Intel Unite® Solution

Plugin Guide for Protected Guest Access

May 2017

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

Table of Contents

1. Introduction

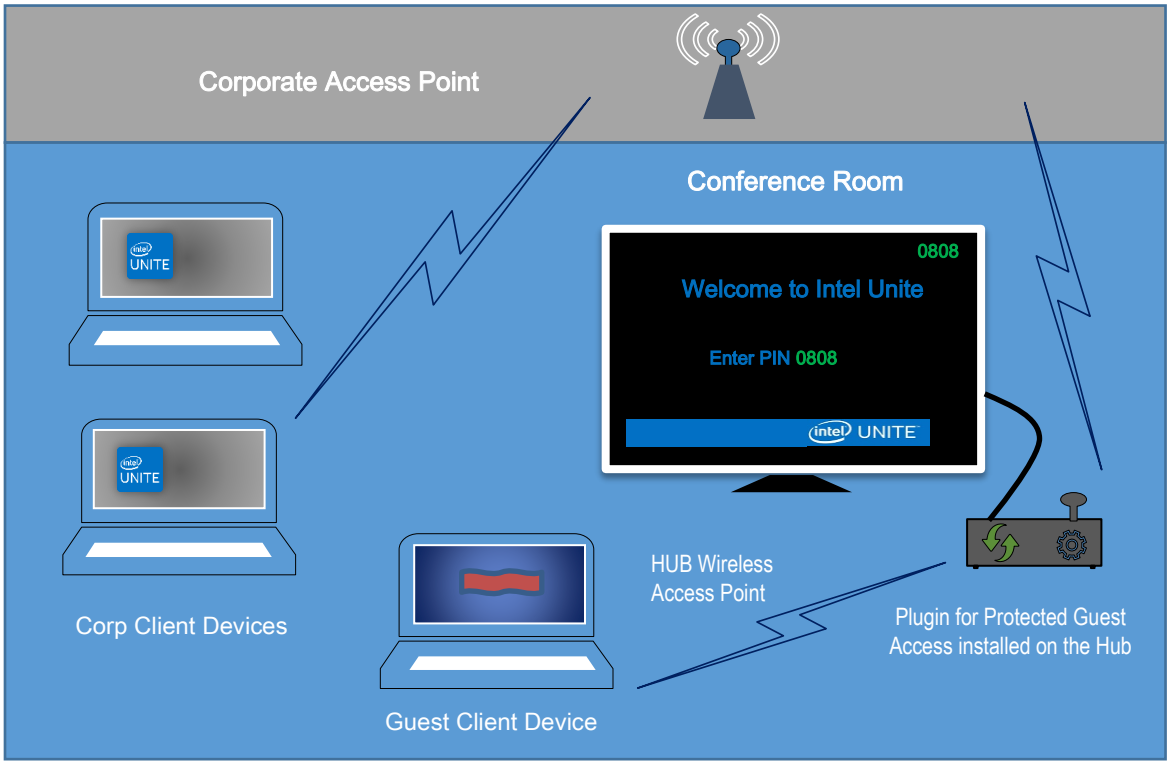
This document explains how to install and use the Intel Unite® plugin for Protected Guest Access on the Intel Unite Solution.

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 Guest Client device can connect, download, or join the Intel Unite application for their client device.



1.3 Recommended Security Controls

It is recommended that 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 limits applications and users (GPO policies).
- Deploy a firewall between Guest Access machines and corporate connections in order to limit unauthorized traffic.
- Ensure there is a firewall on unused ports.
- Deploy software based solutions to prevent unauthorized executables from running on Guest Access machines like McAfee* Application Control or Windows* AppLocker.
    - Go to http://www.mcafee.com/us/products/application-control.aspx for more information on McAfee Application control.
    - Go to https://technet.microsoft.com/itpro/windows/whats-new/whats-new-windows-10-version-1507-and-1511 for more information on Windows AppLocker.
- Deploy hardware and software based solutions to prevent unauthorized executables from running on Guest Access machines like Device Guard on Windows* 10 devices.
    - Go to https://technet.microsoft.com/en-us/itpro/windows/keep-secure/device-guard-deployment-guide for more information on Device Guard.
- For additional information on how to disable network bridging:
    - Go to https://technet.microsoft.com/en-us/library/cc732103(v=ws.10).aspx

2. Plugin Installation and Components

2.1 Plugin Components

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

- Guest Access Client Plugin (dll)
  - This is the plugin that is loaded by the hub. It implements the functionality defined in the CFCPlugin.dll.
- Guest Access Service (Windows service)
  - 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
  - Requires the Intel Unite app v3.0 or higher 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.

2.2 Plugin Installation

To install the Intel Unite® plugin for Protected Guest Access you will need Administrator rights. You will also need to verify compatibility with your target version of your Intel Unite solution (Intel Unite software versions 1.0 and 2.0 will not be compatible with the latest released plugin versions).

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.

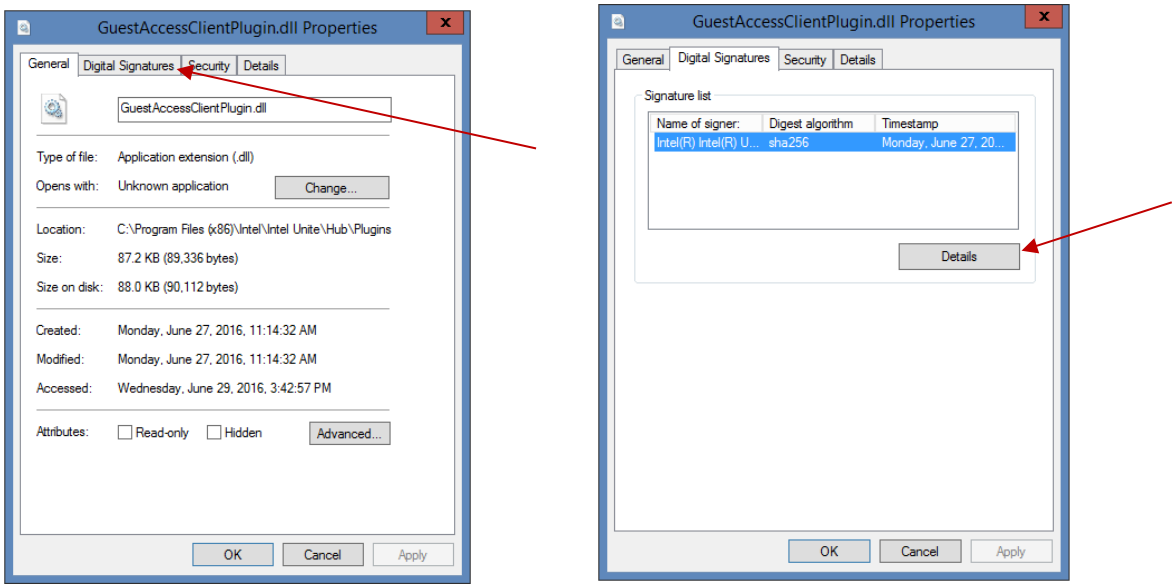
Before you install the Protected Guest Access Plugin, ensure you have the latest Intel Wireless driver. If this is not the case you need to install it.

1. Run the **Intel Unite Plugin for Protected Guest Access installer** (Windows Installer Package) and accept the terms of the License Agreement (check box).
2. Click on **Install,** when the installer finishes the plugin installation go to the **Plugins** folder, located in Program Files(x86) \Intel\Intel Unite****Hub\Plugins, where the GuestAccessClientPlugin.dll has been installed.
3. The next step is to obtain the Certificate Hash value (key value) for the Guest Access Client Plugin. It is recommended to obtain and use key values for plugins vs the default value (default value = blank), as key values add security and prevent malicious plugins from being installed and run on Hubs.

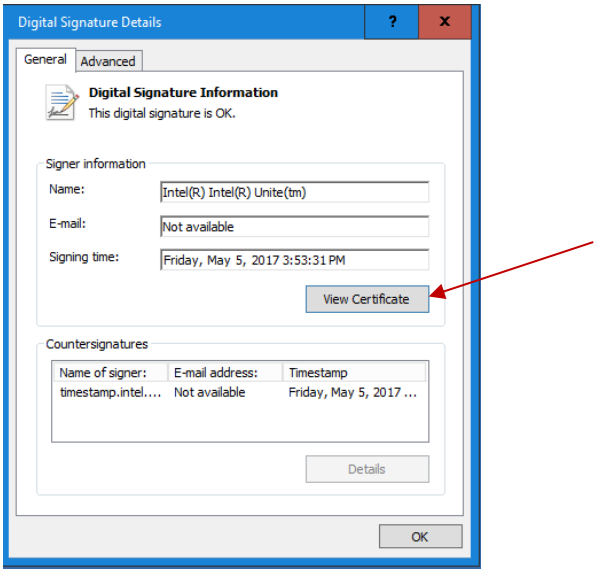
   NOTE: For a test environment you could use the default key value, but this is not recommended for a production environment.

2.2.1 Obtaining the Certificate Hash Value

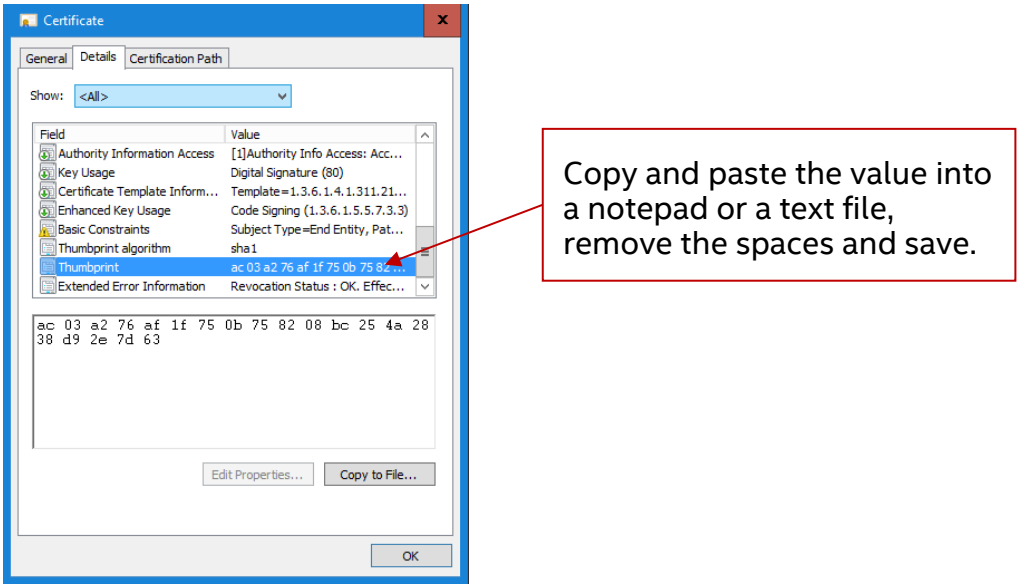
1. In the Intel Unite****Hub\Plugins folder, right click on **GuestAccessClientPlugin.dll** and choose **Properties**.
2. When the plugin **Properties** window opens, open the **Digital Signatures** tab.



4. Select **Intel Unite Plugin** and click on **Details**.
5. On the **Digital Signatures Details** window, click on **View Certificate.**



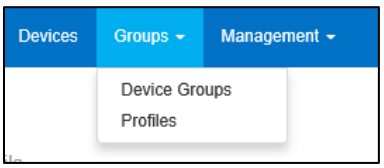
6. In the **Certificate** window, select the **Details** tab and scroll down until you see **Thumbprint**.
7. Select **Thumbprint.** Once the value is displayed, copy and paste it into a notepad or a text file, remove the spaces and save it.



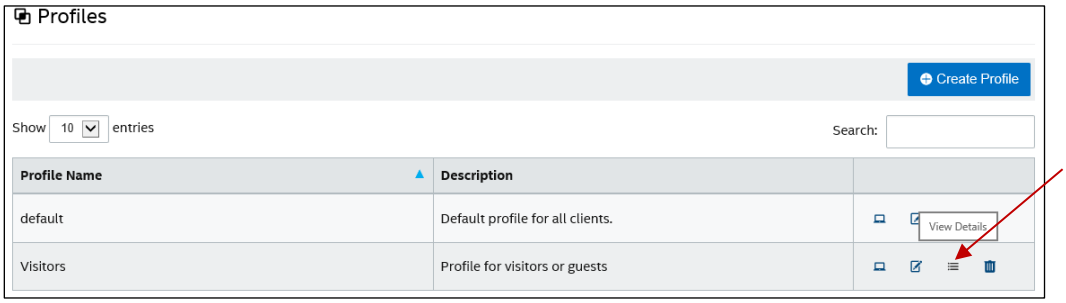
8. This information will be used when you create the Profile for your plugin on the Admin Web Portal. The key value can also be created and entered after the profile has been created.

2.2.2 Edit or create the Profile on the Admin Web Portal

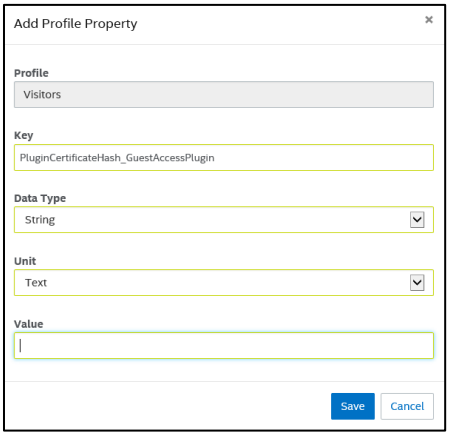
1. Go to the Admin Web Portal, under **Groups**, go to **Profiles.**



2. Under the **Profile Name** list, find the Profile where you want to create the new key and click on the **View Details** icon (located on the last column on the right), alternatively, you may want to create a new Profile instead of using an existing one.



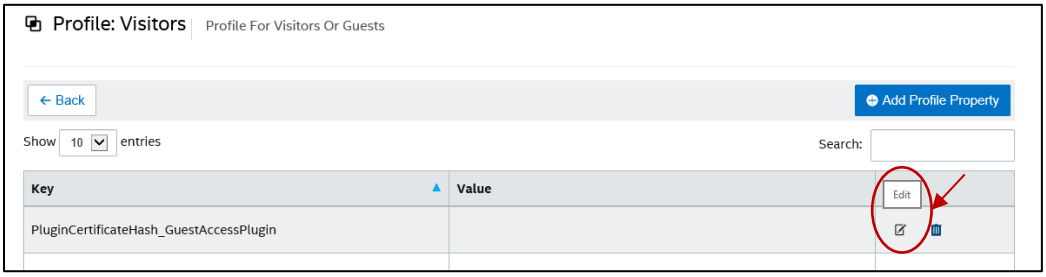
3. Create a Key for the Guest Access Plugin Certificate Hash by clicking on **Add Profile Property**, when the window opens, enter the following:



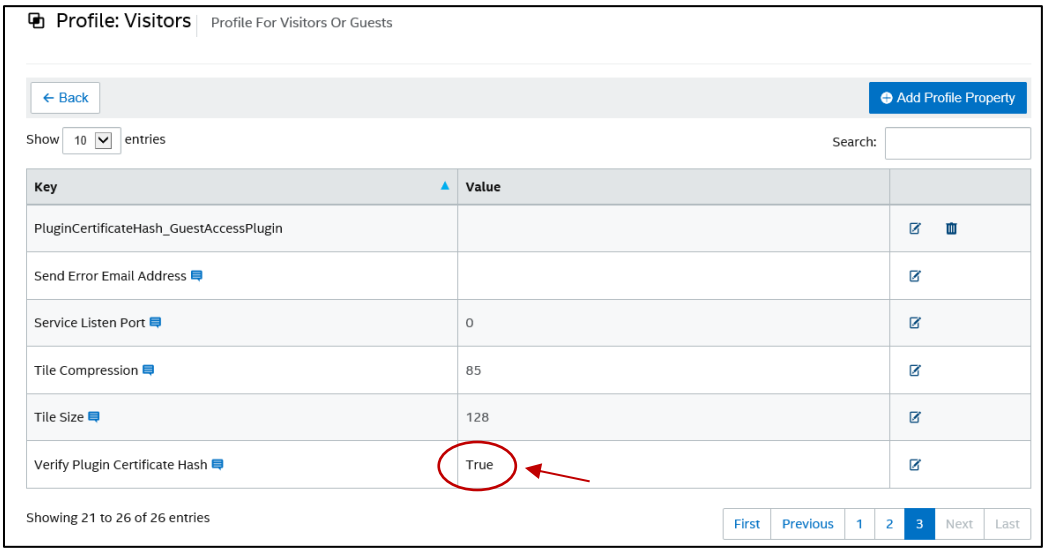
- **Key**: PluginCertificateHash_GuestAccessPlugin
  (The format is PluginCertificateHash_XXXX, where X is the name you are giving the plugin)
- **Data Type:** String
- **Unit:** Text
- **Value:** Paste the value saved in the notepad or text file mentioned in section - Obtaining the Certificate Hash Value - (Thumbprint value). This data can also be entered after creating the key.

4. Click on **Save**.

5. In the **Profile** window, you will see the new plugin key, you can click on Edit to enter its value (if you haven't added it) or to edit this key.



6. You must also ensure the **Verify Plugin Certificate Hash** key is set to **True**, if you want it enabled. If the value is set to **False**, the hub will not check the signing certificate of the installed plugins.



NOTE: For a test environment you could disable the certificate check, in a production environment, the recommendation is to set the value to **True.**

7. Once the profile has been updated with the Protected Guest Access plugin data, remember to assign it to the Hub devices where you want it enabled.

2.2.3 Registry Keys for the Protected Guest Access Plugin

Data defined in the Registry Keys:

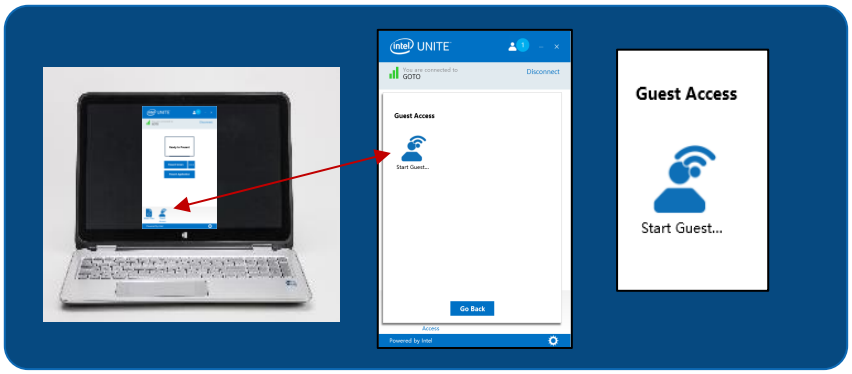
a. HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\SSID

b. HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\PSK

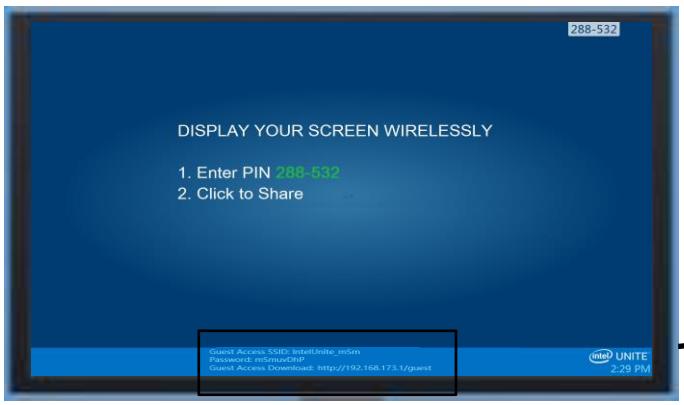
IMPORTANT: If a password is specified, the password must be at least 8 characters; if less than 8 characters Guest Access may not start.

c. HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\Download

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.

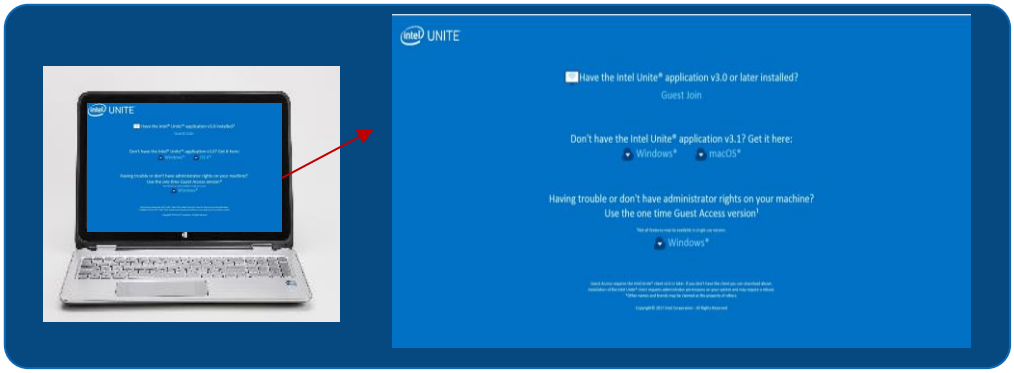


In the Hub, the plugin and the service installed is started.

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

Guest Access SSID: IntelUnite_mSm
Password: mSmuvDhP
Guest Access Download: http://192.168.173.1/guest

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

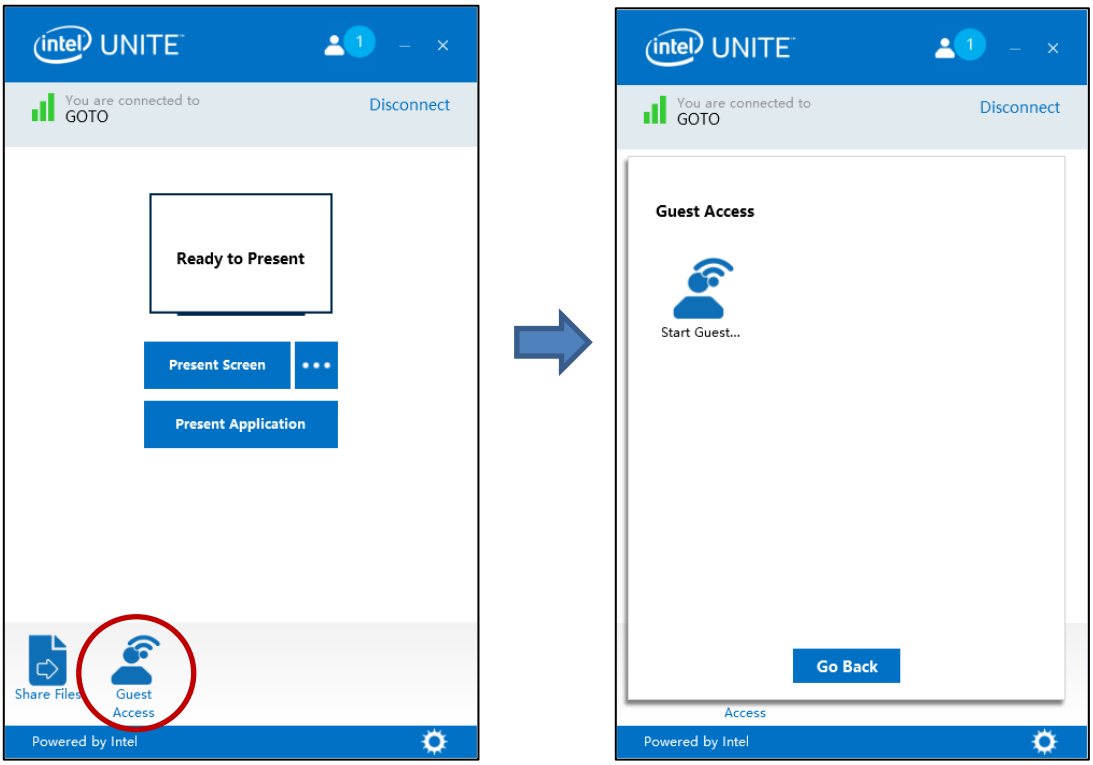


4. How to enable Guest Access with your Client device

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.

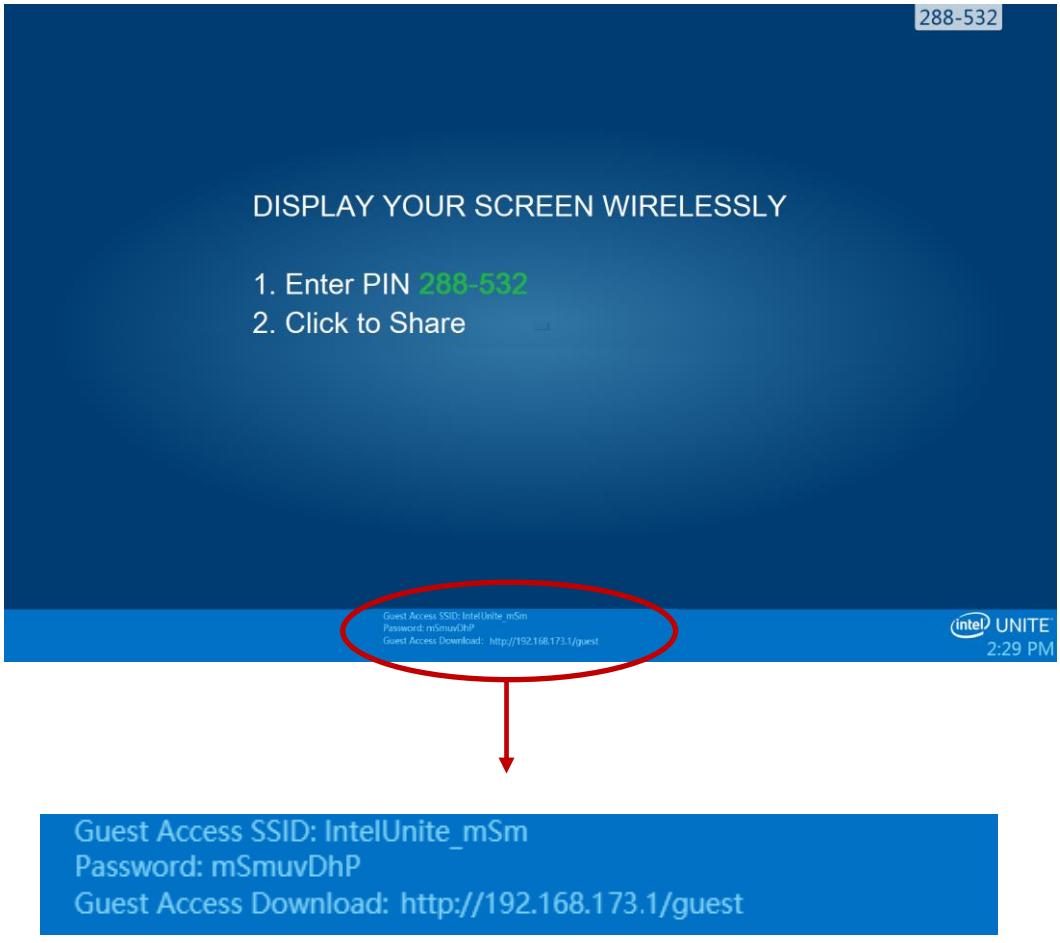
On the Client machine allowing Guest Access:

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 Wi-Fi access for the guest to join.

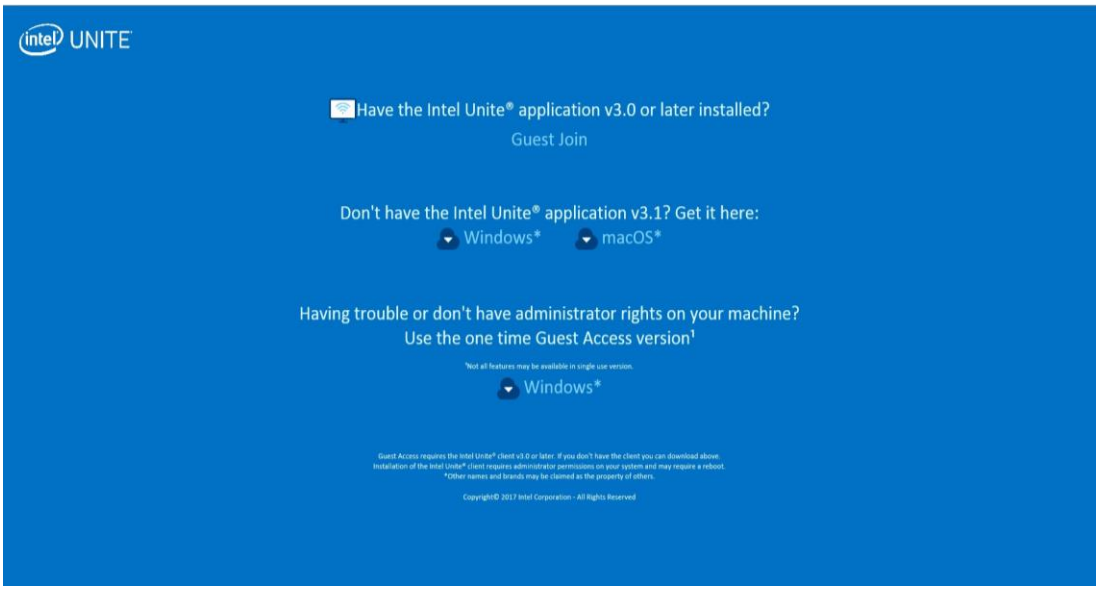
4. The Hub -this is your monitor or display in the room- will show:
    - **Guest Access SSID** “unique network name”
    - **Password** to use
    - **Guest Access Download** link



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. In 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:



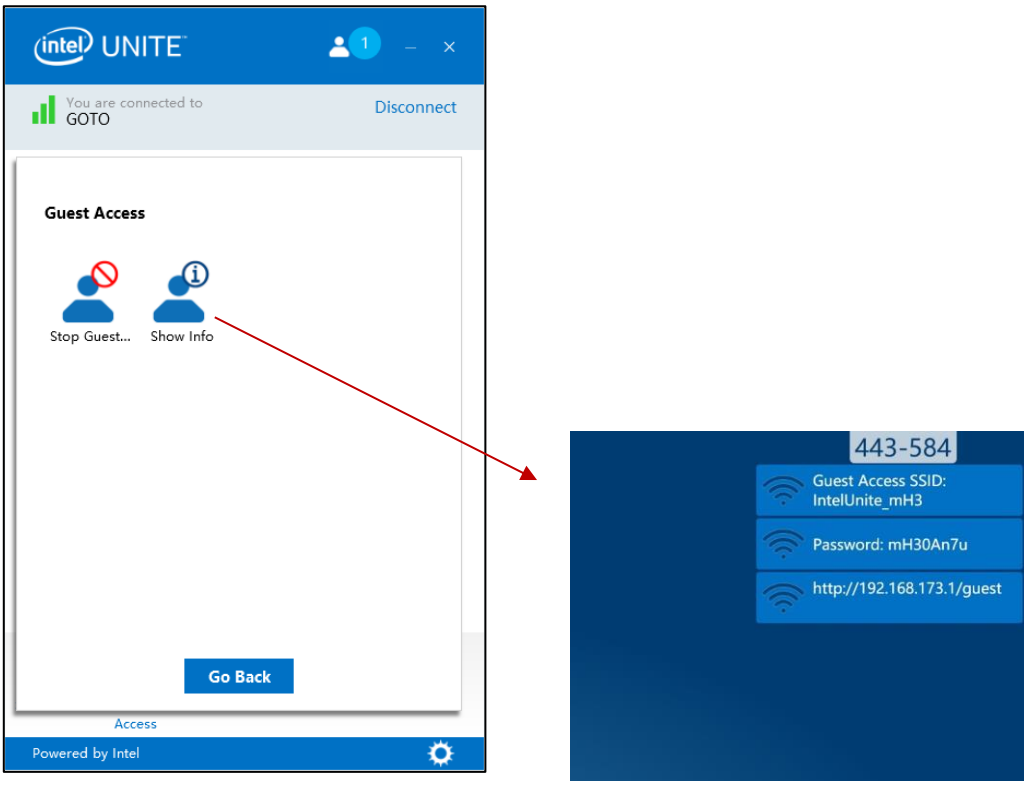
4. Select according to the following 3 options:

- **Have the Intel Unite application v3.0 or later installed?**
  - Use this option when your client machine has the Intel Unite application already installed, just click on **Guest Join** to connect (requires minimum v3.0)
- **Don't have the Intel Unite application v3.1? Get it here:**
  - Use this option when your client machine does not have the Intel Unite app installed. Click on **Windows*** or **macOS 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**
  - 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.

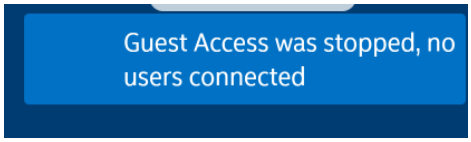
5. Download and run the installer according to your selection.

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 a few seconds a toast message indicating no users are connected through Guest Access.

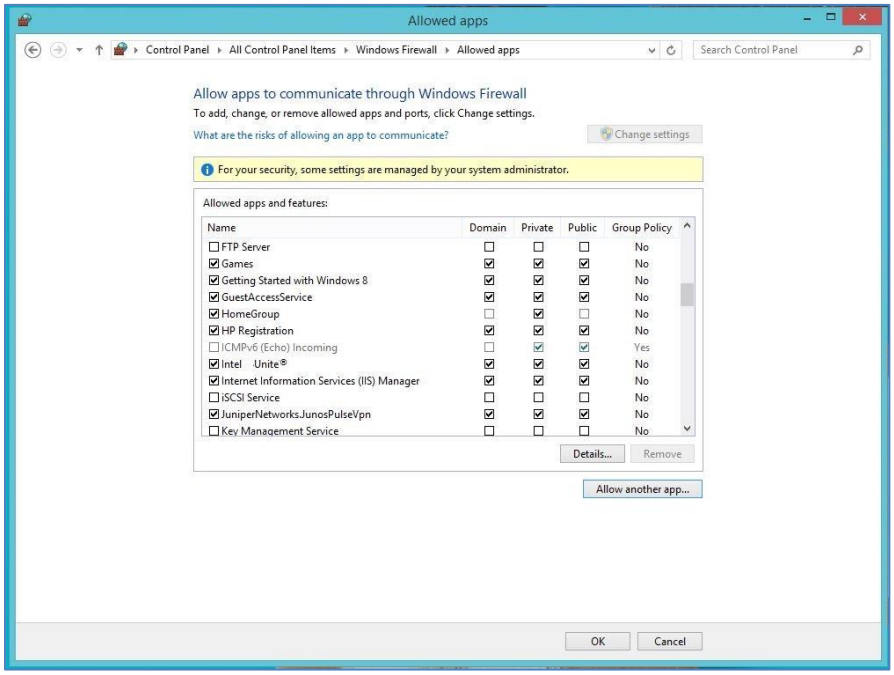


Appendix A. Firewall exceptions

Please verify and validate in the Hub device that the Intel Unite application and World Wide Web Server (HTTP) are added to the Allowed Apps list in the Firewall settings.

When using Windows Firewall, please ensure the following boxes are checked as shown in the example below.

1. IIS Manager - World Wide Web Server (HTTP) - Ensure Public is checked.
2. Intel Unite – Ensure Public, Private, and Domain (if applicable) are checked.



If using a non-Windows Firewall vendor, please check the Firewall settings to allow the Intel Unite app and HTTP (Port 80). If the vendor also blocks traffic on localhost, you will also need to allow traffic to GuestAccessService on the localhost interface.

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 key 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.
- Ensure the profile where you enabled the Protected Guest Access has been assigned to the Hub device (Admin Web Portal-Devices).
- If the password value was changed in the Registry Keys HKCU/software/intel/unite/guestaccess/PSK (you are not using the default value), ensure it contains at least 8 characters.
- Ensure you have the latest Intel Wireless driver.