

Authentication Services ActiveRoles Integration Pack 2.1.x

Release Notes

June 2018

These release notes provide information about the Authentication Services ActiveRoles Integration Pack release.

Topics:

- [About this release](#)
- [Enhancements](#)
- [Resolved issues](#)
- [System requirements](#)
- [Product licensing](#)
- [Upgrade and installation instructions](#)
- [More resources](#)
- [Globalization](#)
- [About us](#)

About this release

ActiveRoles Server offers a practical approach to automated user provisioning and administration, for maximum security and efficiency. It provides total control of user provisioning and administration for Active Directory.

Authentication Services extends the capabilities of UNIX, Linux and Mac systems to seamlessly and transparently join Active Directory and integrate Unix identities with Active Directory Windows accounts.

Through the Authentication Services ActiveRoles Integration Pack, ActiveRoles Server extends management control to Unix and Linux identities such as Unix-enabled users and groups. Query-based management views show all of the identities, business rules ensure and enforce appropriate administrative practices, permission templates make it easy to delegate identity management.

For more information about this Authentication Services ActiveRoles Integration Pack, refer to the Authentication Services ActiveRoles Integration Pack Administration Guide included with the release package.

Enhancements

The Authentication Services ActiveRoles Integration Pack code was recompiled using the latest software development tools so that it is now compatible with ActiveRoles Server versions 7.0 or higher.

Resolved issues

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

Table 1: General resolved issues

Resolved Issue
Added support for Active Roles 7.3.

System requirements

Before installing Authentication Services ActiveRoles Integration Pack, ensure that your system meets the minimum hardware and software requirements for your platform. The operating system patch level, hardware, and disk requirements vary by Unix, Linux, and Active Directory platform, and are details in the *One Identity Authentication Services Administration Guide* in the docs directory of the product DVD.

Use of RFC 2307 attributes in the user object and for storage of NIS maps requires the installation of the Microsoft Windows Server 2003 R2 schema.

Product licensing

This product does not require a license.

Upgrade and installation instructions

The Integration pack is not meant to be upgraded. Each version of the Integration Pack installs its policy objects, access templates, scripts and managed units into a version-specific container to isolate the data objects for each version. However, the Integration Pack shares Web interface modifications between all versions. For this reason, One Identity recommends that you uninstall the previous version before installing the new version.

When upgrading from one version of the Integration Pack to another, any customizations to Integration Pack data objects will be lost. To preserve Integration Pack customizations, One Identity recommends that you backup the modified objects before you uninstall the previous version. That is, copy or move the Access Templates, Policy Objects, Script Modules, or Virtual Attributes created by the old version of the Authentication Services Support Pack for ActiveRoles Server Web Interface to a new location using ActiveRoles Server management console. These objects are located in the ActiveRoles Server configuration container.

Installing the Integration Pack

To install the Authentication Services ActiveRoles Integration

1. Click `arsqas-2.1.x.msi` file to start the InstallShield Wizard.
2. At the **Welcome** page, click **Next**.
3. At the **Licence Agreement** page, accept the terms in the license and click **Next**.
4. At the **Ready to Install** page, click **Install**.
5. When the InstallShield Wizard completes, leave the **Launch setup wizard** option selected and click **Finish**.

Wait while the ActiveRoles Integration Configuration Wizard starts.

6. Select the ActiveRoles Server web sites that you want to extend for Authentication Services and click **Continue**.

NOTE: You can manage your ActiveRoles Server web sites using standard ActiveRoles Server functionality. From the **Start** menu, navigate to **All Programs | Quest Software | Authentication Services ActiveRoles Integration | ActiveRoles Integration Configuration Wizard** to start the wizard which will help you configure web sites including newly created web sites for the ActiveRoles Server web interface.

NOTE: Every time you create and configure a new web site for the ActiveRoles Server Web Interface, you must run the ActiveRoles Integration Configuration Wizard.

7. When the configuration setup wizard completes, click **Restart ActiveRoles Now**.

8. When it becomes active, click the **Close** button and wait for a minute while ActiveRoles Server loads the startup information.
 - ① **NOTE:** Once the service restarts, wait a few minutes before you open the ActiveRoles Server console.
9. There are two ways to start the ActiveRoles Server Console:
 - a. From the **Start** menu, navigate to **All Programs | Quest Software | ActiveRoles Server | ActiveRoles Server Console**.
 - OR-
 - b. You can also access the ActiveRoles Server Console from the Authentication Services Control Center. Navigate to **Start | All Programs | Quest Software | Quest Authentication Services | Authentication Services Control Center**.

Once the console is open, look for the **Authentication Services Integration Pack v2.1.x** folder under these nodes:

- Access Templates
- Managed Units
- Policies | Administration
- Script Modules
- Server Configuration | Policy Types
- Applications

More resources

Additional information is available from the following:

- Online product documentation: <https://support.oneidentity.com/authentication-services/technical-documents>
- One Identity | Privileged Account Management: <https://www.quest.com/community/products/one-identity/f/privileged-account-management>

Globalization

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

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

This release has the following known capabilities or limitations: There is no localization.

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

Copyright 2018 One Identity LLC.

ALL RIGHTS RESERVED.

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

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

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

One Identity LLC.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Refer to our Web site (<http://www.OneIdentity.com>) for regional and international office information.




Patents

One Identity 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 <http://www.OneIdentity.com/legal/patents.aspx>.

Trademarks

One Identity and the One Identity logo are trademarks and registered trademarks of One Identity LLC. in the U.S.A. and other countries. For a complete list of One Identity trademarks, please visit our website at www.OneIdentity.com/legal. All other trademarks are the property of their respective owners.

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.**