Cisco Identity Applications

Applications

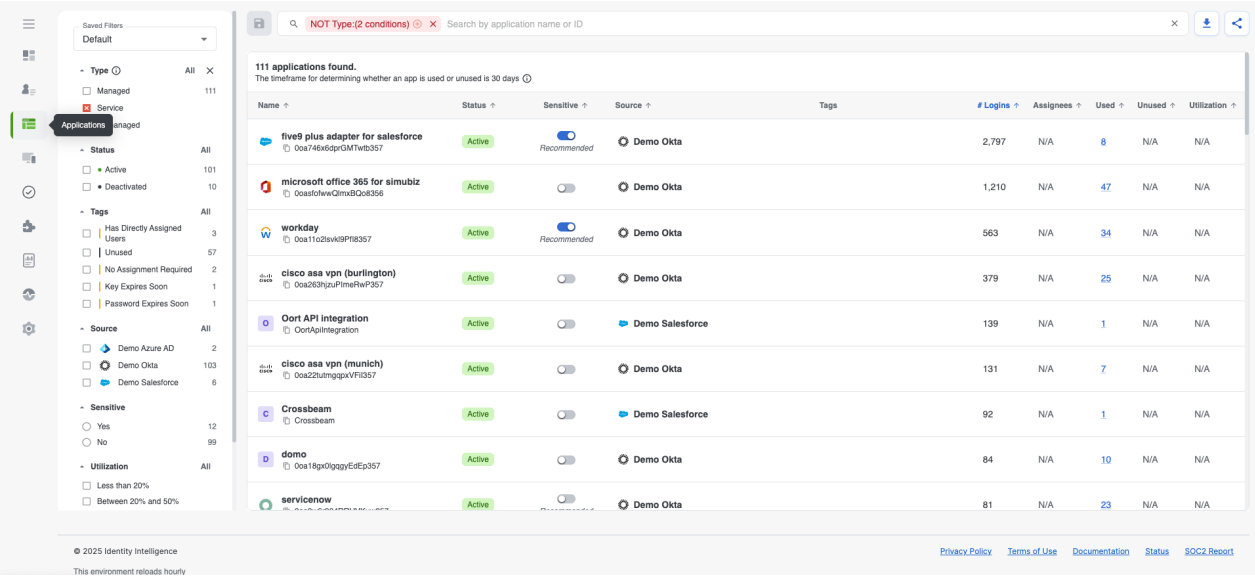
Organizations often have hundreds, or even thousands, of applications connected to their Identity Providers and available to their users; however, understanding what is in their environment, how it gets used, and who it gets used by is a challenging question for many organizations to answer because their applications are sprawled across multiple identity providers (IdPs). When it comes to reporting to answer licensing questions, or compliance and audit purposes, organizations spend countless hours trying to collect the information they can from each system, often painstakingly correlating data across spreadsheets manually, just to answer these simple questions as best they can – and the results often leave much to be desired.

The **Applications** page of Cisco Identity aims to ease the burden that comes with this sprawling data across disparate systems with a unified view into your organization's applications. Much like the Users page, which provides visibility into an organization's identities across the connected identity sources, the Applications page gives organizations cross-platform visibility into the different applications that exist within their ecosystem.

With this consolidated view, it is significantly faster and easier for organizations to get visibility into their app landscape, answer questions, create reports, and ultimately, take action on the applications within their environment to reduce the possible attack surface and improve their overall organizational security.

This article provides information about the different data and functionality that exists in the Applications page such as:

- Definitions of the elements in the table
- Diving deeper into an app
- Customizing the Applications page with sensitive apps and application utilization timeframes
- General functionality such as searching, exporting results, sharing, etc
- Filtering



Applications table elements

By default, the Applications table is sorted by the largest number of logins and only includes `managed` apps, which are apps that are managed by an identity source.

The total number of Applications in the table is displayed above the column headers of the table itself.

The section below details the fields that appear in the table, as well as the definition of each field:

Element	Description
Name	The name given to the app and the assigned app ID from the identity source
Status	The current state of an app such as `active`, `deleted`, `deprovisioned`, etc
Sensitive	Applications that have been flagged as sensitive for your organization will have an enabled (blue) toggle. Applications that are not marked as sensitive will have a disabled (grey) toggle. Learn more about how to configure sensitive apps and why it is important.



Recommended



Source	The identity source where a given application is connected
Tags	Cisco Identity will apply tags to an application if it matches certain criteria, such as `Key Expires Soon` , `Password Expires Soon` or `No Assignment Required`, to highlight applications that may require action or clean up. If you hover over a tag regarding a password or key expiration, a tool tip with more information will appear. An application can have more than one tag applied to it. All the tags present in your environment are displayed in the relevant Tags filter
#Logins	The number of successful sign in events for a given application across all users in your environment
Assignees	The number of users who are assigned, or entitled to access a given application. Select the value in this column to go to the Users page, pre-filtered for the given app and its assigned users so that you can filter or investigate further, export the impacted users, etc. If this column

	displays N/A for a given application it can indicate that there is no assignment required to access the application or that the data is not available from the source
Used	The number of users who have successfully signed in to a given application during the configured application utilization timeframe. Select the value in this column to go to the Users page, pre-filtered for the given app and the users who accessed the app, so that you can filter or investigate further, export the impacted users, etc. By default, the utilization timeframe is set to 30 days but this can be modified if needed. Learn more about how to configure the utilization timeframe
Unused	The number of users who have no successful sign in events to a given application during the configured application utilization timeframe. Select the value in this column to go to the Users page, pre-filtered for the given app and the users who have not accessed the app, so that you can filter or investigate further, export the impacted users, etc. By default, the utilization timeframe is set to 30 days but this can be modified if needed. Learn more about how to configure the utilization timeframe
Utilization	The percentage of users who have successfully signed in during the configured application utilization timeframe out of the total number of assigned users for a given application. If this column displays N/A for a given application it can be because there are no assigned users. This column will also display 100% if there are more users utilizing the application, than users assigned to the application. By default, the utilization timeframe is set to 30 days but this can be modified if needed. Learn more about how to configure the utilization timeframe

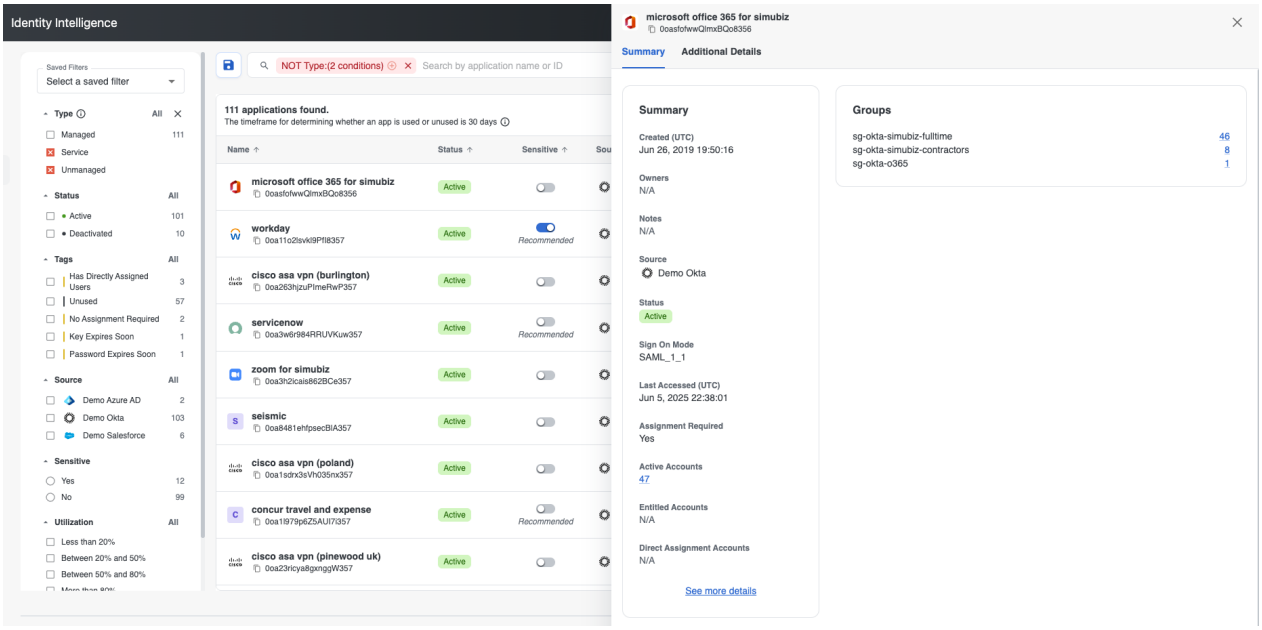
Diving deeper into an app

Like many pages within Cisco Identity, such as the User 360 pages, selecting the name of an application, or anywhere in the row that is not a link, will open the slide panel from the right side of the page that contains more detailed information about a particular app.

The slide panel has 2 tabs - Summary and Additional Details.

- Summary shows you more detailed information about a given app such as created date, sign on mode, App Owners or Notes if available, as well as the Groups assigned to the app and the number of users associated with that group
- Select the value associated with a given group to go to the Users page pre-filtered on that group
- Additional Details shows you the raw data collected about a given application from the source. The data available will vary from source to source, and even application to application.

To close the slide panel, select the **X** in the top right corner, or select anywhere outside of slide panel.



Customizing the Applications page

Adding Sensitive Applications

The importance of configuring sensitive applications

Cisco Identity has the concept of **Sensitive Applications** to help customers indicate which applications are most important to their organization. Applications that are closely monitored because they have access to sensitive data, are critical to business operations, require regular audits, have high license costs, or any other similar reasons, are all good examples of applications that should be treated as sensitive.

It is critical that your organization's most critical and sensitive apps are flagged appropriately as this information is used in various ways throughout Cisco Identity such as in Dashboard widgets, as a contributing factor of the User Trust Level calculation, as a tag in the Activity tab of the User 360, as check settings, and more. If your list of sensitive apps.

Having these applications marked accordingly allows Cisco Identity to provide you with more accurate results and data, and allows you to easily identify your organization's sensitive apps so that you can more easily prioritize and focus on the most important applications when cleaning up or investigating issues.

Sensitive Application Auto-Discovery Mode

Cisco Identity automatically configures sensitive apps for all newly created tenants using its list of “Recommended” sensitive applications, also known as **Auto-Discovery Mode**. These recommendations are based on apps that are known to typically host sensitive data or are commonly considered sensitive in customer environments. If new apps are added to your environment that match Cisco Identity's list of recommendations, it will automatically be marked as sensitive.

If your organization does not maintain a list of critical apps, we suggest keeping auto-discovery mode enabled to keep the default list of sensitive applications configured.

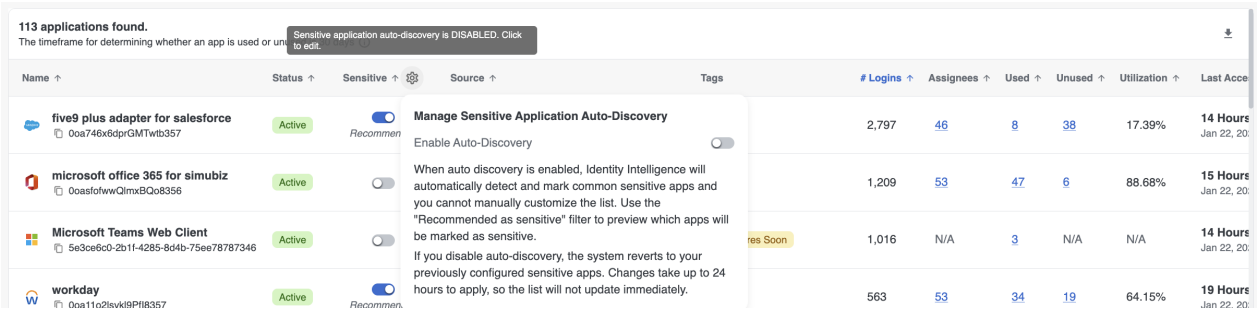
However, we know that every organization is different. What may be a sensitive application to one organization may not be to another organization. Some organizations may have stricter regulations that govern revoking unused application access, while other organizations may be more lenient. Which is why Cisco Identity allows customers the flexibility to customize certain aspects of their Applications view to better align with their organization's policies, processes and risk tolerance thresholds.

Customizing Sensitive Apps

If your organization maintains a list of critical applications, which is often needed for compliance and audit purposes, it is highly recommended that you customize your Cisco Identity tenant to reflect that list of apps.

To set your own list of customized sensitive applications:

1. Disable the default sensitive apps list by selecting the **cog icon** that is directly to the right of the “**Sensitive**“ column header and toggling **off auto-discovery mode** Note: you cannot have default list/auto-discovery mode enabled AND also select custom apps.



2. After you have disabled auto-discovery mode, you can flag applications as sensitive using the **toggle** in the Sensitive column as mentioned in the Applications table elements section of this article

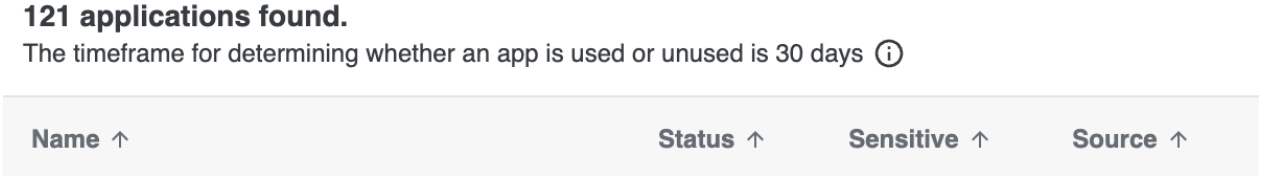




Customizing the application utilization timeframe

As described above in the Applications table elements section of this article, the default timeframe utilized to determine whether an application is used or unused is 30 days. If you would like to adjust the default application utilization timeframe to be longer or shorter, you can do so via the Custom Detection Settings within the **Unused App by Many Users** check.

The text above the Application table column headers will reflect the timeframe setting that is configured on the check.



Applications page general functionality

There are several general actions that exist across the Cisco Identity platform that are also available on the Applications page:

- Search
- Sort columns
- Download results

- Share

Search

Use the search bar to search based on application name or ID, source, or status. When searching, you do not need to provide an exact value. Typing a piece of the word will return related results.

If you have searched on a particular parameter, the search criteria is retained as you navigate between different tabs within the platform.

To clear the search bar, select the **X** on the right most side of the search bar.

Sort columns

Sort columns within the table by selecting the column header you'd like to sort by. Click once to sort in ascending order, select again to sort in descending order.

Multi-column sorting is **not** currently supported.

Download results

You can download tabular data from the table to a CSV using the **Download** icon button on the right after the search bar. All columns displayed and filters applied are included in the CSV output.

If there are no results in the table, the CSV export will contain only headers and no app data.

Share

The **Share** button (on the right of the search bar) copies a link, with the applied filters, that can be easily pasted, bookmarked or shared with anyone who has the appropriate access to your Cisco Identity tenant.

Filters

Much like the Users table, the Applications table is filterable by a number of attributes, enabling you to slice and dice your apps based on the parameters that are important to you.

Filtered results can be saved to access later or share with teammates.

Note: The Apps page currently only supports **Basic** filters and does not have Advanced Query mode available

Applying filters

You can see all the available filters on the left hand side of the Applications page. To enable additional filters, select the value(s) for the attribute you would like to filter by. The applied

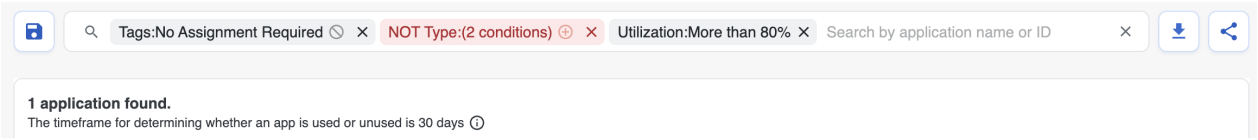
filters will be added to the search bar, as seen in the screenshot below.

The number of apps that you are currently viewing, based on the filters and searches used, will appear in the top left corner of the Apps table above the column headers.

To remove a filter, you can either deselect the attribute from the filters list on left hand side of the Applications table, or select the **X** on the right hand side of the filter box within the search bar. If you select the **X** on the right end of the Search bar, it will remove all filters and search inputs except for the default `Type` filter.

As mentioned above, the Applications table is pre-filtered by default to only include `managed` apps, which are apps that are managed by an identity source. If you want to remove this filter and include the other app types - `unmanaged` apps (appear in SSO events, but are not managed by the provider) or `service` apps (not directly managed by provider by used to access others apps) - you can do so in the same way as the other filters.

After you have selected your filters, the filters are retained as you navigate between different areas within the platform.



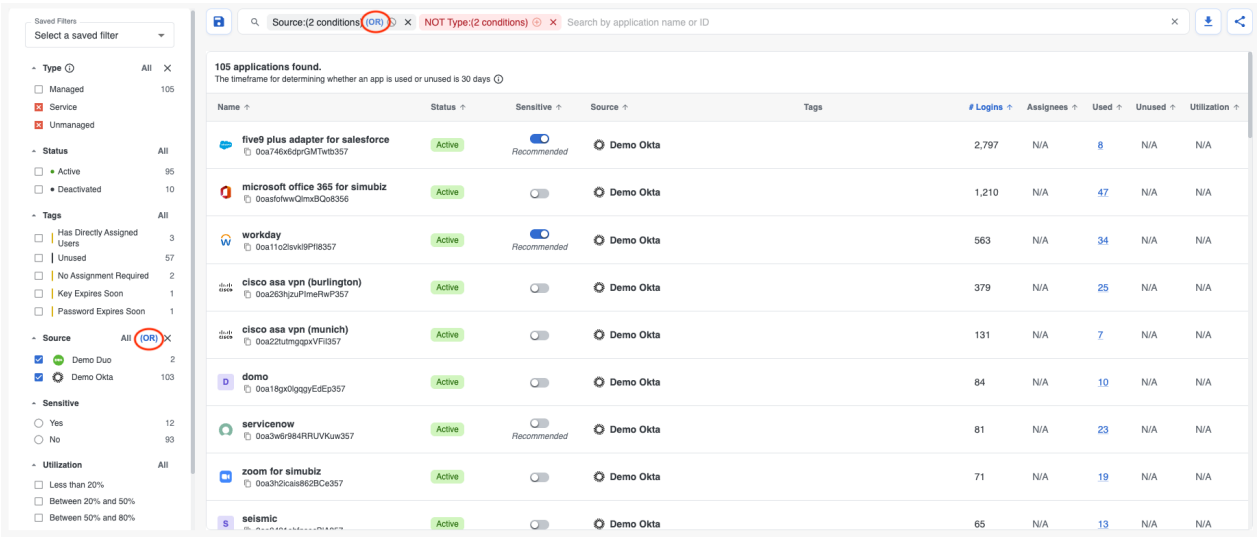
Filter interactions

Distinct filters are separated by an **AND** operator. For example, if you select the `Duo` value from the `Sources` filter and the `Yes` value for the `Sensitive` filter, the table will display all `Duo` apps that are flagged as `Sensitive`.

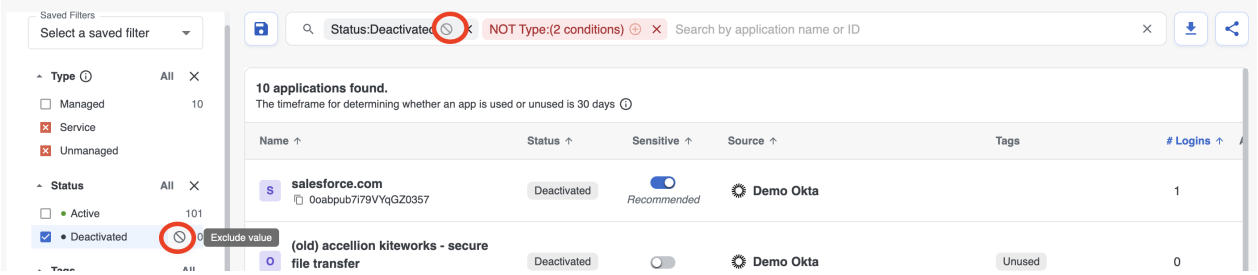
For most filters, you can select more than one value to filter by. Within a given filter, selecting more than one value will separate the values with an **OR** operator by default. For example, if you select the values `Okta` and `Duo` for the `Sources` filter, apps coming from **either** `Okta` **OR** `Duo` will be displayed.

However, if you would like to filter for apps in both `Okta` **AND** `Duo`, you can select the **OR** operator found in the filter box within the search bar or in the left hand filter menu (screenshots below), to switch it to **AND**. Doing this will allow you to see users that are in both `Okta` **AND** `Duo`.

Filters that use radio buttons **cannot** have more than one value selected at once (for ex: `Sensitive`)



Specific values can also be excluded from the results for most filters, except for those that cannot have more than one value selected at once. To exclude a value from filtered results (ie: `NOT`), you can click on the icon in either the filter box in the search bar or the left hand filter menu.



Similarly, you can 'include all' values in the results, except for filters that cannot have more than one value selected at once. To select all values within a given filter, click `All` next to the filter value title.

