Cisco Identity Posture Scores

Identity Posture Scores

Overview

The Identity Posture Scores provide organizations with comprehensive metrics to help assess your current identity security hygiene and easily determine areas of focus to improve it. Scores range from 0 to 100, with corresponding levels from very weak to very good - the higher the score, the better your organization's security posture.

Instead of a single score, these category-level Posture Scores break down security posture into three distinct scores that measure different aspects of your identity ecosystem:

- **Users Score** – measures the security posture of human users (employees, contractors, etc.)
- **MFA Score** – measures multi-factor authentication adoption and strength across all account types
- **NHI Score** – measures the security of non-human identities (service accounts, breakglass accounts, Agentic entities, etc.)

Additionally, relevant recommendations on how to improve your organization's posture are provided with each category score, in order of impact to the respective score, so you can easily determine which identity security hygiene gaps to prioritize.

Each score ranges from 0 to 100 and is classified into one of five levels:

Score Range	Level
0–39	Very Weak
40–59	Weak
60–79	Neutral
80–89	Good
90–100	Very Good

Posture Scores will be calculated based on the data available in your organization's tenant. The more data available from different integration instances, the more accurate your scores will be.

See the Score Calculation section of this article for more information about the other factors used in the Posture Score calculations. You can see more information about your organization's different Posture Scores, as well as the trends over time, on your Dashboard.

Note: There are no settings related to the Posture Scores and they cannot be customized directly. To learn more about tuning checks, which can impact the number of users failing a check and thus, indirectly the Posture Scores, please refer to our documentation on customizing checks.

Understanding the category level scores

Users Score

The Users Score evaluates the security of your human user population across factors including:

- **Account activity** – detects inactive and never-logged-in users
- **Admin account hygiene** – identifies dormant admin accounts and admins sharing authenticators
- **Guest account management** – identifies stale guest accounts
- **HRIS integration** – validates user data against your HR system for missing or discrepant records
- **Active Directory health** – identifies accounts with weak passwords or kerberoastable configurations, if Active Directory is integrated with Cisco Identity

A higher Users Score indicates a well-maintained user population with strong account governance practices.

MFA Score

The MFA Score measures the strength and adoption of multi-factor authentication:

- **MFA adoption** – percentage of users with MFA configured
- **MFA strength** – identifies users with weak MFA methods (SMS, email, security questions) instead of phishing-resistant methods (FIDO2, hardware keys)
- **MFA bypass risks** – detects users with recovery methods that are frequently used, which may indicate bypass activity
- **Priority user coverage** – admins and other high-risk users receive additional weight in the calculation

A higher MFA Score indicates strong MFA adoption and the use of phishing-resistant authentication methods across your organization.

NHI Score

The NHI (Non-Human Identity) Score measures the security of service accounts, applications, and other machine identities:

- **Authentication strength** – detects non-human identities without MFA or phishing-resistant authentication

- **Privilege management** – identifies non-human identities with unnecessary admin privileges
- **Access hygiene** – detects dormant non-human identities and those with browser access
- **Ownership and lifecycle** – identifies non-human identities with no owners or deprovisioned owners
- **Credential rotation** – detects non-human identities with failed password rotation

A higher NHI Score indicates well-managed, secure non-human identities with proper controls and lifecycle management.

Dashboard widgets

Widgets related to the various Posture scores can be found on their respective Dashboard pages. To read more about the widgets, please see our Dashboard documentation for detailed information about each visualization.

The Identity Posture Score is determined based on a number of criteria including integrations connected, number of users impacted by a check, check severity, user context and other factors. See Score Calculation for detailed information on how the score is determined and the thresholds associated with each score category.

Why should I fix my organization's identity posture?

Identity attacks are similar to home burglaries

Think of your organization as a house. You make sure all the doors are closed and locked before you go out to run an errand. While you're away, someone decides to break into your house. They will try to get in through the doors first because that's easiest. When they realize all your doors are locked, they don't give up - they try the windows next. But wait... you didn't check the windows!

If you can't get the basics of closing and locking all your doors and windows down, it wouldn't make sense to install fancy video cameras or alarm systems to monitor your house while you're away because the burglar will still get in! Although these tools can be helpful to identify the burglar later on, or shorten the amount of time they have to take your valuables, it doesn't stop them from getting into your house in the first place and causing damage.

This house example, though simplified, depicts why it is so critical to address postural issues within your organization.

Just like a burglar, a bad actor will try to use the easiest path first, like guessing the password of accounts with no MFA configured. If that doesn't work, they'll try cleverer approaches, like MFA phishing or session theft, to try and gain access to your system. One thing is for certain - while the attack technique might change, **the attacks themselves will not stop.**

With good identity security posture, when a threat comes in (because we know they will come in), you have some peace of mind knowing that the basic protections are in place to ensure your organization is less likely to get “broken into" . You've made sure all the doors AND windows are locked, by requiring basic MFA methods and cleaning up inactive accounts. As your organization's identity security posture matures, you then take more advanced steps to protect it, like enforcing stronger MFA methods and reducing session lengths.

Improving your organization's identity posture won't stop the attacks from coming, nor will it stop a very determined bad actor who is willing to try everything possible to gain access. But it **does** ensure that the attacks that come in are generally less risky because the right precautions and measures were put into place.

With Cisco Identity, you get both sides - Posture Scores and posture checks act as the voice in the back of your head reminding you to lock your doors and windows. While User Trust Levels and threat checks act as the fancy security system to monitor and alert on potentially malicious behavior or threats that should be investigated, and help clean up as soon as possible if someone does slip through the cracks.

Score Calculation

Each score is calculated based on weighted indicators. The weighting reflects both the severity of the security issue and the scope of affected entities:

- **Severity levels of failing checks** – critical issues receive higher weight than low-severity issues. Check severity levels are based on the severity assigned by known attack frameworks such as NIST, MITRE ATT&CK, etc and the potential risk associated with particular hygiene issues. Critical severity issues are weighted more heavily than low severity issues
- **Scale multiplier** – issues affecting more entities have greater impact on the overall scores. Determined by looking at the number of users failing specific posture based checks
- **User context** – For certain category scores, administrators and other privileged users, referred to as Priority Accounts, often receive higher weighting for security-sensitive checks (e.g., MFA requirements) because they carry higher risk and more sensitive than other users if compromised
- Priority Accounts are those listed as Integration Instance Admins and/or Executives based on job titles from the HRIS or IdP connected to Cisco Identity (ex: Chiefs, VPs, President, etc)

Other factors may impact your Identity Posture score as well. Below is a list of factors that can impact your score.

Disabled Checks

To achieve the highest possible scores (90–100 range), one condition must be met: **All relevant posture checks must remain enabled.** This is intentional so that organizations cannot turn off checks to artificially inflate scores instead of investigating and remediating the issues.

Disabling a posture check that is used in the calculation will deduct points from the category score, and an associated recommended action to enable the check will be visible in the list of Posture Score Recommended Actions.

Optional Integration: HRIS Data

If you connect an HRIS system (Workday, manual upload or SCIM), two additional checks become active in the User Identity Posture Score:

- Users not in HRIS
- HRIS discrepancies

If an HRIS integration is **not** configured, these checks remain inactive and do not impact your Users Score. Your Users Score will be calculated from the other identity checks instead. Adding HRIS integration may initially lower your Users Score as discrepancies are discovered, but it enables better long-term user lifecycle management and provides your organization with a more accurate score, so we highly recommend adding this data to Cisco Identity if possible.

New Integration Grace Period

When you first enable a new integration (such as connecting an identity provider or HRIS), your scores may temporarily increase. This grace period lasts for seven days while the system collects baseline data. After seven days, your scores should normalize based on actual security posture and any newly detected issues associated with that data.

Refer to the Posture Trend widgets to see if this event is one of the contributing factors that is surfaced.

Note: Cisco Identity is continuously refining its posture algorithm to include new factors, and/or modify the weighting of factors, to provide the most up-to-date and accurate portrayal of identity posture as possible. Any updates to the calculation will be reflected in this article.

How can I improve my organization's Identity Posture Scores?

Interpreting Your Posture

Review each category score and level alongside the detailed recommendations in your dashboard to understand the full picture across your organization, and which area needs the most attention.

Taking Action

For each score, the respective dashboard widget prioritizes a handful of recommendations based on impact to that score.

Each recommended action will provide high level guidance on what step(s) needs to be taken to review and/or remediate each user that is detracting from your organization's score because of check failures.

Select the number of entities in a posture widget to go to either the relevant check page or the relevant inventory page where you can review each entity that is impacting your posture score via that specific recommended action.

Organizations should review the recommended remediation advice available on a given Checks detail page and investigate each failing entity to determine the appropriate remediation approach for each. Examples of possible remediation include:

- **Making account changes to remediate the account** such as enabling MFA, rotating credentials, updating account settings, etc.
- **Deprovisioning an account** – remove inactive, unneeded, or deprovisioned accounts to resolve issues related to account dormancy (e.g.: this user no longer exists or needs this account)
- **Excluding an account from a check** – exclude specific entities from a particular check when there is a legitimate exception or a specific mitigating control in place (e.g. a user can be excluded from a particular check so that they are no longer failing the check for a specified window of time)
- This action should be used sparingly. For example, a dormant account should be excluded if the user is on medical leave, but if the person has truly left the organization, the account should be deprovisioned across all sources instead of excluded
- **Modify Custom detection settings where necessary** – adjust detection thresholds for your environment (e.g., inactivity periods, new account creation dates, etc) to better align with your organization's processes and policies (e.g. if the default setting for the Inactive Users check is 30 days of inactivity, when your organization's process is to remove dormant accounts after 90 days, you should adjust the check's setting to better reflect that process)
- 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

Improving Your Scores Over Time

Identity posture improvements compound gradually as remediation work progresses:

1. Address high-impact recommendations first (those affecting the most users or the highest-risk identities)

2. When there are similar or related issues to address (e.g. account dormancy, MFA adoption, etc), consider opening a Campaign on the desired issues to make it easier for your team to operationalize the remediation work
3. Focus on the score with the greatest gap to improve your organization's overall security posture
4. Monitor trend data to see the impact of remediation efforts
5. Prioritize phishing-resistant MFA adoption for users, especially admins and VIPs