AuthorizationExecuteWithPrivileges | Apple Developer Documentation

Archived: 2026-04-05 13:51:32 UTC

Discussion

This function enables you to execute the tool you specify in the `pathToTool` parameter as a separate, privileged process. The new process will run with root privileges regardless of the privileges of the invoking process. The new process can retrieve the authorization reference by calling the function `AuthorizationCopyPrivilegedReference`. The arguments you pass in the `arguments` parameter are relayed to the new process's `argv` parameter. A set of file descriptors is linked to the new process's standard input and output so that your process may communicate with the new process.

To check if the user is authorized to perform this operation, you should preauthorize the `kAuthorizationRightExecute` right. See `AuthorizationItem` for a description of what information is included in the authorization item for this right.

Special Considerations

You should use this function only to allow installers to run as root and to allow a `setuid` tool to repair its `setuid` bit if lost. This function works only if the Security Server establishes proper authorization.

This function poses a security concern because it will indiscriminately run any tool or application, severely increasing the security risk. You should avoid the use of this function if possible. One alternative is to split your code into two parts—the application and a setuid tool. The application invokes the setuid tool using standard methods. The setuid tool can then perform the privileged operations. If the tool loses its setuid bit, use the `AuthorizationExecuteWithPrivileges` function to repair it. Factoring your program minimizes the use of this function and reduces the risk of harm. Read *Inside macOS: Performing Privileged Operations With Authorization Services*.

Note that this function respects the setuid bit, if it is set. That is, if the tool you are executing has its setuid bit set and its owner set to foo, the tool will be executed with the user foo's privileges, not root privileges. To ensure that your call to the `AuthorizationExecuteWithPrivileges` function works as intended, make sure the setuid bit of the tool you wish to execute is cleared before calling `AuthorizationExecuteWithPrivileges` to execute the tool.
