Video transcript

Authentication and authorization

If you try to enter a high security event, someone at the event checks to make sure you're supposed to be there before letting you in. They'll check that you're who you say you are and that you're on the list to get in. In a similar way, network authentication and authorization work to verify identity and approval for access for the purpose of allowing or denying usage of a network.

Authentication confirms the identity of a user or device. The system uses credentials such as usernames and passwords, digital certificates, or biometric factors like fingerprints or facial recognition to make sure users are who they say they are.

Authorization determines whether a user or device is allowed access to a specific network resource. The network administrator or security policy typically defines the role, permissions, and access rights of a user or device. When a user tries to log in, the system validates that the user and device are authorized to use a network before allowing the user to access it.

Authentication and authorization work together to affirm identity and access. Both are required to ensure users are who they appear to be, and that each authorized user is approved to use the network and its resources. The security of network resources relies on authentication and authorization. It protects sensitive information and ensures that users can trust everyone on the network and work together with confidence.