Legal Disclaimers & Copyrights

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

Intel technologies’ features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

The products described 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 disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

Intel, the Intel logo, and Intel Unite are trademarks of Intel Corporation in the United States and/or other countries.

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

© 2015 Intel Corporation. All rights reserved.
# Table of Contents

1  Intel Unite Firewall........................................................................................................................................4

1.1  Windows Firewall.....................................................................................................................................4

1.2  McAfee Host Intrusion Prevention........................................................................................................7

1.3  Symantec..................................................................................................................................................13
1 Intel Unite Firewall

This document is a guide to help configure firewall settings to allow Intel Unite application on the end user system. The three sub-sections have instructions on how to allow Intel Unite application on an end user system running Windows Firewall, McAfee Host Intrusion Prevention and Symantec Endpoint Protection agents respectively.

There are 2 ports that Unite listens on and these are randomly chosen by the OS on each launch. The Intel Unite application connects out to remote ports 80, 443 for HTTP and HTTPS connections and randomized ports on remote hubs.

A firewall exception has to be configured for Intel Unite.exe to allow UDP and TCP ports that are bound to the application.

1.1 Windows Firewall

1. In Control Panel, search for Windows Firewall and open the Allow an app through Windows Firewall.

2. Click on Allow another app at the lower right side of the window, you may have to click on Change Settings to activate the Allow another app button.
3. When the **Add an app** window opens, browse for **Intel Unite**.

4. Click on **Network Types**. then choose **Domain Network** and click **OK**.
5. Click **Add** to add the application to the allowed apps.
1.2 McAfee Host Intrusion Prevention

1. In the taskbar, click on the McAfee icon and from the opened menu, select → Manage Features → Host Intrusion Prevention.
2. Click on the Firewall Policy tab and then Click on Global Rules to expand to the options.
3. Select Intel Apps and click on Add..
4. In the name box, enter **Intel Unite**, then select **Either** in the Direction box and **Allow** in the Action box. Click **Next**.
5. In the **Network(s)** window select **IP Protocol** and check **IPv4 Protocol** in the **Network Protocol** box. In the **Media Type(s)** box, check all media types and add any local IP address depending on your organization's requirement. Click **Next**.
6. In the Transport window, use the dropdown menu in Protocol, select TCP. In the Remote Port (TCP and UDP Only) box, enter ports 80 and 443, as http (80) and https (443), click on Add, then click Next.
7. In the **Application** window, browse to the location of the application and add the Intel Unite.exe file. Click on **Finish** to complete the firewall setup.
8. After completing the Firewall Setup, verify that the policy has been added by checking the Firewall Policy tree, as shown below, **Firewall is enabled.**
1.3 Symantec

1. Open Change Settings - Symantec End point Protection on the client

2. In the setting Network Threat Protection (3rd option shown above), click on Configure Settings.
3. Select **Configure Firewall Rules**.

4. Click on **Add..** to add a firewall rule.
5. Enter **Intel Unite** in the **Rule name** box and select **Allow this traffic**.
6. In the **Firewall settings** box, select **All network adapters** and click **OK**.
7. In the **Hosts** tab, select the appropriate option, to either apply the rule to all hosts or a set of hosts within a subnet.
8. In the **Ports and Protocols tab**, select **TCP** for the **Protocol** rule and for **Remote ports** select 80 and 443 for HTTP and HTTPS respectively.
9. In **Traffic direction** select **Both**.
10. Add another rule for **UDP** protocol, all ports and **Traffic direction** as **Both** for this rule.

11. In the **Applications** tab, browse to Intel **Unite.exe** and click **OK**.
12. Finally, verify the rule has been added by checking the list of firewall rules.