

# One Identity Starling Identity Analytics & Risk Intelligence

## Release Notes

### 20 November 2019

These release notes provide information about the 20 November 2019 Starling Identity Analytics & Risk Intelligence release.

## About this release

Accessible from the One Identity Starling site (<https://www.cloud.oneidentity.com/>), this service is used for collecting and evaluating entitlement data. This is done by connecting the cloud-based Starling Identity Analytics & Risk Intelligence with your on-premises data source. Once connected, Starling Identity Analytics & Risk Intelligence analyzes the data to quickly and efficiently compare entitlements and users within those data sources. This allows you to determine which of your users are classified as high risk, which of their entitlement classification rules are the cause of this classification, and to resolve any discrepancies between users who require similar permissions.

Starling Identity Analytics & Risk Intelligence 20 November 2019 is a general release.

## New features

New features in the 20 November 2019 release of Starling Identity Analytics & Risk Intelligence:

- Starling Identity Analytics & Risk Intelligence new subscriptions unavailable – Starling Identity Analytics & Risk Intelligence is in the process of being removed. New subscriptions are no longer available.

# Deprecated features

The following is a list of features that are no longer supported for Starling Identity Analytics & Risk Intelligence.

- Starling Identity Analytics & Risk Intelligence new subscriptions unavailable: Starling Identity Analytics & Risk Intelligence is in the process of being removed. New subscriptions are no longer available.

# Resolved issues

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

- There were no resolved issues.

# Known issues

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

- There are no known issues for this release.

# System requirements

Before using the 20 November 2019 Starling Identity Analytics & Risk Intelligence release, ensure that your system meets the following minimum hardware and software requirements.

# Browser requirements

**Table 1: Browser requirements**

Browser	Minimum OS/Platform	Version
Internet Explorer	Windows 7	11
Google Chrome	Windows 10	Latest
	Android	

Browser	Minimum OS/Platform	Version
	Mac OS X Yosemite	
Mozilla Firefox	Windows 8.1	Latest
Microsoft Edge	Windows 10	Latest
Safari	Mac OS X Yosemite IOS 8	See OS/Platform
Opera	Windows 7 Mac OS X Yosemite	Latest

## Collector agent requirements

The Starling Identity Analytics & Risk Intelligence collector agent has some additional hardware and software requirements before it can be downloaded:

**Table 2: Starling Identity Analytics & Risk Intelligence Collector Agent requirements**

Operating System	Minimum requirements: Windows Server 2008 R2 SP1 x64
Memory	8GB
Server Software	.Net Framework 4.6.1

## Data source module requirements

Once a collector agent has been installed you can begin configuring data sources modules. The following table shows the requirements based on the type of data source module you are configuring.

**Table 3: Starling Identity Analytics & Risk Intelligence data source module requirements**

Type of data source module	Requirements
Active Roles	ARS 6.9 to 7.x  <b>IMPORTANT:</b> Although supported, it is strongly recommended that a collector agent not be installed on a machine with an ARS server.

## Type of data source module

## Requirements

- At minimum a domain member account with read access delegated to the following three Active Roles nodes is required: Configuration, Managed Units, and Active Directory.

The Active Directory template **All Objects - Read All Properties** contains these minimum permissions and can be used. Or you can create a custom template so long as it contains those minimum permissions. See the Active Roles documentation for information on configuring permissions within Active Roles.

**NOTE:** By default, Distributed COM Users should contain Authenticated Users. However, if this is missing then you will be unable to connect to Active Roles remotely. For more information, see this [article](#) on adding MinARSAdmin or the exact account in order to fix this issue.

- If both 6.9 and 7.x ADSI providers are available, the ARS 7.x ADSI provider will take precedence followed by 6.9 unless the ActiveRolesAdsiVersion environment variable (in the collector configuration file) has been edited to indicate either 6.9 or 7.0 (which covers all 7.x versions) as the specific version. No other versions can be used as the ActiveRolesAdsiVersion environment variable.
- If no ADSI providers are installed, 6.9 and 7.2.0 ADSI providers will be installed. If an ADSI provider is detected, the collector agent will attempt to use that ADSI provider without installing additional providers.
- When a collector agent is removed, any ADSI providers that were originally installed by the collector agent will also be removed. Any additional dependencies that were installed will not be removed since they are standard Windows redistributables.
- Should an ARS installation not fully meet the supported version requirements for all detected ARS Administration Services, this will cause a version compatibility problem and the collector agent will be unable to collect from that installation.

### Active Directory

- Active Directory credentials are required for configuring the data source module.
- A global catalog must be available in order to resolve trustees outside of the domain.

Type of data source module	Requirements
	<ul style="list-style-type: none"> <li>A global catalog must be resolvable via its DNS name regardless of whether you are connecting directly to it or to a domain controller connected with a global catalog.</li> </ul>
Safeguard	<p>Safeguard 2.1.0.0 (or greater)</p> <ul style="list-style-type: none"> <li>A Safeguard user with Auditor permissions is required for configuring the data source module.</li> <li>The machine running the Safeguard data source module must have the proper SSL root certificate authority certificate(s) that are being used by Safeguard. For more information, see <i>SSL Certificates</i> in the <i>One Identity Safeguard Administration Guide</i> (<a href="#">Safeguard documentation</a>).</li> </ul>

## Product licensing

Use of this software is governed by the Software Transaction Agreement found at <http://www.oneidentity.com/legal/sta.aspx> and the SaaS Addendum at <http://www.oneidentity.com/legal/saas-addendum.aspx>. This software does not require an activation or license key to operate.

## More resources

Additional information is available from the following:

- [Online product documentation](#)
- [Starling online community](#)

## 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.

# 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](http://www.YouTube.com/OneIdentity)
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product

**Copyright 2019 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](http://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.