

What is the purpose of PCI DSS Requirement 8.2.8, which requires users to reauthenticate after 15 minutes of idle time?

PCI SSC FAQ | Article 1147 | November 2025

The intent of this requirement is to prevent an unauthorized person from using an unattended console/PC to gain access to the user's computer and accounts, and potentially to the company's network.

This requirement is not intended to prevent legitimate activities from being performed while the console/PC is unattended. For example, if a user needs to run a program from an unattended computer, they can login to the computer to initiate the program, and then "lock" the computer so that no one else can use their login while the computer is unattended. An example of how to meet this requirement includes configuring an automated screensaver to launch whenever the console has been idle for 15 minutes and requiring the logged-in user to re-authenticate to re-activate the terminal or session.

Note: Requirement 8.2.8 is not intended to apply to user accounts on point-of-sale terminals that have access to only one card number at a time to facilitate a single transaction.

Source: <https://www.pcisecuritystandards.org/faqs/1147/>