Microsoft® Windows®98 Dial-Up Networking 1.4 Upgrade Release Notes

1. Introduction

This Dial-Up Networking 1.4 upgrade for Windows 98 supports 128 bit encryption for both dial-up and PPTP connections and resolves situations in which PPTP connections would no longer transmit data. It includes all of the features from the earlier Windows 98 Security Upgrade which strengthened password management and data encryption in PPTP connections.

1.1 New Features in DUN 1.4

- 128-bit encryption is supported with the Dial-Up Networking 1.4 Upgrade.
- The Dial-Up Networking 1.4 Upgrade improves the stability of PPTP connections.

1.2 Installation Notes

Execute the Install file and follow the instructions it displays. At the end of the installation process you will be required to reboot your PC.

1.3 MSCHAP V2

A new MSCHAP secure mode (MSCHAP V2) has been implemented, providing mutual authentication, stronger initial data encryption keys, and different encryption keys for the transmit and receive paths.

To minimize the risk of password compromise during MSCHAP exchanges, MSCHAP V2 drops support for the MSCHAP password change V1, and will not transmit the LM password response.

For VPN connections, a PPTP server will negotiate MSCHAP V2 before negotiating the original MSCHAP. An updated Windows 98 client will accept this offer and use MSCHAPV2 as the authentication method. To ensure that no VPN clients authenticate using MSCHAP, the server can be set to require MSCHAP V2. This will prevent legacy clients from presenting their credentials in an MSCHAP or PAP or CHAP exchange, and is a likely configuration for networks that require the most secure authentication method.

1.4 Secure VPN Mode

If there are special circumstances in which you wish to ensure that your PC uses only the new MSCHAP V2 for all VPN connection attempts, a new client-side registry flag, *SecureVPN*, can be used to force this behavior. When this flag is set, your PC will only accept MSCHAP V2 authentication for any VPN connections. In addition, this flag will require data encryption for all VPN connections. Dial-up connections are not affected.

> *NOTE: Most users will not need to use the Secure VPN flag. This flag should be used with care because it will affect the behavior of all VPN connections from your machine. In general, the required use of MSCHAP V2 and data encryption can be enforced more easily on the server.*

The registry setting which will force a Windows 98 client to use only the new MSCHAP V2 secure mode and require data encryption for PPTP connections is defined below. By default, this registry variable is absent, meaning “do not force secure mode on PPTP connections”. The value of this variable is checked just before a connection is attempted.

HKLM\System\CurrentControlSet\Services\RemoteAccess
Default: 0x00000000

DWORD: SecureVPN

Value: 0x00000001 == Force secure mode (MSCHAP V2 plus data encryption) on all PPTP connections
Value: 0x00000000 == Do not force secure mode on PPTP connections

1.5 LM Response Suppression

This release also provides a new registry variable which prevents the client from sending the LM response to a legacy MSCHAP challenge, as defined below. By default, this variable is absent, meaning that the client should send the LM response (in order to maintain compatibility with legacy servers). This variable affects both dial-up and VPN connections; its value is checked just before a connection is attempted.

NOTE: Most users will not need to use this registry variable. The new secure mode MSCHAP V2 will not send the LMHash response, so this registry value is most useful when connecting to older access servers which use the original MSCHAP. Setting this variable on a Windows 98 client will prevent the client from connecting to a Windows 95 or Windows 98 server.

HKLM\System\CurrentControlSet\Services\RemoteAccess

DWORD: UseLmPassword
Default: 0x00000001

0x00000000 = Do not send LM challenge response (send only NT challenge response)
0x00000001 = Send LM challenge response

1.6 Forcing Strong Encryption

Windows 98 Dial-up Networking already supports a checkbox to require encryption for a specific connection. Clients which support 128-bit encryption will accept any level of encryption (128-bit or 40-bit) offered by the server. This upgrade provides a new registry flag, ForceStrongEncryption. When set, this flag will require 128-bit encryption for any connection which has already been set to require encryption. (In other words, setting the new registry flag essentially changes the meaning of the existing checkbox from "require encryption" to "require strong encryption".)

The registry flag which forces strong encryption is defined below. By default, the flag is absent. The value of this flag is checked just before a connection is attempted.

HKLM\System\CurrentControlSet\Services\RemoteAccess

DWORD: ForceStrongEncryption
Default: 0x00000000

0x00000000 = No effect; does not force strong encryption
0x00000001 = Requires 128-bit encryption for any connection which already requires encryption

1.7 Other Changes

The details section of the connection status display has been modified to identify the specific form of CHAP that was used in the connection. Standard CHAP is displayed as "Challenge Authentication Protocol"; legacy MSCHAP is displayed as "Microsoft Challenge Authentication Protocol"; and MSCHAP V2 is displayed as "Microsoft Mutual Challenge Authentication Protocol".

1.8 Removing this Update

To uninstall the Dial-Up Networking 1.4 upgrade for Windows 98, use the “Add/Remove Programs” application in the control panel. This will remove 128 bit encryption (leaving the capability for 40 bit encryption) and will restore Dial-up Networking files to the versions that originally shipped with Windows 98.

> *start -> control panel -> Add/Remove Programs -> Install/Uninstall Tab -> Select "Dial-up Networking 1.4 Update for Windows 98" -> Click "Add/Remove" button*
