Cisco Identity Non-Human Identities (NHI)

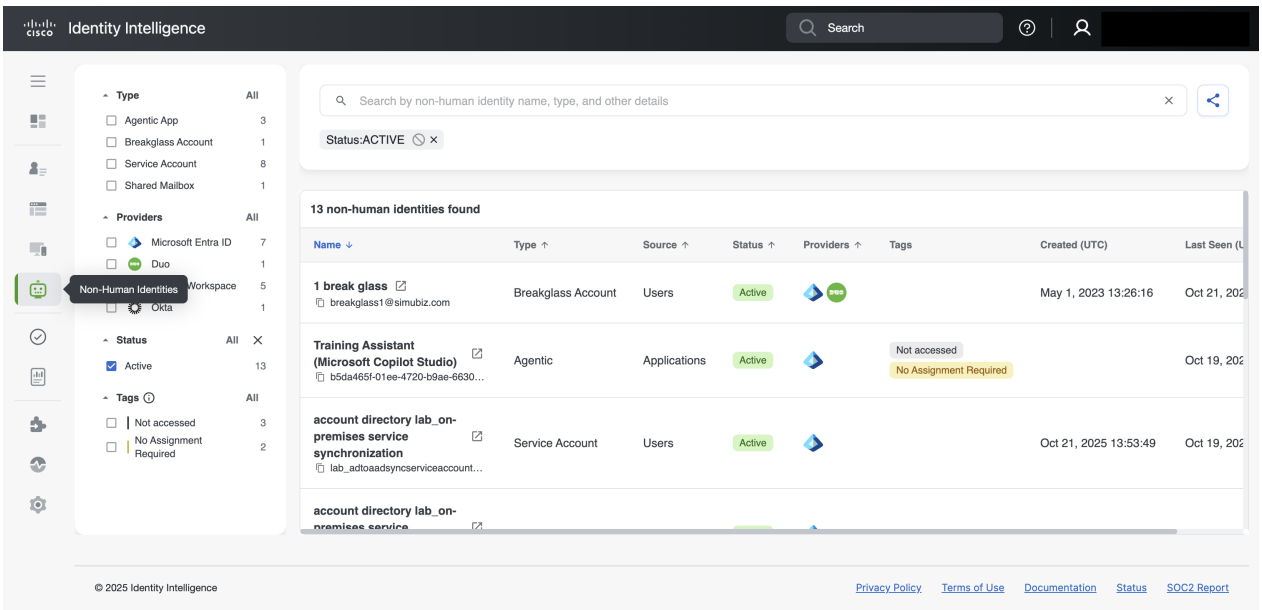
Non-Human Identities (NHI)

Overview

Non-Human Identities (NHI) are accounts or entities within a business that aren't linked to a specific person but are important for tasks like automation, services, or device operations. Examples include service accounts, shared mailboxes, network devices, and other machine identities that help run applications or provide access to different services.

In many organizations, machine identities make up a large part of all digital identities, about 43% on average. Service accounts, a common type of machine identity, are usually set up to help certain applications or services function smoothly. Because these accounts often have higher levels of access and can reach sensitive information, they are a common target for attackers. To keep these accounts secure, it's important to assign clear ownership, ideally tying each account to one or more people. This ensures that someone is always responsible for the account, even if team members change.

When organizations have a single, organized view of all their Non-Human Identities, it becomes much easier and quicker to see what exists, answer questions, and take necessary actions. This helps reduce security risks and strengthens overall protection. This article explains the types of data and features available on the Non-Human Identities page.



The left-hand navigation panel lets you filter and organize non-human identities by different attributes. This makes it easier to see detailed information and gain a better understanding of the identities in the system.

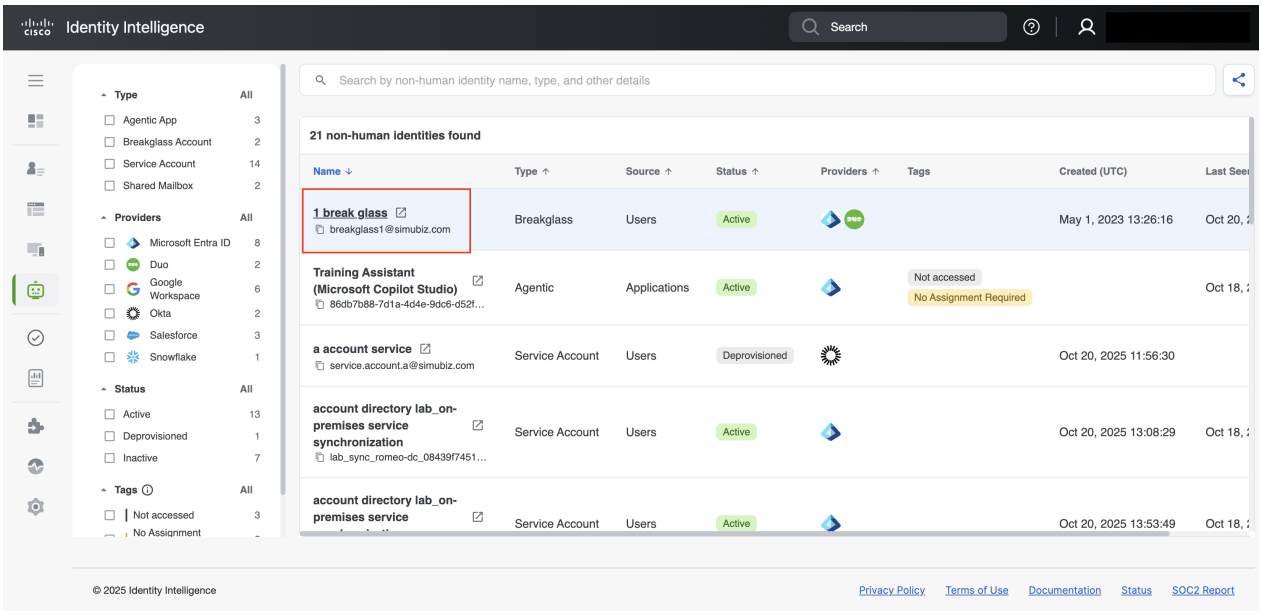
NHI table elements

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

Field	Description
Name	The name or ID given to a non-human identity
Type	The functional category of the identity such as service account, breakglass, Agentic
Source	The identity source where a given NHI is connected.
Status	The current state of an app such as active, inactive, deprovisioned, etc
Providers	The logo icon(s) for the corresponding identity data sources where a user's account has been associated.
Tags	Cisco Identity will apply tags to non-human identities 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. NHI can have more than one tag applied to it. All the tags present in your environment are displayed in the relevant Tags filter
Created	The date and time when the non-human identity was initially created
Last Seen	The date and time of the last login attempt, regardless of outcome, for a non-human identity across all providers

Diving Deeper into NHI

Like many pages within Cisco Identity, such as the User 360 and Applications pages, clicking on the name of a non-human identity in the table will take you to a dedicated NHI 360 page with more detailed information about that specific NHI.

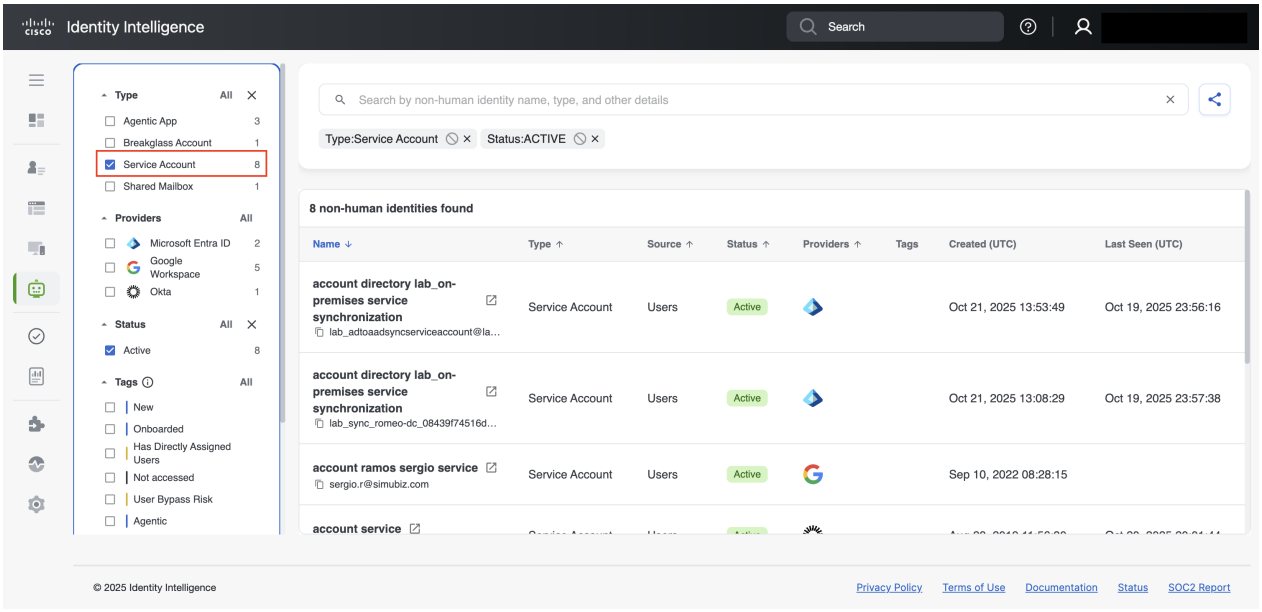


Filters

Similar to the Users and Applications tables, the Non-Human Identities table can be filtered by various attributes, allowing you to view NHIs based on the criteria that matter most to you. You can also save your filtered results for future use or share them with your team.

Applying Filters

All available filters are listed on the left side of the Non-Human Identities page. To add more filters, simply choose the values for the attributes you want to use. Once applied, these filters will appear in the search bar, as shown in the screenshot below.



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

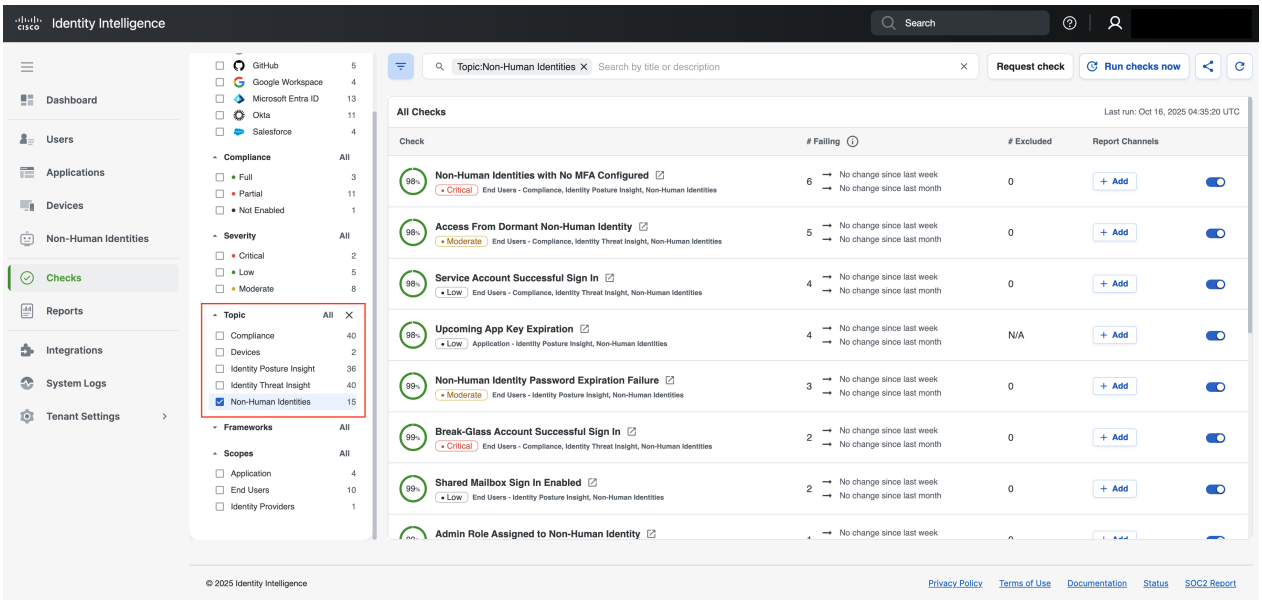
To remove a filter, you can either deselect the attribute from the filters list on left hand side of the Non-Human Identities table or select the X on the right-hand side of the filter box within the search bar. If you select the X on the right end of the Search bar, it will remove all filters and search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

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

Non-Human Identities (NHI) Checks

The Checks page provides high-level information about all checks across all identities in your environment, along with several filters, to quickly understand the state of your environment and assess potential areas in need of attention. The Checks page shows the full list of checks that are compatible with the identity data sources that are connected to your tenant. The checks in the table are ordered by compliance, from lowest to highest compliance, starting with the checks that have the most users failing. Checks that are in full compliance can be found at the bottom of the list.

To access a specific check related to Non-Human Identities, select the Non-Human Identities topic to view all checks related to NHIs.



The full list of available checks can be found in the Understanding Check Failures documentation. Read more about the information presented and actions available on the Check Results page in the Reviewing Check Results documentation.

NHI 360

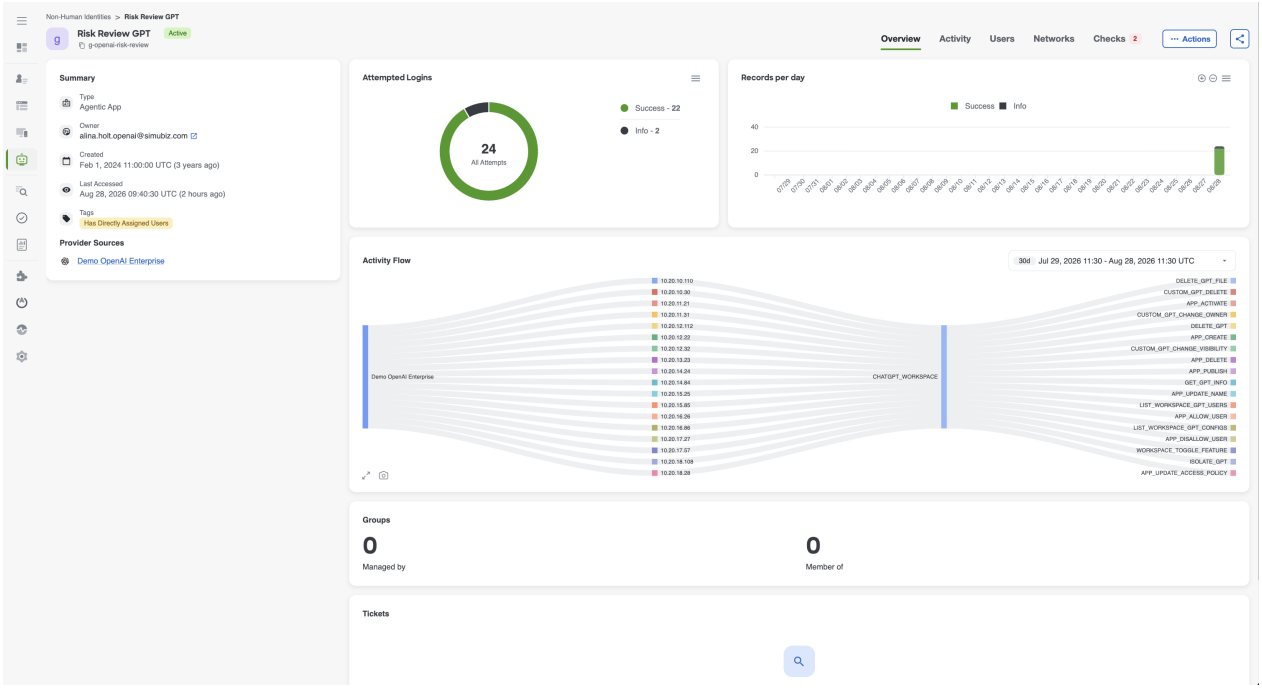
With Cisco Identity's NHI 360 View, you get rich insight into each non-human identity (NHI) in your environment – service accounts, API keys, bots, and other machine identities that access your systems without a human directly behind them. Like the User 360, the NHI 360 profile

consolidates an identity's entitlement data, credentials, and activity across sources into a single view for a given non-human identity, enabling you to easily and quickly gather context on a particular NHI.

To get to an NHI 360, select a specific identity's name from the Non-Human Identities page, or from anywhere in the platform where you see an NHI in a blue hyperlink, such as the failing entities on a specific Check page. To open the NHI 360 in a new tab, use the grey button next to the user's email.

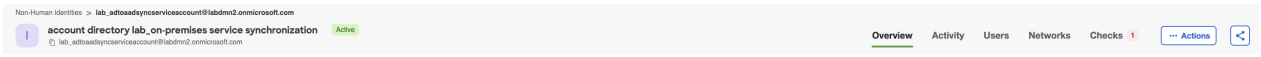
The NHI 360 is broken down into multiple tabs. To learn more about what information and functionality is available in each tab, see the sections below:

- Overview tab
- Activity tab
- Users tab
- Networks tab
- Checks tab



Some information and functionality persists across all tabs of the NHI 360:

- **Identity name** - Top left corner
- **Login/ID** - Top left corner, under the identity name
- **Status** - Tag next to the identity name (**Active**, **Inactive**, **Deleted**, **Deprovisioned**, or **Unknown**)
- **Checks** tab - Shows a count of currently failing checks next to the tab name



Functionality that persists across all tabs:

- **Actions** button – Provides available remediation actions for an identity. Available actions will vary depending on what sources a particular NHI has accounts with. For more info about remediation actions, refer to the Remediation and Triage documentation.
- If no actions are available given your tenant configuration, the button is disabled with an explanatory tooltip
- **Share** button – Copies a link to the exact page you're on, so it can be pasted, bookmarked, or shared with anyone who has appropriate access to your Cisco Identity tenant

Overview Tab

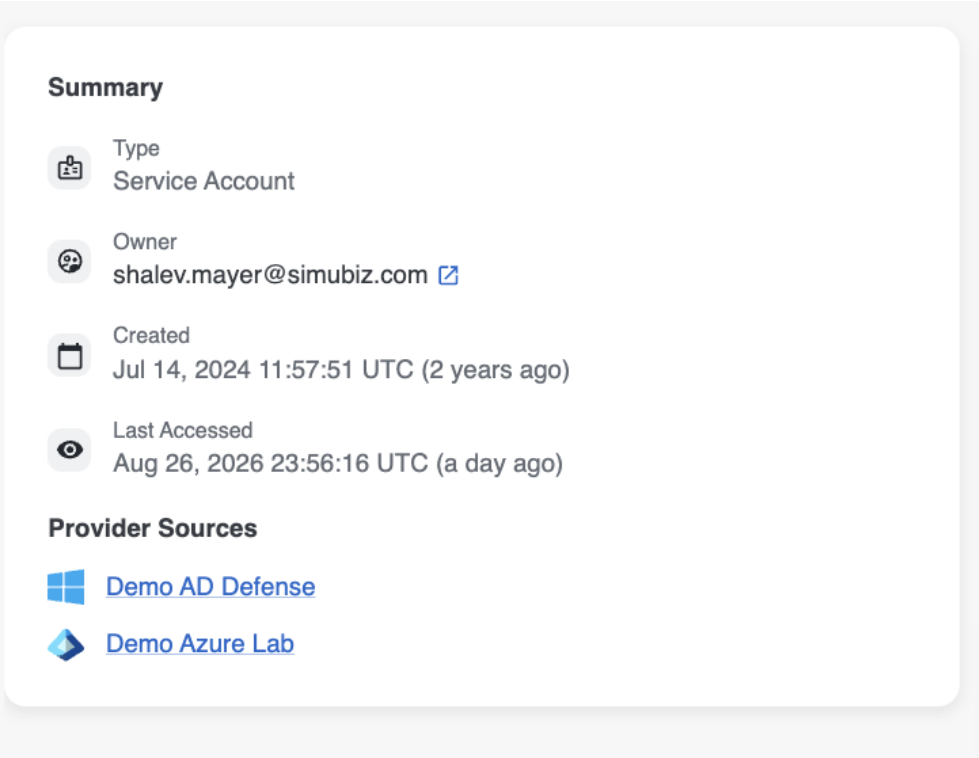
The purpose of the Overview tab is to provide high-level context on what a non-human identity is and how it's used. The Overview tab is the first tab of the NHI 360, and is where you will automatically land upon selecting an identity from the Non-Human Identities listing page.

Summary

The Summary widget displays high-level context about the identity, including:

Field	Description
Type	The type of non-human identity (e.g.: Service Account, Service Secret, API Key, Mailbox, MCP, etc.)
Owner	The owner(s) associated with the NHI, if available
Created	The date the identity was created, and how long ago that was
Created By	Who created the identity. Note: Only shown for Service Secret-type identities
Last Accessed	The last time the NHI was used
Tags	Cisco Identity generated tags associated with the NHI, if any are present
Additional Information	A count of additional attributes available for the identity, with a **View All** link that opens a side panel with the full list

If detailed provider source information isn't available for a given integration, the Summary widget will show “Source not available” for that source, with a tooltip explaining that NHI source details are unavailable for that integration.



Login Attempt visualizations

Attempted Logins

A pie chart breaking down the login attempts by result (success, failure, etc) for the NHI. This visualization is based on the NHI's history since the user has been monitored by Cisco Identity (i.e.: all time)

To export this visualization to a PNG, SVG, or get the raw data in a CSV, select the 3-line button in the top right corner of the widget.

Records per day

A bar graph visualization breaking down the login attempt activity per day, by result. By default, this timeline visualization looks across 30 days of activity. However, to see the same data over a smaller or larger timeframe, you can press the **+** or **-** buttons in the top right corner of the widget.

If the user is **Inactive,** this widget will still be visible but blank with a message stating “No records found" .

To export this visualization to a PNG, SVG, or get the raw data in a CSV, select the 3-line button in the top right corner of the widget.

Activity Flow

Provides a visual representation of a given NHI's activity, similar in purpose to the Activity Flow visualization on the User 360 Overview tab, so you can quickly spot patterns or anomalies at a glance. The Activity Flow includes data regarding locations, applications

accessed, and related events.

The activity flow widget defaults to showing activity over a 30 day window; however, this can be customized as needed using the date picker in the top right corner of the widget. If you would like to full screen the flow, press the **Expand** icon in the bottom left corner of the widget. To save a PNG of the flow, select on the **Camera** icon in the bottom left corner of the widget, next to the Expand icon.

Selecting any of the colored bars within the visualization will take you to the NHI's Activity tab, pre-filtered on all events associated with your selection.

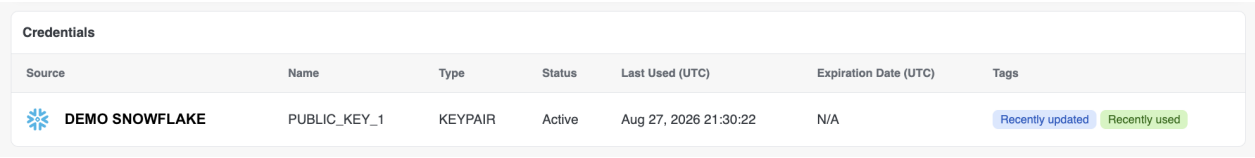
If the NHI is **Inactive,** this widget will still be visible but blank with a message stating “No records found" .



Credentials

If the NHI has any associated credentials, like secrets or tokens, a Credentials table is shown with the following columns: **Source, Name** of the credential, **Type** of credential, **Status, Last Used, Expiration,** and **Tags** assigned by Cisco Identity.

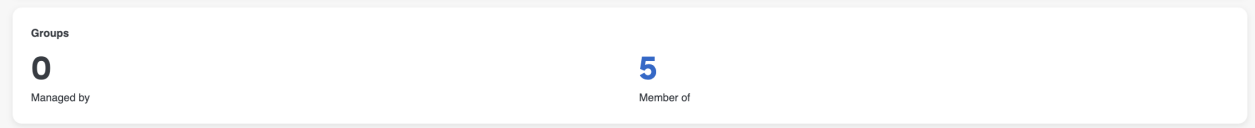
This widget is not shown if the NHI has no associated credentials.



Groups

The Groups widget shows two counts for the NHI:

- **Managed by** - Number of groups that manage this identity
- **Member of** - Number of groups this NHI is a member of



Tickets

If you have a ticketing service integration set up, tickets opened for this identity (via the **Actions** button) appear in a table here. If there are no tickets associated with the identity, or no ticketing integration is configured, this widget will still be visible, but blank, with a message stating “No tickets found" .

Note: If you do not have a ticketing service integration set up, you will not see this widget.

Below are the fields visible in the table once a ticket is created:

Name

NHI's name + name given to a ticket when it was opened (ex. John Smith: Ticket Test)

State

Ticket's state as set in the Ticketing System

Priority

Ticket's priority as set in the Ticketing System

Urgency

Ticket's urgency as set in the Ticketing System

Ticket Opened (UTC)

The date and time the ticket was created

Last Updated (UTC)

The date and time the ticket was most recently updated

Activity Tab

The Activity tab's purpose is to show a detailed view of all activity, across all sources, associated with a given non-human identity over time. It works the same way as the Activity tab on the User 360 - the underlying table, filters, and drill-down behavior are shared between the two.

Activity table elements

Date

The date and time the event/action happened. Hover over the timestamp to see the event time in your local time based on your device settings.

Source

The identity source associated with the event/action

Event

What the event/action was

Initiator

Who or what initiated the event/action, and a session ID for the event if available from the source

Target

The target of the event/action taken

Result

The result of the event/action taken

Geo/IP

The IP address and associated location for the event/action

Tags

Tags associated with the event and/or IP address. Hover over each tag to see a tooltip with the source of the tag (ex: Okta: Password Spray, IP info: Hosting, etc). If no source, it is an Cisco Identity tag (ex: New ISP)

OS

The operating system associated with the event/action. Hover over the icon in this column to see a tooltip with the OS name.

Browser

The browser associated with the event/action. Hover over the icon in this column to see a tooltip with the browser name.

Device Type

The device type associated with the event/action

If there is no activity for the identity, the table shows an empty state: “No activity logs found.”

Diving deeper into an event

Selecting the blank space in a given row within the Activity Tab opens a slide panel with two tabs, **Key Attributes** and **Raw Data,** showing detailed and raw information about the selected event, respectively.

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



General actions on the Activity Tab

- **Search** - Use the search bar above the table to search by things like IP address, session ID, application name, source, location, etc. Use the icons on the left hand side of the search bar to switch between basic, advanced and AI Search modes
- **Adjust timeframe** - Use the period picker to the right of the Search bar to change the window of activity shown. By default, the Activity tab is filtered to display all events over the last 30 days, but this can be adjusted to see a larger or smaller window as needed
- **Filters** - Use the filter sidebar to narrow results, or reset all filters with **Reset filters**
- **Download results** - Export the table's current results to CSV
- **Refresh** - Refresh the table's data

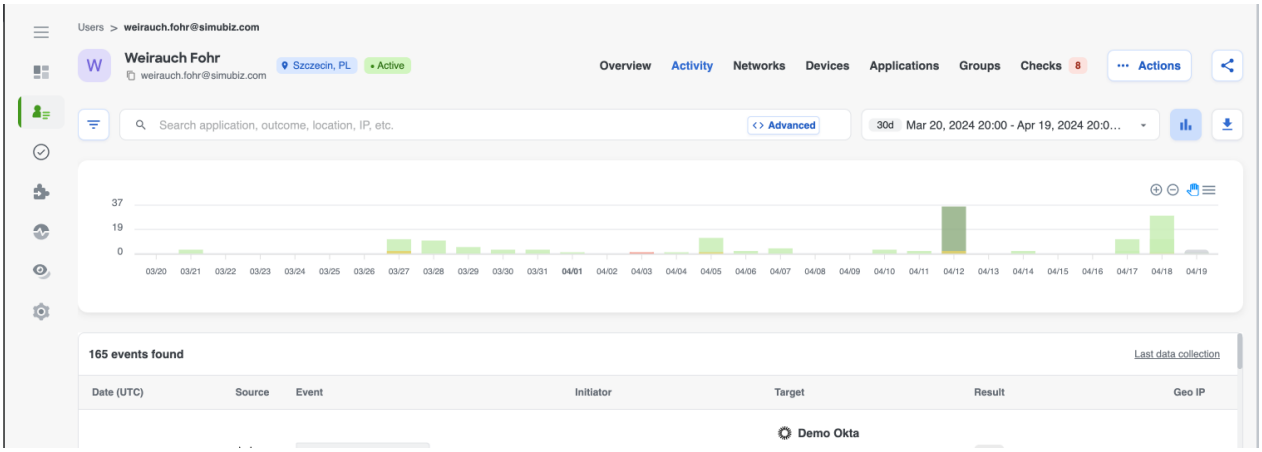
Timeline visualization

The Activity tab has a timeline widget which displays a given NHI's total number of events per day, color coded by result type (ie: success, failure, challenge, etc). Hovering over a segment of the bar will display a tooltip with the date, the result, and the count of events for that result.

By default, the view is set for 30 days but this can be adjusted to see a wider or smaller window of time using the **+** and **-** buttons in the top right corner of the timeline widget.

To export this visualization, press on the 3-line button in the top right corner of the widget. Downloading as a SVG or PNG will export an image, whereas downloading as a CSV will export the raw data for you in CSV format.

If you would like to hide this widget to get more space for the Activity table, press the **Graph** icon button next to the timeframe filter. To get the widget back, press the **Graph** icon button again.



Users Tab

The Users tab shows which human users have interacted with the non-human identity, so you can understand who is using or managing it.

Users table elements

User

The user's name/login

Activity Count

The number of activity events for that user with this non-human identity

Latest Event (UTC)

The date and time of that user's most recent activity with this non-human identity

The table title reflects the total count of users found (for example, “3 users found"), and by default reflects activity over the last 30 days. You can search by user name or login. If there is no user activity for the identity, the table shows an empty state: “No users found.”

Networks Tab

Within the NHI 360 profile, the Networks tab provides context on IP addresses associated with the identity. This tab works the same way as the Networks tab on the User 360 - the underlying table and drill-down behavior are shared between the two.

Networks table elements

IP Address

The IP address

Last Access (UTC)

The date and time the IP address was last seen. Hover over the timestamp to see the event time in your local time based on your device settings.

Hit Count

The number of events associated with this identity and the IP address, regardless of result

Successful Events

The number of successful events associated with this identity and the IP address

Failed Events

The number of failed events associated with this identity and the IP address

Other Events

The number of other events (neither success nor failure)

Tags

Tags associated with the IP address

Location

The location associated with the IP address

Source

The identity source(s) associated with activity from the IP address

Carrier

The carrier associated with the IP address

Same IP Users

The number of other identities in your environment associated with the IP address

The table title reflects the total count of IP addresses found for the selected timeframe.

Diving deeper into an IP address

Selecting the blank space in a given row opens a slide panel titled “IP: {ip address}” with two sections:

- **IP Data** – A summary of information available about the IP address, including ASN details
- **IP Activity** – The identity's associated activity types and applications accessed from that IP address, with counts and results

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

Pivoting on IP Address

A key feature of the Networks tab is the ability to drill down into the detailed activity for the current NHI. The actions menu will pop up when left-clicking on a specific IP address in the Networks table. The actions are:

- **Find identity activity** – Adds the selected IP address as a filter on the given NHI's Activity tab so you can see all the NHI's activity associated with this particular IP address
- **Copy to clipboard** – Copies the IP address to your clipboard so that you can paste it within Cisco Identity or another tool

General actions on the Networks tab

- **Search** – Search by IP address, location, carrier, or tags
- **Adjust timeframe** – Use the period picker to change the window shown
- **Sorting columns** – To sort by a specific column value, select the arrow next to the column header to switch between ascending and descending order. If there is no arrow available, it means this column cannot be sorted. By default, the Networks tab is sorted in

descending order (highest to lowest) on Hit Count

- **Download results** - Export the table's current results to CSV

Checks Tab

The Checks tab shows a detailed view of all of a non-human identity's current check failures and check history, similar to the Checks tab on the User 360.

On the Checks tab, there can be 2 different tables - the first table displays the checks that a given NHI is currently failing. The second table shows the given NHI's resolved checks, which are checks that the user is no longer failing. If the user does not have any resolved checks you will only see the Failing Checks table. If the user is not currently failing any checks, you will only see the Resolved Checks table.

Below, we will explain the fields that appear in each table, as well as the definition of each field.

Failing Checks

Name

The name of the failed check

Result

Failed check status

Times Excluded

The total number of times the identity has been excluded from a particular check

First Observed (UTC)

The date and time of the first failed observation for this check. Hover over the timestamp to see the event time in your local time based on your device settings.

Latest Event (UTC)

The most recent date and time of a failed observation for this check. Hover over the timestamp to see the event time in your local time based on your device settings.

Admin Notified

The number of times an admin has been notified about this check failure

Failing Check Observations

If there has been more than one observation for a check failure, the row can be expanded using the arrow to the left of the check name, so that you can see the history of observations. Up to 5 observations will be displayed by default, but you can select the ‘See More’ button

under the last observation to see additional events if they exist. Observations are displayed in order from newest (top) to oldest (bottom). The fields available for observations are:

Observed At

The date and time a given observation was recorded. See local timestamp on hover.

Source

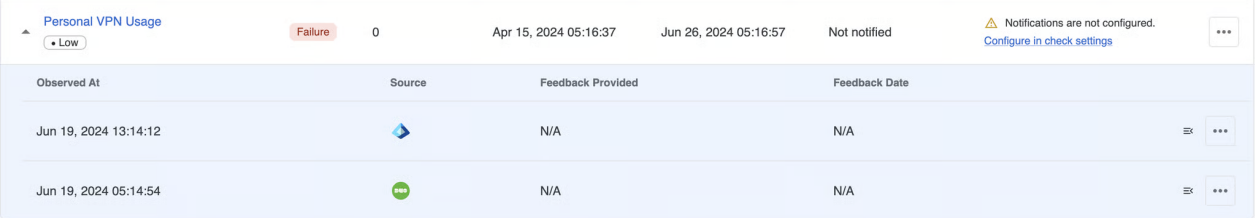
The identity source associated with a given failing observation

Feedback provided

The user who provided feedback on a given observation, if applicable. If there has been no feedback, the value is N/A.

Feedback date

The day and time a user provided feedback on a given observation, if applicable. If there has been no feedback, the value is N/A.



Resolved Checks

Name

The name of the resolved check

Result

Resolved check status

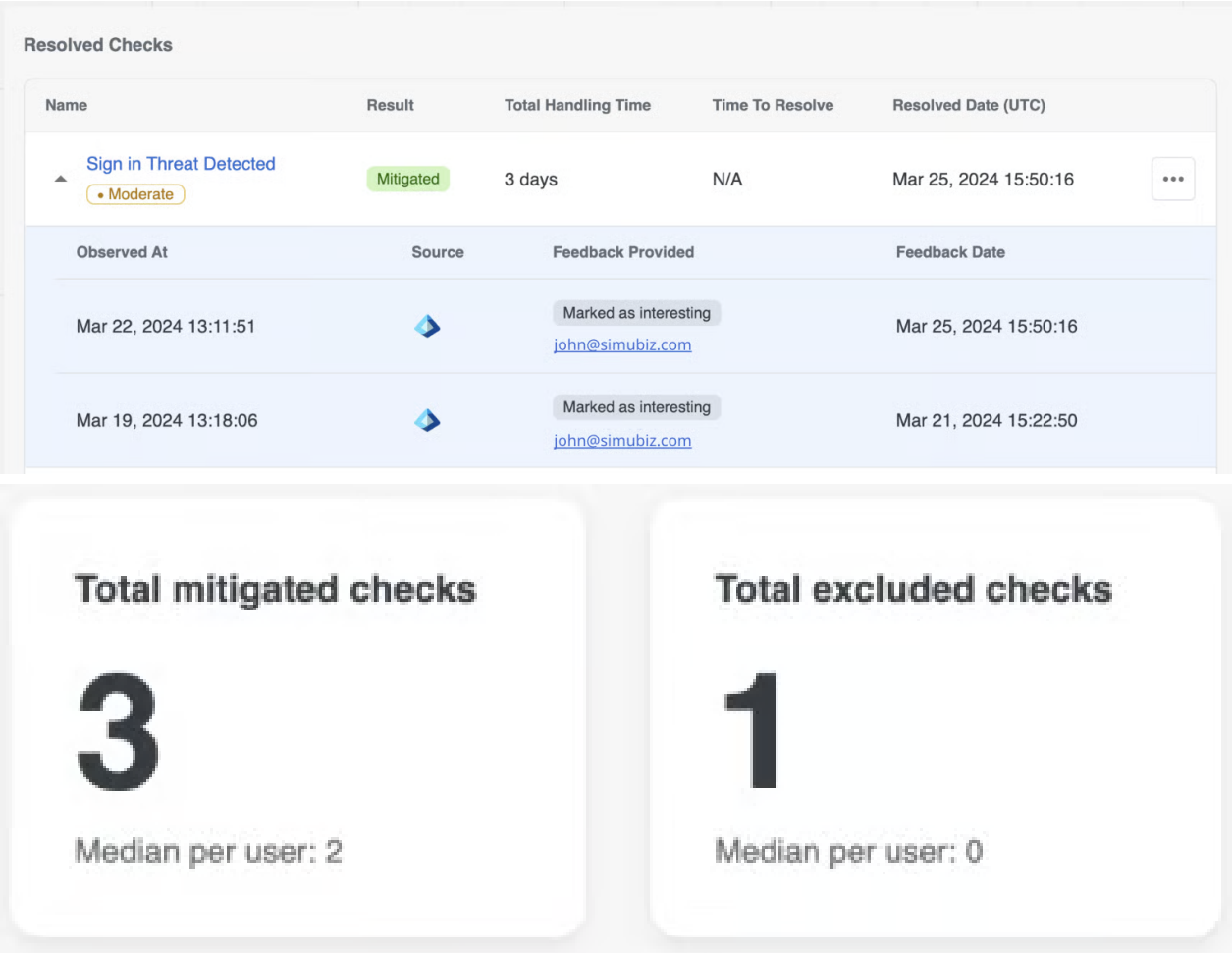
Time to Resolve

The number of days elapsed between the first failure and resolution

Resolved Date (UTC)

The date and time the check was no longer failing. Hover over the timestamp to see the event time in your local time based on your device settings.

Two counters are also shown alongside the tables: total mitigated checks and total excluded checks for the identity.



Diving deeper into a check failure

Selecting the blank space or the **Show Details** icon on the right-hand side of a given row opens a slide panel with explainability details for that check failure. The explainability provides deep context about what caused a particular identity to fail a particular check so that it can be properly investigated and remediated or triaged.

Refer to the User 360 documentation to learn more about how to triage a check failure for an NHI or a human user.

After making a change, allow time for the NHI's checks-related data to update during the next scheduled checks run.