IdentityIQ Risk Scoring

Version: 8.4

Revised: September 2023

Copyright and Trademark Notices

Contents

Configure Risk Scoring

Use the risk scoring configuration pages to define the algorithms used by IdentityIQ to determine risk scores for identities and applications within your organization. Risk scores are used throughout the product to highlight high risk users and accounts and to trigger notices when configured to do so.

To access Risk configuration options, go to **Identities > Identity Risk Model** or **Application > Application Risk Model**. Configuring risk scoring requires the assignment of administrative capabilities within IdentityIQ.

To configure risk scoring for identities and applications refer to following:

- Identity Risk Score Configuration
- Application Risk Score Configuration

Identity Risk Score Configuration

IdentityIQ uses a combination of base access risk and compensated scoring method to determine the overall Identity Risk Scores, or Composite Risk Score, used throughout the product. You configure Baseline Access and Composite risk scoring for identities by navigating to **Identities > Identity Risk Model**.

Base access risk is a measure of inherent user access risk. Base risk scores are set on each role, entitlement, and policy defined. This type of score ranges from 0 (lowest risk) to 1000 (highest risk). The account weight assigned to any additional entitlements that are assigned to an identity also have an impact base risk scores. Account weights are factored in to the entitlement baseline access risk scores.

IdentityIQ applies a series of compensating factors to each base risk score to calculate compensated scores. These compensated scores are then weighted using a maximum contribution percentage and combined to form an overall Composite Risk Score for each user.

The compensating factors and weighted values enable IdentityIQ to accurately identify high-risk users based on more than just the roles they are assigned within your enterprise.

For example, a user assigned only low risk roles might be considered high risk if they have never been included in a certification process or the roles they do have are in violation of separation of duty policies.

Scoring Definitions

There are a number of scores, or types of scores, that contribute to the overall Identity Risk Score, or Composite Risk for each IdentityIQ user. The basic scores that are used to determine the overall score are:

Score	Definition
Base Risk Score	The score assigned to each role, entitlement, or policy violation.
Total Base Risk Score	The total score of all base risk scores of the same component type on a per user basis. For example, add the base risk scores for all roles assigned to a specific user together to determine the role total base risk score.
Compensated Risk Score	The value of the base risk score for a component multiplied by the compensating factor for that component type.
Total Compensated Risk Score	The Total Base Risk Score for a specific component type multiplied by the Compensated Risk Score for that component type.
Composite Risk Score or Identity Risk Score	The overall risk score for a user after the composite weighing, or maximum contribution to total score factor, is applied to the total compensated risk scores for each component.

Score	Definition
	The time since the last certification was performed on the user is also figured into this score with the total compensated scores for role, entitlement, and policy violation.

Use the sliding bars or manually enter a value, to define scoring on each panel.

Use the following tabs to create risk score factors for your enterprise:

- Identity Baseline Access Risk Tab — apply base risk scores to roles, entitlements and policy violations.
- Identity Composite Scoring Tab — apply compensating factors to base risk scores.

Identity Baseline Access Risk Tab

The Baseline Access Risk score is a measure of inherent risk. A user's Baseline Access Risk score rarely changes because their role within the enterprise is the primary factor in defining the score. This type of score ranges from 0 (lowest risk) to 1000 (highest risk).

Select one of the following options to define how IdentityIQ calculates base access risks. Each role, entitlement, and policy violation is assigned a score that falls into a band. The number of bands is configured on the Advanced Configuration page and applies to the entire IdentityIQ application.

To configure baseline access risk scores for role, entitlement, and policy violation access, navigate to **Identities > Identities Risk Model** and select the **Baseline Access Risk** tab.

Role Baseline Access Risk

Role Baseline Access Risk score is calculated based on the roles correlated to the identity. This list contains every role defined in IdentityIQ. To limit the number of items displayed in the list, filter the list by role name and type.

Column	Description
Name	The name of the role.
Type	The role type as defined when the role was modeled.
Description	The description of the role as defined when the role was modeled.
Risk Level	The current risk level assigned to the role.

Click on a role to display the configuration panel to see the role details and set or modify the risk level. Use the slider control to set the risk level or enter a value in the field on the right.

Entitlement Baseline Access Risk

Entitlement Baseline Access Risk score is calculated based on the additional entitlements correlated to an identity. Additional entitlements are entitlements that are assigned to a user, but are not part of any of the roles assigned to that user.

Entitlements fall into two categories: Permissions and Attributes. A Permission is a privilege, such as create, read, update, delete, and execute. Attributes are customized user characteristics made up of an attribute/value pair, such as group/Administrators. A risk score is configured for each Permission and Attribute/Value pair in the system. A user's Entitlement Baseline Access Risk score is determined by summing the risks associated with each of the additional entitlements that they hold.

Use this page to add applications to the list and to work with the entitlements on each. The Entitlement Baseline Access Risk Configuration page contains the following information:

Column	Description
Application	The name of the application with which the entitlements are associated.
Account Weight	The default score assigned to any identity that is assigned entitlements on this application. Account Weight scores are not compensated. This score is not applied to the identity risk score if the entitlements assigned to the user are, either all used as part of roles assigned to the user, or if the risk score for all of the entitlements assigned to the user are zero based on certification rules.
Permissions	Click in this column to modify the weight assigned to the permissions for the associated application. Use the sliding bar or enter a value in the field on the right to modify permission weight.
Attributes	Click in this column to add, delete or modify the weight assigned to the attributes for the associated application. Select an attribute from the drop-down list, type an attribute name, and click **Add** to assign a weight to a new attribute, or modify and existing attribute in the list. Select an attribute using the check-boxes on the left and click **Delete** to remove an attribute from the list.

To add an application to the list, select an application from the drop-down list on the bottom of the page. The list contains all of the application configure to work with IdentityIQ that are not currently on the list. Use the Permissions and Attributes columns to add entitlements to applications for risk tracking.

Policy Violation Baseline Access Risk

Policy Violation Baseline Access Risk score is calculated using policy violations that are detected for a user based on defined policy rules. A risk score is configured for every rule in each policy or for the policy if no rules apply. This score

is calculated by taking the sum of the risks associated with every policy or rule that the user violates.

Use the Policy Violation Baseline Access Risk page to view and modify the risk level associated with each policy or policy rule defined. The page is divided into tables based on policy type. If the policy does not contain rules, set the risk level for the entire policy. Use the slider or type a value in the field to the right.

Identity Composite Scoring Tab

Use the Composite Scoring tab to assign value to the compensating factors for each base component used to calculate the composite risk scores for users. You can also define the maximum contribution of each component to the total score. The maximum composite risk score is 1000. Use the Maximum Contribution to Total Score value to control the impact of compensated scores on composite scores.

Use the Composite Scoring tab to define the maximum impact of a total compensated score on a user's Composite Risk Score. For example, if the time since the last certification on an identity is considered low risk, you can set the Certification Age to a low value, such as 20% so that even at its maximum value that component only contributes 200 points of the total 1000. If, however, policy violations are considered high risk, you can set the Separation of Duty Violation Compensated Score to 100% so that policy violations move users into the high-risk category quickly. Use the Composite Scoring tab to define the maximum impact of a total compensated score on a user's Composite Risk Score.

Category	Compensating Control
Role Compensated Score	Based on applying the following compensating factors to each role base score: The user's role has never been certified before The user's role is approved The user's role was allowed as an exception An allowed exception on the user's role has expired Revocation of the user's role is pending Activity monitoring is enabled on one or more applications associated with the user's role
Entitlement Compensated Score	Based on applying the following compensating factors to each entitlement base score: The user's entitlement has never been certified before The user's entitlement is approved

Category	Compensating Control
	The user's entitlement was allowed as an exception An allowed exception on the user's entitlement has expired Revocation of the user's entitlement is pending Activity monitoring is enabled on one or more applications to which the user's entitlement applies
Policy Violation Compensated Score	Based on applying the following compensating factors to policy base score: The user's violation has never been certified before The user's violation was allowed An allowed exception on the user's policy violation has expired The user's policy violation remains uncorrected Activity monitoring is enabled on the applications on which the user's violation occurred
Certification Age Score	Based on applying the following compensating factors to an expired certification: The risk score starts increasing this many days after the latest certification The risk score reaches its maximum value this many days later
Inactive User Score	looks for inactive users. When this score is enabled any identity is found to be inactive, a default risk score of 500 is assigned for this score component

Application Risk Score Configuration

IdentityIQ uses a combination of Component and Composite scoring to determine the overall application risk scores used throughout the application. You configure Component and Composite risk scoring for your applications by navigating to **Applications > Application Risk Model**.

All scores are calculated by first determining the percentage of accounts that have the qualities tested by the component score. For example, if 10 out of 100 accounts are flagged as service accounts, then the raw percentage is ten percent (.10). This number is then multiplied by a sensitivity value which can be used to increase or decrease the impact of the original percentage. The default sensitivity value is 5 making the adjusted percentage fifty percent (.50). This final percentage is then applied to the score range of 1000 resulting in a component score of 500.

After the component score is calculated a weight, or compensating factor, is applied to each component score to determine the amount each contributes to the overall risk score for the application. The resulting score is the composite score. For example, a few violator accounts might increase risk more than many inactive accounts.

To view the currently configured risk information for an application, go to the **Application Definition** page, click on a listed application, and then select the Risk tab.

Use these tabs to create risk score factors for your enterprise:

- Application Component Scores Tab — apply base risk scores to roles, entitlements and policy violations.
- Application Composite Score Tab — apply compensating factors to base risk scores.

Application Component Scores Tab

Use the Component Scores tab to define the values for each account or component.

Service Account, **Inactive Account**, and **Privileged Account** component scores look for links that have a configured attribute. For example, the component `service` with a configured value `true`.

The **Dormant Account** score looks for a configured attribute that is expected to have a date value, for example `lastLogin`. This algorithm has an argument, `daysTillDormant`, that defaults to thirty (30). If the last login date is more than thirty (30) days prior to the current date, the account is considered dormant and is factored into the risk score.

The **Risky Account** score looks for links whose owning identity has a composite risk score greater than a configured threshold. The default threshold is five hundred (500).

The **Violator Account** score looks for links whose owning identity has a number of policy violations greater than a configured threshold. The default threshold is ten (10).

If you check **Disabled** for any componet, the component is not used to determine the application risk score.

Application Composite Score Tab

Use the **Composite Scoring** tab to apply a weight or compensating factor for each component. Specify the percentage of contribution for the component scores.

Viewing Application and Identity Risk Scores

Use the **Intelligence > Identity Risk Score** page to view individual risk scores for users. The page displays one tab for each risk level defined in IdentityIQ. The risk criteria and number of risk levels are defined during the configuration process.

Use the **Intelligence > Application Risk Scores** page to view the risk scores associated with each application. This page displays a table that summarizes all of the applications score cards. The score information for each applications is separated into scoring components that were defined when the product was configured.

Identity Risk Scores

Use this page to view individual risk scores for users. The page displays one tab for each risk level defined in IdentityIQ. Click a tab to display a list of all of the users that fall into that risk level.

You can access this page from the navigation menu bar. Go to **Intelligence > Identity Risk Scores**.

Use the **Filter** options to reduce the number of identities displayed on the list.

- The **Group to filter by** drop-down list is contains all of the groups defined for your enterprise when IdentityIQ was configured and is based on attributes use for identity mapping.
- The **Value** drop-down list contains all of the values assigned to the selected attribute.

Identity risk scores are determined by weighted scores assigned to components that comprise the individual's Identity Cube. The identity risk scores table lists the component scores and enables you to identify the areas most at risk and take the appropriate actions.

From the **Identity Risk Scores** table you can schedule Identity Certifications for any or all identities listed. Identity Certifications are certification requests for identities with risk scores that warrant special attention. For example, a contract database administrator might require more frequent certification than a full-time employee. These do not replace the regularly scheduled certification requests, such as Manager or Application, but are in addition to those certifications.

This Identity Risk Scores table includes the following:

Column Name	Description
Identity selec-	Activate this check-box to mark this user as one for whom to request an Identity

Column Name	Description
tion box	Certification.
Name	The login name of the user. Only users with risk scores that fall into the risk band associated with the selected tab are displayed.
First Name	The first and last name of the user.
Last Name	
Composite Score	The total composite risk score for the user. This score is based on risk factors defined when IdentityIQ was configured for your enterprise.
Role	The sum of compensated role risk scores as defined when IdentityIQ was configured.
Entitlement	The sum of compensated entitlement scores as defined when IdentityIQ was configured.
Policy	The sum of compensated risk scores associated with policy violations as defined when IdentityIQ was configured.
Certification	The sum of compensated risk scores associated with certifications as defined when IdentityIQ was configured.

Click a user in the table to open the **View Identity** page. The View Identity page contains individual Identity Cube risk information. Identity Cubes are multi-dimensional data models of identity information that offer a single, logical representation of each managed user. Each Cube contains information about user entitlements, associated context and historical records of user access configurations and activity.

Application Risk Scores

Use this page to view the risk scores associated with each application. You can access this page from **Intelligence > Application Risk Scores**.

This page displays a table summarizing all of the applications score cards. The score information for each applications is broken down by the scoring components defined when the product was configured. The first column in the table contains the composite risk score for the application. The composite score is calculated by combining the compensated scores of the individual components.

Click an application in the table to display the **Edit Application** page. Click the **Risk** tab to view the latest score card for the application.

The algorithms used by the **Refresh Application Scoring** task to update this page are defined on the Application Risk page.

All scores are calculated by first determining the percentage of accounts that have the qualities tested by the component score. For example, if 10 out of 100 accounts are flagged as service accounts, then the raw percentage is ten

percent (.10). This number is then multiplied by a sensitivity value which can be used to increase or decrease the impact of the original percentage. The default sensitivity value is 5 making the adjusted percentage fifty percent (.50). This final percentage is then applied to the score range of 1000 resulting in a component score of 500.

After the component score is calculated, a weight or compensating factor is applied to each component score to determine the amount each will contribute to the overall risk score for the application. For example, a few violator accounts might increase risk more than many inactive accounts.

Service, **Inactive**, and **Privileged** component scores look for links that have a configured attribute. For example, the component `service` with a configured value `true`.

The **Dormant Account** score looks for a configured attribute that is expected to have a date value, for example `lastLogin`. This algorithm has an argument, `daysTillDormant`, that defaults to thirty (30). If the last login date is more than thirty (30) days prior to the current date, the account is considered dormant and is factored into the risk score.

The **Risky Account** score looks for links whose owning identity has a composite risk score greater than a configured threshold. The default threshold is five hundred (500).

The **Violator Account** score looks for links whose owning identity has a number of policy violations greater than a a configured threshold. The default threshold is ten (10).