Network Level Authentication and Encryption

Published 16 February 08 06:00 AM

Welcome to Day Sixteen. We're continuing on with our series on Windows Server 2008 in preparation for the launch. Today, we're going to look at Terminal Server security in Windows Server 2008 - specifically Network Level Authentication and Encryption.

Terminal Server security may be enhanced by providing user authentication earlier in the connection process when a client connects to a Terminal Server. This early user authentication method is referred to as Network Level Authentication. This is a new authentication method that completes user authentication before you establish a Remote Desktop connection and the logon screen appears. This is a more secure authentication method that can help protect the remote computer from malicious users and malicious software. The advantages to Network Level Authentication are:

- Requires fewer remote computer resources initially. The remote system uses a limited number of resources before authenticating the user, rather than starting a full Remote Desktop connection as in previous versions
- Provides better security by reducing the risk of denial of service attacks

There are specific requirements to use Network Level Authentication:

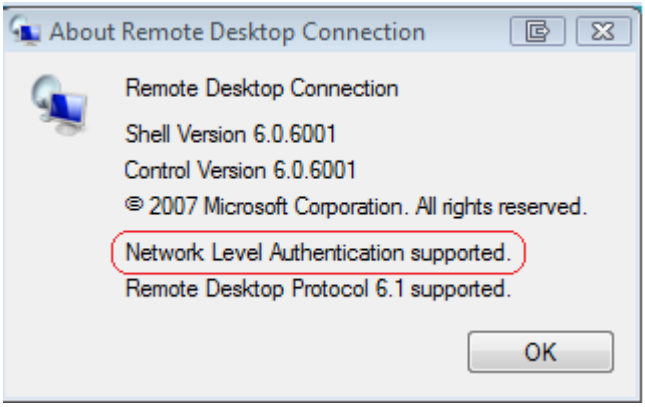
- The client computer must be running at least Remote Desktop Connection 6.0
- The client computer must be using an operating system (such as Windows Vista) that supports the new Credential Security Support Provider (CredSSP) protocol
- The Terminal Server must be running Windows Server 2008

The Terminal Server can be configured to only support connections from clients running Network Level Authentication. This setting can be configured in a couple of different ways:

- During the installation of the Terminal Server role service in Server Manager, on the Specify Authentication Method for Terminal Server page in the Add Roles Wizard
- On the Remote Tab in the System Properties dialog box on a Terminal Server
- On the General tab of the Properties dialog box for a connection in the Terminal Services Configuration tool by selecting the **Allow connections only from computers running Remote Desktop with Network Level Authentication** check box
- By applying the **Require user authentication for remote connections by using Network Level Authentication** Group Policy setting. If the **Allow connections from computers running any version of Remote Desktop (less secure)** option is not selected and is grayed out in the dialogs mentioned above, then the **Require user authentication for remote connections by using Network Level Authentication** Group Policy setting has been enabled for the Terminal Server.

2 Windows Server 2008 : Network Level Authentication and Encryption

To determine if a system is running a version of Remote Desktop Connection software that supports Network Level Authentication, start the Remote Desktop Connection client application, click the icon in the upper-left corner of the Remote Desktop Connection dialog box and click About. Look for the phrase, "**Network Level Authentication**" in the About window as shown below.



By default, Terminal Services sessions use native Remote Desktop Protocol (RDP) encryption. However, RDP does not provide authentication to verify the identity of a Terminal Server. You can enhance the security of Terminal Services sessions by using Transport Layer Security (TLS) 1.0 for server authentication and to encrypt Terminal Server communications. The Terminal Server and client system must be configured correctly for TLS to provide enhanced security. There are three available security layers outlined in the table below:

Security Layer	**Description**
SSL (TLS 1.0)	SSL (TLS 1.0) will be used for server authentication and for encrypting all data transferred between the server and the client
Negotiate	The most secure layer that is supported by the client will be used. If supported, SSL (TLS 1.0) will be used. If the client does not support SSL (TLS 1.0), then the RDP Security Layer will be used. This is the default setting
RDP Security Layer	Communication between the server and the client will use native RDP encryption. If you select RDP Security Layer, you cannot use Network Level Authentication

When SSL (TLS 1.0) is used to secure communications between a client and Terminal Server, a certificate is needed. You can select a certificate that you have already installed on the Terminal Server or you can use the default self-signed certificate.

3 Windows Server 2008 : Network Level Authentication and Encryption

For Terminal Services connections, data encryption protects data by encrypting it on the communications link. By default, Terminal Services connections are encrypted at the highest available level of security - 128-bit. However, some older versions of the Terminal Services client application do not support this high level of encryption. The encryption level of the connection may be configured to send and receive data using different encryption levels to support legacy clients. There are four configuration options as outlined below:

Level of Encryption	**Description**
Low	Data sent from the client to the server is encrypted using 56-bit encryption. Data sent from the server to the client is not encrypted
Client Compatible	Encrypts client / server communication at the maximum key strength supported by the client. Use this level when the Terminal Server is running in an environment containing mixed or legacy clients. This is the default setting
High	Encrypts client / server communication using 128-bit encryption. Use this level when the clients that access the Terminal Server also support 128-bit encryption. If this option is set, clients that do not support 128-bit encryption will not be able to connect
FIPS-Compliant	All client / server communication is encrypted and decrypted with the Federal Information Processing Standard (FIPS) encryption algorithms. FIPS 140-1 (1994) and its successor, FIPS 140-2 (2001) describe these requirements

These encryption levels are stored in the **MinEncryptionLevel** value in the following registry key: *HKLM₩SYSTEM₩CurrentControlSet₩Control₩TerminalServer₩WinStations₩RDP-Tcp*. There are four possible values for **MinEncryptionLevel** that correspond to the settings in the table above:

- 1 = low
- 2 = client compatible
- 3 = high
- 4 = fips

From: http://blogs.technet.com/askperf/archive/2008/02/16/ws2008-network-level-authentication-and-encryption.aspx