Release Notes for Version 5.0.3

Created: December 11, 2009
# Table of Contents

- What's New ............................................................................................................................................ 3
- System Requirements ................................................................................................................................. 4
- Build Version ............................................................................................................................................... 4
- Product Binary Checksums ......................................................................................................................... 4
- Compatibility ............................................................................................................................................... 4
- IPsec Compliance ........................................................................................................................................ 5
- Supported Algorithms ................................................................................................................................. 5
- Installation and Upgrade Instructions ......................................................................................................... 6
- Known Issues .............................................................................................................................................. 6
What’s New

Fixes

Problems described in the table below have been fixed since StoneGate IPsec VPN client version 5.0.2. A workaround solution is presented for earlier versions where available.

<table>
<thead>
<tr>
<th>Synopsis</th>
<th>Description</th>
<th>Workaround for previous versions</th>
</tr>
</thead>
<tbody>
<tr>
<td>DSA certificates stored in Microsoft Certificate Store do not work correctly (#52841)</td>
<td>When using DSA certificate stored in Microsoft Certificate Store, the authentication to Firewall/VPN gateway fails with error &quot;Invalid signature (signature check failed)&quot;.</td>
<td>N/A</td>
</tr>
<tr>
<td>Mobile Broadband adapter type not supported on Windows 7 (#53630)</td>
<td>Some 3G mobile broadband adapters like Dell Wireless 5530 HSPA Mini-Card Network Adapter and Ericsson F3507g Mobile Broadband Module cannot be used on Windows 7 to establish VPN connection with StoneGate IPsec VPN Client.</td>
<td>N/A</td>
</tr>
<tr>
<td>Deep directory hierarchies are not supported in certificate key containers (#54007)</td>
<td>If the directory hierarchy of a certificate’s key container is deeper than one, the StoneGate IPsec VPN client fails to handle the certificate/keys correctly.</td>
<td>N/A</td>
</tr>
<tr>
<td>IPsec VPN client security checks do not detect the status of all products (#54291)</td>
<td>IPsec VPN client local security checks do not detect the status of all products, for example, &quot;Microsoft Security Essentials&quot; may not be detected.</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Changes Introduced in Version 5.0

Please refer to the Release Notes for version 5.0.0 for information on new features and changes in this software version series.
System Requirements

General Requirements

- Processor: Pentium 4 processor or higher recommended
- Hard disk space: 300 MB of free disk space
- Memory: 512 MB
- Mouse or other pointing device
- SVGA (800x600) display or higher
- IPv4 TCP/IP installed and configured

Operating Systems

- Windows XP 32-bit Professional or Home with Service Pack 2 or Service Pack 3
- Windows Vista 32/64-bit versions, Service Pack 1 or Service Pack 2
- Windows 7 32/64-bit versions

Build Version

The StoneGate IPsec VPN client version 5.0.3 build version is 2028.

Product Binary Checksums

StoneGate_IPsec_VPN.msi
MD5SUM     a1ff6662460a32156c68bab11e49a857
SHA1SUM    169179104ceec673e713331a56f1182ec08336c9

StoneGate_IPsec_VPN_5.0.3.2028.exe
MD5SUM     224c0e544d2560e9c8eccf9c9bcdbce4
SHA1SUM    c609db76c1d0ede058371dcbf32bb586eb3e36cd

StoneGate_IPsec_VPN_5.0.3.2028_with_NET2.0.exe
MD5SUM     d81b469409906ad2131923da738087bb
SHA1SUM    2e33002eb4313032d27539b77409a3c77cdf3410

Compatibility

StoneGate IPsec VPN client version 5.0.3 is compatible with StoneGate Firewall/VPN version 4.2.0 and later. New algorithms are supported only with Firewall/VPN version 5.0.0 or newer. StoneGate Management Center (SMC) version 4.3.0 or later is required. SMC 5.0.0 or later is required when using client security checks.
### IPsec Compliance

StoneGate IPsec VPN client is compliant with the IPsec and IKEv1 standards. StoneGate IPsec VPN client can only be used with a StoneGate Firewall/VPN gateway because of the proprietary automatic configuration methods.

### Supported Algorithms

StoneGate IPsec VPN client version 5.0.3 supports the following algorithms:

<table>
<thead>
<tr>
<th>Negotiation Phase</th>
<th>Algorithm</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKE (Phase 1)</td>
<td>Cipher</td>
<td>AES-128, AES-256, 3DES</td>
</tr>
<tr>
<td></td>
<td>Message Digest</td>
<td>MD5, SHA-1, SHA-256</td>
</tr>
<tr>
<td></td>
<td>Diffie-Hellman Groups</td>
<td>2, 5, 14</td>
</tr>
<tr>
<td>IPsec (Phase 2)</td>
<td>Cipher</td>
<td>AES-128, AES-256, AES-GCM, 3DES</td>
</tr>
<tr>
<td></td>
<td>Message Digest</td>
<td>AES-XCBC-MAC , MD5, SHA-1, SHA-256</td>
</tr>
<tr>
<td></td>
<td>Compression</td>
<td>Deflate, None</td>
</tr>
<tr>
<td></td>
<td>Perfect Forward Secrecy (PFS) groups</td>
<td>2, 5, 14</td>
</tr>
</tbody>
</table>

StoneGate IPsec VPN client version 5.0.3 also supports the following algorithms when CryptoPro Version 3.6.5402 is loaded:

<table>
<thead>
<tr>
<th>Negotiation Phase</th>
<th>Algorithm</th>
<th>Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKE (Phase 1)</td>
<td>Cipher</td>
<td>DES, GOST 28147-89</td>
</tr>
<tr>
<td></td>
<td>Message Digest</td>
<td>GOST R34.11</td>
</tr>
<tr>
<td>IPsec (Phase 2)</td>
<td>Cipher</td>
<td>DES, GOST 28147-89</td>
</tr>
<tr>
<td></td>
<td>Message Digest</td>
<td>G28147 IMIT, GOST R34.11</td>
</tr>
</tbody>
</table>
Installation and Upgrade Instructions

The main installation steps for the StoneGate IPsec VPN client are as follows:

1. If you are running a StoneGate VPN client older than 4.2.0, uninstall that version.

2. Ensure you have administrator privileges (or on Vista, that UAC is enabled) and start the installation by running the setup file.

3. If you are installing on a Windows XP system that does not have the Microsoft .NET Framework version 2.0 or newer installed, select the installation package that also contains the .NET framework.

4. If the StoneGate IPsec VPN client must be installed in silent mode, start the installer from the command line and add options /s /v"/qn" to the command line.

5. Follow the on-screen instructions to complete the installation.

6. Connect to a gateway to get the configuration settings for the VPN client.

The detailed installation instructions can be found in the StoneGate IPsec VPN Client User’s Guide. For more information on using StoneGate, refer to the Online Help system or the StoneGate Administrator’s Guide. For background information on how the StoneGate system works, consult the Management Center Reference Guide and Firewall/VPN Reference Guide.

There have been reports that in some pre-installed Windows Vista systems the junctions to the C:\ProgramData folder have been set up erroneously. StoneGate IPsec VPN client must not be installed on these machines before correcting the junctions to point to the correct folder (C:\ProgramData).

Known Issues

There are currently no known issues for the StoneGate IPsec VPN client.
Copyright and Disclaimer

© 2000—2009 Stonesoft Corporation. All rights reserved.
These materials, Stonesoft products, and related documentation are protected by copyright and other laws, international treaties and conventions. All rights, title and interest in the materials, Stonesoft products and related documentation shall remain with Stonesoft and its licensors. All registered or unregistered trademarks in these materials are the sole property of their respective owners. No part of this document or related Stonesoft products may be reproduced in any form, or by any means without written authorization of Stonesoft Corporation.

Stonesoft provides these materials for informational purposes only. They are subject to change without notice and do not represent a commitment on the part of Stonesoft. Stonesoft assumes no liability for any errors or inaccuracies that may appear in these materials or for incompatibility between different hardware components, required BIOS settings, NIC drivers, or any NIC configuration issues. Use these materials at your own risk. Stonesoft does not warrant or endorse any third party products described herein.

THESE MATERIALS ARE PROVIDED "AS-IS." STONESOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO, THE INFORMATION CONTAINED HEREIN. IN ADDITION, STONESOFT MAKES NO EXPRESS OR IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE WITH RESPECT THE INFORMATION CONTAINED IN THESE MATERIALS. IN NO EVENT SHALL STONESOFT BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL OR INCIDENTAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING FROM THE USE OF THESE MATERIALS, EVEN IF ADVISED IN ADVANCE OF THE POSSIBILITY OF SUCH DAMAGES.

Trademarks and Patents

Stonesoft, the Stonesoft logo and StoneGate are all trademarks or registered trademarks of Stonesoft Corporation. Multi-Link technology, Multi-Link VPN, and the StoneGate clustering technology—as well as other technologies included in StoneGate—are protected by patents or pending patent applications in the U.S. and other countries. All other trademarks or registered trademarks are property of their respective owners.