How to Provision a Windows* Web Server for Intel® AES-NI

Abstract:

This guide will review the steps to configure a server and client to use Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) when performing secure web transactions. Intel AES-NI provides significant performance improvements allowing the use of data protection not feasible before. Intel AES-NI is a set of seven new instructions in the Intel® Xeon® processor 5600 series (formerly codenamed Westmere-EP). The instructions are also available on certain desktop and mobile processors. Microsoft* Windows Server* 2008 Release 2 and Windows* 7, have built-in support for the new instructions. The steps outlined in this paper ensure the software is configuration to use this new capability.

1.1 Background Information

A secure web transaction, like accessing one's bank account, encrypts the data before sending it over the internet. Secure Socket Layer (SSL) and the newer Transport Layer Security (TLS) are the protocols typically used to deliver secure transactions over the network. When a client machine wants to securely access a server machine over TLS or SSL a handshake occurs to choose the encryption protocol. For the new instructions to be used, the AES cipher must be selected during the handshake. The encryption cipher is chosen based on the preferred order that is configured in the software. To use AES and therefore Intel AES-NI, the AES cipher should be first on each priority list. The web server should be configured to have the AES cipher as the preferred choice, highest on the cipher list. For the client computers under your control you want to also establish AES as the default cipher. These settings will be reviewed in the steps below to ensure they use the new capabilities offered by the Intel Xeon processor 5600 series.

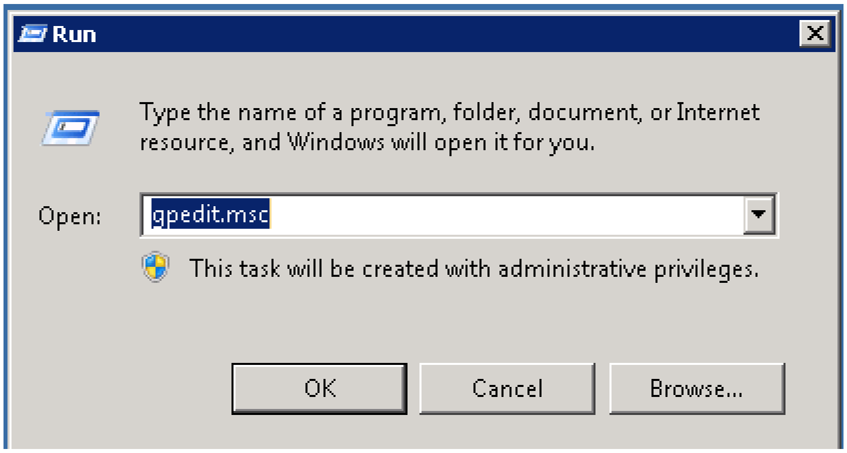
See http://www.intel.com/technology/security/ for more details on how Intel AES-NI works.

1.2 Server Configuration Settings

The following discussion is for web servers that use Microsoft Internet Information Services (IIS) with ASP.NET applications.

1. Launch the Local Group Policy Editor by executing GPEDIT in administrator mode from start-run dialog. (see Figure 1)
2. Select Computer Configuration → Administrative Templates → Network → SSL Configuration. (see Figure 2)

Figure 1- Launch the Local Group Policy Editor

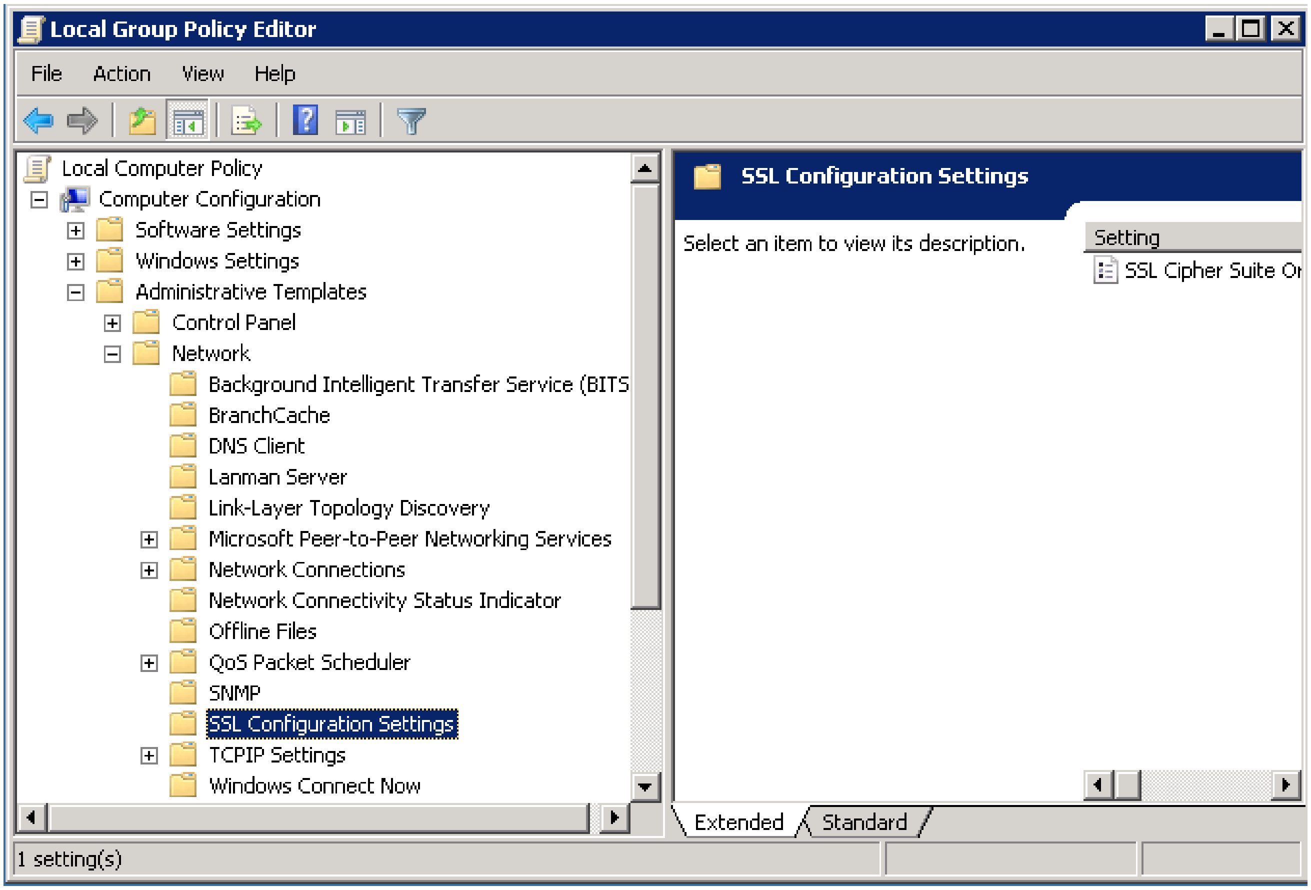


Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: gpedit.msc

This task will be created with administrative privileges.

Figure 2 – Select the SSL Configuration Settings



- Local Computer Policy
  - Computer Configuration
    - Software Settings
    - Windows Settings
    - Administrative Templates
      - Control Panel
      - Network
        - Background Intelligent Transfer Service (BITS
        - BranchCache
        - DNS Client
        - Lanman Server
        - Link-Layer Topology Discovery
        - Microsoft Peer-to-Peer Networking Services
        - Network Connections
        - Network Connectivity Status Indicator
        - Offline Files
        - QoS Packet Scheduler
        - SNMP
        - SSL Configuration Settings
        - TCPIP Settings
        - Windows Connect Now

SSL Configuration Settings

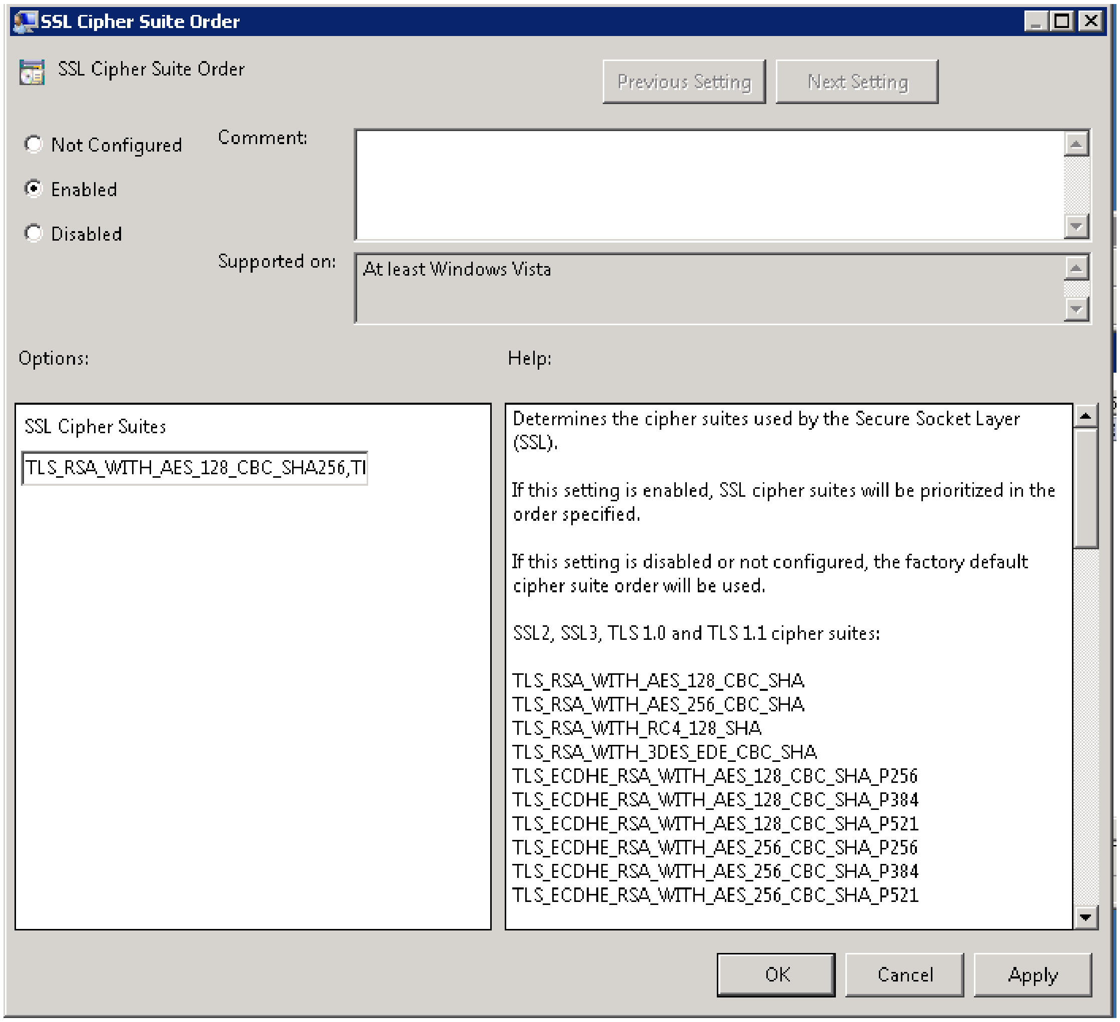
Select an item to view its description.

Setting
SSL Cipher Suite Or

1 setting(s)

3. Double click on SSL cipher suite order in the right hand pane. Select the enable button. Ensure TLS_RSA_WITH_AES_128_CB_SHA or TLS_RSA_WITH_AES_256_CB_SHA cipher is the first on the list in the SSL Cipher Suites text box on the left. (see Figure 3)
4. If it is not the first on the list carefully edit the list in the textbox to place it first.

Figure 3 - Ensure TLS_RSA_WITH_AES is First Cipher on the list



○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

SSL Cipher Suites

TLS_RSA_WITH_AES_128_CBC_SHA256,TI

Help:

Determines the cipher suites used by the Secure Socket Layer (SSL).

If this setting is enabled, SSL cipher suites will be prioritized in the order specified.

If this setting is disabled or not configured, the factory default cipher suite order will be used.

SSL2, SSL3, TLS 1.0 and TLS 1.1 cipher suites:

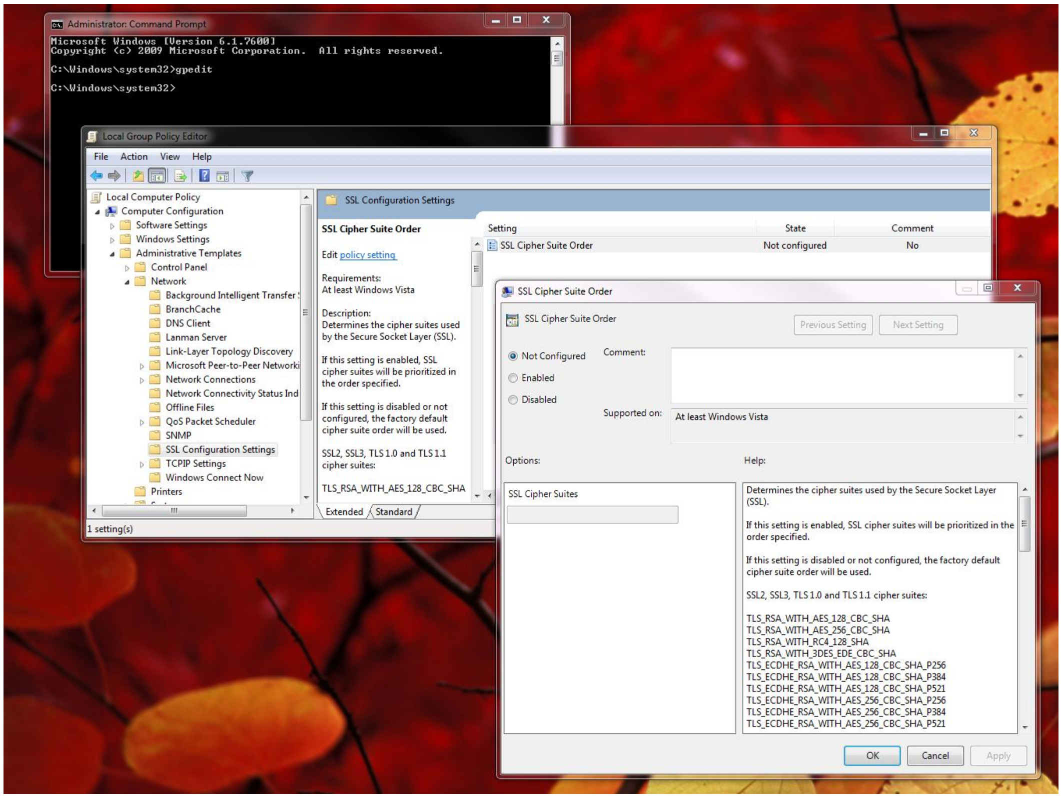
TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P521
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P521

1.3 Client Configuration Settings

Since the handshake picks the highest common cipher supported by both server and client, for the clients systems under your control establish AES as the default cipher.

1. Launch a Command Prompt in Administrator mode then execute the GPEDIT command. Note, GPEDIT is not available on lower-end versions of Windows 7
2. Choose Administrative Templates, Network, SSL Configuration Settings to confirm TLS_RSA_WITH_AES_128_CB_SHA or TLS_RSA_WITH_AES_256_CB_SHA cipher is the first on the list, which should be the default setting.

Figure 4 - Confirm TLS_RSA_WITH_AES_xxx_CBC_SHA is First Cipher on List



```
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>gpedit

C:\Windows\system32>
```

SSL Cipher Suite Order

Edit policy setting

Requirements:
At least Windows Vista

Description:
Determines the cipher suites used by the Secure Socket Layer (SSL).

If this setting is enabled, SSL cipher suites will be prioritized in the order specified.

If this setting is disabled or not configured, the factory default cipher suite order will be used.

SSL2, SSL3, TLS 1.0 and TLS 1.1 cipher suites:

TLS_RSA_WITH_AES_128_CBC_SHA

Setting	State	Comment
SSL Cipher Suite Order	Not configured	No

SSL Cipher Suite Order

● Not Configured
○ Enabled
○ Disabled

Comment:

Supported on: At least Windows Vista

Options:

SSL Cipher Suites

Help:

Determines the cipher suites used by the Secure Socket Layer (SSL).

If this setting is enabled, SSL cipher suites will be prioritized in the order specified.

If this setting is disabled or not configured, the factory default cipher suite order will be used.

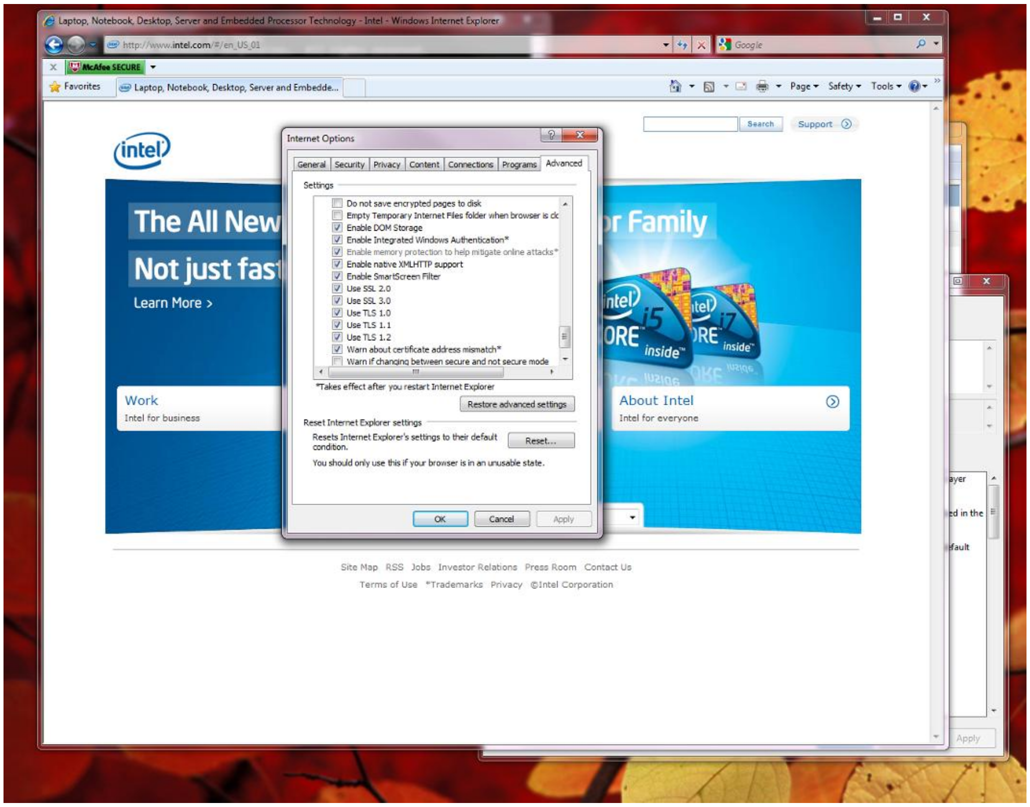
SSL2, SSL3, TLS 1.0 and TLS 1.1 cipher suites:

TLS_RSA_WITH_AES_128_CBC_SHA
TLS_RSA_WITH_AES_256_CBC_SHA
TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_3DES_EDE_CBC_SHA
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P256
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA_P521
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P384
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA_P521

3. Now open the Microsoft Internet Explorer browser
4. In the Advanced tab scrolls down to ensure that TLS 1.0 and higher are checked.

Note: Steps 3 and 4 are dependent on the specific browser used. These steps will vary if a different browser is used.

Figure 5 - Browser Must Have TLS Selected



Internet Options

Settings

- ☐ Do not save encrypted pages to disk
- ☐ Empty Temporary Internet Files folder when browser is cl
- ☑ Enable DOM Storage
- ☑ Enable Integrated Windows Authentication*
- ☑ Enable memory protection to help mitigate online attacks*
- ☑ Enable native XMLHTTP support
- ☑ Enable SmartScreen Filter
- ☑ Use SSL 2.0
- ☑ Use SSL 3.0
- ☑ Use TLS 1.0
- ☑ Use TLS 1.1
- ☑ Use TLS 1.2
- ☑ Warn about certificate address mismatch*
- ☐ Warn if changing between secure and not secure mode

*Takes effect after you restart Internet Explorer

Reset Internet Explorer settings

Resets Internet Explorer's settings to their default condition.

You should only use this if your browser is in an unusable state.

Laptop, Notebook, Desktop, Server and Embedded Processor Technology - Intel - Windows Internet Explorer
http://www.intel.com/#/en_US_01
Favorites
General
Security
Privacy
Content
Connections
Programs
Advanced
Restore advanced settings
Reset...
OK
Cancel
Apply
The All New
Not just fast
Learn More >
r Family
Work
Intel for business
About Intel
Intel for everyone
Search
Support
Site Map RSS Jobs Investor Relations Press Room Contact Us
Terms of Use *Trademarks Privacy ©Intel Corporation

1.4 Summary

The system is now provisioned for Intel AES-NI which can greatly accelerate the AES encryption algorithm in SSL.

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel may make changes to specifications and product descriptions at any time, without notice. All products, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice.

Performance tests and ratings are measured using specific computer systems and/or components and reflect the approximate performance of Intel products as measured by those tests. Any difference in system hardware or software design or configuration may affect actual performance.

Westmere and other code names featured are used internally within Intel to identify products that are in development and not yet publicly announced for release. Customers, licensees and other third parties are not authorized by Intel to use code names in advertising, promotion or marketing of any product or services and any such use of Intel's internal code names is at the sole risk of the user

Intel, Xeon and the Intel logo are trademarks of Intel Corporation in the United States and other countries.

*Other names and brands may be claimed as the property of others.