client computers so administrators can quickly view Group Policy object application and errors on remote computers. The Client-side Troubleshooting page provides several options to make management easier.

Topics

- Enabling logging
- Updating Group Policy

To troubleshoot Group Policy

1. Select **Group Policy | Troubleshooting**.
2. Type a computer name, or browse to locate a computer.
3. Click **Retrieve Events**.
4. Use the tool bar to set up logging and update group policies.

Table 87. Client-side troubleshooting tool bar

Option	Description
Refresh Events	Refresh the list of events log entries.
Apply Changes	Apply changes to the logging settings. See Enabling logging.
Update Group Policies	Update group policies. You can choose to force an update even if no changes were made. See Updating Group Policy.
View Logs	View the contents of the user config log or the software deployment log. See Enabling logging.

Enabling logging

By default, no logging is enabled. Be aware that selecting any logging option can cause an increase in disk usage as the log files grow.

To enable logging for troubleshooting

1. Select **Group Policy | Troubleshooting**.

2 Type a computer name, or browse to locate a computer.

3 Click **Retrieve Events**.

All Group Policy Events for the selected computer display. To refresh the Group Policy events list, click **Refresh Events**.

4 Set Group Policy logging options. By default, no logging is enabled.

Table 88. Group policy logging options

Option	Description
Generate GP events to the Application Event Log	Select **Detailed** to enable detailed Group Policy logging to the Windows® application log. **NOTE:** Enabling Group Policy logging slows down the logon process and affects the rate at which the application log will grow.
Generate logging relating to Software Deployment Group Policies	Select **Verbose** to enable logging of the Group Policy Application Deployment process. **NOTE:** Enabling Group Policy software deployment logging slows down the logon process and generates a log file that records the steps of the Group Policy application deployment component. • To start logging, reboot the computer after applying the changes or have the user log off and then back on. • To view the Appmgmt.log file, select **View Logs | Software Deployment Log**.
Generate logging for Group Policies relating to User Configuration	By default, Active Administrator® generates a troubleshooting file. To enable detailed logging, select **Verbose Logging** from the **Level** list. **NOTE:** Verbose logging significantly increases the size of the UserEnv.log file on the target computer. • To view the UserEnv.log file, select **View Logs | User Config Log**.

5 Click **Apply Changes**.

Updating Group Policy

To update Group Policy

1 Select **Group Policy | Troubleshooting**.

2 Type a computer name, or browse to locate a computer.

3 Click **Retrieve Events**.

4 From the tool bar, select the option for updating group policies.

- To apply Group Policy settings whether they have changed or not, select **Force Update**.
- To apply only changed Group Policy settings, select **Do Not Force Update**.

5 Click **Update Group Policies**.

Purging GPO history

You can purge GPO history on demand or schedule a GPO history purge.

Topics

- Purging GPO history on demand
- Scheduling a GPO history purge

To purge GPO history

1 Select **Group Policy | Purge GPO History**.

The top pane displays the GPO history. To view details about a selected GPO history item, hover the cursor over .

The bottom pane displays the maintenance tasks specific to the Purge GPO History feature. See Managing tasks.

2 Use the options on the tool bar to manage purging and archiving.

Table 89. Purge GPO history tool bar

Option	Description
Purge Now	Purge Group Policy history from the live audit database. See Purging GPO history on demand.
Schedule	Schedule a Group Policy history purge. See Scheduling a GPO history purge.
Refresh	Refresh the display.
Export History	Save the Group Policy history to a .csv file.
Clear History	Clear the Group Policy history.
Tasks	Refresh the task display, view task properties, send a task to email recipients, and group the task display by status. See Managing tasks.

Purging GPO history on demand

Deletes Group Policy history items permanently from the live audit database based on the selected purge options. To schedule the purge process, see Scheduling a GPO history purge.

To purge GPO history

1 Select **Group Policy | Purge GPO History**.

2 Click **Purge Now**.

3 By default, only the last 90 days of group history items are kept. To change the value, type in the box.

4 Click **Purge Now**.

Scheduling a GPO history purge

To schedule a GPO history purge

1 Select **Group Policy | Purge GPO History**.

2 Click **Schedule**.

3 By default, scheduling is enabled. You can create a schedule and then disable it until you need it.

4 By default, only the last 90 days of group history items are kept. To change the value, type in the box.

5 To change the default schedule, click **Update**, set the schedule, and click **OK**.

6 Click **Save**.

8

Active Directory Recovery

Active Directory Recovery provides the ability to recover deleted Active Directory® objects and properties, as well as to manage Active Directory backup retention. The preview and compare functions allow administrators to preview the object before it is restored or compare the attributes of the selected object in the archive with those of the same object in the Active Directory.

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

Topics

- Using the Active Directory Recovery landing page
- Managing Active Directory backups
- Restoring from a backup
- Purging Active Directory backups

Using the Active Directory Recovery landing page

The landing page displays the active tiles for each feature in the section. The active tiles automatically update every 30 minutes, but you can use the icons to refresh the tiles at any time. You also can pause and resume the refresh of data. To customize the active tile refresh, see Setting general user options.

To use the Active Directory Recovery landing page

1. Click **Recovery**.
2. To access the features in this section, click an active tile or choose from the tree.
   - **Recovery** (see Managing Active Directory backups)
   - **Purge backups** (see Purging Active Directory backups)

Managing Active Directory backups

To manage Active Directory® backups

1. Select **Recovery | Object Recovery**.
2. Use the tool bar to manage the backup files.

Table 90. Object Recovery tool bar

Option	Description
Domain	Select a single domain or all domains to help manage the list of backup files.
Refresh	Refresh the display.
Backup Now	Back up Active Directory. You also can schedule backups. See Setting recovery options.
Restore	Restore selected objects and attributes from a backup file. See Restoring from a backup.
Delete	Delete a selected backup file.
View Log	View the log for a selected backup file. You can filter the contents and clear the log.

Restoring from a backup

A wizard guides you through selecting objects and attributes to restore from a selected backup file. You also can set options for restoring a user password.

IMPORTANT: If Password Recovery was disabled when the backup occurred, passwords were not backed up. If you restore a backup that does not contain passwords, you must dis-join and then rejoin computer accounts. To see if Password Recovery is enabled, select **Configuration | Recovery Settings**. See Setting recovery options.

To restore from a backup file

1. Select **Recovery | Object Recovery**.
2. Select a backup file, and click **Restore**.

   TIP: To narrow the list of backup files, you can select a single domain from the **Domain** list.
3. On the Welcome page, click **Next**.
4. Locate the objects to restore using one of these methods:
   - To use the search feature to find the objects, click **Find**.
   - To browse through the backup file to locate the objects, click **Browse**.
5. Select an object, and click **Compare**.

   Before restoring an archived object, you might want to compare the attributes with those of the same object in the Active Directory®.
6. To filter the list, select which attributes to display.

   Table 91. Filter options

Option	Description
Only attributes that differ	Select to show only the attributes whose values are different in the backup file and Active Directory.
Only attributes that are the same	Select to show only the attributes whose values are the same in the backup file and Active Directory.
Show all attributes	Select to show all the attributes in the backup file and Active Directory.
7. Click **Refresh**.
8. After examining the comparison, click **Close**.
9. Click **Next**.

10 Select the attributes to restore.

Table 92. Restore options for attributes

Option	Description
Restore all attributes	By default, all attributes for the specified object are restored.
Restore only security attributes	Select to restore only security attributes.
Restore only these attributes	Select to restore only the attributes selected in the list.

11 Click **Next**.

12 Browse to select the domain controller to restore to, if necessary.

13 Select how to restore the attributes.

Table 93. Restore options for attributes

Option	Description
Only	By default, only the specified attributes for the selected object are restored.
And all objects it contains	Select to restore the specified attributes for objects contained by the selected object.
And all objects it contains of this type	Select to restore the specified attributes for objects of the selected type contained by the selected object. Select a type from the list.
Only recover deleted objects	Select to restore only objects that are in the backup file, but not the live database.

14 Click **Next**.

When restoring a user that was deleted previously, you can enter a new password and require them to reset the password when they first log on.

IMPORTANT: If Password Recovery was disabled when the backup occurred, passwords were not backed up. If you restore a backup that does not contain passwords, you must dis-join and then rejoin computer accounts.

15 Set the options for restoring passwords.

Table 94. Restore options for passwords

Option	Description
Recover passwords from Active Directory	By default, passwords are restored. Password Recovery must be enabled when the backup occurs for passwords to be restored. See Setting recovery options. **NOTE:** If selected, the Force change password at next logon check box is selected automatically and cannot be changed. Users must change their password the next time they logon.
Use this password for all undeleted user objects	Select to assign the same password to all undeleted user objects. Type a password in the Password and Confirm Password boxes.
Generate random passwords for undeleted user objects	Select to let Active Administrator® generate passwords. Browse to create a text file in which to record the passwords that are generated. You can change the minimum and maximum number of characters in the password. Each password has at least one lower-case character, one upper-case character, and one numeric character.
Force change password at next logon	Requires the user to change their password once they log on with the password you specified here (default). **NOTE:** This check box is selected and disabled automatically if the **Recover passwords from Active Directory** check box is selected.

16 Click **Next**.

17 Review the settings.

- To check the object before you start the restore process, click **Preview**.
- To save the preview to a .txt file, click **Save**.

18 To start the recovery, click **Next**.

19 Click **Finish**.

Purging Active Directory backups

You can purge Active Directory® backups on demand or schedule a backup purge.

Topics

- Purging Active Directory backups on demand
- Scheduling an Active Directory backup purge

To purge Active Directory backups

1 Select **Recovery | Purge Backups**.

The top pane displays the history of purging Active Directory backups. To view details about a selected Active Directory backup purge history item, hover the cursor over .

The bottom pane displays the maintenance tasks specific to purging Active Directory backups.

2 Use the options on the tool bar to manage Active Directory backup history.

Table 95. Purging Active Directory backups tool bar

Option	Description
Purge Now	Purge backup files from the live audit database. See Purging Active Directory backups on demand.
Schedule	Schedule the purge process. See Scheduling an Active Directory backup purge.
Refresh	Refresh the display.
Export History	Export the backup purge history to a .csv file.
Clear History	Clear the backup purge history.
Tasks	Refresh the tasks list, view task properties, send a selected task to email recipients, and group the list of tasks by status. See Managing tasks.

Purging Active Directory backups on demand

Deletes backups permanently from the live audit database based on the selected purge options.

NOTE: To schedule the purge process, see Scheduling an Active Directory backup purge.

To purge Active Directory® backups

Deletes backups permanently from the live audit database based on the selected purge options.

1 Select **Recovery | Purge Backups**.

2 Click **Purge Now**.

3 Type a date or select a date from the calendar.

4 Click **Purge Now**.

Scheduling an Active Directory backup purge

To schedule an Active Directory® backup purge

1 Select **Recovery | Purge Backups**.

2 Click **Schedule**.

3 By default, scheduling is enabled. You can create a schedule and then disable it until you need it.

4 Active Administrator® keeps 90 days of backups in the Active Administrator share. To change the value, type a number in the box.

5 Type a description of the schedule.

6 To change the default schedule, click **Update**.

7 Set the schedule.

8 Click **OK**.

9 Click **Save**.

9

Active Directory Infrastructure

The Active Directory Infrastructure module enables you to manage Active Directory® sites, subnets, site links, replication, and global catalog servers.

Topics

- Using the Active Directory Infrastructure landing page
- Managing Active Directory sites
- Monitoring replication
- Using the replication analyzer
- Managing Active Directory trusts

Using the Active Directory Infrastructure landing page

The landing page displays the active tiles for each feature in the section. The active tiles automatically update every 30 minutes, but you can use the icons to refresh the tiles at any time. You also can pause and resume the refresh of data. To customize the active tile refresh, see Setting general user options.

To use the Active Directory Infrastructure landing page

1. Click **Active Directory Infrastructure**.
2. To access the features in this section, click an active tile or choose from the tree.
    - Active Directory Sites (see Managing Active Directory sites)
    - Trusted Domains (see Managing Active Directory trusts)
    - Replication Monitoring (see Monitoring replication)

Managing Active Directory sites

Topics

- Browsing Active Directory
- Building Active Directory structure
- Reporting on Active Directory

To manage Active Directory® sites

1. Select **Active Directory Infrastructure | Active Directory Sites**.

2 Select a domain controller.

> **NOTE:** Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3 Use the tool bar to manage Active Directory objects.

The options on the tool bar vary depending on the selected Active Directory object.

Table 96. Active Directory sites tool bar

Option	Description
Refresh All	Refresh all objects and connections.
Refresh Selected	Refresh selected objects and connections.
New	Create new Active Directory objects: sites, connections, site links, and site link bridges. See Building Active Directory structure.
Edit	Open the editor for the selected Active Directory object. Modify the replication schedule for connections and site links.
Move	Move the selected server to a different site.
Replicate Connections	Replicate the connections for the selected server.
Reports	Run a report on a selected Active Directory object. See Reporting on Active Directory.
Transports	Select the type of transports for the forest. You can bridge all IP and/or SMTP site links and ignore schedules for IP and/or SMTP.
Replication Analyzer	Open the Replication Analyzer. See Using the replication analyzer.

Browsing Active Directory

When you first open Active Directory Sites, the **Forest Details** page displays for the selected domain controller. You can change the view to subnets or site links by clicking the links in the upper-right corner of the window.

To browse Active Directory

1 Select **Active Directory Infrastructure | Active Directory Sites**.

2 Select a domain controller.

> **NOTE:** Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3 Select a forest or site.

4 Select the information to display:

- To view details about the selected forest, click **Forest Details**.
- To view servers for the selected site, click **Servers**.
- To view subnets for the selected forest or site, click **Subnets**.
- To view site links for the selected forest or site, click **Site Links**.

Building Active Directory structure

You can use Active Administrator® to add new Active Directory® objects, such as sites, connections, subnets, site links, and site link bridges.

Topics

- Adding a new site
- Adding a new connection
- Adding a new subnet
- Adding a new site link
- Adding a new site link bridge

Adding a new site

To add a new site

1. **Select Active Directory Infrastructure | Active Directory Sites**.
2. Select a domain controller.

   NOTE: Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3. Select a forest, and select **New | New site**.
4. On the **Welcome** page, click **Next**.
5. Type a name and description for the new site.
6. Click **Next**.
7. Select the subnets for the new site. If you do not see the subnet you need, click **Add Subnets**. See Adding a new subnet.
8. Click **Next**.
9. Select site links. If you do not see the site link you need, click **Add Site Link**. See Adding a new site link.
10. Click **Next**.
11. Click **Finish**.
12. Click **Finish**.

Adding a new connection

To add a new connection

1. Select **Active Directory Infrastructure | Active Directory Sites**.
2. Select a domain controller.

   NOTE: Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3. Select a forest.
4. Select a site.
5. Select the server to replicate to, and select **New | New Connection.**
6. Type a name and description for the new connection.
7. Browse to select a server to replicate from.
8. To replicate now, click **Replicate Now**.

   -OR-

   To schedule a replication, click **Change Replication Schedule**.

a Select the days and times to run replications using one of these methods:

- Click a time across the top row to select that time for every day of the week.
- Click a day in the left list to select all times for that day.
- Click and drag to select blocks of time for blocks of days.

b Select to enable or disable replication.

- To enable replication for the selected days and times, select **Replication Available**.
- To clear replication for the selected days and times, select **Replication Not Available**.

c Click **OK**.

9 Click **OK**.

Adding a new subnet

To add a new subnet

1 Select **Active Directory Infrastructure | Active Directory Sites**.

2 Select a domain controller.

> **NOTE:** Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3 Select a forest or site, and select **New | New Subnet**.

4 Type the name of the new subnet.

Enter the address prefix using network prefix notation (address/prefix length), where the prefix length indicates the number of fixed bits. You can enter either an IPv4 or an IPv6 subnet prefix.

IPv4 example: 157.54.208.0/24

IPv6 example: 3FFE:FFFF:0:C000::/64

5 Type a description.

6 Click **OK**.

Adding a new site link

To add a new site link

1 Select **Active Directory Infrastructure | Active Directory Sites**.

2 Select a domain controller.

> **NOTE:** Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3 Select a forest or site, and select **New | New Site Link**.

4 Type a name and description for the new site link.

5 Choose the transport type from the list.

6 Set the cost.

7 Set the replication frequency.

8 To schedule a replication, click **Change Replication Schedule**.

a Select the days and times to run replications using one of these methods:

- Click a time across the top row to select that time for every day of the week.

- Click a day in the left list to select all times for that day.
- Click and drag to select blocks of time for blocks of days.

b Select to enable or disable replication.

- To enable replication for the selected days and times, select **Replication Available**.
- To clear replication for the selected days and times, select **Replication Not Available**.

c Click **OK**.

9 Select sites from the list.

10 Click **OK**.

Adding a new site link bridge

To add a new site link bridge

1 Select **Active Directory Infrastructure | Active Directory Sites**.

2 Select a domain controller.

> **NOTE:** Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3 Select a forest or site, and select **New | New Site Link Bridge**.

4 Type a name and description for the new site link bridge.

5 Choose the transport type from the list.

6 Select a site link from the list.

7 Click **OK**.

Reporting on Active Directory

The type of report available varies depending on the type of object selected. You can save, print, export, or email a report.

To build a report

1 Select **Active Directory Infrastructure | Active Directory Sites**.

2 Select a domain controller.

> **NOTE:** Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3 Select the Active Directory® object to report on, click **Reports**, and choose the report to build.

Table 97. Active Directory report types

Report	Forest	Site	Subnet	Site Link	Server
Build Forest Report	X	X	X	X	X
Build Site Report		X	X	X	X
Build Subnet Report	X				
Build Site Links Report	X				
Build Global Catalogs Report	X				
Build Server Report					X

Monitoring replication

You can monitor replication on servers in a selected forest.

NOTE: You can create replication schedules when you create connections and site links. To change the schedule, edit the connection or site link. See Adding a new connection and Adding a new site link.

Topics

- Adding a forest

To monitor replication

1. Select **Active Directory Infrastructure | Replication Monitoring**.
2. Replication monitoring is enabled by default. You can disable replication monitoring for all listed forests or you can disable replication monitoring for a single forest.
    - To disable a single forest, select the forest, click **Edit**, and clear the check box.
3. By default, the Active Directory® replication is tested every 30 minutes. To change the value, use the arrow keys.

    NOTE: To be notified of the replication test results, create an Active Administrator alert that includes the **Active Directory Replication Test Succeeded** and **Active Directory Replication Test Failed** events. See Creating an alert.
4. Use the tool bar to manage replication monitoring.

Table 98. Replication monitoring tool bar

Option	Description
Refresh	Refresh the display.
Check Now	Run a replication test.
Save	Save changes to replication monitoring.
Add Forest	Add a forest to the list for replication monitoring.
Edit Forest	Edit a selected forest to disable monitoring or to change the account.
Delete Forest	Delete a forest from the list.
Replication Details	View details of a selected replication.

Adding a forest

To add a forest to replication monitoring

1. Select **Active Directory Infrastructure | Replication Monitoring**.
2. Click **Add Forest**.
3. By default, replication monitoring is enabled. To disable replication monitoring for the forest, clear the check box.
4. Browse to select a forest.
5. Select to use either the Active Administrator® Foundation Server (AFS) service account or a different account. If you chose a different account, enter the user name and password.
6. In the **Excluded domain controllers** area, expand domains, and select the domain controllers to exclude.

    NOTE: To filter the list of domain controllers, start typing in the **Filter** box.

    NOTE: If you changed the account, click **Refresh** to load the list of domain controllers.

7 Optionally, type the name of a domain controller to exclude in the **Enter domain controller name if you don't see it in the list** text box and click **Add**.

8 Click **Validate** to verify the account.

9 Click **OK**.

Using the replication analyzer

Before you replicate Active Directory® for an entire forest, site, or single domain controller, you can test the replication to check for any errors. You also can monitor the replication as it progresses.

To run a replication

1 Select **Active Directory Infrastructure | Replication Analyzer**.

2 Select a domain controller.

> **NOTE:** Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3 Set options for the replication analyzer.

   a Click **Options**.

   b Accept the current account, or select **Use the following account**, and enter the user name and password.

   c Click **OK**.

4 Test the replication.

   a In the left pane, select the domain to replicate.

   b Select either the forest root to test all servers in the forest, a site to test all servers in that site, or an individual server to test just that server.

   c Click **Start Test**.

   d Check the list of included servers. All domain controllers are selected by default. To exclude a domain controller from the test, clear the check box.

   e Click **OK**.

   During the analysis **(pending)** displays after each server being analyzed. To stop the analysis, click **Stop Test**. When the analysis is complete, the results display in the **Replication Test Results** area.

   f Double-click an item in the **Replication Test Results** area to view the details. You can copy the results and paste into a text file.

   g Click **Close**.

5 Check the topology.

   a Click **Check Topology**.

   b Check the list of included servers. All domain controllers are selected by default. To exclude a domain controller from the test, clear the check box.

   c Click **OK**.

6 Select the forest root, a site, or an individual server, and then **Replicate All** or **Replicate**.

Managing Active Directory trusts

You can now manage forests and trusts from within Active Administrator®.

Topics

- Adding a forest trust
- Adding a domain trust

To manage Active Directory® trusts

1 Select **Active Directory Infrastructure | Active Directory Trusts**.

2 Select a domain controller.

> **NOTE:** Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3 Use the options on the tool bar to manage Active Directory trusts.

The options change depending on whether a forest or a domain is selected.

Table 99. Active Directory trusts tool bar

Option	Description
Refresh Tree	Refresh the tree.
Refresh Trusts	Refresh the list of trusts.
New Forest Trust	Add a forest trust. See Adding a forest trust.
New Domain Trust	Add a domain trust. See Adding a domain trust.
Edit	Edit the selected trust.
Delete	Delete the selected trust. **NOTE:** You can remove the trust from the local domain only or from both domains. If you choose to remove the trust from both domains, you must enter the user name and password for the account with administrative privileges in the target domain.
Build Forest Trusts Report	Generate a forest trusts report that you can print, email, or export.
Build Domain Trusts Report	Generate a domain trusts report that you can print, email, or export.

Adding a forest trust

To add a forest trust

1 Select **Active Directory Infrastructure | Active Directory Trusts**.

2 Select a domain controller.

> **NOTE:** Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3 Click **New Forest Trust**.

4 Type a target forest, or browse to select a forest.

5 Select the direction.

Table 100. Options for authentication

Option	Description
Bidirectional (two-way)	Users can be authenticated in the source and target forest.
Incoming (one-way)	Users in the source domain can be authenticated in the target forest.
Outgoing (one-way)	Users in the target forest can be authenticated in the source domain.

6 Select the sides of the trust. If you choose both sides of the trust, you must enter the user name and password for the account with administrative privileges in the target domain.

Table 101. Options for authentication

Option	Description
This domain only	Creates the trust relationship in the local domain.
Both this domain and the specified domain	Creates the trust relationship in the local domain and the target domain. You must have appropriate permissions in both domains.

7 Select the authentication for the source and target: **Forest-wide** or **Selective**.

8 Click **OK**.

9 Click **Validate**.

10 Click **OK**.

Adding a domain trust

To add a domain trust

1 Select **Active Directory Infrastructure | Active Directory Trusts**.

2 Select a domain controller.

> **NOTE:** Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3 Select a forest.

4 Select a domain.

5 Click **New Domain Trust**.

6 Select a trust type from the list.

7 Type a domain, or browse to select a domain.

8 Select the direction.

Table 102. Options for authentication

Option	Description
Bidirectional (two-way)	Users can be authenticated in the source and target forest.
Incoming (one-way)	Users in the source domain can be authenticated in the target forest.
Outgoing (one-way)	Users in the target forest can be authenticated in the source domain.

9 Select the sides of the trust. If you choose both sides of the trust, you must enter the user name and password for the account with administrative privileges in the target domain.

Table 103. Options for authentication

Option	Description
This domain only	Creates the trust relationship in the local domain.
Both this domain and the specified domain	Creates the trust relationship in the local domain and the target domain. You must have appropriate permissions in both domains.

10 Click **OK**.

Passwords are used by Active Directory® domain controllers to confirm trust relationships. The same password must be used when creating this trust relationship in the specified domain. After the trust is created, the trust password is periodically updated for security purposes.

IMPORTANT: Before this trust can function, it also must be created in the other domain. Ensure the same trust password is used in both domains.

11 Type password twice, and click **OK**.

12 Click **Validate**.

13 Click **OK**.

10

DC Management

The DC Management module enables you to view performance and specifications of your domain controllers, manage Windows® services, and view event logs.

Topics

- Using the DC Management landing page
- Checking domain controller status
- Managing services
- Monitoring domain controller performance
- Managing event logs

Using the DC Management landing page

The landing page displays the active tiles for each feature in the section. The active tiles automatically update every 30 minutes, but you can use the icons to refresh the tiles at any time. You also can pause and resume the refresh of data. To customize the active tile refresh, see Setting general user options.

To use the DC Management landing page

1. Click **DC Management**.
2. To access the features in this section, click an active tile or choose from the tree.
   - DC Status (See Checking domain controller status.)
   - Services (See Managing services.)
   - Performance (See Monitoring domain controller performance.)
   - Event Logs (See Managing event logs.)

Checking domain controller status

To check the status of a domain controller

1. Select **DC Management | DC Status**.
2. Select a domain controller.

   NOTE: Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3. The server status is divided into sections. You can expand or collapse the sections.

- To refresh the status, click **Refresh**.
- To copy all the information, click **Copy**, and paste into an email or .txt file.

Managing services

You can manage Windows® services from within the Active Administrator® console.

To manage Windows services

1 Select **DC Management | Services**.

2 Select a domain controller.

> **NOTE:** Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3 Use the tool bar to manage the displayed services.

Table 104. Services tool bar

Option	Description
Refresh	Refresh the list of services.
Start	Start the selected service.
Stop	Stop the selected service.
Restart	Restart the selected service.
Pause	Pause the selected service.
Refresh Selected	Refresh the selected service.
Properties	Set the startup account for the selected service. **NOTE:** If you change the startup account, you should restart the service.
Sort	Sort the list of services.

Monitoring domain controller performance

The **Domain Controller Performance** window displays information in real-time for selected counters. You can add or remove counters to customize the display.

To monitor domain controller performance

1 Select **DC Management | Performance**.

2 Select a domain controller.

> **NOTE:** Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3 Use the tool bar to customize the display.

Table 105. Domain controller performance tool bar

Option	Description
Counters	Add or remove counters to customize the display.
Options	Set data collection options. You can enable or disable auto updates, change the sample time and duration of the sample.
Reload	Reload to start the sample over.
Disable auto updates	Disable auto updates. You can update the display manually by clicking **Update Now**. You also can disable auto updates by clicking **Options**.
Enable auto updates	Enable auto updates.
Update Now	Update the display.

Managing event logs

Active Administrator® captures many different types of events to assist you in troubleshooting your system. The types of event logs you can view are:

- Active Directory® Web Services
- Application
- DFS Replication
- Directory Service
- DNS Server
- File Replication Service
- Hardware Events
- Internet Explorer
- Key Management Service
- Security
- System
- Windows PowerShell®

To manage event logs

1 Select **DC Management | Event Logs**.

2 Select a domain controller.

> **NOTE:** Use the icons to manage the selected managed domain controller. See Managing domain controllers.

3 Select a log to view from the list.

The latest 1000 events for the last 24 hours display in the top area of the display. Select an event to view the details in the bottom area of the display. You can copy selected events to paste into a .txt file or email.

4 Use the tool bar to manage the event logs.

Table 106. Event logs tool bar

Option	Description
Event Log	Select an event log.
Refresh	Refresh the displayed event log.

Table 106. Event logs tool bar

Option	Description
Stop	Stop loading an event log if it is taking too long.
Copy	Copy selected events to paste into an email or a .txt file.
Clear	Clear the displayed event log. A message displays asking if you want to save the log before it is cleared. • To save the log before clearing it, click **Save and Clear**. The log contents are saved to an Event file (*.evtx), which you can view using the Windows® Event Viewer. • To clear the log without saving it, click **Clear**.
Options	Set the event period and the number of events to display. The default is 24 hours and 1000 events.
Sort	Sort the displayed event log in ascending or descending order by errors, warnings, information, success audits, or failed audits.
Custom Filters	Use a custom filter to filter event logs. You can add, edit, or delete custom filters.

11

DNS Management

The DNS Management module offers you the ability to manage, monitor, and analyze Domain Name System (DNS) servers. You can search resource records on multiple servers and view DNS event logs.

IMPORTANT: An Active Administrator license or an Active Directory Health license is required for the DNS Management module. If you do not have either of these licenses applied to your installation, the DNS Management module will not appear in Active Administrator.

NOTE: Users must have the DNS Management permission to manage DNS servers. See Defining role-based access.

Topics

- Using the DNS Management landing page
- Managing DNS servers
- Monitoring DNS servers
- Using the DNS analyzer
- Viewing the DNS event log
- Searching for DNS records

Using the DNS Management landing page

The landing page displays the active tiles for each feature in the section. The active tiles automatically update every 30 minutes, but you can use the icons to refresh the tiles at any time. You also can pause and resume the refresh of data. To customize the active tile refresh, see Setting general user options.

To use the DNS Management landing page

1. Click **DNS**.
2. To access the features in this module, click an active tile or choose from the tree.
   - DNS Management (See Managing DNS servers.)
   - DNS Monitoring (See Monitoring DNS servers.)
   - DNS Analyzer (See Using the DNS analyzer.)
   - DNS Event Logs (See Viewing the DNS event log.)
   - DNS Search (See Searching for DNS records.)

Managing DNS servers

Only managed DNS servers can be monitored, analyzed, logged, and searched. See Adding managed DNS servers.

Topics

- Adding managed DNS servers
- Adding records
- Editing records
- Deleting records
- Running reports
- Editing DNS server properties
- Editing zone properties
- Editing zone permissions
- Scavenging records

To manage DNS servers

1 Select **DNS | DNS Management**.

2 Select a DNS server from the list, or click  to add a DNS server, if necessary. See Adding managed DNS servers.

Expand the tree in the left pane to view objects in the right pane.

- To filter the list of objects, start typing in the **Filter Objects** box. The display updates as you type.
- To remove the filter, click **X**.
- To view the properties of a record, double-click a record.
- To refresh the entire tree, click **Refresh**.
- To refresh only the selected domain in the tree, click **Refresh Domain**.

3 From this page, you can add managed DNS servers, add/edit/delete records, run reports, edit DNS server and zone properties, edit zone permissions, and scavenge records.

Adding managed DNS servers

To view and add managed DNS servers

1 Select **DNS | DNS Management**.

1 Click  . The list of managed DNS servers displays.

- To filter the list of managed DNS servers, start typing in the **Filter DNS Servers** box. The display updates as you type.
- To remove the filter, click **X**.

2 Type the server name, and click **Connect**.

- To remove a selected DNS server from the list, click **Remove**.

3 Click **OK**.

Adding records

To add a record

1. Select **DNS | DNS Management**.
2. Select a DNS server from the list.
3. Click **New**.
4. Select a listed record type, or select **Other new records** to view a list of all available records.
5. Define the record.
6. Click **OK**.

Editing records

The properties that you can edit on a record vary with the type of record selected. You also can edit records during a search. See Searching for DNS records.

To edit a record

1. Select **DNS | DNS Management**.
2. Select a DNS server from the list.
3. Expand the tree to locate the record to edit.
4. Select the record, and click **Properties**.

   -OR-

   Right-click the record, and choose **Edit**.
5. Make the necessary changes.
6. Click **OK**.

Deleting records

You also can delete records during a search. See Searching for DNS records.

To delete a record

1. Select **DNS | DNS Management**.
2. Select a DNS server from the list.
3. Expand the tree to locate the record to delete.
4. Select the record, and click **Delete**.
5. Click **Yes**.

Running reports

You can run a server or domain report on a selected server. The server report lists zones for the selected server. The domain report lists the domains and resource records for the selected server.

To run reports

1 Select **DNS | DNS Management**.

2 Select a DNS server from the list.

3 Click **Reports,** and select a report.

4 Use the print editor icons to print, save, export, or email the report.

5 Click **Back** to return to the DNS Management window.

Editing DNS server properties

You can edit most properties of a DNS server.

NOTE: DNS Security Extensions (DNSSEC) Sign the Zone and the monitoring features for DNS servers cannot be set using this feature in Active Administrator.

To edit server properties

1 Select **DNS | DNS Management**.

2 Select a DNS server from the list, and click **Properties**.

3 Use the tabs to make the necessary changes.

Table 107. DNS server properties tabs

Tab	Description
Interfaces	Select the IP addresses that will service DNS requests. You can select all IP addresses or individual IP addresses.
Forwarders	View a list of DNS servers that the selected server uses to resolve DNS queries if it is unable to resolve the query. To modify the list, click **Edit**. You can add more servers to the list, reposition the servers in the list, and delete servers from the list. • To add servers to the list, type the IP address in the box, and click **Add**. • To reposition a selected server in the list, click **Up** or **Down**. • To delete a selected server from the list, click **Delete**.
Advanced	Select advanced options for the selected DNS server: • Disable recursion • Enable BIND secondaries • Fail on load if bad zone data • Enable round robin • Enable network ordering • Secure cache against pollution • Enable DNSSEC validation for remote responses • Set name checking. • Set how to load zone data on startup. Automatic scavenging is not enabled by default. You can enable automatic scavenging and set a time period for the records. **NOTE:** If you do not want to do automatic scavenging, you can run scavenging manually at any time. See Searching for DNS records. To return the settings to the default, click **Reset to Default**.
Debug Logging	Select to record packets sent and received by the selected DNS server to a log file. **Debug logging** is enabled by default.
Event Logging	Select the level of events to record in the DNS event log.

5 Click **OK.**

Editing zone properties

You can edit most properties of a zone.

To edit zone properties

1 Select **DNS | DNS Management**.

2 Select a zone from the list, and click **Properties**.

3 Use the tabs to make the necessary changes.

Table 108. Zone properties tabs

Tab	Description
General	Displays information about the zone. To set aging/scavenging properties, click **Aging**.
Start of Authority (SOA)	Modify the SOA record for the domain.
Name Servers	Add, edit, or remove servers.
Zone Transfers	Unavailable for edit.

4 Click **OK**.

Editing zone permissions

You can edit the permissions of only zones that are integrated with Active Directory® Domain Services. The icon next to the zone indicates if it is integrated () or not integrated ().

To edit permissions on a single zone

1 Select **DNS | DNS Management**.

2 Select a DNS server from the list.

3 Right-click an integrated zone, and choose **Zone Permissions**.

The **Zone permissions** window displays the accounts and their permissions. You can add, remove, or view/edit the permissions of a selected account. You also can disable inheritance on a selected account.

To edit permissions on multiple zones

1 Select **DNS | DNS Management**.

2 Select a DNS server from the list.

3 Click **Delegate Permissions**.

4 Select to add or remove permissions.

5 Click **Next**.

6 Select one or more zones.

7 Click **Next**.

8 Select a principal, permission type, and the objects.

9 Select the permissions to add or remove.

You can filter the list of permissions by typing in the **Filter permissions** box or selecting an option in the **Show** list. Click Show advanced permissions to expand the list of permissions.

10 Click **Next**.

11 Review your selections.

12 Click **Finish**.

Scavenging records

Stale resource records can degrade the performance of a DNS server over time. Periodically, you should run scavenging to clean up any stale records. You also can set up automatic scavenging. See Editing DNS server properties.

To run scavenging

1 Select **DNS | DNS Management**.

2 Select a DNS server from the list, and click **Start Scavenging**.

3 Click **Yes**.

Monitoring DNS servers

You can create tests to run on selected DNS servers at a specified time. By default, DNS monitoring is enabled and tests are run every 15 minutes. You can disable all DNS monitoring and run tests on demand, or disable just specific tests and let the rest run automatically.

You also can set up an on-demand test to run on multiple servers at one time. See Using the DNS analyzer.

Topics

- Setting testing options
- Creating tests
- Running tests
- Editing a test
- Deleting a test

Setting testing options

To set testing options

1 Select **DNS | DNS Monitoring**.

2 By default, DNS monitoring is enabled. To disable automatic testing, clear the check box.

3 By default, tests run every 15 minutes. To change the time period, type a value in the box. Acceptable time period values are 5 to 1440 minutes.

4 Click **Save Settings**.

Creating tests

You can create a new test or copy an existing test to modify as a new test.

To create a new test

1. Select **DNS | DNS Monitoring**.
2. Click **Add**.
3. Type a name for the test.
4. Type the DNS server to test.

   By default, the test is enabled so it automatically runs at the specified time duration set on the main page. If you want to disable the test, clear the check box. You can run the test manually.
5. Select to run an Active Directory® domain test or create a custom test.

   To create an Active Directory Domain test

   a. Select **Active Directory Domain Test**.

   b. Browse to locate the domain to test.

   c. The domain controller IP addresses are validated by default. If you do not want the validation performed, clear the check box.

   To create a custom test

   a. Select **Custom Test**.

   b. Click **Add**.

   c. Select the type of record to test.

   d. Type the query.

   e. Click **OK**.
6. Click **OK.** See Running tests.

To create a new test by copying an existing test

1. Select **DNS | DNS Monitoring**.
2. Select a test, and click **Copy.**
3. Modify the test to meet the needs of the new test.
4. Click **OK**. See Running tests.

Running tests

You can wait until the automatic testing is run, or run the tests manually.

To run all listed enabled tests manually

1. Select **DNS | DNS Monitoring**.
2. Click **Run Test.**

To view test results

- Select a test, and click **Test Details**.

Editing a test

To edit a test

1. Select **DNS | DNS Monitoring**.

2 Select a test, and click **Edit**.

3 Make the necessary changes to the test.

4 Click **OK**. See Running tests.

Deleting a test

To delete a test

1 Select **DNS | DNS Monitoring**.

2 Select a test, and click **Delete**.

3 Click **Yes**.

Using the DNS analyzer

The DNS analyzer allows you to test one or more servers by name or IP address. You also can test the Active Directory® domain. If you want tests to run automatically on a schedule, see Monitoring DNS servers.

To run a test on selected servers

1 Select **DNS | DNS Analyzer**.

2 Type the fully qualified domain name (FQDN) of the servers you want to test.

> **NOTE:** Separate multiple servers with a semicolon. Do not include spaces between the server names. The format should be **server1.domain.local;server2.domain.local;server3.domain.local**.

3 You can test for records on the listed servers or the Active Directory® domain.

To test for specific records on the selected servers

a Select the type of records to search.

b Select **TCP** or **UDP** transport.

c Type the question. Separate multiple questions with a semicolon.

Examples

- **Gold_dc3.gold_sales.acme.local**
- **www.quest.com; mail-server.acme.net**

To run an Active Directory domain test

a Select **Test Active Directory Domain**.

b To validate domain controller IP addresses, select the check box. Each domain controller in DNS for the domain specified in the **Question** box is pinged during the test.

*Available only when the **Test Active Directory** check box is selected.*

c In the **Question** box, type the FQDN of the domain you want to test, such as **Acme.local**.

4 Set the number of attempts and timeouts.

5 To test only the servers listed in the **Servers** box, leave the **Recursion** check box unselected.

6 Click **Test**.

One set of results is listed. If you entered more than one server, select the server from the **Test results for** list.

- If an error occurs during the test, click **View Details**.

- To expand the categories in the list of test results, click **Expand all**.
- To collapse all the categories, click **Collapse all**.
- To copy the test results to a txt file, click **Copy**.

Viewing the DNS event log

The DNS event log displays 100 events over a 24 hour period by default. You can change the amount of data that displays. See Setting display options.

You can sort all events in ascending or descending order, or by error, warning, information, success audit, or failed audit in ascending or descending order. You actively can filter the list of events by typing in the **Filter Event Log** box or you can create a custom filter for views you frequently use. See Using custom filters.

Topics

- Using custom filters
- Setting display options

To view the DNS event log

1. Select **DNS | DNS Event Logs**.
2. Select the DNS server from the list, or click  to add a DNS server, if necessary. See Adding managed DNS servers.
   - To sort the list of events, select a sort order from the **Sort** list.
   - To filter the list of events, start typing in the **Filter Event log** box. The display updates as you type.
   - To remove the filter, click **X**.
   - To clear the log, select **More | Clear**, and click **Yes**.

Using custom filters

You can create custom filters to help you manage the amount of information contained in the event log.

Topics

- Creating custom filters
- Applying custom filters
- Editing custom filters
- Deleting custom filters

Creating custom filters

To create a custom filter

1. Select **DNS | DNS Event Logs**.
2. Select the DNS server from the list, or click  to add a DNS server, if necessary. See Adding managed DNS servers.
3. Click **Filters**.
4. Click **Add**.

5 Type a name for the filter.

6 Select the type of events to filter.

7 Define the filter.

8 Click **OK**. The custom filter is applied automatically.

Applying custom filters

To apply a custom filter

- Click **Filters**, and select a filter from the list.

To remove an applied custom filter

- Click **Filters**, and select **All Events** from the list.

Editing custom filters

To edit a custom filter

1 Click **Filters**, and select a filter from the list.

2 Click **Filters**, and select **Edit**.

3 Make the necessary changes.

4 Click **OK**.

Deleting custom filters

To delete a custom filter

1 Click **Filters**, and select a filter from the list.

2 Click **Filters**, and select **Delete**.

3 Click **Yes**.

Setting display options

To set display options for the DNS event log

1 Select **DNS | DNS Event Logs**.

2 Select the DNS server from the list, or click  to add a DNS server, if necessary. See Adding managed DNS servers.

3 Select **More | Options**.

4 Set the time period (in hours) to display events. The default is 24 hours.

5 Set the number of events to display. The default is 100 events.

6 Click **OK**.

Searching for DNS records

You can search multiple DNS servers for records. By default, all records display, but you can choose to search for only a specific type of record. From the results, you can edit or delete selected DNS objects. Searches are saved until you choose to delete them, so you can return to a specific search at a later time.

To search DNS servers for records

1. Select **DNS | DNS Search**.
2. Type the DNS servers to search, separated by semicolons.
3. Select the type of records to search.
4. Type search criteria, separated by commas. The use of wildcards is supported.
5. Click **Search**.

   The search results display in the right pane.

   - To edit a selected DNS object, Click **Edit**. See Editing records.
   - To delete selected DNS objects, click **Delete DNS Object(s)**. See Deleting records.

   As you create searches, they are added to the list in the left pane.

   - To delete selected searches, click **Delete Template**.

12

Configuration

The Configuration section contains the setup that was defined during installation through the AA Configuration Wizard. You can make additional changes here or launch the AA Configuration Wizard from the Start menu. Also included are the options from the Settings menu and the AA Server Manager feature.

Topics

- Using the Configuration landing page
- Managing tasks
- Defining role-based access
- Setting email server options
- Configuring SCOM and SNMP Settings
- Setting notification options
- Setting Active Template options
- Setting agent installation options
- Setting recovery options
- Setting GPO history options
- Setting certificate configuration
- Setting service monitoring policy
- Managing archive databases
- Migrating data to another database
- Setting a preferred domain controller
- Setting up workstation logon auditing
- Managing configuration settings
- Setting user options
- Managing the Active Directory server

Using the Configuration landing page

The landing page displays the active tiles for each feature in the section. The active tiles automatically update every 30 minutes, but you can use the icons to refresh the tiles at any time. You also can pause and resume the refresh of data. To customize the active tile refresh, see Setting general user options.

To use the Configuration landing page

1. Click **Configuration**.
2. To access the features in this section, click an active tile or choose from the tree.
    - Tasks (See Managing tasks.)

- Role Based Access (See Defining role-based access)
- Email Settings (See Setting email server options)
- Notification Settings (See Setting notification options)
- Active Template Settings (See Setting Active Template options)
- Agent Installation Settings (See Setting agent installation options)
- SCOM and SNMP Integration (See Configuring SCOM and SNMP Settings)
- Recovery Settings (See Setting recovery options)
- GPO History Settings (See Setting GPO history options)
- Certification Configuration (See Setting certificate configuration)
- Service Monitoring Policy (See Setting service monitoring policy)
- Active Archive Databases (See Managing archive databases)
- Workstation Logon Settings (See Setting up workstation logon auditing)

Managing tasks

The **Task** tab lists the tasks performed in Active Administrator®. The indicator bar at the top of the list summarizes the number of tasks running, pending, completed, failed, canceled, and aborted. Various modules in Active Administrator display a subset of these tasks.

To manage tasks in Active Administrator

1 Select **Configuration | Tasks**.

You can click a column heading to sort a single column.

2 Use the tool bar to manage the listed tasks. You also can right-click a task and choose from the shortcut menu.

Table 109. Tasks tool bar

Option	Description
Refresh	Refresh the task list.
Properties	View status, details, and extended properties about a selected task. From the **Task Details** page, click **Send** to send the task in an email.
Cancel	Cancel the selected pending tasks.
Retry	Retry selected aborted, canceled, or failed tasks.
Send Email	Send the selected tasks to specified recipients in an email.
Group by status	Group the tasks by the entries in the **Status** column. You also can sort the tasks by clicking on the column heading. Click **Ungroup Tasks** to return the display.
Clear	Clear all tasks, selected tasks, completed tasks, failed tasks, canceled tasks, or aborted tasks.

Defining role-based access

Set up permissions to restrict access to the various modules in Active Administrator. Permissions are evaluated when a user starts Active Administrator. If the user does not have permission to an Active Administrator module,

that module does not display. If the user does not have permission to any modules, Active Administrator Console shuts down. All modifications to the permissions are audited by the Active Administrator audit agent.

IMPORTANT: If Active Administrator cannot access the Active Administrator database to validate permissions, the user will have access to all modules in the console.

Topics

- Adding a new user or group to Active Administrator

Refer to the following table to determine the access to give to users.

Table 110. Role-based access

Role	Area
Full Control	Full access to all modules in Active Administrator. Clear the check box to configure individual roles.
Active Templates	Dashboard Search (Search only) Delegation Status Active Templates Tasks Search quick task
Alert Editor	Dashboard Search (Search only) Alerts Tasks Search quick task
Alert Viewer	Dashboard Search (Search only) Alerts (Read only) Tasks Search quick task
Audit Report Management	Dashboard Search (Search only) Audit Reports Archives Tasks Search quick task
Audit Report Viewer	Dashboard Search (Search only) Audit Reports (Read only but can add tags and comments) Archives (Read only but can add tags and comments) Tasks Search quick task

Table 110. Role-based access

Role	Area
Domain Controller Management	Dashboard Search (Search only) DC Status Services Performance Event Logs Tasks Search quick task
Group Policy History	Dashboard Search (Search only) Group Policy History Task Search quick task
Group Policy Object Management	Dashboard Search (Search only) Group Policy Objects GPO By Container GPO Modeling GPO Backup Troubleshooting Tasks Search quick task
Group Policy Repository	Dashboard Search (Search only) GPO Repository Tasks Search quick task
Password Policy	Dashboard Search (Search only) Password Policies Tasks Search quick task
Recovery	Dashboard Search (Search only) Object Recovery Tasks Search quick task
Security	Dashboard Search (Search and Edit) User Logon Activity Delegation Status Tasks All quick tasks items

Table 110. Role-based access

Role	Area
Site Management	Dashboard Search (Search only) Active Directory Sites Replication Monitoring Replication Analyzer Tasks Search quick task
Trusts Management	Dashboard Search (Search only) Active Directory Trusts Tasks Search quick task
DNS Management	Full access to the DNS module.
Certificate Management	Full access to the Certificate module. **NOTE:** If the Certificate Management role is selected, the Certificate Manager Viewer role is also selected and the check box is disabled. Clear the **Certificate Management** check box to limit the user to read-only access.
Certificate Management Viewer	Read-only access to the Certificate module.
Active Directory Health Alert Viewer	Read-only access to Active Directory Health Analyzer alerts.
Active Directory Health Analyzer	Read-only access to the Active Directory Health Analyzer module. **NOTE:** Must be selected to configure other Active Directory Health Analyzer roles.
Microsoft Entra Connect	Full access to **Active Directory Health | Microsoft Entra Connect**.
Active Directory Health Agent Management	Access to **Active Directory Health Analyzer | Agents** to install, remove, edit, and start/stop/restart agents. If disabled, user can view agent properties and workload details.
Active Directory Health Alert Management	Full access to **Active Directory Health Analyzer | Agents | Alert Settings** to edit settings for alerts. If disabled, user can view, but not edit alert settings.
Active Directory Health Data Collector Management	Full access to **Active Directory Health Analyzer | Agents | Data Collectors** to edit settings for data collectors. If disabled, user can view, but not edit data collector settings.
Active Directory Health Notification Management	Full access to managing Active Directory Health Analyzer notifications.
Active Directory Health Troubleshooter	Full access to **Active Directory Health | Troubleshooter**. If disabled, user cannot run reports, run jobs, delete reports and jobs results, clear history or replicate connections between domain controllers in replication view. User can open existing reports from history, view previous job results, and view generated replication views.
Active Directory Health Check Management	Full access to the Active Directory Health Check module.
Active Directory Health Check Viewer	Read-only access to the Active Directory Health Check module.

Table 110. Role-based access

Role	Area
User Provisioning	Full access to user provisioning actions. **NOTE:** By default, users who hold the Full Access role are automatically granted the User Provisioning role.
User Provisioning read-only access	Read-only access to user provisioning. **NOTE:** By default, all users are granted the User Provisioning read-only access role.

To manage role-based access

1 Select **Configuration | Role Based Access**.

> **NOTE:** To configure individual roles, you must clear the **Full Control** check box. To configure individual Active Directory Health Analyzer roles, you must select the **Active Directory Health Analyzer** check box.

2 Use the tool bar to manage role-based access.

Table 111. Role-based access tool bar

Option	Description
Refresh	Refresh the list.
New	Click to add users and groups to the list. See Adding a new user or group to Active Administrator.
Save	Save any changes.
Delete	Click to remove selected users and groups from the list.
Select All Permissions	Select all modules for the selected user or group.
Clear All Permissions	Clear all modules for the selected user.

Adding a new user or group to Active Administrator

To add a new user or group to Active Administrator

1 Select **Configuration | Role Based Access**.

2 Click **New**.

3 Search for users or groups.

4 Add optional comments.

5 By default, users and groups have access to the listed permissions in Active Administrator. To deny access, clear the check box.

- To select all, click **Select All Permissions**.
- To clear all, click **Clear All Permissions**.

6 Click **Save**.

Setting email server options

To set email server options

1 Select **Configuration | Email Settings**.

2 Select to use either **SMTP** or **Exchange Online**.

Email Option	Procedure
SMTP	1 Type the name of the SMTP server that sends the alert emails. 2 Type the number of the TCP/IP port on which the SMTP server is listening. 3 Type the User name and password required to authenticate the SMTP server. 4 Type the email address that to appear in the **From** box of the alert email. By entering something meaningful, you can use the **From** box to filter your email. By default, the email of the current user displays.
Exchange Online	1 Type the Exchange service URL, the tenant ID, and the Application ID. 2 Type the mailbox name and select the required certificate for authentication. **NOTE:** • The certificate must be previously uploaded to Microsoft Entra App certificates & secrets. • The application ID, tenant ID, tenant name, certificate, and certificate password are set when you register Active Administrator to use Office 365 Exchange Online through Microsoft Entra ID. See Appendix: Registering Active Administrator for Office 365 Exchange Online.

3 Choose a format for the email.

4 Click **Test Settings** to verify the values.

5 Click **Save**.

Configuring SCOM and SNMP Settings

If you have a license for the Active Directory Health module and are using Microsoft® System Center Operations Manager (SCOM), you can deploy the Quest® Active Administrator® management pack, which establishes a connection to SCOM. If you are using an SNMP manager, you can configure the integration from the Active Administrator console. Once an alert manager has been configured, Active Directory Health alerts from the Active Directory Health Analyzer agent are displayed in the Operations Manager **Monitoring** pane under the **Quest Active Administrator** folder and in the **SNMP Manager**.

NOTE: Only System Center 2016 Operations Manager is supported.

NOTE: Only SNMP management software capable of TRAP v2 notifications processing is supported.

NOTE: After you complete the configuration, you can edit the **System Center Operations Manager Notification** to configure which Active Directory Health Analyzer alerts to push to SCOM or an SNMP manager. See Pushing alerts to System Center Operations Manager and SNMP managers.

To configure Systems Center Operations Manager and SNMP integration

1. Select **Configuration | SCOM and SNMP Settings**.
2. Optionally, select **Forward alert events to SCOM server** to forward alert events and to deploy the Quest Active Administrator management pack to the specified SCOM management server.

   Type the name of the SCOM management server.

   Type or browse for an account with SCOM administrator rights, and type the password.

   > **NOTE:** The account must be a member of the SCOM Administrator group and a member of the local Administrators group on the computer where Active Administrator Server is installed.

   To test the SCOM connection, click **Test Settings**.
3. Optionally, select **Enable SNMP notification** and enter the IP address of the SNMP notification target computer.

   To test the SNMP connection, click **Test Settings**.

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

Setting notification options

To set notification options

1. Select **Configuration | Notification Settings**.
2. In the **Alert Limit** box, type the number of hours to use as a limit for issuing alerts.

   For example, if an alert occurred within the last 24 hours (by default), an alert email is sent. However, if the event occurred further out than the number shown here, no alert email is generated, but the event is recorded in the database.
3. Select the mode of notification.

   Table 112. Options for notification

Option	Description
Batch Mode	By default, when more than 5 event notifications occur within a 60 minute period, one email is sent.
Non-Batch Mode	Select to send an email immediately after every event occurs.

4. By default, 1000 alerts are returned. To change the value, type in the box.
5. By default, the Alert Notification Policy is enabled. To disable the policy, clear the check box.
6. Click **Save**.

Setting Active Template options

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

To set Active Template options

1 Select **Configuration | Active Template Settings**.

2 By default, Active Administrator checks for broken Active Templates every 30 seconds and automatically repairs any broken Active Templates found. To disable automatic repair, clear the check box. You also can change the time period.

3 By default, a report of broken templates found and repaired is sent to the Active Administrator owner. You can add additional email addresses.

> **NOTE:** The Active Administrator owner was identified in the AA Configuration Wizard. To change the AA Owner email address, see Managing email addresses.
>
> **NOTE:** To manage the Active Template email address list, see Managing email addresses.

4 Click **Save**.

Setting agent installation options

The options set on this page determine the default settings that appear when you select to install an audit agent. You can change the default setting for each individual install.

To set audit agent installation options

1 Select **Configuration | Agent Installation Settings**.

2 Select the default action for agent installation.

Table 113. Options for default action for agent installation

Option	Description
Install and Activate	By default, the agent is activated after installation so event collection begins immediately.
Install Only	Select to install the agent without activation. You will need to activate the agent to begin collection.

3 By default, service monitoring and recovery is enabled. To disable, clear the check box. When installing an agent, you can select this option if needed.

4 In the **Event Collection Limit** box, type the number of days to go back when looking for events.

5 By default, events are collected for the last 7 days. If you are not interested in retrieving historical events, you can limit the collection to few days. You might find this option useful for the initial collection of data to prevent very large event logs from being examined in full.

6 By default, Advanced Auditing is enabled on domain controllers.

7 When Advanced Auditing is enabled, both before and after values are reported. For example, if you change a telephone number, Active Administrator reports on both the old number and the new number. If you want only the after value reported, clear the check box.

8 By default, you receive a warning when a domain controller is missing an audit agent. To disable the warning, clear the check box.

9 Click **Save**.

Setting recovery options

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

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

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

Topics

- Adding a domain
- Enabling or disabling password recovery

To set up Active Directory recovery

1. Select **Configuration | Recovery Settings**.

   The Active Administrator AD Object Backup Service backs up the listed domains based on the settings in the **Run backup** boxes.

   - To add a domain, click **Add**. See Adding a domain.
   - To edit a selected domain, click **Edit**.
   - To remove a selected domain, click **Remove**.
   - To disable or enable Password Recovery on a selected domain, click **Password Recovery**. See Enabling or disabling password recovery.

2. By default, backups occur twice a day at 6:00 A.M. and 6:00 P.M. To change the frequency, select to run the backup **Every Day, Twice a Day**, or **Weekly** in the **Run backup** box. To change the day of the week or time(s), select from the list.

3. Change the folder where temporary backup files are processed, if desired.

   To change the folder where temporary backup files are processed

   a. Select the **Override the default temporary folder** check box.

   b. Browse to locate or create a folder.

   c. Click **OK**.

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

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

   To change the folder where backup files are stored

   a. Select the **Override AD Backup share path** check box.

   b. Browse to locate or create a folder.

   c. Click **OK**.

5. Click **Save**.

Adding a domain

To add a domain

1 Select **Configuration | Recovery Settings**.

2 Click **Add Domain**.

3 In the **Domain** box, type a domain name, or browse to locate a domain.

4 Specify the domain controller to perform the backup.

Table 114. Options for domain controller backup

Option	Description
Use automatically selected domain controller	By default, Active Administrator® uses a domain controller automatically selected by Active Directory®.
Use the domain controller specified here	Select to use a different domain controller, and then browse to locate a domain controller.

5 Click **OK**.

Enabling or disabling password recovery

Active Administrator can restore passwords when you restore accounts that were deleted.

IMPORTANT: If you choose to disable password recovery, passwords are not backed up. If you restore a backup that does not contain passwords, you must dis-join and then rejoin computer accounts.

NOTE: Enabling password recovery changes the searchFlags attribute of the Unicode-PWD object in the Active Directory® schema, but does not alter the schema structure.

To enable or disable password recovery

1 Select **Configuration | Recovery Settings**.

The **Password Recovery** column indicates if password recovery is enabled or disabled.

2 Select the domain, and click **Password Recovery**.

3 Click **Yes** in response to the displayed message.

Setting GPO history options

The Group Policy History service should be installed on only one computer. The service needs to be configured to run as a domain account that has enough privileges to read all of the Group Policy object (GPO) settings on the domain, as well as to write permissions to the Group Policy History Path.

To set GPO history options

1 Select **Configuration | GPO History Settings**.

2 Select how often you want the Group Policy History service to poll the domain controllers for Group Policy object (GPO) changes at a specified polling interval.

NOTE: The GPO service polls the domain controllers for GPO changes at a specified polling interval. The polling interval is set to 60 seconds by default. We recommend a polling interval of 60 seconds as this gives the administrators enough time to make a few changes to the GPO without creating new versions for every change.

3 The GPO History Service checks for GPO Policy changes on the listed domains.
   - To add a domain to the list, click **Add Domain**, and select a domain.
   - To remove a selected domain from the list, click **Remove.**
4 Click **Save**.

Setting certificate configuration

The Certificates feature monitors the state of certificates on managed computers and the security on the repository. You can enable or disable certificate monitoring, and send a notification email when the state of a certificate changes.

Topics

- Setting certificate notifications
- Setting up certificate email notifications
- Configuring certification authority
- Setting security on the repository

Setting certificate notifications

Notifications are sent to accounts on the email list based on the settings you configure.

To set certificate notifications

1 Select **Configuration | Certificate Configuration**.
2 Open the **General** tab, if necessary.
3 By default, certificate monitoring is enabled for the Certificate Management and Certificate Repository modules. To disable the feature, clear the check box
4 By default, security on the Certificate Repository is not checked. If you select this feature, an email notification will indicate if the modify permission was granted using system-provided tools, but not from within Active Administrator®, if the modify permission was deleted using system-provided tools, or if the user/group was deleted using system-provided tools.

   NOTE: Users and groups need the modify permission on the Certificates Repository folder to make changes to certificates stored in the Certificate Repository. See Setting security on the repository.

5 Select the state of the certificate to trigger the notification email. You can select to send an email notification to the listed email addresses when a certificate is:

Table 115. Certificate states that trigger an email notification

Certificate state	Description
deleted	*Certificate Management only* Select to enable or disable notifications for certificates that were deleted.
added	*Certificate Management only* Select to enable or disable notifications for certificates that were added. You also can further specify to only send notifications when a certificate is added using system-provided tools.

Table 115. Certificate states that trigger an email notification

Certificate state	Description
going to expire	Select to enable or disable notifications for certificates that are going to expire. To exclude expiring certificates in the repository and PFX files, clear the check boxes. You also can select to send notifications to the user prior to a password expiring The maximum value is 90 days. Select to send additional levels of notification, if desired. Select to repeat the notifications after the final notification, if desired. The setting for the final notification will repeat, so if the final notification is set to 5 days, the user will continue to receive the notification daily after 5 days until they change their password.
expired	Select to enable or disable notifications for certificates that are expired. To exclude expired certificates in the repository and PFX files, clear the check boxes.
uses a cryptographic hash algorithm	Select to enable or disable notifications for certificates that use a cryptographic hash algorithm. By default, only SHA1RSA is included in the notification. To include other hash algorithms, select the check boxes. **NOTE:** If you enable notification, you can choose to disable specific certificates from the notification. See Excluding certificates that support cryptography.
revoked	Select to enable or disable notifications for certificates that were revoked. To exclude revoked certificates in the repository and PFX files, clear the check boxes. **NOTE:** If you enable notification for revoked certificates, you can choose to disable specific certificates from the notification. See Excluding revoked certificates.

6 Set the window to check for certificate expiration. The default is for certificates set to expire within the next 30 days.

7 Set the time to check the certificates.

8 Click **Save**.

Setting up certificate email notifications

Email notifications are sent to the listed accounts based on the settings on the **General** tab. See Setting certificate notifications.

To set up the email list for certificate notifications

1 Select **Configuration | Certificate Configuration**.

2 Click **Email Addresses**.

3 Add, edit, or remove emails from the list. Each listed email address receives the certificate notification.

> **NOTE:** You also can manage the Certificate Settings email address list from the **Settings** menu. See Managing email addresses.

4 Click **Save**.

Configuring certification authority

When searching for Certificate Authority (CA) certificates, you can employ the search cache instead of searching Active Directory. You can choose to cache an entire forest to maximize the speed of retrieving results, or you can choose to cache only found objects in Active Directory to quickly retrieve the object again from the cache for a certain amount of time.

To configure certificate authority

1. Select **Configuration | Certificate Configuration**.
2. Click **Certificate Authority**.
3. Checking CA services is set to every 10 minutes by default. To change the frequency for checking the CA services, enter a number greater than 10 minutes.
4. Search caching is enabled by default. To disable search caching, clear the check box.

   NOTE: If you disable search caching, all searches are preformed against Active Directory. You also can disable search caching for specific searches.

5. Choose the type of search caching.

Option	Description
Full	The entire forest (users and computers with CA certificates) is cached in memory. Set the cache refresh rate. By default, the cache is refreshed every 20 minutes.
Minimal	Only objects that are found during the search are cached. If you search for the object again, the object is found first in the cache. The object is removed from the cache after 20 minutes.

6. If you want to exclude certain domains from the search cache, click **Add** and select the domain.
7. Click **Save**.

Setting security on the repository

To make changes to certificates in the repository, users and groups must be granted the modify permission on the Certificate Repository folder. Active Administrator provides the tool to help you manage who has the modify permission to the certificate repository.

To set security on the repository

1. Select **Configuration | Certificate Configuration**.
2. Click **Edit permissions**.

   The users and groups listed have the modify permission to the Certificate Repository folder.

   - To add a user or group to the list, click **Add** and select an account.
   - To remove a selected user or group from the list, click **Remove**.

3. Click **Update**.
4. Click **Save**.
5. Click **Yes** to acknowledge that permissions on the Certificate Repository folder will be updated.

   Active Administrator runs a check on the Certificate Repository folder. You will see warnings if the:

   - modify permission was granted using system-provided tools, but not from within Active Administrator
   - modify permission was deleted using system-provided tools

- user/group was deleted using system-provided tools

Setting service monitoring policy

The Service Monitoring feature monitors and reports on all core Active Administrator® services, and if a service stops, there is an attempt to restart it.

To set the service monitoring policy

1. Select **Configuration | Service Monitoring Policy**.
2. By default, the maintenance service monitors the selected services, and restarts the service if it stops. There is a check box for each service: **Notification**, **Data Services**, **Audit Agent**, and **Advanced Agent.** By default, all check boxes are checked. To stop monitoring of a service, clear the check box.

   The bottom pane displays the status of the services.
3. By default, the audit agent monitor checks the database for the last time an event is written to verify that the audit agent has a valid connection to the database. If the auditing agent has not written a heartbeat flag to the database within the minutes specified, a notification is sent to the recipients listed on the Notification page.
   - To stop audit agent monitoring, clear the check box.
   - To change the number of minutes, type a value in the box.
4. Click **Notification**.
5. By default, details about the service configuration, such as the service startup account, the database server name, and the state of the service are included in the notification email. You may want to turn it off if you have security concerns.
6. To add email addresses to the list of recipients, click **Add**.

   NOTE: You can also manage the Service Monitoring Policy email address list from the **Settings** menu. See Managing email addresses.
7. By default, only one notification is sent. If you want to send more notifications, select Notification frequency, and type the frequency notifications are sent. By default, notifications are sent every 4 hours until the problem is resolved.
8. Click **Delivery Options**.
9. For each service, type a new custom subject line or accept the default. Use the variables listed as needed. To reset the message to the default, click **Reset**.

   Table 116. Variables for the custom subject line

Variable	Description
%ServerName%	Inserts the name of the server on which the service is running.
%ServiceName%	Inserts the name of the service that is either stopped or started.
%ServiceStatus%	Inserts the status of the service that is either stopped or started.

10. Select the priority of the email: Normal (default), High, or Low.
11. Click **Save**.

Managing archive databases

You can add or remove archive databases.

Topics

- Creating an archive database
- Modifying archive database settings

To manage archive databases

1 Select **Configuration | Archive Databases**.

2 Use the tool bar options to manage the listed archive databases.

Table 117. Archive databases tool bar

Option	Description
Refresh	Refresh the selected archive databases.
New	Create a new archive database. See Creating an archive database.
Properties	Modify the selected archive database. See Modifying archive database settings.
Make Active	Set the selected database to Active status.
Remove	Remove the selected databases.

Creating an archive database

To create a new archive database

1 Select **Configuration | Archive Databases**.

2 Click **New**.

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

You can either type the instance name or browse to it. If you browse, you will see all SQL servers in your subnet that are configured to advertise their presence. If you do not see your server on the list, you must type the name.

4 Type a name for the archive database.

5 Select the encryption to use for all data sent from the named server to the Active Administrator archive database.

Strict: Select this option for SQL Server 2022 and Azure SQL Managed Instance or when the instance has **Force Strict Encryption** enabled.

Mandatory: Select this option when the instance has **Force Encryption** enabled. It can also be used when no encryption is configured for the instance, but Trust server certificate is enabled. While this method is less secure than installing a trusted certificate, it does support an encrypted connection.

Optional

6 Enabling **Trust server certificate**, when 'Optional' or 'Mandatory' encryption is selected, or if the server enforces encryption, means that SQL Server will not validate the server certificate on the client computer when encryption is enabled for network communication.

> **NOTE:** If the **Trust Server Certificate** check box is not selected, Active Administrator will walk the validation chain until it finds a valid authority.

7 Under **Host name in the certificate**, you can provide an alternate, yet expected, Common Name (CN) or Subject Alternative Name (SAN) in the server certificate. You would use this option when the server name does not match the CN or SAN, for example, when using DNS aliases.

Leaving this option blank allows certificate validation to confirm that the CN or SAN matches the server name.

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

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

9 Type a name for the archive.

10 Select to make this new archive database active.

   If you do not select the check box, you can make it active at a later time.

11 Type a description.

12 Click **Advanced**.

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

14 Select the security group type for the SQL groups.

   Using the default group types is recommended.

15 If you want to override the default file locations, select the check box and locate paths for the database and log files.

16 Click **OK**.

Modifying archive database settings

To modify an archive database

1 Select **Configuration | Archive Databases**.

2 Select an archive database from the list.

3 Click **Properties**.

4 You can change the Archive Name, encryption settings, Description, and the Active/Inactive status.

5 Click **Test** to check if the server can connect to the selected archive database and to verify that the selected archive database is an Active Administrator® database.

6 Click **OK**.

Migrating data to another database

The Active Administrator® Database Migration Tool helps you migrate data quickly and efficiently from a source database to a target database. For example, you created a new Active Administrator database and want to copy custom reports and alerts from an existing database. Use the Database Migration Tool to copy the existing data to your new database.

NOTE: The source and target databases must exist within the same version of Active Administrator. It is recommended that you back up the target database before you begin the migration.

To use the Database Migration Tool

1 Stop the Active Administrator Foundation and Active Administrator Notification services.

2 Select **Start | Quest | AA Database Migration Tool**.

3 On the **Welcome** page, click **Next**.

4 Type the names or browse to locate the source server and database that contains the data to migrate to the target database.

5 Type the names or browse to locate the target server and database to receive the data from the source database.

6 Click **Next**.

7 Select the data that you want to migrate from the source to the target database.

- To select all the options, click **Select all**.
- To clear all the selections, click **Clear all**.

8 Click **Next**.

9 Review the selections you made.

10 Click **Finish**.

11 After the data migration is finished, you can view details about the migration.

12 Click **Finish**.

13 Start the Active Administrator Foundation and Active Administrator Notification services.

Setting a preferred domain controller

Preferred domain controllers are used when requesting resources from Active Directory®. Normally, Active Directory assigns you the closest domain controller. You can use this feature to specify a domain controller to be used when a domain controller has not already been specified.

NOTE: Preferred domain controllers retrieve objects from Active Directory, such as a list of domain controller or a list of users. If all domain controllers in the domain are required to be scanned, such as the Inactive Accounts feature, the preferred domain controllers are not used.

You can select to verify if a preferred domain controller is offline before use. If the preferred domain controller is offline, you can choose to use the primary domain controller (PDC) of the domain or allow Active Directory to select a domain controller. The offline preferred domain controller is recorded in the server log.

To add preferred domain controllers

1 Select **Configuration | Preferred Domain Controllers**.

2 Click **Add**.

3 Type the name of the domain controller.

-OR-

Browse for and select a domain. Select a domain controller.

4 Click **OK**.

To delete preferred domain controllers

1 Select **Configuration | Preferred Domain Controllers**.

2 Click **Delete All** to delete all domain controllers in the list.

-OR-

Select specific domain controllers, and click **Delete**.

Setting up workstation logon auditing

With workstation logon auditing, you can audit user logon and logoff events including lock and unlock. See Monitoring user logon activity.

Deploying the workstation logon audit agent adds these workstation events to the event definitions:

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

Topics

- Deploying the workstation logon audit agent
- Enabling the default port for the workstation logon auditing agent

Deploying the workstation logon audit agent

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

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

Topics

- Enabling workstation auditing
- Deploying the workstation logon agent from a GPO

Enabling workstation auditing

To enable workstation logon auditing

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

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

3. Click **Save**.

Deploying the workstation logon agent from a GPO

To deploy the workstation logon agent from a GPO

1. Open Windows Explorer.
2. Navigate to C:\Program Files\Quest\Active Administrator\Server\WorkstationLogonAuditAgent.
   - Copy **ActiveAdministrator.admx** to C:\Windows\PolicyDefinitions on a domain controller.
   - Copy **ActiveAdministrator.adml** to C:\Windows\PolicyDefinitions\en-US on a domain controller.
   - Copy **Active Administrator 8.7 Workstation Audit Agent.msi** to a share where everyone has access.
3. Log on to the domain controller where you copied the .ADMX and .ADML files in step 2.

4 Open the Group Policy Management Console (GPMC) and create a new Group Policy Object (GPO), such as *Active Administrator Workstation Logon Agent*.

5 Edit the GPO. Navigate to **Computer Configuration | Policies | Software Settings | Software installation**, right click and choose **New | Package**.

6 Select the **Active Administrator 8.7 Workstation Audit Agent.msi** package that you copied in step 2.

7 Choose the **Assigned** deployment method, and click **OK**.

8 On the same GPO, navigate to C**omputer Configuration | Administrative Templates | Quest Software | Active Administrator**, and edit the **Enable Workstation Audit Agent** setting.

- Select **Enabled**.
- In the **Server Name** box, type the fully qualified domain name (FQDN) of the Active Administrator server.
- In the **Server Port** box, type 15601.

9 Enable the GPO and apply it to the computers where you want to deploy the workstation logon agent.

Enabling the default port for the workstation logon auditing agent

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

To enable the default port

1 On the workstation where the workstation logon auditing agent is installed, start the Windows Firewall with Advanced Security snap-in, right-click on **Outbound Rules**, and choose **New Rule**.

2 Select **Port**.

3 Click **Next**.

4 Select **Specific local ports**, and type **15601**.

5 Click **Next**.

6 Select **Allow the connection**.

7 Click **Next**.

8 Click **Next**.

9 Type a name for the rule, and (optionally) a description.

10 Click **Finish**.

Managing configuration settings

The **Settings** menu offers many options to help you customize and manage Active Administrator®.

Topics

- Setting the Active Administrator server
- Viewing license details
- Running an assessment report

- Scheduling an assessment report
- Running a configuration report
- Managing email addresses
- Scheduling a configuration report
- Checking status of the AFS server

Setting the Active Administrator server

If you have more than one Active Administrator® server, you can switch to another server.

To set the Active Administrator server

1. Select **Settings | AA Server**.
2. Select a connection point from the list.

   –OR-

   Type a server name.

   NOTE: If a connection point is not listed, you must type the server name in the **Server** box. If you do not want to use connection points, you can disable the feature. See Setting general user options.
3. Change the port number if desired.
4. Click **OK**.

Viewing license details

License details include the license type and expiration date. For the Active Administrator® license, you also see the number of licensed servers and users. You can remove a domain from the Active Administrator license.

IMPORTANT: Before removing a domain from the Active Administrator license, you must remove all the domain controllers for the domain. See Managing domain controllers.

NOTE: If you are not compliant with the Active Administrator license, a warning message is sent once a day. In addition, the number of licensed users and enabled users in Active Directory® display at the bottom of the console display. If you click the numbers, the License Dashboard opens.

To view license details

1. Select **Settings | License Dashboard**.
2. Select the license.
   - To remove a selected domain from the Active Administrator license, click **Remove**, and click **Yes**.

Running an assessment report

There are two different reports you run. The **Forest Report** contains information about the forest, sites, domains, and domain trusts. The **Replication Status Report** contains information about the replication status for each domain controller, and errors that occurred during the replication process.

You can send the report by email and/or save it to a file. You also can generate the report in a report editor. To schedule the report, see Scheduling an assessment report.

To send an assessment report by email or save to a file

1 Select **Settings | Assessment Report**.

2 Select a forest**.**

3 **Select the type of report to run: Forest Report or Replication Status Report.**

4 Select **Delivery report**, if necessary.

5 Change the default report name if desired.

6 By default, the date and time are appended to the end of the file name. Clear the check box if you do not want the date and time appended to the file name.

7 By default, a PDF file is created. You can choose a different format.

8 You can send the report by email and save it to a file.

To send an email

a Click **Email**, if necessary.

b By default, the logged in account displays in the **Email Addresses** list. To add more recipients, click **Add**, type the email addresses, and click **OK**.

> **NOTE:** To manage the Forest Assessment Report and the Replication Status Assessment Report email address lists, see Managing email addresses.

c Modify the default subject line if desired.

d Set the priority of the email.

To save the file to a folder

a Click **Save to Folder**.

b Click **Add**.

c Add a path to the location where you want to store the report file.

d Click **OK**.

9 Click **OK**.

To generate an assessment report and display in a report editor

1 Click **Settings | Assessment Report**.

2 Select a forest**.**

3 Select the type of report to run: **Forest Report** or **Replication Status Report.**

4 Select **Interactive**.

5 Click **OK**.

Scheduling an assessment report

To schedule an assessment report

1 Select **Settings | Assessment Report**.

2 Click **Schedule.**

3 To add a new scheduled report, click **Add.**

–OR-

To edit a selected scheduled report, click **Edit.**

4 By default the report is generated and sent by email to the listed recipients and/or copied to a file in the specified location on the **Save to Folder** tab. To disable the schedule, clear the **Enable** check box.

5 Set up the new report or edit the selected report. See Running a configuration report.

- To change the default schedule, click **Set schedule**, set the schedule, click **OK**, and click **Close**.
- To remove a selected scheduled report, click **Remove**.

6 Click **OK**.

Running a configuration report

The configuration report captures all the settings for Active Administrator® servers.

You can send the report by email and/or save it to a file. You also can generate the report in a report editor. To schedule the report, see Scheduling a configuration report.

NOTE: The generation time is dependent on the number of servers. The **Delivery Report** option does not load a report editor and is therefore recommended.

To send a configuration report by email or save to a file

1 Select **Settings | Configuration Report**.

2 Select **Delivery report**, if necessary.

3 Change the default report name if desired.

4 By default, the date and time are appended to the end of the file name. Clear the check box if you do not want the date and time appended to the file name.

5 By default, a PDF file is created. You can choose a different format.

6 You can send the report by email and save it to a file.

To send an email

a Click **Email**, if necessary.

b By default, the logged in account displays in the **Email Addresses** list. To add more recipients, click **Add**, type the email addresses, and click **OK**.

NOTE: To manage the configuration report email address list, see Managing email addresses.

c Modify the default subject line if desired.

d Set the priority of the email.

To save the file to a folder

a Click **Save to Folder**.

b Click **Add**.

c Add a path to the location where you want to store the report file.

d Click **OK**.

7 Click **OK**.

To generate a configuration report and display in a report editor

1 Click **Settings | Configuration Report**.

2 Select **Interactive**.

3 By default, the status of the agent is included. To exclude the agent status, clear the check box.

4 Click **OK**.

Managing email addresses

You can manage the lists of email addresses used when sending most notifications in Active Administrator. The email addresses display as the default in the individual feature. Changes can be made to the lists within the individual feature, so click **Refresh** to load the current email address lists.

Topics

- Managing the AA Owner email address

To manage email addresses

1 Select **Settings | Email Configuration**.

2 Expand the module to view the email lists you can manage. Select the email list to display the email addresses.

Table 118. Email address lists

Module	Email address list	Original email list
AA Owners Address	See Managing the AA Owner email address.	The Active Administrator owner was identified in the AA Configuration Wizard.
Configuration	Service Monitoring Policy	Setting service monitoring policy
	Assessment Report: Forest	Running an assessment report
	Assessment Report: Replication Status	Running an assessment report
	Configuration Report	Running a configuration report
Security & Delegation	Inactive Accounts	Managing inactive accounts
	Password Reminder Settings	Sending password reminders
	Account Expiration	Sending account expiration notifications
	Active Templates	Setting Active Template options
Active Directory Health	Active Directory Health Agent Auto Deploy	Setting up automatic Active Directory Health Analyzer agent deployment
	Active Directory Health Agent Daily Performance	Setting up performance monitoring
	Active Directory Health Agent Notification Settings	Sending agent notifications
	Microsoft Entra Connect Notifications	Viewing Microsoft Entra Connect alerts
	All Active Directory Health Notifications | *notification name*	Creating alert notifications
Certificates	Certificate Settings	Setting up certificate email notifications
Auditing & Alerting	Agent Auto Deploy Configuration	Automating audit agent deployment
	Auditing and Alerting Alerts | *alert name*	Creating an alert

3 Use the tool bar options to manage the lists of email addresses.

Table 119. Email address options

Option	Description
Add	Add email addresses.
Delete	Delete selected email addresses.

Table 119. Email address options

Option	Description
Save	Save the changes on the selected feature. **NOTE:** There is only one email address for **AA Owners Address** so **Save** is the only option. You have options to apply the email address change to the other email lists. See Table 120.
Save All	Save all changes on all features.
Filter	Filter the list of Auditing and Alerting History Items to display specific history items.You can filter by date, date range, and event definition. See Scheduling a configuration report.
Refresh	Refresh the list of email addresses from the Active Administrator database.

Managing the AA Owner email address

The Active Administrator owner was identified in the AA Configuration Wizard. The address of the AA Owner also appears as the default in all email lists. When you change the email address of the AA Owner, you can choose how to apply the new email address in the other email lists. See Table 120.

To manage the AA Owner email address

1 Select **Settings | Email Configuration**.

1 Select **AA Owners Address**.

2 Click **Add**.

3 Type the email address, and click **OK**.

4 Select how to apply the setting. See Table 120.

Table 120. AA Owner Address options

Option	Description
Do not update other settings	Do not change the address of the AA Owner in the other email lists. Only the global AA Owner email is changed.
Overwrite old email with new one in all settings	In all email lists, change the email address of the AA Owner to the new email address.
Add new email in all settings	Keep the old email address of the AA Owner in all email lists and add the new email address.

Scheduling a configuration report

You can schedule the Configuration Report to run at a specified time, to deliver the report by email to specified recipients, and to save the configuration report to a file share.

To schedule a configuration report

1 Select **Settings | Schedule Configuration Report**.

2 Select the check box to enable the schedule.

3 By default, the status of the agent is included. To exclude the agent status, clear the check box.

4 Set the delivery options. See Running a configuration report.

- To change the default schedule, click **Set schedule**, set the schedule, and click **OK**.

5 Click **OK**.

Checking status of the AFS server

To check the status of the Active Administrator® Foundation Server (AFS), you can view real-time events, system logs, or system errors. You can save system logs and errors to a file and clear selected logs to manage disk space utilization.

To check the status of the AFS server

1 Select **Settings | AFS Server Status**.

2 You can view real-time events, system logs, or system errors.

Table 121. AFS server status options

Option	Description
General	View real-time events. The real-time event trace displays 500 events before the display rolls over. You can pause the event trace if you see an item you want to investigate. • To pause the event trace, click **Pause Events**. When you are done examining the list of events, click **Resume Events**. • To select all events to copy to the clipboard, click **Select All Events**. • To clear the display, click **Clear All Events**. • To filter the displayed events, click , and select one or more filters. • To limit the information that displays, click , and select a display option. • To enable verbose logging, click , and click **Enable Verbose Logging**. **NOTE:** Verbose logging can impact performance. It is not recommended that you keep verbose logging enabled.
System Logs	View system logs. • To limit the type of log entries that display, select a category. All log entries display by default. • To filter the displayed log entries, start typing in the box. • To copy the displayed log entries to the clipboard, click **Copy**. • To save the displayed log entries to a .log file, click **Save**. • To clear a selected log, click **Clear Log**.
System Errors	View system errors. • To limit the type of log entries that display, select a category. All log entries display by default. • To filter the displayed log entries, start typing in the box. • To copy the displayed log entries to the clipboard, click **Copy**. • To save the displayed log entries to a .log file, click **Save**.

Setting user options

The Users Options feature provides many options for customizing Active Administrator® to fit your specific environment.

Use the following pages in User Options to customize Active Administrator:

- **General**: set options for the display and audit agents, check for new versions of Active Administrator, and opt in or out of the Software Improvement Program. See Setting general user options.
- **Audit Reports**: set how events display in audit reports. See Setting options for audit reports.

- **User Logon Activity**: set how information displays on the User Logon Activity page. See Setting user log on activity.
- **Active Directory Health Analyzer**: set options for the Active Directory Health Analyzer screens. See Setting Active Directory Health Analyzer options.
- **Advanced**: enable console logging to the AAConsoleLog.log file. See Enabling console logging.

Topics

- Setting general user options
- Setting options for audit reports
- Setting user log on activity
- Setting Active Directory Health Analyzer options
- Enabling console logging

Setting general user options

To set general user options

1. Select **Settings | User Options**.
2. Click **General**, if necessary.
3. Set options for landing pages and active tiles.

   By default, the active tiles on the Home page and landing pages automatically refresh every 30 minutes and rotate every 30 seconds.

   - To disable the refresh and rotation, clear the check box.
   - To modify the values, type in the boxes.
4. By default animation for screen transitions is enabled. To disable animation, clear the check box.
5. By default, the audit agent is loaded when you start Active Administrator. If you want to load the agent manually, clear the check box.
6. By default, active template delegation is not enabled in the Configuration partition in Active Directory®. To enable active template delegation in the Configuration partition in Active Directory, select the check box. See Adding a delegation link.
7. By default, the option to use service connection points is enabled. If you do not want to use connection points when setting the Active Administrator server, clear the check box. See Starting Active Administrator console.
8. Click **OK**.

Setting options for audit reports

You can change how events display in audit reports (**Auditing & Alerting | Audit Reports**). See Managing audit reports for more information on audit reports.

To customize the display of events in audit reports

1. Select **Settings | User Options**.
2. Click **Audit Reports**.
3. By default, events display in local time and use the system settings for the date and time format. You can choose to display events in universal time and set a custom date and time format. The date and time display in the **Time Generated** column on the auditing report.

4 By default, only the latest 100 events display in reports. To change the value, type in the box or use the arrows to increase or decrease the value.

5 By default, only the reports scheduled by the logged on user. To view scheduled reports for all users, select **Show scheduled reports for all users**.

6 Click **OK**.

Setting user log on activity

You can customize the display on the **User Logon Activity** page. See Monitoring user logon activity.

To customize the User Logon Activity page

1 Select **Settings | User Options**.

2 Click **User Log on Activity**.

3 By default, user log on activity is updated automatically when an event occurs. To disable, this feature, clear the check box. You also can disable or enable this feature on the **User Logon Activity** page.

4 By default, all the user log on events are enabled. You can selectively disable or enable specific events.

5 By default, the last 24 hours of events display on the **User Logon Activity** page. To change the value, type in the box.

6 By default, the last 120 hours of user log on activity displays in the log on activity detail for a selected user. To change the value, type in the box.

7 By default, 1000 events display on the **User Logon Activity** page and in the user log on history. To change the value, type in the box.

8 Click **OK**.

Setting Active Directory Health Analyzer options

The Active Directory Health Analyzer is used in the Active Directory Health module to monitor and troubleshoot Active Directory®. See Active Directory Health.

To set Active Directory Health Analyzer options

1 Select **Settings | User Options**.

2 Click **Active Directory Health Analyzer**.

3 By default the Active Directory Health Analyzer screen you are viewing, which is the active screen, is refreshed every 60 seconds. You can turn off the refresh or adjust the refresh rate from 30 to 3600 seconds. If you turn off the refresh, you can refresh the screen manually.

4 By default, the Active Directory Health Analyzer screens are cached. As you view more and more screens on multiple domain controllers, more memory is consumed. To clear the cache, you must restart Active Administrator®. If you turn off the cache, screens are not saved as you navigate from screen to screen.

5 By default, pending Active Directory Health Analyzer alerts display. If you want to view only the alerts, clear the check box.

6 By default, unmonitored domain controllers display in the tree. If you want to view only monitored domain controllers, clear the check box.

7 Click **OK**.

Enabling console logging

To enable console logging

1. Select **Settings | User Options**.
2. Click **Advanced**.
3. By default, console logging is disabled. To enable console logging, select the check box.
   - To view the contents of the AAConsoleLog.log file, click **View Log File**.
4. Click **OK**.

Managing the Active Directory server

Using the AA Server Manager, you can manage the Active Administrator Foundation Service (AFS), the Active Administrator Data Service (ADS), and the Active Administrator Notification Service. You also can enable Full-Text Search, update the Active Administrator license, and configure the web server.

NOTE: The tasks available in AA Server Manager are also available as PowerShell® cmdlets. See Appendix C: PowerShell cmdlets

The AA Server Manager is available from the **Start** menu. You can perform these tasks with AA Server Manager:

- Stopping and starting AFS and ADS services
- Setting the services startup accounts
- Managing logging for services
- Clearing the AFS cache
- Setting port numbers for services
- Enabling Full-Text Search
- Updating Active Administrator licenses
- Managing Security
- Managing Notification Services
- Configuring the Web server

Stopping and starting AFS and ADS services

You can stop and start the Active Administrator Foundation Service (AFS) and the Active Administrator Data Services (ADS).

To stop and start services

1. From the **Start** menu, open **AA Server Manager**, and select the **AFS & ADS Services** tab.

Table 122. Stop and start services

To:	Click:
Stop the AFS service	Stop AFS Service
Start the AFS service	Start AFS Service
Stop the ADS service	Stop ADS Service
Start the ADS service	Start ADS Service

Setting the services startup accounts

You can change the password for the Active Administrator Foundation Service (AFS) and the Active Administrator Data Services (ADS) startup account.

To change the password for the startup account

1. From the **Start** menu, open **AA Server Manager**, and select the **AFS & ADS Services** tab.
2. Click **Set Account**.
3. Type a new password for the account.
4. Click **OK**.

Managing logging for services

You can enable or disable logging of the Active Administrator Foundation Service (AFS) and the Active Administrator Data Services (ADS). You also can view the contents of the log files.

1. From the **Start** menu, open **AA Server Manager**, and select the **AFS & ADS Services** tab.
2. Choose an option:
   - **Enable AFS Logging**
   - **Disable AFS logging**
   - **View AFS Log**
   - **Enable ADS logging**
   - **Disable ADS logging**
   - **View ADS Log**

Clearing the AFS cache

There may be a need to clear the Active Administrator Foundation Service (AFS) cache.

To clear the AFS cache

1. From the **Start** menu, open **AA Server Manager**, and select the **AFS & ADS Services** tab.
2. Click **Clear AFS Cache**.
3. Click **Yes**.

Setting port numbers for services

The default value for the Active Administrator Foundation Service (AFS) port is 15601. The default value for the Active Administrator Data Services (ADS) port is 15602.

To set the port for AFS

1. From the **Start** menu, open **AA Server Manager**, and select the **AFS & ADS Services** tab.
2. Type a value in the **Foundation Service Port Number** box.
3. Click **Set AFS Port**.

To set the port for ADS

1. From the **Start** menu, open **AA Server Manager**, and select the **AFS & ADS Services** tab.
2. Type a value in the **Data Service Port Number** box.
3. Click **Set ADS Port**.

Enabling Full-Text Search

When filtering event descriptions for audit reports (see Creating a new audit report), Active Administrator can use Full-Text Search.

To use this feature, you must first install Full-Text Search, and enable the feature in Active Administrator.
For information on installing Full-Text Search, refer to the documentation for SQL Server® Database Engine.

To enable Full-Text Search

1. From the **Start** menu, open **AA Server Manager**, and select the **AFS & ADS Services** tab.
2. Under SQL Full-Text Search, click **Enable**.

Updating Active Administrator licenses

NOTE: If you are not compliant with the Active Administrator license, a warning message is sent once a day. In addition, the number of licensed users and enabled users in Active Administrator display at the bottom of the console display. If you click the numbers, the License Dashboard opens.

To apply a new license file

1. From the **Start** menu, open **AA Server Manager**, and select the **Licensing & Security** tab.
2. Click **Update License**.
3. To view details about the current license, click **Details**.
4. To update the license, click **Update License**.
5. Locate the license file (*.dlv), and click **Open**.

Managing Security

Active Administrator makes use of FIPS 140-2 compliant software to secure information and includes security management in the Active Administrator Server Manager.

To manage security

1. From the **Start** menu, open **AA Server Manager**, and select the **Licensing & Security** tab.
2. Under **Security Manager**, click **Manage**.

   From here, you can manage the passphrase, file security, and database security

Managing the passphrase

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

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

CAUTION: If the passphrase is lost, it will be impossible to access Active Administrator data. You will have to uninstall Active Administrator, remove all associated files, and start a new installation of Active Administrator. See the Active Administrator Installation Guide for details.

To change a passphrase

1. Under the **Passphrase Management** section, click **Change**.
2. Type the current passphrase.
3. Type a new passphrase that is between 25 and 32 characters in length and then type it again to confirm.
4. Record the passphrase in a secure location.

   CAUTION: You must know the current passphrase to change or restore the passphrase. It is very important to record the passphrase in a secure location where it can be retrieved when required.
5. Click **OK**.
6. Review the informational message.
7. Click **Yes** to proceed.

   The registry files and database will be secured using the new passphrase.
8. Review the reminder to create new backups.
9. Click **OK**.

Managing file security

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

To secure files

1. In the **Files Security Management** section, click **Secure Files**.
2. Type the current passphrase.
3. Click **OK.**

To clean the registry

1. In the **Files Security Management** section, click **Clean Registry**.
2. Review the informational message.
3. Click **Yes** to proceed.

Managing database security

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

To validate the security of a database

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

   - OR -

   Click the ellipsis to browse, select the server, and click **OK**.
2. Type the database name.

   - OR -

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

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

To secure a database

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

- OR -

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

2 Type the database name.

- OR -

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

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

4 Click **Secure Database**.

5 Type the current passphrase.

6 Click **OK.**

Managing Notification Services

To start or stop the Notification Services

1 From the **Start** menu, open **AA Server Manager**, and select the **Other Services** tab.

2 Under **Notification Service**, click **Start** or **Stop** as required.

To change the password for the Notification Service startup account

1 From the **Start** menu, open **AA Server Manager**, and select the **Other Services** tab.

2 Under the Set Notification Service Startup Account option, sclick **Set Account**.

3 Type a new password for the account.

4 Click **OK**.

Configuring the Web server

By default, the port used by the Web server is 8080, logging is enabled, and 7 days of logs are saved. A new log file is created each day and the logs are stored in C:\ProgramData\Quest\Active Administrator\Logs. You can change the port used by the Web server and the logging settings. When you click **OK**, the port is checked to see if it is in use. For example, if the server is running a Web server such as IIS, and you enter port 80, you will receive an error because IIS is already using port 80.

To configure the Web server

1 From the **Start** menu, open **AA Server Manager**, and select the **Other Services** tab.

2 Under **Web Service**, click **Configure**.

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

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

5 Optionally, **Enable Windows Authentication**.

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

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

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

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

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

Optionally, click **Generate** to generate a certificate.

Optionally, click **Browse** to locate a certificate.

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

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

9 Click **OK**.

13

Diagnostic Console

The Diagnostic Console is a powerful diagnostic and resolution tool. Its unique user interface provides a real-time representation of the data flow in your forest, allowing you to detect, diagnose, and resolve Active Directory problems.

IMPORTANT: The Diagnostic Console is not included by default with Active Administrator. To download and install the console search the Knowledge Base articles found on the Quest Support portal.

NOTE:

- The Active Directory Health license is required for the Active Directory Health module. If you do not have a license applied to your installation, the Active Directory Health module will not appear in Active Administrator®.
- To run the Diagnostic Console, the Domain Administrator permission is recommended.
- The Performance Monitor Users and Performance Log Users permissions are the minimum permissions required to collect most, but not all, Active Directory performance data on the target domain controller.
- To collect performance counter values, the Active Administrator Console user account must be a member of the local administrator group on the target domain controller.

The Diagnostic Console offers expert help that explains each process and counter on a domain controller, and what a raised alarm means. The help system offers suggestions on how to resolve the alarm, common solutions, and next steps.

Graphical flows illustrate the rate at which data is moving between domain controller components. Components display the value of key statistics and metrics. The power of the Diagnostic Console lies in its ability to provide visual and audible warnings if performance metrics exceed acceptable thresholds. Components change color to show you the source of the problem.

A range of reports and graphs provide you with detailed information about a domain controller. This information can be viewed on the screen, or printed.

Topics

- Opening the Diagnostic Console
- Using components
- Using indicators
- Using drilldowns

Opening the Diagnostic Console

The Diagnostic Console opens in a separate window. You can move it aside while you work in Active Administrator.

IMPORTANT: To use the Diagnostic Console, you must set a default printer. Windows Server 2016, Windows Server 2019, and Windows Server 2022 set the default printer automatically, but you should verify that it is set.

NOTE: For assistance, use the Help menu within the console. You also can pause the cursor over items to display helpful tips.

To open the Diagnostic Console

- Select a managed domain controller, and click  . See Managing domain controllers.

  -OR-

  Select **Active Directory Health | Analyze**, select a domain controller, and click **Diagnose**.

Using components

The components on the Diagnostic Console home page correspond to the elements of the domain controller that is being diagnosed. Components change color to alert you to specific performance problems.

To see an explanation of the performance, hold the cursor over the component to open a tool tip. To see a definition, click the component to open a help box. From the help box, you can open the associated drilldown to view the associated statistics in table and graph format. See Using drilldowns.

Each component has a right-click shortcut menu from where you can open a help box, show the history in a graph, view details (opens the associated drilldown), restore default settings, view metrics, and view properties.

The home page for the selected domain controller displays the following types of components:

- Network components
- Dataflow components
- LSASS components
- File Replication components
- AD Store components
- Active Directory components
- Operating System components

Network components

To see a definition, click the component to open a help box. From the help box, you can open a drilldown to view the associated statistics. See Using drilldowns.

Table 123. Network components

Network component	Description
Connected Users	The number of clients connected to this server. It does not show users connected to other applications that may be running on this computer; for example, Microsoft® Exchange or SQL Server®. It only shows the users that have established a Microsoft networking connection to the system. This component opens the Network drilldown.
LDAP Client Sessions	The number of LDAP clients that have sessions with this domain controller. This component opens the LDAP drilldown.
Ping Time	The ping time, or average round trip time, from the computer where the Diagnostic Console is running to the connected domain controller. This component opens the Network drilldown.
LDAP Bind Time	The time it took for the last LDAP client to bind to this domain controller. This component opens the LDAP drilldown.
LDAP Search Time	The time taken for a simple LDAP search against the domain controller. The time taken to bind to LDAP is not included in this value, providing a better representation of LDAP search performance.
Theoretical Bandwidth	The level of network traffic graphed against a theoretical maximum bandwidth. The maximum bandwidth is calculated by totaling the capacity of all network devices reported by the operating system. This component opens the Network drilldown.

Dataflow components

Dataflows illustrate the rate at which data is moving through the system and change their speed and color to alert you to performance issues. You can display a dataflow as a flow and graph.

NOTE: Kerberos is the default authentication mechanism in most Active Directory® forests and is more secure than the older NTLM authentication. NTLM authentications are performed in many scenarios. Primarily, they are performed by programs that use LanMan APIs. However, they may also be performed when Kerberos is unavailable or when Kerberos authentication fails.

NOTE: The following dataflow components are not available when running the Diagnostic Console on a server:

- LSASS Kilobytes Read
- LSASS Kilobytes Written
- NTFRS/DFSR Kilobytes Read
- NTFRS/DFSR Kilobytes Written

Table 124. Dataflow components

Dataflow component	Description
Authentications	The number of Kerberos and NTLM Authentications per second handled by the DC. This component should show activity over time. Prolonged periods of high usage or zero activity should be investigated. The PDC Emulator tends to show higher values for Kerberos authentication than other DCs as many older programs only authenticate with a PDC. Client programs can also ask for NTLM authentication as a preference over Kerberos.
Directory Searches	The number of search operations that have been requested by LDAP clients. This component opens the LDAP drilldown.

Table 124. Dataflow components

Dataflow component	Description
Directory Reads	The rate at which clients are reading data from the Active Directory Data Store. Global Catalog servers tend to have higher levels of directory activity than other domain controllers. This component opens the LSASS drilldown.
Directory Writes	The rate at which clients are writing data to the Active Directory Data Store. Global Catalogs tend to see higher levels of directory activity than other domain controllers. This component opens the LSASS drilldown.
DRA Inbound Kbytes	The number of kilobytes per second the server receives through replication. This component opens the Replication drilldown.
DRA Outbound Kbytes	The number of kilobytes per second that the server sends through replication. This component opens the Replication drilldown.
LSASS Kilobytes Read	The number of kilobytes per second that have been read from the Active Directory database by the LSASS process. The LSASS process is the part of Active Directory that is responsible for LDAP requests and for authentication requests. This component opens the LSASS drilldown.
LSASS Kilobytes Written	The number of kilobytes that have been written to the Active Directory database by the LSASS process. The LSASS process is the part of Active Directory that is responsible for LDAP requests and for authentication requests. This component opens the LSASS drilldown.
NTFRS/DFSR Kilobytes Read	The number of kilobytes that have been read from the Active Directory database by the NTFRS or DFSR process (depending on the type of replication service used). The process is the part of Active Directory that is responsible for file replication. This component opens the Activity tab on the Replication drilldown.
NTFRS/DFSR Kilobytes Written	The number of kilobytes that have been written to the Active Directory database by the NTFRS or DFSR process (depending on the type of replication service used). The process is the part of Active Directory responsible for file replication. This component opens the Activity tab on the Replication drilldown.

LSASS components

To see a definition, click the component to open a help box. From the help box, you can open a drilldown to view the associated statistics. See Using drilldowns.

Table 125. LSASS Components

LSASS component	Description
CPU Usage	The total amount of CPU used by the LSASS process. This component opens the LSASS drilldown.
Memory Usage	The total amount of physical memory (RAM) available and the total amount used by the LSASS process. This component opens the All Processes tab on the Performance drilldown.
Replication Queue (DRA)	The number of directory synchronizations queued for this server but not yet processed. This component opens the Replication Queues drilldown.

File Replication components

To see a definition, click the component to open a help box. From the help box, you can open a drilldown to view the associated statistics. See Using drilldowns.

Table 126. File Replication Components

File Replication component	Description
CPU Usage	The total amount of CPU used by the NTFRS or DFSR process (depending on the type of replication service used). If you are using NTFRS and are migrating to DFSR file replication, this counter shows CPU usage for both NTFRS and DFSR services.
Memory Usage	The total amount of physical memory used by the NTFRS or DFSR process (depending on the type of replication service used). If you are using NTFRS and are migrating to DFSR file replication, this counter shows CPU usage for both NTFRS and DFSR services.
Replication Queue	The number of changes to files detected on this domain controller that have not yet been processed for replication. This component opens the Queues tab on the Replication drilldown.

AD Store components

To see a definition, click the component to open a help box. From the help box, you can open a drilldown to view the associated statistics. See Using drilldowns.

Table 127. AD Store Components

AD Store component	Description
Database Size	The total size in megabytes of the file that stores Active Directory®. This file represents all of the data in the Active Directory and will grow as new objects are added.
Free Space	Total drive space available.
Total Space	The total drive space in use where Active Directory is stored.
Objects Applied/Second	The rate at which objects are being applied to the Active Directory database. This component opens the Replication drilldown.
Remaining Objects	The number of object updates remaining in the current replication update packet that have not yet been applied on the local domain controller. This component opens the Replication drilldown.

Active Directory components

The following table describes the Active Directory® components:

Table 128. Active Directory Components

Active Directory component	Description
Replication Links	The number of active replication links for the target domain controller. This component opens the Directory Partners tab on the Replication drilldown.
DNS Entries	Shows whether or not the domain controller has registered the proper DNS entries with its DNS server. The component is running the DNS check from the computer where the Diagnostic Console is running on and not the domain controller to which it is connected. This component opens the DNS drilldown.
Schema Mismatches	The number of replication errors that have occurred as a result of a schema mismatch since the last refresh of the Diagnostic Console.
DRA Errors	The number of replication errors that have occurred since the last refresh of the Diagnostic Console.

Operating System components

The following table describes the operating system components:

Table 129. Operating System Components

Operating system component	Description
CPU Usage	The total amount of CPU being used on the computer being monitored. It includes CPU consumed by all Windows® processes. This component opens the CPU drilldown.
System Disk (Free Space/Total Space)	The total unused disk space on the system disk (the disk that houses the Windows operating system). There should be enough free disk space to accommodate the operational requirements of the Windows operating system. Total space refers to the total size of the system disk.
Physical RAM	The amount of physical memory (RAM) Windows is using. Physical memory usage normally remains close to the total amount of physical memory installed on the system unless the amount of physical memory exceeds the amount of virtual memory that Windows is using. Windows normally keeps some physical memory available for immediate reuse. This component opens the Memory drilldown.
Processor Queue	The number of process threads (program execution units) waiting to be run on all processors. A sustained processor queue length can indicate processor congestion. This component opens the CPU drilldown.
Top CPU Consumer	The process name that is consuming the most CPU on this domain controller. This component opens the Top CPU Consumers tab on the Performance drilldown.
Top Memory Consumer	The process name that is consuming the most physical memory on this domain controller. This component opens the Top Memory Consumers tab on the Performance drilldown.

Using indicators

Indicators give more information about the selected domain controller. The indicator is green if it is active. Hold the cursor over an indicator to see a definition and any current alarms.

Table 130. Indicators

Indicator	Description
ISTG	Indicates if the domain controller is an Intersite Topology Generator (ISTG). An ISTG considers the cost of intersite connections, checks if previously available domain controllers are no longer available, and checks if new domain controllers have been added. The Knowledge Consistency Checker (KCC) then updates the intersite replication topology accordingly.
GC	Indicates if the domain controller is a Global Catalog. The Global Catalog stores full replicas of all object attributes created within the domain and also partial replicas of all object attributes within other domains in the forest.
S	Indicates if the domain controller is the Schema Master for its forest. All changes to the schema of a forest must be made on that computer. There is only one Schema Master for a forest.
D	Indicates if the domain controller is the Domain Naming Master for its forest. Each forest has only one Domain Naming Master. The Domain Naming Master is contacted whenever a new domain is added to the forest to ensure its name is unique.
RID	Indicates if the domain controller is the RID Master for its domain. The RID Master is responsible for handing out RID pools to the other domain controllers in a domain. A RID pool is used to generate RIDs, which are a part of every object created by Active Directory. There is one RID Master per domain.
I	Indicates if the domain controller is the Infrastructure Master for its domain. Each domain has an Infrastructure Master, which is used to maintain the integrity of Active Directory's internal database.
PDC	Indicates if the domain controller is the PDC Emulator for its domain. The PDC Emulator acts like the PDC for pre-Windows® 2000 applications and performs time synchronization for the enterprise. It is contacted by default when other domain controllers in the domain fail to authenticate. Password changes are duplicated here as well. There is one PDC Emulator per Active Directory domain.
RO	Shows if the domain controller is a Read-Only Domain Controller (RODC).

Using drilldowns

Drilldowns display detailed information about the domain controller you are analyzing.

The Diagnostic Console is designed to help you locate and identify problem areas quickly using a visual representation of the major components in the domain controller being monitored. When you have isolated a problem, you can see a detailed breakdown by viewing a drilldown that displays the underlying statistics.

You can display drilldowns by clicking a component in the main screen or by clicking a drilldown button on the toolbar. You can modify the way drilldowns display information.

Each drilldown page contains displays that provide you with specific information about the components of your system. Drilldowns mainly use two different types of displays - tables and charts. Drilldowns have the following features:

- There is more than one way to view a specified drilldown.
- They can be configured to show all or some of the metrics associated with components.
- You can access further information about displays in drilldowns by moving the mouse over the displays, or by clicking or right-clicking on them.
- You can copy the data shown in drilldowns to other applications or save it to a file

The Diagnostic Console provides the following drilldowns:

- Performance drilldown

- Replication drilldown
- Configuration drilldown
- DNS drilldown
- LSASS drilldown
- LDAP drilldown
- FSMO Roles drilldown

Performance drilldown

Displays information on the applications running on a domain controller, including the process name and ID of the application, the percentage of CPU usage, and the physical memory usage in megabytes.

To display the Performance drilldown

1 Click  (Performance).

2 Open the following tabs:

- Top CPU Consumers tab
- Top Memory Consumers tab
- All Processes tab

Top CPU Consumers tab

Displays the top ten CPU-consuming processes running on the selected domain controller.

Table 131. Top CPU Consumer tab

Column	Description
Process Name	The process name of the application.
% CPU	The percentage of CPU that the process is using.

Top Memory Consumers tab

Displays the top ten memory- consuming processes running on the selected domain controller.

Table 132. Top Memory Consumers tab

Column	Description
Process Name	The process name of the application.
Physical Memory (MB)	The amount of physical memory in megabytes that the process is consuming.

All Processes tab

Displays all processes running on the selected domain controller.

Table 133. All Processes tab

Column	Description
Process Name	The process name of the application.
Process ID	The unique ID for the process.
% CPU	The percentage of CPU that the process is using.

Table 133. All Processes tab

Column	Description
Physical Memory (MB)	The amount of physical memory in megabytes that the process is consuming.
Virtual Memory (VB)	The amount of virtual memory in megabytes that the process is consuming.

Replication drilldown

The Replication drilldown displays

- the amount of traffic to and from the domain controller and its replication partners
- the length of the Replication Queue
- the number of updates remaining in the replication packet
- the number of objects received per second from replication partners and applied by the local directory service
- the name, path, size, and staging information for FRS replicas
- the occurrence of any replication collisions

The Diagnostic Console can show one or both of the NTFRS and DFSR actions in the Assistant pane, depending on the state of domains in the current forest. If all domains in the forest have been configured to use entirely NTFRS or DFSR file replication, then only the appropriate action is available. If domains in the forest have been configured to use different services, or if one or more domains in the forest are migrating from NTFRS to DFSR replication, then both actions are available.

The file replication actions available, when you right-click a server, depend on which services are active on the currently selected servers. If the selected servers are running NTFRS or DFSR file replication, then only the appropriate menu entries are available. If the selected servers are running different versions of file replication, or if one or more selected servers are migrating from NTFRS to DFSR file replication, then menu entries for both NTFRS and DFSR actions are available.

To display the Replication drilldown

1 Click  (Replication).

2 Open these tabs:

- Activity tab
- Queues tab
- Directory Partners tab
- FRS Replicas tab
- Collisions tab

Activity tab

Displays graphs that show the amount of inbound and outbound traffic being received and sent by the domain controller to its replication partners.

Table 134. Activity tab graphs

Graph	Description
DRA Activity	Amount of inbound/outbound replication traffic the domain controller is sending and receiving from its replication partners. The graph shows occasional bursts of high activity during replication events followed by periods of zero activity where no replication is taking place. Inbound activity is shown in orange. Outbound activity is shown in blue.
File Replication I/O Activity	Amount of Kbytes/sec that have been read from the Active Directory® database by the NTFRS or DFSR process (depending on the type of replication service used). Read activity is shown in orange, and write activity is shown in blue.
File Replication CPU Usage	Percentage of the CPU used by the NTFRS or DFSR process (depending on the type of replication service used).

Queues tab

Displays graphs that show:

- the length of the replication queue,
- the number of updates remaining in the replication packet, and
- the number of objects received per second from replication partners and applied by the local directory service.

Table 135. Queues tab graphs

Graph	Description
Replication Queues	Number of directory synchronizations queued for the domain controller, but not yet processed. It helps determine the replication backlog; the higher the counter, the higher the backlog. The Objects series indicates the number of Active Directory objects queued for synchronization by the Directory Replication Agent (DRA). The Files series indicates the number of files queued for replication by the NTFRS or DFSR file replication service.
Remaining Objects	Number of object updates remaining in the current replication update packet that have not been applied on the local server.
Objects Applied per Second	Rate at which the objects are applied to the Active Directory database.

Directory Partners tab

NOTE: If two or more links created contain the same information, then only one instance is displayed. If information is coming from a read-only domain controller (RODC), the link entry will be missing. RODCs do not contain naming contexts, and, therefore, will not display link information.

The Directory Partners tab displays the following information about inbound and outbound replication links.

Table 136. Directory Partners tab

Column	Description
Replication Partner	The name of the domain controller with which the server is replicating.
Link Direction	Shows whether replication is inbound (coming to the server from this replication partner) or outbound (going to the indicated replication partner.)
Site	The name of the site where the replication partner is located.

Table 136. Directory Partners tab

Column	Description
IP Address	The IP address of the replication partner.
Enabled/Disabled	Shows whether the connection to the indicated replication partner is enabled or disabled.
Transport Type	The transport type being used for replication.
Options	Shows whether or not the replication link was automatically generated by the Knowledge Consistency Checker (KCC).
Consecutive Failures	The number of consecutive replication errors that have occurred.
Naming Context	The naming context that can be replicated between the replication partner and the currently connected domain controller.
Last Status	The result of the last replication attempt.
Last Replication Attempt	The time at which the last replication was attempted.
Last Successful Replication	The time at which the last successful replication was completed.
Consecutive Failures	The number of consecutive replication errors that have occurred.

FRS Replicas tab

The FRS Replicas tab displays the following information about FRS Replicas.

Table 137. FRS Replicas tab

Column	Description
Replica Name	The display name of the FRS Replica.
Replica Path	The path to the FRS Replica.
Replica Size (MB)	The path to the replica staging folder. This folder acts as a queue for changed files and folders to be replicated to downstream partners.
Replica Staging Path	The size of the FRS Replica.
Replica Staging Size (MB)	The size of the replica staging folder.

Collisions tab

The Collisions tab displays the following information about any collisions that occurred during replication.

Table 138.

Column	Description
Distinguished Name	The distinguished name of the object involved in the replication collision.
Collision Time	The time the collision occurred.

Configuration drilldown

The Configuration drilldown displays information on installed software, hotfixes, and installed network adapters.

To display the Configuration drilldown

1 Click  (Configuration).

2 Open these tabs:

- Installed Hotfixes tab

- Installed Software tab
- Network Adapters tab

Installed Hotfixes tab

The Installed Hotfixes tab displays information on all installed hotfixes. A browser window in the lower half of the tab automatically opens to the corresponding support center home page for the installed operating system. If a specific hotfix is selected, the browser window opens to the Microsoft® Knowledge Base article for that specific hotfix.

Table 139. Installed Hotfixes tab

Column	Description
Name	The name of the installed hotfix
Description	The description for the hotfix
Type	The type of hotfix that is installed
Installed By	The user that installed the hotfix
Installed Date	The date the hotfix was originally installed

Installed Software tab

The Installed Software tab displays the application names of the software installed on a domain controller.

Network Adapters tab

The Network Adapters tab displays the following information on all network adapters installed on a domain controller.

Table 140. Network Adapters tab

Column	Description
Network Card	The display name of the network card.
IP Address	The IP address associated with the network card.
DNS Servers	The DNS Servers associated with the network card. Multiple entries are separated by a | delimiter.
Is DHCP Enabled	Whether DHCP is enabled for the network card.

DNS drilldown

The Domain Naming System (DNS) drilldown indicates whether the DNS entries are registered by the currently connected domain controller, registered by another domain controller in the forest, or not registered at all.

To display the DNS drilldown

- Click  (DNS)

The DNS drilldown displays the following information.

Table 141. DNS drilldown

Column	Description
Record	The name of the DNS record.
Registration Status	Whether the DNS record is registered or not.

LSASS drilldown

The Local Security Authority Subsystem (LSASS) drilldown displays information on database traffic and authentication requests.

To display the LSASS drilldown

- Click  (LSASS)

The LSASS drilldown displays the following information in graphs:

Table 142. LSASS drilldown

Graph	Description
LSASS CPU Usage	The percentage of the CPU used by the LSASS process.
LSASS I/O Activity	How many bytes have been read from or written to the Active Directory database by the LSASS process. Read activity is shown in orange. Write activity is shown in blue.
Authentications	The number of NTLM NT Lan Manager Authentications and Kerberos Authentications per second being handled by the currently connected domain controller. NTLM Authentications are shown in orange and Kerberos Authentications are shown in blue.
Directory Activity	The number of directory read and write operations per second occurring on this domain controller. Read activity is shown in orange, and write activity is shown in blue.

LDAP drilldown

The LDAP drilldown displays detailed information regarding communications between clients and the domain controller.

To display the LDAP drilldown

- Click  (LDAP)

The LDAP drilldown displays the following graphs:

Table 143. LDAP Drilldown

Graph	Description
LDAP Client Sessions	The number of clients that currently have open LDAP sessions with this domain controller.
LDAP Bind Time	The amount of time necessary to perform the last LDAP bind. Consistently high values might indicate a hardware or networking problem.
Directory Searches Per Second	The number of directory searches that are being run per second on this domain controller.
LDAP Search Time	The time taken for a simple LDAP search against the domain controller.

FSMO Roles drilldown

The Flexible Single-Master Operation (FSMO) Roles drilldown indicates which domain controller owns each FSMO role. It also indicates which domain controller is the Global Catalog (GC) server.

To display the FSMO Roles drilldown

- Click  (FSMO Roles)

NOTE: By default, the FSMO Roles drilldown collects only the FSMO roles for the domain where the domain controller is located. Select **Collect FSMO role holders from other domains** to collect all FSMO roles in the forest. If selected, this check box is applied to all current connections as well as new future connections.

The FSMO Roles drilldown displays the following information.

Table 144. FSMO Roles Drilldown

Column	Description
FSMO Role	The five main roles a server can fulfill. These include Domain Naming Master, Schema Master, Infrastructure Master, PDC Emulator, and RID Server. Global Catalog and Intersite Topology Generator are not FSMO roles; they are listed here as extra information.
Domain Controller	The network name of the computer that fulfills the associated FSMO role.
Domain	The name of the domain to which the computer belongs.
Site	The site to which the computer belongs.
IP Address	The IP address of the computer.

a

Alerts Appendix

This appendix provides details on the alerts within the Active Directory Health Analyzer. Along with a detailed description of the event that triggers the alert, a resolution is provided.

Topics

- Domain controller alerts
- Domain alerts
- Site alerts
- Forest alerts
- Microsoft Entra Connect alerts

Domain controller alerts

- Active Directory Certificate Services service is not running
- Active Directory Domain Services is not running
- Active Directory Web Services service is not running
- Consecutive replication failures
- DC cache hits
- DC DIT disk space
- DC DIT log file disk space
- DC LDAP load
- DC LDAP response too slow
- DC Memory Usage
- DC properties dropped
- DC RID pool low
- DC SMB connections
- DC SYSVOL disk space
- DC time sync lost
- Detected NO_CLIENT_SITE record
- DFS Replication service not running
- DFS service is not running
- DFSR conflict area disk space
- DFSR conflict files generated
- DFSR RDC not enabled

- DFSR sharing violation
- DFSR staged file age
- DFSR staging area disk space
- DFSR USN records accepted
- DFSRS CPU load
- DFSRS unresponsive
- DFSRS virtual memory
- DFSRS working set
- DNS Client Service is not running
- Domain controller CPU load
- Domain controller page faults
- Domain controller unresponsive
- File Replication Service is not running
- File replication (NTFRS) staging space free in kilobytes
- GC response too slow
- Group policy object inconsistent
- Hard disk drive
- Intersite Messaging Service is not running
- Invalid primary DNS domain controller address
- Invalid secondary DNS domain controller address
- KDC service is not running
- LSASS CPU load
- LSASS virtual memory
- LSASS working set
- Hard disk drive
- Missing SRV DNS record for either the primary or secondary DNS server
- NETLOGON not shared
- NetLogon service is not running
- Orphaned group policy objects exist
- Physical memory
- Power supply
- Primary DNS resolver is not responding
- Secondary DNS resolver is not responding
- Security Accounts Manager Service is not running
- SRV record is not registered in DNS
- SYSVOL not shared
- W32Time service is not running
- Workstation Service is not running

Active Directory Certificate Services service is not running

Indicates Active Directory® Certificate Services service is currently not running on the domain controller.

Data collector

- **Category**: Windows Services
- **Name:** Active Directory Certificate Services
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions:** When monitored locally or remotely, domain administrator privilege is required.

Description

The Directory Analyzer agent periodically checks to ensure Active Directory Certificate Services is running.

Resolution

Use the Services MCC snap-in or another SCP application to restart Active Directory Certificate Services.

Active Directory Domain Services is not running

Indicates Active Directory® Domain Services is currently not running on the domain controller.

Data collector

- **Category**: Windows Services
- **Name:** Active Directory Domain Service
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions:** When monitored locally or remotely, domain administrator privilege is required.

Description

The Directory Analyzer agent periodically checks to ensure Active Directory Domain Services is running.

The most typical cause of this alert is when a server administrator shuts down the Distributed File System (DFS) service and forgets to restart it.

Resolution

Use the Services MCC snap-in or another SCP application to restart Active Directory Domain Services.

Active Directory Web Services service is not running

Indicates Active Directory® Web Services service is currently not running on the domain controller.

Data collector

- **Category**: Windows Services

- **Name:** Active Directory Web Services
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions:** When monitored locally or remotely, domain administrator privilege is required.

Description

The Directory Analyzer agent periodically checks to ensure Active Directory Web Services is running.

Resolution

Use the Services MCC snap-in or another SCP application to restart Active Directory Web Services.

Consecutive replication failures

Indicates that the number of consecutive replication failures equals or exceeds the configured threshold.

Data collector

- **Category:** General
- **Name:** Consecutive replication failures
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions:** When monitored locally and remotely, only domain user privilege is required. When monitored remotely, the target server must have WMI remote access enabled and the user must be a member of the Distributed COM Users group.

Description

The Directory Analyzer agent constantly monitors replication events on a server. When replication fails too many consecutive times, this alert is issued.

Resolution

- Check connectivity between the domain controller and the replication partner in question. Check to see that the link is reasonably clear, especially during replication (check the replication schedule for the connection).
- Make sure that each partner has adequate CPU and memory resources to ensure timely servicing of replication requests.
- Make sure that the link between partners is adequate for the amount of traffic carried during replication. For example, if thousands of objects are being replicated over a slower connection link, the link should be upgraded, or the replication topology reconsidered.

DC cache hits

Indicates the performance of the server may be degraded because of too few cache read hits.

Data collector

- **Category:** Performance Counters
- **Name:** Cache copy read hits
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions:** When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs User group.

Description

The Directory Analyzer agent monitors the cache copy read hits data collector on the domain controller. If the value of the data collector drops below the configured threshold for a period exceeding the configured duration, the agent sets this alert condition.

Resolution

- Reduced cache hits are due to excessive disk I/O or insufficient memory, or both. When the cache hit percentage drops, the system spends more time waiting for disk accesses to complete, and overall system throughput suffers enormously.
- If possible, try to reduce the number of applications running on the server that is generating disk I/O. If you are running several batch jobs on the server, running them one after the other, rather than all at the same time, may actually be faster.
- You can also try to reduce the number of users accessing the server by moving heavily-used files to other, less-loaded servers.

DC DIT disk space

Indicates that the amount of disk space available on the volume that Active Directory® uses for its database is less than or equal to the configured threshold.

Data collector

- **Category:** General
- **Name:** Active Directory database details
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions:** When monitored locally and remotely, only domain user privilege is required. When monitored remotely, the target server must have WMI remote access enabled and the user must be a member of the Distributed COM Users group.

Description

The Directory Analyzer agent monitors the disk space available on the volume containing the Active Directory database. If the amount of disk space available on this volume drops below the configured threshold for a period exceeding the configured duration, the agent sets this alert condition.

If Active Directory runs out of disk space during processing, it will eventually fail, and the server will shut down immediately.

A low disk space condition can be due to many different things, such as:

- a user copying large amounts of data to the server for temporary storage
- an excessively large print job in the print queue
- an excessively large number of print jobs in the print queue
- a widely distributed email with large attachments arriving on the server from outside

It is also possible that Active Directory may be using up more disk space than normal by importing a large number of objects into the directory through replication or by creating a large number of users or other directory objects.

The directory service agent (DSA) periodically runs a cleanup task that recovers space from deleted objects in the directory for reuse by Active Directory.

Resolution

Check the registry on the server to determine the disk volume that contains the Active Directory database. Under the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters** registry key, the value **DSA Database file** contains the path of the file in which Active Directory keeps its database. If the Active Directory

database is stored on the C: drive and this is the same drive that contains the system TEMP directory (usually C:\TEMP), delete all of the files in the TEMP directory.

Determine what directories are using the most disk space. Using Windows® Explorer, right-click on each directory and select **Properties**. The disk space used by the directory sub-tree will appear on the **Properties** page. After you determine what is causing the directories to grow, run Ntdsutil.exe to compact files, move files to another volume, or move transaction logs to another volume.

CAUTION: Use Ntdsutil with great care. Improper use of Ntdsutil can destroy directory data.

If Active Directory ran low on disk space during a server backup, the problem may be due to the space used by temporary files created by the backup process. If this is the case, you can configure Active Directory to keep its backup files on a different volume.

As a general tip, it is a good idea to put the Active Directory database on its own file volume with only Administrator access so that the disk space available to Active Directory cannot be reduced by other applications.

DC DIT log file disk space

Indicates that the amount of disk space available on the volume Active Directory® uses for its log files is less than or equal to the configured threshold.

Data collector

- **Category:** General
- **Name:** Active Directory database log details
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions:** When monitored locally and remotely, only domain user privilege is required. When monitored remotely, the target server must have WMI remote access enabled and the user must be a member of the Distributed COM Users group.

Description

The Directory Analyzer agent monitors the disk space available on the volume containing the Active Directory log files. If the amount of disk space available on this volume drops below the configured threshold for a period exceeding the configured duration, the agent sets this alert condition.

If Active Directory runs out of disk space during processing, it will eventually fail, and the server will shut down immediately.

A low disk space condition can be due to many different things, such as:

- a user copying large amounts of data to the server for temporary storage
- an excessively large print job in the print queue
- an excessively large number of print jobs in the print queue
- a widely distributed email with large attachments arriving on the server from outside

The directory service agent (DSA) periodically runs a cleanup task that recovers space from deleted objects in the directory for reuse by Active Directory.

Resolution

First, check the registry on the server to determine the disk volume that contains the Active Directory log files. Under the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters** registry key, the value **Database log files path** contains the path of the file in which Active Directory keeps its log files.

If you have recently deleted a large number of objects, you can reclaim disk space from the directory using Ntdsutil.exe to compact files.

CAUTION: Use Ntdsutil with great care. Improper use of Ntdsutil can destroy directory data.

DC LDAP load

Indicates that the amount of Lightweight Directory Access Protocol (LDAP) traffic serviced by the domain controller equals or exceeds the configured threshold.

Data collector

- **Category:** Performance Counters
- **Name:** NTDS LDAP writes a second
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

The Directory Analyzer agent monitors the **NTDS LDAP writes a second** performance counter on the domain controller. If the value goes above the configured threshold for a period exceeding the configured duration, the agent sets this alert condition.

Active Directory® clients use LDAP to communicate with the Directory Service Agent (DSA). A high LDAP load indicates that a lot of clients are making many requests of the DSA. Increased LDAP load can reduce the throughput of the DSA, and can cause important directory transactions, such as login and authentication, to fail.

Resolution

Identify the source of the LDAP traffic by using a network traffic analyzer. Note that a traffic analyzer will not detect the traffic generated by a process running on the domain controller itself.

- If the majority of LDAP traffic is due to a single process, end that process or redirect it to another less loaded server.
- If the traffic is due to many different workstations, the problem may be that there are not enough functioning domain controllers or global catalogs in the site.

DC LDAP response too slow

Indicates that the response time of the domain controller to a Lightweight Directory Access Protocol (LDAP) request equals or exceeds the configured threshold.

Data Collector

- **Category:** General
- **Name:** LDAP response time
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required.

Description

The Directory Analyzer agent periodically issues a simple LDAP query to each domain controller in the site it monitors and measures the time between issuing the LDAP request and receiving a response. An alert is generated if the response time exceeds the configured threshold for longer than the configured duration.

Active Directory® clients use LDAP to communicate with the Directory Service Agent (DSA). A high response time value indicates that the domain controller is not satisfying directory requests quickly, which can result in poor client response times and, if bad enough, login and authentication failures.

Anything that could cause a reduction in overall system performance can increase LDAP response time. For instance, running too many processes, or running processes that use too much memory or CPU can reduce system performance and increase LDAP response times.

A poorly configured server can also increase LDAP response times. For instance, if the paging file is not large enough or if the disks are badly fragmented, poor disk performance can increase LDAP response time.

In some cases faulty hardware can also cause an increase in LDAP response time. For instance, a marginal Network Interface Card (NIC) can reduce network performance on the server, and a failing disk can make directory queries take a long time.

It is possible that the DSA on the domain controller is overloaded by incoming directory requests, by excessive Access Control List (ACL) propagation, or by too many complex directory queries.

Resolution

- Determine if anything is degrading overall system performance, or if just Active Directory performance is poor.
- Check the LDAP load on the server. If this is high, try to identify the traffic that is causing the LDAP load on the server.
- Determine what processes are using the most CPU and generating the most disk I/O.
    - If a single process is generating most of the load, see if that process can be run on a different server.
    - If there are many processes using a significant amount of system resources, try to remove several of them.
    - If Local Security Authority Subsystem Service (LSASS) is using more than its share of server resources, then something is overloading the DSA.

DC Memory Usage

Indicates that the RAM memory usage on the domain controller is greater than 60 percent. The alert becomes critical if the memory usage is greater than 80 percent.

Data collector

- **Category:** Performance Counters
- **Name:** Memory Usage
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

The Directory Analyzer agent monitors the Memory Usage performance counter on the domain controller. If the value of the performance counter goes above the configured threshold for a period exceeding the configured duration, the agent will set this alert condition.

Increased memory usage is a result of running too many applications on the server, or running applications that require too much physical memory.

It is also possible that memory use has increased due to some pathological condition in a particular application. For instance, Active Directory® itself requires substantial resources when it is processing inherited Access Control Lists (ACLs). Active Directory can also require a lot of resources when it processes complex, non-indexed directory searches.

Resolution

First, try to determine if the increased memory use is due to a particular program, or if it is due to running too many programs. Use a utility like Task Manager to inspect the memory usage of all processes on the system. If there are several processes getting more than 60% of the memory, then the problem is most likely due to running too many programs on the server. If possible, stop some of the programs.

If one process is using all of the memory for an extended period of time, it may be due to a bug in the software, or it may be that the program just requires too much memory. If possible, stop the program and run it on a different computer.

DC properties dropped

Indicates directory property updates were dropped during replication.

Data collector

- **Category:** Performance Counters
- **Name:** NTDS DRA inbound properties filtered a second
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

The Directory Analyzer agent monitors the **NTDS\DRA Inbound Properties Filtered\second** performance counter on the domain controller. If the value of the performance counter goes above the configured threshold for a period exceeding the configured duration, the agent sets this alert condition.

During the replication process, Directory Service Agent (DSA) checks each incoming attribute and determines if it was modified subsequent to the version the DSA already has. If the incoming version is later than what the DSA has, the DSA will store the attribute in the directory. If the attribute is the same version or earlier than what the DSA already has, the DSA will drop the attribute, ignoring it for the purposes of replication. This is called a dropped property.

An occasional dropped property is not cause for concern, but a consistent rate of dropped properties may indicate a problem with the replication topology or with the behavior of the domain controllers. A domain controller that is consistently dropping properties during replication is wasting network bandwidth and processing time checking replicated properties that it cannot use.

Resolution

- Wait for several replication cycles to see if the problem clears up by itself.
- If the alert persists, check that the server has good connectivity with each of its replication partners.
- If the alert does not clear by itself in a reasonable amount of time, contact your Microsoft® Windows® support representative.

DC RID pool low

Generated when the available pool of relative identifiers (RIDs) on the selected domain controller is less than or equal to the configured threshold.

Data collector

- **Category:** General
- **Name:** Domain controller relative identifier (RID)

- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required.

Description

Each Directory Analyzer agent monitors the RID pool assigned to the domain controller. If the number of RIDs available to the server goes below the threshold configured by the administrator, the Directory Analyzer agent will issue this alert.

All security principals in the Windows NT Security Architecture are assigned a unique security ID (SID). The SID is made up of a domain identifier and a RID. RIDs are sequential numbers issued by the domain each time a new security principal (for instance a user object) is created in that domain.

Because each domain controller can create security principals, Active Directory® breaks the available range of RIDs into allocation pools that it assigns to each domain controller. Active Directory assigns one domain controller in each domain to be responsible for allocating RID pools to all of the other domain controllers in the domain; this is the RID Operations Master. When a domain controller uses up its allocation, it requests a new range from the RID Operations Master.

If a domain controller has a problem contacting the RID Operations Master, the domain controller can actually use up its entire allocation of RIDs, and be unable to create new security principals, which can result in failures when adding new users, services, and domain controllers to the domain.

Resolution

Contact your Microsoft Windows support representative.

DC SMB connections

Indicates the number of Server Message Block (SMB) connections in use on the domain controller equals or exceeds the configured threshold.

Data collector

- **Category:** Performance Counters
- **Name:** Server sessions
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

The Directory Analyzer agent monitors the Server\Server Sessions performance counter on the domain controller. If the value of the performance counter goes above the configured threshold for a period exceeding the configured duration, the agent will set this alert condition.

System Message Block (SMB) is the protocol for file and print access. Whenever a client workstation accesses files or directories on a server, or whenever the workstation prints a document to a network printer, the client uses an SMB connection.

The number of SMB connections in use on a server is a rough indication of the number of client workstations that are accessing the servers. An unusually high number of SMB connections indicates a large number of clients accessing the server.

A large number of SMB connections will use some amount of memory on the server, though this is generally not a big problem. However, the inordinate number of clients accessing the server can have a negative effect on overall server performance and consequently a negative effect on directory performance as well.

Resolution

Determine if the increased number of SMB connections is degrading the overall performance of the server. If the performance is being affected, you will see other alerts from Active Directory Health Analyzer, including DC LDAP response too slow, Domain controller CPU load, DC cache hits, and Domain controller page faults.

- If you are not getting these additional alerts, the increased number of SMB connections is not adversely affecting the performance of the domain controller. You may wish to increase the threshold for this alert.
- If you are getting these additional alerts, the performance of the DSA is being adversely affected, and you should try to reduce the number of clients connected to the domain controller.

DC SYSVOL disk space

Indicates that the available disk space on the volume host SYSVOL is less than or equal to the configured threshold.

Data collector

- **Category:** General
- **Name:** SysVol details
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required. When monitored remotely, the target server must have WMI remote access enabled and the user must be a member of the Distributed COM Users group.

Description

The Directory Analyzer agent monitors the disk space available on the partition containing the SYSVOL directory. If the amount of free disk space on this partition drops below the threshold set by the administrator for a period exceeding the configured duration, the agent will set this alert condition.

The SYSVOL is a directory that contains user profile information that is replicated (via File Replication Services) to each domain controller in the domain. Although the SYSVOL is not actually part of Active Directory®, a failure in SYSVOL replication can cause user login failures.

Resolution

Find the directory containing the SYSVOL information by checking the registry key **\\HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NetLogon\Parameters** and looking at the value for the **Sysvol** value. This is the path of the SYSVOL directory.

If files in the SYSVOL directory are using the disk space, remove as many of these files as you can.

DC time sync lost

Indicates that the time of the target domain controller differs from one of its reference sources by more than the configured threshold (in seconds).

Data collector

- **Category:** General
- **Name:** Domain controller time synchronization
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required. When monitored remotely, the target server must have WMI remote access enabled and the user must be a member of the Distributed COM Users group.

Description

The Directory Analyzer agent periodically checks its local time against the configured time reference servers. If the time is off by more than the configured threshold (in seconds), the alert is raised.

The Windows® Time (W32Time) service on a domain controller is responsible for maintaining the accuracy of the clock with respect to the time sources. Active Directory® defines rules for time sources as follows:

- A domain controller in a domain will synchronize its clock to the domain controller in the domain that is the PDC Role Owner for its domain, unless the domain controller in question is the PDC Role Owner.
- If the domain controller is the PDC Role Owner, it will synchronize its clock with the PDC Role Owner of its parent domain, unless the domain controller is in the root domain.
- If the domain controller is in the root domain and it is the PDC Role Owner for that domain, it must be configured to synchronize its clock to an external time source.

A special case exists for the PDC Role Owner in domains that are at the root of the forest but are not the root domain (the root domain being defined as the first domain ever created in the forest). These domain controllers synchronize themselves to the PDC Role Owner in the root domain.

Any domain controller can have these settings overridden by configuring the domain controller to synchronize with an external time source using the Net Time command. If the domain controllers are so configured, then the Directory Analyzer agent will check the time against the configured external time source(s).

Resolution

- Ensure that the W32Time service is running on the domain controller that has this alert.
- Check the event log on the domain controller to determine ensure that the W32Time service is not reporting errors.
- Since the domain controller must have connectivity to its time source in order to synchronize its clock, use Active Directory Health Analyzer to determine if other connectivity related alerts may be occurring.

Detected NO_CLIENT_SITE record

Detected NO_CLIENT_SITE record in netlogon.log file.

Data collector

- **Category:** General
- **Name:** NO_CLIENT_SITE record in netlogon.log file
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required. When monitored remotely, the target server must have WMI remote access enabled and the user must be a member of the Distributed COM Users group.

Description

Identifies NO_CLIENT_SITE entries in the Netlogon logs of domain controllers, which helps you detect gaps in your environment where you may have straying clients. Clients that are not assigned to sites will randomly choose a domain controller to authenticate to, which means authentication requests could take much longer than expected.

Resolution

The alert detail indicates the client that is not assigned to a site.

DFS Replication service not running

Indicates that a server hosting Distributed File System (DFS) is running, but the DFS Replication (DFSR) service is not. A DFSR service not running can affect group policies.

Data collector

- **Category:** Windows Services
- **Name:** DFS Replication Service
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally, only domain user privilege is required. When monitored remotely, domain administer privilege is required.

Description

The Directory Analyzer agent periodically queries the Service Control Manager (SCM) to determine if the DFS Replication service is up and running. If the service is available on the domain controller, but it is currently not running, the agent issues this alert.

DFS Namespaces and DFS Replication offer simplified but highly-available access to files, load sharing, and WAN-friendly replication.

The most typical cause of this alert is when a server administrator shuts down the DFS service and forgets to restart it.

Resolution

- Check the status of the service by running the Services MMC snap-in. Select the Server DNS (not DNS Client) entry. If the status is stopped, then the service is actually down.
- If the DFS service is stopped, use the Services MCC snap-in or another SCP application to restart the DFS Service. Check the Event Logs and fix any problems indicated by the logs.

DFS service is not running

Indicates the Distributed File System (DFS) Namespace Service is stopped.

Data collector

- **Category:** Windows Services
- **Name:** DFS Namespace Service
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally, only domain user privilege is required. When monitored remotely, domain administrator privilege is required.

Description

The Directory Analyzer agent periodically checks to ensure the DFS Namespace Service is running.

Resolution

Use the Services MCC snap-in or another SCP application to restart the DFS Namespace Service.

DFSR conflict area disk space

Detects that the amount of disk space allocated for conflict files during replication is less than or equal to the specified threshold.

Data collector

- **Category:** Windows Services
- **Name:** DFSR conflict area disk space
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

If the ConflictAndDeleted folder runs out of space, DFS Replication removes older conflicting or deleted files to free up disk space, which might temporarily decrease replication performance.

If a staging folder quota is configured to be too small, DFS Replication might consume additional CPU and disk resources to regenerate the staged files. Replication might also slow down because the lack of staging space can limit the number of concurrent transfers with partners. Increasing the size of the staging folder and the ConflictAndDeleted folder can increase replication performance and the number of recoverable conflicting and deleted files.

Resolution

Delete files from the ConflictAndDeleted folder or increase the quota of the ConflictandDeleted folder for the appropriate replicated folder(s).

Related article

https://msdn.microsoft.com/en-us/library/cc754229(v=ws.11).aspx

DFSR conflict files generated

Indicates that there are conflicted files in the ConflictAndDeleted folder assigned to the replicated folder.

Data collector

- **Category:** Windows Services
- **Name:** DFSR conflict files generated
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

Monitoring this performance counter enables administrators to keep track of the number of replication conflicts generated for replicated folders on the monitored computer. Monitoring the space utilization of the Conflict and Deleted area helps ensure that there is enough space to store replication conflicts and files deleted from replicated folders on the monitored computer. You can view a log of conflict files and their original file names by viewing the ConflictandDeletedManifest.xml file in the DfsrPrivate folder.

Frequent conflicts indicate that files in a replicated folder are frequently being modified on multiple servers in a short period.

Resolution

In general, resolution of this alert condition involves deciding whether a conflict object contains useful information, moving that information into a different directory object, and then deleting the object. Determining whether the conflict object has any useful information is up to you, the administrator.

DFSR RDC not enabled

Indicates that any of Distributed File System Replication (DFSR) connections have the Remote Differential Compression (RDC) option disabled.

Data collector

- **Category:** Windows Services
- **Name:** DFSR RDC not enabled
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

Remote Differential Compression (RDC) only updates changes to files, which is useful when replicating across a wide area network.

Resolution

Enable Remote Differential Compression.

DFSR sharing violation

Indicates that a sharing violation exists for a period greater than or equal to the specified threshold.

Data collector

- **Category:** Windows Services
- **Name:** DFSR sharing violation
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

The Directory Analyzer agent monitors the DFRS debug log for reports of sharing violations. If the sharing violation exists for a period exceeding the configured duration, the agent sets this alert condition.

One possibility for the sharing violation is that other sources may have opened the file to be replicated on the target computer.

Another possibility for a sharing violation is that other sources have open handles to the file to be replicated. Typically, programs that can instigate sharing violations are:

- Antivirus programs
- Disk optimization tools
- File system policies that repeatedly apply access control list (ACL) changes
- A user profile or personal data that is constantly in use that is placed on the replica set

- Any other type of data that is held open for long periods by an end user, a program, or a process

Resolution

- Rename the locked file.
- Identify the locked files and release the handles.

Related article

https://support.microsoft.com/en-us/help/822300/frs-encounters-error-sharing-violation-errors-when-it-tries-to-replicate-data-that-is-still-in-use

DFSR staged file age

Indicates that the age of files in the Distributed File System Replication (DFSR) staging folder is greater than or equal to the specified threshold.

Data collector

- **Category:** Windows Services
- **Name:** DFSR staged file age
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

The Directory Analyzer agent monitors the age of files in the DFRS staging area. If the file is older than the configured time then the alert condition is set.

This problem could be caused by the following factors:

- The replication schedule is too short to allow all data to replicate to other members.
- Network bandwidth is affecting the speed at which files replicate, causing a delay.
- A downstream partner is unavailable due to network problems or other issues.
- Possibly caused by a non-authoritative restore (also called D2) on a downstream partner.

Resolution

If a D2 was not performed on a downstream partner, look for failure indicators at either the upstream or downstream partners. If you cannot find failure indicators, re-examine the schedule and network bandwidth on this connection to ensure that enough replication time is scheduled to allow the data to replicate.

DFSR staging area disk space

Indicates that the amount of disk space allocated for staging files during replication is less than or equal to the specified threshold.

Data collector

- **Category:** Windows Services
- **Name:** DFSR staging area disk space
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022

- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

The Directory Analyzer agent monitors the DFSR staging area disk space performance counter on the domain controller. If the value of the performance counter drops below the configured threshold for a period exceeding the configured duration, the agent will set this alert condition.

If the File Replication Service (FRS) runs out of staging disk space, replication will stop. The size of the contents of the staging areas for all active replication sets are subtracted from the user controlled size.

A low disk space condition can be due to many different things. Some possibilities are: the size of the data to be replicated is larger than the staging area, there are too many replica sets active at once, or there are files destined for one or more out-bound partners that have not been connected for a while.

Resolution

- Increase the amount of space allowed for file staging.
- Check replication schedules and connectivity between partners.

Related article

https://msdn.microsoft.com/en-us/library/cc754229(v=ws.11).aspx

DFSR USN records accepted

Detects that there is heavy file replication traffic.

Data collector

- **Category:** Windows Services
- **Name:** DFSR USN records accepted
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

The Directory Analyzer agent monitors the **DFSR USN records accepted** performance counter on a domain controller. The agent will set this alert condition if the value of this performance counter goes above the configured threshold for a period exceeding the configured duration.

Replication is triggered by entries to the NTFS update sequence number (USN) change journal. A high value on this counter, such as one every five seconds, indicates heavy replication traffic and may result in replication latency.

NOTE: You can adjust the volume instance for the DFS Replication Service. See Setting alerts.

Resolution

None.

DFSRS CPU load

Indicates that the CPU for the Distributed File System Replication (DFSR) service is too busy.

Data collector

- **Category:** Performance Counters
- **Name:** DFSRS % processor time
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

The Active Administrator Foundation Service (AFS) periodically checks the CPU utilization by the DFSR service. If the utilization is above the configured threshold, an alert is generated.

Resolution

Wait for a while to see if the error clears itself. For example, a high CPU utilization that occurs during an initial replication is transitory in nature.

Review the system configuration and tune the environment to optimize DFSRS performance.

DFSRS unresponsive

Indicates that the DFS Replication Service (DFSRS) is unresponsive on the domain controller.

Data collector

- **Category:** General
- **Name:** DFSRS unresponsive
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally, only domain user privilege is required. When monitored remotely, the target server must have WMI remote access enabled and the user must be a member of the Distributed COM Users group.

Description

The Directory Analyzer agent periodically checks to ensure that the DFS Replication Service (DFSRS) is responsive. If the DFSRS is unresponsive while listed as running in the services list, the alert condition is set.

Resolution

Review the system configuration and tune the environment to optimize the DFS Replication Service (DFSRS). To do this, review the event logs for DFSRS-related errors and warnings and validate that sufficient resources are available.

DFSRS virtual memory

Indicates that the virtual memory allocated to the Distributed File System Replication Service (DFSRS) is too high.

Data collector

- **Category:** Performance Counters
- **Name:** DFSRS private bytes
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

The Directory Analyzer agent monitors the **DFSRS private bytes** performance counter on the domain controller for the DFS Remote Service. If the value in the performance counter goes above the configured threshold for a period exceeding the configured duration, the agent will set this alert condition.

Resolution

Review the system configuration and tune the environment to optimize DFSRS performance as described in these references:

- https://blogs.technet.microsoft.com/askds/2010/11/01/common-dfsr-configuration-mistakes-and-oversights/

DFSRS working set

Indicates that the working set allocated to the DFS Replication service is too high.

Data collector

- **Category:** Performance Counters
- **Name:** DFSRS working set
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

The Directory Analyzer agent monitors the **DFSRS working set** performance counter on the domain controller for the DFSR service. If the value in the performance counter goes above the configured threshold for a period exceeding the configured duration, the agent will set this alert condition.

Resolution

Review the system configuration and tune the environment to optimize DFSRS performance as described in these references:

- https://blogs.technet.microsoft.com/askds/2010/11/01/common-dfsr-configuration-mistakes-and-oversights/

DNS Client Service is not running

Indicates the DNS Client Service is currently not running on the domain controller.

Data collector

- **Category**: Windows Services
- **Name:** DNS Client
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions:** When monitored locally or remotely, domain administrator privilege is required.

Description

The Directory Analyzer agent periodically checks to ensure DNS Client Service is running.

Resolution

Use the Services MCC snap-in or another SCP application to restart the DNS Client Service.

Domain controller CPU load

Indicates that the CPU for the domain controller is too busy, which may indicate a problem with directory service or it can indicate that a problem may occur because the domain controller cannot respond to requests quickly enough.

Data collector

- **Category:** Performance Counters
- **Name:** CPU Processor time
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

The Directory Analyzer agent monitors the **Processor\% Processor Time** performance counter on the domain controller. If the value of the performance counter goes above the configured threshold for a period exceeding the configured duration, the agent will set this alert condition.

Increased CPU load is a result of running too many applications on the server, or running applications that require too much CPU time.

It is also possible that the CPU load has increased due to some pathological condition in a particular application. For instance, Active Directory® itself requires substantial CPU resources when it is processing inherited Access Control Lists (ACLs). Active Directory can also require a lot of CPU resources when it processes complex, non-indexed directory searches.

Resolution

First, try to determine if the increased CPU load is due to a particular program, or if it is due to running too many programs. Use a utility like Task Manager to inspect the CPU usage of all processes on the system. If there are several processes getting more than 10% of the CPU, then the problem is most likely due to running too many programs on the server. If possible, stop some of the programs.

If one process is using all of the CPU for an extended period of time, it may be due to a bug in the software, or it may be that the program just requires too much CPU. If possible, stop the program and run it on a different computer.

Domain controller page faults

Indicates that the performance of the server may be degraded because of too many page faults.

Data collector

- **Category:** Performance Counters
- **Name:** Memory page faults a second
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

The Directory Analyzer agent constantly monitors the **Page Faults/sec** performance counter on the domain controller. If this number exceeds the configured threshold, the agent will issue an alert.

A page fault occurs whenever the operating system tries to access a virtual memory page that is not currently in memory or is in the incorrect place in memory. The process requesting the page must wait while the operating system makes room for the requested page in memory and reads it from disk or relocates it, which may cause a significant delay for the faulting process. If many processes are causing page faults, a condition known as thrashing can occur. If this happens, the performance of the server goes to zero as the operating system spends most of its time managing memory and very little running applications.

A continuously high page fault rate is an indication that the server is running too many processes with insufficient real memory. If left unattended, Active Directory® performance will suffer greatly, and eventually the directory system agent (DSA) will be unable to service requests, which can result in failed logins and authentications, as well as the inability of some applications and services to run at all.

Resolution

First, determine if the page fault rate is too high or if the threshold is set too low. Assess the overall performance of the server while the page fault rate is high. If the performance seems adequate, increase the threshold; if the performance seems poor, try to reduce the page fault rate.

To reduce the page fault rate on the server, determine if the page faults are due to a single process or a combination of several processes.

1. Run the Windows NT Task Manager and open the **Processes** tab.
2. Select **View | Select Columns**.
3. Select **Memory Delta** and **Page Fault Delta**, if necessary.
4. Observe the numbers to determine if there is one process generating page faults, or if there are several.

If there is only one process, run that program on another server or at a different time when the server is not as loaded.

If there are several processes that are generating high page fault rates, you will either have to run some of them on another server, or you will have to add more RAM to the server.

Domain controller unresponsive

Indicates that the domain controller is unresponsive.

Data collector

- **Category:** General
- **Name:** Domain controller unresponsive
- **Supported on:** Windows Server 2016, and Windows Server 2019
- **Required permissions**: Domain user privilege required.

Description

Active Administrator Data Service (ADS) periodically monitors TCP port 135. If ADS cannot connect to port 135, the alert is triggered.

This error can occur if any of the following occurs:

- The indicated server is not actually a domain controller.
- The domain controller no longer has connectivity to the network.
- The DNS records for the domain controller are incorrect.
- Active Directory on the domain controller has failed in some way.

- Active Directory on the domain controller is overloaded and is taking too long to respond.
- The domain controller is not running.

Resolution

- Make sure the indicated server is actually a domain controller. If it is not, run NTDSUTIL and select the metadata cleanup option to clean up the erroneous objects in the directory.
- Make sure the domain controller is running. If the domain controller is not running, start it.
- Ping the domain controller to see if there is connectivity. If there is not, fix that problem. The problem may be that DNS has the incorrect address or that the IP stack for the domain controller is misconfigured.
- Check the LDAP response time for the domain controller. If it is too high, you may need to add another domain controller for the same domain in the same site.
- If the domain controller is also a global catalog, you may need to add another global catalog to the site.

File Replication Service is not running

Indicates the File Replication Service is currently not running on the domain controller.

Data collector

- **Category**: Windows Services
- **Name:** File Replication Service
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions:** When monitored locally or remotely, domain administrator privilege is required.

Description

The Directory Analyzer agent periodically checks to ensure the File Replication Service is running.

Resolution

Use the Services MCC snap-in or another SCP application to restart the File Replication Service.

File replication (NTFRS) staging space free in kilobytes

Indicates that the amount of disk space allocated for staging files during replication is less than or equal to the specified threshold.

Data collector

- **Category:** Performance Counters
- **Name:** File replication staging space free in kilobytes
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

The Directory Analyzer agent monitors the **FileReplicaSet\KB of Staging Space Free** performance counter on the domain controller. If the value of the performance counter drops below the configured threshold for a period exceeding the configured duration, the agent will set this alert condition.

If the File Replication Service (FRS) runs out of staging disk space, replication will stop. The size of the contents of the staging areas for all active replication sets are subtracted from the user controlled size.

A low disk space condition can be due to many different things. Some possibilities are:

- The size of the data to be replicated is larger than the staging area
- There are too many replica sets active at once
- There are files destined for one or more out-bound partners that have not been connected for a while

Resolution

One possible solution is to increase the amount of space allowed for file staging.

1. Determine that the number and size of the files that need replicating will fit in the amount of space allocated. The staging areas can be found by searching the registry.

   The **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NtFrs\Parameters\ReplicaSet** registry key contains one or more sub-keys using a GUID as the key name for each active replica set. Each replica set contains both a **Replica Set Root** and **Replica Set Stage** value.

   - The **Replica Set Root** value describes the file system folder that will be replicated.
   - The **Replica Set Stage** value describes the folder that is used for the staging area. The staging areas can be inspected to determine which one(s) are consuming disk space.

2. Check the amount of space allocated by viewing the **Staging Space Limit in KB** value under the **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NtFrs registry key**. This value defines the maximum amount of disk space that can be consumed by all staging areas at any one time.
3. If you determine that the staging areas need more disk space, increase the value of the **Staging Space Limit in KB**.

If the problem cannot be resolved by adjusting the amount of space needed and allowed, turn your attention towards replication schedules and the connectivity between computers. The SYSVOL share is replicated between all domain controllers in the same domain. Other replication partners can be found using the Distributed File System (DFS) console.

1. Check that the server has good connectivity with each of its replication partners. Ping the replication partners from the domain controller that issued this alert to determine if there is connectivity. The problem may be that DNS has the incorrect address or that the IP stack for the domain controller or the Directory Analyzer agent is misconfigured.
2. Use the Active Directory® Sites and Services snap-in to confirm that replication schedules allow replication partners to communicate.

GC response too slow

Indicates that the response time of the servers that host the replica of the Global Catalog (GC) equals or exceeds the configured threshold value.

Data collector

- **Category:** Performance Counters
- **Name:** NTDS LDAP searches a second
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

The Directory Analyzer agent periodically issues a query against a well-known object in the GC and records the time that it takes to receive a response. If the time taken exceeds the configured threshold for a period exceeding the configured duration, the agent will set this alert condition.

This error can occur if any of the following occurs:

- The indicated domain controller does not exist.
- The server might not host the replica of the Global Catalog.
- The domain controller no longer has connectivity to the network.
- The DNS records for the domain controller are incorrect; e.g., the IP address for the domain controller is not what is published in DNS as viewed by the Directory Analyzer agent.
- Active Directory® on the domain controller has failed in some way.
- Active Directory on the domain controller is overloaded and is taking too long to respond.
- The domain controller is not running.

Resolution

Make sure the indicated domain controller actually exists. If it is not, run NTDSUTIL and select the metadata cleanup option to clean up the erroneous objects in the directory.

Make sure the domain controller is running. If the domain controller is not running, start it.

Make sure the domain controller hosts a replica of the Global Catalog.

Ping the domain controller to see if there is connectivity. If there is not, fix that problem. The problem may be that DNS has the incorrect address or that the IP stack for the domain controller or the Directory Analyzer agent is misconfigured.

Check the LDAP response time for the domain controller on the Active Directory Health Analyzer Summary tab for the domain controller. If the LDAP response time is too high, you may need to add another domain controller for the same domain in the same site.

If this is the only server that hosts a replica of global catalog, you may need to add another global catalog to the site.

Group policy object inconsistent

Indicates the Group Policy object (GPO) for a given policy has fallen out of sync with the representation stored on the local SYSVOL share.

Data collector

- **Category: General**
- **Name:** Group policy object inconsistent
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Permission requirements:** When monitored locally and remotely, only domain user privilege is required.

Description

The Directory Analyzer agent periodically compares the directory representation of GPOs in a domain to their representation on the local SYSVOL. This alert is active when the version number stored in SYSVOL differs from the version number expected in the local directory. This situation typically arises from high replication latency or duplicated NTDS Connection Objects.

Resolution

A Group Policy Object on <*server-name*> is represented inconsistently between the local directory and the local file system. This problem can be remedied by forcing NTFRS and Active Directory® to refresh.

Hard disk drive

Indicates that issues have been detected for the hard disk drive on the domain controller.

Data collector

- **Category:** General
- **Name:** Hard drive failed
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Not supported on**: Virtual computers
- **Required permissions**: When monitored locally, only domain user privilege is required. When monitored remotely, the target server must have WMI remote access enabled and the user must be a member of the Distributed COM Users group.

Description

The Active Directory Health agent monitors the *Hard drive failed* data collector on the domain controller. When the hard disk drive of the selected domain controller has a status other than OK for a period of time equal to or longer than the configured threshold, this alert is raised.

Resolution

Review the device configuration and contact your hardware vendor if required.

Intersite Messaging Service is not running

Indicates the Intersite Messaging Service is currently not running on the domain controller.

Data collector

- **Category**: Windows Services
- **Name:** Intersite Messaging
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions:** When monitored locally or remotely, domain administrator privilege is required.

Description

The Directory Analyzer agent periodically checks to ensure the Intersite Messaging Service is running.

Resolution

Use the Services MCC snap-in or another SCP application to restart the Intersite Messaging Service.

Invalid primary DNS domain controller address

Indicates that the primary DNS service is reporting one or more invalid IP addresses for domain controllers in the domain in which the DNS server is located. An invalid IP address can cause the domain controller to be unreachable by some or all clients.

Data collector

- **Category:** General
- **Name:** Invalid primary DNS domain controller address
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required. When monitored remotely, the target server must have WMI remote access enabled and the user must be a member of the Distributed COM Users group.

Description

Active Directory Health Analyzer queries DNS for the Service (SRV) records and compares the results to the IP address reported by the Directory Analyzer agent hosted on the domain controller. This alert is raised if the address retrieved in the DNS query is malformed, does not exist, or does not match the address reported by the agent.

This alert is accompanied by a list of aberrant DNS SRV entries. Each entry consists of an IP address and a DNS name delimited by a single space. For example:

```
194.165.85.104 mothra.destroy.all.monsters.com
194.165.85.99 gammra.destroy.all.monsters.com
```

Typically, this alert condition is raised due to invalid SRV entries in the DNS database file, or interrupted connectivity between the domain controller and the DNS Server. This condition may also occur if a domain controller is configured to obtain its IP address dynamically (via DHCP). If the DNS server is either not configured to use Dynamic DNS or does not recognize the new lease once the domain controller is rebooted, an alert is raised. Note that it is strongly recommended that the IP addresses of all domain controllers be statically assigned.

Resolution

Reconcile the DNS SRV entries with the IP address reported by the network adapter (or by DHCP, if applicable). The SRV entries appear under **_ldap._tcp.dc._msdcs.<zone-name>** in the DNS Management Console.

Invalid secondary DNS domain controller address

Indicates that the secondary DNS service is reporting one or more invalid IP addresses for domain controllers in the domain in which the DNS server is located. An invalid IP address can cause the domain controller to be unreachable by some or all clients.

Data collector

- **Category:** General
- **Name:** Invalid secondary DNS domain controller address
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required. When monitored remotely, the target server must have WMI remote access enabled and the user must be a member of the Distributed COM Users group.

Description

Active Directory Health Analyzer produces this alert by querying DNS for the Service (SRV) records and compares the results to the IP address reported by the Directory Analyzer agent hosted on the domain controller. This alert is raised if the address retrieved in the DNS query is malformed, does not exist, or does not match the address reported by the agent.

This alert is accompanied by a list of aberrant DNS SRV entries. Each entry consists of an IP address and a DNS name delimited by a single space. For example:

```
194.165.85.104 mothra.destroy.all.monsters.com
194.165.85.99 gammra.destroy.all.monsters.com
```

Typically, this alert condition is raised due to invalid SRV entries in the DNS database file, or interrupted connectivity between the domain controller and the DNS Server. This condition may also occur if a domain controller is configured to obtain its IP address dynamically (via DHCP). If the DNS server is either not configured to use Dynamic DNS or does not recognize the new lease once the domain controller is rebooted, an alert is raised. Note that it is strongly recommended that the IP addresses of all domain controllers be statically assigned.

Resolution

Reconcile the DNS SRV entries with the IP address reported by the network adapter (or by DHCP, if applicable). The SRV entries appear under **_ldap._tcp.dc._msdcs.<zone-name>** in the DNS Management Console.

KDC service is not running

Indicates the Kerberos Key Distribution Center (KDC) service is not currently running on the domain controller.

Data collector

- **Category:** Windows Services
- **Name:** Kerberos Key Distribution Center Service
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally, only domain user privilege is required. When monitored remotely, domain administrator privilege is required.

Description

The Directory Analyzer agent periodically checks to ensure that the KDC service is running.

Resolution

Use the Services MCC snap-in or another SCP application to restart the KDC service.

LSASS CPU load

Indicates that the CPU for the Local Security Authority Service (LSASS) service on the domain controller is too busy, which can indicate a problem with directory service.

Data collector

- **Category:** Performance Counters
- **Name:** LSASS % processor time
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

The Directory Analyzer agent monitors the **Process(lsass)\% Processor Time** performance counter on the domain controller for the LSASS service. If the value of the performance counter goes above the configured threshold for a period exceeding the configured duration, the agent will set this alert condition.

LSASS virtual memory

Indicates that the virtual memory used for Local Security Authority Service (LSASS) on the domain controller is above the preset threshold.

The amount of memory used for LSASS varies depending on the load of the computer. As the number of running threads increases, so does the number of memory stacks. Lsass.exe usually uses 100 MB to 300 MB of memory. Lsass.exe uses the same amount of memory no matter how much RAM is installed in the computer. However, when a larger amount of RAM is installed, Lsass.exe can use more RAM and less virtual memory.

NOTE: Alert threshold defaults should be reviewed and adjusted based on your environment as a number of thresholds are impacted by factors such as server hardware and size of Active Directory.

Data collector

- **Category:** Performance Counters
- **Name:** LSASS private bytes
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be a part of the Performance Logs user group.

Description

The Directory Analyzer agent monitors the **Process(lsass)\Virtual Memory** performance counter on the domain controller for the lsass service. If the value in the performance counter goes above the configured threshold for a period exceeding the configured duration, the agent will set this alert condition.

This problem may occur when event tracing for Security Accounts Manager (SAM) events is enabled. When event tracing for SAM events is enabled, the remote procedure call (RPC) binding is not released. Therefore, a memory leak occurs in the Lsass.exe process.

LSASS working set

Indicates that the working set memory used for Local Security Authority Service (LSASS) on the domain controller is above the preset threshold.

The amount of memory used for LSASS varies depending on the computer's load. As the number of running threads increases, so does the number of memory stacks. LSASS.exe usually uses 100 MB to 300 MB of memory. Lsass.exe uses the same amount of memory no matter how much RAM is installed in the computer. However, when a larger amount of RAM is installed, Lsass.exe can use more RAM and less virtual memory.

Data collector

- **Category:** Performance Counters
- **Name:** LSASS working set
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required and the user must be part of the Performance Logs user group.

Description

The Directory Analyzer agent monitors the **Process(lsass)\Working Set** performance counter (corresponding to Mem Usage from Task Manager) on the domain controller for LSASS. If the value in the performance counter goes above the configured threshold for a period exceeding the configured duration, the agent will set this alert condition.

It is also possible that the number of bytes allocated to the working set has increased to some pathological condition in a particular application.

Resolution

Please refer to the Microsoft knowledge base article listed below.

Related articles

- https://support.microsoft.com/en-us/help/3155218/memory-leak-occurs-in-the-lsass.exe-process-after-you-install-security-update-3067505-in-windows

Missing SRV DNS record for either the primary or secondary DNS server

Indicates one or more requisite Domain Name System (DNS) Service (SRV) entries are not defined. DNS SRV entries are vital to the proper functioning of Active Directory®.

Data collector

- **Category:** General
- **Name:** Missing domain controller SRV DNS record
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required. When monitored remotely, the target server must have WMI remote access enabled and the user must be a member of the Distributed COM Users group.

Description

Active Directory Health Analyzer queries the DNS service for the SRV entries required for each zone hosted on the server. Note that this applies exclusively to zones designated as primary. If any of the SRV entries are not present, this alert is raised. Active Directory Health Analyzer does not evaluate SRV entries for accuracy, but only checks if the entries are present.

Active Directory Health Analyzer confirms the existence of the following SRV entries for each zone hosted on the server:

```
_ldap._tcp.<zone-name>
_ldap._tcp.dc._msdcs.<zone-name>
_ldap._tcp.pdc._msdcs.<zone-name>
_kerberos._tcp.<zone-name>
_kerberos._udp.<zone-name>
_kerberos._tcp.dc._msdcs.<zone-name>
_kpasswd._tcp.<zone-name>
_kpasswd._udp.<zone-name>
```

This alert is accompanied by a list of the missing SRV entries.

Whenever a domain controller is promoted, the Microsoft NetLogon process registers the applicable SRV entries with the primary DNS server of the affected domain. As SRV entries are used to identify the constituent domain controllers, the Primary Domain Controller(PDC), and the owner of the global catalog of each zone, the absence of an SRV entry can have serious consequences for Active Directory.

The presence of all requisite SRV locator entries is evaluated for top-level zones exclusively. However, SRV locator entries of sub-zones that host at least one domain controller (with a Directory Analyzer agent) are evaluated.

Cause

Typically, missing SRV entries indicate that Dynamic DNS has been disabled for one or more DNS zones. Active Directory relies on Dynamic DNS to update all affected entries when network resources are altered or relocated. Other possible causes include DCPROMO failure, and erroneous manual configuration of SRV entries.

NOTE: Dynamic DNS can be disabled explicitly via Windows Registry settings.

Resolution

Confirm that Dynamic DNS is enabled on all applicable zones. Either add the SRV entries manually in the DNS Management Console or cause the entries to be refreshed (for example, by demoting and subsequently promoting the effected domain controllers).

NETLOGON not shared

Indicates that the NETLOGON folder is not shared. File Replication Service requires this folder to be shared on domain controllers for replication to work correctly.

Data collector

- **Category:** Validations
- **Name:** Is the domain controller folder Netlogon shared
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required. When monitored remotely, the target server must have WMI remote access enabled and the user must be a member of the Distributed COM Users group.

Description

Logon scripts for a domain controller are found under the NETLOGON admin share for Windows NT. On Windows NT domain controllers, the **%SystemRoot%\System32\Repl\Import\Scripts** folder is shared as NETLOGON. Dcpromo modifies the registry value that defines the path to the NETLOGON share to **%SystemRoot%\Sysvol\Sysvol\domain_name\Scripts**.

The default folder structure is:

```
%SystemRoot%\Sysvol\Sysvol\domain_name\Policies
%SystemRoot%\Sysvol\Sysvol\domain_name\Scripts
```

Any changes to the **%systemroot%\SYSVOL** folder on any domain controller are replicated to the other domain controllers in the domain. Replication is RPC based.

You can use NETLOGON and SYSVOL to distinguish between a domain controller and a member server. If both the NETLOGON and SYSVOL shares exist on a server, it is a domain controller. When dcpromo demotes a domain controller to a member server, the NETLOGON share is removed, so the presence of only SYSVOL indicates a member server.

Resolution

All potential source domain controllers in the domain should themselves have shared the NETLOGON and SYSVOL shares and applied default domain and domain controllers policy.

SYSVOL directory structure:

```
Domain
   DO NOT REMOVE NtFrs PreInstall Directory
   Policies
      {GUID}
            Adm
            Machine
            User
```

```
   {GUID}
        Adm
        Machine
        User
   {etc.,}
Scripts
Staging
Staging Areas
   MyDomainName.com
Scripts
Sysvol( sysvol share )
   MyDomainName.com
        DO NOT REMOVE NtFrs PreInstall Directory
        Policies
             {GUID}
                  Adm
                  Machine
                  User
             {GUID}
                  Adm
                  Machine
                  User
             {etc.,}
        Scripts(NETLOGON share)
```

To set the Netlogon path

1. Click **Start**, Click **Run**, type **regedit**, and press **ENTER**.
2. Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters**.
3. Right-click **NetLogon**, and select **Modify**.
4. In the **Value data** box, enter the new path, including the drive letter, and click **OK**.
5. Close the Registry Editor.

To share folders with other users on your network

1. Open **My Documents** in Windows® Explorer.
2. Click **Start**, point to **All Programs**, point to **Accessories**, and click **Windows Explorer**.
3. Navigate to the NETLOGON folder.
4. Click **Share this folder in File and Folder Tasks**.
5. In the **Properties** dialog box, select **Share this folder to share the folder with other users on your network**.

Related articles

- https://support.microsoft.com/en-us/help/2958414/dfs-replication-how-to-troubleshoot-missing-sysvol-and-netlogon-shares

NetLogon service is not running

Indicates the NetLogon service is currently not running on the domain controller.

Data collector

- **Category:** Windows Services
- **Name:** Netlogon Windows Service

- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally, only domain user privilege is required. When monitored remotely, domain administrator privilege is required.

Description

The Directory Analyzer agent periodically checks to ensure that the Net Logon service is running.

Resolution

Use the Services MCC snap-in or another SCP application to restart the Net Logon service.

Orphaned group policy objects exist

Indicates that the representation of a Group Policy object (GPO) stored on the local SYSVOL share is not found in Active Directory.

Data collector

- **Category**: General
- **Name:** Orphaned group policy objects exist
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions:** When monitored locally or remotely, read access to SYSVOL.

Description

The Directory Analyzer agent compares the representation of GPOs stored in the local SYSVOL with GPOs found in Active Directory. This alert is active when a GPO represented in the local SYSVOL is not found in Active Directory.

Resolution

Review the reported orphaned GPO folders in the local SYSVOL and remove any that are obsolete.

Physical memory

Indicates that issues have been detected for the physical memory on the domain controller.

Data collector

- **Category:** General
- **Name:** Memory degrade
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Not supported on**: Virtual computers
- **Required permissions**: When monitored locally, only domain user privilege is required. When monitored remotely, the target server must have WMI remote access enabled and the user must be a member of the Distributed COM Users group.

Description

The Directory Analyzer agent monitors the *Memory degrade* data collector on the domain controller. When the physical memory of the selected domain controller has a status other than OK for a period of time equal to or longer than the configured threshold, this alert is raised.

Resolution

Review the device configuration and contact your hardware vendor if required.

Power supply

Indicates that issues have been detected for the power supply on the domain controller.

Data collector

- **Category:** General
- **Name:** Power supply failed
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Not supported on**: Virtual computers
- **Required permissions**: When monitored locally, only domain user privilege is required. When monitored remotely, the target server must have WMI remote access enabled and the user must be a member of the Distributed COM Users group.

Description

The Active Directory Health agent monitors the *Power supply failed* data collector on the domain controller. When the power supply of the selected domain controller has a status other than OK for a period of time equal to or longer than the configured threshold, this alert is raised.

Resolution

Review the device configuration and contact your hardware vendor if required.

Primary DNS resolver is not responding

Indicates one or more of the configured primary DNS resolver for a domain controller is not responding.

Data collector

- **Category:** General
- **Name:** Primary DNS resolver is not responding
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required. When monitored remotely, the target server must have WMI remote access enabled and the user must be a member of the Distributed COM Users group.

Description

The Directory Analyzer agent periodically checks each of its configured DNS resolvers to make sure that they are responding within an acceptable duration. If any configured resolver is unavailable or not responding within a preset duration threshold, this alert is generated.

The test for responsiveness is done by timing the lookup of critical DNS service records from each resolver.

Resolution

Check to make sure that the identified resolver is actually available and responsive.

Secondary DNS resolver is not responding

Indicates one or more of the configured secondary DNS resolver for a domain controller is not responding.

Data collector

- **Category:** General
- **Name:** Secondary DNS resolver is not responding
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required. When monitored remotely, the target server must have WMI remote access enabled and the user must be a member of the Distributed COM Users group.

Description

The Directory Analyzer agent periodically checks each of its configured DNS resolvers to make sure that they are responding within an acceptable duration. If any configured resolver is unavailable or not responding within a preset duration threshold, this alert is generated.

The test for responsiveness is done by timing the lookup of critical DNS service records from each resolver.

Resolution

Check to make sure that the identified resolver is actually available and responsive.

Security Accounts Manager Service is not running

Indicates the Security Accounts Manager Service is currently not running on the domain controller.

Data collector

- **Category**: Windows Services
- **Name:** Security Accounts Manager Service
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions:** When monitored locally or remotely, domain administrator privilege is required.

Description

The Directory Analyzer agent periodically checks to ensure the Security Accounts Manager Service is running.

Resolution

Use the Services MCC snap-in or another SCP application to restart the Security Accounts Manager Service.

SRV record is not registered in DNS

Indicates that a record from the netlogon.dns file is not registered in DNS.

Data collector

- **Category**: General
- **Name:** Compare SRV DNS records with netlogon.dns file

- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions:** When monitored locally and remotely, only domain user privilege is required. When monitored remotely, the target server must have WMI remote access enabled and the user must be a member of the Distributed COM Users group.

Description

The Directory Analyzer agent checks each domain controller for service records. If a service record is missing, check the details for the alert. See Viewing alerts and alert history.

Resolution

Stop and start the Netlogon service to force the domain controller to re-register the appropriate SRV records.

Related article

https://support.microsoft.com/en-us/help/241505/srv-records-missing-after-implementing-active-directory-and-domain-nam

SYSVOL not shared

Indicates that the SYSVOL folder is not shared. File Replication Service requires this folder to be shared on domain controllers for replication to work correctly.

Data collector

- **Category:** Validations
- **Name:** Is the domain controller folder SysVol shared
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally and remotely, only domain user privilege is required. When monitored remotely, the target server must have WMI remote access enabled and the user must be a member of the Distributed COM Users group.

Description

The SYSVOL folder is shared on an NTFS volume on all the domain controllers in a particular domain and is used to deliver the policy and logon scripts to domain members. By default SYSVOL includes two shared folders, where the scripts folder is shared with the name NETLOGON:

- %SystemRoot%\Sysvol\Sysvol\domain_name\Policies
- %SystemRoot%\Sysvol\Sysvol\domain_name\Scripts

The file replication service (FRS) replicates these folders among all domain controllers in the domain. If this folder is not shared, the FRS cannot replicate it.

The alert checks the **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\Shares\SYSVOL** registry key. If the key is not present, the SYSVOL folder is not shared and cannot be replicated and this alert is triggered. The alert is removed when the SYSVOL folder status is set to be shared.

Resolution

SYSVOL directory structure:

Domain

```
DO NOT REMOVE NtFrs PreInstall Directory
Policies
        {GUID}
             Adm
             Machine
```

```
                User
          {GUID}
                Adm
                Machine
                User
          {etc.,}
    Scripts
    Staging
    Staging Areas
          MyDomainName.com
```

Scripts

```
    Sysvol( sysvol share )
         MyDomainName.com
              DO NOT REMOVE NtFrs PreInstall Directory
              Policies
                   {GUID}
                        Adm
                        Machine
                        User
                   {GUID}
                        Adm
                        Machine
                        User
                   {etc.,}
         Scripts(NETLOGON share)
```

To set the SYSVOL path

1. Click **Start**, click **Run**, type **regedit** and press **Enter**.
2. Navigate to **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters**.
3. Right-click **SYSVOL**, and select **Modify**.
4. In the **Value data** box, enter the new path, including the drive letter, and click **OK**.
5. Close the Registry Editor.

> **NOTE:** The path in the registry points to the SYSVOL folder located inside the SYSVOL folder that is under the root. When updating the path in the registry, ensure that it still points to the SYSVOL folder inside the SYSVOL folder that is under the root.

To share folders with other users on your network

1. Open My Documents in Windows® Explorer.
2. Click **Start**, point to **All Programs**, point to **Accessories**, and click **Windows Explorer**.
3. Navigate to the SYSVOL folder.
4. Click **Share this folder in File and Folder Tasks**.
5. In the **Properties** dialog box select **Share this folder to share the folder with other users on your network**.

W32Time service is not running

Indicates the Windows® Time (W32Time) service is not currently running on the domain controller.

Data collector

- **Category:** Windows Services

- **Name:** Windows Time service
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: When monitored locally, only domain user privilege is required. When monitored remotely, domain administrator privilege is required.

Description

The Directory Analyzer agent periodically checks to ensure that the W32Time service is running.

Resolution

Use the Services MCC snap-in or another SCP application to restart the W32Time service.

Workstation Service is not running

Indicates the Workstation Service is currently not running on the domain controller.

Data collector

- **Category**: Windows Services
- **Name:** Workstation Service
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions:** When monitored locally or remotely, domain administrator privilege is required.

Description

The Directory Analyzer agent periodically checks to ensure the Workstation Service is running.

Resolution

Use the Services MCC snap-in or another SCP application to restart the Workstation Service.

Domain alerts

Topics

- Conflict encountered during replication
- DNS server missing domain SRV records
- Domain FSMO role placement
- Global catalog server replication latency
- Infrastructure operations master hosts a global catalog server
- Infrastructure operations master inconsistent
- Infrastructure operations master not responding
- Missing root PDC time source
- Objects exist in the Lost and Found container
- RID operations master inconsistent
- PDC operations master not responding
- Replication latency

- RID operations master inconsistent
- RID operations master not responding
- RODC allowed password replication policy inconsistent
- RODC denied password replication policy inconsistent

Conflict encountered during replication

Indicates that conflicting objects were encountered during replication and reported by Active Directory®.

Data collector

- **Name:** Conflict encountered during replication
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege is required.

Description

Active Administrator® Data Service (ADS) periodically monitors for conflicting objects in the domain and generates an alert when it encounters one.

Conflicts arise when two objects are created independently at separate locations in the domain. When a conflict is detected during replication, Active Directory® creates a conflict entry appending the following to the domain name of the object:

CNF:<GUID-of-authoritative-object>

Resolution

- If the conflict object contains useful information, move that information into a different directory object, and then delete the object.
- If the conflict object does not contain useful information, delete the object.

DNS server missing domain SRV records

Indicates one or more requisite Domain Name System (DNS) service (SRV) entries are not defined.

Data collector

- **Name:** DNS server missing domain SRV records
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege is required.

Description

Service Records or SRV records are registered specifically for domain controllers when a member server is promoted to a domain controller. The Netlogon service on the domain controller is responsible for registering SRV records. Because Active Directory® depends on DNS, if SRV records of domain controllers are missing from the DNS Zone of the domain, critical failures of Active Directory services can occur.

Resolution

The following methods can be used to re-register SRV records of a domain controller in the domain DNS zone:

- Restart the Netlogon service on domain controller.

- Run DcDiag /fix.
- Run NetDiag /fix.
- Re-register from Netlogon.dns file in \Windows or Winnt\System32\Config directory.

Related article

https://support.microsoft.com/en-us/help/241505/srv-records-missing-after-implementing-active-directory-and-domain-name-system

Domain FSMO role placement

Indicates that Active Directory® Flexible Single-Master (FSMO) roles are not configured according to Microsoft® recommendations.

Data collector

- **Name:** Domain FSMO role placement
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege is required.

  NOTE: As part of the data collector setup, you can select to validate the RID Master, the Naming Master, the Schema Master, and the Infrastructure Master role. By default, all are selected for validation. You must, however, select at least one FSMO role validation option to enable the data collector.

Description

The Active Directory Installation Wizard performs the initial placement of roles on domain controllers and is often correct for directories that have just a few domain controllers. A directory that has many domain controllers may require manual intervention to optimize placement.

Resolution

- Place the schema master on the PDC of the forest root domain.
- Place the domain naming master on the forest root PDC.
- Place the RID master on the domain PDC in the same domain.
- Legacy guidance suggests placing the infrastructure master on a non-global catalog server.

Global catalog server replication latency

Indicates that the replication latency of the server that hosts a replica of the global catalog equals or exceeds the configured threshold.

NOTE: The Global catalog server replication latency data collector is disabled by default. If you want to monitor global catalog replication latency, enable this data collector. See Analyzing health of a selected domain and Setting data collectors.

Data collector

- **Name:** Global catalog server replication latency
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privileges with rights to list contents, create objects, read and write properties under the AATemp organizational unit in the domain root.

Description

Active Administrator Data Service (ADS) periodically queries to find the elapsed time between changing a distinct object on each domain controller and the time the change appears in every copy of the global catalog. If the elapsed time exceeds the configured threshold, the alert is activated.

This alert applies to all domain controllers that host a replica of the Global Catalog.

Resolution

- Check connectivity between both the domain controller and the replication partner in question.
- Check to see that the link is reasonably clear, especially during replication.
- Check the replication schedule for the connection.
- Make sure that each partner has adequate CPU and memory resources to ensure timely servicing of replication requests.
- Make sure that the link between partners is adequate for the amount of traffic carried during replication.

Infrastructure operations master hosts a global catalog server

Indicates that the infrastructure operations master hosts a global catalog server.

NOTE: If all domain controllers in a domain host a global catalog, it is recommended that you disable this alert for the domain. This alert is disabled by default.

Data collector

- **Name:** Infrastructure operations master hosts a global catalog server
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege is required.

Description

Active Directory Health Analyzer monitors the infrastructure operations master, as well as the global catalog hosting attribute of each server in a domain. When a server is found to have both a global catalog and the infrastructure operations master responsibility, an alert will be generated.

The infrastructure operations master updates references from objects in other domains by comparing local data to data from a global catalog, which is always up to date. If discrepancies are found, the infrastructure operations master updates the local object data from the global catalog, and then replicates the updated object data to all other domain controllers in the domain. If a global catalog exists on the same domain controller as the infrastructure operations master, the infrastructure operations master will never find data that is out of date.

Resolution

Remove the global catalog from the infrastructure operations master domain controller.

Infrastructure operations master inconsistent

Indicates that the infrastructure operations master is not consistent among all domain controllers in the domain.

Data collector

- **Name:** Infrastructure operations master inconsistent
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022

- **Required permissions**: Domain user privilege is required.

Description

The Active Administrator Foundation Service (AFS) periodically checks the consistency of the infrastructure operations master value across all of the domain controllers in the domain. If any of the domain controllers has a differing value for the infrastructure operations master, AFS will issue this alert.

The infrastructure operations master is contained in the fSMORoleOwner property of the infrastructure object contained by each domain object. Every domain controller in the domain has a copy of the infrastructure operations master.

Active Directory objects can contain links to other objects in the directory. Active Directory keeps these links up-to-date even if the linked-to object is moved to another container or is renamed. This update cannot happen if the linked-to object is in another domain.

If the infrastructure operations master is inconsistent, it is possible that two copies will run simultaneously on two different domain controllers, with potentially disastrous consequences.

The Infrastructure operations master can become inconsistent because an administrator used NTDSUTIL.EXE to move the Operations Master when there was incomplete connectivity to all domain controllers in the domain. It can also occur because of replication errors.

Resolution

First, wait to see if the error clears itself. An inconsistent operations master alert can be transitory in nature. If an administrator has moved an operations master to another domain controller, replication to all domain controllers in the domain can take some time. During this period, Active Directory Health Analyzer will indicate this alert condition.

If you have waited long enough for replication to have occurred to all domain controllers in the domain and the alert has not cleared itself, contact your Microsoft Windows support representative.

Related article

https://blogs.technet.microsoft.com/mempson/2007/11/08/how-to-find-out-who-has-your-fsmo-roles/

Infrastructure operations master not responding

Indicates that the infrastructure operations master is not responding within the configured threshold.

Data collector

- **Name:** Infrastructure operations master not responding
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege is required.

Description

The Active Administrator® Foundation Service (AFS) periodically queries to find the response time of the infrastructure operations master. If the response time is above the threshold, an alert is generated.

This error can occur if any of the following occurs:

- The indicated server domain controller does not exist.
- The domain controller no longer has connectivity to the network and to the Directory Analyzer agent.
- The DNS records for the domain controller are incorrect; e.g., the IP address for the domain controller is not what is published in DNS as viewed by the Directory Analyzer agent.

- Active Directory® on the domain controller has failed in some way.
- Active Directory on the domain controller is overloaded and is taking too long to respond.
- The domain controller is not running.

Resolution

- Ping the domain controller from the Directory Analyzer agent to see if there is connectivity. If there is not, fix that problem. The problem may be that DNS has the incorrect address or that the IP stack for the domain controller or the Directory Analyzer agent is misconfigured.
- Make sure the domain controller is running. If the domain controller is not running, start it.
- Make sure the indicated domain controller actually exists. If it does not exist, run NTDSUTIL and select the **metadata cleanup** option to clean up the erroneous objects in the directory.
- Check the LDAP response time for the domain controller on the **Active Directory** tab in Active Directory Health Analyzer. If it is too high, you may need to add another domain controller for the same domain in the same site.

Missing root PDC time source

Indicates the PDC Role Owner of the root domain in the forest is not configured to use an external time source. All domain controllers in the forest synchronize their time by the clock of the PDC Role Owner.

Data collector

- **Name:** Missing root PDC time source
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege is required and the target server must have WMI remote access enabled. The user must be a member of the Distributed COM Users group.

Description

Since Active Directory®, by default, sets all the clocks on all of the domain controllers in the forest from the PDC Role Owner of the root domain, it is recommended that the domain controller be configured to synchronize its time with an external time source. This alert is active if the root domain PDC Owner is not so configured.

Resolution

Use the w32time command at an elevated PowerShell session to configure the PDC Role Owner to use an external time source.

```
w32tm /config /manualpeerlist:TimeSource /syncfromflags:MANUAL
```

Where TimeSource is one or more NTP servers noted by DNS or IP address. When TimeSource is a list of time servers the list must be enclosed in double quotes and each entry must be separated by at least one space. Some examples are listed below:

```
w32tm /config /manualpeerlist:pool.ntp.org /syncfromflags:MANUAL
w32tm /config /manualpeerlist:”1.pool.ntp.org 2.pool.ntp.org“ /syncfromflags:MANUAL
```

Objects exist in the Lost and Found container

Generated when Active Directory Health Analyzer discovers objects in the Lost And Found container of a naming context.

Data collector

- **Name:** Objects exist in the Lost and Found container

- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege is required.

Description

The Active Administrator® Foundation Service (AFS) periodically checks to see if there are any objects in the Lost And Found container in the domain. If there are, the DC Agent will issue an alert.

During the replication process, Active Directory® may encounter orphaned objects, which are objects that have no parent container. For example, a user deletes container X on domain controller A, and another user modifies object Y contained in container X on domain controller B. During replication, domain controller A will receive an update operation for an object that has no container because container X was deleted. In this case, the directory system agent (DSA) on domain controller A puts the object in the Lost And Found container.

The DSA will place objects in the Lost And Found container as part of its normal operation. However, serveral Lost And Found objects may indicate a replication problem, or at least the deletion of a container that should not have been deleted.

Resolution

Inspect the objects in the Lost And Found container of the replica indicated in the alert using an appropriate utility. Move the objects to an appropriate container or delete them from the Lost And Found container.

PDC operations master inconsistent

Indicates that the domain PDC (primary domain controller) operations master is not consistent among all domain controllers in the domain.

Data collector

- **Name:** PDC operations master inconsistent
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege is required.

Description

The Active Administrator® Foundation Service (AFS) periodically checks the consistency of the domain PDC operations master value across all of the domain controllers in the domain. If any of the domain controllers has a differing value for the domain PDC operations master, an alert is issued.

The domain PDC operations master is contained in the fSMORoleOwner property of the domain object itself. Every domain controller in the domain has a copy of the domain PDC operations master.

The domain PDC operations master determines which domain controller in the domain is responsible for acting as a downlevel primary domain controller (PDC). If the domain PDC operations master is inconsistent, it is possible that two different domain controllers will act as the PDC, with potentially disastrous consequences.

The domain PDC operations master can become inconsistent because an administrator used NTDSUTIL.EXE to move the operations master when there was incomplete connectivity to all domain controllers in the domain. It can also occur because of replication errors.

Resolution

Wait to see if the error clears. An inconsistent operations master alert can be transitory in nature. If an administrator has moved an operations master to another domain controller, replication to all domain controllers in the domain can take some time. During this period, Active Directory Health Analyzer will indicate this alert condition.

If alert does not clear, contact your Microsoft Windows support representative.

Related article

https://blogs.technet.microsoft.com/mempson/2007/11/08/how-to-find-out-who-has-your-fsmo-roles/

PDC operations master not responding

Indicates that the PDC (primary domain controller) operations master is not responding within the configured threshold.

Data collector

- **Name:** PDC operations master not responding
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege is required.

Description

The Active Administrator® Foundation Service (AFS) periodically queries to find the response time of the PDC operations master. If the response time is above the configured threshold, an alert is issued.

This error can occur if any of the following occurs:

- The indicated domain controller does not exist.
- The domain controller no longer has connectivity to the network.
- The DNS records for the domain controller are incorrect; e.g., the IP address for the domain controller is not what is published in DNS.
- Active Directory® on the domain controller has failed in some way.
- Active Directory on the domain controller is overloaded and is taking too long to respond.
- The domain controller is not running.

Resolution

- Ping the domain controller from the Active Directory Health Analyzer to see if there is connectivity. If there is not, fix that problem.
- Make sure the domain controller is running. If the domain controller is not running, start it.
- Make sure the indicated domain controller actually exists. If it does not exist, run NTDSUTIL and select the metadata cleanup option to clean up the erroneous objects in the directory.
- Check the LDAP response time for the domain controller. If it is too high, you may need to add another domain controller for the same domain in the same site.

Replication latency

Indicates that replication changes from one domain controller to all other domain controllers in the naming context exceeds the configured threshold.

NOTE: The Replication latency data collector is disabled by default. If you want to monitor replication latency, enable this data collector. See Analyzing health of a selected domain and Setting data collectors.

Data collector

- **Name:** Replication latency
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022

- **Required permissions**: Domain user privileges with rights to list contents, create objects, read and write properties under the AATemp organizational unit in the domain root.

Description

The replication latency data collector checks latency between each domain controller in the domain by creating an object on a domain controller and then checking every other domain controller for the change. Once the change is noticed, the time difference is recorded.

NOTE: On service startup there is a 5 minute delay before Active Administrator® Data Service (ADS) starts checking replication, and then every hour after that. If the latency container does not exist, it is created and there is a 10 minute delay. The latency containers are located at AATemp\Latency under the domain.

There is a timeout for the test. The timeout is the alert value plus three minutes. If the alert is set to 20 minutes and the test is still running at 23 minutes it will end.

High replication latency values mean that changes you make in the directory are taking too long to replicate to all of the other domain controllers, which can cause operational difficulties. For example, a user cannot use a new password if the password has not replicated to their domain controller. High replication latency values can also cause directory problems. If you make a change to the Configuration naming context by adding a new site or a new domain controller, the replication process will not work correctly until all domain controllers have a copy of the new site or new domain controller.

High latency times are usually due to poor network connectivity, non-functional domain controllers, or incorrect replication schedules.

NOTE: Active Directory Health Analyzer only measures replication latency to another domain controller if replication actually occurs on that domain controller. If the domain controller is down or disconnected, Active Directory Health Analyzer will not measure the latency to that domain controller.

Resolution

Make sure that the replication latency is actually too high. In a site with fewer than five domain controllers, the intra-site replication latency should be around five minutes. As you add domain controllers in a site, the intra-site replication latency should go up to about 20-30 minutes, and then stabilize. Inter-site replication latency depends entirely on the link schedules between the sites.

If the latency truly is too high, make sure there are no domain controllers that are down. If a single domain controller acts as a bridgehead between sites, and it goes down, replication will never actually occur.

RID operations master inconsistent

Indicates that the relative identifier (RID) operations master is not consistent among all domain controllers in the domain.

Data collector

- **Name:** RID operations master inconsistent
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege is required.

Description

The Active Administrator Foundation Service (AFS) periodically checks the consistency of the domain RID operations master value across all of the domain controllers in the domain. If any of the domain controllers has a differing value for the domain RID operations master, the alert is generated.

The domain RID operations master is contained in the fSMORoleOwner property of the RID Manager object in the CN=System,DC=<domain> container. Every domain controller in the domain has a copy of the domain RID operations master. The RID operations master allocates sequences of RIDs to each of the various domain controllers in its domain. At any time, there can be only one domain controller acting as the RID master in each domain in the forest.

Whenever a domain controller creates a user, group, or computer object, the domain controller assigns the object a unique security ID (SID). The SID consists of a domain SID, which is the same for all SIDs created in the domain, and a RID, which is unique for each SID created in the domain. If the domain RID operations master is inconsistent, it is possible that two different domain controllers will assign overlapping RID ranges to other domain controllers in the domain, with potentially disastrous consequences.

The domain RID operations master can become inconsistent due to replication errors or if an administrator used NTDSUTIL.EXE to move the operations master when there was incomplete connectivity to all domain controllers in the domain.

Resolution

Wait to see if the error clears. An inconsistent operations master alert can be transitory in nature. If an administrator has moved an operations master to another domain controller, replication to all domain controllers in the domain can take some time. During this period, Active Directory Health Analyzer will indicate this alert condition.

If the alert does not clear, contact your Microsoft Windows support representative.

Related article

https://blogs.technet.microsoft.com/mempson/2007/11/08/how-to-find-out-who-has-your-fsmo-roles/

RID operations master not responding

Indicates that the relative identifier (RID) operations master is not responding within the configured threshold.

Data collector

- **Name:** RID operations master not responding
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege is required.

Description

The Active Administrator® Foundation Service (AFS) periodically queries to find the response time of the RID operations master. If the response time is above the threshold, an alert is issued.

This error can occur if any of the following occurs:

- The indicated server is not actually a domain controller.
- The domain controller no longer has connectivity to the network.
- The DNS records for the domain controller are incorrect; e.g., the IP address for the domain controller is not what is published in DNS.
- Active Directory® on the domain controller has failed in some way.
- Active Directory on the domain controller is overloaded and is taking too long to respond.
- The domain controller is not running.

Resolution

- Ping the domain controller from the Directory Analyzer agent to see if there is connectivity. If there is not, fix that problem. The problem may be that DNS has the incorrect address or that the IP stack for the domain controller or the Directory Analyzer agent is not configured correctly.
- Make sure the domain controller is running. If the domain controller is not running, start it.
- Make sure the indicated domain controller actually exists. If it does not exist, run NTDSUTIL and select the **metadata cleanup** option to clean up the erroneous objects in the directory.

- Check the LDAP response time for the domain controller. If it is too high, you may need to add another domain controller for the same domain in the same site.

RODC allowed password replication policy inconsistent

Indicates the allowed password replication policy for this server is not consistent with the selected authoritative read-only domain controller (RODC) for the domain.

Data collector

- **Name:** RODC allowed password replication policy inconsistent
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege is required.

  IMPORTANT: To enable this data collector, you must set at least one authoritative RODC. See Setting an authoritative RODC.

Description

The **msDS-RevealOnDemandGroup** property contains a list of groups whose credentials will be replicated to the given RODC. It is recommended that each RODC in a given naming context have the same groups in its **msDS-RevealOnDemandGroup** property. To facilitate the comparison of the lists of groups among a number of RODCs, the user selects an RODC as the authoritative source for the **msDS-RevealOnDemanGroup** in a given naming context. The Active Administrator® Foundation Service (AFS) compares all other RODCs in the domain to the authoritative list.

Resolution

Compare the **msDS-RevealOnDemandGroup** attribute of the authoritative RODC to that of the inconsistent RODC, and modify the **msDS-RevealOnDemandGroup** on the inconsistent server to match the authority.

RODC denied password replication policy inconsistent

Indicates the denied password replication policy for this server is not consistent with the authoritative read-only domain controller (RODC) for the domain.

Data collector

- **Name:** RODC denied password replication policy inconsistent
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege is required.

  IMPORTANT: To enable this data collector, you must set at least one authoritative RODC. See Setting an authoritative RODC.

Description

The **msDS-NeverRevealGroup** property contains a list of groups (Deny List) whose credentials will be replicated to the given RODC. It is recommended that each RODC in a given naming context have the same groups in its **msDS-NeverRevealGroup** property. To facilitate the comparison of the lists of groups among a number of RODCs the user selects an RODC as the authoritative source for the **msDS-NeverRevealGroup** in a given naming context. The Active Administrator® Foundation Service (AFS) compares all other RODCs in the domain to the authoritative list.

Resolution

Compare the **msDS-NeverRevealGroup** attribute of the authoritative RODC to that of the inconsistent RODC, and modify the **msDS-everRevealGroup** on the inconsistent server to match the authority.

Site alerts

Topics

- Inter-site replication manager
- Inter-site replication topology generation disabled
- Intra-site replication topology generation disabled
- Morphed directories exist in site
- No authority in site to resolve universal group memberships
- Too few global catalog servers in site

Inter-site replication manager

Indicates that a domain controller, other than the preferred bridgehead server(s), is actively replicating outside of its current state.

Data collector

- **Name:** Inter-site replication manager
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege is required.

Description

Active Directory® allows administrators to configure preferred bridgehead servers for each site. Sometimes connection objects are created manually to solve a quick problem, but they are never removed. If these manually-created links are actively replicating, undesirable results may occur.

If any server other then the preferred bridgehead server(s) has a connection object that handles intersite replication, this alert will be triggered.

If no server if configured as the preferred bridgehead server, this alert is never triggered because the Knowledge Consistency Checker (KCC) is handling all topology replication.

Resolution

It is possible that this is a transient issue caused by Active Directory replication delays associated with updating File Replication service (FRS) configuration objects. If file replication does not take place after an appropriate waiting time, which could be several hours if cross-site Active Directory replication is required, you must manually reset the preferred bridgehead server.

Relevant articles

https://technet.microsoft.com/en-us/library/cc794778(v=ws.10).aspx

Inter-site replication topology generation disabled

Indicates inter-site replication topology generation for a site is disabled.

Data collector

- **Name:** Inter-site replication topology generation disabled
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege is required.

Description

The Active Administrator® Foundation Service (AFS) periodically checks the Knowledge Consistency Checker (KCC) configuration for each site and alerts when the replication topology generation functionality of the KCC has been explicitly disabled. While disabling the KCC is a valid administrator action, it can result in poorly-tuned replication topologies.

Resolution

Clear the fifth bit (16) of the **<Root Domain>\Configuration\Sites\<Site name>\NTDS Site Settings\options** value to re-enable inter-site topology generation.

Related articles

- https://technet.microsoft.com/en-us/library/cc961781.aspx
- https://technet.microsoft.com/en-us/library/dd723682(v=ws.10).aspx

Intra-site replication topology generation disabled

Indicates the intra-site replication topology generation for a site is disabled.

Data collector

- **Name:** Intra-site replication topology generation disabled
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege is required.

Description

The Active Administrator® Foundation Service (AFS) periodically checks the Knowledge Consistency Checker (KCC) configuration for each site and alerts when the replication topology generation functionality of the KCC has been explicitly disabled. While disabling the KCC is a valid administrator action, it can result in poorly-tuned replication topologies.

Resolution

Clear the first bit (1) of the **<Root Domain>\Configuration\Sites\<Site name>\NTDS Site Settings\options** value to re-enable inter-site topology generation.

Related articles

- https://technet.microsoft.com/en-us/library/cc961781.aspx

- https://technet.microsoft.com/en-us/library/dd723682(v=ws.10).aspx

Morphed directories exist in site

Generated when morphed directories are found in a replica tree.

Data collector

- **Name:** Morphed directories exist in site
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege is required.

Description

All files and folders that File Replication Service (FRS) manages are uniquely identified internally by a special file identifier. FRS uses these identifiers as the canonical identifiers of files and folders that are being replicated. If FRS receives a change order to create a folder that already exists, which by definition has a different file identifier than the duplicate folder, FRS protects the conflicting change by leaving the original directory structure intact, and renaming the conflicting directory to a unique name so that underlying files and folders can be preserved. The conflicting folder is given a new name in the following format: ***<FolderName>*_NTFRS_*<GUID>***, where ***<FolderName>*** is the original name of the folder and <***GUID***> is a unique character string, such as 001a84b2.

Common causes of this condition are:

- A folder is created on multiple machines in the replica set before the folder has been able to replicate. This could be due to the administrator or application duplicating folders of the same name on multiple FRS members.
- You initiated an authoritative restore on one server and did not stop the service on all other members of the re-initialized replica set before restarting FRS after the authoritative restore.
- You initiated an authoritative restore on one server and did not set the D2 registry key for the authoritative restore on all other members of the re-initialized replica set before a server replicated outbound changes to re-initialized members of the replica set.
- You initiated an authoritative restore on one server and manually copied directories with names identical to those being replicated by FRS to computers in the replica set.

Resolution

- Move the morphed directories out of the replica tree and back in. This method works well for small amounts of data on a small number of targets. However, if you miss end-to-end replication of the move-out, this method can cause morphed directories. This method also requires all members to re-replicate data.
- Rename the morphed directories. This method does not require re-replication of data, however, it can cause a denial-of-service condition by giving an invalid path when the originating path is renamed.

No authority in site to resolve universal group memberships

Indicates a site has no global catalog and universal group membership caching is disabled.

Data collector

- **Name:** No authority in site to resolve universal group memberships
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege is required.

Description

The Active Administrator® Foundation Service (AFS) periodically checks the Knowledge Consistency Checker (KCC) configuration for each site. If universal group membership caching is disabled and there are no global catalogs in the site, an alert is issued.

While this is a valid configuration for a site, if the site is connected through a slow link, it can result in poor logon performance.

Resolution

- Configure a domain controller as a global catalog server.
- Enable universal group membership caching.

Too few global catalog servers in site

Indicates the number of global catalog servers in a given site is less than or equal to the configured threshold.

Data collector

- **Name:** Too few global catalog servers in site
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege is required.

Description

The Directory Analyzer agent checks the state of all of the domain controllers in the site, and if the number of domain controllers that host a global catalog is less than the configured threshold for a period exceeding the configured duration, an alert is issued.

Each site in an Active Directory® enterprise should have at least one domain controller configured as a global catalog. The workstation login process always attempts to contact a global catalog server, and if none are running at the site where the workstation resides, the workstation will connect to a global catalog server outside of the site, which can cause excess WAN traffic and unnecessary delays in the login process.

Resolution

- Configure a domain controller as a global catalog server.

Forest alerts

Topics

- Domain naming and schema operations masters differ
- Domain naming operations master inconsistent
- Domain naming operations master is not a GC
- Naming operations master not responding
- Schema operations master inconsistent
- Schema operations master not responding
- Schema version inconsistent
- Site link settings inconsistent with PDC
- Site settings inconsistent with PDC

- Subnet settings inconsistent with PDC

Domain naming and schema operations masters differ

Indicates the domain naming and schema operations masters reside on separate domain controllers.

Data collector

- **Name:** Domain naming and schema operations masters differ
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege in the domain where the schema and naming masters reside.

Description

The Active Administrator® Foundation Service (AFS) monitors the owners of the domain naming operations master and schema operations master. When AFS finds that they reside on separate servers, an alert is issued.

Resolution

1 Determine which domain controllers have the domain naming and schema operations masters.

To determine the controllers have the domain naming and schema operations masters

a Select **Active Directory Health | Analyzer**.

b Expand **Sites**, and select the site.

c Locate the domain controllers with **Yes** in the **Schema** and **Naming** columns.

2 Decide which domain controller you want to host both the domain naming and the schema operations masters.

3 Transfer the operations master roles to the selected domain controller.

Domain naming operations master inconsistent

Indicates that the domain naming operations master is not consistent among all domain controllers in the forest.

Data collector

- **Name:** Domain naming operations master inconsistent
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege in all domains in the forest.

Description

The Active Administrator® Foundation Service (AFS) periodically checks the consistency of the domain naming operations master value across all of the domain controllers in the forest. If any of the domain controllers has a differing value for the domain naming operations master, the alert is issued.

The domain naming operations master is contained in the fSMORoleOwner property of the CN=Partitions,CN=Configuration,DC=<root domain> container. Because the partitions container is part of the configuration naming context, every domain controller in the forest has a copy of the domain naming operations master. The domain naming operations master determines what domain controller in the forest can initiate a domain renaming operation. If the domain naming operations master is inconsistent, it is possible to issue a

domain renaming operation simultaneously at two different domain controllers, with potentially disastrous consequences.

The domain naming operations master can become inconsistent because an administrator used NTDSUTIL.EXE to move the operations master when there was incomplete connectivity to all domain controllers. It can also occur because of replication errors.

Resolution

- Make sure that no one attempts to rename a domain while this alert is active.
- Wait to see if the error clears. An inconsistent operations master alert can be transitory in nature. If an administrator has moved an operations master to another domain controller, replication to all domain controllers in the forest can take a long time. During this period, Active Directory Health Analyzer will indicate this alert condition.
- If the alert does not clear, contact your Microsoft® Windows® support representative.

Domain naming operations master is not a GC

Indicates that a server possessing the domain naming operations master does not host a global catalog (GC).

Data collector

- **Name:** Domain naming operations master is not a GC
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege in the domain where the schema and naming masters reside.

Description

The Active Administrator® Foundation Service (AFS) monitors the domain naming operations master status for each domain in Active Directory®, continually checking to see that each domain naming operations master also hosts a global catalog. When a domain naming operations master is found that does not host a global catalog, this alert is triggered.

The domain naming operations master must be a global catalog server because the domain naming operations master is responsible for creating objects that represent new domains. In order to do this, the domain naming operations master must be able to make sure that no other object — whether it is a domain object or not — has the same name as the new domain object. The domain naming operations master always runs a global catalog, which contains a partial replica of every object, to allow the domain naming operations master to quickly check for a duplicate object name prior to creating a new domain object.

Resolution

- Enable a global catalog on the domain naming operations master identified in this alert.

Naming operations master not responding

Indicates that the naming operations master is not responding within the configured threshold.

Data collector

- **Name:** Naming operations master not responding
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege is required.

Description

The Active Administrator® Foundation Service (AFS) periodically queries to find the response time of the naming operations master. If the response time is above the threshold, an alert is generated.

This alert is generated if any of the following occurs:

- The domain controller does not exist, is not running, or lost connectivity to the network
- The DNS records for the domain controller are incorrect; e.g., the IP address for the domain controller is not what is published in DNS.
- Active Directory® on the domain controller has failed, or is overloaded and taking too long to respond.

Resolution

- Ping the domain controller to see if there is connectivity. If there is not, fix that problem. The problem may be that DNS has the incorrect address or the IP stack for the domain controller is misconfigured.
- If the domain controller does not exist, run NTDSUTIL and select the **metadata cleanup** option to clean up the erroneous objects in the directory.
- Check the LDAP response time for the domain controller on the **Active Directory** tab in the Active Directory Health module. If it is too high, you may need to add another domain controller for the same domain in the same site.

Schema operations master inconsistent

Indicates that the schema operations master is not consistent among all domain controllers in the forest.

Data collector

- **Name:** Schema operations master inconsistent
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege is required.

Description

The Active Administrator® Foundation Service (AFS) monitors the value of the schema operations master attribute on each domain controller in the forest. If the value is not the same on each domain controller, an alert is generated.

The schema operations master object (CN=&ldots;) contains an attribute called fSMORoleOwner, which contains the distinguished name of the domain controller that is allowed to originate changes to the Active Directory® schema. When an administrator attempts to modify the Active Directory schema, the directory system agent (DSA) makes sure that the fSMORoleOwner property refers to the server on which the administrator is making the change. If it does not refer to that server, the DSA will not modify the schema. The schema operations master ensures that the schema cannot become inconsistent because of conflicting changes issued from different domain controllers.

If the schema operations master is inconsistent, meaning the domain controllers have differing values for the fSMORoleOwner attribute, it is possible for administrators (or others) to issue conflicting updates to the schema, potentially causing sufficient damage to Active Directory that replication will fail. It is important to not attempt to modify the Active Directory schema when the schema operations master is inconsistent.

The schema operations master can become inconsistent due to replication failures or due to an administrator using NTDSUTIL.EXE to require the operations master to another domain controller. This can also be a transient alert if the replication latency for the schema naming context is fairly large.

Resolution

- Make sure that no one attempts to modify the Active Directory schema while the schema operations master is inconsistent.

- Normally, the Active Directory replication process will correct this error, so the next step is to wait awhile to see if the alert clears by itself. The amount of time you should wait depends on the replication latency for the schema naming context. Active Directory Health Analyzer does not measure the latency of the schema naming context, but it does measure the latency of the configuration naming context, which will be the same.
- If the alert does not clear itself in a reasonable amount of time, contact your Microsoft® Windows® support representative.

Schema operations master not responding

Indicates that the schema operations master is not responding within the configured threshold.

Data collector

- **Name:** Schema operations master not responding
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege is required.

Description

The Active Administrator® Foundation Service (AFS) periodically queries to find the response time of the schema operations master. If the response time is above the threshold, an alert is generated.

This alert is generated if any of the following occurs:

- The domain controller does not exist, is not running, or lost connectivity to the network
- The DNS records for the domain controller are incorrect; e.g., the IP address for the domain controller is not what is published in DNS.
- Active Directory® on the domain controller has failed, or is overloaded and taking too long to respond.

Resolution

- Ping the domain controller to see if there is connectivity. If there is not, fix that problem. The problem may be that DNS has the incorrect address or the IP stack for the domain controller is misconfigured.
- If the domain controller does not exist, run NTDSUTIL and select the **metadata cleanup** option to clean up the erroneous objects in the directory.
- Check the LDAP response time for the domain controller on the **Active Directory** tab in the Active Directory Health module. If it is too high, you may need to add another domain controller for the same domain in the same site.

Schema version inconsistent

Indicates that the schema version is not consistent across all domain controllers in the forest.

Data collector

- **Name:** Schema version inconsistent
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege is required.

Description

The Active Administrator® Foundation Service (AFS) periodically checks the consistency of the schema version across all of the domain controllers in the forest. If any of the domain controllers has a differing value for the schema version, the alert is generated.

Resolution

- Wait for a while to see if the error clears itself. An inconsistent schema version alert can be transitory in nature.
- If you have waited long enough for replication to have occurred to all domain controllers and the alert does not clear itself, contact your Microsoft® Windows® support representative.

Site link settings inconsistent with PDC

Indicates that some of the site link settings on domain controllers in the forest do not match the same settings on the primary domain controller (PDC).

Data collector

- **Name:** Site link settings inconsistent with PDC
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege is required.

Description

The Active Administrator® Foundation Service (AFS) periodically checks the site link settings (Description, Assigned sites, Cost, Replication interval and Schedule) of the PDC and compares them to the other domain controllers in the forest. If any of the domain controllers has a differing value from the PDC, an alert is issued.

Resolution

- Wait for a while to see if the error clears itself. An inconsistent site link settings alert can be transitory in nature.
- If alert does not clear, contact your Microsoft® Windows® support representative.

Site settings inconsistent with PDC

Indicates that some of the site settings on domain controllers in the forest do not match the same settings on the primary domain controller (PDC).

Data collector

- **Name:** Site settings inconsistent with PDC
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege is required.

Description

The Active Administrator® Foundation Service (AFS) periodically checks the site settings (name, description, cn, displayName, location, managedBy, objectCategory, Subnets, and Servers) of the PDC and compares them to the other domain controllers in the forest. If any of the domain controllers has a differing value from the PDC, an alert is issued.

Resolution

- Wait for a while to see if the error clears itself. An inconsistent site settings alert can be transitory in nature.
- If alert does not clear, contact your Microsoft® Windows® support representative.

Subnet settings inconsistent with PDC

Indicates that some of the subnet settings on domain controllers in the forest do not match the same settings on the primary domain controller (PDC).

Data collector

- **Name:** Subnet settings inconsistent with PDC
- **Supported on:** Windows Server 2016, Windows Server 2019, and Windows Server 2022
- **Required permissions**: Domain user privilege is required.

Description

The Active Administrator® Foundation Service (AFS) periodically checks the settings (Description, Assigned site, Prefix) of the PDC and compares them to the other domain controllers in the forest. If any of the domain controllers has a differing value from the PDC, an alert is issued.

Resolution

- Wait for a while to see if the error clears itself. An inconsistent subnet settings alert can be transitory in nature.
- If alert does not clear, contact your Microsoft® Windows® support representative.

Microsoft Entra Connect alerts

Topics

- Windows Services alerts
- Connectivity alerts
- Event ID alerts

Windows Services alerts

Table 145. Windows Services alerts

Alert	Description
Microsoft Entra Connect Sync service status	Microsoft Entra Connect Sync service is in a stopped state.
Microsoft Entra Connect Health Sync Insights service status	Microsoft Entra Connect Health Sync Insights is in a stopped state.
Microsoft Entra Connect Health Sync service	Microsoft Entra Connect Health Sync service is in a stopped state.

Connectivity alerts

Table 146. Connectivity alerts

Alert	Description
Microsoft Entra connectivity	Microsoft Entra connectivity test failed.
Microsoft Entra database connectivity	Connectivity to the Microsoft Entra Connect database was lost.

Event ID alerts

Table 147. Event ID alerts

Alert	Description
Event ID 106	Failed to connect to Microsoft Entra ID during the Export step.
Event ID 109	Failed to connect to Microsoft Entra ID during the Import step.
Event ID 6801	Error occurred communicating with Microsoft Entra ID.
Event ID 6803	Generic - the Export step encountered one or more errors.
Event ID 6941	Export encountered one of the following errors: DataValidatinFailed, InvalidSoftMatch, or AttributeValueMustBeUnique. The 6941 error will be logged for each error.
Event ID 6001	Run profile failed because a connection could not be established to the server.
Event ID 611	Password Synchronization Full Sync has failed.
Event ID 6012	Full Import failed - no objects were returned from the operation.
Event ID 6100	Run profile step completed with errors. The event is logged as a warning. Additional information will be returned.
Event ID 6105	The “Exported Change not Reimported” error was returned during an Import run profile operation.
Event ID 6610, 6126, and 6127	The configuration has changed since the last run profile of this type (Import or Sync). A full import or sync was not performed.

b

Event Definitions

Event definitions are used to create alerts and reports. The event definitions file, EventDefinitions.edx, is located in the **Active Administrator\Server** folder. Occasionally new event definition files are made available. You can import these new event definitions into your auditing database. See Managing event definitions.

Table 148. Event Definitions

Event	Type
Active Administrator AFS Service Started	Active Administrator
Active Administrator AFS Service Stopped	Active Administrator
Active Administrator Alert Added	Active Administrator
Active Administrator Alert Deleted	Active Administrator
Active Administrator Alert Updated	Active Administrator
Active Administrator Audit Agent Activated	Active Administrator
Active Administrator Audit Agent Configuration Changed	Active Administrator
Active Administrator Audit Agent Installation Failed	Active Administrator
Active Administrator Audit Agent Installation Succeeded	Active Administrator
Active Administrator Audit Agent Moved	Active Administrator
Active Administrator Audit Agent Uninstalled	Active Administrator
Active Administrator Delegation Added	Active Administrator
Active Administrator Delegation Broken	Active Administrator
Active Administrator Delegation Removed	Active Administrator
Active Administrator Delegation Repaired	Active Administrator
Active Administrator Delegation Updated	Active Administrator
Active Administrator DNS Test Failed	Active Administrator
Active Administrator DNS Test Succeeded	Active Administrator
Active Administrator Domain Controller Excluded	Active Administrator
Active Administrator Event Definition Disabled	Active Administrator
Active Administrator Event Definition Enabled	Active Administrator
Active Administrator Event Purge History Cleared	Active Administrator
Active Administrator Event Purged / Archived	Active Administrator
Active Administrator Global Alert Quiet Time Added	Active Administrator
Active Administrator Global Alert Quiet Time Changed	Active Administrator
Active Administrator Global Alert Quiet Time Removed	Active Administrator
Active Administrator GPO History Backups Purged	Active Administrator
Active Administrator GPO Rollback Completed	Active Administrator
Active Administrator GPO Rollback Failed	Active Administrator
Active Administrator GPO Rollback Started	Active Administrator
Active Administrator Group Policy Object Added to the Repository	Active Administrator
Active Administrator Group Policy Object Checked Into the Repository	Active Administrator

Table 148. Event Definitions

Event	Type
Active Administrator Group Policy Object Checked Out of the Repository	Active Administrator
Active Administrator Group Policy Object Published to Active Directory	Active Administrator
Active Administrator Group Policy Object Removed from the Repository	Active Administrator
Active Administrator Group Policy Object Restored	Active Administrator
Active Administrator new Domain Controller Discovered	Active Administrator
Active Administrator Trustee Added	Active Administrator
Active Administrator Trustee Removed	Active Administrator
Active Directory Backup Completed	Active Administrator
Active Directory Backup Failed	Active Administrator
Active Directory Backup Purge History Cleared	Active Administrator
Active Directory Backup Started	Active Administrator
Active Directory Backups Purged	Active Administrator
Active Directory Replication Test Failed	Active Administrator
Active Directory Replication Test Succeeded	Active Administrator
Active Directory Restore Completed	Active Administrator
Active Directory Restore Failed	Active Administrator
Active Directory Restore Started	Active Administrator
Active Directory Shared Folder Changed	Shared Folder
Active Directory Shared Folder Created	Shared Folder
Active Directory Shared Folder Deleted	Shared Folder
AD Object Changed	General
AD Object Created	General
AD Object Renamed / Moved	General
Audit Agent Database Connectivity Lost	Active Administrator
Audit Agent Database Connectivity Restored	Active Administrator
Microsoft Entra Group Added	Microsoft Entra ID
Microsoft Entra Group Deleted	Microsoft Entra ID
Microsoft Entra Group Updated	Microsoft Entra ID
Microsoft Entra User Added	Microsoft Entra ID
Microsoft Entra User Deleted	Microsoft Entra ID
Microsoft Entra User Updated	Microsoft Entra ID
Certificate Added to Repository	Active Administrator
Computer Account Changed	Computer
Computer Account Created	Computer
Computer Account Deleted	Computer
Contact Changed	Contact
Contact Created	Contact
Contact Deleted	Contact
Domain Master Changed	FSMO
Domain Trust Created (Windows 2000 only)	Trust
Event Log Cleared	Security
Global Distribution Group Changed	Group

Table 148. Event Definitions

Event	Type
Global Distribution Group Created	Group
Global Distribution Group Deleted	Group
Global Group Changed	Group
Global Group Created	Group
Global Group Deleted	Group
GPO Changed	Group Policy
GPO Created	Group Policy
GPO Deleted	Group Policy
GPO Password Complexity Disabled **NOTE:** The added alert will not state the name of the changed GPO; there is an action description only.	Group Policy
GPO Password Complexity Enabled **NOTE:** The added alert will not state the name of the changed GPO; there is an action description only.	Group Policy
GPO Security Group Filters Changed	Group Policy
Group Policy Links Changed	Group Policy
Group Type Changed	Group
Infrastructure Master Changed	FSMO
Kerberos authentication ticket (TGT) was requested	User
Kerberos Pre-Auth Failed (Bad Password)	User
Local Distribution Group Changed	Group
Local Distribution Group Created	Group
Local Distribution Group Deleted	Group
Local Group Changed	Group
Local Group Created	Group
Local Group Deleted	Group
Logged onto DC (Local)	User
Logged onto DC (Remote)	User
Logon Failed (Bad Password)	User
Logon Failed (NTLM - Bad Password)	User
Logon Failed (NTLM - Unknown Username)	User
Logon Failed (Unknown Username)	User
Member Added to BUILTIN Group	Group Membership
Member Added to Global Distribution Group	Group Membership
Member Added to Global Group	Group Membership
Member Added to Local Distribution Group	Group Membership
Member Added to Local Group	Group Membership
Member Added to Universal Distribution Group	Group Membership
Member Added to Universal Group	Group Membership
Member Removed from BUILTIN Group	Group Membership
Member Removed from Global Distribution Group	Group Membership
Member Removed from Global Group	Group Membership
Member Removed from Local Distribution Group	Group Membership

Table 148. Event Definitions

Event	Type
Member Removed from Local Group	Group Membership
Member Removed from Universal Distribution Group	Group Membership
Member Removed from Universal Group	Group Membership
Object Owner Changed	Security
Object Permissions Changed	Security
One Way Incoming Trust Created	Trust
One Way Outgoing Trust Created	Trust
OU Changed	Organizational Unit
OU Created	Organizational Unit
OU Deleted	Organizational Unit
PDC Master Changed	FSMO
Printer Changed	Printer
Printer Created	Printer
Printer Deleted	Printer
Rejected Simple LDAP Bind Requests	LDAP Signing
Repository Certificate Delete	Active Administrator
Repository Certificate Updated	Active Administrator
RID Master Changed	FSMO
Schema Master Changed	FSMO
Site Changed	Site
Site Created	Site
Site Deleted	Site
SMTP Virtual Directory Changed	Exchange Server
Subnet Changed	Subnet
Subnet Created	Subnet
Subnet Deleted	Subnet
System Audit Policy Was Changed	Group Policy
System Time was Changed	System
Trust Deleted	Trust
Trust Modified	Trust
Two Way Trust Created	Trust
Universal Distribution Group Changed	Group
Universal Distribution Group Created	Group
Universal Distribution Group Deleted	Group
Universal Group Changed	Group
Universal Group Created	Group
Universal Group Deleted	Group
Unsigned LDAP Client Details	LDAP Signing
User Account Changed	User
User Account Created	User
User Account Deleted	User
User Account Disabled	User

Table 148. Event Definitions

Event	Type
User Account Enabled	User
User Account Locked Out	User
User Account Type Changed	User
User Account Unlocked	User
User Attribute Changed	User
User Change Password Attempt Failed	User
User Change Password Attempt Succeeded	User
User Locked Workstation	Workstation
User Logoff	Workstation
User Logon (Interactive for Windows 2016 Server)	Workstation
User Logon (Interactive)	Workstation
User Logon (Remote Desktop)	Workstation
User Password Reset	User
User Unlocked Workstation	Workstation
Windows Shutdown	System
Windows Started	System

PowerShell cmdlets

Microsoft® Windows PowerShell® is a Windows® command-line shell and scripting language designed specifically for system administrators and built on top of the Microsoft .NET Framework. Active Administrator supports the use of PowerShell cmdlets.

Topics

- What are cmdlets?
- Using Active Administrator cmdlets
- Using cmdlets to get information about the Active Administrator server
- Using cmdlets to manage the Active Administrator server
- Using cmdlets to manage Active Administrator tasks

What are cmdlets?

Windows PowerShell® has the concept of cmdlets. A cmdlet is a simple, single-function command that manipulates objects and is designed to be used in combination with other cmdlets.

If you already had Windows PowerShell installed on your computer before you installed Active Administrator®, the Active Administrator cmdlets were automatically installed and registered with Windows PowerShell.

The examples in this section show you leverage the cmdlets available in Active Administrator. These cmdlets allow you to perform many of the functions of Active Administrator in an automation environment. The cmdlets also can be of great use in any environment where a repetitive process involving Active Administrator is needed.

The complete set of cmdlets shipped with the module AA.ServerManagerPowerShellModule.dll is as follows.

NOTE: All cmdlets should be run while logged on as an Administrator. Some Active Administrator cmdlets must be run as an Administrator with elevated privileges (if UAC is enabled). The Active Administrator cmdlets should be used only by those familiar with Windows PowerShell.

NOTE: Those scripts that run under standard privileges are marked with an asterisk, others require elevated privileges.

Table 149. AA Server Manager cmdlets for use with Windows PowerShell®

Cmdlet	Module	Reference
Clear-AFSCache	AA.ServerManagerPowerShellModule	Clearing the AFS cache
Get-AAFeaturesLicenseStatus*	AA.ServerManagerPowerShellModule	Getting the status of Active Administrator licenses
Get-AAWebServerConfiguration	AA.ServerManagerPowerShellModule	Getting configuration settings for the Web server
Get-ADSLoggingStatus	AA.ServerManagerPowerShellModule	Getting logging status for ADS
Get-ADSOperationStatus*	AA.ServerManagerPowerShellModule	Getting operation status for ADS
Get-ADSPort	AA.ServerManagerPowerShellModule	Getting the port number for ADS

Table 149. AA Server Manager cmdlets for use with Windows PowerShell®

Cmdlet	Module	Reference
Get-AFSLoggingStatus	AA.ServerManagerPowerShellModule	Getting logging status for AFS
Get-AFSOperationStatus*	AA.ServerManagerPowerShellModule	Getting operation status for AFS
Get-AFSPort	AA.ServerManagerPowerShellModule	Getting the port number for AFS
Get-AFSHTTPOperationStatus	AA.ServerManagerPowerShellModule	Getting operation status for the HTTP service
Get-FullTextSearchStatus	AA.ServerManagerPowerShellModule	Getting the status of Full-Text Search
Get-NotificationService OperationStatus*	AA.ServerManagerPowerShellModule	Getting operation status for the Active Administrator Notification Service
Set-AALicense	AA.ServerManagerPowerShellModule	Updating the Active Administrator license
Set-AAWebServerConfiguration	AA.ServerManagerPowerShellModule	Setting configuration for the Active Administrator Web server
Set-ADSPort	AA.ServerManagerPowerShellModule	Setting the port for ADS
Set-AFSAndADSStartup Account	AA.ServerManagerPowerShellModule	Setting the startup account for AFS and ADS
Set-AFSPort	AA.ServerManagerPowerShellModule	Setting the port for AFS
Set-NotificationServiceStartup Account	AA.ServerManagerPowerShellModule	Setting the startup account for the Active Administrator Notification Service
Switch-ADSLoggingStatus	AA.ServerManagerPowerShellModule	Switching logging status of ADS
Switch-ADSOperationStatus	AA.ServerManagerPowerShellModule	Switching operation status of ADS
Switch-AFSLoggingStatus	AA.ServerManagerPowerShellModule	Switching logging status of AFS
Switch-AFSOperationStatus	AA.ServerManagerPowerShellModule	Switching operation status of AFS
Switch-AFSHTTPOperationSatus	AA.ServerManagerPowerShellModule	Switching operation status of the HTTP service
Switch-FullTextSearchStatus	AA.ServerManagerPowerShellModule	Switching the setting of Full-Text Search
Switch-NotificationService OperationStatus	AA.ServerManagerPowerShellModule	Switching operation status of the Active Administrator Notification Service

Using Active Administrator cmdlets

IMPORTANT: All command utilities should be run while logged on as an Administrator. Some cmdlets must be run as an administrator with elevated privileges (if UAC is enabled). The cmdlets should be used only by those familiar with Windows PowerShell®.

The Active Administrator® cmdlets function very similarly to the included utilities in the AA Server Manager application. The cmdlets are located at C:\Program Files\Quest\Active Administrator\Server\PowerShell.

Viewing help

You can view help by typing the cmdlt name with no arguments or by using `get-help`.

Running cmdlets

You can run the cmdlets from the PowerShell console (right-click the cmdlet, and choose **Run with PowerShell**) or PowerShell ISE (open the cmdlet in ISE and click **Run**).

Using cmdlets manually

If you want to use the cmdlets manually, you must include the two cross-cutting scripts for configuration (ConfigAndLoadModule.ps1) and rights management (EnsureElevatedPrivileges.ps1).

- ConfigAndLoadModule.ps1 loads the module and updates PowerShell configuration with necessary settings.

  Example

  ```
  if(-Not(&($PSScriptRoot + "\ConfigAndLoadModule.ps1"))){ exit; }
  ```

- EnsureElevatedPrivileges.ps1 uses UAC to rerun the script at the given path with elevated privileges if it finds that the script was run without proper permissions granted. It accepts as a parameter the path to the script that is to be rerun. The script can run from another script as follows, with the caller path detected at run time.

  NOTE: To run the elevated privileges cmdlet manually, the PowerShell should just be run as administrator.

  Example

  ```
  if(-Not(&($PSScriptRoot + "\EnsureElevatedPrivileges.ps1") -scriptPath
  $myinvocation.mycommand.definition)){ exit; }
  ```

Using cmdlets to get information about the Active Administrator server

Use these Active Administrator® cmdlets to see the current settings for the Active Administrator server.

NOTE: These cmdlets use `<CommonParameters>`, which are a set of PowerShell® cmdlet parameters that you can use with any cmdlet.

Topics

- Getting the status of Active Administrator licenses
- Getting configuration settings for the Web server
- Getting logging status for ADS
- Getting operation status for ADS
- Getting the port number for ADS
- Getting logging status for AFS
- Getting operation status for AFS
- Getting the port number for AFS
- Getting operation status for the HTTP service
- Getting the status of Full-Text Search
- Getting operation status for the Active Administrator Notification Service

Getting the status of Active Administrator licenses

Use this cmdlet to view the current status of Active Administrator® licenses. To update the Active Administrator licenses, use `Set-AALicense`. See Updating the Active Administrator license.

Syntax

```
Get-AAFeaturesLicenseStatus [<CommonParameters>]
```

Output

```
ProductName                     : Active Administrator
LicenseStatus                   : Installed
EvaluExpirationDateString       :
MaintenanceExpirationDateString :
LicenseMode                     : Perpetual
LicenseNumber                   : 123-456-789
Version                         : 8
IsEnterprise                    : False

ProductName                     : Active Administrator for Certificate Management
LicenseStatus                   : Installed
EvaluExpirationDateString       :
MaintenanceExpirationDateString :
LicenseMode                     : Perpetual
LicenseNumber                   : 123-456-789
Version                         : 8
IsEnterprise                    : False

ProductName                     : Active Administrator for DNS Management
LicenseStatus                   : Installed
EvaluExpirationDateString       :
MaintenanceExpirationDateString :
LicenseMode                     : Perpetual
LicenseNumber                   : 123-456-789
Version                         : 8
IsEnterprise                    : False

ProductName                     : Active Administrator for Active Directory Health
LicenseStatus                   : Installed
EvaluExpirationDateString       :
MaintenanceExpirationDateString :
LicenseMode                     : Perpetual
LicenseNumber                   : 123-456-789
Version                         : 8
IsEnterprise                    : False
```

Getting configuration settings for the Web server

This cmdlet returns the configuration settings for the Active Administrator® Web server. To change the settings for the Web server, use `Set-AAWebServerConfiguration`. See Setting configuration for the Active Administrator Web server.

Syntax

```
Get-AAWebServerConfiguration [<CommonParameters>]
```

Output

```
ServerPort               : 8080
LoggingEnabled           : True
LogFilesToKeep           : 7
SessionTimeoutEnabled    : True
```

```
SessionTimeout             : 60
AuthTokenExpirationPeriod : 1440
AuthTokenRefreshInterval  : 30
SslEnabled                 : False
SslPort                    : 9443
SslCertificateName         :
SslCertificateThumbprint   :
```

Getting logging status for ADS

Logging for the Active Administrator® Data Services (ADS) is either Enabled or Disabled. To switch the logging status, use `Set-ADSLoggingStatus`. See Switching logging status of ADS.

Syntax

```
Get-ADSLoggingStatus [<CommonParameters>]
```

Output

`Disabled` or `Enabled`

Getting operation status for ADS

Operation status for the Active Administrator® Data Services (ADS) is either Running or Stopped. To switch the operation status, use `Switch-ADSOperationStatus`. See Switching operation status of ADS.

Syntax

```
Get-ADSOperationStatus [<CommonParameters>]
```

Output

`Running` or `Stopped`

Getting the port number for ADS

This cmdlet returns the port number for Active Administrator® Data Services (ADS). To set the port number, use `Set-ADSPort`. See Setting the port for ADS.

Syntax

```
Get-ADSPort [<CommonParameters>]
```

Output

‘Port number for ADS.

Getting logging status for AFS

Logging for the Active Administrator® Foundation Services (AFS) is either Enabled or Disabled. To switch the logging status, use `Set-AFSLoggingStatus`. See Switching logging status of AFS.

Syntax

```
Get-AFSLoggingStatus [<CommonParameters>]
```

Output

`Disabled` or `Enabled`

Getting operation status for AFS

Operation status for the Active Administrator® Foundation Services (AFS) is either **Running** or **Stopped**. To switch the operation status, use `Switch-AFSOperationStatus`. See Switching operation status of AFS.

Syntax

```
Get-AFSOperationStatus [<CommonParameters>]
```

Output

`Running` or `Stopped`

Getting the port number for AFS

To set the port number for the Active Administrator® Foundation Service (AFS), use `Set-AFSPort`. See Setting the port for AFS.

Syntax

```
Get-AFSPort [<CommonParameters>]
```

Output

‘Port number for AFS.

Getting operation status for the HTTP service

Operation status for the Active Administrator® Foundation Services (AFS) HTTP service is either **Running** or **Stopped**. To switch the operation status, use `Switch-AFSHTTPOperationStatus`. See Switching operation status of the HTTP service.

Syntax

```
Get-AFSHTTPOperationStatus [<CommonParameters>]
```

Output

`Running` or `Stopped`

Getting the status of Full-Text Search

When filtering event descriptions for audit reports (see Creating a new audit report), Active Administrator® can use Full-Text Search. Status of Full-Text Search is either **Enabled** or **Disabled**. To switch the status of Full-Text search, use `Switch-FullTextSearchStatus`. See Getting the status of Full-Text Search.

Syntax

```
Get-FullTextSearchStatus [<CommonParameters>]
```

Output

`Disabled` or `Enabled`

Getting operation status for the Active Administrator Notification Service

Operation status for the Active Administrator® Notification Service is either **Running** or **Stopped**. To switch the operation status, use `Switch-NotificationServiceOperationStatus`. See Switching operation status of AFS.

Syntax

```
Get-NotificationServiceOperationStatus [<CommonParameters>]
```

Output

`Running` or `Stopped`

Using cmdlets to manage the Active Administrator server

These Active Administrator® cmdlets mirror the options provided in AA Server Manager. See Managing the Active Directory server.

Topics

- Updating the Active Administrator license
- Setting configuration for the Active Administrator Web server
- Switching the setting of Full-Text Search
- Setting the startup account for AFS and ADS
- Setting the port for ADS
- Switching logging status of ADS
- Switching operation status of ADS
- Setting the port for AFS
- Switching logging status of AFS
- Switching operation status of AFS
- Switching operation status of the HTTP service
- Clearing the AFS cache
- Setting the startup account for the Active Administrator Notification Service
- Switching operation status of the Active Administrator Notification Service

Updating the Active Administrator license

This cmdlet updates the Active Administrator® license. For the corresponding option in AA Server Manager, see Updating Active Administrator licenses.

NOTE: After upgrading the license, you should restart the Active Administrator® Foundation Service (AFS), Active Administrator Data Services (ADS), and the AFS HTTP service. See Switching operation status of AFS, Switching operation status of ADS, and Switching operation status of the HTTP service.

Syntax

```
Set-AALicense [-FilePath <string>] [<CommonParameters>]
```

Example

This example updates the Active Administrator license. To see the current Active Administrator license details, use `Get-AAFeaturesLicenseStatus`. See Getting the status of Active Administrator licenses.

Setting configuration for the Active Administrator Web server

This cmdlet updates the configuration settings for the Active Administrator® Web server. For the corresponding option in AA Server Manager, see Configuring the Web server.

Syntax

```
Set-AAWebServerConfiguration [-ServerPort <int>] [-LoggingEnabled <bool>] [-
LogFilesToKeep <int>] [-SessionTimeoutEnabled <bool>] [-SessionTimeout <int>] [-
AuthTokenExpirationPeriod <int>] [-AuthTokenRefreshInterval <int>] [-SslEnabled
<bool>] [-SslPort <int>] [-SslCertificateName <string>] [-SslCertificateThumbprint
<string>] [<CommonParameters>]
```

Example

In this example, the port for the Web Server is set to 8080; logging is enabled and 10 log files are kept; session timeout is enabled and the duration is set to 30; and SSL is not enabled, and the port is set to 9443. To view the current settings, use Get-AAWebServerConfiguration. See Getting configuration settings for the Web server.

```
Set-AAWebServerConfiguration [-ServerPort <8080>] [-LoggingEnabled <True>] [-
LogFilesToKeep <10>] [-SessionTimeoutEnabled <True>] [-SessionTimeout <30>] [-
AuthTokenExpirationPeriod <1440>] [-AuthTokenRefreshInterval <25>] [-SslEnabled
<False>] [-SslPort <9443>]
```

Switching the setting of Full-Text Search

This cmdlet switches the setting of Full-Text Search from **Enabled** to **Disabled**, or **Disabled** to **Enabled**. For the corresponding option in AA Server Manager, see Enabling Full-Text Search.

Syntax

```
Switch-FullTextSearchStatus [<CommonParameters>]
```

Example

If the status is **Disabled**, running this command changes the status to **Enabled**. To view the current status, use `Get-FullTextSearchStatus`.See Getting the status of Full-Text Search.

Setting the startup account for AFS and ADS

This cmdlet sets the username and password for the startup account for both the Active Administrator® Foundation Service (AFS) and Active Administrator Data Services (ADS). For the corresponding option in AA Server Manager, see Setting the services startup accounts.

Syntax

```
Set-AFSAndADSStartupAccount [-UserName <string>] [-Password <string>]
[<CommonParameters>]
```

Example

This example sets the AFS and ADS startup account to SALES\administrator and the password to 456PP988.

```
Set-AFSAndADSStartupAccount [-UserName <SALES\administrator>] [-Password <456PP988>]
```

Setting the port for ADS

This cmdlet sets the port for Active Administrator® Data Services (ADS). For the corresponding option in AA Server Manager, see Setting port numbers for services.

Syntax

```
Set-ADSPort [-PortNumber <int>] [<CommonParameters>]
```

Example

This example sets the port for ADS to 15602. To see the current port setting for ADS, use `Get-ADSPort`. See Getting the port number for ADS.

```
Set-ADSPort [-PortNumber <15602>]
```

Switching logging status of ADS

This cmdlet switches the logging status of Active Administrator® Data Services (ADS) from **Enabled** to **Disabled**, or **Disabled** to **Enabled**. For the corresponding option in AA Server Manager, see Managing logging for services.

Syntax

```
Switch-ADSLoggingStatus [<CommonParameters>]
```

Example

If the logging status is **Disabled**, running this cmdlet changes the status to **Enabled**. To view the current status, use `Get-ADSLoggingStatus`. See Getting logging status for ADS.

Switching operation status of ADS

Switch the operation status of Active Administrator® Data Services (ADS) from **Running** to **Stopped**, or **Stopped** to **Running**. For the corresponding option in AA Server Manager, see Stopping and starting AFS and ADS services.

Syntax

```
Switch-ADSOperationStatus [<CommonParameters>]
```

Example

If the operation status is **Running**, running this cmdlet changes the status to **Stopped**. To view the current status, use `Get-ADSOperationStatus`. See Getting operation status for ADS.

Setting the port for AFS

This cmdlet sets the port for Active Administrator® Foundation Service (AFS). For the corresponding option in AA Server Manager, see Setting port numbers for services.

Syntax

```
Set-AFSPort [-PortNumber <int>] [<CommonParameters>]
```

Example

This example sets the port for AFS to 15601. To see the current port setting for ADS, use `Get-AFSPort`. See Getting the port number for AFS.

```
Set-AFSPort [-PortNumber <15601>]
```

Switching logging status of AFS

Switch the logging status of Active Administrator® Foundation Service (AFS) from **Enabled** to **Disabled**, or **Disabled** to **Enabled**. For the corresponding option in AA Server Manager, see Managing logging for services.

Syntax

```
Switch-AFSLoggingStatus [<CommonParameters>]
```

Example

If the logging status is **Disabled**, running this cmdlet changes the status to **Enabled**. To view the current status, use `Get-AFSLoggingStatus`. See Getting logging status for AFS.

Switching operation status of AFS

This cmdlet switches the operation status of Active Administrator® Foundation Service (AFS) from **Running** to **Stopped**, or **Stopped** to **Running**. For the corresponding option in AA Server Manager, see Stopping and starting AFS and ADS services.

Syntax

```
Switch-AFSOperationStatus [<CommonParameters>]
```

Example

If the operation status is **Running**, running this cmdlet changes the status to **Stopped**. To view the current status, use `Get-AFSOperationStatus`. See Getting operation status for AFS.

Switching operation status of the HTTP service

This cmdlet switches the operation status of Active Administrator® Foundation Service (AFS) HTTP service from **Running** to **Stopped**, or **Stopped** to **Running**.

Syntax

```
Switch-AFSHTTPOperationStatus [<CommonParameters>]
```

Example

If the operation status is **Running**, running this cmdlet changes the status to **Stopped**. To view the current status, use `Get-AFSHTTPOperationStatus`. See Getting operation status for the HTTP service.

Clearing the AFS cache

Use this cmdlet to clear the Active Administrator® Foundation Service (AFS) cache. For the corresponding option in AA Server Manager, see Clearing the AFS cache.

Syntax

Clear-AFSCache [<CommonParameters>]

Setting the startup account for the Active Administrator Notification Service

This cmdlet sets the username and password for the startup account for the Active Administrator® Notification Service. For the corresponding option in AA Server Manager, see Setting the services startup accounts

Syntax

```
Set-NotificationServiceStartupAccount [-UserName <string>] [-Password <string>]
[<CommonParameters>]
```

Example

This example sets the Notification Service startup account to SALES\administrator and the password to 456PP988.

```
Set-NotificationServiceStartupAccount [-UserName <SALES\administrator>] [-Password
<456PP988>]
```

Switching operation status of the Active Administrator Notification Service

This cmdlet switches the operation status of Active Administrator® Notification Service from **Running** to **Stopped**, or **Stopped** to **Running**. For the corresponding option in AA Server Manager, see Stopping and starting AFS and ADS services.

Syntax

```
Switch-NotificationServiceOperationStatus [<CommonParameters>]
```

Example

If the operation status is **Running**, running this cmdlet changes the status to **Stopped**. To view the current status, use `Get-NotificationServiceOperationStatus`. See Getting operation status for the Active Administrator Notification Service.

Using cmdlets to manage Active Administrator tasks

The ActiveAdministrator module contains cmdlets used to support the management of Active Administrator tasks. This module is imported with the Active Administrator console and can be accessed using the **Settings | AA PowerShell Console** menu option.

To use the ActiveAdministrator module cmdlets for managing Active Administrator tasks without installing the Active Administrator console, the following configuration is required:

- Copy the cmdlets are located at C:\Program Files\WindowsPowerShell\Modules to your local computer.
- Run the `Import-Module ActiveAdministrator` command to import the module.
- Run the configuration command `Set-AFSConnectionSettings -Host 127.0.0.1 -Port 15600` to set up the AFS service connection service settings for the module. Provide the host IP and port that your Active Administrator Console is using to configure the module server connection. This configuration command must be used at least once before the first use of the ActiveAdministrator PowerShell module and each time the server configuration settings are changed.

Topics

- Active Templates and Delegations Cmdlets

Active Templates and Delegations Cmdlets

To display all cmdlets in the module, use the command

```
Get-Command -Module ActiveAdministrator.ClientDelegations
```

Table 150. Active Templates and Delegations Cmdlets

Cmdlet	Module
Get-AASchemaClasses	Active Administrator.ClientDelegations
Get-AASchemaPermissions	Active Administrator.ClientDelegations
Get-ActiveTemplate	Active Administrator.ClientDelegations
Get-ActiveTemplateCategories	Active Administrator.ClientDelegations
Get-ADObjects	Active Administrator.ClientDelegations
Get-Delegation	Active Administrator.ClientDelegations
New-ActiveTemplate	Active Administrator.ClientDelegations
New-Delegation	Active Administrator.ClientDelegations
Remove-ActiveTemplate	Active Administrator.ClientDelegations
Remove-Delegation	Active Administrator.ClientDelegations
Set-ActiveTemplateDescription	Active Administrator.ClientDelegations
Set-ActiveTemplateName	Active Administrator.ClientDelegations
Set-ActiveTemplatePermissions	Active Administrator.ClientDelegations
Set-AFSConnectionSettings	Active Administrator.ClientDelegations
Set-DelegationDescription	Active Administrator.ClientDelegations
Set-DelegationExpirationDate	Active Administrator.ClientDelegations
Set-DelegationPath	Active Administrator.ClientDelegations
Set-DelegationStartDate	Active Administrator.ClientDelegations
Set-DelegationTemplate	Active Administrator.ClientDelegations

To display the parameters available with a cmdlet, use the Get-Help command. There are four options for the Get-Help command.

- `Get-Help <command name>` shows the common information about the cmdlet.
- `Get-Help <command name> -examples` shows the examples of how the cmdlet can be utilized.
- `Get-Help <command name> -detailed` shows common information about the cmdlet, describes parameter formats, and provides examples of how the cmdlet can be utilized.
- `Get-Help <command name> -full` shows common information about the cmdlet, describes parameter formats and specifications, and provides examples of how the cmdlet can be utilized.

Example

```
Get-Help New-ActiveTemplate.

NAME

     New-ActiveTemplate

SYNOPSIS

     Creates a new active template and returns its Id.
```

```
SYNTAX

     New-ActiveTemplate [-Category <string>] [-Forest <string>] [-Name <string>] [-
     Description <string>] [-Allow<string[]>] [-Deny <string[]>] [-Create
     <string[]>] [-Delete <string[]>] [<CommonParameters>]

DESCRIPTION

     Creates a new active template for the forest and returns its newly generated
     Id.

RELATED LINKS

REMARKS

     To see the examples, type: "get-help New-ActiveTemplate -examples".

     For more information, type: "get-help New-ActiveTemplate -detailed".

     For technical information, type: "get-help New-ActiveTemplate -full".
```

d

Appendix: Registering Active Administrator for Office 365 Exchange Online

To use email notifications using Office 365 Exchange Online, you need to register Active Administrator with Microsoft Entra ID. During the registration process, the following variables are generated. These variables are used when you configure Exchange Online authentication.

- Application ID: Required to authenticate to your Microsoft Entra tenant.
- Tenant ID: The tenant associated with the client.

To register an application for Office 365 Exchange Online through Microsoft Entra ID:

1. Log into the Microsoft Entra admin center (https://portal.azure.com/) with your global administrator user account.
2. In the Microsoft Azure dashboard, go to **Microsoft Entra ID | App registrations**, and click **New Registration**.
3. Enter a name for the application.
4. Under Supported account types, select **Accounts in this organizational directory only (Single tenant)** for the accounts that can access the application API.
5. Leave the **Redirect URI (optional)** field empty.
6. Click **Register**.
7. On the **Overview** tab, go to View API Permissions. Click **Add a permission**, click **Microsoft Graph | Application Permissions** and add the **Mail.ReadWrite and Mail.Send** permissions. See Microsoft documentation for details on limiting permissions to specific Exchange Online mailboxes. (Note: The **Enforce approver account validation** option found when configuring email notifications will not function if you select to follow the Microsoft article to restrict access to a single mailbox.)
8. Click **Add Permission**.
9. On the **API Permissions** tab, under **Grant consent**, click **Grant admin consent** for tenant name.
10. Click **Yes** to confirm.
11. On the preview screen, click **Overview**, and note the application ID and the directory ID. (You will need these values when setting up email settings.)
12. Go to **Manage | Certificates & secrets**, select **Upload certificate** and upload the required .cer file.

About us

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

Technical support resources

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

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

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