

One Identity Starling Identity Analytics & Risk Intelligence

Release Notes

20 June 2018

These release notes provide information about the 20 June 2018 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 June 2018 is a general release, with new features and functionality.

New features

New features in the 20 June 2018 release of Starling Identity Analytics & Risk Intelligence:

- Two new rules added – New entitlement classification rules (Account Best Practices – Computers and Account Best Practices – Users) are available for evaluating Active Directory and Active Roles Server data sources.

See also:

- [Resolved issues](#) on page 4

The following were new features in previous releases of Starling Identity Analytics & Risk Intelligence.

23 May 2018 new features

- General Data Protection Regulation changes – Due to the new GDPR requirements, a GDPR contact is now required for your Starling account. For more information, see the Starling User Guide. Also, please take time to review the [One Identity legal page](#).

9 May 2018 new features

- Compare Entitlements page changes – The Compare Entitlements page now displays the differences between two accounts by default.
- Active Roles 6.9 to 7.x support – See [System requirements](#) for information.
- Dashboard page – A risk trend indicator and new filtering option has been added to the Dashboard page.

25 April 2018 new features

- Help button – A help button ([?](#)) is now available in the title bar of Starling Identity Analytics & Risk Intelligence containing links to the Support portal and documentation.

28 March 2018 new features

- Compare Entitlements page – Performance updates to the Compare Entitlements page.

14 March 2018 new features

- Nested group membership – The Rule Evaluation Details page now displays information regarding nested group membership.

14 March 2018 new features

- Nested group membership – The Rule Evaluation Details page now displays information regarding nested group membership.

28 February 2018 new features

- Licensing page changes – The Licensing page now displays the type of license associated with each data source. Additional changes have also been made to the page.

14 February 2018 new features

- Safeguard data source modules – Starling Identity Analytics & Risk Intelligence can now collect data from Safeguard.

31 January 2018 new features

- Changed risk indicators– Icons are now used to indicate new or increased risk levels for an account.

17 January 2018 new features

- Dashboard page widgets – Widgets that use graphs to display data now have a filtering option for selecting different lengths of time.
- Customizable rule descriptions – Customizable descriptions are available for non-default entitlement classification rules.

6 December 2017 new features

- Active Roles 7.2 support – See [System requirements](#) for information.
- ServiceNow integration – Starling Identity Analytics & Risk Intelligence can now be configured to connect with ServiceNow in order to create incident tickets for rejected verification requests.
- Administration Group Members rule – a new entitlement classification rule is available that allows you to evaluate accounts within specific domains or groups.

8 November 2017 new features

- Active Directory data source modules – Starling Identity Analytics & Risk Intelligence can now collect data from Active Directory.

11 October 2017 new features

- Reporting – Downloadable reports are now available.

8 September 2017 new features

- Users page – A new page is available for managing Starling users.

30 August 2017 new features

- Active Roles 7.1 support – See [System requirements](#) for information.

16 August 2017 new features

- Starling Identity Analytics & Risk Intelligence is now available for purchase and can also be tried for thirty days.

- Verification page – a new page is available for verifying high risk accounts have the appropriate permissions within your data source.
- A new Starling online community is available [here](#).

2 August 2017 new features

- Licensing page – A new page is available for monitoring and configuring the license associated with your Starling Identity Analytics & Risk Intelligence account.

Deprecated features

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

- There were no deprecated features for the 20 June 2018 release. See below for information regarding deprecated features in previous releases.

The following features were deprecated in previous releases of Starling Identity Analytics & Risk Intelligence.

6 December 2017 deprecations

- DataSource Administrators rule: This entitlement classification rule was removed. Any historical data associated with the rule will still be available on the Verification and Reports pages.

Resolved issues

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

Table 1: General resolved issues

Resolved Issue	Issue ID
When cloning the Highly Privileged Group Members rule, Active Roles filtering criteria appears even when there is no Active Roles data source configured.	30378

The following issues were resolved in previous releases of Starling Identity Analytics & Risk Intelligence.

25 April 2018 resolved issues

Table 2: General resolved issues

Resolved Issue	Issue ID
Adding and changing the name of a previously removed verifier will instead add the verifier using the original name.	27049

11 April 2018 resolved issues

Table 3: General resolved issues

Resolved Issue	Issue ID
Nested group not showing in rule evaluation details for permission with multiple entitlements.	26959

28 March 2018 resolved issues

Table 4: General resolved issues

Resolved Issue	Issue ID
The following pages are not automatically refreshing after changes are made that impact the displayed data: Risk Profile, Rule Evaluation Details, Licensing, and Target Details.	25682
Verification page errors after removing verifier.	26532

14 March 2018 resolved issues

Table 5: General resolved issues

Resolved Issue	Issue ID
Dashboard shows duplicated dates in the IARI metrics.	23487

28 February 2018 resolved issues

Table 6: General resolved issues

Resolved Issue	Issue ID
For a Safeguard data source module, if the certificate is removed the collector agent will continue collecting data despite the missing certificate.	25632

14 February 2018 resolved issues

Table 7: General resolved issues

Resolved Issue	Issue ID
Multiple Admin Group Members Rules Result in Merging All Entitlements Under All Triggered Rules.	23670
Invalid argument error on Internet Explorer when opening the Rule Details page. No other browsers are impacted.	25012
In some cases a recently invited and verified collaborator that is then assigned the verifier role will appear as pending.	22610

31 January 2018 resolved issues

Table 8: General resolved issues

Resolved Issue	Issue ID
In Windows 2016 the Active Directory permission to Create Group Objects for current object and all descendant objects is not firing off Create Groups Rule.	22200
The Active Directory permission to Read All Properties for User objects is firing off Delete Organizational Units Rule.	21922

3 January 2018 resolved issues

Table 9: General resolved issues

Resolved Issue	Issue ID
Documentation will not be updated for the 20 December 2017 release.	

6 December 2017 resolved issues

Table 10: General resolved issues

Resolved Issue	Issue ID
Documentation will not be updated for the 22 November 2017 release.	
Collector evaluation status icon doesn't always update when collecting has begun.	22176
When comparing Active Directory entitlements for two different Domain Controller Computer Accounts, the permissions column is displaying an incorrect access type for certain targets.	21701

Resolved Issue	Issue ID
Computer accounts are appearing in the High Risk Accounts search when using the Risk Level All filter.	22172
Collector agents failing to check or return errors when a compression file is problematic.	22327

8 November 2017 resolved issues

Table 11: General resolved issues

Resolved Issue	Issue ID
An entitlement classification rule that has been disabled for a long period of time may block you from enabling the rule.	21973

13 September 2017 resolved issues

Table 12: General resolved issues

Resolved Issue	Issue ID
Should the last collaborator leave the service, the account creator will be unable to resubscribe to the service using that account.	12399

19 July 2017 resolved issues

Table 13: General resolved issues

Resolved Issue	Issue ID
Opening the End Preview drop-down menu for Starling Identity Analytics & Risk Intelligence, clicking End Preview, then clicking Cancel on the confirmation dialog will cause you to lose access to all services until you refresh the page.	19411

Known issues

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

Table 14: General known issues

Known Issue	Issue ID
ARS data source modules showing as active despite the collector agent being inactive.	22066
Safeguard module reports session access when asset has it disabled.	25607
For Active Directory, the highest number of High Risk Accounts that will be reported is 1500 per group.	30081
Documentation will not be updated for the 4 July 2018 release.	

System requirements

Before using the 20 June 2018 Starling Identity Analytics & Risk Intelligence release, ensure that your system meets the following minimum hardware and software requirements.

Browser requirements

Table 15: Browser requirements

Browser	Minimum OS/Platform	Version
Internet Explorer	Windows 7	11
Google Chrome	Windows 10 Android Mac OS X Yosemite	Latest
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 16: 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 17: Starling Identity Analytics & Risk Intelligence data source module requirements

Type of data source module	Requirements
Active Roles	ARS 6.9 to 7.x i IMPORTANT: Although supported, it is strongly recommended that a collector agent not be installed on a machine with an ARS server. <ul style="list-style-type: none">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.

Type of data source module

Requirements

i **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. See this [article](#) for more information 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.
- 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.

Safeguard

Safeguard 2.1.0.0 (or greater)

- A Safeguard user with Auditor permissions is required for configuring the data source module.
- 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 *SSL Certificates* in the *One Identity Safeguard Administration Guide* ([Safeguard documentation](#)).

Product licensing

This product does not require licensing.

New service instructions

The following instructions explain how to add the Starling Identity Analytics & Risk Intelligence service to an existing One Identity Starling Identity Analytics & Risk Intelligence organization.

Adding the Starling Identity Analytics & Risk Intelligence service

1. Sign in to One Identity Starling (<https://www.cloud.oneidentity.com/>).
2. From the home page, locate the Starling Identity Analytics & Risk Intelligence service and click **Trial**.

The service will be added to the My Services section and be available for use for the length of the trial. At any point you can click the **More Information** button associated with the service for purchasing information.

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
- 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.