

Intel[®] Unite[™]

Standalone Setup Guide



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	Introdu	uction	4
	1.1	Intel Unite Terminology	4
	1.2	Intel Unite Overview	
2	Intel U	nite Standalone Requirements	6
	2.1	Software Requirements	6
	2.2	Hardware Minimum Requirements	6
	2.3	Network Recommendations	6
3	Intel U	nite Standalone Installation	7
	3.1	Getting Started	7
	3.2	Intel Unite Hub Installation	7
	3.3	Selecting a Shared Key	10
	3.4	Intel Unite Client Installation	12
	3.5	Launching Intel Unite	15
4	Advand	ced Configuration	17
	4.1	Advanced Configuration (Hub Configuration)	17
	4.2	Valid Keys for Configuration	18
APPENDIX A			20
	Help G	uide to Configure Firewall Settings	20
	A1	Windows Firewall	20
	A2	McAfee Host Intrusion Prevention	23
	A3	Symantec	29



1 Introduction

Welcome to the Intel[®] Unite[™] Standalone Setup Guide. Intel Unite modernizes meeting spaces for a better way to work, with a simple application, you can create an innovative conference space anywhere a display is located, allowing functionality, communication, and flexibility while incorporating business needs.

Intel[®] Unite[™] Standalone was designed for use by Small Business Professionals, where there is no a dedicated IT department, little to no networking or computer security knowledge is needed.

Businesses using Intel Unite Standalone is recommended for up to 25 users, in no more than 5 conference rooms or simultaneous sessions, (recommendation: 25 users and 5 conference rooms).

1.1 Intel Unite Terminology

Through this setup guide the following terms will be used:

Client - Client software installed on a client system and connects to a hub

Hub – a system that is displaying a PIN and hosting plugins as in a conference room display

IP Address – Internet Protocol Address

Plugin - a software component installed on a hub that surfaces additional functionality

Flat Network - a network in which all stations can reach other without going through any intermediary hardware devices, such as a bridge or router

Shared key – it refers to a key that would be shared among participants in Intel Unite sessions. Only Intel Unite Hubs and Clients that use the same shared key will be able to participate in collaboration sessions

1.2 Intel Unite Overview

Intel Unite software is designed to allow fast wireless screen sharing and collaboration in few steps:

- Get to a display where Intel Unite is installed
- Launch the client application in your device
- Enter the Shared Key provided by the Administrator
- Enter the PIN number displayed in the Hub to connect to a specific session
- Once you are connected , click 'Share' to display content

Intel Unite uses a non-touch display and can support any size monitor. User interaction is limited to wireless display but includes easy connection via PIN entry and easy handover between presenters.

Once Intel Unite has been installed, the Hub creates its own WiFi hotspot, displaying the instructions for the clients to connect to this hotspot. The Intel Unite Software should be downloaded in each client that connects to the Intel Unite session.



	Intel Unite Features
Wireless Display from Anywhere	Users can connect to a session and display their screen or display, no cables needed to connect to a projector
Up to 4 Split Screen View	Multiple users can connect and share concurrently to the same monitor/ display or projector
File Transfer	Users can send and receive files during sessions
Interactive Participant List	Users can see all participants connected to the same session. The user list includes avatars, location, presenters and sharing status.
Annotation	Users can make annotations on the presenter's display, this is a simple and instant collaboration tool
Supported Clients	Works with v-Pro Platforms, Client App Microsoft [®] Windows 7, 8.1, 10, Mac [®] OS X



2 Intel Unite Standalone Requirements

Please verify that the software, hardware and network requirements are met as specified below.

2.1 Software Requirements

HUB	Client
 Microsoft[®] Windows 7, 8, 8.1 or 10 Microsoft[®] .Net 4 	 Microsoft[®] Windows 7, 8, 8.1 or 10 Microsoft[®] .Net 4 Mac[®] OSX 10.9 or greater

2.2 Hardware Minimum Requirements

HUB	Client
 System meeting the Intel[®] vPro Technology 4 GB RAM Wired or Wireless Network Connection 32GB available storage 	1 GB Ram1 GB available storage

2.3 Network Recommendations

Intel Unite Standalone requires a Flat Network which is typically used in homes or small businesses where network requirements are low.

It is recommended, but not required, to connect all hubs to a wired LAN for these two reasons:

- 1. The display quality of high frame rate improved over LAN compared to WLAN
- 2. WWLAN infrastructure bandwidth optimization through avoiding the room system to access point WLAN traffic



3 Intel Unite Standalone Installation

3.1 Getting Started

- 1. If a Mini-PC would be used as Hub, connect it to the monitor that will be used with Intel Unite, using the cables contained in the box.
- 2. Browse the drive of the Mini-PC or the PC to be used as a Hub, and identify the location of the folder or media provided containing the 2 Intel Unite installers:
 - Hub Installer : Intel Unite Hub.mui.msi
 - Client Installer: Intel Unite Client.mui.msi
- 3. Start with the Hub installation, then you will continue with the Client installation

3.2 Intel Unite Hub Installation

- 1. Locate the installer folder and run the file for the Hub: Intel Unite Hub.mui.msi
- 2. The Intel Unite Setup window will be displayed

6		Intel® Unite™ Setup	– – ×
(int	el	Welcome to the Intel® Unite Wizard	e™ Setup
		The Setup Wizard will install Intel® Unite [†] computer. Click Next to continue or Cance Wizard.	
		Back Next	Cancel

- 3. Click Next to continue.
- 4. The End-User License Agreement window will be displayed



17	Intel® Unite™ Setup 📃 🗖 🗙
E	End-User License Agreement Please read the following license agreement carefully
	Intel® Unite TM Software End User License Agreement
	IMPORTANT - READ BEFORE COPYING, INSTALLING OR USING. Do not copy, install, distribute, publicly display, or use the software and the accompanying documentation ("Software") until you ("You") have carefully read and agreed to the following terms and conditions.
	This agreement ("Agreement") forms a legally binding contract between You and Intel Corporation ("Intel") (collectively, the "Parties") regarding Your use of the Software. By copying, installing, distributing, publicly displaying, or otherwise using the Software, You agree to be bound by the terms of this Agreement. If You do not agree to the terms of this Agreement, do not copy, \vee
	☑ I accept the terms in the License Agreement
	Print Back Next Cancel

5. Check the box I accept the terms in the License Agreement and click Next to continue

₿	Intel® Unite™ Setup – □ ×
C	Choose how to install Intel® Unite™. Install Intel® Unite™ with Enterprise or Standalone settings.
	Enterprise: For use in business environments with multiple office locations (● and networks. This option requires Intel® Unite™ enterprise server components. O Standalone: Designed for simple installations on a single business network. This option does not require any server components.
	<u>B</u> ack <u>N</u> ext Cancel

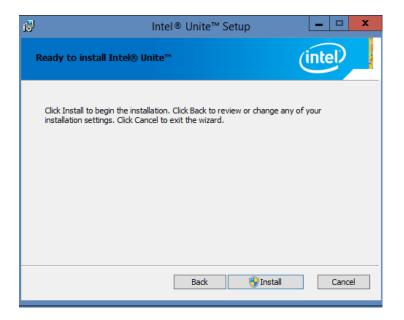
6. Select **Standalone** and click **Next** to continue.

7. The next section will prompt you to select a **Destination Folder**, click **Next** to accept the default. In this step you can also create a desktop icon.



15	Intel® Unite™ Setup
	Destination Folder Click Next to install to the default folder or click Change to choose another.
	Install Intel® Unite™ to:
	C:\Program Files (x86)\Intel\Intel Unite Standalone\Hub\ Change
	Create a desktop icon
	Back Next Cancel

8. When you see the **Ready to install Intel Unite** window, you can go back to review your settings or click on **Install** to continue. You can also Cancel the installation.



9. Once the installation has ended, you will see the **Completed the Intel Unite Setup Wizard** window.



₿		Intel® Unite™ Setup 📃 🗖 🗙
	(intel)	Completed the Intel® Unite™ Setup Wizard Click the Finish button to exit the Setup Wizard.
		✓ Launch Intel® Unite™ application
		Back Finish Cancel

10. Click **Finish** to end the Hub installation process, make sure you launch the application (select box **Launch Intel Unite**), we needed launched in order to continue with the next step.

3.3 Selecting a Shared Key

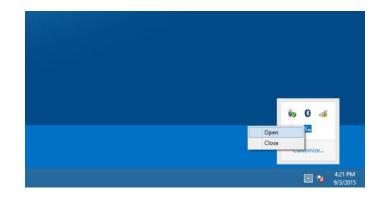
After the Hub installation has ended, proceed to select a Shared Key. A common password, known here as Shared Key, must be created in order for the Clients to access the application, it is used to enhance security. Only Intel Unite Hubs and Clients that use the same shared key will be able to participate in a collaboration session.

- 1. You must select a Shared key that will be used by Intel Unite session participants or presenters. Please note that all systems must have the same Key (access password) to communicate. The shared key is at least 8 characters, you can have any combination of characters (alphanumeric, numeric, symbols, etc.).
- 2. Go to the task bar, find the Unite icon, make sure the Hub has been launched, otherwise the icon will not appear in the task bar.



3. Right click on the unite icon, when the Open/Close menu opens, select Open.





4. The following window will be displayed:

инте	Intel® Unite™	- 🗆 🗙
Current Pin		\mathbf{C}
932-28	6	ĸ
Access Password		Apply
(1	nust be 8 characters or lon	ger)
Exit Application		

- 5. Select and enter the 8 character Access Password which will become the **Shared Key**.
- 6. Click on **Apply** and then on **Exit Application** to close this window.
- 7. The Shared Key window each Client will see when launching Intel Unite is the following:

-	Shared Key
UNITE	The Intel Unite application requires a shared key to allow you access to other Intel Unite devices in your environment. Please set your shared key below to use the Intel Unite application.
S	hared Key

8. Continue with the Intel Unite Client installation.



3.4 Intel Unite Client Installation

- 1. Locate the installer folder and run the file for the Client: Intel Unite Client.mui.msi
- 2. The Intel Unite Setup window will be displayed



3. Click **Next** to continue.

nd-User License Please read the fol	Agreement lowing license agreement carefully	(intel)
Intel®	Unite TM Software End User Li	icense Agreement
Do not copy, inst accompanying do	EAD BEFORE COPYING, INS all, distribute, publicly display, cumentation ("Software") until o the following terms and condi	or use the software and the you ("You") have carefully
and Intel Corpora of the Software. otherwise using	'Agreement'') forms a legally b tion ("Intel") (collectively, the By copying, installing, distrib the Software, You agree to be ou do not agree to the terms of	"Parties") regarding Your use outing, publicly displaying, or
✓ I accept the terr	ns in the License Agreement	
		an 100 m

3. Check the box I accept the terms in the License Agreement, and click Next



1	Intel® Unite™ Setup – □ ×
	Choose how to install Intel® Unite™. Install Intel® Unite™ with Enterprise or Standalone settings.
	Enterprise: For use in business environments with multiple office locations ● and networks. This option requires Intel® Unite [™] enterprise server components. Ostandalone: Designed for simple installations on a single business network. This option does not require any server components.
	Back Next Cancel

- 4. Select **Standalone** and click **Next** to continue.
- 5. The next section will prompt you to select a **Destination Folder**, click **Next** to accept the default. In this step you can also create a desktop icon.

_ 🗆 🗡			ntel® Unite™ Setup
D	(intel	t folder or dick Change to choose anoth	estination Folder Click Next to install to the default fol
			Install Intel® Unite™ to:
		Unite Standalone \Client \	C:\Program Files (x86)\Intel\Intel Un Change
			🔽 Create a desktop icon
- 1			
	Can	Back Next	

6. When you see the **Ready to install Intel Unite** window, you can go back to review your settings or click on **Install** to continue. You can also Cancel the installation.



₿	Intel® Unite™ Setup	- • ×
F	Ready to install Intel® Unite™	(intel)
	Click Install to begin the installation. Click Back to review or change any installation settings. Click Cancel to exit the wizard.	/ of your
	Back 🛞 Install	Cancel

7. Once the installation wizard has ended, you will see the **Completed the Intel Unite Setup Wizard** window.

(intel)	Completed the Intel® Unite™ Setup Wizard
	Click the Finish button to exit the Setup Wizard.

8. Select the **Launch Intel Unite application** box if you wish to open the application, or click **Finish** to end the Client installation process. If you choose to launch the application in the Client continue to the next section.



3.5 Launching Intel Unite

Once the installation has finished, launch the Client application, before it opens, you may get the Privacy Statement window and the Shared Key window.

- 1. **Privacy Statement:** The Intel Unite Privacy Statement function is used to collect anonymous usage data. Intel is always looking to improve its products and would like to collect data to continue to improve the product. Please select **YES** or **NO** and check the box if you do not want to show the dialog box again.
- 2. Then the **Shared Key** window will be displayed.

Shared Key		×
UNITE	The Intel® Unite [™] application requires a sha key to allow you access to other Intel® Unite devices in your environment. Please set your shared key below to use the Intel® Unite [™] application.	
	Арр	ly

- 3. Enter the **Shared Key** provided by the system Administrator and click on **Apply.** Remember to use the same Shared Key later on.
- 4. The following **Connect to a screen** window appears:

1	2	3
4	5	6
7	8	9
<	0	Clear



5. To connect to an Intel Unite session, enter the PIN displayed in the Hub/ monitor you wish to connect.



6. Once connected, you can click on "Share" if you wish to present or show the Intel Unite session.

NOTE: If you are having problems connecting, make sure the firewalls are disabled or have exceptions in place for Intel Unite.exe. **APPENDIX A** of this guide will guide you to configure Firewall Settings.



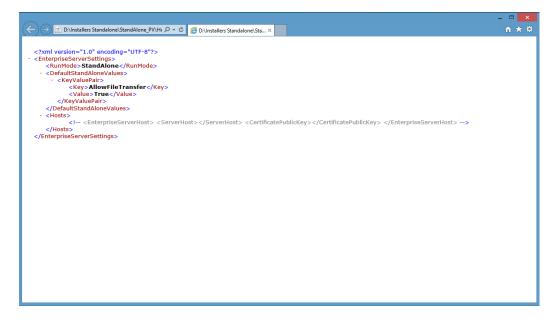
4 Advanced Configuration

4.1 Advanced Configuration (Hub Configuration)

The Intel Unite Hub can be customized to fit the needs of your organization. Additional options allows you to add a theme to the hub, or enable/disable features such as file share, this a manual editing process.

Additional configuration requires you to manually modify the "serverconfig.xml" settings file. This file can be found in the installation path (default: C:\Program Files (x86)\Intel\Intel Unite\Hub\ServerConfig.xml).

Here is an example of the contents of ServerConfig.xml:



Within **DefaultStandAloneValues**, you can specify additional settings (KeyValuePair) on the hub application. <u>Example:</u>

```
<DefaultStandAloneValues>
<KeyValuePair>
<Key></Key>
<Value></Value>
</KeyValuPair>
<KeyValuePair>
<Key></Key>
<Value></Value>
</KeyValuePair>
.
.
.
```



4.2 Valid Keys for Configuration

This table outlines the valid Key/Value pairs:

Key	Description	Data Type	Default Value
DisplayPinSize	Size in Pixels. The value is the height in pixels for the onscreen pin (larger values make the pin easier to read from across the room)	Integer	48
TileCompression	JPG compression level. % of compression to apply to a changed portion of the display (tile) being transmitted over the network	Integer	80 (valid range: 5-100)
TileSize	Tile size for breaking screen into chunks. The size, in pixels, for each tile. A tile is a section of the screen which is evaluated for change. Only changed tiles are transmitted	Integer	128 (valid range: 32-512)
ServiceListenPort	The TCP port that the service should listen on	Integer	0 (0 indicates OS assigned port)
FileMaxSize	Max file size for file transfers	Integer	2000000000 (2GB) (valid range: 0-2GB)
FileBlockedExtensions	Comma separated list of blocked file extensions	String (example: exe, bin)	
FullScreenRoomMode TextColor	Text color of onscreen text	Hex Color Code (Example: #ffffff)	
FullScreenRoomMode PinColor	Text color of PIN	Hex Color Code (Example: #ffffff)	
FullScreenRoomMode TextFont	Name of font for instructions	String (Example: Ariel)	



	-		
AllowFileTransfer	Flag to enable/disable the ability for a hub or client to transfer a file	Boolean (True or False)	True
HubLockKeyboard	Lock out the following: Ctrl-Esc, Alt-Tab, Charms bar, Windows keys and Alt-F4 in Hub If set to True hub lock out is enabled. Can override with password set in Reg Key Machine	Boolean (True or False)	False
HubShowClock	Show clock in bottom right corner	Boolean (True or False)	True
FullScreenRoomMode	Enable/disable hub full screen False: Pin in upper right only True: Pin in upper right and a full screen background	Boolean (True or False)	True
FullScreenRoomMode BackgroundURL	Sets the Hub background to the URL or image (jpg/png) specified. Set value to True if you want this feature Example: http://myserver.com/background.jpg	Boolean (True or False)	(none)
FullScreenRoomMode BackgroundColor	Background color of the Hub. Named color or html style color Valid values are named colors or RGB values/HTML colors in the format: #000000 (For example red is #FF0000)	Hex Color Code	(none)
FullScreenRoomMode ShowPin	Show instructions. Set value to True if you want this feature.	Boolean	True
FullScreenRoomMode Instructions	Text instructions to be displayed on Hub. can use {pin} and {host} as replacements URL for download of the client. This item is displayed on the full screen room mode screen.	String	
VerifyPluginPublicKey	Verify plugin public key before loading plugins	Boolean	False



APPENDIX A

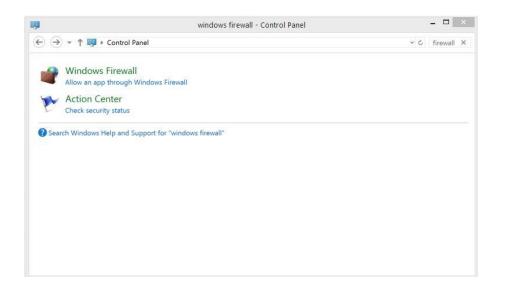
Help Guide to Configure Firewall Settings

Users need to ensure the operating system firewalls have exceptions in place for Intel Unite.exe (both TCP and UDP). A firewall exception has to be configured for **Intel Unite.exe** to allow UDP and TCP ports that are bound to the application.

This section 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.

A1 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.



Allow apps to communicate through Windows Firewall To add, change, or remove allowed apps and ports, click Change settings. What are the risks of allowing an app to communicate? Image: communicate Image: communicationsapp: 17.4 secon 1044.
To add, charge, or remove allowed apps and ports, click Charge settings. What are the risks of allowing an app to communicate?
What are the risks of allowing an app to communicate? Image: calculate the risks of allowing and app to communicate? Image: calculate the risks of allowing and point and restricts Image: calculate the risks of allowing and restricts Allowed apps and features: Image: calculate the risks of allowing and restricts Image: calculate the risks of the
For your security, some settings are managed by your system administrator. Allowed apps and features: Name Domain Private Public Group Policy Ø jointorsoft kindowscommunicationsapps, 17,4,600,1638, Ø No Ø jointorsoft kindowschedinglist, 5,3,000,1638, Jointo, B No Ø jointorsoft kindowschedinglist, 5,3,000,1638, Jointo, B No Ø jointorsoft kindowschedinglist, 5,3,000,1638, Jointo, B No Ø jointorsoft kindowsRedinglist, 5,3,000,1638, Jointo, B No Ø jointorso
Allowed apps and features: Name Domain Private Public Group Policy Ø @ Intercrost and/ovscommunicationsapps 17.4.500.1638. Ø No No Ø @ Intercrost and/ovscommunicationsapps 17.4.500.1638. Ø No No Ø @ Intercrost and/ovscommunicationsapps 17.4.500.1638. Ø No No Ø @ Intercrost and/ovscommunicationsapps 17.4.500.01638.4.64.8m. Ø No Ø @ Intercrost And/ovschadmigstat 6.3.6000.1638.4.64.8m. Ø No Ø @ Intercrost VindowsReadmigstat 6.3.6000.1638.4.64.8m. Ø No Ø @ Intercrost VindowsReadmigstat 6.3.6000.1638.4.64.8m. Ø No Ø @ Intercrost VindowsReadmigstat 6.3.6000.1638.4.64.8m. Ø No Ø E S Client (CNP4) Ø Ø No Ø E S Client (CNP4) Ø Ø No
Name Domain Private Public Group Policy Ø [Privirosoft windowscommunicationsapps; 17.4.4900.1034. Ø Ø No Ø [Privirosoft windowscommunicationsapps; 17.4.4900.1034. Ø Ø No Ø [Privirosoft windowscommunicationsapps; 17.4.4900.1034. Ø Ø No Ø [Privirosoft windowscommunicationsapp; 17.4.4900.10384. Ø Ø No Ø [Privirosoft WindowsReadingList_5.4.504.00.10384.pd4Bwill Ø Ø No Ø [Privirosoft WindowsReadingList_5.3.4900.10384.pd4Bwill Ø Ø No Ø [Privirosoft WindowsReadingList_5.3.4900.10384.pd4_Bwill Ø Ø No Ø [Privirosoft WindowsReadingList_5.3.4900.
Implementation Impleme
Ø (#)microsoft windowscommunicationsapp: 17.4.960.1381. Ø No Ø (#)microsoft windowscommunicationsapp: 17.4.960.1384.v648w Ø Ø No Ø (#)microsoft windowsceadingLinf_5.3.960.1384.v648w Ø Ø No Ø (#)Microsoft WindowsReadingLinf_5.3.960.1384.v648w Ø Ø No Ø (#) Afficiant (#) (#) (#) (#) (#) (#) (#) (#) (#) (#)
Ø (#)microsoft windowscommunicationsapp: 17.4.960.1381. Ø No Ø (#)microsoft windowscommunicationsapp: 17.4.960.1384.v648w Ø Ø No Ø (#)microsoft windowsceadingLinf_5.3.960.1384.v648w Ø Ø No Ø (#)Microsoft WindowsReadingLinf_5.3.960.1384.v648w Ø Ø No Ø (#) Afficiant (#) (#) (#) (#) (#) (#) (#) (#) (#) (#)
Ø@Microsoft.WindowsReadingList_63.9600.16384_y54_8w Ø No Ø@Microsoft.WindowsReadingList_63.9800.16384_y54_8w Ø No Ø@Microsoft.WindowsReadingList_63.9800.16384_y54_8w Ø Ø No Ø@Microsoft.WindowsReadingList_63.9800.16384_y54_8w Ø Ø No Ø@ESC.Client CUMP44 Ø Ø Ø No ØESC.Scient (CUMP44) Ø Ø Ø No ØESE.Scient (CUMP44) Ø Ø Ø No
Ø @ Netrosoft. WindowsReadingList_6.3.9400.1584_0468m. Ø Ø No Ø @ Netrosoft. WindowsReadingList_6.3.9450.4.25349_4648m. Ø Ø Ø No Ø IBES Client Ø Ø Ø No Ø Ø No Ø ISES Client Ø Ø Ø No Ø Ø No Ø ISES Client OLMPAN Ø Ø Ø No Ø ISES Client OLMPAN Ø Ø No
29 @ Microsoft.WindowsReadingList_6.3.9400.16384_1640Hv. 27 27 No 29 @ Microsoft.WindowsReadingList_6.3.9654.20349_0640Hv. 27 27 No 20 ES Client Client 27 27 No
년 BES Client 전 년 년 No 전 BES Client (CMP4) 년 년 년 No 전 BES Client (CMP4) 년 년 년 No
전 EES Client 전 전 전 전 No 전 EES Client (CMP4) 전 전 전 No 전 EES Client (CMP4) 전 전 전 No
ØBES Client (ICMPv6) Ø Ø Ø No
ØBES Client (ICMPv6) Ø Ø No
BranchCache - Hosted Cache Client (Uses HTTPS)
BranchCache - Hosted Cache Server (Uses HTTPS)
BranchCache - Peer Discovery (Uses WSD)
Details Remov
Allow another ap
Allow another ap

3. When the Add an app window opens, browse for Intel Unite.

	Ad	dd an ap	р	X
	pp you want to add, hen click OK.	or click Brov	wse to find one	that is not
Apps:				
💿 Google	Chrome			^
🛛 🧱 GUID G	enerator			
🛛 🐴 НР Муғ	Room			
📝 IL Disa:	ssembler (x64)			
Intel So	oftware Market			
Intel(R) PROSet Wireless T	ools		
Intel(R				
) WiDi Remote			
	HD Graphics Control			
-	Management and S	ecurity Statu	5	
ាក Intel®				
C Interne	t Explorer			*
Path:	C:\Program Files (x86)\Intel\In	tel Unite\Clier	Browse
What are the	e risks of unblocking	an app?		
You can choo	ose which network t	ypes to add t	his app to.	
Netwo	ork types		Add	Cancel

- 4. Click on **Network Types...**
- 5. In the **Choose Network Types** window, select **Domain: Networks at a workplace that are attached to a Domain** and click **OK**.



indows Firewall →	Allowed apps		
Allow apps to	communicate through Windows Firewall		
	remove allowed apps and ports, click Change settings.		
	of allowing an app to communicate?		😚 Change settings
what are the risks o	or allowing an app to communicate?		Change settings
For your sec	Add an app	×	
Allowed apps ar	Select the app you want to add, or click Browse to find one listed, and then click OK.	that is not	
Name	nacca, and then ener ore		roup Policy
☑ @{microsoft.	Apps:		No
☑ @{microsoft.	😨 Google Chrome	^	No
🗹 @{microsoft.	GUID Generator		No
☑ @{Microsoft	P MyRoom		No
☑ @{Microsoft	🗾 IL Disassembler (x64)		No
☑ @{Microsoft	😭 Intel Software Market		No
BES Client	Intel(R) PROSet Wireless Tools		Chapse Natwork Types
BES Client (IC	Intel(R) WiDi		Choose Network Types
BES Client (IC	Intel(R) WiDi Remote		
BranchCache	Sintel® HD Graphics Control Panel		p or port to communicate through Windows he selected network type:
BranchCache	Intel® Management and Security Status		
BranchCache	Intel® Unite™		in: Networks at a workplace that are ed to a domain
BranchCache	C Internet Explorer	decours	
	Path: C:\Program Files (x86)\Intel\Intel Unite\Clier		e: Networks at home or work where you
		know a netwo	and trust the people and devices on the
	What are the risks of unblocking an app?	netwo	16
	You can choose which network types to add this app to.		: Networks in public places such as ts or coffee shops
	Network types Add		

- Click Add to add the application to the allowed apps.
 You have allowed Intel Unite in your Windows Firewall.



A2 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 General window, enter **Intel Unite** in the name box, then select **Either** in the Direction box and **Allow** in the Action box. Click **Next**.

Action and Directi Enter a name, se	ect an action and direction, and indicate whether the rule is enabled.	
Name:		
Intel Unite		
🔽 Enabled		
Direction		
⊖ In		
◯ Out		
Either		
Action —		
Allow	Treat as intrusion	
O Block	Log matching traffic	



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 organizations requirement. Click **Next.**

IP Protocol	O Non-IP Protocol
IPv4 Protocol	0x
IPv6 Protocol	,
Vireless	🔽 Virtual
	Add
	Remove
	✓ IPv4 Protocol □ IPv6 Protocol



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**.

Note: 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.

Δ	Transport	×
Protocol and Ports Select an appropriate	protocol, then indicate port(s), if necessary.	
Protocol:	•	
Local Port (TCP and U		Add
		Remove
Remote Port (TCP and	UDP Only) thttp (80) https (443)	Add
		Remove
Message Type (ICMPv4	I and ∨6 Only):	
,	_	
	< Back Next > Finis	sh Cancel



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.

Μ		Applica	ation			X
Application Select an app	lication.					
Application					_	1
Application	i 🖬 Intel® Unitel (In	tel Unite.exe)		-	Browse	
		< Back	Next >	Finish	Cancel	



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**.

					McAfe	e Hos	t Intru	usion	Prev	entio	n			_)
sk Edit	View H	elp														
S Policy	<u>F</u> irewall	Policy	Blocked	Hosts	Applicatio	n Proter	rtion List	Activ	tv Log							1
oroney		,	Diocided		repriced			1,100	9 209							1
	Use this ta	1b to er	able or di	sable fi	rewall pro	ection a	nd creat	e or ed	t firewal	l client r	ules.					
✓ Enabl	ed								Т	ructod N	letworks	1				
	Learn Mod				🗖 Ada	ntivo Me	do			rusteur						
					E Auo	puve m <u>e</u>										
	Incomir															
	C Outgoir	ıg														
-	🕥 Windov	vs AD A	uthenticatio	on											^	
y 🕀	NetBIO	s														
y 🗄	Networ	k Tools														
	Endpoi		rotion													
	Loopba															
	VPN															
		Kerberr	ne -													
			15 0 01													
															- 10	
-	Inside Intel															
-	Outside Inte		rusted Net	work												
_	🔂 🐳 Inte															
	📕 Path =				IlIntel Unite	Client\In	itel Unite.	exe								
	— Descrij	otion = I	ntel® Unite	711												
	— Signer	= CN=l	ntel(R) Unit	e(tm) Si	igning Cert	ficate, O=	Intel Cor	poration	n, L=San	ta Clara	S=CA, C	=US				
	— Hash =	AC536	1D2123FE	C8FF85	598B82DE0	80875										
-	Network La	yer Pro	tocol(s) = If	Pv4												
	IP Protocol	= TCP														
	Remote Po	rt(s) = h	ttp (80), htt	ps (443))											
	😑 🐳 Bloo	:k All Tra	affic												~	
		Prop	erties	1	<u>D</u> uplica	te		<u>R</u> emov	8		Add		1	Apply		
	nabled			_				_	_		_					

9. You have allowed Intel Unite in your McAfee Firewall.



A3 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.

Status Scan for Threats Change Settings		There are multiple warnings (2					
Scan for Threats			2)		Deta	ils	
Change Cattings		Proactive Threat Protection is malfunction	oning.				
		Protection definitions are unusable.					
		Click Details for more information.					
View Quarantine 📙						_	
View Loas	The fe	nfigure Firewall Rules	had on your o	orgador (
	Fir	rewall rules allow, block, and log network traffic.					
LiveUpdate		Rule Name	Hosts	Ports and Protocols	Action	Network Adap	ot Sched
Liveopuate		Block IPv6 (Ethernet type 0x86dd)	All hosts	ethernet type 34525; both inco	Block	All network ad	Sched
		Block IPv6 over IPv4 (Teredo) Remote UDP port 3544	All hosts	UDP remote port(s) 3544; both	Block	All network ad	Sched
		Block IPv6 over IPv4 (ISATAP)	All hosts	IP protocol type 41; both inco	Block	All network ac	Sched
		Allow common ICMPv6 traffic	All hosts	ICMPV6 type 1-4,128-132,141	Allow	All network ac	Sched
		Allow EAPOL wireless traffic	All hosts	ethernet type 0x888E; both inc	Allow	All network ad	Sched
		Allow BOOTP protocol	All hosts	UDP local port(s) 68,67; both i	Allow	All network ac	Sched
		Allow UPnP Discovery from private IP addresses	10.0.0.0-10.25	UDP local port(s) 1900; both in	Allow	All network ac	Sched
		Block UPnP Discovery	All hosts	UDP local port(s) 1900; both in	Block	All network ad	Sched
			10.0.0-10.25		Allow	All network ac	I Sched
			10.0.0-10.25			All network ac	
		Z Block Web Service requests part A	All hosts	TCP local port(s) 5357,5358; b	Block	All network ad	
		Block Web Service requests part B	All hosts	UDP local port(s) 5357,5358; b		All network ad	
		Allow Ipv4 LLMNR from private IP addresses	10.0.0-10.25		Allow	All network ac	
		Block Ipv4 LLMNR	0.0.0.1-255.25	UDP local port(s) 5355; both in		All network ac	
de .		Z Allow Ipv6 LLMNR	All hosts	UDP local port(s) 5355; both in		All network ad	
Symantec.		Allow Web Services Discovery from private IP addre	10.0.0-10.25	UDP local port(s) 3702; both in	Allow	All network ac	Sched
		Add Edit Delete 1					

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.

U Add Firewall Rule	ζ
General Hosts Ports and Protocols Applications Scheduling	
Rule name	
Intel Unite	
Action	
Block this traffic Allow this traffic	
Firewall settings	
Apply this rule to the following network adapter:	
All network adapters	
Apply this rule while the screen saver is:	
Either On or Off 🔹	
Record this traffic in the Packet Log	
Rule Summary: Allow both incoming and outgoing traffic to/from: All hosts. This applies to traffic from the following protocols and ports: All IP protocol types. For these network adapters: All network adapters.	
OK Cancel Help	

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.

Apply this rule to: All hosts		
MAC address:		
 IPv4 addresses: IPv6 addresses: 	Example: 10.0.0.1, 192.168.0.1-192.168.0).76
IPv4 Subnet	Subnet IP address:	
IPv6 Subnet	Subnet mask:	
	oing traffic to/from: All hosts. This applie All IP protocol types. For these network	
dapters.		



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.

Note: 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.

U Edit Firewall Rule	X
General Hosts Ports and Protocols Applications Scheduling	
Apply this rule to	
Protocol: TCP 🗸	
Example: 80, 1450, 1024-1209	
Remote ports: 80,443	
Local ports:	
Traffic direction: Both	
Rule Summary: Allow both incoming and outgoing traffic to/from: All hosts. This applies to traffic from the following protocols and ports: TCP remote port(s) 80,443. For these network adapters: All network adapters. The following applications will be affected by this rule: Intel® Unite [™] .	*
OK Cancel He	elp

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**.



	eral Hosts Ports and Protocols		Is Applications Scheduling		
Applica	tions:			Display selected	applications only
Applic	ation		Version	Path	
Intel® Unite™			1.0.12.8	C:\Program Files (x86)\In	tel\Intel Unite\Client\Int
	Sele	ect All		Unselect All	Browse
	tion Path				
C-\Drog		s (xoo)/iii	itel/intel On	te\Client\Intel Unite.exe	
			l outaoina t	affic to/from: All hosts. This ap	oplies to traffic from the
Rule St		ning and		remote port(s) 443. For these i	
Rule Su Allow b followin	oth incor g protoc		ports: TCP	emote polit(s) 445. Politilese i	network adapters. An network
Rule Su Allow b followin adapte	oth incor g protoc rs.	ols and p		fected by this rule: Intel® Unite	

- Finally, verify the rule has been added by checking the list of firewall rules.
 You have allowed Intel Unite in your Symantec Firewall.