One Identity Active Roles Diagnostic Tools 1.4.0

Release Notes

December 2019

These release notes provide information about the One Identity Active Roles Diagnostic Tools release.

About One Identity Active Roles Diagnostic Tools 1.4.0

This release of Diagnostic Tools provides the following tools:

- System Checker Check your computer, SQL Server, and Active Directory domains to see if you are ready to deploy Active Roles.
- Log Viewer Examine Active Roles diagnostic logs and event logs. Find Knowledge Articles that may help you resolve errors.
- Directory Changes Monitor Get statistic of directory changes that occurred in a particular Active Directory domain.

System Checker

System Checker performs a number of checks on your computer, and produces a report allowing you to see if the computer is ready for Active Roles versions 7.2, 7.3, or 7.4. You must fix any reported errors before you install Active Roles. In addition, you can use System Checker to see if a given SQL Server instance can host Active Roles databases and whether a given Active Directory domain can be managed by Active Roles.

System Checker performs, and reports the results of the following checks:

- System readiness checks that verify:
  - The hardware prerequisites, including the amount of installed physical memory (RAM), the processor speed and architecture (x86 or x64)
  - The version and edition of the Windows operating system that the computer runs
- Whether Active Roles software prerequisites are installed, including:
  - Microsoft .NET Framework 4.7.2
  - Windows Management Framework 5.1
  - Microsoft Visual C++ 2017 Redistributable
  - Microsoft OLE DB Driver for SQL Server
  - Web Server (IIS)
  - Windows PowerShell Execution Policy
  - Azure Active Directory Module for Windows PowerShell
  - Windows PowerShell Module for Lync/Skype for Business
  - SharePoint Online Management Shell
- Whether the PowerShell execution policy allows running PowerShell scripts on the computer

Which system readiness checks are performed depends upon the operating system the computer runs and upon the Active Roles components you are going to install. System Checker allows you to select the desired components, and then performs only the checks that apply to the components you selected. For example, the check for the Web Server (IIS) server role is performed only if you have selected the Web Interface component.

- SQL Server checks where you specify the SQL Server instance to check, along with the connection authentication method and credentials, and get a report showing:
  - Whether the specified SQL Server instance can be contacted on the network with the specified connection credentials
  - Response time, which indicates how fast the SQL Server instance is
  - Whether the version and edition of the SQL Server instance meet the minimum requirements for the Active Roles database server and replication
  - Whether the server collation of the SQL Server instance meets the requirements for the Active Roles database server
  - Whether the specified connection credentials have sufficient rights to create an Active Roles database.
- Active Directory checks where you specify the Active Directory domain or the domain controller to check, along with domain connection credentials, and get a report showing:
  - Whether the specified domain or domain controller can be contacted on the network with the specified connection credentials
  - Response time, which indicates how fast the domain controller is

- Whether the specified connection credentials have sufficient rights to publish the Active Roles Administration Service in the specified domain
- Whether the specified connection credentials provide sufficient rights for the Active Roles Administration Service to perform Exchange recipient management tasks in the specified domain

Log Viewer

Log Viewer enables you to browse and analyze diagnostic log files created by the Active Roles Administration Service as well as event log files created by saving the Active Roles event log in Event Viewer on the computer running the Administration Service. This tool can help you drill down through the sequence or hierarchy of requests processed by the Administration Service, identify error conditions that the Administration Service encountered during request processing, and find Knowledge Articles that apply to a given error condition.

With Log Viewer, you can open an Active Roles diagnostic log file (ds.log) or saved event log file (.evtx) and view a list of:

- Errors encountered by the Administration Service and recorded in the log file
- Requests processed by the Administration Service and traced in the log file
- All trace records found in the diagnostic log file
- All events found in the event log file

When you select an error in the list, you can choose a command to look for solution in Knowledge Base. The command performs a search in One Identity Software Knowledge Base to list the Knowledge Articles that can provide helpful information on how to troubleshoot the error you selected.

Log Viewer also enables you to:

- Search the list for a particular text string, such as an error message
- Filter the list by various conditions, to narrow the set of list items to those you are interested in
- View detailed information about each list item, such as error details, request details or stack trace

Directory Changes Monitor

Directory Changes Monitor is a command-line tool that enables you to create a log of changes that occur in a particular Active Directory domain within a given time frame. The statistic of changes may be helpful in diagnosing error conditions that are due to a large number of search results Active Roles receives from the DirSync control when polling for changes in Active Directory.

The log file created by this tool provides statistic information about the number of detected changes and, for each of the detected changes, includes a record identifying:

- The time that the change occurred
- The changed object
- The type of the change
- The type of the changed object
- The object's attributes that were changed

Known issues

There are no issues known to exist at the time of release.

System requirements

Before installing Active Roles Diagnostic Tools 1.4.0, ensure that your system meets the following minimum hardware and software requirements.

Table 1: Active Roles Diagnostic Tools hardware and software requirements

Requirement	Details
Platform	1 gigahertz (GHz) or faster 32-bit (x86) or 64-bit (x64) processor
Memory	At least 1 GB of RAM The amount required depends upon the size of the log file opened by Log Viewer.
Hard disk space	About 10 MB of free disk space.
Operating system	Any of the following: • Microsoft Windows 8 or 8.1 • Microsoft Windows 10 • Microsoft Windows Server 2008 R2 Service Pack 1 • Microsoft Windows Server 2012 or 2012 R2 • Microsoft Windows Server 2016 • Microsoft Windows Server 2019

Requirement	Details
Microsoft .NET Framework	Log Viewer and Directory Changes Monitor require .NET Framework 4.7.2. System Checker requires .NET Framework 4.7.2 or later. For .NET Framework installation instructions, see "Installing the .NET Framework" at http://go.microsoft.com/fwlink/?LinkId=257868.

Product licensing

Use of this software is governed by the Software Transaction Agreement found at www.oneidentity.com/legal/sta.aspx. This software does not require an activation or license key to operate.

Getting started with Active Roles Diagnostic Tools 1.4.0

- Installation instructions
- Using System Checker
- Using Log Viewer
- Using Directory Changes Monitor

Installation instructions

To install Active Roles Diagnostic Tools, run the file **ActiveRolesDiagnosticTools.msi**, and follow the instructions in the Setup wizard.

Using System Checker

You can start System Checker by running the **Active Roles System Checker** application from the **Start** menu or **Apps** page, depending upon your version of the Windows operating system.

From the System Checker main window, you can perform the following tasks:

- To check your computer, click **System Readiness Checks**, select the Active Roles version 7.0, 7.1, 7.2, 7.3, or 7.4, and select the Active Roles components for which to perform the checks.
- To check a particular SQL Server instance, click **SQL Server Checks** and specify the SQL Server instance to check. You can also specify the authentication method and connection credentials for access to the SQL Server instance.
- To check a particular Active Directory domain or a particular domain controller, click **Active Directory Checks** and specify the name of the domain or the name of the domain controller. You can also specify connection credentials for access to the domain/domain controller.

System Checker creates a report depending upon what you selected to check, and displays the report in the report viewer. Reports are divided into sections each of which represents the results of a single check (for a list of all possible checks, see System Checker earlier in this document). If a given report section includes any error or warning messages, you can view the messages by expanding the section in the report viewer.

The report viewer also allows you to:

- Print the report
- Export the report to an HTML file, so you can open the report in a Web browser
- Save the report to a report file, so you can open the saved report in the report viewer
- To open a saved report, click **Open** in the System Checker main widow and select the report file.
- Rebuild the report, possibly changing the report options

To rebuild the report, click **Recheck** on the toolbar in the report viewer.

Using Log Viewer

You can start Log Viewer by running the **Active Roles Log Viewer** application from the **Start** menu or **Apps** page, depending upon your version of the Windows operating system.

Once you have started Log Viewer, open your Active Roles diagnostic log file or saved event log file: Click **Open** on the Log Viewer toolbar, and supply the path and name of the log file.

By default, Log Viewer displays a list of errors encountered by the Administration Service and recorded in the log file. You can use Log Viewer to look for information on how to troubleshoot a given error: Right-click the error in the list and then click **Look for solution in Knowledge Base**. Log Viewer performs a search in all the Knowledge Bases to list the Knowledge Articles that apply to the error you selected.

Other tasks you can perform:

- To view a list of requests processed by the Administration Service and traced in the log file, click **Requests** in the **View** area on the Log Viewer toolbar.

- To view all trace records found in the diagnostic log file or all events found in the event log file, click **Raw log records** in the **View** area on the Log Viewer toolbar.
- To search the list for a particular text string, such as an error message, type the text string in the **Search** box on the Log Viewer toolbar and press Enter.
- To narrow the set of list items to those you are interested in, click **Filter** on the Log Viewer toolbar and specify the desired filter conditions.
- To view detailed information about an error, request, trace record or event, right-click the corresponding list item, and click **Details**.
- To view all trace records that apply to a given request, right-click the corresponding item in the **Requests** list and click **Stack trace**. This task is unavailable in case of an event log file.
- To view the request that caused a given error, right-click the error in the **Errors** list and click **Related request**. This task is unavailable in case of an event log file.
- To view all trace records that apply to the request that caused a given error, right-click the error in the **Errors** list and click **Stack trace for related request**. This task is unavailable in case of an event log file.

Using Directory Changes Monitor

Directory Changes Monitor is a command-line tool. To use this tool, run `cmd.exe` to open a command prompt; then, at the command prompt, switch to the folder containing the file `dirchangesmon.exe`, and execute that file with the appropriate parameters. For parameter descriptions, type `dirchangesmon.exe /?`.

The parameter set includes a single required parameter that identifies the domain controller of the Active Directory domain from which you want to get statistic of directory changes. To be able to retrieve information from a given domain, the tool must be run under a domain user account from that domain (or from a trusted domain).

Globalization

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

This release is Unicode-enabled and supports any character set. It supports simultaneous operation with multilingual data. This release is targeted to support operations in the following regions: North America, Western Europe and Latin America, Central and Eastern Europe, Far-East Asia, Japan.

About us

One Identity solutions eliminate the complexities and time-consuming processes often required to govern identities, manage privileged accounts and control access. Our solutions enhance business agility while addressing your IAM challenges with on-premises, cloud and hybrid environments.

Contacting us

For sales or other inquiries, visit https://www.oneidentity.com/company/contact-us.aspx or call +1-800-306-9329.

Technical support resources

Technical support is available to One Identity customers with a valid maintenance contract and customers who have trial versions. You can access the Support Portal at https://support.oneidentity.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 at www.YouTube.com/OneIdentity
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

Legend

WARNING: A WARNING icon indicates a potential for property damage, personal injury, or death.

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

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

Active Roles Diagnostic Tools Release Notes
Updated - December 2019
Version - 1.4.0