New Information in the AWS IAM Console Helps You Follow IAM Best Practices | Amazon Web Services

Published: 2017-07-05 · Archived: 2026-04-05 12:57:59 UTC

AWS Security Blog

Today, we added new information to the **Users** section of the AWS Identity and Access Management (IAM) console to make it easier for you to follow IAM best practices. With this new information, you can more easily monitor users' activity in your AWS account and identify access keys and passwords that you should rotate regularly. You can also better audit users' MFA device usage and keep track of their group memberships. In this post, I show how you can use this new information to help you follow IAM best practices.

Monitor activity in your AWS account

The IAM best practice, monitor activity in your AWS account, encourages you to monitor user activity in your AWS account by using services such as AWS CloudTrail and AWS Config. In addition to monitoring usage in your AWS account, you should be aware of inactive users so that you can remove them from your account. By only retaining necessary users, you can help maintain the security of your AWS account.

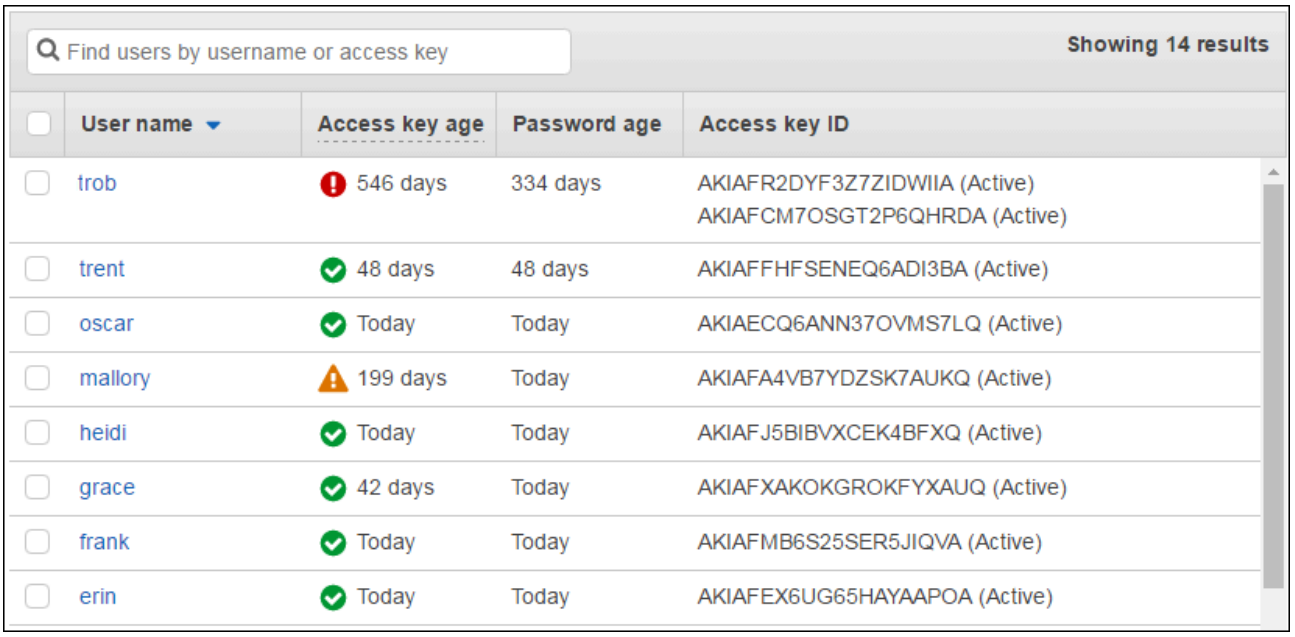
To help you find users that are inactive, we added three new columns to the IAM user table: **Last activity**, **Console last sign-in**, and **Access key last used**.

1. **Last activity** – This column tells you how long it has been since the user has either signed in to the AWS Management Console or accessed AWS programmatically with their access keys. Use this column to find users who might be inactive, and consider removing them from your AWS account.
2. **Console last sign-in** – This column displays the time since the user's most recent console sign-in. Consider removing passwords from users who are not signing in to the console.

3. **Access key last used** – This column displays the time since a user last used access keys. Use this column to find any access keys that are not being used, and deactivate or remove them.

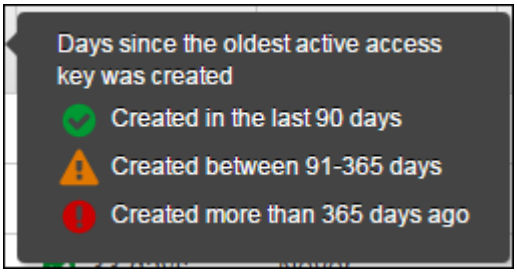
Rotate credentials regularly

The IAM best practice, rotate credentials regularly, recommends that all users in your AWS account change passwords and access keys regularly. With this practice, if a password or access key is compromised without your knowledge, you can limit how long the credentials can be used to access your resources. To help your management efforts, we added three new columns to the IAM user table: **Access key age**, **Password age**, and **Access key ID**.



1. **Access key age** – This column shows how many days it has been since the oldest active access key was created for a user. With this information, you can audit access keys easily across all your users and identify the access keys that may need to be rotated.

Based on the number of days since the access key has been rotated, a green, yellow, or red icon is displayed. To see the corresponding time frame for each icon, pause your mouse pointer on the **Access key age** column heading to see the tooltip, as shown in the following screenshot.



2. **Password age** – This column shows the number of days since a user last changed their password. With this information, you can audit password rotation and identify users who have not changed their password

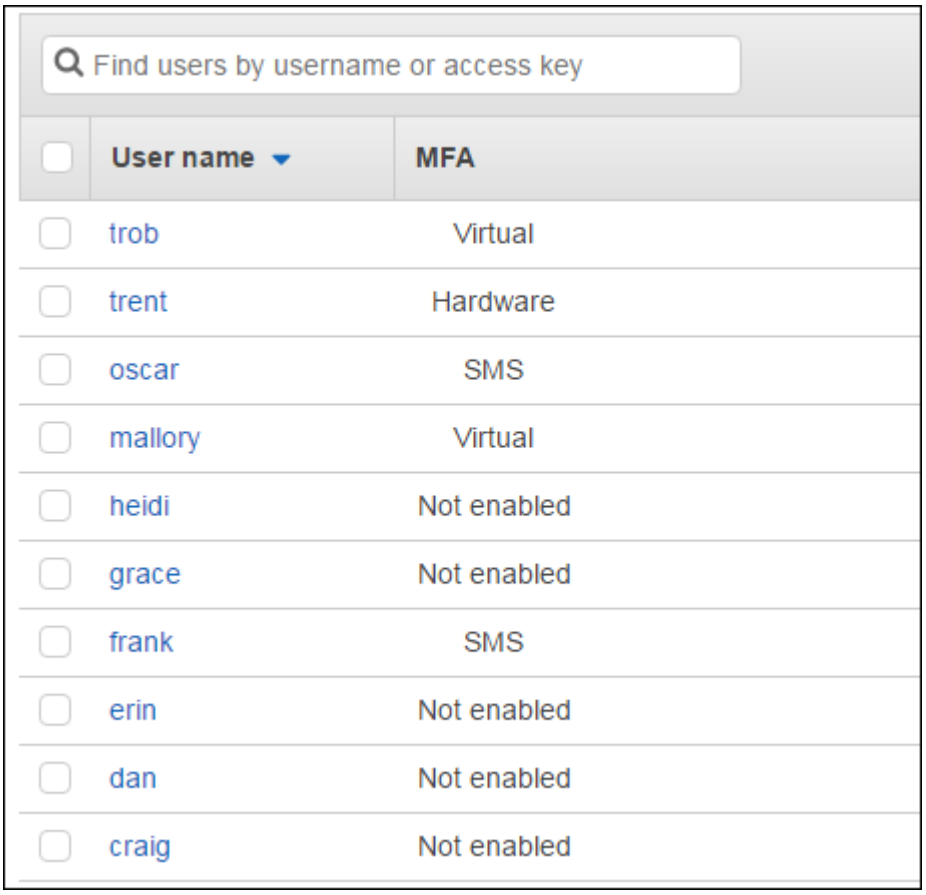
recently. The easiest way to make sure that your users are rotating their password often is to establish an account password policy that requires users to change their password after a specified time period.

3. **Access key ID** – This column displays the access key IDs for users and the current status (**Active**/**Inactive**) of those access key IDs. This column makes it easier for you to locate and see the state of access keys for each user, which is useful for auditing. To find a specific access key ID, use the search box above the table.

Enable MFA for privileged users

Another IAM best practice is to enable multi-factor authentication (MFA) for privileged IAM users. With MFA, users have a device that generates a unique authentication code (a one-time password [OTP]). Users must provide both their normal credentials (such as their user name and password) and the OTP when signing in.

To help you see if MFA has been enabled for your users, we've improved the **MFA** column to show you if MFA is enabled and which type of MFA (hardware, virtual, or SMS) is enabled for each user, where applicable.

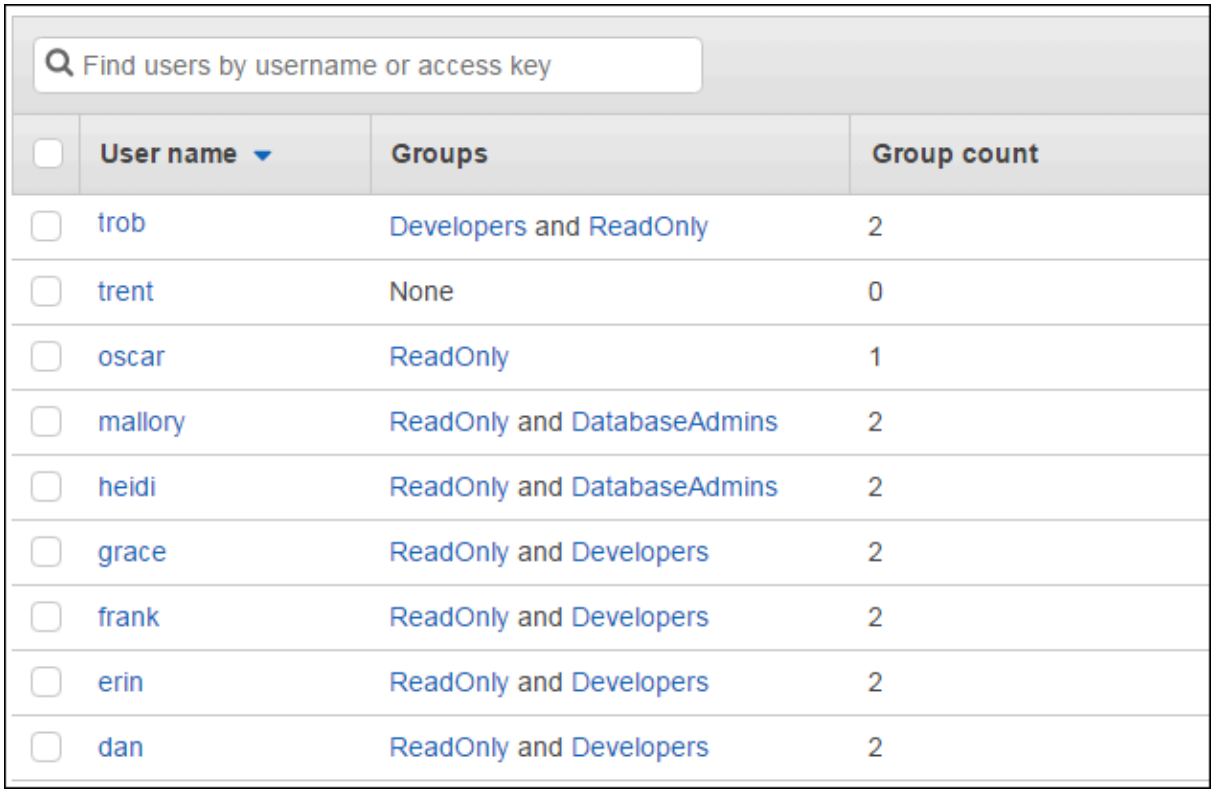


Use groups to assign permissions to IAM users

Instead of defining permissions for individual IAM users, it's usually more convenient to create groups that relate to job functions (such as administrators, developers, and accountants), define the relevant permissions for each group, and then assign IAM users to those groups. All the users in an IAM group inherit the permissions assigned to the group. This way, if you need to modify permissions, you can make the change once for everyone in a group instead of making the change one time for each user. As people move around in your company, you can change the group membership of the IAM user.

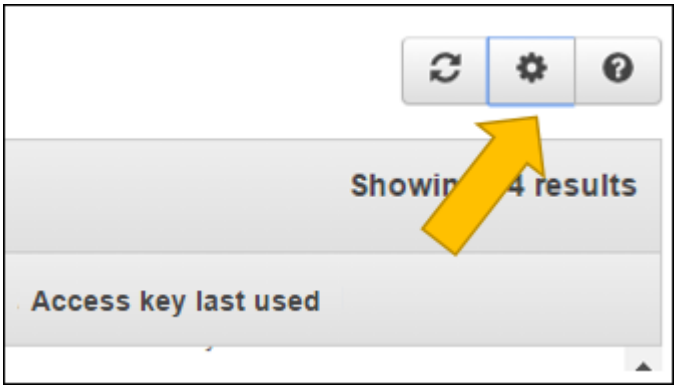
To better understand which groups your users belong to, we've made updates:

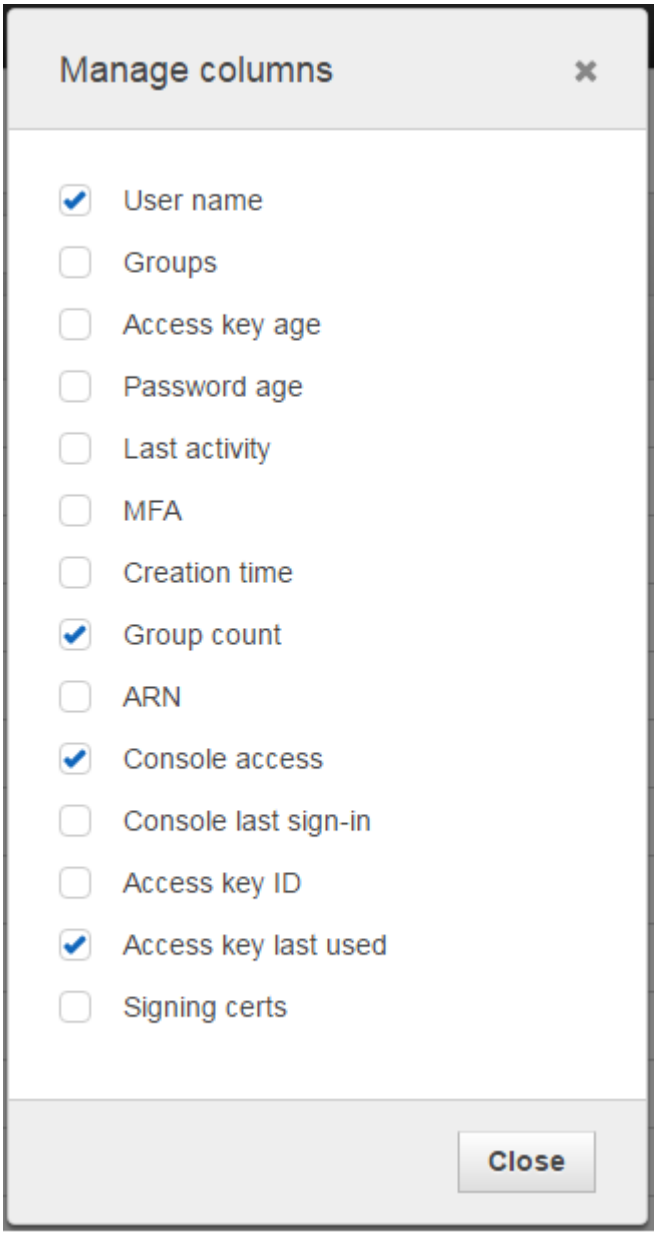
1. **Groups** – This column now lists the groups of which a user is a member. This information makes it easier to understand and compare multiple users' permissions at once.
2. **Group count** – This column shows the number of groups to which each user belongs.



Customize your view

Choosing which columns you see in the **User** table is easy to do. When you click the button with the gear icon in the upper right corner of the table, you can choose the columns you want to see, as shown in the following screenshots.





Conclusion

We made these improvements to the **Users** section of the IAM console to make it easier for you to follow IAM best practices in your AWS account. Following these best practices can help you improve the security of your AWS resources and make your account easier to manage.

If you have comments about this post, submit them in the “Comments” section below. If you have questions or suggestions, please start a new thread on the IAM forum.

– Rob
