One Identity Starling Identity Analytics & Risk Intelligence

User Guide

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.

Starling Identity Analytics & Risk Intelligence User Guide
Updated - June 2018

Contents

Starling Identity Analytics & Risk Intelligence

Introduction to Starling Identity Analytics & Risk Intelligence

Accessible from the 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 accounts within those data sources. This allows you to determine which accounts are classified as high risk, which of their entitlement classification rules are the cause of this classification, and to resolve any discrepancies between accounts that require similar permissions.

IMPORTANT: In order to use Starling Identity Analytics & Risk Intelligence some additional software and hardware requirements must be met. See Additional hardware and software requirements for more information.

NOTE: To view the documentation or contact support while using One Identity Starling or any of the related services, click the ? button.

Supported browsers

The following browsers are supported when accessing the Starling service:

Table 1: Supported browsers

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

Browser	Minimum OS/Platform	Version
	Android 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

Navigating Starling Identity Analytics & Risk Intelligence using a mobile device

Along with the main Starling portal, Starling Identity Analytics & Risk Intelligence is compatible with mobile devices. Use the  button at the top of your screen to display the navigation bar options and account information.

Additional hardware and software requirements

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 IMPORTANT: Although supported, it is strongly recommended that a collector agent not be installed on a machine with an ARS server. • 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. 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

Type of data source module	Requirements
	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).

The Starling Identity Analytics & Risk Intelligence service

Once you have created a Starling organization, you can add the Starling Identity Analytics & Risk Intelligence service to that organization. The types of subscriptions available for Starling Identity Analytics & Risk Intelligence fall into different categories:

- Paid subscription
- Trial subscription

Paid subscription

A Starling Identity Analytics & Risk Intelligence subscription can be purchased by a Starling organization. A subscription to this service will provide you with full access to the product for the length of your contract. If you do not renew your subscription, you will lose access to Starling Identity Analytics & Risk Intelligence and data collection will stop. However, if you decide to renew your subscription at a later date, the Starling Identity Analytics & Risk

Intelligence service will be restored in the same condition it was in when it expired. This includes all data that was collected prior to the expiration. For information on purchasing a subscription to the Starling Identity Analytics & Risk Intelligence service, use the **More Information** button associated with the service.

NOTE: Contact Sales or Support to cancel a paid subscription.

Trial subscription

The services available for trial can be subscribed to for a limited period of time before they require a full subscription. This allows you to view and test the product before making a longer term commitment to using the service. If you do not decide to upgrade your subscription, you will lose access to Starling Identity Analytics & Risk Intelligence and data collection will stop once the trial has ended. However, if you decide to upgrade to a paid subscription at a later date, the Starling Identity Analytics & Risk Intelligence service will be restored in the same condition it was in when it expired. This includes all data that was collected prior to the expiration.

- Starting a service trial
- Ending a service trial

Starting a service trial

Once logged in to Starling you can trial the Starling Identity Analytics & Risk Intelligence service.

To start a service trial

1. Sign in to Starling.
2. On the home page, locate the Starling Identity Analytics & Risk Intelligence service and click **Trial**.
3. On the dialog, select your country from the drop-down list. This field only appears the first time you add a service to your organization.
4. If applicable, a second field will appear in which you must select your state or province from the drop-down list. This field only appears the first time you add a service to your organization.
5. Click **Confirm**.

   The service will be added to the My Services section and be available for use until the trial period has ended. The number of days left in your trial is indicated by a countdown at the top right of the service access button on the home page of Starling. At any point in the trial you can use the **More Information** button associated with the service to find out how to purchase the product.

Ending a service trial

The number of days left in your trial is indicated in the upper right corner of the service access button. Once your trial period has ended the service will no longer be accessible. Please use the contact information associated with the service to inquire about purchasing options.

Inviting an administrator to a service

The following procedure applies to organization administrators. It is designed to allow additional administrators to be added and to allow a new administrator to be invited to a service in cases where the last administrator assigned to that service has left the organization.

To invite an administrator to a service

1. From the home page of Starling, click the button associated with the service to which you want to invite a new administrator.
2. Select **Invite Administrator**.
3. Depending on the type of account, the following methods can be used for inviting a new administrator to the service:
    - To invite an administrator:
        a. Click **Unable to find an administrator**.
        b. Enter the name and email address of the user.
        c. Click **Invite**. An invitation to the service will be sent to the user.
    - To invite an administrator with an Azure AD work account:

        NOTE: This option is only available for organization administrators with an Azure AD work account.

        a. Click the drop-down menu field.
        b. In the blank search box, begin typing the name of the user. When you have located the user, select them from the list.
        c. Click **Invite**. An invitation to the service will be sent to the user.

Managing multiple subscriptions of Starling Identity Analytics & Risk Intelligence

Starling users have the option of adding additional collaborators to their Starling Identity Analytics & Risk Intelligence service (Adding additional collaborators). In cases where an

invited collaborator has already created a Starling organization, they can switch between subscriptions from within Starling Identity Analytics & Risk Intelligence.

To switch between Starling Identity Analytics & Risk Intelligence subscriptions

1. From the Starling Identity Analytics & Risk Intelligence home page, click the  button in the title bar to open a drop-down menu listing the names of the organizations to which you have access.
2. Select the name of the organization to which you want to switch. The Starling Identity Analytics & Risk Intelligence service will update to display the information associated with the organization listed in the title bar.

Using the Starling Identity Analytics & Risk Intelligence service

Once you have added the Starling Identity Analytics & Risk Intelligence service to your One Identity Starling organization, as either a trial or paid subscription, you have full access to the Starling Identity Analytics & Risk Intelligence service.

The service is navigated using the title bar along the top of the site which contains the following links:

-  - This button (displaying the name of the organization you are currently viewing) opens a drop-down menu which allows you to move between organizations associated with your account. See Introduction to Collaborators for related information.
-  - This button (displaying the first name of the account owner) opens a drop-down menu that allows you to select one of the following options:
  - **My Services** - Clicking this link takes you to the One Identity Starling home page.
  - **Sign out** - Clicking this link signs you out of One Identity Starling.
-  - This button opens a dialog displaying notifications related to your Starling Identity Analytics & Risk Intelligence service. See Notifications for information on this feature.
-  - This button opens the Settings page where you can manage your entire Starling account.

The main pages available within Starling Identity Analytics & Risk Intelligence are listed in the navigation bar which is located directly beneath the title bar:

- Dashboard page - This is the home page of Starling Identity Analytics & Risk Intelligence and provides insight into the current status of your service.
- Risk - This drop-down menu provides access to pages with information on the accounts associated with your data sources.
- Rules - This page is used to configure the entitlement classification rules associated with your data sources.
- Configuration - This drop-down menu provides access to pages for configuring Collector agents, data sources, and Licensing.
- Collaborators - This page is used to add additional collaborators to your Starling Identity Analytics & Risk Intelligence service.

- Verification - This page is used to review entitlement verification requests for the high risk users within your data sources.
- Reports - This page is used to download reports from the Starling Identity Analytics & Risk Intelligence service.

Dashboard page

Upon opening Starling Identity Analytics & Risk Intelligence, you will be directed to the Dashboard page. The Dashboard page is used for navigating through Starling Identity Analytics & Risk Intelligence and also provides a quick overview of the current status of your service. It includes information, links, and Widgets regarding your service. First time users, and those who have not yet configured Starling Identity Analytics & Risk Intelligence, will see information on what needs to be configured in order to begin using this service.

The following information is displayed at the top of the Dashboard page once data sources have been configured:

Risk Trend

This indicates the current risk trend by showing whether or not there has been an increase (), decrease (), or no change () to the level of risk within the set time period. This is calculated by first checking to see if there was an increase or decrease to the number of accounts. If there was no change to the number of accounts being reported as high risk then changes to high risk entitlements are considered. You can use the **Filter By** drop-down to change the amount of time to consider when calculating the risk trend.

High Risk Accounts

This displays the current number of high risk accounts associated with data sources that have an active license. The total number of evaluated accounts associated with those data sources appears beneath the high risk accounts value. Clicking this will open the High Risk Accounts page.

High Risk Entitlements

This displays the current number of high risk entitlements associated with data sources that have an active license. The total number of evaluated entitlements associated with those data sources appears beneath the high risk entitlements value.

Filter By

This drop-down is used to set the period of time for which data will be displayed (by default the last 15 days). The Risk Trend indicator and any widgets that display data

based on time period will update according to the selection. The High Risk Account and High Risk Entitlement counts are not impacted by this filter.

Widgets

On the bottom of the Starling Identity Analytics & Risk Intelligence Dashboard page, are widgets offering a brief overview of information regarding your service. These widgets vary in style based on the type of information they display. The following are the types of widget and how they are used:

NOTE: The **Filter By** drop-down at the top of the page is used to set the period of time for which data will be displayed (by default the last 15 days). The risk trend indicator and any widgets that display data based on time period will update according to the selection.

- Graphs: These widgets are graphs that can be filtered to show specific time periods and hovering over a data point will display the specifics about what occurred on the corresponding date.
- Lists: These widgets are lists that show changed data and provide links to the pages where these changes can be viewed in full. For example, new high risk accounts may have been found during an evaluation so information on which accounts and a link to the high risk accounts page will appear in the widget.
- Pie charts: These widgets are circular and display the portion each element takes up of the total. You can remove data from the chart by clicking the name of the element within the legend. Clicking the name a second time will add the data back into the chart.

Some examples of the widgets that may be displayed on this page:

NOTE: All widgets that display information based on date use UTC.

- Metric Totals
- High Risk Accounts - By Rule
- Increased High Risk Accounts
- New High Risk Accounts
- High Risk Accounts - By Data Source
- High Risk Accounts - By Module (this chart will not display if only one data source is present)

Settings

Introduction to the Settings page

The Settings page is displayed when the button is clicked in the upper right corner while on the Starling home page. From this page you can access the following settings:

IMPORTANT: The following option vary depending on the type of user account you have. For example, only organization administrators will see the User Access and Delete Organization options.

- **Notifications**: This page is used to configure the notifications that you recieve. See Notifications for more information.
- **Event Forwarding**: This page is used to configure event data to be sent to a SYSLOG service. See Starling event forwarding for more information.
- **Third Party Applications**: This page is used to connect Starling Identity Analytics & Risk Intelligence with ServiceNow. See Connecting with ServiceNow for more information.
- **User Access**: This page is used for managing users. See Users page for more information.
- **Delete Organization/Leave Organization**: The displayed setting depends on the type of account you have. See Deleting an organization or Leaving an organization for more information.

Notifications

Within the title bar, you can view notifications regarding changes to your Starling Identity Analytics & Risk Intelligence service by clicking the button. These notifications cover the last 30 days and are related to things such as account risk levels, entitlement classification rules, collector agents, data sources, and rejected verifications. You can also customize and view information regarding the notifications you can receive using the Settings page (click the button).

The dialog that opens displays your notifications according to the time in which they occurred with the latest appearing at the top of the list. Clicking on a listed notification will expand it to provide additional information and, in some cases, a link to where you can view additional information. For information on deleting a notification, see Deleting notifications.

Customizing notifications

Notifications for your Starling Identity Analytics & Risk Intelligence service can be customized to best fit your account. The custom notification settings are applied at the account level in order to allow each account to select their own notification preferences independently of any other accounts within the same organization(s). For example, when an account with Starling Identity Analytics & Risk Intelligence wants to know when new high risk accounts are added they can opt to only receive those types of notifications without impacting another account within the same organization that wants information on when new ECRs are added to Starling Identity Analytics & Risk Intelligence.

NOTE: You can customize your notifications at any time using this page and all applicable notices from the past 30 days will appear should you re-enable a notification at a later time.

To customize notifications

1. From the home page of Starling, click the button in the upper right corner.
2. In the Notifications section of the Settings page, click **Change**.
3. On the Which notifications do you want to receive page, click the On/Off toggle for each of the notification types and switch it to the **Off** position to turn off any notification type for which you no longer want to receive notices. Edits will be saved automatically.

   NOTE: Click the **Details** drop-down menu for any of the items to customize exactly which notifications to disable and to better understand which notifications will be impacted should the entire notification type be disabled.

Deleting notifications

A notification can be deleted to acknowledge it has been seen and reviewed. This happens at the account level, so other accounts within the same organization will still see their copy of the notification.

To delete notifications

1. Click the button to open the Notifications dialog.
2. Use one of the following methods:
   - To delete individual notifications: Locate the notification you want to delete and click the button. The notification will be permanently removed.
   - To delete all notifications: Click **Clear all**. All listed notifications will be permanently removed.

Starling event forwarding

The Event Forwarding section of the Settings page allows you to send Starling event data to a service that supports SYSLOG. This feature is not enabled by default.

To enable event forwarding

IMPORTANT: Only events occurring after the feature has been configured will be sent to your SYSLOG service and then able to be stored according to your preferences. Events that occur prior to configuration are not forwarded nor are they accessible within Starling.

1. From the home page of Starling, click the button in the upper right corner.
2. In the Event Forwarding section of the Settings page, click **Change**.
3. On the Configure Event Forwarding page, click the On/Off toggle to switch it to the **On** position.
4. Fill in the following configuration fields:
    - Hostname/IP Address: Enter the hostname or IP address to which the event data will be sent.
    - Port: Enter the port number in this field. By default this is 6514.
    - Structured Data ID: (Optional) Use this field to specify an ID that can be passed to the Loggly logging service (https://www.loggly.com/) to identify a specific customer tenant within Loggly.

    Once you have filled in these fields the information will be saved automatically.

Connecting with ServiceNow

The Third Party Applications option on the Settings page allows you to connect Starling Identity Analytics & Risk Intelligence to the third party application ServiceNow in order to create incident tickets for rejected verification requests which can be managed and assigned within the ServiceNow application. This feature is not enabled by default.

To connect ServiceNow with the Starling Identity Analytics & Risk Intelligence service

1. From the home page of Starling, click the button in the upper right corner.
2. In the Third Party Applications section of the Settings page, click **Change**.
3. On Third Party Applications page, click the On/Off toggle to switch it to the **On** position.
4. Fill in the following configuration fields:

- Instance URL: Enter the URL of the ServiceNow instance to which Starling Identity Analytics & Risk Intelligence will connect.
- Username: Enter the username for a ServiceNow account with the itil role.
- Password: Enter the password associated with the account.

Once you have filled in these fields the information will be saved automatically.

5. Click **Test Connection** to ensure Starling is able to connect with ServiceNow.
6. In the Integration with Starling services section at the bottom of the page, click the On/Off toggle to switch it to the **On** position for Starling Identity Analytics & Risk Intelligence. Once this feature has been enabled, all rejected verification requests within Starling Identity Analytics & Risk Intelligence will create an incident ticket within ServiceNow.

Managing GDPR contacts

The General Data Protection Regulation (GDPR) is a European Union regulation that requires information to be reported regarding sub-processor changes and data breaches. The Manage GDPR Contacts page allows organization administrators to manage the users that will be contacted regarding these GDPR items. This page is used for the following tasks:

NOTE: By default, the organization administrator is automatically added as the GDPR contact.

- Adding GDPR contacts
- Editing GDPR contacts
- Deleting GDPR contacts

Adding GDPR contacts

The Manage GDPR Contacts page allows organization administrators to add users that will be contacted regarding GDPR (General Data Protection Regulation) items.

To add a GDPR contact

NOTE: Only organization administrators can add GDPR contacts within an organization.

1. From the home page of Starling, click the  button in the upper right corner.
2. In the Manage GDPR Contacts section of the Settings page, click **Manage**.
3. Click **Add Contact**.
4. On the GDPR Contact dialog, enter a first and last name for the contact.

5. In the Email field, enter an email address for the contact. All related GDPR emails will be sent to this address.
6. Select the check box for each type of email that the contact will be sent.
7. Click **Save**.

   The new contact will now be listed on the Manage GDPR Contacts page.

Editing GDPR contacts

The Manage GDPR Contacts page allows organization administrators to manage the users that are being contacted regarding GDPR (General Data Protection Regulation) items.

To edit a GDPR contact

NOTE: Only organization administrators can edit GDPR contacts within an organization.

1. From the home page of Starling, click the button in the upper right corner.
2. In the Manage GDPR Contacts section of the Settings page, click **Manage**.
3. Locate the user to edit. You can use the button to filter the listed users.
4. Click the button associated with the user.
5. Click **Edit**.
6. On the GDPR Contact dialog, make any necessary changes to the GDPR contact. At least one contact must be configured for each type of email.
7. Click **Save**.

Deleting GDPR contacts

The Manage GDPR Contacts page allows organization administrators to delete a user that is being contacted regarding GDPR (General Data Protection Regulation) items.

To delete a GDPR contact

NOTE: At least one contact must be configured to receive each type of email.

1. From the home page of Starling, click the button in the upper right corner.
2. In the Manage GDPR Contacts section of the Settings page, click **Manage**.
3. Locate the user to delete. You can use the button to filter the listed users.
4. Click the button associated with the user.

5. Click **Delete**.
6. Click **OK** to confirm. The contact will no longer appear listed on the Manage GDPR Contacts page.

Leaving an organization

NOTE: If there are no other administrators associated with your services, the Leave Organization option will not appear.

This section allows you to disassociate your account from the Starling service while still allowing any other administrators access to the organization.

Leaving an organization

1. From the home page of Starling, click the button in the upper right corner.
2. In the Leave Organization section of the Settings page, click **Leave**.
3. On the Leave Organization dialog, click **Yes**.

IMPORTANT: If you are the only administrator associated with the organization, you will only see the Delete Organization option. See Deleting an organization for more information.

Deleting an organization

This section allows you to permanently delete your organization from Starling in addition to all of its associated services. This will impact all administrator accounts associated with your Starling services.

IMPORTANT: Deleting an organization is permanent and you may continue being billed for any paid subscriptions. Contact Sales or Support if you have any billing issues or concerns.

Deleting an organization

1. From the home page of Starling, click the button in the upper right corner.
2. In the Delete Organization section of the Settings page, click **Delete**.
3. On the Delete Organization dialog, click **Yes**.

Users page

IMPORTANT: Only organization administrators can access this page.

The Users page (see Accessing the Users page for information on accessing this page), allows you to view and manage the user accounts associated with your organization. The individual user information panes which appear on this page contain information on confirmed users such as their name, email, type of user, which services they have access to, and authentication type.

The following options and information appears on this page:

Filter Users

Opening this drop-down displays additional filtering options which can be used independently or in addition to the filtering field. These additional filtering options are to narrow down the listed users based on which service they have access to, the type of user, and by authentication method. Clicking **Reset all** removes all of the previously selected filters and closes the dialog.

Hovering over this icon displays a field that is used for filtering the displayed user information panes. This can be used independently or in addition to the **More Filters** button.

User information panes

The Users page displays individual panes for each user containing information and options specific to that user account. Within each pane you can click the email address link to send them an email, view their user type, use the service icons associated with each information pane to open each service's access management page, and view their authentication method.

Additional information about the user is displayed by clicking the  button associated with the user information pane. The following options are available after clicking the button:

Demote to Collaborator/Promote to Organization Admin

NOTE: This option does not appear when you are viewing your own account since you cannot demote your own role. It also does not appear for users that don't have a Starling account (for example, Two-Factor Authentication end users).

Depending on the type of account you are looking at, one of these two options will be available. Selecting the available option will immediately update the user account to the new type (Collaborator or Organization Admin).

View Details

Selecting this option opens a new dialog listing specifics about the information, as well as provides links to each service's access management page.

Accessing the Users page

The User Access section of the Settings page allows you to view and manage the users associated with your Starling organization.

To access the Users page

NOTE: Only organization administrators can access the Users page.

1. From the home page of Starling, click the button in the upper right corner.
2. In the User Access section of the Settings page, click **Manage**.

Editing organization roles

The Users page allows organization administrators to manage the users associated with your Starling organization and promote or demote a users access level within your organization.

To edit a user role within an organization

NOTE: Only organization administrators can edit user roles within an organization.

1. From the home page of Starling, click the button in the upper right corner.
2. In the User Access section of the Settings page, click **Manage**.
3. Locate the user whose role you want to edit. You can use the filtering options at the top of the page to filter the listed users.
4. Click the button associated with the user and, depending on their current role, you can select to either demote the user to a collaborator or promote them to an organization administrator.
    - **Demote to Collaborator**: Selecting this option will demote the user to a collaborator within the organization. This role retains access to all services they are currently assigned, but they have limited capabilities when it comes to configuring the organization. This means they will be unable to access the Users page and cannot delete the organization.
    - **Promote to Organization Admin**: Selecting this option will promote the user to an organization administrator within the organization. This role retains access to all services they are currently assigned and also allows them to configuring the organization. This means they will be able to access the Users page and can delete the organization.

    The new user role will automatically save once an option has been selected.

2

Collaborators

Introduction to Collaborators

Starling Identity Analytics & Risk Intelligence allows users to add collaborators to their service (as administrator, verifier, or both) based on the type of access required for the user. Adding additional collaborators is optional and can be done at any time using the Collaborators page.

The following roles are available for your collaborators:

- Administrator: This role allows you full access to all parts of the Starling Identity Analytics & Risk Intelligence service and allows you full configuration capabilities. There must always be at least one administrator associated with the account.
- Verifier: This role allows you limited access to the Starling Identity Analytics & Risk Intelligence service. Specifically, collaborators that are assigned only the verifier role will only have access to the Verification page in order to allow for the handling of entitlement verification requests. All other pages within Starling Identity Analytics & Risk Intelligence will be hidden from collaborators unless they are also assigned the administrator role.

Collaborators page

The Collaborators page is displayed when the **Collaborators** link is clicked in the navigation bar. The Collaborators page is used for adding and managing the collaborators currently associated with the Starling Identity Analytics & Risk Intelligence service.

The following options appear on this page:

Invite Collaborator

This opens the Invite Collaborator dialog so you can add new collaborators to your Starling Identity Analytics & Risk Intelligence service.

Show

Use this drop-down menu to display collaborators based on role. The available options are: **All Roles**, **Administrator Role**, **Verifier Role**.

Hovering over this icon displays a search box used to locate specific collaborators within the Collaborator table. To use the field, start typing the name or email of the collaborator in the field and the table will automatically update to display users that match.

The following information and button appears in the Collaborator table on this page:

Name

This displays the name specified in the collaborator invite.

Email

This displays the email address to which the collaborator invite was sent.

Roles

This displays the roles currently assigned to the collaborator.

Status

This displays the status of the user. When a user is added they will be marked as Invited until the invitation has been accepted, at which point the Status column will update to display Registered.

This button appears for each collaborator and is used for editing the roles for the collaborator and removing collaborators from the account.

NOTE: You are unable to remove yourself as a collaborator, and if you are an administrator for the account then only another administrator can remove your administrator role. Coordinate with other administrators before making edits to their roles to avoid removing each other as administrators.

NOTE: Until an invite has been accepted, the following options are available when clicking the  button:

- **Re-send Invitation**: Selecting this option will resend the invitation.
- **Cancel Invitation**: Selecting this option will cancel the invitation. The invited user will not be notified that the invitation was canceled, however when logged in they will be unable to access the service.

Managing collaborators

The following sections provide information on managing collaborators for the Starling Identity Analytics & Risk Intelligence service.

- Adding additional collaborators
- Adding additional Azure AD work account collaborators
- Editing roles
- Removing collaborators

Adding additional collaborators

Collaborators are optional and can be added at any time. For information on adding a collaborator from within your Azure AD account, see Adding additional Azure AD work account collaborators.

To add additional collaborators

1. On the Collaborator page, click **Invite Collaborator**.
2. On the Invite Collaborator dialog, enter the name and email address of the user you would like to add as a collaborator to your organization.
3. In the Collaborator Roles section, select the check box associated with the role(s) that will be assigned to the new collaborator (at least one role must be assigned):
    - **Administrator**: This role allows you full access to all parts of the Starling Identity Analytics & Risk Intelligence service and allows you full configuration capabilities. There must always be at least one administrator associated with the account.
    - **Verifier**: This role allows you limited access to the Starling Identity Analytics & Risk Intelligence service. Specifically, collaborators that are assigned only the verifier role will only have access to the Verification page in order to allow for the handling of entitlement verification requests. All other pages within Starling Identity Analytics & Risk Intelligence will be hidden from collaborators unless they are also assigned the administrator role.
4. Click **Invite**.
5. An email will be sent with a link to either registering a new account that has access to your organization or, if the recipient has already registered with Starling using this email address, a notification they now have access to your organization's Starling Identity Analytics & Risk Intelligence service. They will be marked as Invited until the invitation has been accepted, at which point the Status column will update to display Registered.

NOTE: Administrators and collaborators associated with multiple organizations can switch between Starling subscriptions once they have logged in (Managing multiple subscriptions of Starling Identity Analytics & Risk Intelligence).

NOTE: Until an invite has been accepted, the following options are available when clicking the ⋮ button:

- **Re-send Invitation**: Selecting this option will resend the invitation.
- **Cancel Invitation**: Selecting this option will cancel the invitation. The invited user will not be notified that the invitation was canceled, however when logged in they will be unable to access the service.

Adding additional Azure AD work account collaborators

Collaborators are optional and can be added at any time. For information on adding a collaborator from outside your Azure AD account, see Adding additional collaborators.

To add additional Azure AD work account collaborators

1. On the Collaborator page, click **Invite Collaborator**.
2. Click in the **Search for collaborator** field and begin typing in the empty field to filter the available collaborators.
3. Click the name of the collaborator you want to add to populate the field.

   NOTE: If the collaborator cannot be found or is not associated with your Azure AD tenant, click **Unable to find collaborator** and enter the name and email address of the user you would like to add as a collaborator to your organization.

4. In the Collaborator Roles section, select the check box associated with the role(s) that will be assigned to the new collaborator (at least one role must be assigned):
   - **Administrator**: This role allows you full access to all parts of the Starling Identity Analytics & Risk Intelligence service and allows you full configuration capabilities. There must always be at least one administrator associated with the account.
   - **Verifier**: This role allows you limited access to the Starling Identity Analytics & Risk Intelligence service. Specifically, collaborators that are assigned only the verifier role will only have access to the Verification page in order to allow for the handling of entitlement verification requests. All other pages within Starling Identity Analytics & Risk Intelligence will be hidden from collaborators unless they are also assigned the administrator role.
5. Click **Invite**.
6. An email will be sent with a link to either registering a new account that has access to

your organization or, if the recipient has already registered with Starling using this email address, a notification they now have access to your organization's Starling Identity Analytics & Risk Intelligence service.

NOTE: Administrators and collaborators associated with multiple organizations can switch between Starling subscriptions once they have logged in (Managing multiple subscriptions of Starling Identity Analytics & Risk Intelligence).

Editing roles

The following procedure explains how to edit a collaborators assigned role(s).

To edit roles for a collaborator

NOTE: It can take up to 15 minutes for changes to take effect for currently logged in users.

1. On the Collaborators page, locate the collaborator whose roles you want to edit. You can use the **Search for collaborators** field at the top of the page to filter the listed collaborators.
2. Once you have located the collaborator to edit, click the button.
3. Select the **Edit Roles** option.
4. On the Collaborator Roles dialog, select the check box associated with the role(s) that will be assigned to the collaborator (at least one role must be assigned):
   - **Administrator**: This role allows you full access to all parts of the Starling Identity Analytics & Risk Intelligence service and allows you full configuration capabilities. There must always be at least one administrator associated with the account.
   - **Verifier**: This role allows you limited access to the Starling Identity Analytics & Risk Intelligence service. Specifically, collaborators that are assigned only the verifier role will only have access to the Verification page in order to allow for the handling of entitlement verification requests. All other pages within Starling Identity Analytics & Risk Intelligence will be hidden from collaborators unless they are also assigned the administrator role.

   NOTE: If you are an administrator for the account then only another administrator can remove your administrator role. Coordinate with other administrators before making edits to their roles to avoid removing each other as administrators.
5. Click **Save** to save your changes and return to the Collaborators page.

Removing collaborators

If a collaborator is no longer needed, you can remove their access to the Starling Identity Analytics & Risk Intelligence service.

To remove collaborators

1. On the Collaborators page, locate the user you want to remove as a collaborator. You can use the **Search for collaborators** field at the top of the page to filter the listed collaborators.
2. Click the  button associated with the user you want to remove.
3. Select the **Remove Collaborator** option.

   NOTE: You are unable to remove yourself as a collaborator, and if you are an administrator for the account then only another administrator can remove your administrator role. Coordinate with other administrators before making edits to their roles to avoid removing each other as administrators.
4. On the confirmation dialog, click **OK** to remove their access to your subscription of Starling Identity Analytics & Risk Intelligence.

3

Collector agents

Introduction to Collector Agents

Accessed from the Configuration drop-down menu, the Collector Agents page is used for configuring the collector agents that Starling Identity Analytics & Risk Intelligence will use to collect entitlement data which can then be evaluated to better understand the data source. The Collector Agents page is also available to view status information and messages once you have installed the Starling Identity Analytics & Risk Intelligence collector agent to collect entitlement data from a data source.

Adding collector agents to Starling Identity Analytics & Risk Intelligence

The following explains how to add a collector agent to Starling Identity Analytics & Risk Intelligence in order to begin collecting entitlement data.

NOTE: You cannot install multiple collector agents on the same machine.

NOTE: The data collected by the data source module(s) associated with the collector agent will remain within Starling Identity Analytics & Risk Intelligence until it has been purged. See Purging data for more information.

IMPORTANT: Read the Additional hardware and software requirements before installing a collector agent.

To add a collector agent

1. From the Collector Agent page, click **Add a collector agent** to open the Add Collector Agent dialog.
2. Copy and save the registration code. This code is requested during the collector agent installation and will only be valid for 15 minutes.

3. Use **Download Collector Agent Installer** to download the collector agent installer. Clicking **About Collector Agent** on the dialog provides additional copyright and third party component information.
4. Once downloaded, run the **IAI.Collector.Installer.msi** installer package and follow the instructions on the Starling IARI Collector Setup dialog to complete the installation. The installer will automatically close once installation is complete.
5. Once installation has been successfully completed, close the Add Collector Agent dialog to return to the Collector Agents page.

   The page will automatically refresh once the collector agent has been installed. The new collector agent appears listed on the Collector Agents page with a green check mark to indicate the collector agent has been installed correctly and is able to communicate with Starling Identity Analytics & Risk Intelligence. You are now able to add modules to the collector agent (see Adding data source modules to Starling Identity Analytics & Risk Intelligence).

Collector Agent page

The Collector Agent page is displayed when the **Collector Agents** link is selected from the Configuration drop-down menu located in the navigation bar. The Collector Agent page is used for adding and managing the collector agents and data source modules that are configured for your account.

The following information appears once at least one collector agent has been installed.

Search for collector agents

Use this field to filter the list of collector agents appearing at the bottom of this page.

Add Collector Agent

This button is used for adding a new collector agent. See Adding collector agents to Starling Identity Analytics & Risk Intelligence for more information.

The following information appears in the table at the bottom of the page once at least one collector agent has been configured.

Host

This is the host name for the collector agent.

Number of Modules

This is the number of data source modules currently configured for the collector agent.

Last Communication

This displays the time of the last communication between the collector agent and the Starling Identity Analytics & Risk Intelligence cloud service. This communication is done through an HTTPS call on port 443 and cannot be configured. This check is in order to ensure communication between the two components is active and secure.

Status

This indicates the current status of the connection. Mousing over the displayed icon provides a brief explanation of the current status.

More Details

Clicking this button displays information regarding the currently installed versions of both the collector agent and the installer.

Actions

This drop-down menu displays the following configuration options:

- **Edit**: This option provides access to the Data Source Modules page where you can add and manage data source modules for use by the collector agent.
- **Uninstall**: This option uninstalls the collector agent as well as any configured data source modules. See Uninstalling a collector agent for more information.
- **About Collector Agent**: This option provides additional copyright and third party component information regarding the installed collector agent.

Adding data source modules to Starling Identity Analytics & Risk Intelligence

Once you have finished Adding collector agents to Starling Identity Analytics & Risk Intelligence you need to configure modules for that source.

NOTE: Only one module of each type can be added to each collector agent.

NOTE: The amount of time needed to collect data will increase if the network is slow between the machine where the collector agent is installed and the machine it is collecting data from.

IMPORTANT: Read the Additional hardware and software requirements before adding a data source module.

To add an Active Directory data source module

1. From the Collector Agents page, expand the **Action** drop-down menu associated with the collector agent to which you want to add an Active Directory data source module.
2. Select **Edit**. This will open the Data Source Modules page.
3. Click the **Add Module** button to open the Configure New Module dialog.
4. Expand the **Module Type** drop-down menu and select **Active Directory**.
5. (Optional) Enter a Host Name or IP Address. If you have more than one Active Directory data source available in the environment then you need to specify which one to connect with, otherwise Starling Identity Analytics & Risk Intelligence will randomly select one.

   IMPORTANT: 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.

6. In the **Data Collection Frequency (hours)** field, enter how often Starling Identity Analytics & Risk Intelligence should initiate a collection. By default, collections will occur every 24 hours. This process will be indicated by an alert bar in Starling Identity Analytics & Risk Intelligence followed by the impacted pages automatically updating once the evaluation has completed.

   NOTE: The Data Collection Frequency (hours) value must be between 1-576.

7. In the **Username** field, enter the name of a user with appropriate permissions to the data source.
8. In the **Password** field, enter the password associated with the user.
9. Click **Save** to save the module and close the dialog.

   Once you have completed adding the data source, the following information may appear indicating the state of the connection:

   - Upon initial completion, a icon appears to indicate the module is validating.
   - The next step in this process is the actual collection of the data which is indicated by a  icon. During this step, the data source will begin the process of connecting with and sending data to Starling Identity Analytics & Risk Intelligence. This process may take a while depending upon a number of factors (for example, the amount of data that needs to be collected).

     The data being collected includes information regarding disabled accounts since, although inactive, they still exist, and therefore can provide important information about both the account and the data source overall. However, this account information will not include data related to actions an account cannot perform. For example, expired entitlements within Safeguard are not considered when calculating the risk level of an account since an expired entitlement is the same as the entitlement not existing.

- Once the module has successfully connected and a  appears, the module data will be available within Starling Identity Analytics & Risk Intelligence.
- Should the data collection or module validation fail, a  appears indicating a problem has occurred (for example, incorrect configuration settings, the data source being inaccessible at this time, and so on).

To add an Active Roles data source module

1. From the Collector Agents page, expand the **Action** drop-down menu associated with the collector agent to which you want to add an Active Roles data source module.
2. Select **Edit**. This will open the Data Source Modules page.
3. Click the **Add Module** button to open the Configure New Module dialog.
4. Expand the **Module Type** drop-down menu and select **ActiveRoles**.
5. (Optional) Enter a Host Name or IP Address. If you have more than one Active Roles data source available in the environment then you need to specify which one to connect with, otherwise Starling Identity Analytics & Risk Intelligence will randomly select one.

   IMPORTANT: The collector agent must also be able to resolve the DNS names of all computers hosting Active Roles Administration Services in the Active Roles installation.
6. In the **Data Collection Frequency (hours)** field, enter how often Starling Identity Analytics & Risk Intelligence should initiate a collection. By default, collections will occur every 24 hours. This process will be indicated by an alert bar in Starling Identity Analytics & Risk Intelligence followed by the impacted pages automatically updating once the evaluation has completed.

   NOTE: The Data Collection Frequency (hours) value must be between 1-576.
7. In the **Username** field, enter the name of a user with appropriate permissions to the data source.
8. In the **Password** field, enter the password associated with the user.
9. Click **Save** to save the module and close the dialog.

   Once you have completed adding the data source, the following information may appear indicating the state of the connection:

   - Upon initial completion, a icon appears to indicate the module is validating.
   - The next step in this process is the actual collection of the data which is indicated by a  icon. During this step, the data source will begin the process of connecting with and sending data to Starling Identity Analytics & Risk Intelligence. This process may take a while depending upon a number of factors (for example, the amount of data that needs to be collected).

     The data being collected includes information regarding disabled accounts since, although inactive, they still exist, and therefore can provide important

information about both the account and the data source overall. However, this account information will not include data related to actions an account cannot perform. For example, expired entitlements within Safeguard are not considered when calculating the risk level of an account since an expired entitlement is the same as the entitlement not existing.

- Once the module has successfully connected and a  appears, the module data will be available within Starling Identity Analytics & Risk Intelligence.
- Should the data collection or module validation fail, a  appears indicating a problem has occurred (for example, incorrect configuration settings, the data source being inaccessible at this time, and so on).

To add a Safeguard data source module

1. From the Collector Agents page, expand the **Action** drop-down menu associated with the collector agent to which you want to add a Safeguard data source module.
2. Select **Edit**. This will open the Data Source Modules page.
3. Click the **Add Module** button to open the Configure New Module dialog.
4. Expand the **Module Type** drop-down menu and select **Safeguard**.
5. (Optional) Enter a Host Name or IP Address. If you have more than one Safeguard data source available in the environment then you need to specify which one to connect with, otherwise Starling Identity Analytics & Risk Intelligence will randomly select one.
6. **Safeguard Appliance DNS Name or IP Address**: It is strongly recommended that you enter the DNS Name of the Safeguard appliance to which you are connecting. In order to use an IP address for connecting with Starling Identity Analytics & Risk Intelligence the SSL certificate must have that IP address listed as a Subject Alternative Name.
7. In the **Data Collection Frequency (hours)** field, enter how often Starling Identity Analytics & Risk Intelligence should initiate a collection. By default, collections will occur every 24 hours. This process will be indicated by an alert bar in Starling Identity Analytics & Risk Intelligence followed by the impacted pages automatically updating once the evaluation has completed.

   NOTE: The Data Collection Frequency (hours) value must be between 1-576.
8. **Authentication Type**: From the drop-down menu, select whether to use the Local or Certificate authentication provider.
9. Based on your Authentication Type, enter the following information:
   - **Local**: Enter the name of a user with appropriate permissions to the data source and the associated password.
   - **Certificate**: Enter the client Certificate Thumbprint (SHA-1) that will be used for authentication. This certificate must exist in the Personal (Local Computer) certificate store of the collector agent machine.
10. Click **Save** to save the module and close the dialog.

Once you have completed adding the data source, the following information may appear indicating the state of the connection:

- Upon initial completion, a icon appears to indicate the module is validating.
- The next step in this process is the actual collection of the data which is indicated by a  icon. During this step, the data source will begin the process of connecting with and sending data to Starling Identity Analytics & Risk Intelligence. This process may take a while depending upon a number of factors (for example, the amount of data that needs to be collected).

  The data being collected includes information regarding disabled accounts since, although inactive, they still exist, and therefore can provide important information about both the account and the data source overall. However, this account information will not include data related to actions an account cannot perform. For example, expired entitlements within Safeguard are not considered when calculating the risk level of an account since an expired entitlement is the same as the entitlement not existing.
- Once the module has successfully connected and a  appears, the module data will be available within Starling Identity Analytics & Risk Intelligence.
- Should the data collection or module validation fail, a  appears indicating a problem has occurred (for example, incorrect configuration settings, the data source being inaccessible at this time, and so on).

Data Source Modules page

The Data Source Modules page is displayed by editing a configured collector agent (see Adding data source modules to Starling Identity Analytics & Risk Intelligence). The Data Source Modules page is used for adding and managing the data source modules for a collector agent.

Once a collector agent has been installed, the following information appears on this page:

Search for modules

Use this field to filter the list of data source modules appearing at the bottom of this page.

Add Module

This button is used for adding a new data source module. See Adding data source modules to Starling Identity Analytics & Risk Intelligence for more information.

The following information appears in the table at the bottom of the page once at least one data source module has been configured for the collector agent.

Module

This is the type of data source module.

Host

This is the host name for the collector agent.

Last Updated

This is the last update from the data source module to Starling Identity Analytics & Risk Intelligence. These updates can occur manually and are also configurable for each data source module (see Editing a data source module for information on configuring those settings).

Status

This indicates the current status of the connection. Mousing over the displayed icon provides a brief explanation of the current status.

More Details

Clicking this button displays information regarding the currently installed versions of both the collector agent and the installer.

Actions

This drop-down menu displays the following configuration options:

- **Edit**: This option provides access to the Edit Module Configuration dialog where you can edit the current data source module configuration.
- **Initiate Collection**: This option is for manually initiating data collection outside of the scheduled collection times. See Initiating data source module collection for more information.
- **Uninstall**: This option uninstalls the data source module. See Uninstalling a data source module for more information.

Managing data sources

Once a data source has been added to Starling Identity Analytics & Risk Intelligence and appears on the Data Source Modules page, the following actions can be taken:

- Editing a data source module
- Initiating data source module collection
- Uninstalling a data source module

Editing a data source module

After Adding collector agents to Starling Identity Analytics & Risk Intelligence and Adding data source modules to Starling Identity Analytics & Risk Intelligence, you can edit the data source module at any point.

To edit a data source module

NOTE: Editing the data source while it is working (for example, collecting data) will stop any processes. Once changes have been saved, the processes will start over again using the new settings.

1. From the Collector Agents page, expand the **Action** drop-down menu associated with the collector agent to which you want to add a data source module.
2. Select **Edit**. This will open the Data Source Modules page.
3. This will open the related Data Source Modules page.
4. From the Actions drop-down menu associated with the data source module to be edited, select **Edit** to open the Edit Module Configuration dialog.
5. On the Edit Module Configuration dialog, make any necessary changes to the current module configuration settings.
6. Click **Save** to save the changes and close the dialog.

Initiating data source module collection

After Adding collector agents to Starling Identity Analytics & Risk Intelligence and Adding data source modules to Starling Identity Analytics & Risk Intelligence, you can initiate data collection outside of the scheduled collection times.

To initiate data source module collection

1. From the Collector Agents page, expand the **Action** drop-down menu associated with the collector agent containing the module for which you want to initiate a collection.
2. Select **Edit**. This will open the related Data Source Modules page.
3. From the Actions drop-down menu associated with the data source module, select **Initiate Collection** to immediately begin data collection.

   NOTE: The amount of time needed to collect data will increase if the network is slow between the machine where the collector agent is deployed and the server where your data source module is installed.

Uninstalling a data source module

When a data source module is no longer needed it can be removed while still leaving the collector agent installed and connected with Starling Identity Analytics & Risk Intelligence. To remove both the data source module and its associated collector agent, see Uninstalling a collector agent.

To uninstall a data source module

1. From the Collector Agents page, expand the **Action** drop-down menu associated with the collector agent containing the module to be uninstalled.
2. Select **Edit**. This will open the related Data Source Modules page.
3. Expand the **Action** drop-down menu associated with the data source module to be uninstalled.
4. Select **Uninstall**.
5. On the Delete Module dialog, click **OK**.

NOTE: The data collected by the data source module will remain within Starling Identity Analytics & Risk Intelligence until it has been purged. See Purging data for more information.

Uninstalling a collector agent

This procedure will uninstall a collector agent as well as any associated data source modules.

NOTE: The data collected by the data source module(s) associated with the collector agent will remain within Starling Identity Analytics & Risk Intelligence until it has been purged. See Purging data for more information.

To uninstall a collector agent

1. From the Collector Agents page, expand the **Action** drop-down menu associated with the collector agent to be uninstall.
2. Select **Uninstall**.

   IMPORTANT: Any data source module configured for the collector agent will be deleted. To only delete a data source module without uninstalling the collector agent, see Uninstalling a data source module.
3. On the Uninstall Collector Agent dialog, click **OK**.

Introduction to Licensing

Accessed through the Configuration drop-down menu, the Licensing page allows you to view and manage the license associated with your Starling Identity Analytics & Risk Intelligence account.

Licensing page

The Licensing page is displayed when the **Licensing** link is selected from the Configuration drop-down menu located in the navigation bar. The Licensing page is used for managing the data source instances that are configured for use by your account, as well as provides information on your license.

The following information appears on this page:

License information pane

Located in the upper left corner of the page is a pane displaying the type and name of your license, the number of accounts covered by your license, and information on how those accounts are currently configured for the license. The following information is displayed regarding the accounts:

- **Used Licenses**: This displays the number of accounts that are currently licensed and being analyzed.
- **Unused Licenses**: This displays the number of licenses that are not currently being used (due to an inactive licensed instance, when there are more licenses than accounts, or both).
- **License Overage**: This displays the number of accounts that are not covered by your license.
- **Subscription Licenses**: This displays the number of licenses associated with your subscribed data sources. These accounts do not count towards your license's account allotment.

Instances

This displays the total number of instances. The number of data sources appears beneath the number of instances.

Data Collectors

This displays the number of data collectors currently configured for your account. The total number of accounts found within those data collectors appears beneath the number of data collectors.

For information on the table appearing at the bottom of the Licensing page, see Licensing table.

Licensing table

The Licensing table is displayed at the bottom of the Licensing page. It displays information on the instances associated with your account.

The following information and options appear listed in the table:

Instance

This displays the name of the instance.

Collected Accounts

This displays the number of accounts that were collected from the instance.

Status

This displays the status of the instance.

- **Inactive**: This status indicates the instance is currently inactive.
- **Subscription**: This status indicates the instance is currently licensed and that the license is provided as part of a subscription. Any associated accounts will not count towards your license's account allotment.
- **Licensed**: This status indicates the instance is currently licensed. Any associated accounts will count towards your license's account allotment.

Last Instance Update

This displays information on when the instance was last updated.

Data Source

This displays the type of data source.

Collectors

This displays the number of data collectors for the instance.

Clicking a listed instance will provide the following options:

Active/Inactive

Clicking this link (which changes based on whether or not the license for the instance is active) will activate or deactivate licensing for the instance. An active license means the instance will be analyzed during data collection. An inactive license means the instance will not be analyzed during data collection until the license is reactivated. If this is a licensed instance, an inactive status means associated accounts will not count towards your license's account allotment until the license is reactivated. See Activating or deactivating licenses for more information.

Purge Data

Clicking this link will delete the instance. This is only available if the data source module associated with it has been uninstalled or redirected to use a different data source, and there must be no custom rules currently associated with the data source module. See Purging data for more information.

Collected Accounts

This displays the number of accounts collected from the instance.

Collector agent

This displays the name of the collector agent as a link. Clicking the link opens the Data Source Modules page for the collector agent.

Last updated

This displays the date and time the instance was last updated.

Activating or deactivating licenses

The following explains how to activate or deactivate a license for an instance. An active license means the instance will be analyzed during data collection and the accounts associated with the instance will count towards your license's account allotment. An inactive license means the instance will not be analyzed during data collection until the license is reactivated and the accounts associated with the instance will not count towards your license's account allotment.

To activate or deactivate a license

1. Sign in to Starling.
2. Open the Starling Identity Analytics & Risk Intelligence service.
3. Expand the **Configuration** drop-down menu in the navigation bar.
4. Select **Licensing** from the Configuration drop-down menu.

5. In the Licensing table, click the name of the instance for which you want to activate or deactivate a license.
6. Depending on whether or not the license is active, one of the following links will appear:
    - **Active**: This link means the license is currently active. Clicking the link will deactivate the license.
    - **Inactive**: This link means the license is currently inactive. Clicking the link will activate the license.

Purging data

IMPORTANT: Purging data is permanent and also removes the instance. Some metrics from when the instance was connected will remain, however all identity data is deleted.

To purge data

1. Sign in to Starling.
2. Open the Starling Identity Analytics & Risk Intelligence service.
3. Expand the **Configuration** drop-down menu in the navigation bar.
4. Select **Licensing** from the Configuration drop-down menu.
5. In the Licensing table, click the name of the instance for which you want to purge data to expand the selection.
6. Click **Purge Data**.

    In order to purge the data, the data source module associated with it must be uninstalled or redirected to use a different data source, and there must be no custom rules currently associated with the instance. If a warning appears informing you there are rules currently associated with the instance, go to the Rules page and select a different instance for the rule or delete the rule if there are no other instances available.
7. To permanently delete the data source instance and all of its associated data, click **OK** on the confirmation dialog.

4

Rules

Introduction to Rules

Accessed through the **Rules** link in the navigation bar, the Rules page is used for selecting and managing the entitlement classification rules that are available for the configured data sources. Starling Identity Analytics & Risk Intelligence evaluates these entitlement classification rules in order to identify the high risk accounts associated with your data source(s).

Default rules

A number of default entitlement classification rules are included. These default rules perform their evaluations against configured data sources, however by overriding a default rule you can select individual data sources. Adding a new rule will override any existing default rule of that type until the custom rule is deleted. Once the custom rule is deleted, the default rule (including any previous edits) will reappear on the Rules page. See Available rules for information on the default rules.

Rules page

The Rules page is displayed when the **Rules** link is clicked in the navigation bar. The Rules page is used for managing the entitlement classification rules that Starling Identity Analytics & Risk Intelligence will use to help you identify high risk accounts.

The following options appear on this page:

New Rule

This opens the New Rule page used to add a rule from the data source. See Adding a new rule for more information.

Hovering over this icon displays a search box used to locate specific rules within the Rules table. To use the field, start typing the name of the rule in the field and the table will automatically update to display rules that match.

For information on the table appearing at the bottom of the Rules page, see Rules table. See Available rules for information on the default rules.

Rules table

The Rules table is displayed at the bottom of the Rules page. It displays information on the entitlement classification rules currently configured for Starling Identity Analytics & Risk Intelligence.

The following information and options appear listed in the table:

Name

This is the name of the entitlement rule. If the rule is only applicable to a specific type of data source module, the type of data source module will be indicated before the rule's name (for example, ActiveRoles: Configuration Modify and Safeguard: Admin or Partition Owner).

Description

This is a description of the rule.

Matched Accounts

This displays the number of matched accounts.

Status

This is the current status of the entitlement rule.

Clicking one of the rules (or the › button associated with it) will open the Rule Details page where you can modify the current settings and view additional information about the rule. See Available rules for information on the default rules.

IMPORTANT: You are unable to delete a default rule, but default rules can be disabled using the Rule Details page (for more information, see Disabling a rule).

IMPORTANT: Adding a new rule will override any existing default rule of that type. The default rule will then be hidden until the overriding custom rule is deleted. Once the custom rule is deleted, the default rule (including any previous edits) will reappear on the Rules table.

Available rules

The following table lists all of the rules that are available on the Rules page and the related permissions that impact an evaluation:

Table 4: List of available rules

Rule name	Data source(s)	Permissions
Account Best Practices - Computers	AD	**Detected Practices**: • Password Doesn't Expire • Password Not Required • Password Can't Be Changed • Password Uses Weak Encryption • Password Uses Reversible Encryption • Kerberos Preauthentication Not Required • Kerberos Delegation Not Authorized • Trusted For Kerberos Delegation
	ARS	**Detected Practices**: • Password Doesn't Expire • Password Not Required • Password Can't Be Changed • Password Uses Weak Encryption • Password Uses Reversible Encryption • Kerberos Preauthentication Not Required • Kerberos Delegation Not Authorized • Trusted For Kerberos Delegation
Account Best Practices - Users	AD	**Detected Practices**: • Password Doesn't Expire • Password Not Required • Password Can't Be Changed • Password Uses Weak Encryption • Password Uses Reversible Encryption • Kerberos Preauthentication Not Required • Kerberos Delegation Not Authorized • Trusted For Kerberos Delegation

Rule name	Data source(s)	Permissions
		• Account Is Trust Account
	ARS	**Detected Practices**: • Password Doesn't Expire • Password Not Required • Password Can't Be Changed • Password Uses Weak Encryption • Password Uses Reversible Encryption • Kerberos Preauthentication Not Required • Kerberos Delegation Not Authorized • Trusted For Kerberos Delegation • Account Is Trust Account
ActiveRoles: Configuration Full Control	ARS	**Detected permissions**: • Create Child AND Delete Child AND List Children AND Self AND Read Property AND Write Property AND List Object AND Extended Rights AND Delete AND Read Control AND Write DACL AND Write Owner AND Delete Tree AND Copy Object
ActiveRoles: Configuration Modify	ARS	**Detected permissions**: • Create Child • Delete Child • Write Property • Extended Rights • Delete • Write DACL • Write Owner • Delete Tree • Copy Object **Ignored permissions**: • Write Property: EDSVA-Client-Version on EDS-Client-Session AND Write Property: EDSA-LDAP-Server on Domain AND Extended Right: Access Personal Settings on EDS-WI-Interface
Change Group	ARS	**Detected permissions**:

Rule name	Data source(s)	Permissions
Type and Scope		• Write Property: Group Type of Groups
	AD	**Detected permissions**: • Write Property: Group Type of Groups
Create Groups	ARS	**Detected permissions**: • Create Child: Groups
	AD	**Detected permissions**: • Create Child: Groups
Create Organizational Units	ARS	**Detected permissions**: • Create Child: Organizational Unit
	AD	**Detected permissions**: • Create Child: Organizational Unit
Create Users	ARS	**Detected permissions**: • Create Child: Users
	AD	**Detected permissions**: • Create Child: Users
Delete Groups	ARS	**Detected permissions**: • Delete Child: Groups • Delete: Groups • List Objects In: Domain AND Delete Tree Containing: Groups • List Objects In: Managed Unit AND Delete Tree Containing: Groups • List Objects In: Built In Domain AND Delete Tree Containing: Groups • List Objects In: Container AND Delete Tree Containing: Groups • List Objects In: Organizational Unit AND Delete Tree Containing: Groups
	AD	**Detected permissions**: • Delete Child: Groups • Delete: Groups

Rule name	Data source(s)	Permissions
Delete Organizational Units	ARS	**Detected permissions**: • Delete Child: Organizational Unit • Delete: Organizational Unit • List Objects In: Domain AND Delete Tree Containing: Organizational Units • List Objects In: Managed Unit AND Delete Tree Containing: Organizational Units • List Objects In: Organizational Unit AND Delete Tree Containing: Organizational Units
	AD	**Detected permissions**: • Delete Child: Organizational Unit • Delete: Organizational Unit
Delete Users	ARS	**Detected permissions**: • Delete Child: Users • Delete: Users • List Objects In: Domain AND Delete Tree Containing: Users • List Objects In: Managed Unit AND Delete Tree Containing: Users • List Objects In: Container AND Delete Tree Containing: Users • List Objects In: Organizational Unit AND Delete Tree Containing: Users
	AD	**Detected permissions**: • Delete Child: Users • Delete: Users
Enable/Disable Users	ARS	**Detected permissions**: • Write Property: User Account Control of Users • Write Property: EDSA-Account-Is-Disabled of Users
	AD	**Detected permissions**: • Write Property: User Account Control of Users
Highly Privileged	ARS, AD, Safeguard	See Highly Privileged Group Members rule for more information.

Rule name	Data source(s)	Permissions
Group Members		
Modify Group Members	ARS	**Detected permissions**: • Write Property: Member of Groups
	AD	**Detected permissions**: • Write Property: Member of Groups
Reset User Passwords	ARS	**Detected permissions**: • Read Property: Object Class of Users AND Extended Right: Reset Password on Users • Write Property: EDSA-Password of Users
	AD	**Detected permissions**: • Read Property: Object Class of Users AND Extended Right: Reset Password on Users
Safeguard: Access Request by Local User	Safeguard	**Detected permissions**: • Local User AND Password Access Request • Local User AND Session Access Request Account Scope • Local User AND Session Access Request Asset Scope • Local User AND Session Access Request Linked Account
Safeguard: Access Request via Emergency Access	Safeguard	**Detected permissions**: • Emergency Access AND Password Access Request • Emergency Access AND Session Access Request Account Scope • Emergency Access AND Session Access Request Asset Scope • Emergency Access AND Session Access Request Linked Account
Safeguard: Access Request without 2FA	Safeguard	**Detected permissions**: • User does not require 2FA or certificate/smart card authentication AND Password Access Request • User does not require 2FA or certificate/smart card authentication AND Session Access Request Account Scope

Rule name	Data source(s)	Permissions
		• User does not require 2FA or certificate/smart card authentication AND Session Access Request Asset Scope • User does not require 2FA or certificate/smart card authentication AND Session Access Request Linked Account
Safeguard: Admin or Partition Owner	Safeguard	**Detected permissions**: • Any user that has been granted one or more of the following permissions in Safeguard: Authorizer, User, Help Desk, Appliance, Operations, Asset, Directory, Security Policy. • Any user that is a Delegated Owner of a Partition.
Safeguard: Session and Password Access Request to Same Account	Safeguard	**Detected permissions**: • Password Access Request AND Session Access Request Account Scope • Password Access Request AND Session Access Request Asset Scope • Password Access Request AND Session Access Request Linked Account
Unlock Users	ARS	**Detected permissions**: • Write Property: Lockout Time of Users • Write Property: EDSA-Account-Locked-Out of Users
	AD	**Detected permissions**: • Write Property: Lockout Time of Users

Adding a new rule

From the Rules page, you can add new rules for the configured data sources.

NOTE: Adding a new rule will override any existing default rule of that type. The default rule will then be hidden until the overriding custom rule is deleted. Once the custom rule is deleted, the default rule (including any previous edits) will reappear on the Rules table.

Adding a new rule

1. From the Rules page, click **New Rule** to open the New Rule page.
2. Use the configuration options to identify and add a new rule. The new rule must have a unique name, a description, and at least one data source must be selected.

   NOTE: To edit the name or description of a rule, click the button to the right of the field. Once you finish editing the rule name or description, you must click the button to save your edits. This will only save the changes made in that field. To remove any edits made in those fields, use the button.

   NOTE: There are additional configuration options for the Highly Privileged Group Members rule. See Highly Privileged Group Members rule for more information.

   NOTE: Once you have finished configuring the rule, clicking **Preview** shows what happens if the new rule is applied.
3. Click **Save** to add the rule. The rule will now be available for use.

Rule Details page

Once an entitlement classification rule has been added to Starling Identity Analytics & Risk Intelligence and appears in the table on the Rules page. Clicking one of the rules (or the button associated with it) will open the Rule Details page from which the following actions can be taken:

- Cloning a rule
- Editing a rule
- Deleting a rule

NOTE: There are specific configuration options for the Highly Privileged Group Members rule. See Highly Privileged Group Members rule for more information.

When rules are added, removed, or modified, an evaluation will automatically occur in order to update Starling Identity Analytics & Risk Intelligence with the latest information. A blue alert bar will appear across the top of the possibly impacted pages alerting you that an evaluation is in progress as well as how many are pending. A green alert bar will appear to inform you that the evaluation was successfully completed. Once the evaluations have completed, the Starling Identity Analytics & Risk Intelligence pages automatically update to take into account the impact of those configuration changes.

Viewing information about a matched account

From the Rule Details page, you can access additional information on the matched accounts which are impacted by the selected entitlement classification rule.

To view information about a matched account

1. From the Rules page, click a rule (or the › button associated with it) that has at least one matched account. This opens the Rule Details page.
2. On the Rule Details page, click **Matched Accounts**.
3. From the expanded Matched Accounts list, select the account for which you want to view additional information. This opens the Risk Profile page which contains the following information:
    - User information pane: This displays the name of the user and the time at which the account was last evaluated.
    - # of Matches over time: This graph shows the number of matches over time for the user based on entitlements.
    - Percent of grants via group access: This graph shows the percentage of grants based on group versus direct access.
    - Matched Rules table: This table displays the matched rules for the account. Selecting a rule from the list opens the Rule Evaluation Details page.

Cloning a rule

From the Rule Details page, you can clone an entitlement classification rule listed in the table at the bottom of the page.

To clone a rule

1. From the Rules page, click the rule (or the › button associated with it) that you want to clone. This opens the Rule Details page.
2. On the Rule Details page, click **Clone**.
3. Use the configuration options to make any changes to the cloned entitlement rule. The cloned rule must have a unique name, a description, and at least one data source must be selected.

    NOTE: To edit the name or description of a rule, click the ✎ button to the right of the field. Once you finish editing the rule name or description, you must click the ✔ button to save your edits. This will only save the changes made in that field. To remove any edits made in those fields, use the ✖ button.

NOTE: There are additional configuration options for the Highly Privileged Group Members rule. See Highly Privileged Group Members rule for more information.

NOTE: Once you have finished configuring the rule, clicking **Preview** shows what happens if the new rule is applied.

4. Click **Save** to add the cloned rule. The rule will now be available for use.

Editing a rule

From the Rule Details page, you can edit an existing entitlement classification rule.

To edit a rule

1. From the Rules page, click the rule (or the › button associated with it) that you want to edit. This opens the Rule Details page.
2. On the Rule Details page, use the configuration options to make any changes to the rule. The rule must have a unique name, a description, and at least one data source must be selected.

   NOTE: To edit the name or description of a custom rule, click the button to the right of the field. Once you finish editing the rule name or description, you must click the button to save your edits. This will only save the changes made in that field. To remove any edits made in those fields, use the button.

   NOTE: There are additional configuration options for the Highly Privileged Group Members rule. See Highly Privileged Group Members rule for more information.

   NOTE: Once you have finished editing the rule, clicking **Preview** shows what happens if the new rule is applied.
3. Click **Save** to save changes and close the dialog.

Highly Privileged Group Members rule

From the Rules page, you can configure the Highly Privileged Group Members rule for each configured data source to focus on accounts within specific domains or groups.

NOTE: Adding a new rule will override any existing default rule of that type. The default rule will then be hidden until the overriding custom rule is deleted. Once the custom rule is deleted, the default rule (including any previous edits) will reappear on the Rules table.

Configuring the Highly Privileged Group Members rule

1. From the Rules page, use one of the following methods to open the Rule Details page:
    - To create a new Highly Privileged Group Members rule:
        a. Click **New Rule** to open the New Rule page.
        b. In the Select Rule Template drop-down menu, select **Highly Privileged Group Members**.
    - To clone the existing Highly Privileged Group Members rule:
        a. Click the Highly Privileged Group Members rule (or the › button associated with it) that you want to clone. This opens the Rule Details page.
        b. On the Rule Details page, click **Clone**.
2. Enter a unique name for the rule.
3. Click the ✔ button to the right of the name to save the changes to this field.
4. Enter a description for the rule.
5. Click the ✔ button to the right of the name to save the changes to this field.
6. Select which data source(s) will be evaluated by the rule. For each selected data source a new pane will be made available under Groups.
7. For each data source you can use the following configuration options:
    - (Optional) **Groups with data source domain** drop-down menu: Use these settings to specify data source domains. Specifying a name in the **Enter a data source domain** field will evaluate data source domains based on that name. Use the **Groups in any data source domain** if you do not want to limit the evaluations to specifically named domains, but still want to evaluate based on the configured group.
    - (Optional) To remove a previously configured domain, click the 🗑 button.
    - (Optional) **Groups with name** drop-down menu: Use these settings to specify groups by name. Specifying a name in the **Enter a group name** field will evaluate groups based on that name and that match the above configured domain. Leave the field blank if you do not want to limit the evaluations to specifically named groups, but still want to evaluate based on the configured domain.
    - (Optional) Click **Add Group** to configure additional data source domains and groups.

    The default Highly Privileged Group Members rule is configured to evaluate groups in any data source domain with the name Administrators, Domain Admins, Enterprise Admins, Schema Admins, Hyper-V Administrators, DnsAdmins, Account Operators, Backup Operators, Cert Publishers, Group Policy Creator Owners, Protected Users, and Server Operators for each of your configured Active Directory and Active Roles data sources.

NOTE: Once you have finished configuring the rule, clicking **Preview** shows what happens if the new rule is applied.

8. Click **Save** to add the rule. The rule will now be available for use.

Disabling a rule

From the Rule Details page, you can disable any entitlement classification rules currently configured for Starling Identity Analytics & Risk Intelligence. This includes disabling any of the default rules, which cannot be deleted from Starling Identity Analytics & Risk Intelligence.

To disable a rule

1. From the Rules page, click the rule (or the › button associated with it) that you want to disable. This opens the Rule Details page.
2. On the Rule Details page, click **Enabled** to switch the rule to disabled. The option will now display Disabled.

   NOTE: To re-enable the rule, click **Disabled** to switch the rule to enabled.

3. Click **Save** to save changes and close the dialog.

Deleting a rule

From the Rule Details page, you can delete non-default entitlement classification rules.

NOTE: You are unable to delete a default rule, but default rules can be disabled (for more information, see Disabling a rule).

To delete a rule

1. From the Rules page, click the rule (or the › button associated with it) that you want to delete. This opens the Rule Details page.
2. On the Rule Details page, click **Delete** to permanently delete the rule. You will be redirected to the Rules page once the rule has been deleted.

5

Risk

Introduction to Risk

The Risk drop-down menu is used for accessing the Starling Identity Analytics & Risk Intelligence pages that allow you to locate and manage accounts within your data sources in order to identify and understand the entitlement classification rules currently applicable to them.

The following pages can be accessed from the Risk drop-down menu:

- Introduction to Compare Entitlements
- Introduction to High Risk Accounts
    - Introduction to Risk Profile
    - Introduction to Rule Evaluation
        - Introduction to Target Details

Introduction to Compare Entitlements

The Compare Entitlements page is used for comparing the entitlements of accounts. This allows you to quickly verify they are assigned entitlements appropriate to their needs and helps ensure consistency between similar accounts in order to avoid inadvertently assigning unnecessary entitlements.

Comparing entitlements

From the Compare Entitlements page you can compare the current entitlements for two accounts.

To compare entitlements

1. Within Starling Identity Analytics & Risk Intelligence, click **Risk** in the navigation bar.
2. From the drop-down menu, select **Compare Entitlements**.
3. On the Compare Entitlements page, use the **Select a data source** drop-down menu to select the data source which contains the two accounts for which you want to compare entitlements. Once you have selected a data source, two additional drop-down menus will appear.
4. Click the drop-down associated with the first **Search for Account** field.
5. To locate an account, begin typing in the empty field to filter the available accounts. Once the first account to compare is located, click the account name to populate the field.
6. Click the drop-down associated with the second **Search for Account** field.
7. To locate an account, begin typing in the empty field to filter the available accounts. Once the second account to compare is located, click the account name to populate the field.
8. Click **Compare**.

   All of the entitlement grants that are different between the two accounts will appear listed in a table at the bottom of the page. To the right of the entitlement grant information (permissions, status, target, and trustee) is a column for each account. A ✔ is used to indicate the account has the entitlement grant, while a ✖ is used to indicate the entitlement grant is not associated with the account. The following options are also available at the top of the table:

   - **Show All Entitlements**: Select this check box to display all entitlement grants for the two accounts.
   -  : Click this button to refresh the information displayed in the table
   -  : Click this button to open the print options for this table.
   - 

     : These buttons appear if more than one page is required to list the entitlement grants. Use the arrow buttons to move back and forth between pages.

Introduction to High Risk Accounts

The High Risk Accounts page is used for locating and identifying accounts based on their level of risk. The risk level is based on the entitlement classification rules the accounts are associated with. For example, by default an account that matches the Create Users rule will be considered a high risk since it has permissions to create users.

High Risk Accounts page

To display the High Risk Accounts page, click the **Risk** drop-down in the navigation bar and select **High Risk Accounts** from the drop-down menu. The High Risk Accounts page is used for identifying high risk accounts in your data source based on their association with the entitlement classification rules enabled in Starling Identity Analytics & Risk Intelligence.

The following information appears on this page:

Entitlement rules last evaluated

This displays the date and time that the entitlement rules were last evaluated by Starling Identity Analytics & Risk Intelligence.

High Risk Accounts

The number of accounts classified as being High Risk. The total number of evaluated accounts which are associated with your data sources appears beneath the number of high risk accounts.

Increased High Risk Accounts

The number of accounts that have had an increase in risk level since the last evaluation. The number of newly designated high risk accounts appears beneath the number of increased high risk accounts. These new high risk accounts are accounts that increased enough in risk level to become high risk since the last evaluation.

Data Sources

This displays the number of types of data sources that have been configured. The number of instances appears beneath the number of data sources and refers to the total number of instances regardless of data source type.

Evaluated Rules

This displays the number of rules that were last evaluated by Starling Identity Analytics & Risk Intelligence.

The following filtering options appear on this page:

NOTE: You must click **Search** in order to filter the High Risk Accounts table based on your selected parameters.

Risk Level

Use to search for accounts of a specific risk level. The following options are available: **Only High Risk** (default), **Only New High Risk**, **Only Increased High**

Risk, **Only Low Risk**, or **All**. You can use the search box at the top of the drop-down menu to narrow down the options.

Trustee Type

Use to search based on the type of trustee. The following options are available: **All**, **Direct Access**, or **Group Access**. You can use the search box at the top of the drop-down menu to narrow down the options.

Data Sources

Use to search for accounts in a specific data source. You can use the search box at the top of the drop-down menu to narrow down the options.

Rules

Use to search for accounts by a specific entitlement classification rule. You can use the search box at the top of the drop-down menu to narrow down the options.

Search for accounts

This field allows you to search for an account by name in the table appearing at the bottom of the High Risk Accounts page.

Search

Click this button to apply the selected filtering options.

For information on the table appearing at the bottom of the High Risk Accounts page, see High Risk Accounts table.

High Risk Accounts table

The High Risk Accounts table is displayed at the bottom of the High Risk Accounts page. It displays information on the accounts within your data sources. To filter the results displayed in this table, use the filtering options available above the table.

The following information and options appear listed in the table:

Name

This is the name of the account. Clicking on the name of an account will open the Risk Profile page. Increased high risk accounts are indicated by a  icon. Newly designated high risk accounts are indicated by a  icon.

Matched Entitlement Rules

This column displays the number of entitlement classification rules that are currently triggered by the account's entitlements. Clicking the value in this column will display a list of those rules. Clicking **See All** in the dialog will open the Rule Evaluation Details page.

Entitlements

This column displays the number of entitlements that currently trigger entitlement classification rules for the account. Clicking on the value in this column will open the Risk Profile page.

These buttons appear if more than one page is required to list the high risk accounts. Use the arrow buttons to move back and forth between pages.

Introduction to Risk Profile

The Risk Profile page is used to display the details for an account with high risk entitlement classification rules when the account name is clicked on the High Risk Accounts page or on the Rule Details page. This page is displayed when additional information is needed regarding a specific high risk account. For information on accessing this page, see Accessing the Risk Profile page or Viewing information about a matched account.

Accessing the Risk Profile page

The Risk Profile page provides insight into the selected high risk account.

To access the Risk Profile page

1. Click **Risk** in the navigation bar to open a drop-down menu with additional links.
2. Click **High Risk Accounts** in the drop-down menu to open the High Risk Accounts page.
3. Locate the high risk account you want to view additional details on in the High Risk Accounts table at the bottom of the page. You can use the filtering options available on the page to locate the account.
4. After locating the high risk account, click in the row associated with that account.

> NOTE: Clicking the value in the Matched Entitlement Rules column displays a list of the high risk entitlement rules associated with the account. Clicking **See All** on that dialog opens the Rule Evaluation Details page.

Risk Profile page

To access the Risk Profile page, see Accessing the Risk Profile page. The Risk Profile page is used for information regarding the risk level of an account.

The following information appears on this page:

(Account name)

This pane displays the name and information regarding the account.

of Entitlements over Time

This chart displays the entitlements that triggered entitlement classification rules for each of the listed dates. Clicking the name of an entitlement type within the legend will remove the related data from the chart. Clicking the name of the entitlement type a second time will add the data back into the chart.

Percentage of Entitlements via Group Access

This chart displays the entitlements that triggered entitlement classification rules during the last evaluation date. Clicking a type of access within the legend will remove the related data from the chart. Clicking the type of access a second time will add the data back into the chart.

For information on the table appearing at the bottom of the Risk Profile page, see Risk Profile table.

Risk Profile table

The Risk Profile table is displayed at the bottom of the Risk Profile page. It displays information on the matched rules for the account.

The following information and filtering option appear on this table:

Matched Rules

This displays the number of entitlement classification rules that are currently triggered by the account's entitlements. The table below specifies each of those matched entitlement classification rules.

To search based on a rule name, hover over this icon to display the Filter Rules field. Begin typing the name of the rule you want to locate and the Risk Profile table will update accordingly.

Rules

This column lists the name of the rule. A rule that resulted in an increased risk level for an existing high risk account is indicated by a icon. A rule that resulted in a newly designated high risk account is indicated by a icon.

Direct Entitlements/Group Entitlements display

The center portion of this table uses colored bars (a key is provided at the bottom of the table) to reflect the type and number of entitlement(s) associated with the entitlement classification rule (for example, a combination bar of light and dark blue shows that within the same entitlement classification rule both Direct Entitlements and Group Entitlements were matched). Hover over the bar for an explanation of what is being displayed.

Entitlements

This displays the total number of entitlement matches within the entitlement classification rule, regardless of whether they were direct or group entitlements.

Selecting any rule listed in this table will display the associated Rule Evaluation Details page

Introduction to Rule Evaluation

The Rule Evaluation Details page is used for displaying information regarding individual rules assigned to an account in your data source. This page is displayed by clicking any of the rules listed for an account on the Risk Profile page.

Rule Evaluation Details page

To display the Rule Evaluation Details page, click any of the matched rules listed for an account on the Risk Profile page. The Rule Evaluation Details page is used for displaying information regarding the rules assigned to an account in your data source.

The following information appears on this page:

(Account name)

This pane displays the name and information regarding the account. Increased high risk accounts are indicated by a icon. New high risk accounts are indicated by a icon.

Matched Rules

This displays the number of entitlement classification rules that are currently triggered by the account's entitlements.

Entitlements

This displays the total number of entitlement matches within the entitlement classification rule.

The table at the bottom of the page displays the specific information regarding the rules. See Rule Evaluation Details table for more information.

Rule Evaluation Details table

The Rule Evaluation Details table is displayed at the bottom of the Rule Evaluation Details page. It displays information on a specific rule assigned to an account in your data source.

The following information appears listed in the table:

(Rule name)

This is the name of the rule. A rule that resulted in an increased risk level for an existing high risk account is indicated by a icon. A new high risk rule that is associated with the account is indicated by a icon.

To locate a specific rule, hover over the icon above the table to display the Filter Rules field. Begin typing the name of the rule you want to locate and the Rule Evaluation Details table will update accordingly.

Entitlements

This displays the total number of entitlement matches within the entitlement classification rule. Depending on the data collected, there may be multiple permissions listed that are related to a single entitlement. For example, a permission may be assigned to both a local and built-in account, however it is still related to the same entitlement and so is only counted once. In some cases there may be multiple entitlements that when combined will match the entitlement classification rule. When this occurs a **Multiple Entitlements** drop-down menu can be expanded to show the entitlements which were combined.

(Verification)

This column displays the current verification status for the associated rule. The following statuses may appear:

- **Request verification**: This link is available for requesting verification that the listed user should in fact match this rule. For more information see Requesting

verification.

- **Pending verification**: This status shows that a request for verification has occurred but has not yet been completed. Click the icon for additional information on the status. A pending verification request may be canceled by an administrator manually on the Verification page, or may be canceled automatically by Starling Identity Analytics & Risk Intelligence if the configuration or data is changed which causes the rule to no longer be matched for the account. This can occur when the rule is disabled or deleted, a default rule is replaced with a cloned rule, the data source instance is unlicensed, or the matched entitlements are removed from the data source instance for the account.
- **Risk verified**: This status shows that the user has been confirmed as needing to match the listed rule. Click the icon to open the Verification Details page for additional information on the status.
- **Requires mitigation**: This status shows that although the data source currently has the user matching this rule, this should not be the case. Any rules marked as Requires mitigation should be removed for the user within the data source.

Expanding a rule on the table displays the following information regarding the rule:

Permissions

This is the type of permission assigned to the entitlement classification rule. A icon appearing to the left of a permission name indicates the entitlement is new.

Trustee Type

This is the type of trustee associated with the rule. The following types may appear:

- **Direct**: Indicates a direct membership.
- **Group**: Indicates a direct member of a group that gives them rights to the trustee.
- **Group (Member & Nested)**: Indicates both a direct member and a member of a nested group that gives them rights to the trustee.
- **Group (Nested)**: Indicates a member of a nested group that gives them rights to the trustee.

Trustee

This is the trustee associated with the rule. If the permission is granted due to a nested membership, indicated by a Trustee Type of either Group (Member & Nested) or Group (Nested), the name of the trustee can be clicked to open the Group Membership Details dialog. This dialog displays the name of the account, the trustee, whether it is a direct (true) or indirect (false) group membership, and lists the nested groups that allowed for rights to the trustee.

Data Source

This is the type of data source associated with the rule.

Instance

This is the instance associated with the rule.

Target

For Active Directory and Active Roles rules this column shows the target container (Group, Domain-DNS, Organizational-Unit, and so on) associated with the granted permission. For Safeguard rules this column shows either the entitlement name, user name, or a path-like value (which includes the entitlement name, policy name, and possibly an account name) associated with the granted permission.

Affected (object type)

This is the number of objects affected by the permission.

NOTE: Currently the Create Groups, Create Organizational Units, and Create Users entitlement classification rules display as zero in the Affected (object type) column.

Clicking on an expanded rule with one or more affected objects opens the Target Details page which lists the affected and unaffected objects associated with the rule. If there are no affected objects then the Target Details page will not be available for the rule.

Requesting verification

The following procedure explains how to request verification that the listed user should in fact match this rule.

To request verification

1. Click **Risk** in the navigation bar to open a drop-down menu with additional links.
2. Click **High Risk Accounts** in the drop-down menu to open the High Risk Accounts page.
3. Locate the high risk account you want to view additional details on in the High Risk Accounts table at the bottom of the page. You can use the filtering options available on the page to locate the account.
4. After locating the high risk account, click in the row associated with that account to open the **Risk Profile** page.
5. Click one of the rules listed in the Matched Rules section to open the Rule Evaluation Details page.
6. On the Rule Evaluation Details page, locate the rule for the user that you want to

verify and click the associated **Request verification**. To locate a specific rule, use the button at the top of the table to search according to rule name.

NOTE: If you do not have a verifier account available, you will be unable to proceed until a new collaborator with the appropriate permissions is invited to your organization.

7. On the Request Verification dialog, the information to be verified will be listed along with the Assign to verifier drop-down menu. Select the name of the verifier using the drop-down menu.
8. Click **Submit Request**. The selected verifier will be notified that verification has been requested and the Rule Evaluation Details page will update to display the current status of your verification request. The request will also be listed on the Verification page.

   After a request has been sent, clicking on the verification column will direct you to additional information regarding the status of the request. See Verification Details page for more information.

Introduction to Target Details

The Target Details page is used for displaying the affected and unaffected targets associated with a rule. This page is displayed by clicking on the expanded information for any of the rules listed on the Rule Evaluation Details page.

Target Details page

To display the Target Details page, click on the expanded information for any of the rules listed on the Rule Evaluation Details page. The Target Details page is used for listing the affected and unaffected targets associated with the rule.

The following information appears on this page:

(Account name)

This pane displays the name and information regarding the account. Increased high risk accounts are indicated by a . New high risk accounts are indicated by a icon.

(Rule name)

This displays the name and information regarding the rule. A rule that resulted in an increased risk level for an existing high risk account is indicated by a icon. A new high risk rule that is associated with the account is indicated by a icon. An icon will also appear next to the permissions to indicate the change to the entitlements.

(Object type) affected

This displays the percentage of this object type (for example, Group or OrganizationalUnit) impacted by this rule. The total number of affected objects appears beneath the percentage.

(Object type) unaffected

This displays the percentage of this object type (for example, Group or OrganizationalUnit) not impacted by this rule. The total number of unaffected objects appears beneath the percentage.

The table at the bottom of the page displays specific information regarding the affected and unaffected objects. See Target Details table for more information.

Target Details table

The Target Details table is displayed at the bottom of the Target Details page. It displays information on the affected and unaffected objects associated with a rule.

The following information appears listed in the table:

Show

Use this drop-down menu to filter the listed objects by **Affected targets only** (default), **Unaffected targets only**, or **All targets**.

Hovering over this icon displays a search box used to locate a specific object. To use the field, start typing in the field to search according to name or location. The table will automatically update to display results that match.

(Object type)

This displays the name of the affected object.

Location

This column displays the location of the parent node for the object.

Inherited from

This column displays where the permission is inherited from. In cases where the permission is inherited directly from the listed object it will display the word Self.

Status

This is the status of the object (Affected or Unaffected).

These buttons appear if more than one page is required to list the objects. Use the arrow buttons to move back and forth between pages.

Verification

Introduction to Verification

Starling Identity Analytics & Risk Intelligence allows administrators and verifiers the ability to review entitlement verification requests for the high risk users within their data sources. Verification does not automatically alter your data source to correspond with the decisions recorded for a user within Starling Identity Analytics & Risk Intelligence. Instead the verification feature is a way for you to easily understand, make, and track decisions regarding user access.

For example, Starling Identity Analytics & Risk Intelligence alerts you to there being a new high risk user due to an account being granted the ability to create groups within Active Roles. This capability is outside the normal responsibilities for this account so you request that a verifier (other than yourself) takes a second look at the appropriateness of this access (see Requesting verification). That verifier can then either approve it as being acceptable or they can mark it as being unacceptable (see Verifying high risk entitlement requests). Once a response has been received you will have a record of the request within Starling Identity Analytics & Risk Intelligence in case this access level is ever questioned. And in cases where the decision was that the access was inappropriate you have a record of that user needing to be removed from the rule within Active Roles.

This verification process is available to users designated as administrator or verifier for the Starling Identity Analytics & Risk Intelligence service using the Collaborators page.

NOTE: Collaborators that are only assigned the verifier role will only be allowed to access this page within Starling Identity Analytics & Risk Intelligence. All other configuration pages will be hidden from verifiers unless they are assigned the administrator role. In addition, verifiers will only see the items assigned to them on this page whereas administrators will see all verifications.

Verification page

The Verification page is displayed when the **Verification** link is clicked in the navigation bar. The Verification page is used for reviewing entitlement verification requests for high risk users.

IMPORTANT: Administrators will see information on all verifications while verifiers will only see the items assigned to them.

IMPORTANT: Should a data source instance be purged, account data related to the instance will be permanently removed from the verification history. This includes verification details for the requests related to the purged data source instance and requests with no remaining associated data source instances.

The following information and options appear on this page:

Approved Requests

This is the number of requests that have already been approved.

Pending Requests

This is the number of requests that have yet to be responded to by the assigned verifier.

Rejected Requests

This is the number of requests that have been rejected. The rejected requests should be reviewed and any necessary changes made within the data source to ensure a user has not been granted access beyond that which is required for their position.

NOTE: Customers that use ServiceNow can create incident tickets for rejected requests. See Connecting with ServiceNow for more information.

Show

This drop-down menu is for selecting the types of requests to display on this page. The following options are available: **All requests**, **Approved requests only**, **Pending requests only** (default), **Rejected requests only**, or **Canceled requests only**.

Hovering over this button displays a search box used to locate specific requests within the listed verifications. To search, click in the empty field and start typing the name of the request in the field and the table will automatically update to display requests that match. If you have configured ServiceNow (Connecting with ServiceNow) then you can also search based on the ticket number.

The following information and button appears in the list of verifications on this page:

(Account name)

This displays the name of the account to which the rule applies and shows the rule that needs to be verified.

Requested by

This displays the name of the person requesting the verification.

Assigned to

This displays the name of the person who is responsible for verifying the request.

(Status)

This column displays the current verification status for the associated rule and the time at which the status was last updated. The following statuses may appear and when selected will direct you to the Verification Details page for more information:

- **Pending verification**: This status indicates that a request for verification has occurred but has not yet been completed. A pending verification request may be canceled by an administrator manually, or may be canceled automatically by Starling Identity Analytics & Risk Intelligence if the configuration or data is changed which causes the rule to no longer be matched for the account. This can occur when the rule is disabled or deleted, a default rule is replaced with a cloned rule, the data source instance is unlicensed, or the matched entitlements are removed from the data source instance for the account.
- **Risk verified**: This status indicates that the user has been confirmed as needing to match the listed rule.
- **Requires mitigation**: This status indicates that although the data source currently has the user matching this rule this should not be allowed for the user. Any rules marked as Requires mitigation should be removed for the user within the data source.
- **Canceled**: This status indicates that a pending verification has been canceled. The verification request can be canceled by an administrator manually, or may be canceled automatically by Starling Identity Analytics & Risk Intelligence if the configuration or data is changed which causes the rule to no longer be matched for the account. This can occur when the rule is disabled or deleted, a default rule is replaced with a cloned rule, the data source instance is unlicensed, or the matched entitlements are removed from the data source instance for the account.

NOTE: The following options appear for each request depending on the role of the current account.

(administrators)

This displays additional options for administrators regarding the request. The following options appear:

- **Review**: This opens the Verification Details page.
- **Re-send request**: Selecting this option will re-send the email request to the verifier.
- **Cancel request**: Selecting this option allows you to cancel the verification request. You will be prompted for confirmation before the request is canceled.

Review (verifiers)

Clicking this link opens the Verification Details page where the verifier can select whether they agree or disagree with this level of access for the user. Once they have made their selection, the status of the request will be updated.

Verification Details page

The Verification Details page is displayed when you click on the verification status for a rule on the Rule Evaluation Details page or you click on a verification request listed on the Verification page. The Verification Details page is used for reviewing information on a specific entitlement verification request and is also used by verifiers to respond to their requests.

The following information appears on this page:

(Account name)

This pane displays the name and information regarding the account.

High risk access

This pane displays why the access is considered high risk.

Verdict Summary

This pane displays the current status of the request, who initiated the request, the name of the verifier, and when the request occurred.

IMPORTANT: This pane is replaced with response options when the verifier opens the page. Verifiers use this pane to select whether they agree or disagree with this level of access for the user. For information on how to respond to requests, see Verifying high risk entitlement requests.

Additional information

Clicking this button will add a new pane which shows specific information regarding the rule. It includes the following information:

- **Rule name**: This is the name of the rule. A rule that resulted in an increased risk level for an existing high risk account is indicated by a icon. A new high risk rule that is associated with the account is indicated by a icon.
- **Rule name**: This is the name of the rule. A rule that resulted in an increased risk level for an existing high risk account is indicated by a icon. A new high risk rule that is associated with the account is indicated by a icon.
- **Entitlements**: This displays the total number of entitlement matches within the entitlement classification rule. Depending on the data collected, there may be multiple permissions listed that are related to a single entitlement. For example, a permission may be assigned to both a local and built-in account, however it is still related to the same entitlement and so is only counted once. In some cases there may be multiple entitlements that when combined will match the entitlement classification rule. When this occurs a **Multiple**

Entitlements drop-down menu can be expanded to show the entitlements which were combined.

- **Permissions**: This is the type of permission assigned to the entitlement classification rule. A icon appearing to the left of a permission name indicates the entitlement is new.
- **Trustee Type**: This is the type of trustee associated with the rule. The following types may appear: Direct which indicates a direct membership, Group which indicates a direct member of a group that gives them rights to the trustee, Group (Member & Nested) which indicates both a direct member and a member of a nested group that gives them rights to the trustee, and Group (Nested) which indicates a member of a nested group that gives them rights to the trustee.
- **Trustee**: This is the trustee associated with the rule. If the permission is granted due to a nested membership, indicated by a Trustee Type of either Group (Member & Nested) or Group (Nested), the name of the trustee can be clicked to open the Group Membership Details dialog. This dialog displays the name of the account, the trustee, whether it is a direct (true) or indirect (false) group membership, and lists the nested groups that allowed for rights to the trustee.
- **Data Source**: This is the type of data source associated with the rule.
- **Instance**: This is the instance associated with the rule.
- **Target**: For Active Directory and Active Roles rules this column shows the target container (Group, Domain-DNS, Organizational-Unit, and so on) associated with the granted permission. For Safeguard rules this column shows either the entitlement name, user name, or a path-like value (which includes the entitlement name, policy name, and possibly an account name) associated with the granted permission.

Verifying high risk entitlement requests

The following procedure explains how verifiers respond to requests.

IMPORTANT: Once a request has been responded to there is no way to undo the decision within Starling Identity Analytics & Risk Intelligence, however there is no impact on your data source. So a rule marked as requiring mitigation will not remove the user from the rule and an approved verification will not stop a user from being removed from the rule within the data source.

To verify a high risk entitlement request

1. Click **Verification** in the navigation bar to open the Verification page.
2. Locate the request you want to verify and click **Review**.

3. On the Verification Details page, review the request details (click **Additional Information** for more information regarding the entitlement). Select one of the following options depending on whether or not the request should be approved:
    - **Yes, I understand the risk with this level of access and agree that <*account name*> should possess it**: Selecting this option will approve the access level as being appropriate. The rule will now be marked as being verified for that user.
    - **No, I do not believe <*account name*> should have such a high level of access and request it to be reviewed**: Selecting this option will flag the access level as being inappropriate for the user. Any rules marked as requiring mitigation should be removed for the user within the data source.

        NOTE: Customers that use ServiceNow can create incident tickets for rejected requests. See Connecting with ServiceNow for more information.
4. Once you have selected the appropriate action for the rule, click **Submit Response**.

Reports

Introduction to Reports

Customized reports can be generated and downloaded from Starling Identity Analytics & Risk Intelligence in order to view and preserve data outside of the cloud service as a CSV file.

The following reports are available:

IMPORTANT: Reports only cover data which is currently available within Starling Identity Analytics & Risk Intelligence. If you have a scheduled data collection occurring at the same time you request a report, the report will not include the data which has not yet finished being collected. Use the Data Source Modules page to check that data collection has completed and the time of the last update.

NOTE: Reports that have been generated will be retained within Starling Identity Analytics & Risk Intelligence for 30 days. Reports older than 30 days will be permanently deleted.

- Weekly Summary: This report covers a high level view of the previous 7 days from when the report was created. It includes general data regarding accounts, entitlements, rules, and data sources.
- High Risk Accounts: This reports covers information on the current high risk accounts.
- Rules: This report covers information regarding the currently configured rules.
- Verification: This report covers information regarding all requested verifications.

Reports page

IMPORTANT: Reports only cover data which is currently available within the Starling Identity Analytics & Risk Intelligence. If you have a scheduled data collection occurring at the same time you request a report, the report will not include the data which has not yet finished being collected. Use the Data Source Modules page page to check that data collection has completed and the time of the last update.

NOTE: Reports that have been generated will be retained within Starling Identity Analytics & Risk Intelligence for 30 days. Reports older than 30 days will be deleted.

The Reports page is displayed when the **Reports** link is selected from the navigation bar. The Reports page is used for downloading customized reports.

The following buttons appear on this page:

New Report

Click this button to open the New Report dialog which allows you to generate a new report. The following reports are available:

- **Weekly Summary**: This report covers a high level view of the previous 7 days from when the report was created. It includes general data regarding accounts, entitlements, rules, and data sources.
- **High Risk Accounts**: This reports covers information on the current high risk accounts.
- **Rules**: This report covers information regarding the currently configured rules.
- **Verification**: This report covers information regarding all requested verifications.

See Generating a report for more information.

Show

This drop-down menu filters the displayed reports based on type: All Reports (default), Weekly Summary Reports, High Risk Accounts Reports, Rules Reports, Verification Reports.

Once reports have been generated, the following information and options appear for each report:

Category

This column displays the type of report (Weekly Summary, High Risk Accounts, Rules, Verification).

Created by

This column displays the name of the account that requested the report.

Report date

This column displays the date and time the report was created.

Status

This displays the current status for the report. The following information may appear:

- **Queued**: This status indicates the report has been created but not yet begun processing.
- **Processing**: This status indicates the report is currently being generated.
- **Complete**: This status indicates the report has completed processing and is available for downloading.

Click this button to select what to do with the report: **Download report** (see Downloading a report) or **Delete report** (see Deleting a report).

Generating a report

The following explains how to generate a report from Starling Identity Analytics & Risk Intelligence so that it will be available for downloading as a CSV file.

To generate a report

IMPORTANT: Reports only cover data which is currently available within Starling Identity Analytics & Risk Intelligence. If you have a scheduled data collection occurring at the same time you request a report, the report will not include the data which has not yet finished being collected. Use the Data Source Modules page to check that data collection has completed and the time of the last update.

1. From the Reports page, click **New Report**.
2. Use the **Select a Category** drop-down menu to select the type of report that will be generated.
3. Click **Create Report** to generate the report. Once the report has finished processing it will be available for download as a CSV file. See Downloading a report for more information.

   NOTE: Once a report has been created it will remain available in Starling Identity Analytics & Risk Intelligence for 30 days or until it has been manually deleted (see Deleting a report).

Downloading a report

The following explains how to download a report from Starling Identity Analytics & Risk Intelligence.

To download a report

NOTE: A report must finish processing before it will be available for download. See Generating a report for more information.

1. From the Reports page, click the  button associated with the report you want to download.

2. Select **Download report** from the drop-down menu.
3. Follow the prompts to complete downloading the report as a CSV file.

Deleting a report

The following explains how to delete a report from Starling Identity Analytics & Risk Intelligence.

To delete a report

1. From the Reports page, click the ⋮ button associated with the report you want to delete.
2. Select **Delete report** from the drop-down menu.
3. Click **OK** on the confirmation dialog. The report will now be permanently deleted from Starling Identity Analytics & Risk Intelligence.

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