

console session security with multiple ...



deptrev 21 posts since

Mar 14, 2006 We currently run multiple apps on Windows Servers, some of which are maintained via direct console interaction via VirtualCenter. I am concerned about the security of this connection method. As we consolidate, more people will be accessing desktops directly through VirtualCenter.

What I would like to see as a feature is explained in the following scenario:

Employee "A" is an admin and logs into a VM using their credentials via the VirtualCenter console to access confidential data.

Employee "A" leaves station, but locks screen on main desktop, leaving the virtual session exposed to anyone else with access to that server via VirtualCenter.

Employee "B" is a user with access to that same VM in VirtualCenter for user level access, and when he opens the console, the desktop is clearly showing the logged in session from Employee "A" thus exposing confidential data.

Proposed solution:

When Employee "B", as shown above attempts to open a console to ANY VM already logged into by another user, they get a message stating "Please wait for permission to be granted or denied to <VM name> from <username>"

If another (VirtualCenter granted) admin attempts to connect to a console, they should be given an option to over-ride the "wait" message and connect anyway

Employee "A" then gets a popup request (at top of console screen where current notifications reside) to grant or deny access from user <name> to view or interact with said VM. Choices could include "Allow/Deny/View Only".

As servers get consolidated more and more, and remote access methods become more commonplace for various functions on a single VM, the risk for accidental or intentional exposure of confidential data, or admin functionality for non-admin users becomes a real concern. Not implementing this feature exposes a company using VMware to a very serious security concern.