

If you don't trust your administrators, you've already lost

 devblogs.microsoft.com/oldnewthing/20060921-02

September 21, 2006



Raymond Chen

Occasionally, a customer will ask for a way they can restrict what the administrator can do. The short answer to this is, “Um, no, that’s why they’re called ‘Administrator’.” You can try to set up roadblocks, say, ACL files to revoke access to a file you don’t want the administrator to read, but the Administrator can always take ownership of the file and read the contents that way. At the end of the day, the Administrator owns the local machine. Often, people ask this question because they want to grant certain employees selected subsets of the full set of capabilities available to the Administrator. The way to do this is not to make the user an administrator and then try to rope off the parts you don’t want them to use. Rather, you take the things that you do want them to be able to do and delegate that permission and only that permission to them (discretionary access control).

For more information, check out [this column on trustworthy administrators](#) (based, I am told, on a TechEd presentation) by [Steve Riley](#) (and his uncredited co-presenter [Jesper Johansson](#)).

[Raymond Chen](#)

Follow

