

Real-World Scenario 14-4: Disabling the LM Hash

Scenario: Your organization is concerned about the current level of password security. Your task is to make sure that a strong cryptographic hash is being used.

If you find that the organization is currently using the LANMAN hash, what should you upgrade to?

In what two ways can you disable the LM hash?

Real-World Scenario 14-4 Solution

You should upgrade to the NTLMv2 cryptographic hash. Make sure it is running and that the LM hash has been disabled. This can be done by turning it off in the local security policy—OU or domain policy if configuring it for a Microsoft domain—and by disabling it in the Registry.

Remember that Windows Server 2012 and higher disable the LM hash by default, but as a security administrator it is something you should check to make sure, especially if your servers have been interfacing with older legacy systems in the past.

Video Solution: Watch the video solution “14-4: Disabling the LM Hash.”