Identity Security Insights
Tenant Console Guide 24.04

Table of Contents

# Identity Security Insights Tenant Console Administration

The Identity Security Insights Tenant console provides the majority of views into your connected applications and services.

> ℹ️ *Identity Security Insights supports "direct linking" from all available pages, including filtered and sorted results, via the page URL. Authorized users are asked to log in before being directed to the linked page.*

Access Your Tenant Dashboard

Once logged in, your **Tenant** dashboard can be accessed from the main welcome screen by clicking the name of any existing tenant.

You can also access the existing tenants by clicking the name of your organization in the top navigation, and then selecting your tenant from the dropdown menu.
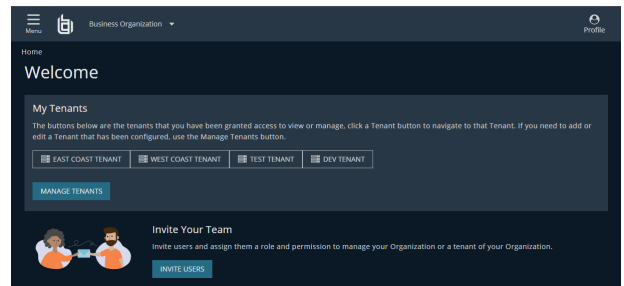

Tenant Dashboard Views

The **Tenant** dashboard is divided into a series of summarized views, granting you at-a-glance insights into your connected identities, accounts, and generated reports.

Overview

The console **Overview** provides a summary of your connectors, accounts, and associated entitlements.

- **Connectors** represent third- and first-party integrations from which Insights generates summaries and reports.
- **Total Accounts** displays all linked identities found by your active connectors.
- **Privileged Accounts** and **Accounts with Key Entitlements** display connected identities with high-level or administrative privileges, or accounts with membership in security groups or roles known to represent exploitable privileges.
- **Dormant Accounts** contains a list of all accounts which have not logged in for over three months, and have not rotated their password in over a year.
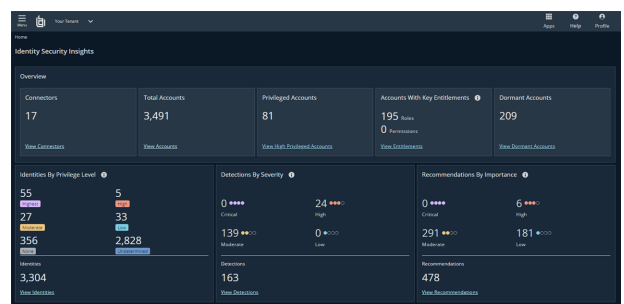
> ℹ️ *For more information, please see [Identity Security Insights Connector Administration](https://beyondtrust.com/docs/identity-security-insights/how-to/connectors/index.htm) at https://beyondtrust.com/docs/identity-security-insights/how-to/connectors/index.htm.*

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

3

Identities

The **Identities** summary displays color-coded risk assessments, displayed by importance and potential privilege, for connected accounts.

> ℹ️ *For more information, please see "Identity Security Insights Identities Dashboard" on page 7.*

Detections

The **Detections** tile summarizes potentially compromised identities. Examples of detections surfaced by Insights include suspicious login failures, missing multi-factor authentication, and stale or dormant accounts.

> ℹ️ *For more information, please see "Identity Security Insights Detections Dashboard" on page 9.*

Key Entitlements

Key Entitlements grant accounts a higher level of access or privilege. The Key Entitlements dashboard provides an at-a-glance view of elevated entitlements granted to your associated accounts and identities, allowing you to monitor and assess administrative roles, excess permissions, and more.

> ℹ️ *For more information, please see "Identity Security Insights Entitlements Dashboard" on page 11.*

Recommendations

Identity Security Insights provides **Recommendations** for security health and remediation based on automatic detections. Recommendations are organized by importance and severity. Addressing critical and high importance recommendations greatly improves your security posture.

> ℹ️ *For more information, please see "Identity Security Insights Recommendations Dashboard" on page 12.*

SALES: www.beyondtrust.com/contact **SUPPORT:** www.beyondtrust.com/support **DOCUMENTATION:** www.beyondtrust.com/docs

4

Identity Security Insights Accounts Dashboard

Overview

The **Accounts** page provides a view into the registered accounts associated with any registered connectors. Accounts can be viewed by source, linked identities, amount of privileged access, and more. Discover which accounts possess high-level or administrative privileges, and track membership in security groups or role access. Areas of potential risk and remediation are displayed in the **Detections** and **Recommendations** columns, respectively.

Accounts are displayed in order of privileged access and associated key entitlements by default. Privilege is broken down into *Highest*, *High*, *Moderate*, *Low*, *None*, and *Undetermined*, based on each account's administration and access capabilities.

Clicking any individual account name displays additional information associated with the account, including assigned roles, permissions, and linked identities.
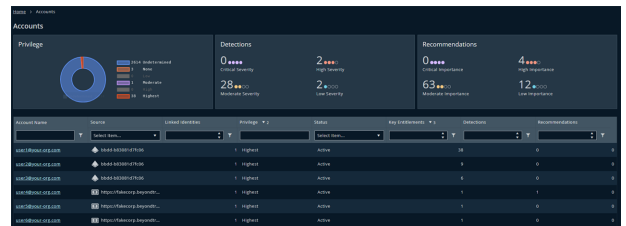
Filter and Export Results

The **Accounts** list can be sorted by any displayed column by clicking the column header. Columns can be shown or hidden using checkboxes by clicking the **Columns** button.

The **Label** column displays active and Disabled or **Dormant** accounts. Dormant accounts have not logged in for over three months, and have not rotated their password in over a year. Accounts can be further divided into **Human daily drivers** and **Password Safe managed** accounts.

The **Type** distinguishes between **Users**, **Service Principals**, and **Identity Center Users**.

Sorting the accounts dashboard by a combination of privilege, source, type, and other columns, can assist in identifying excessive or unnecessary privilege. For example, setting the source to Okta and the privilege to Highest will display all Okta accounts with the highest level of privilege detected. The resulting grid can be exported as a **CSV file** by clicking the download button to the right of the results.


Advanced Filters can be added to the grid by clicking **Add Filter** in the upper-left. Adding an advanced filter allows you to display results based on the provided expression. Multiple filters can be added at one time, and filters can be saved and linked to directly via the page URL.
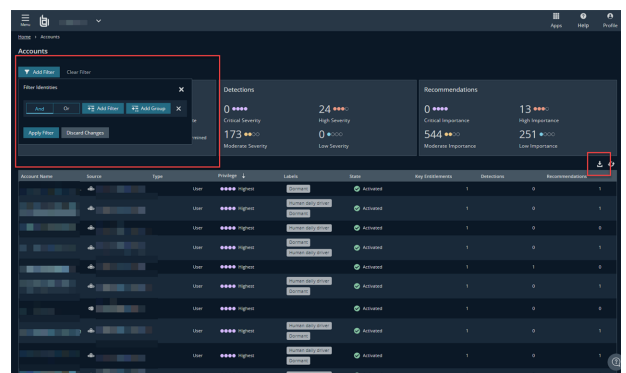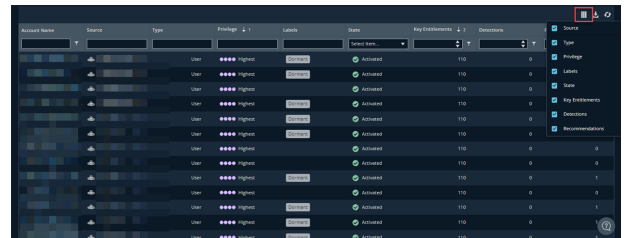
Account Details

Viewing **Account Details** displays additional information regarding an individual identity. This dashboard summarizes the account status, source, and assigned privilege, as well as a description of the detection, and includes additional attributes depending on the account source.

Any provisioned roles, access permissions, or associated accounts and identities discovered by Identity Security Insights are listed beneath the account summary. The **Detections** tab ranks any areas of risk according to possible severity. The **Recommendations** tab allows you to see what critical resolutions are available to mediate risk.
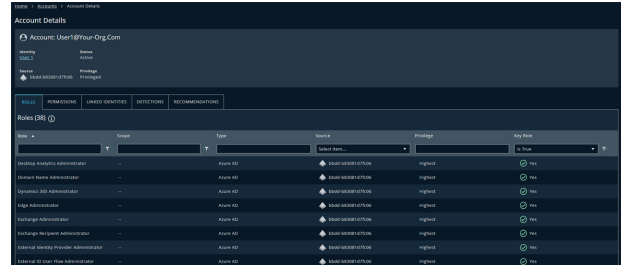
Entitlements

Entitlements grant an account a higher level of access or privileged permissions. The **Entitlements** tab allows you at-a-glance access to the identity's roles or permissions by source, enabling you to quickly identify areas of potential risk or elevated privilege.

Linked Identities

The **Identities** tab displays any user identities associated with the individual account, as well as their associated level of privilege. Clicking on any identity name displays the associated Identity dashboard.

> ℹ️ *For more information, please see the Identities guide at https://www.beyondtrust.com/docs/identity-security-insights/getting-started/tenant-console/identities.htm.*

Detections and Recommendations

Identity **Detections** are available to identify the individual risk assessed by Identity Security Insights. Clicking any individual detection displays detailed results, enabling you to understand both the risk and its importance or severity. The **Recommendations** tab provides a list of mediation possibilities for any potential vulnerabilities.

Detect Account-Related Risks

Sorting an account's detections by **Severity** displays the areas of greatest potential risk. Detections can further be organized by **Source** to limit the display to only detections associated with the selected connector, and the **Detection Summary filter** allows for filtering results by expressions. The dashboard shows **New** and **Under Review** detections by default.

Identity Security Insights uses custom machine learning methods to detect over-privileged accounts, allowing you to highlight accounts with unnecessary, unusual, or unused privileges. For example, a non-IT account with privileged roles in Entra ID can generate the detection **Entra ID Anomalous Privilege Based on Department**.

Evaluating the account-related detections generated by Insights can identify concerns like foreign Entra applications, overly-permissive IAM policies, and anomalous department- or title-based privileges.
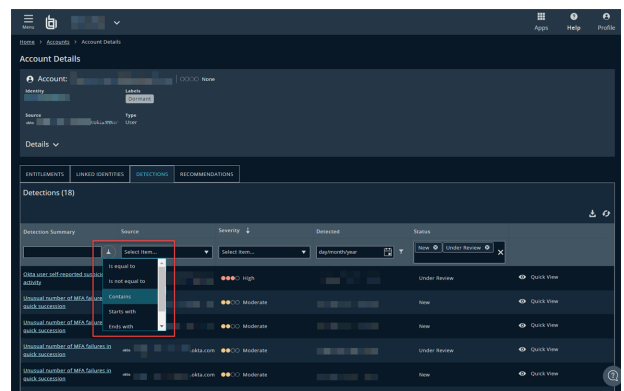
# Identity Security Insights Identities Dashboard

Overview

The **Identities** dashboard provides a view into all accounts and identities associated with your connected applications and services.

This dashboard displays accounts ranked by **Privilege**. Privilege is further broken down into **Highest**, **High**, **Moderate**, **Low**, **None**, and **Undetermined**, based on each identity's administration and access capabilities

An identity's privilege can represent direct administration access, or indirect or *shadow* access. *Shadow* administrators might have role or group permissions elevating their privilege, or otherwise possess powerful entitlements or objects potentially outside the scope of their role.

The **Detections** tab ranks the risk among linked identities according to possible severity. The **Recommendations** tab allows you to see what critical resolutions are available to mediate risk.
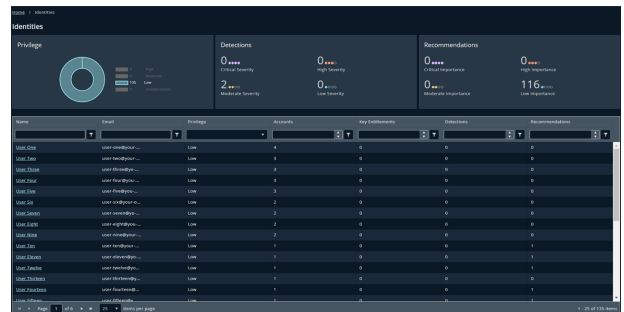
Search and Filter

The identities list allows searching and filtering based on a number of parameters, including text-based name and email searching, as well as filtering by privilege determination. Identities can also be filtered by number of associated accounts, number of entitlements, number of detections, and number of recommendations.

Searching and filter results are displayed instantly, allowing you to easily narrow down your list of identities to only those required. Columns can be shown or hidden using checkboxes by clicking the **Columns** button.
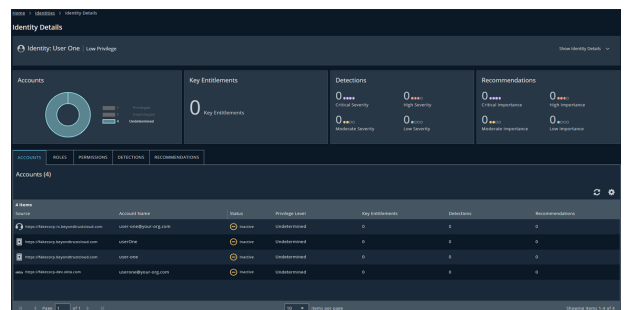
Identity Details

Clicking any user in the **Identities** dashboard displays a detailed report of that identity's accounts, roles, permissions, and more. Viewing an identity at the details level enables you to see an individual user's potential levels of access and risk and quickly assess mediation based on security recommendations.

The primary summaries display the identity's associated privileged and unprivileged accounts and key entitlements, which represent elevated permissions. Individual detections and recommendations are also available.

Accounts

The **Accounts** tab in the identity details report displays all the accounts Insights uncovers that are associated to the identity. This tab shows the account source, or connected product or service, as well as the related account name.

For each source, you can also view the account's status (active or inactive), as well as the entitlements and detections.

Roles and Permissions

The **Roles** and **Permissions** tabs allow you at-a-glance access to the identity's roles or permissions by source, enabling you to quickly identify areas of potential risk or elevated privilege.

Detections

Identity **Detections** are available to identify the individual risk assessed by Identity Security Insights. Clicking any individual detection displays detailed results, enabling you to understand both the risk and its importance or severity.
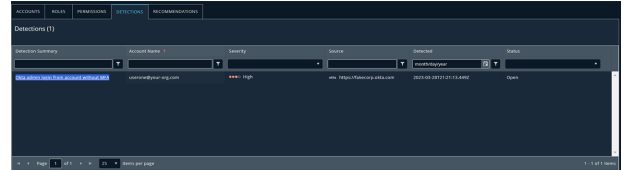
> ℹ️ *For more information, please see ["Identity Security Insights Detections Dashboard" on page 9](#).*

Recommendations

Identity **Recommendations** provide research-backed suggestions for resolving any potential risk vectors with associated accounts.

> ℹ️ *For more information, please see ["Identity Security Insights Recommendations Dashboard" on page 12](#).*

SALES: www.beyondtrust.com/contact   **SUPPORT:** www.beyondtrust.com/support   **DOCUMENTATION:** www.beyondtrust.com/docs

8

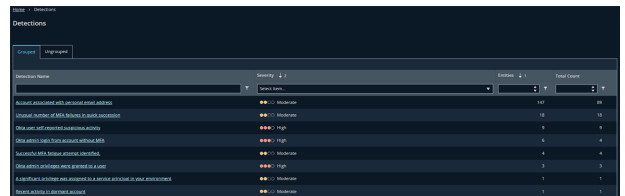# Identity Security Insights Detections Dashboard

Overview

The **Detections** page summarizes areas of potential risk or compromised entities, including suspicious login failures, missing multi-factor authentication, and stale or dormant accounts. Detections include the source system and entity type by default, allowing at-a-glance views into potentially compromised services, applications, or accounts. Detections can also be viewed in a ungrouped list by clicking the **Ungrouped** tab.

By default, new and in-progress detections are displayed in order of severity and discovery date.

Clicking any individual detection displays additional information detailing the identified risk and its importance or severity.

The detections grid can be exported as a **.csv** by clicking the download button to the right of the results.

Detection Capabilities

Identity Security Insights leverages multiple methods to detect malicious and anomalous activity.

Tactics, Techniques, and Procedures (TTP) , Indicators of Compromise (IOC), and Indicators of Attack (IOA) represent activity that is strongly associated with attackers. Identity Security Insights is updated regularly with the latest in known attack strategies to ensure you are provided a comprehensive picture of identity-related risk. TTP, IOC, and IOA detections include areas of risk, like logins without MFA, dormant account activity, and new Identity Provider enrollment. Viewing the details of any detection provides a reason for the concern, and an example of how to address the threat.

Anomaly-based detections use AI-backed methods to report on unusual and specific account activity. This activity may not represent an attack signature, but instead allows Insights to detect novel and suspicious activity outside of recognized methods of compromise. Anomaly-based detections report on risk, like infrastructure changes following suspicious MFA events, which could indicate a compromised account; changes to Azure service principals which seem unusual compared to other environments, which can indicate a breach; and excessive Secret Safe read events, which may represent suspicious access within PasswordSafe. The details for these detections describe how to determine if they are malicious.

Additional detections exist around integrated BeyondTrust products, allowing you to receive detections on anomalous activity and malicious IP access within your organization.

Sort, Filter, and Display

The **Detections** list allows searching and filtering based on a number of parameters, including text-based source, account, or detection name searching, as well as filtering by severity, detection date, and status. Search and filter results display instantly, allowing you to easily narrow down your list of detections to those desired. Columns can be shown or hidden using checkboxes by clicking the **Columns** button.

Clicking **Quick View** on any detection row displays a preview window without leaving the detections dashboard. This preview provides a high-level summary to aid in quickly evaluating areas of potential risk.

Click **View Full Details** to view additional information, or **Close** to return to your position on the dashboard.
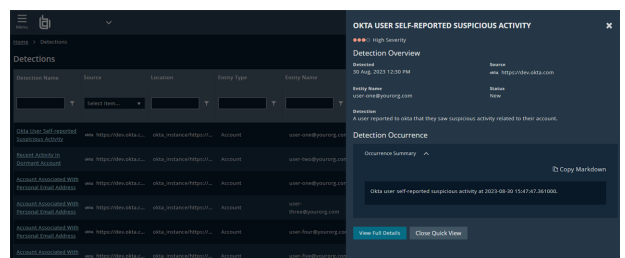
View Detection Details

Viewing **Detection Details** displays additional information regarding an individual detection. Along with viewing the severity, this dashboard provides a description of the detection, as well as an explanation of the risk and potential solutions to address the threat.

The **Entity Details** section shows any relevant entity information, such as the entity type (e.g., account), and the connected name or email. Clicking the entity name displays associated account information. Clicking the linked identity displays associated identity information.

Depending on the nature of the detection, the **Detection Details** page also displays additional key-value pairs and any associated context.
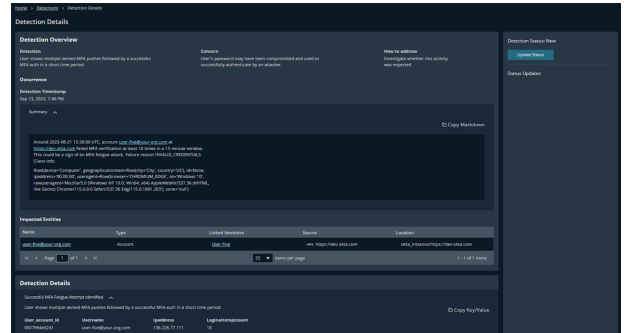
Status and Comments

The status of a detection can be changed by authorized users, and can optionally include a comment to describe the nature of the update or change. The history of status changes and comments can be viewed in the **Detection Details** dashboard at any time.

To change a status or add a comment, click **Update Status** on the right side of the detection details. Select a new status from the dropdown menu, or the same status to add a new comment. Once finished, click **Update Status** to save, or **Cancel** to discard your changes.

The detection status can be set to **New**, **In Progress**, **Resolved**, **False Positive**, or **Ignored**.

SALES: www.beyondtrust.com/contact **SUPPORT:** www.beyondtrust.com/support **DOCUMENTATION:** www.beyondtrust.com/docs

10

Identity Security Insights Entitlements Dashboard

Overview

Entitlements grant an account a higher level of access or privileged permissions. The **Entitlements** dashboard allows you to review the key entitlements associated with your organization, and evaluate whether to remove or replace them with lower privileges. Entitlements can be viewed by provider, type, amount of privileged access, and more. Discover how many accounts have access to high-level administrative privileges, and view which entitlements grant access to connected applications or permissions.

Entitlements are displayed in order of privileged access and associated accounts by default. Privilege is broken down into *Highest*, *High*, *Moderate*, *Low*, *None*, and *Undetermined*, based on each entitlement's administration and access capabilities.

Click on any entitlement summary to display a detailed list of the accounts privileged with the selected entitlement, including the source system, account name, and provider. Columns can be shown or hidden using checkboxes by clicking the **Columns** button.

Detect Entitlement-Related Risks

The entitlements page can be used to highlight unnecessary, unusual, or unused levels of privileged access.

Sorting your entitlements by **Privilege** displays the highest level of privileged permissions. Entitlements can further be organized by **Source** and **Provider** to limit the display to only detections associated with the selected system, or filtered by **Scope** to show entitlements associated with environments, groups, tenants, and more. The **Type** column can be filtered by *Role*, *Permission, App* (such as associated Identity Providers), and *Group*.

Identity Security Insights allows you to view which accounts have access to your organization's key entitlements. Evaluating entitlements detected by Insights can identify concerns like dormant account access, over-permissioned accounts, and the environments and sources to which they are provisioned.

The entitlements grid can be exported as a **CSV file** by clicking the download button to the right of the results.
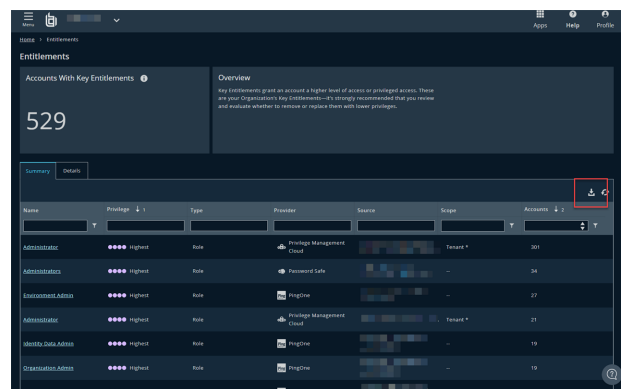
Identity Security Insights Recommendations Dashboard

Overview

The **Recommendations** dashboard displays your detections and identities by recommended solutions to potential risks. By default, the **Recommendations Overview** sorts any item by importance and impacted entities, which are then grouped by recommendation summary in a sortable list. Recommendations can also be viewed in a ungrouped list by clicking the **Ungrouped** tab.

Recommendations are generated automatically by Identity Security Insights and represent researched-backed suggestions based on security community standards.

The recommendations grid can be exported as a **.csv** by clicking the download button to the right of the results.
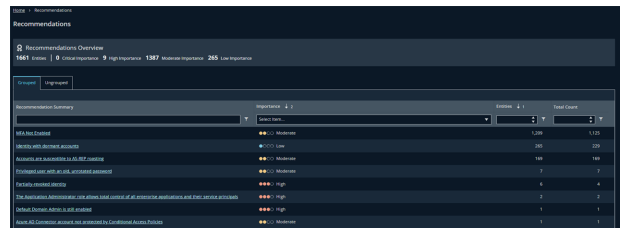
Recommendation Details

Clicking any recommendation summary in the dashboard list view displays a list of all accounts or entities that would benefit from the recommended action, such as enabling multi-factor authentication, identifying linked account privileges, or verifying dormant accounts. Accounts associated multiple times with the same recommendation across separate sources are listed as **Multiple**.

This list can be sorted by any column, including the recommendation status, source application or service, or the entity name. Columns can be shown or hidden using checkboxes by clicking the **Columns** button.
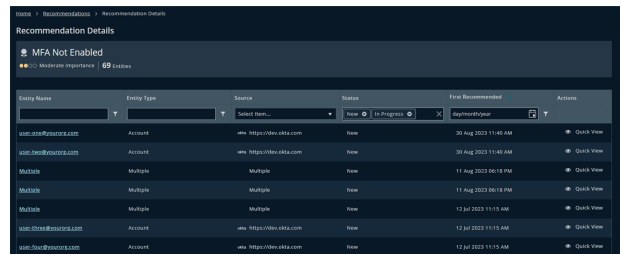
Quick View

Clicking **Quick View** on any recommendation row displays a preview window without leaving the recommendations dashboard. This preview provides a high-level summary to aid in quickly evaluating areas of potential risk.

Click **View Full Details** to view additional information, or **Close** to return to your position on the dashboard.
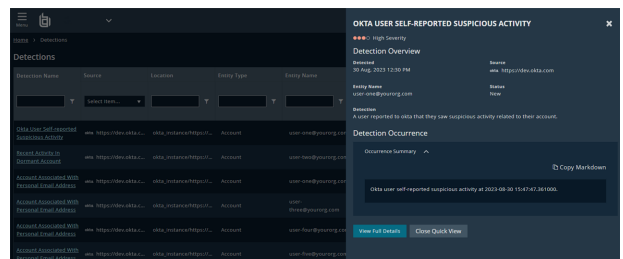
Instance Details

Clicking an entity name in the **Recommendation Details** window displays an in-depth summary for the individual recommendation instance. This page provides the detection's severity, as well as the recommendation's description and underlying concern, and potential options for resolution.

The **Entity Details** section shows any relevant entity information, such as the entity type (e.g., account), and the connected name or email. Clicking the entity name displays associated account information. Clicking the linked identity displays associated identity information.
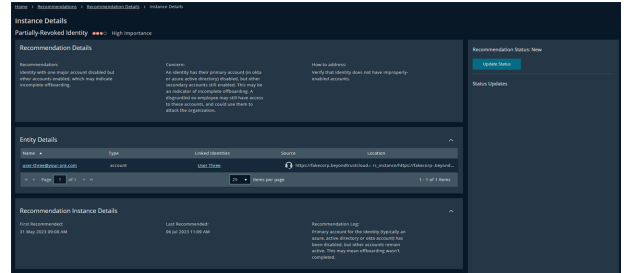
Status and Comments

The status of a recommendation can be changed by authorized users, and can optionally include a comment to describe the nature of the update or change. The history of status changes and comments can be viewed in the **Instance Details** dashboard at any time.

To change a status or add a comment, click **Update Status** on the right side of the detection details. Select a new status from the dropdown menu, or the same status to add a new comment. Once finished, click **Update Status** to save, or click **Cancel** to discard your changes.

The recommendation status can be set to **New**, **In Progress**, **Resolved**, **False Positive**, or **Ignored**.

Manage Exclusion Rules

To exclude specific results from appearing in a tenant's detections or recommendations, Identity Security Insights allows the creation of **exclusion rules,** which can be defined to fine-tune the results displayed in your dashboards.

To add or manage exclusion rules, click the **Menu** button in your navigation bar, and click **Exclusion Rules**. If any exclusion rules exist, a list displays an overview of the rule's name and description.
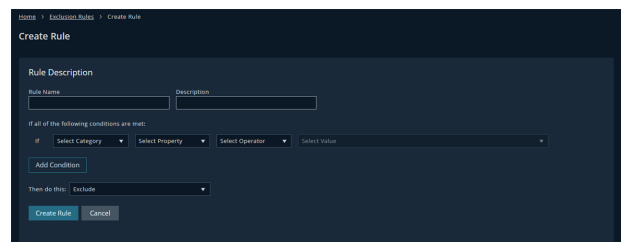
Existing rules can be edited by clicking the rule's **Name**, and deleted by clicking the ellipses to the right of the rule and selecting **Delete**.

Add a New Exclusion Rule

Click **Create Rule** to add a new exclusion rule, and provide the rule a user-friendly **Name** and **Description**.

Under **If all of the following conditions are met:**, select **detection** from the **Category** dropdown, and select values for the following:

- The **Property** dropdown allows you to select which property of the detection (e.g., name) you would like to filter on.
- The **Operator** dropdown determines the relationship of the property to the value (e.g. **is** or **is not**).
- The **Value** dropdown allows you to select the specific detection or recommendation to filter on.

For example, a condition with the property **Name**, the operator **Is**, and the value **Account associated with personal email** will exclude personal email detections from your dashboards.

Click **Create Rule** to save the rule to your tenant. The rule will immediately apply.

Filter by Account or Identity

Exclusion rules can be further filtered by specific account or identity matches. Adding this condition will apply the rule to only the matching account or identity.

Click **Add Condition** to add a second condition to your exclusion rule, and select values for the following:

- The **Category** dropdown allows you to select between filtering on an **account** or an **identity**.
- The **Property** dropdown allows you to select which property of the category (i.e., name) you would like to filter on.
- The **Operator** dropdown determines the relationship of the property to the value (i.e. **is** or **is not**).
- The **Value** dropdown allows you to select the specific detection to filter on.

For example, a condition with the category **Account**, the property **Name**, the operator **Is**, and the value of an email address will only apply the exclusion rule to the provided email.

Click **Create Rule** to save the rule to your tenant. The rule will immediately apply.

> 📌 **Note:** *An account or identity condition can only be added as a second condition to an exclusion rule.*