Intel® Unite™ Solution

Plugin Guide for Protected Guest Access

July 2016

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 does not control or audit third-party benchmark data or the web sites referenced in this document. You should visit the referenced web site and confirm whether referenced data are accurate.

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

© 2016 Intel Corporation. All rights reserved.

Table of Contents

1. Introduction

This document explains how to install and use the Intel® Unite™ plugin for Protected Guest Access on the Intel Unite Solution.

1.1   Audience

This document is designed for use by IT professionals within a corporate environment responsible for installing the Intel Unite software and adding optional features to the application, such as enabling Guest Access for their business.

1.2   Overview

The Intel Unite plugin for Protected Guest Access allows a Guest Client device to connect to a Hub without the need to be on the same Enterprise network. This is possible because the Hub can create an ad-hoc/hosted network (Access Point) where the device can connect, download, or join the Intel Unite application for their client device.
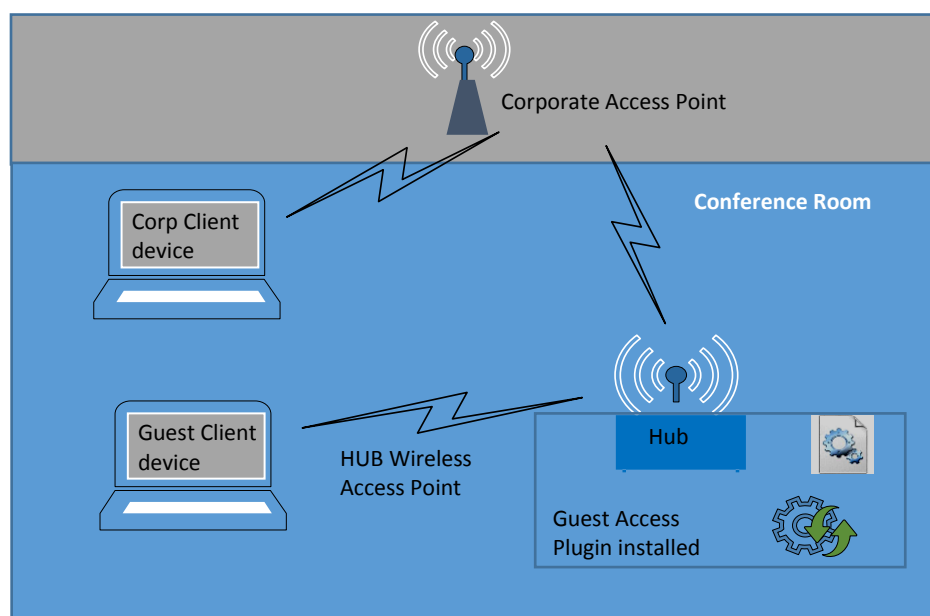
1.3   Recommended Security Controls

It is recommended IT personnel follow the recommended security controls mentioned below:

- Turn off network bridging on the hub that is running Guest Access.
- In an Active Directory environment, set Group Policy Object on the hub which limit applications and users (GPO policies).
- Deploy a firewall between Guest Access machines and corporate connections in order to limit unauthorized traffic.
- Deploy software based solutions to prevent unauthorized executables from running on Guest Access machines like McAfee Application Control and Windows* App Locker.
    o Go to http://www.mcafee.com/us/products/application-control.aspx for more information on McAfee Application control.
- Deploy hardware based solutions to prevent unauthorized executables from running on Guest Access machines like Device Guard on Windows* 10 devices
    o Go to https://technet.microsoft.com/en-us/itpro/windows/whats-new/device-guard-overview on Windows Device Guard

2. Plugin Installation and Components

To install the Intel® Unite™ plugin for Protected Guest Access you will need Administrator rights.

LAN cable required: In addition to the minimum Hub requirements, the only supported network configuration is if the Hub is connected to the corporate network through a wired connection, and the wireless network adapter is not connected to another access point.

The following components are part of the Protected Guest Access plugin:

- Guest Access Client Plugin (dll)

    o This is the plugin that is loaded by the hub. It implements the functionality defined in the CFCPlugin.dll.

- Guest Access Service (Windows service)

    o This is a windows service that is in charge of the creation and configuration of the ad-hoc/hosted network (access point), the GuestAccessClientPlugin.dll sends commands that are received and processed by this service.

- Client Download Page

    o Requires the Intel Unite app v3.0 for the client, configured to run and connect to the Hub that hosts the ad-hoc network. It is available for downloading once the network is created.

Install the plugin by running the application on the Hub machine as an Administrator and follow the notes below according to the software install you performed (Enterprise vs Standalone).

Additional Installation Notes:

➢ Enterprise version. Ensure you add the Plugin Certificate Hash value (Thumbprint) on the Admin Web Portal (**Groups** > **Profiles** Details section) by following the next steps:

    o Locate the installation file – Intel Unite Plugin for Protected Guest Access.msi – and right click on Properties

o When the **Intel Unite Plugin for Protected Guest Access.msi** window opens, locate the **Digital Signature** tab, click to open.

o Select **Intel Unite** and click on **Details**.

o In the **Digital Signature Details** window, click on **View Certificate.**

o Select the **Details** tab and scroll down until you see **Thumbprint**.

o Select **Thumbprint**, once the value is displayed, copy and paste in a notepad, remove the spaces and save it.

o In the Admin Web Portal, go to **Groups**, Select **Profiles**, scroll down, under Description, locate the **PLUGIN CERTIFICATE HASH** key and enter the value saved on the notepad mentioned in the previous step.
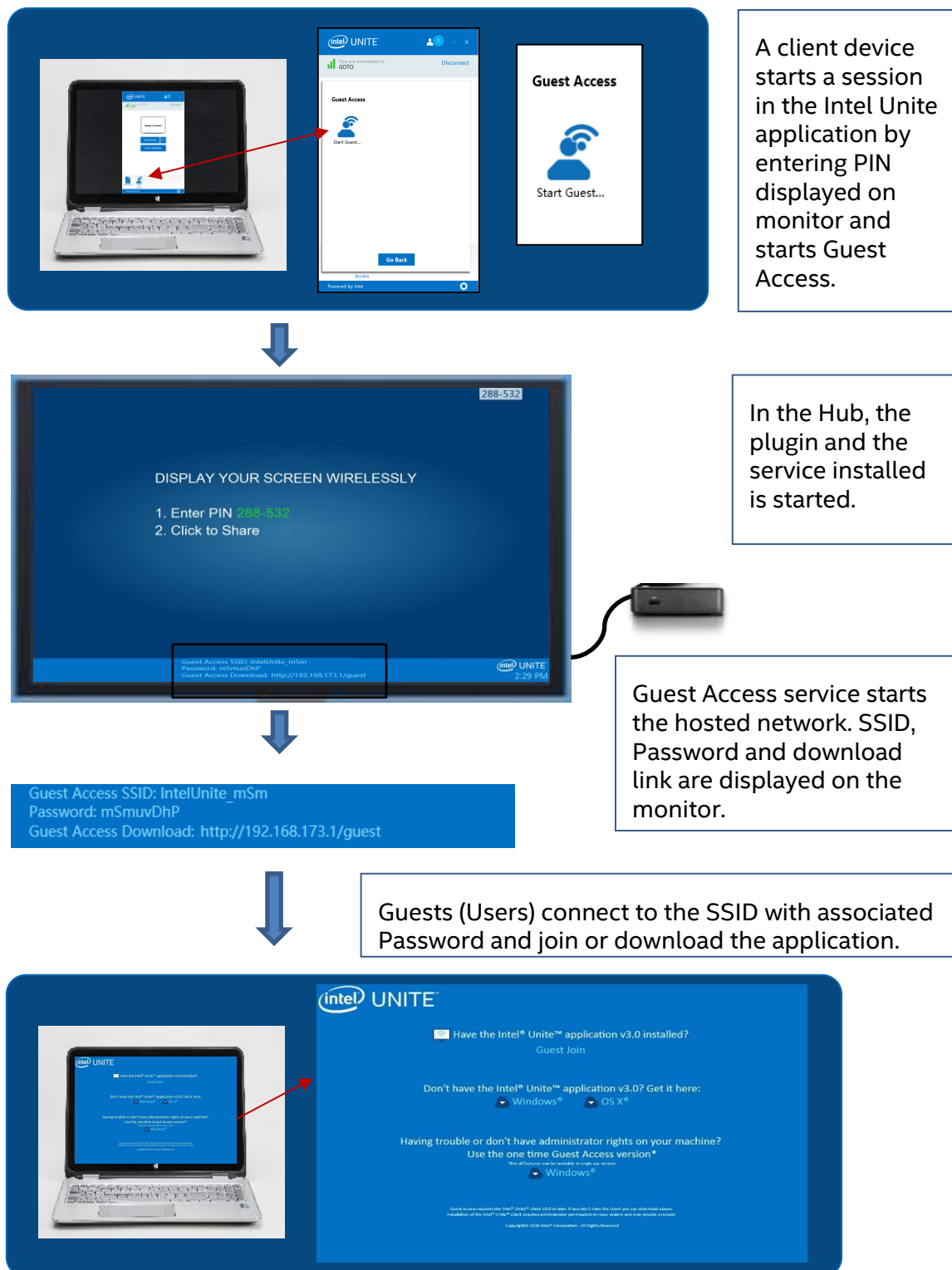

o Also, in the Admin Web Portal, confirm that the key Verify Plugin Certificate Hash is enabled (green box).
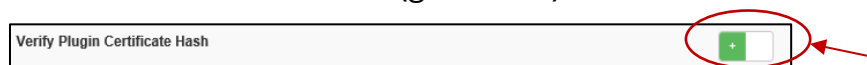
o You have now entered the Certificate Hash for the Protected Guest Access Plugin.

➢ Enterprise version. Defined in Registry Keys, it uses this data:

o HKEY_LOCAL_MACHINE\software\Intel\Unite\GuestAccess, if not, it generates them randomly.

o HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\SSID

o HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\PSK

o HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\Download

➢ Standalone version: After you run the plugin, go to the Intel Unite application Settings, locate the **Plugins** Tab and click on the checkbox **Trusted Plugins** to enable this plugin.

# 3. Protected Guest Access Plugin Flow

A client device starts a session in the Intel Unite application by entering PIN displayed on monitor and starts Guest Access.

In the Hub, the plugin and the service installed is started.

Guest Access service starts the hosted network. SSID, Password and download link are displayed on the monitor.

Guests (Users) connect to the SSID with associated Password and join or download the application.

4. How to enable Guest Access with your Client device

The user will require a client machine locally connected to the Hub (in-room participant) using the PIN displayed on the monitor or display where the Guest Access Client will be able to connect.
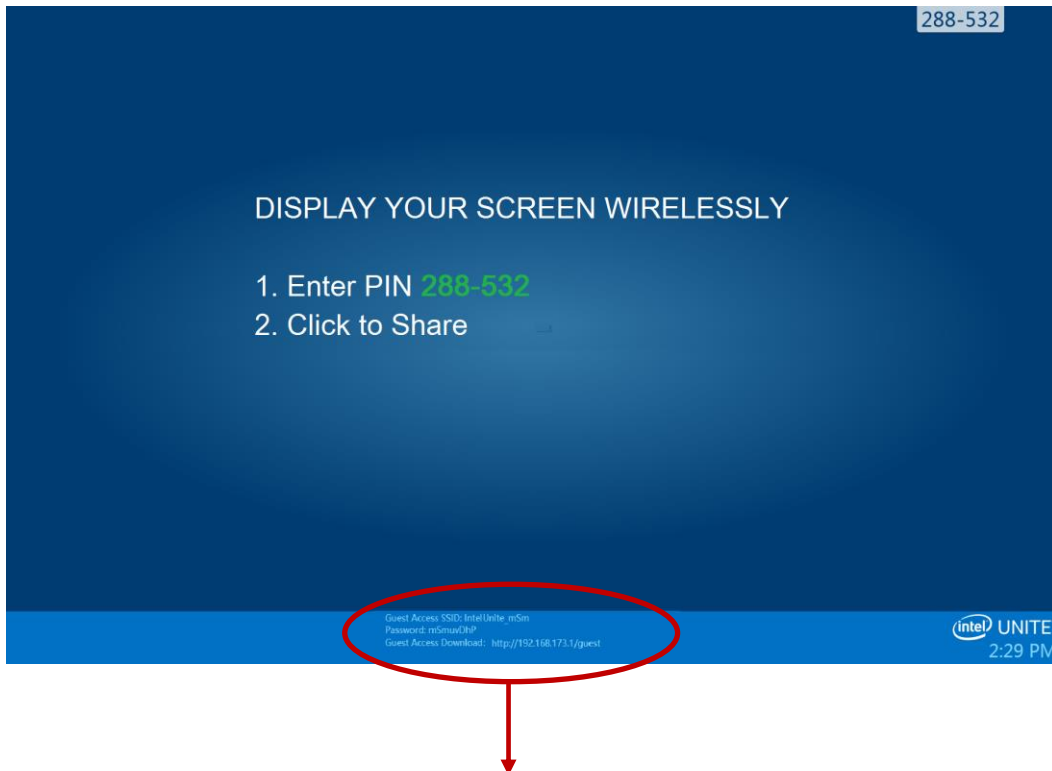
On the Client machine allowing Guest Access:

1. Connect to the Intel Unite application using the PIN shown on the Hub.
2. Once connected, click on the **Guest Access** icon displayed on the window.
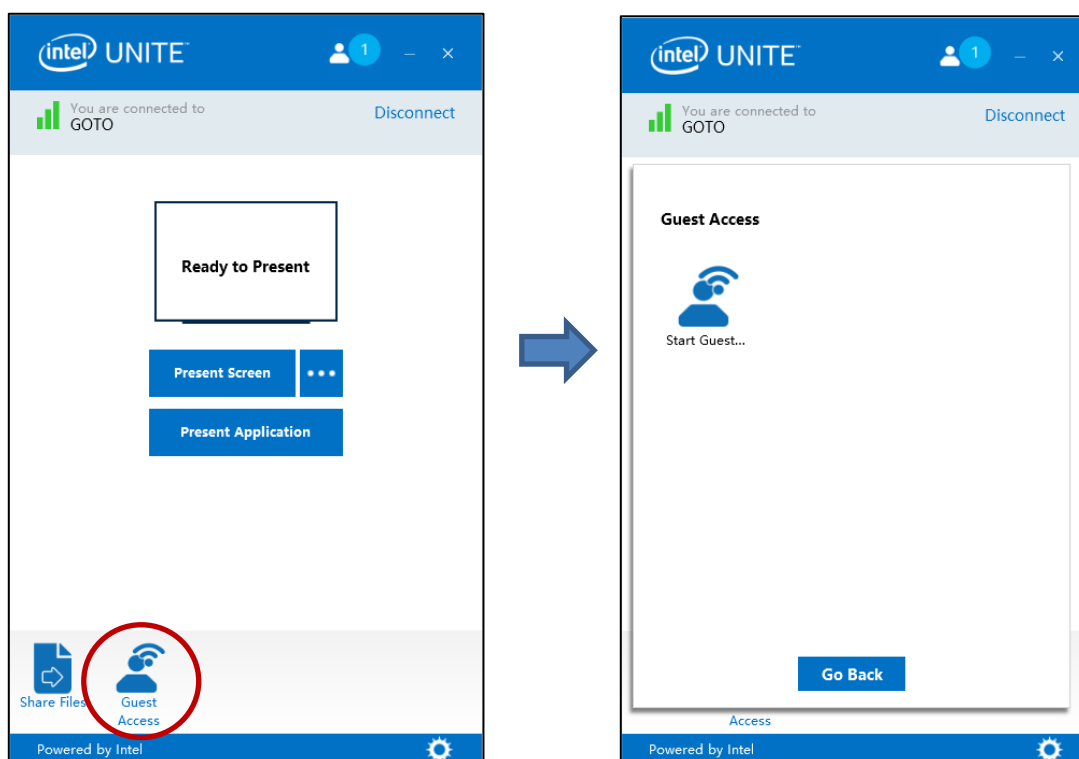
3. The **Guest Access** window will be displayed, you can now click on **Start Guest Access** to enable local WiFi access for the guest to join.

4. The Hub -this is your monitor or display in the room- will show:

- **Guest Access SSID** "unique network name"
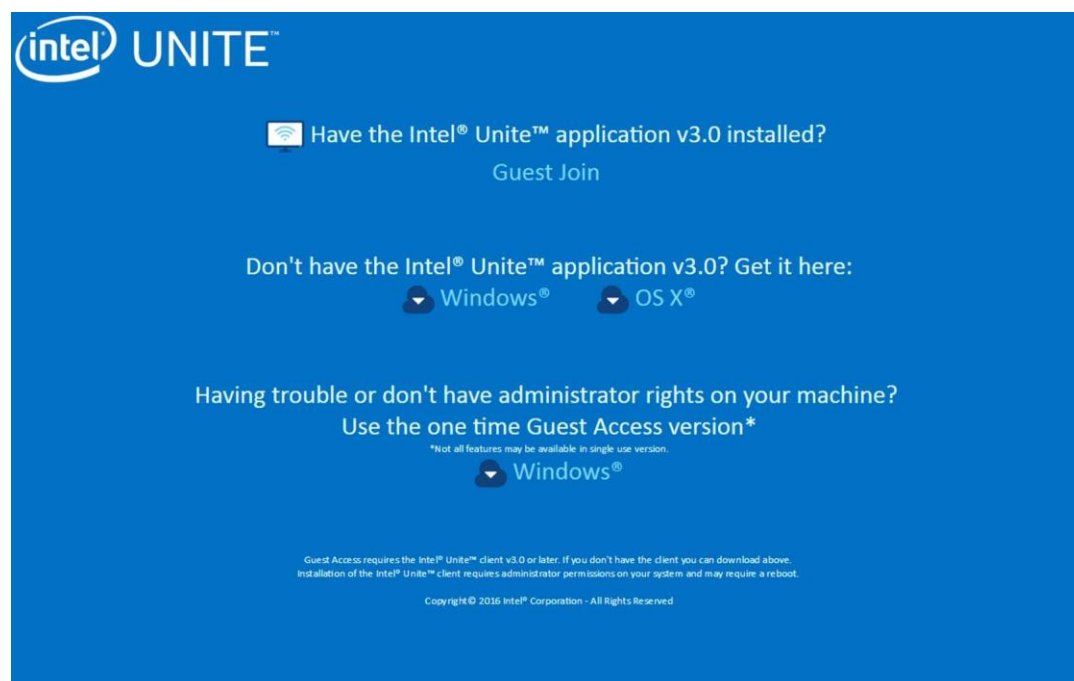- **Password** to use
- **Guest Access Download** link

On the Client machine connecting through Guest Access (Session Guest):

1. Connect to the **Guest Access SSID** and enter the **Password** shown on the Hub.

2. On your browser, go to the **Guest Access Download** link shown on the monitor, use the displayed format http://<hostIP>/guest.

3. The following Web page will be displayed:

4. Select according to the following 3 options:

*   **Have the Intel Unite application v3.0 installed?**
    o   Use this option when your client machine has the Intel Unite application already installed, just click on **Guest Join** to connect (requires v3.0)
*   **Don't have the Intel Unite application v3.0? Get it here:**
    o   Use this option when your client machine does not have the Intel Unite app installed, click on **Windows*** or **OS X*** according to your OS and download the app to connect.
*   **Having trouble or don't have administrator rights on your machine?**
Use the one time Guest Access version
    o   Use this option if you do not have the Intel Unite application on your machine and/or if you had trouble downloading the application (previous 2 options) or do not have administrator rights to download and install the app. You can use the one time Guest Access version. With this option the Intel Unite app will be opened for a one time use and will not reside on your client machine. This option is only available for **Windows*** OS.

5. Download and run the installer according to your selection.

6. After finishing the installation the Client machine will display the **Connect to** window, the guest will be able to enter the PIN and connect to the session.

7. On the Guest Access window, you will be able to see guests that are connected to the session when the **Show info** icon is displayed. When clicking on the **Show info** icon, the monitor (Hub) will display a toast message with the Guest Access information used by guests.
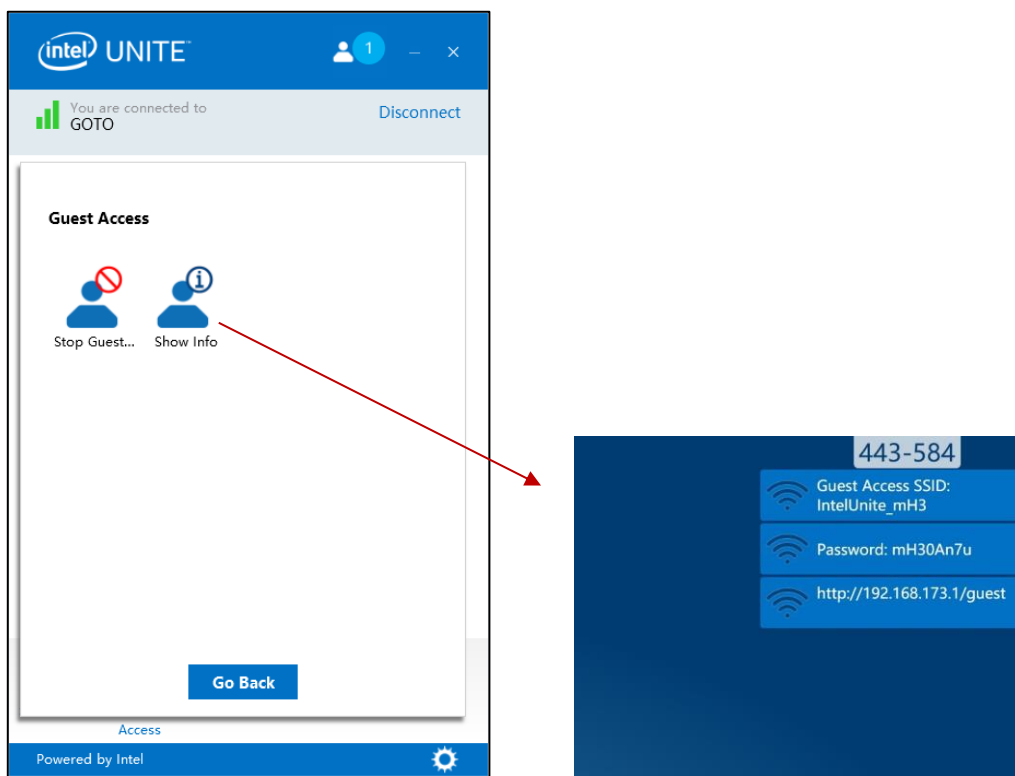
8. When all users are disconnected from the session the client devices using Guest Access will be disconnected. The Hub (your monitor or display) will show for few seconds a toast message indicating no users are connected through Guest Access.
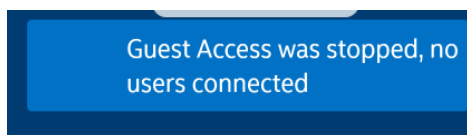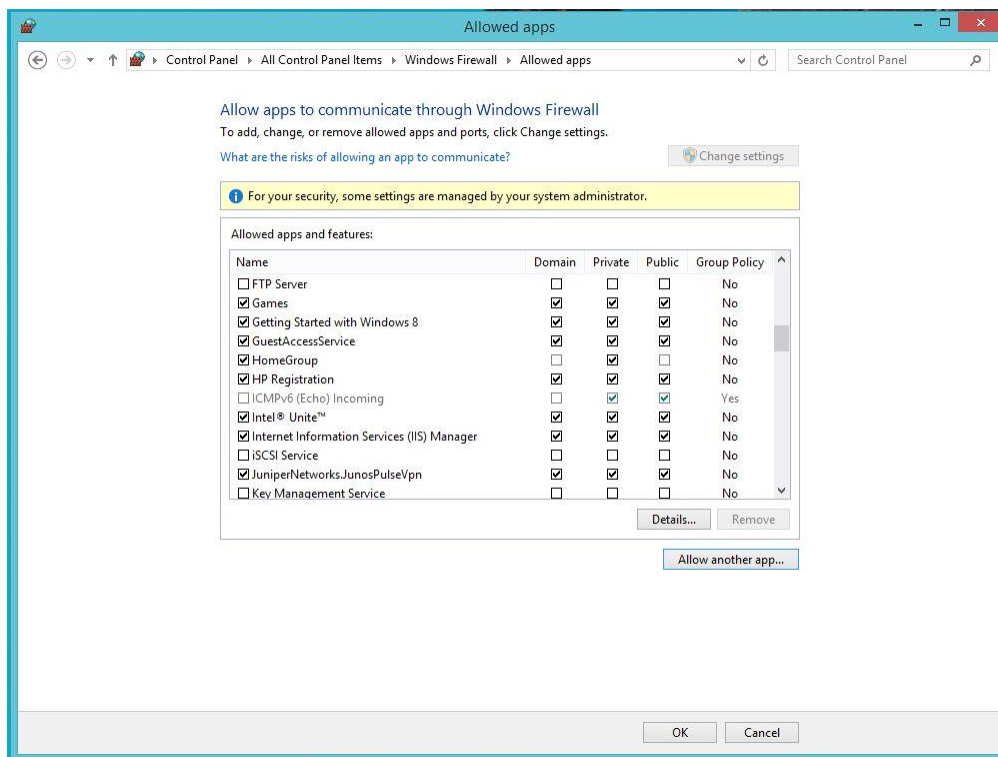
Appendix A. Firewall exceptions

Please verify and validate that the Intel Unite application and the GuestAccessService is added to the Allowed Apps list in your Firewall settings.

The following boxes need to be checked as shown in the example below.

1. Internet Information Service (IIS)
2. Manager and World Wide Web (HTTP)
3. GuestAccessService

Appendix B. Troubleshooting

You can also consult the Windows* event log for additional information.

Guest Access is not starting (or not showing up)

- Verify that Certificate hashes preventing the plugin to work are not entered in the admin portal.

- Your organization GPO Policies (Group Policy Object) might not allow virtual hosted networks, please consult with your system Administrator.

- Ensure the Plugin Certificate Hash value for Protected Guest Access has been entered on the Admin Web Portal.

- Ensure the Plugin Certificate Hash has been enabled on the Admin Web Portal.

- Ensure the hub is connected to the corporate network through a wired connection.

- When in Standalone version, verify that you have enabled the plugin in the Settings – Plugin Tab- section by clicking on the checkbox "Trusted Plugins".