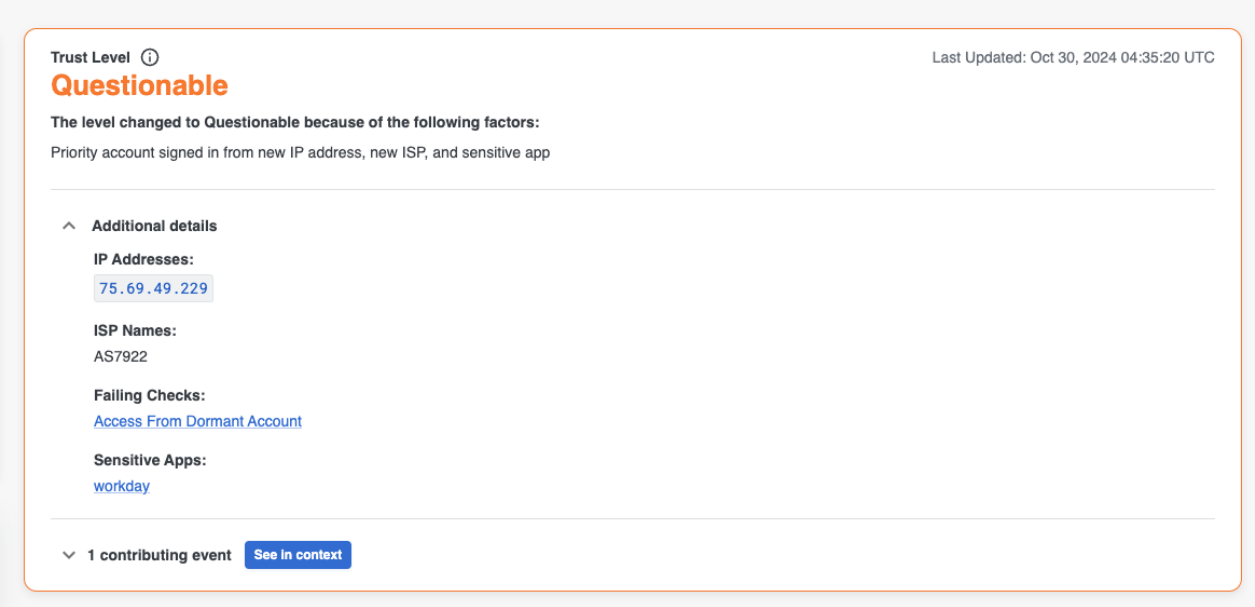
Cisco Identity User Trust Level

Overview

Whether you have hundreds or thousands or tens of thousands of users in your environment, it can be challenging to identify which users currently pose the most risk to your organization. Finding that needle in a haystack out of all the other users in your environment who also (intentionally or not) engage in risky behavior or have identity attacks flying at them, is not only time consuming but also time sensitive. If an account has been compromised, you need to be sure that account is identified as quickly as possible so the necessary remediation steps can happen to stop the attacker from causing further damage.

Because Cisco Identity contains so much rich context and data about your users, across multiple identity sources, there are countless data points that we can use to more accurately identify and rate these risky users than other identity security tools can. Which is why we developed the concept of User Trust Levels.

The User Trust Level is calculated for each user in your organization, based on the user's context, behavior and common tendencies, to help you focus on the most important threats. Trust Levels allow you to quickly and easily pick the riskiest users out of the crowd, so that you can investigate with urgency and remediate the situation as quickly as possible, reducing the attack timeframe or even preventing an attack from happening in the first place.



See Calculation of User Trust Level for high level information on how the Trust Level is determined. You can see more information about the Trust Levels of the users across your organization, as well as Trust Level trends over time, on your Dashboard.

Note: There are no settings related to User Trust Level and it cannot be customized directly. To learn more about tuning checks, which can impact the users failing a check and thus indirectly the User Trust Levels, please refer to our documentation on customizing checks.

Dashboard widgets

To read more about the Trust Level widgets on the Dashboard, please see our Dashboard docs for detailed information about the visualizations and exportability of the data.

Calculation of Trust Level

Cisco Identity weighs several factors together in a proprietary algorithm to produce a User Trust Level for each user in your organization, which ranges from Untrusted to Trusted:

- **Trusted** indicates the user has an exceptional level of safety
- **Favorable** indicates the user has a level of safety
- **Neutral** indicates the user has been evaluated and has neither positive or negative behavior
- **Questionable** indicates the user is displaying behavior that may indicate risk or may be undesirable
- **Untrusted** indicates the user is displaying behavior that is exceptionally bad, malicious or undesirable
- **Unknown** - Users can also have an Unknown Trust Level which indicates the user was not previously evaluated, or is lacking recent account activity, specifically successful sign-in activity, to assert a trust level.

Types of User Risk

Users and their accounts are complicated. User risk is not a monolithic concept and it is important to first understand the different types of risk to understand how a user's Trust Level is calculated. Cisco Identity breaks down the different components that make up user risk to calculate a single User Trust Level that aggregates all the risk types:

Risk Type	Definition	Example
Inherent	The risk/impact of a user's account being taken over assuming no controls are added to the system to reduce the risk	How likely is it that this account will be targeted? (Admins, Execs, etc)
Posture	The risk of an account takeover given the posture of the account	How easy is it to take over this account? (MFA configured, password strength, factor strength, etc)

Behavioral	The risk/likelihood of account takeover based on deviations from the user's normal behavior	How likely is it that their account is compromised already? (recent behaviors, unusual activity)
Action	The risk of account takeover given the specific event and action a user is trying to take at a point in time	How likely is it that this action is legitimate? (IP, location, device, factors, apps, etc)

How User Trust Level is calculated

Cisco Identity takes inputs from all 4 types of risks listed above to calculate the User Trust Level. The User Trust Level will be calculated based on the data available for the users in your organization's tenant. The more data available from different integration instances, the more accurate the Trust Level will be. Some of factors used in this algorithm include the following:

- **User Context:**
- **Priority Users:** Just like with the Identity Posture Score, Priority Users impact the calculation of the user's Trust Level differently because these accounts carry higher risk and are more sensitive than other users in your organization. Priority users are those listed as Integration Instance Admins and/or those who have Executive level titles (ex: Chiefs, President, VPs, etc)
- **Account activity:** If a user's account was recently created, this impacts the calculation of the user's Trust Level differently than other users in your organization
- **User's postural habits:** If a user has poor posture, they are more likely to be successfully compromised if their account were to be targeted. Cisco Identity uses a variety of methods to determine the user's hygiene such as factor enrollment and usage, device ownership, browser usage, etc.
- **User's event behavior:** Looks at the user's typical behavior to determine a baseline so that anomalous or rare events impact the Trust Level. Cisco Identitys looks at things such as IP and networks usage patterns, device patterns, app access patterns, multi-factor patterns and much more to determine events that may be higher risk. Some of this data can come from failing checks.

A single user can generate many events each day. The Trust Level calculation generates a level for each event, and then uses the maximum final level for all events in the given time period, not the average or the sum.

Other factors in your Cisco Identity tenant can also impact User Trust Levels such as:

- **Disabled checks:** Checks that are included as part of the User Trust Level calculation but have been disabled in your organization are not used in the Trust Level Calculation. For the most accurate User Trust Levels, ensure that all checks are enabled in your tenant

- **Integration Instance configuration:** The more integration instances that are connected in your tenant, the more data that is available to contribute to the User Trust Level calculation. The more data available, the more accurate a user's Trust Level will be since Cisco Identity can establish stronger user baselines across systems, analyze more event data points as part of the calculation and compare events across systems to reduce false flags. For this reason it is important to **set up all available integration instances** that exist for your environment. To learn more about what data integrations are available and how to configure them, refer to our documentation on Configuring Integrations
- **Sensitive Apps configuration:** User Trust Levels weighs sensitive apps differently than regular apps. You may need to modify the list of sensitive apps in Cisco Identity to align with your organization's list. Cisco Identity has a pre-configured list of sensitive apps that can be modified using the toggles on the Applications page
- **Check configuration settings:** Cisco Identity analyzes various check failures as part of the User Trust Level calculation. You may find that certain checks are too lenient or too strict and need to be customized to better align with your organization's risk tolerance thresholds
- To configure a check's settings, navigate to the check you'd like to modify. If **Check Settings** are available for that particular check, it will be located in the top right corner of the Check page, and select **Custom Detection Settings**. Note that not all checks have settings that can be modified

Note: Cisco Identity is continuously refining its Trust Level algorithm to include new factors, and modifying the weighting of factors, to provide the most up-to-date and accurate portrayal of user trust as possible. Any updates to the calculation will be reflected on this page

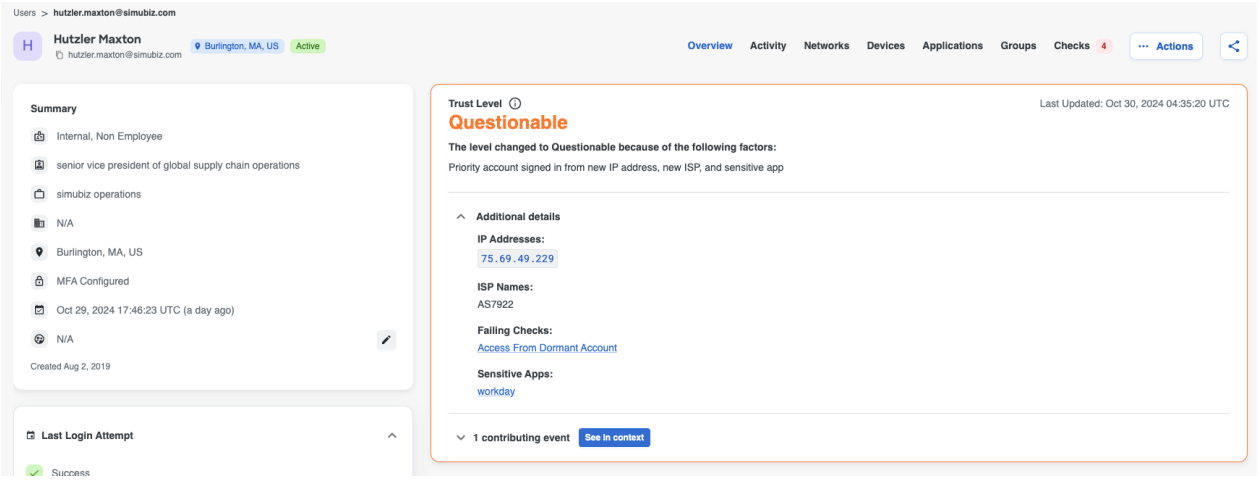
Where to find User Trust Level information within Cisco Identity

Throughout Cisco Identity there are a few places where you can see User Trust Level information with different degrees of detail:

- Dashboard widgets - displays aggregated User Trust Level data across your organization. Useful to quickly find users with Trust Levels you want to investigate
- Users page - displays the current trust level per user and can be used as a filter. Useful to quickly find users with Trust Levels you want to investigate
- User 360 Overview tab - shows a given user's current Trust Level and context about why the user has that trust level. Read more about this below
- Check Failure Explainability and Notifications - shows a given failing user's current Trust Level, regardless of relation to the given check failure, to act as additional context for check failure investigations

User 360 Trust Level widget

Once you have identified a user with a trust level that you want to investigate, click that user's name to open the User360. The User Trust Level widget displayed at the top the Overview tab of the User 360 (screenshot below) shows the most detail and context about a given user's trust level. It is a great starting off point for an investigation.



The Trust Level widget will show you the User's current Trust Level and if available, what the previous Trust Level was and when the Trust Level changed from the previous level to the current level. You may not see the previous level and the date the level changed for all users in cases where this is the first time a Trust Level was calculated for the particular user, or if the previous trust level wasn't different than the current level.

Below this you will information about why the given user received this Trust Level including:

- **Summary** - High level description of what happened with the given account to trigger the current Trust Level (ex: Priority account signed in from new IP address, new ISP, etc etc)
- **Additional details** - Information related to the events described in the Summary, such as IPs, App Names, Device info, etc and any relevant checks failures triggered by the given account
- **Contributing events** - The events that contributed to the user's current Trust Level.
- To see a summary of the actual events, use the v arrow next to the title to expand this part of the widget. You will see up to 5 events in this view by default. You can see the other events by using the arrows at the bottom of the widget, or you can add more rows to the initial view using the **Rows per page** button
- Click the **See in Context** button**,** which is directly above the event table, to navigate to the given user's Activity tab, pre-filtered to display all the events that contributed to the user's current trust level, surrounded by the context of the events that happened in the 48 hours before and after the user's trust level changed
- Click anywhere in a given event row, or click the **View Event Details** button, to open a side panel with the detailed event attributes for the selected event
- **Last Updated -** the last date and time that data was collected and calculations were run to determine if there has been a change to the given user's trust level