

AppAssure Software Inc.

Written By: Kaustubh Pradhan

# [REPLAY: NTLM AND PASS-THROUGH AUTHENTICATION]

This guide describes how to manage the NTLM blocking feature on Windows 7 and Windows Server 2008 R2 to support Pass-through authentication.








## TABLE OF CONTENTS

---

TABLE OF CONTENTS	2
INTRODUCTION	3
THE POLICIES EXPLAINED	3
Pass-through authentication	4
POLICY SETTINGS to Enable NTLM Pass-Through authentication	4

## INTRODUCTION

Windows Server 2008 R2 and Windows 7 restricts NTLM authentication usage out of the box. This feature is known as NTLM blocking. NTLM blocking prevents NTLM from being used for authentication. IT works in both for incoming and outgoing connections, and allows you to create exceptions. NTLM Blocking is implemented using Group Policies that can be accessed under *Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options*. These settings are

 Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication	Not Defined
 Network security: Restrict NTLM: Add server exceptions in this domain	Not Defined
 Network security: Restrict NTLM: Audit Incoming NTLM Traffic	Not Defined
 Network security: Restrict NTLM: Audit NTLM authentication in this domain	Not Defined
 Network security: Restrict NTLM: Incoming NTLM traffic	Not Defined
 Network security: Restrict NTLM: NTLM authentication in this domain	Not Defined
 Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers	Not Defined

Using a combination of these policies it is possible to control and audit the flow of NTLM traffic to and from computers running Windows Server 2008 R2/Windows 7 and other computers that may be within or outside the domain.

## THE POLICIES EXPLAINED

POLICY	DESCRIPTION
<b>Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication</b>	This policy setting allows you to create an exception list of remote servers to which clients are allowed to use NTLM authentication if the "Network Security: Restrict NTLM: Outgoing NTLM traffic to remote servers" policy setting is configured.
<b>Network security: Restrict NTLM: Add server exceptions in this domain</b>	This policy setting allows you to create an exception list of servers in this domain to which clients are allowed to use NTLM pass-through authentication if the "Network Security: Restrict NTLM: Deny NTLM authentication in this domain" is set.
<b>Network security: Restrict NTLM: Incoming NTLM traffic</b>	This policy setting allows you to deny or allow incoming NTLM traffic.
<b>Network security: Restrict NTLM: NTLM authentication in this domain</b>	This policy setting allows you to deny or allow NTLM authentication within a domain from this domain controller. This policy does not affect interactive logon to this domain controller.
<b>Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers</b>	This policy setting allows you to deny or audit outgoing NTLM traffic from this Windows 7 or this Windows Server 2008 R2 computer to any Windows remote server.
<b>Network security: Restrict NTLM: Audit Incoming NTLM Traffic</b>	This policy setting allows you to audit incoming NTLM traffic.
<b>Network security: Restrict NTLM: Audit NTLM authentication in this domain</b>	This policy setting allows you to deny or audit outgoing NTLM traffic from this Windows 7 or this Windows Server 2008 R2 computer to any Windows remote server.

## PASS-THROUGH AUTHENTICATION

The NetLogon service is responsible for implementing pass-through authentication. To perform pass-through authentication the service

- Selects the domain to pass the authentication request to.
- Selects the server within the domain.
- Passes the authentication request through to the selected server.

Selecting the domain is straightforward. The domain name is passed to LsaLogonUser. LsaLogonUser supports interactive logons, service logons, and network logons. Since the domain name specified is not trusted by the domain, the authentication request is processed on the computer being connected to as if the domain name specified were that domain name. NetLogon does not differentiate between a nonexistent domain, an untrusted domain, and an incorrectly typed domain name.

## POLICY SETTINGS TO ENABLE NTLM PASS-THROUGH AUTHENTICATION

If pass-through authentication on a Windows Server 2008 R2 machine fails, then check for the presence of *Network Security: Restrict NTLM*: policy settings under the aforementioned policy location. To disable restrictions on NTLM authentication

1. Run command prompt as administrator.
2. At the command prompt type gpedit.msc and press enter.
3. In the local policy window, navigate to **Local Computer Policy** → **Computer Configuration** → **Windows Settings** → **Security Settings** → **Local Policies** → **Security Options** and set the following policies

Policy	Purpose	Security Settings
<b>Network security: Restrict NTLM: Incoming NTLM traffic</b>	This policy setting allows you to deny or allow incoming NTLM traffic.	<b>Allow all</b>
<b>Network security: Restrict NTLM: Outgoing NTLM traffic to remote servers</b>	This policy setting allows you to deny or audit outgoing NTLM traffic from this Windows 7 or this Windows Server 2008 R2 computer to any Windows remote server.	<b>Allow all</b>
<b>Network security: Restrict NTLM: Audit NTLM authentication in this domain</b>	This policy setting allows you to audit NTLM authentication in a domain from this domain controller.	<b>Enable all</b>
<b>Network security: Restrict NTLM: Audit Incoming NTLM Traffic</b>	This policy setting allows you to audit incoming NTLM traffic.	<b>Enable auditing for all accounts</b>

4. Close the policy window and type, gpupdate /force
5. Close command prompt.