



Microsoft Network Mapped Drives are not recommended

Using mapped drives creates a known security flaw

Network mapped drives is a storage feature that enables the Microsoft-based servers to utilize storage on other Microsoft-based servers storage across a network.

While it is possible to use this feature in DPView™, there are limitations and security vulnerabilities that make it impractical to utilize. Mapping a drive under a local account will allow access to that mapped drive for anyone (or any process) that has a logon session on that server.

An excerpt from MS knowledge base number: Q180362

Redirected Drives on Microsoft Windows XP

On Windows XP and on Microsoft Windows Server 2003, each logon session receives its own set of drive letters, A through Z. Therefore, redirected drives cannot be shared between processes that are running under different user accounts. Additionally, a service (or any process that is running in its own logon session) cannot access the drive letters that are established in a different logon session. However, drive letters that are mapped from a service that is running under the local System account are visible to all logon sessions.

©Copyright 2008. All rights reserved. Integrian and DigitalPatroller are registered trademarks and DPView is a trademark of Integrian, Inc.



Feature Description Video – Storage

30-July-08

Integrian Inc. Corporate Headquarters 511 Davis Drive, Suite 300, Morrisville, NC USA 27560 (919) 472-5000
www.integrian.com