Using security policies to restrict NTLM traffic

By Archiveddocs

Archived: 2026-04-05 21:02:55 UTC

Updated: November 21, 2012

Applies To: Windows 7, Windows 8, Windows Server 2008 R2, Windows Server 2012

This topic describes the available security policies introduced in Windows Server 2008 R2 and Windows 7 and how you can use them to restrict NTLM traffic in your system and domain.

For every policy to restrict NTLM, there are policies or options to first audit NTLM traffic. This permits you to log and analyze authentication activity between clients and member servers, or within a domain before restricting the traffic and potentially causing service interruptions. For information how to discover NTLM traffic in your domain, see Assessing NTLM usage in this guide.

In this topic

- Restricting NTLM traffic in the domain
- Restricting incoming NTLM traffic to a remote server
- Restricting outgoing NTLM traffic from a client computer to a remote server

The following conditions and procedures can help you determine the level of NTLM authentication traffic within a target domain so you can eventually restrict the NTLM traffic and promote Kerberos authentication.

Warning

Setting the policy **Restrict NTLM: NTLM authentication in this domain** without performing an impact assessment first might cause service outage for those applications and users still using NTLM authentication. For information about performing an assessment, see Assessing NTLM usage in this guide.

Conditions

You need to meet the following conditions to restrict NTLM traffic in a domain:

- Assessment of NTLM usage within the domain.
- Ability to configure a security policy on the domain controller.
- Access to the event logs on the member servers and domain controller.
- Knowledge that the list of server names on the security policy **Network security: Restrict NTLM: Add server exceptions in this domain** is correct, if configured.

1. On the domain controller, use the Group Policy Management Console (GPMC) to open the Group Policy **Restrict NTLM: NTLM authentication in this domain** located under the Computer Configuration/Security Settings/Security Options node.

   This policy setting allows you to deny or allow NTLM authentication within this domain. This policy does not affect interactive logon to this domain controller.

2. Select one of the following options that are supported by your assessment:

   - Allow domain logon-related NTLM and NTLM traffic to servers in this domain

     The domain controller will allow all NTLM pass-through authentication requests within the domain. This is the behavior if this policy is not configured.

   - Allow domain logon-related NTLM traffic or NTLM traffic to servers in this domain

     The domain controller will deny all NTLM authentication logon attempts to all servers in the domain that are using domain accounts and display an NTLM blocked error unless the server name is on the exception list in the **Network Security: Restrict NTLM: Add server exceptions for NTLM authentication in this domain** policy setting.

   - Deny domain logon-related NTLM traffic in this domain

     The domain controller will deny all NTLM authentication logon attempts from domain accounts and display an NTLM blocked error unless the server name is on the exception list in the **Network Security: Restrict NTLM: Add server exceptions for NTLM authentication in this domain** policy setting.

   - Deny NTLM traffic to servers in this domain

     The domain controller will deny NTLM authentication requests to all servers in the domain and display an NTLM blocked error unless the server name is on the exception list in the **Network Security: Restrict NTLM: Add server exceptions for NTLM authentication in this domain** policy setting.

   - Deny NTLM traffic in this domain

     The domain controller will deny all NTLM pass-through authentication requests from its servers and for its accounts and display an NTLM blocked error unless the server name is on the exception list in the **Network Security: Restrict NTLM: Add server exceptions for NTLM authentication in this domain** policy setting.

1. Using Event Viewer on the domain controller, navigate to Applications and Services Logs/Microsoft/Windows/NTLM and open the Operational log.

2. Investigate NTLM authentiction failed events to determine if NTLM authentication should be allowed or should be restricted by using a different option. Note server names.

3. You can adjust the NTLM authentication usage by resetting this policy to a different option or adding other servers to the exception list.

The following conditions and procedures can help you determine the level of incoming NTLM authentication traffic from a client computer to a remote server so you can eventually restrict the NTLM traffic and promote Kerberos authentication.

Warning

Setting the policy **Network Security: Restrict NTLM: Incoming NTLM traffic** without performing an impact assessment first might cause service outage for those applications and users still using NTLM authentication. For information about performing an assessment, see Assessing NTLM usage in this guide.

Conditions

You need to meet the following conditions to restrict NTLM traffic on a remote server:

- Ability to configure a security policy on the remote server.
- Access to the event logs on the remote server and domain controller.
- Knowledge that the list of server names on the security policy **Network security: Restrict NTLM: Add server exceptions for NTLM authentication in this domain** is correct, if configured.
- Established connection to the remote server.

1. On the remote server, use the Group Policy Management Console (gpmc.msc) to open the security policy **Restrict NTLM: Incoming NTLM traffic** located under the Computer Configuration/Security Settings/Security Options node.
2. Select one of the following options that supports your assessment strategy:
    - Allow all incoming NTLM traffic

      The server will allow all NTLM authentication requests. This is the behavior if this policy is not configured.
    - Deny all incoming domain logon related NTLM traffic

      The server will deny NTLM authentication requests for domain logon and display an NTLM blocked error.
    - Deny all incoming NTLM traffic

      The server will deny NTLM authentication requests from incoming traffic and display an NTLM blocked error.

1. Using Event Viewer on the domain controller and the remote server, navigate to Applications and Services Logs/Microsoft/Windows/NTLM and open the Operational log on each.

2. Investigate NTLM authentication failed events to determine if NTLM authentication should be allowed or should be restricted. Note computer names.

3. You can adjust the NTLM authentication usage by resetting this policy to a different option or adding other servers to the exception list.

The following conditions and procedures can help you determine the level of outgoing NTLM authentication traffic from a client computer to a remote server so you can eventually restrict the NTLM traffic and promote Kerberos authentication.

Warning

Setting the policy **Restrict NTLM: Outgoing NTLM traffic to remote servers** without performing an impact assessment first might cause service outage for those applications and users still using NTLM authentication. For information about performing an assessment, see Assessing NTLM usage in this guide.

Conditions

You need to meet the following conditions to restrict NTLM traffic to a remote server:

- Assessment of NTLM usage between this server and client computers.
- Ability to configure a security policy on the client computer.
- Access to the event logs on the client computer.
- Knowledge that the list of server names on the security policy **Network security: Restrict NTLM: Restrict NTLM: Add remote server exceptions for NTLM authentication** is correct, if configured.

1. On the client computer, use the Group Policy Management Console (gpmc.msc) to open the network security policy **Restrict NTLM: Outgoing NTLM traffic to remote servers** located under the Computer Configuration/Security Settings/Security Options node. This policy setting allows you to deny or audit outgoing NTLM traffic to remote servers.

2. Select one of the following options that supports your assessment strategy:

    - Deny all outgoing NTLM traffic to remote servers.

      The client computer cannot authenticate identities to a remote server by using NTLM authentication. You can use the **Network Security: Restrict NTLM: Add remote server exceptions for NTLM authentication** policy setting to define a list of remote servers to which clients are allowed to use NTLM authentication.

    - Allow all outgoing NTLM traffic to remote servers.

      The client computer can authenticate identities to a remote server by using NTLM authentication. This is the default behavior if this policy is not configured.

1. Open the Group Policy Management Console (gpmc.msc) on the client computer.

2. Navigate to the **Security Options** node under Local Computer Policy/Computer Configuration/Windows Settings/Security Settings/Local Policies.

3. Configure the security policy **Network security: Restrict NTLM: Add remote server exceptions for NTLM authentication** by listing the names of the servers that you will allow NTLM authentication. The naming format for servers on this exception list is the fully qualified domain name (FQDN) or NetBIOS server name used by the calling application listed one per line. A single asterisk (*) can be used at the beginning or end of the string as a wild card character.

1. Using Event Viewer on the domain controller, navigate to Applications and Services Logs/Microsoft/Windows/NTLM and open the Operational log.

2. Investigate NTLM authentication failed events to determine if NTLM authentication should be allowed or should be restricted. Note server names.

Restricting NTLM usage
