

Microsoft IPSec settings

(via Microsoft Management Console (MMC) control)

IPsec binaries are
The IPsec driver file: **Ipsec.sys**
IKE component: **Oakley.dll**

1. If you are adding or modifying a key exchange security method, in the IKE Security Algorithms dialog box, select an Integrity algorithm:

- **MD5** to use a 128-bit key (faster).
- **SHA1** to use a 160-bit key (stronger).

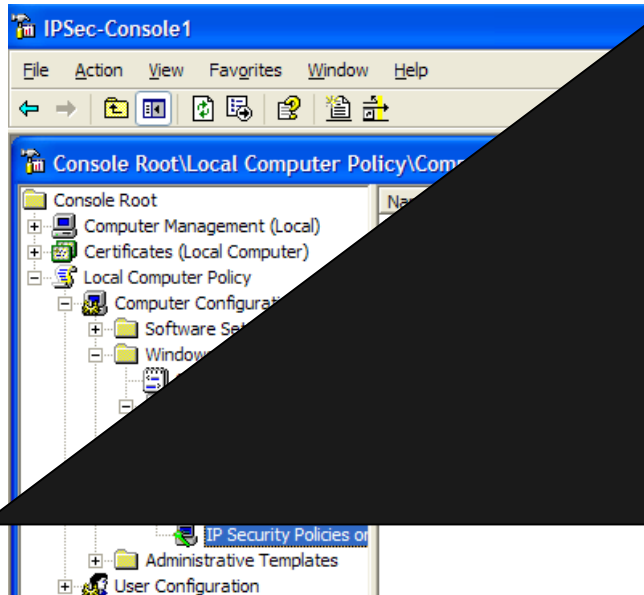
If PFS, **Perfect Forward Secrecy**, is used, a new Diffie-Hellman exchange is performed for each phase-2 negotiation.

2. Select an Encryption algorithm:

- **3DES** to use the triple Data Encryption Standard (3DES) algorithm and three unique 56-bit keys.
- **DES** to use the DES algorithm and a single 56-bit key. Use this option if you are required to connect to computers that do not have 3DES or if you do not need the higher security and overhead of 3DES.

3. Select a **Diffie-Hellman** group to set the length of base keying material used to generate the actual keys:

- Low (1) to generate 768 bits of master key keying material.
- Medium (2) to generate **1,024** bits of master key keying material (stronger).
- High (2048) to generate **2,048** bits of master key keying material (strongest). – Windows **2K3** OS
- For enhanced security, do not use Diffie-Hellman Group 1 (low). For maximum security, use Group 2048 whenever possible. For interoperability with Windows 2000 and Windows XP, use Group 2 when required for interoperability with Windows 2000 and Windows XP. When you use a stronger group, the confidentiality of the Diffie-Hellman exchange has greater strength.
- A key exchange security method is a combination of three settings (**integrity** algorithm, **encryption** algorithm, and **Diffie-Hellman group**). The initiator and the responder must have a method in common (one that uses the same settings).
- **Diffie-Hellman Group 2048 is provided only with the Windows Server 2003 family.**
- Computers running Windows 2000 must have the High Encryption Pack or **Service Pack 2** installed to support the 3DES algorithm. If a computer running Windows 2000 receives a 3DES setting, but does not have Service Pack 2 (or later) installed, the 3DES setting in the security method is set to the DES algorithm to ensure confidentiality for communication, rather than blocking all communication. However, not all computers in your environment support the use of 3DES. Computers that do not support 3DES and do not require installation of the High Encryption Pack will not be able to communicate with systems that support 3DES and do not require installation of the High Encryption Pack.



COPYRIGHT
©ITcharts.com