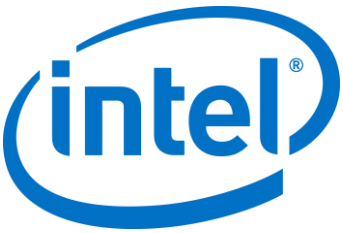
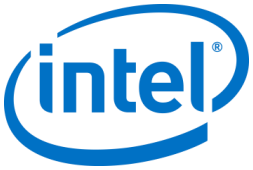


# Intel® Unite™ Solution

## Enterprise Deployment Guide

June 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.

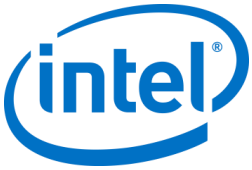
The products described may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

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.

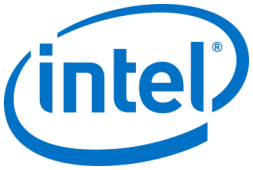
Intel does not control or audit third-party benchmark data or the web sites referenced in this document. You should visit the referenced web site and confirm whether referenced data are accurate.

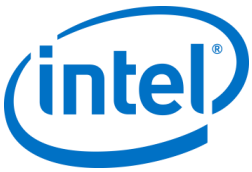
Intel, the Intel logo, and Intel Unite are trademarks of Intel Corporation in the United States and/or other countries.

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



# Table of Contents





# 1 Introduction

Intel® Unite™ software powers secure, connected meeting spaces that simplify collaboration. It was designed to connect everyone in a meeting, quickly and easily. The Intel Unite solution is a simple and instant collaboration solution today and a foundation for added capabilities and innovation in the future.

This document can be used to install the Intel Unite software in enterprise mode, learn more about features and assist with troubleshooting.

## 1.1 Audience

This document is designed for use by IT professionals within a corporate environment and for other audiences that will be deploying Intel Unite solution in an enterprise environment.

## 1.2 Intel Unite Solution Terminology & Definitions

**Enterprise Server (Server)** – This term refers to the web server, PIN service running on the server that will assign and resolve pins, provide a download page for the Clients, and provide the admin portal for configuration.

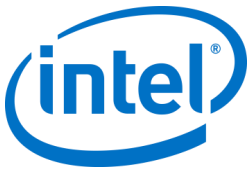
**Client** – This term refers to a device (Windows* or Mac*) that will be used to connect to the Hub.

**Hub** – This term refers to a mini form factor PC with Intel® vPro™ technology that is connected to a display in a conference room running the Intel Unite application.

**FQDN** – This acronym stands for Fully Qualified Domain Name.

**Plugin** – This term refers to a software component that is installed on the Hub which extends the functionality of the Intel Unite solution.

**IIS** – This acronym stands for Internet Information Services, which is a webserver provided by Microsoft*.



# 2 Intel Unite Solution Requirements

## 2.1 Enterprise Server Requirements

- Microsoft Windows* Server 2008 or greater
- Microsoft Internet Information Services with SSL enabled
    - This will require a trusted web server certificate with an internal or public root of trust
- Microsoft SQL Server 2008 R2 or greater
- Microsoft .NET* 4.5 or greater
- 4 GB RAM
- 32 GB available storage
  **NOTE:** The IIS web server and Microsoft SQL database server can be installed on separate machines

## 2.2 Hub Requirements

- Microsoft Windows 7, 8, 8.1 or 10
    - Recommended latest patch level
- Microsoft .NET 4.5 or greater
- 4th generation or newer Intel® Core™ vPro™ processor-based mini PC
- Wired or wireless network connection
- 4 GB RAM
- 32 GB available storage

## 2.3 Client Requirements

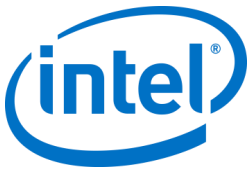
- Microsoft Windows 7, 8, 8.1 or 10
    - Recommended latest patch level
- Microsoft .NET 4.5 or greater
- OS X* 10.10.5 and greater
- iOS 9.3 or higher
- Wired or wireless network connection
- 1 GB Ram
- 1 GB available storage

## 2.4 IT Considerations and Network Requirements

Hub and Client installation should be managed using your IT department's established process for software distribution.

To ensure reliability, it is strongly recommended that the Hub uses a wired network connection. This will prevent wireless bandwidth saturation, especially in congested areas.

Another consideration is that you will need to allow the Intel Unite software to accept incoming connections. This may require you to add an exception to the firewall installed on the Hub. Please contact your firewall vendor for specific details on how to create application exceptions.



In a production environment, it is strongly recommended that you use a Fully Qualified Domain Name (FQDN) and to setup a DNS service record, which points to the Enterprise Server. This provides the easiest method for Hubs and Clients to locate the Enterprise Server.

As a security upgrade, the application accepts only SHA-2 or greater certificates. This may require you to upgrade the certificates on your web server. Work with your IT Security team to get SHA-2 certificates during setup.

# 3 Deployment Overview

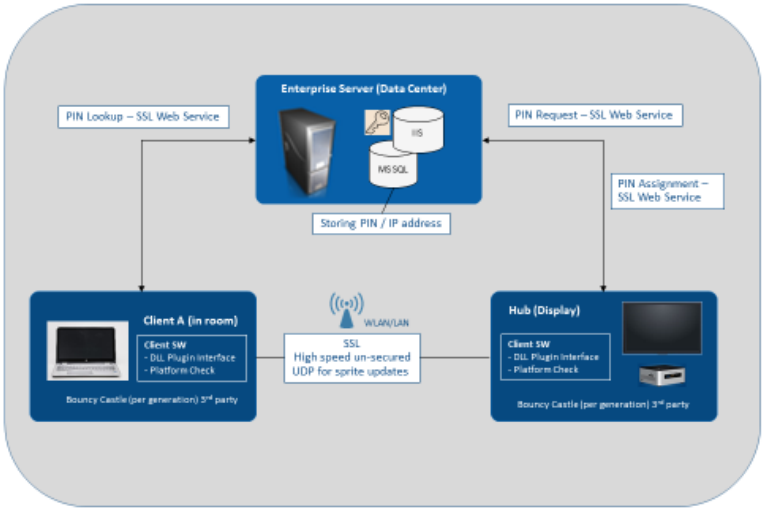
The Intel Unite solution consists of three components – an Enterprise Server, Hub and a Client.

Enterprise Server is the first component you will need to set up. When the Hub and Client applications are launched, they will use the Enterprise Server to exchange connection information and receive PIN assignments.

Hub is the Intel Core vPro processor-based mini PC that is typically connected to a display or projector in a conference room.

Clients follow the instructions displayed on the Hub to download the Client software and connect to the Hub by entering the displayed PIN. Once connected, a Client can present content, view and annotate, and share files with other participants connected to the same Hub.

This diagram provides an overview of the installed components.



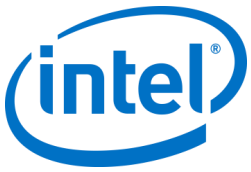

## 3.1 Deployment Resources

In order to complete the installation, you will need the following:

- Administrative rights on the database
- Administrative rights on the Enterprise Server
- Administrative rights on the Hub

You may also need:

- IT security administrator to issue the SHA-2 certificate
- IT security administrator for firewall policies
- IT administrator to create a DNS service record which is used by Hub and Clients to locate the Enterprise Server (strongly recommended)



# 4 Enterprise Server Installation

## 4.1 Enterprise Server Overview

The Enterprise Server Installer includes the Database, PIN server, Admin web portal, and Client download page.

The Enterprise Server contains 4 components:

1) Microsoft SQL database: maintains all state information for the Intel Unite solution infrastructure.
2) Web Service: is a standardized messaging service that communicates with the database and the Hubs and Clients.
3) Administration Portal Website: manages Hubs and Clients, generates statistics, and provides monitoring and alerting.
4) Client download landing webpage: contains the Intel Unite software for the Client.

In addition, it is important to know that the Hubs and Clients locate your Enterprise Server on your network infrastructure through one of the following two methods: ServerConfig.xml file or DNS Service Record.

It is recommended that you use the DNS service record as this enables zero-touch configuration for the Client and Hub. See section on Creating a DNS Service Record. However, if you are not able to acquire a DNS service record, the Enterprise Server can be mentioned in the ServerConfig.xml file. See Appendix B for Example of a ServerConfig.xml file.

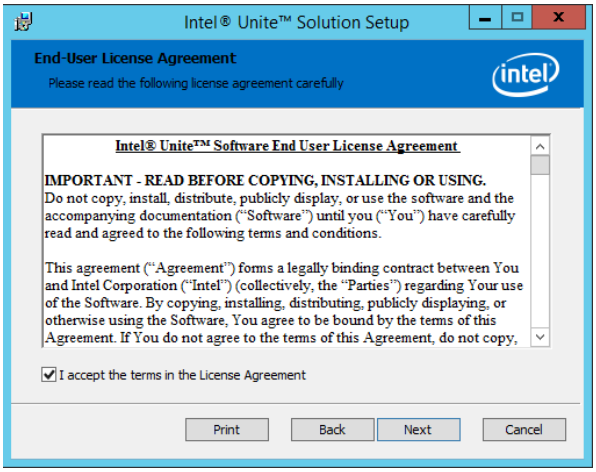
## 4.2 Enterprise Server Pre-Installation

- Verify that the Server meets the minimum software and hardware requirements specified.
- Verify that IIS version 7.0 or greater is installed on your Server. The Server installer requires IIS to be enabled, otherwise it will fail. For help enabling and setting up IIS, see section on Enabling IIS.
- Make sure you have installed and enabled ASP.NET 4.5.
- Ensure SSL is enabled in IIS (https sites should work). **NOTE:** This may require you to work with your IT department to install a SHA-2 certificate with a valid root of trust.
- Make sure you have administrative access to MS SQL via Windows authentication or SQL authentication, see section on Microsoft SQL Server Install.
- Add a DNS Service record to enable automatic lookup of the Enterprise Server. See section on Creating a DNS Service Record.

## 4.3 Enterprise Server Installation

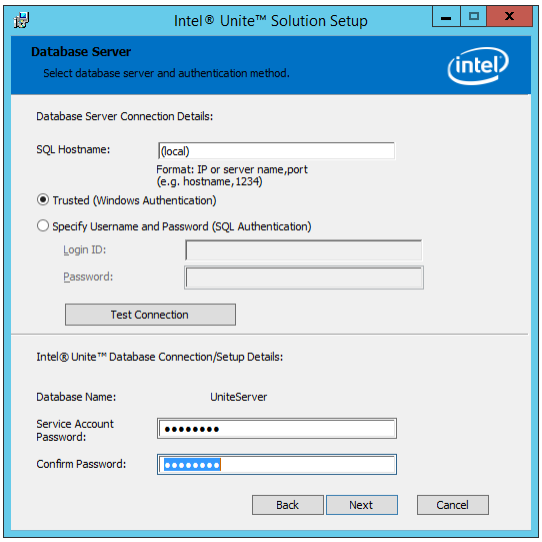
Once you have verified all the steps in the previous section (Enterprise Server Pre-Installation), continue with the Intel Unite software installers (this process needs to be run on the server that hosts the IIS environment).

- Locate the **Intel Unite Server.mui.msi** file and double-click to install on the target server(s).
- The installation wizard provides the option to install these components: a Database, Web Service, Client Download page, and Administration Portal.
- After launching **Intel Unite Server.mui.msi**, accept the license agreement, by checking **I accept the terms of the License Agreement** box.

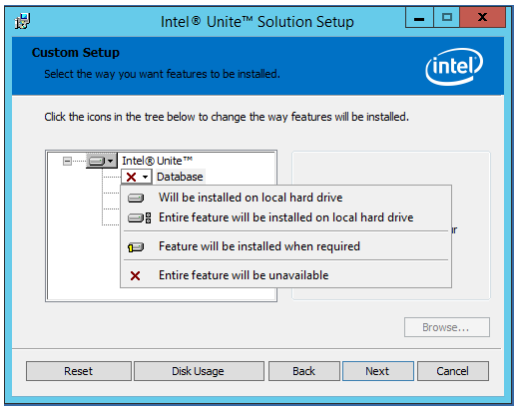


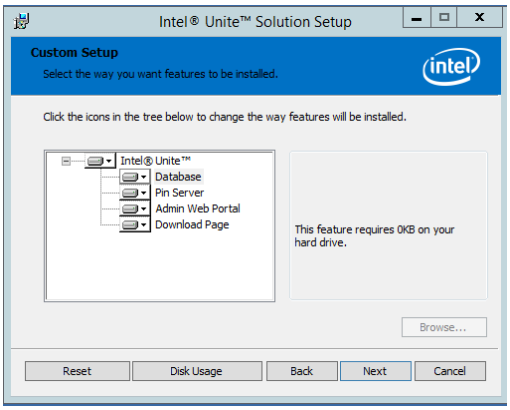

- Click **Next** to continue to the Database Server window.

- In the Database Server window, select the **Database Server Connection Details**. Available options are:
  - In the **SQL Hostname** box, **(local)** is the default value for the SQL server. You can change it by editing your Hostname or leave the default value (leave **(local)** if SQL is installed on the same server).
  - The default value for the Server is **Trusted (Windows Authentication)**, (if you are already logged in), or select **Specify Username and Password (SQL Authentication)** if you have valid credentials that have access to the database and prefer SQL authentication. If you choose the latter, make sure you TEST the database connection by clicking **Test Connection**.
  - In the **Database Connection/Setup Details** section, you need to create a password for **UniteServiceUser** which is used to access the new database named UniteServer. **Confirm Password** in the next box.
  - The password must contain at least 8 characters, at least one uppercase character, one lowercase character, one digit and one symbol.

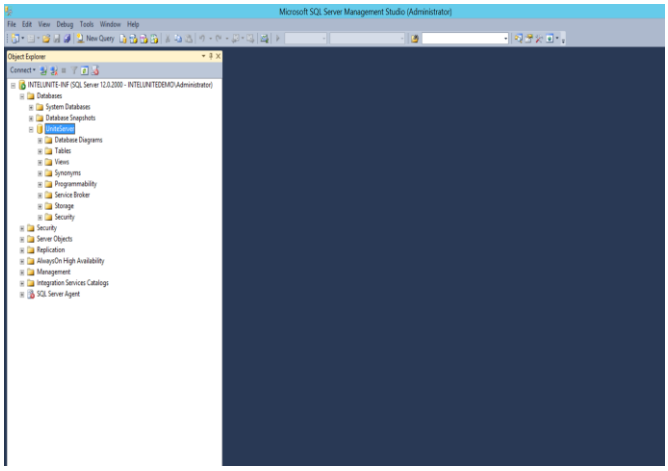


- Click **Next** to continue to the **Custom Setup** window for feature selection. Expand the Database feature and select one of the Database features **Will be installed on local hard drive** or **Entire feature will be installed in local hard drive**. This will create the Database in the SQL server provided in the previous step.



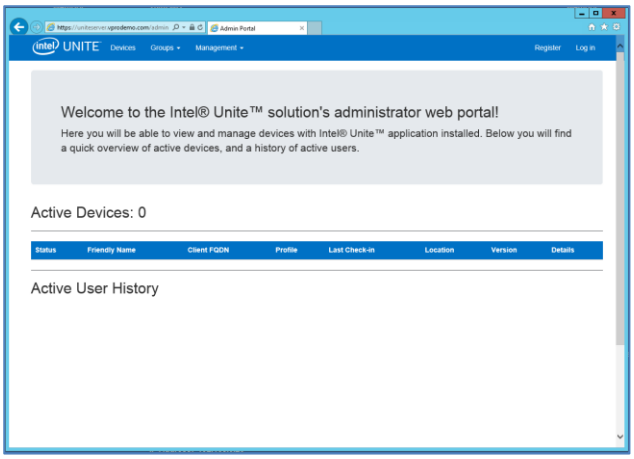




- Click **Next** to verify feature selection and begin the installation by clicking on **Install**.
- Click **Finish** to complete the setup.
- Optional:
  - Verify that the UniteServer database has been created by using SQL Management Studio Open SQL Management Studio on your server and connect to the SQL server. Expand Databases on the left side pane and make sure UniteServer Database has been created.



- Verify the installation was successful by accessing the Admin Portal (if it is installed on the server along with the database and PIN Server), following the link: https://<yourservername>/admin

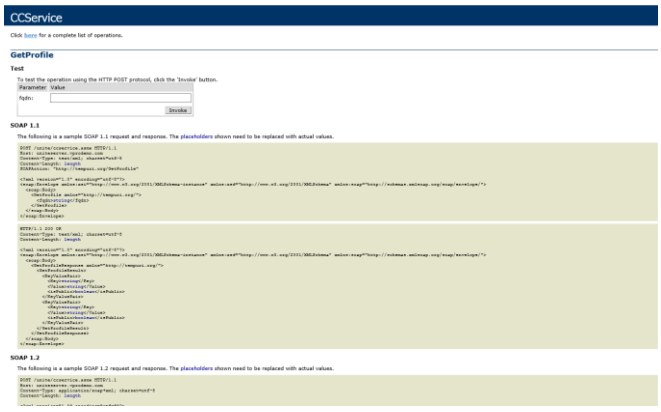
  Default admin account:
  User: admin@server.com
  Password: Admin@1



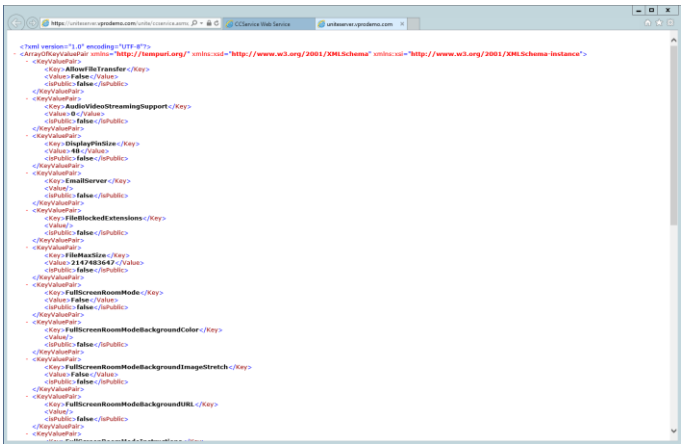

**Note:** If you receive an error page when accessing the Admin Portal, which complains about a specific xml tag in the Web.config, remove the tag from the Web.config in the top level of the portal's virtual directory (accessible from IIS management console).

- Verify the Web Service installation was successful, following the link: https://<yourservername>/unite/ccservice.asmx

  - Select **GetProfile**.
  - Enter **test** in the value field and press invoke.



- Verify that you can view a default profile in the xml file as shown below. This indicates that the pin service can access the database and successfully retrieve data.



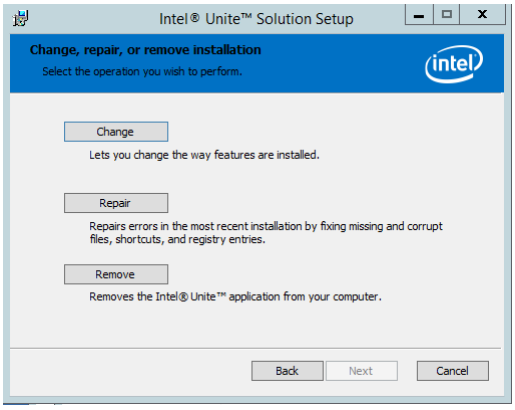
- You have now installed Enterprise Server. Continue to the next section to install the Hub.

## 4.4 Uninstalling the Intel Unite Application

If for any reason you need to uninstall the application, you would also need to delete the UniteServer database and the UniteServiceUser login created previously to avoid conflict within the application.

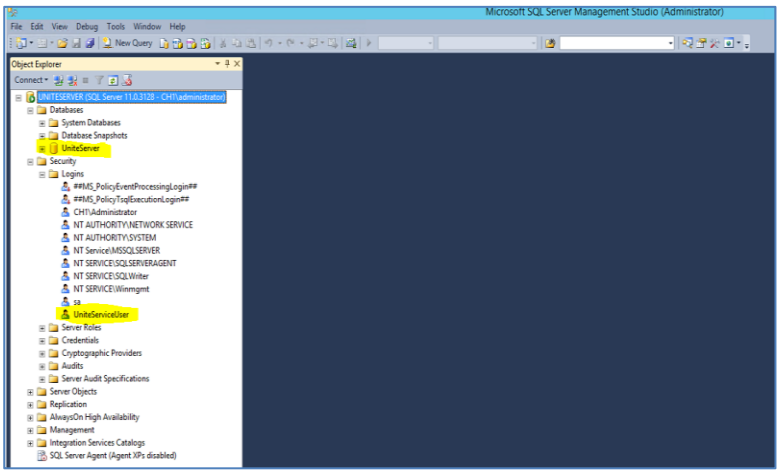
When the installer is launched, you will have the following options:

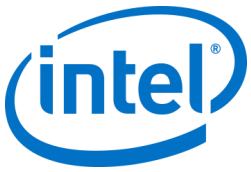
1. Change: change how the features were installed.
2. Repair: fix and repair missing or corrupted files and registry entries.
3. Remove: remove according to the installer you are running.



For a clean uninstallation,

- Click on **Remove** to uninstall and **Next** to continue.
- After the un-install has ended, go to Microsoft SQL Server Management Studio.
- Manually delete the UniteServer SQL Database and the UniteServiceUser account located under Logins. See the highlighted areas in the image below.





# 5 Hub Installation

## 5.1 Hub Pre-Installation

The Intel Unite application needs an exemption in the Hub firewall to check in and communicate with the Enterprise Server, since the Hub needs to be able to locate and check in with the Enterprise Server.

When you run the Hub installer, it will prompt you for server connection details and give you the option of bypassing the manual lookup (named **Specify Server** in the install process) in favor of retrieving information from the DNS Service Record. When Hub installer is run, it will edit the ServerConfig.xml.

Depending on the method chosen for PIN look up, you need to know if you will use the **Automatically Find Server** or **Specify Server** selection when executing the installation.

If you know that the DNS Service record exists, then you can select **Automatically Find Server**. It is preferable to use the automatic lookup to avoid mistyping errors. If unsure, use the **Specify Server** option (manual lookup), where you would need to know the hostname for the Enterprise Server.

If you have edited the ServerConfig.xml with the public key (see next section Public Key), you are not required to input the key again for the Client and Hub installers.

**Note:** If a server is defined in the ServerConfig.xml, it will take precedence over the DNS Service Record.

### 5.1.1 Public Key

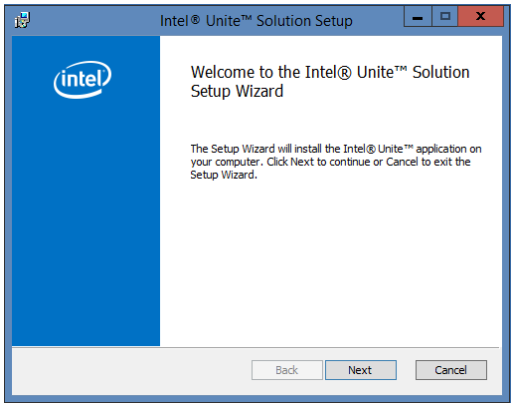
The public key is optional; what it does is specify how the Hub or Client will talk to the Enterprise Server. If left blank or unspecified, the Hub and the Client will validate the root of trust. If the application does not accept the certificate it will prompt for the user.
The public key would be used when you execute the installation of the Hub and the Client. You will need this key when running the installers for the Hub and the Client. To obtain the public key, go to: https://yourservername/unite/ccservice.asmx

In the URL bar, click the lock and view the certificate information. Go to details, click show all, scroll down the field to “Public Key”, then click public key to view. Optionally, you may copy the value out there and paste it into the ServerConfig.xml file.

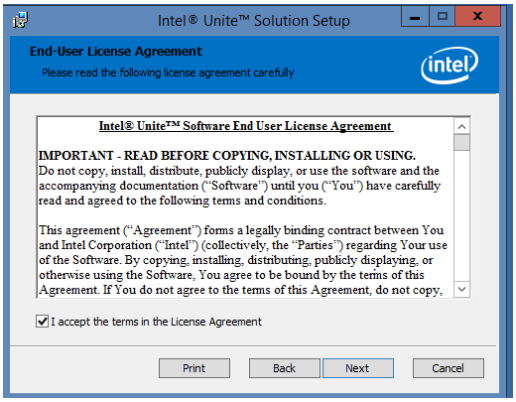
Make sure you remove the spaces from the string after you paste in the ServerConfig file. If you have edited the ServerConfig.xml with the public key, you are not required to input the key again for the Client and Hub installers. See Appendix B for an Example of ServerConfig.xml.

## 5.2 Hub Installation

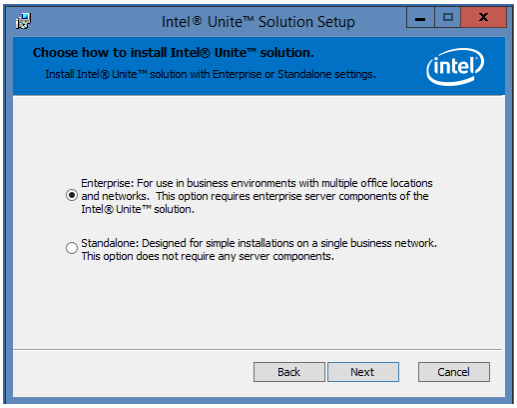
- Locate the installer folder and run the installer for the Hub: **Intel Unite Hub.mui.msi**
- Click **Next** to continue.




- Click **Next** after you check the box **I accept the terms in the License Agreement**.

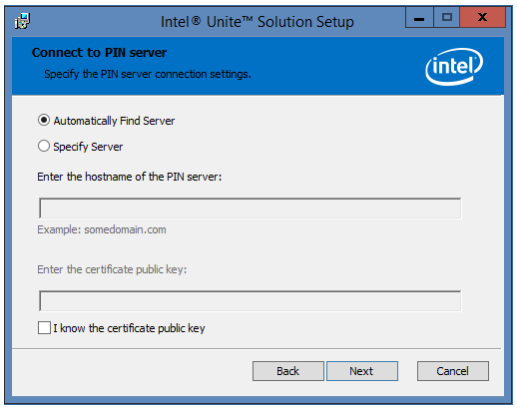



- Choose **Enterprise** and click **Next**.

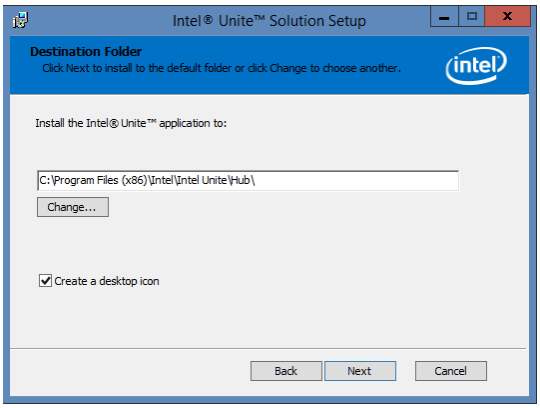


- In this window you must specify the PIN server connection settings, your choices are:
  - **Automatically Find Server**: This is the most convenient choice (default).
  - **Specify Server**: In this step you need to know the hostname for Enterprise Server
    - **Enter the hostname of the PIN Server.**
    - Enter the **certificate public key** if you have checked the **I know the certificate public key** box.

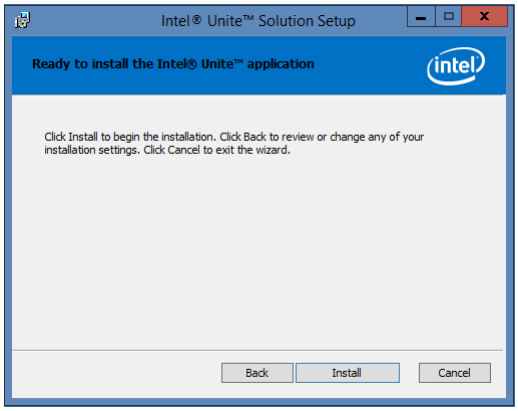
  Select your choice and click on **Next**.



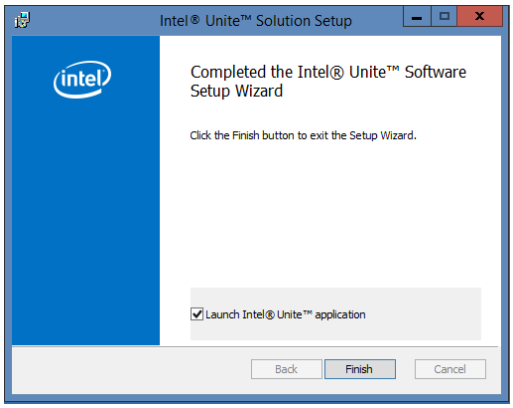

- The **Destination Folder** window will open up with the default folder where the Hub will be installed. You can change the destination folder if you wish, otherwise keep the default location. In this step you can also create a desktop icon. Click **Next** to continue.



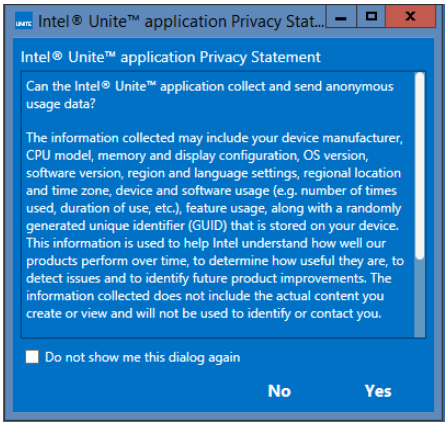

- In this step you can go back to review your settings or click on **Install** to continue.



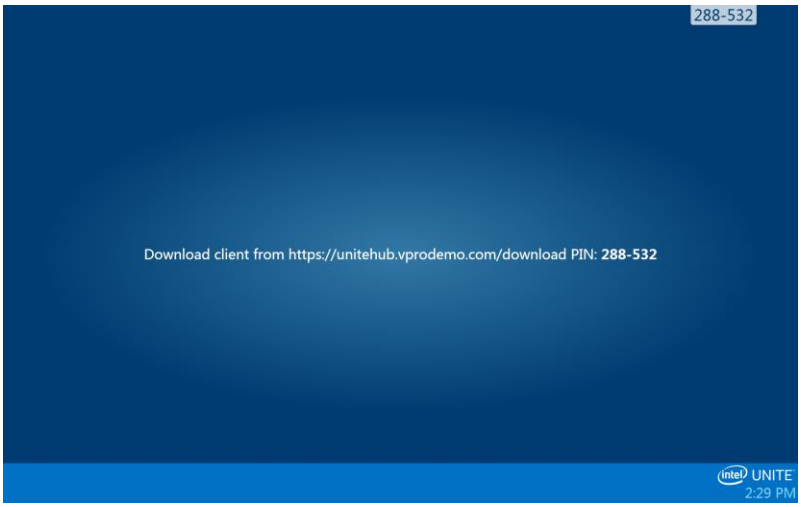

- Once the installation has ended, you will see the **Completed the Intel® Unite™ Software Setup Wizard** window. If you want to launch the application, select **Launch Intel Unite application** and click on **Finish** or just click on **Finish** to end the installation process.



- When you launch the application for the first time, you will see the following Intel Unite application Privacy Statement.




- The Intel Unite application 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.
- You will now see a PIN displayed on your screen or monitor. This is the PIN you will need for the Clients to connect to the Hub. (Please refer to the Troubleshooting section if the PIN is not displayed.)




## 5.3 Hub Configuration

The configuration options for Hubs running Intel Unite software can be modified via Admin Portal. The Admin Portal contains a default profile with default configuration settings that are applied to all Hubs that are checking in with the Enterprise Server. The configuration options are pushed to the Hubs after a connection from the Hub to the Enterprise Server is established. The settings are updated each time the Hub checks in. Some examples of settings that can be customized are background image for Hub display, PIN size, font color and content.

Refer to Profile Configuration to understand your configuration options.

## 5.4 Hub Recommended Practices

In order to ensure the best possible end user experience, the Hub should be configured so that it is always ready to be used and system alerts or popups that display on the screen are suppressed. Recommended practices include the following:

- Windows should automatically log in the domain or user that Intel Unite application will execute.
- Screen savers should be disabled.
- The system should be set to never go to standby.
- The system should be set to never log out.
- Display should be set to never turn off.
- System alerts should be suppressed.

## 5.5 Hub Security

The Hub administrator should ensure that recommended security practices are followed for each attended and unattended Hub. If the local user is logged on automatically, ensure that the user does not run with administrative privileges.

## 5.6 Plugins

Intel Unite application supports the use of plugins. Plugins are software elements that extend the features and capabilities of the application, implementing user experience modalities. Plugins may be unique to each system.

The following plugins are currently available for the Intel Unite application:

Plugin for Guest Access: this plugin allows a computer to connect to a Hub without the need to be on the same enterprise network and without the enterprise server PIN validation. The Hub creates an ad-hoc/hosted network (access point) where the computer can connect to the Intel Unite application.

Plugin for Skype for Business: This plugin is a solution for including people from an online Skype meeting into an Intel Unite app session. The plugin runs on the Hub of the Intel Unite software and manages a mail account specific to each instance.

Plugin Software Development Kit (SDK): Application Interface Guide to assist software developers or anyone looking to develop additional functionality for the Intel Unite application.

**Note:** Please refer to the specific plugin guides if you want to install or find out more about each plugin component.

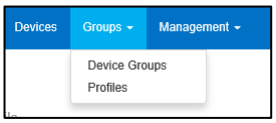
### 5.6.1 Plugin installation notes

Each plugin should be installed in the plugin directory within the installation directory ([..Root\Plugins\[PluginNamespace]Plugin.dll). Plugins are enumerated at start of the application. If a new plugin is added the application will need to be restarted.

Before you install the plugin, verify compatibility with your target version of your Intel Unite solution.

You must also ensure you add the Plugin Certificate Hash value on the Admin Web Portal for each plugin used.

Once you have the Plugin Certificate Hash Value, go to the Admin Web Portal, **Profiles** under the **Group** menu, and enter the key next to the plugin name. Go to the next section to obtain the key for your plugin.

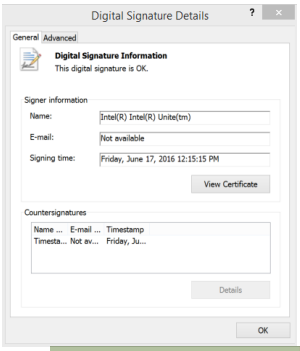


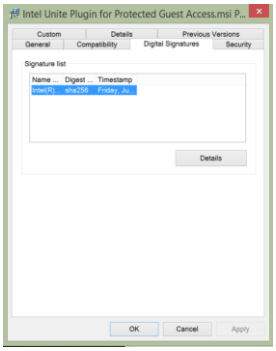


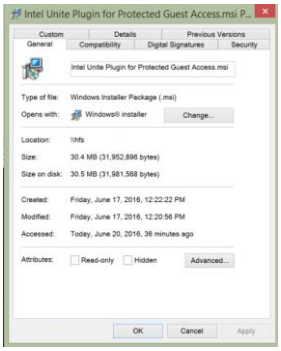
## 5.6.2 Plugin Certificate Hash Value

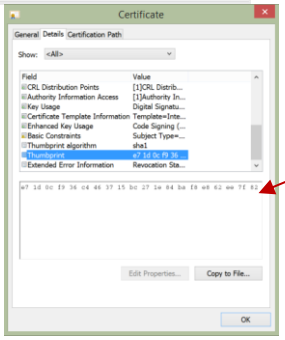
Follow these steps to find the Certificate Hash key value for your Plugin:

- Locate the plugin installation file – Intel Unite Plugin for XXXX.msi – and right click on Properties
- When the **Intel Unite Plugin for XXXX.msi** window opens, locate the **Digital Signature** tab, click to open.
- Select **Intel Unite** and click on **Details**.
- In the **Digital Signature Details** window, click on **View Certificate.**
- Select the **Details** tab and scroll down until you see **Thumbprint**.
- Select **Thumbprint**, once the value is displayed, copy and paste in a notepad, remove the spaces and save it.
- 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.




Copy and paste on notepad or a text file, remove spaces before you save it.

# 6 Client Installation

## 6.1 Client Pre-Installation

A Client needs to be able to locate and check in with the Enterprise Server. Intel Unite application needs an exemption in the Client firewall to check in and communicate with the Enterprise Server.

When you run the Client installer, it will prompt you for server connection details and give you the option of bypassing the manual lookup (named **Specify Server** in the install process) in favor of retrieving information from the DNS Service Record. When running the installer, it will edit the ServerConfig.xml.

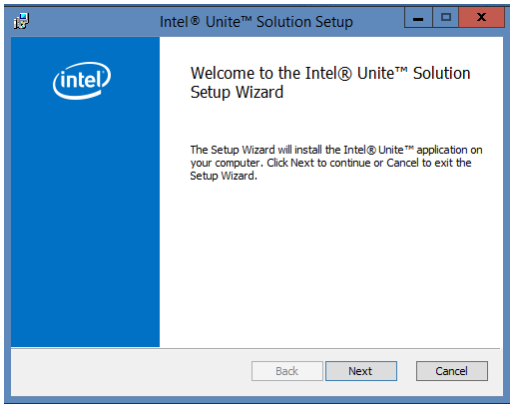
Depending on the method chosen for PIN lock up, you need to know if you will use the **Automatically Find Server** or the **Specify Server** selection when executing the installation.

If you know that the DNS Service record exists, then you can select **Automatically Find Server**, it is preferable to use the automatic lookup to avoid mistyping errors. If unsure, use the **Specify Server** option (manual lookup), where you would need to know the hostname for the Enterprise Server.

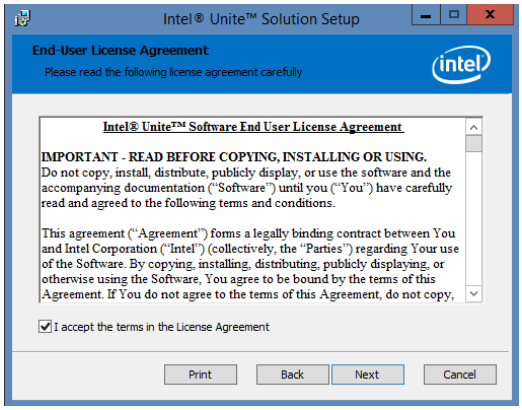
**Note:** If a server is defined in the ServerConfig.xml, it will take precedence over the DNS Service Record.

## 6.2 Windows Client Installation

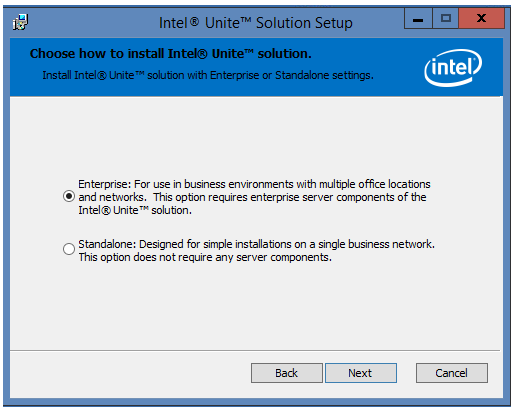
- Locate the installer folder and run Client installer: **Intel Unite Client.mui.msi.** Click **Next** to continue.



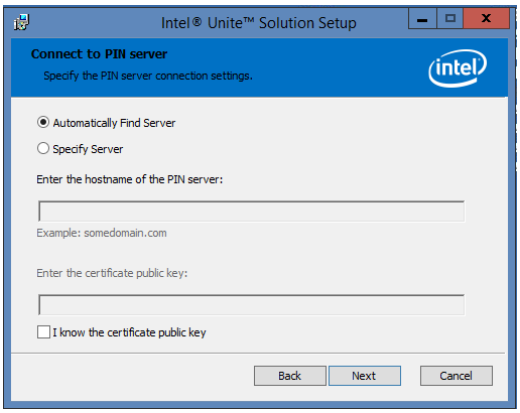
- Click **Next** after you check the box **I accept the terms in the License Agreement**.



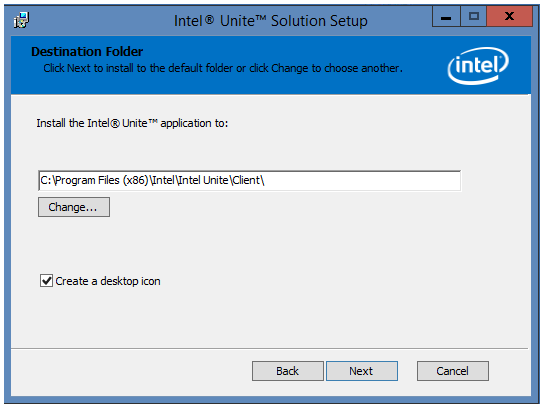

- Select **Enterprise** and click **Next**



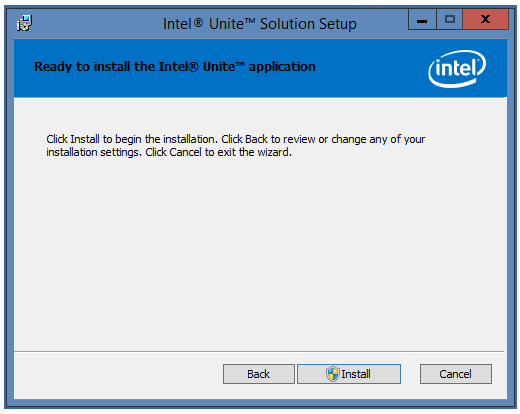
- In this window you must specify the PIN server connection settings. Your choices are:
  - **Automatically Find Server**: This is the most convenient choice (default).
  - **Specify Server**: In this step you need to know the hostname for the Enterprise Server.
    - **Enter the certificate public key**: this option will be enabled when you select **Specify Server**.
    - Enter the **certificate public key** if you have it and have selected this method.
- Select your choice and click on **Next** to continue.



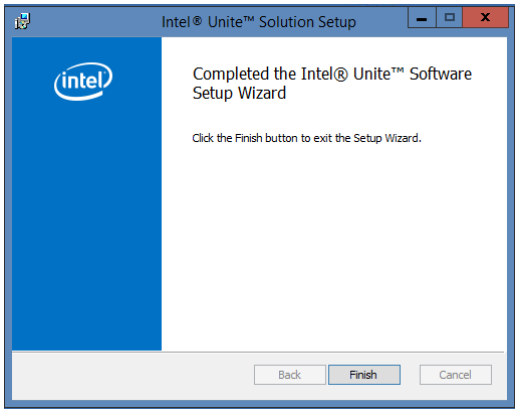

- The **Destination Folder** window will open up with the default folder where Intel Unite application is installed on Client, you can change the destination folder if you wish, otherwise keep the default location. In this step you can also create a desktop icon.




- At this point, you can go back to review your settings or click on **Install** to continue.

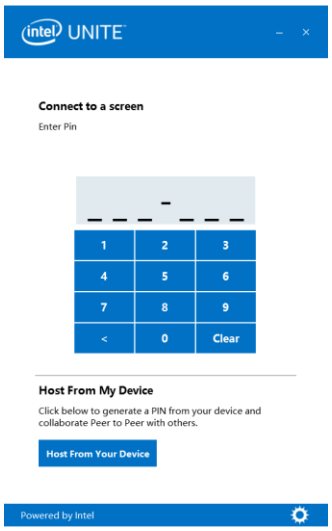



- Once the installation has ended, you will see the **Completed the Intel® Unite™ Software Setup Wizard** window. Click on **Finish** and launch the application if you wish.



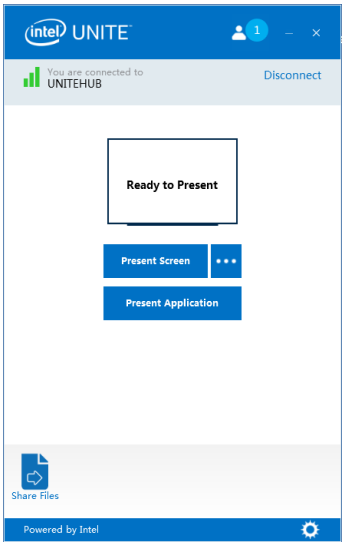

To connect to the display once you have installed the Client, click **Launch Intel® Unite™ application**.

- The following **Connect to a screen** window appears:




- The user then needs to enter a PIN number to connect. This PIN is the one displayed on the Hub. The user can also request a PIN and be the Hub.

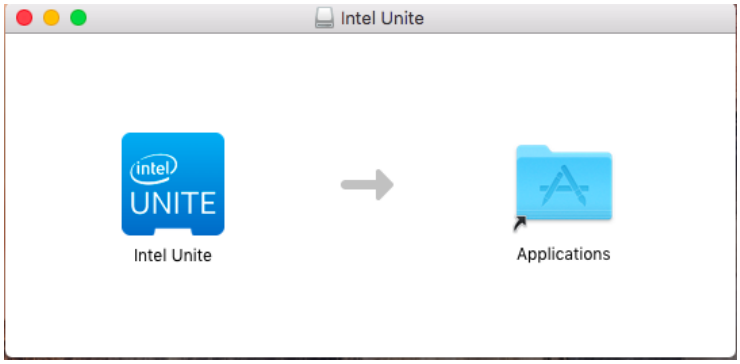
- You will see the **trying to contact your server** screen. The PIN changes every five minutes (by default).
- Once connected, you have the option to click on **Present Screen** or **Present Application**.



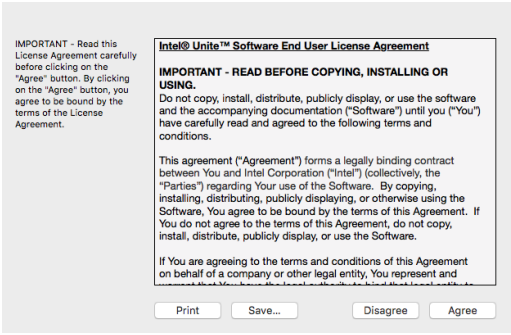

Please refer to the **Intel® Unite™ Solution User Guide** for additional user information about the Intel Unite application.

## 6.3 OS X Client Installation

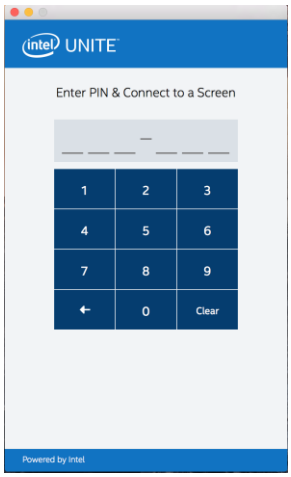
- On your OS X Client download Intel Unite software for Mac Client. Double click the dmg file to extract the application. Drag and drop it to the Applications folder on your Client.

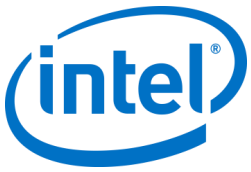



- You will be prompted to accept an end user license agreement. Click **Agree** to continue.




- Once it is installed, you can either launch it by clicking the icon for Intel Unite application in the Applications folder or by running the following command from the terminal (/Applications/Utilities) /pathToUnite/Intel\ Unite.app/Contents/MacOS/Intel\ Unite
- A screen to enter a PIN will be opened and you may connect to the Hub and start sharing.





Without any IT settings defined, the application will use DNS Auto Discovery (DNS service record) to locate the Enterprise Server. Or a default Enterprise Server can be specified by changing the settings to the com.intel.Intel-Unite.plist located in the user's ~/Library/Preferences folder:

defaults write com.intel.Intel-Unite EnterpriseServer myServer.mydomain.myTLD

For more information refer to Intel® Unite™ solution for Mac OS X section of this guide.

## 6.4 iOS Client Installation

- On your iOS Client (i.e. your iPad device) go to the Apple app store and download the Intel Unite software for your Client. The app is compatible with all iPads except the original 2010 iPad.

## 6.5 Client Configuration

Client configuration settings can be changed via the Admin Portal. The Admin Portal contains a default profile with default configuration settings that are applied to all Clients that are checking in with the server. The configuration options are pushed to the Client after a connection from the Client to the Enterprise Server is established. The settings are updated each time the Client checks in.

Please refer to Profile Configuration to understand your configuration options.

# 7 Advanced Installation

## 7.1 Scripted Installers

This section provides information to run the installers silently, without any menus or windows appearing. In this way, property parameters will be passed to the installer via command line.

To run the silent installers, open the command prompt and use the following command line:

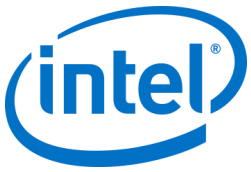
msiexec /i "PATH_TO_CLIENT_MSI" PARAMETER=VALUE PARAMETER=VALUE ... /qn /l* “PATH_TO_LOG”

- The /i flags the specified MSI for installation. “PATH_TO_CLIENT_MSI” is the file name to the installer you are calling.
- “PARAMETER=VALUE PARAMETER=VALUE ...” is a list of the parameters specified in the table below.
- The /qn flag will run the installer in quiet mode.
- The /l* flag will log output to the logfile you specify.

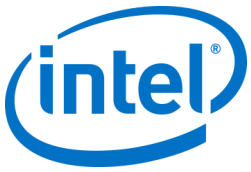
**NOTE:** You can see all options for **msiexec** by running the command: msiexec /?

Below is the full list of property parameters that can be passed into each installer:

| Server Installation Parameters | Description |
|---|---|
| DBHOSTNAME = “local” or “{IP}” or “{server},{port}”<br><br>(defaults to local) | Host name of the Microsoft SQL Server. This will be where the installer creates the UniteServer database and adds the database service account. If installing the database to the current machine, you do not need to include this parameter, as it defaults to local. |
| DBLOGONTYPE = “WinAccount” or “SqlAccount” → defaults to WinAccount | Specifies the logon type to access the Microsoft SQL Server. Options are Windows authentication or SQL authentication. |
| DBUSER = “{SQL username}”<br><br>DBPASSWORD = “{SQL password}” | If logon type is SqlAccount, provide the username and password via these below.<br><br>NOTE: This account must have permissions to add the Database, and create the database service account. |
| DBLOGONPASSWORD = “{service account password}” | The password to be used by the service account to connect to the UniteServer database. |



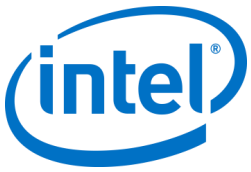
| | |
|---|---|
| DBLOGONPASSWORDCONF = “{service account password}” | This variable must have the same value as specified in DBLOGONPASSWORD |
| **Server Feature Selection Parameters** | **Description** |
| ADDLOCAL = “ALL” | There are only two options: ALL = Install the database AND PIN server, admin portal, and download page.<br><br>(do not specify this variable) = Install Pin Server, admin portal, and download page. |
| **Client and Hub Installation Parameters** | **Description** |
| PINSERVERLOOKUPTYPE = “Lookup” or “Manual”<br><br>defaults to Lookup | Specifies how the application will find the PIN server. Lookup will utilize the DNS service record, while Manual requires the input of the parameters PINSERVER. |
| PINSERVER = “{hostname}” | The host name of the server to connect to. |
| CERTKEYCHECKED = “1” or “0”<br><br>Defaults to 0 | This parameter is optional.<br><br>0 = Don’t check certificate key hash<br><br>1= Check certificate key hash, CERTKEY must also be specified. |
| CERTKEY = “{certificate key}” | This parameter is optional.<br><br>Enter the certificate public key of the PIN Server. |
| SHORTCUTS | Optional. Set to "1" to place desktop shortcut icons. |
| INSTALLTYPE = two possible values "Enterprise" and "Standalone". | If INSTALLTYPE is "Enterprise", then the Client/Hub will install as enterprise. If INSTALLTYPE is "Standalone", then the Client/Hub will install as standalone. |



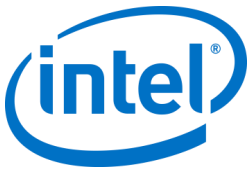
## 7.2 Registry Keys

The registry keys are written to the registry when you run the installers and application. Values in some of these keys can be adjusted in accordance to the desired outcome. See the list below to understand the keys that are written by the Intel Unite application:

| Registry Keys: (current user) | Value | Device |
|---|---|---|
| HKEY_CURRENT_USER\software\Intel\Unite\ ActiveConnection (DWORD) | [0 no users connected, 1 users connected] | Hub |
| HKEY_CURRENT_USER\software\Intel\Unite\ PublicKey (String) | [public key of connection certificate] | Both |
| HKEY_CURRENT_USER\software\Intel\Unite\ CurrentPin (string) | [current PIN of this system] | Hub |
| HKEY_CURRENT_USER\software\Intel\Unite\ DoNotShowPrivacyStatement (DWORD) | [0 show privacy statement on launch, 1 do not show statement] | Both |
| HKEY_CURRENT_USER\software\Intel\Unite\ HWThumbprint (String) | [hash of HW] | Both |
| HKEY_CURRENT_USER\software\Intel\Unite\ LogFile (String) | [path to filename with write access to log runtime debug messages] | Both |
| HKEY_CURRENT_USER\software\Intel\Unite\ ServicePort (DWORD) | [port that service is listening on] | Hub |
| HKEY_CURRENT_USER\software\Intel\Unite\ ActivePresenter | [1 or 0 depending on if an active presentation] | Hub |
| HKEY_CURRENT_USER\software\Intel\Unite\PinPadWindows (DWORD) | [1 if the application is ready to enter a pin, 0 otherwise] | Client |



| | | |
|---|---|---|
| HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\SSID<br><br>Reference: GUEST ACCESS Plugin Guide | Setting a default value will decrease security in Guest Access | Hub |
| HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\PSK<br><br>Reference: GUEST ACCESS Plugin Guide | Setting a default value will decrease security in Guest Access | Hub |
| HKEY_CURRENT_USER\software\Intel\Unite\GuestAccess\Download<br><br>Reference: GUEST ACCESS Plugin Guide | The default download link is `http://192.168.173.1/download` | Hub |
| **Registry Keys: (machine)** | **Value** | **Device** |
| HKEY_LOCAL_MACHINE\software\Intel\Unite\ HubUnlockPassword (String) | [password to exit Hub application] | Hub |
| HKEY_LOCAL_MACHINE\software\Intel\Unite\ DisableCheckCertificateChain (DWORD) | [Set for Self-Signed Certificates, where if 1 = do not check certificate chain of Enterprise (Server Certificate)] | Both |
| HKEY_LOCAL_MACHINE\software\Intel\Unite\ DisableUsageCollection (DWORD) | [1 = Disable telemetry data collection] | Both |



| | | |
|---|---|---|
| HKEY_LOCAL_MACHINE\software\Intel\Unite\WindowedMode (DWORD) | [1 in case the user wants the hub to launch in windowed mode (with minimize, maximize and exit buttons), 0 otherwise] | Hub |
| HKEY_LOCAL_MACHINE\software\Intel\Unite\AllowInsecureCertificates (DWORD) | [1 if certificate algorithm check should be skipped, 0 otherwise. (if value is 0, we force the enterprise certificate to use a SHA2 certificate)] | Both |
| HKEY_LOCAL_MACHINE\software\Intel\Unite\ShowOnlyInOneMonitor (DWORD) | [This key only works if windowed mode is set to 1. If this key is set to 1 it will only show one pin window even though it has more monitor plugged] | Hub |
| HKEY_LOCAL_MACHINE\software\Intel\Unite\GuestAccess | Key used for the Guest Access Plugin | Hub |

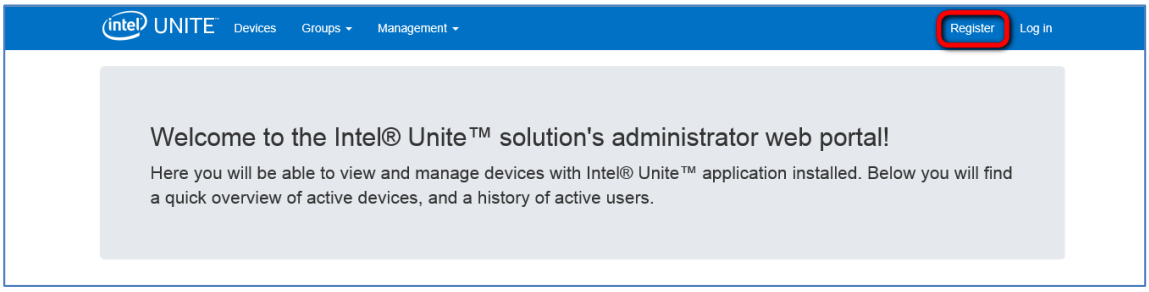
# 8 Admin Portal Guide

Admin Portal is the administrator web portal for Intel Unite application which will let you view and manage the devices on which the Intel Unite application is installed. It is one of the components installed on the Enterprise Server along with the PIN service and Web Server during the installation. (See section on Enterprise Server Installation). Admin Portal need not be on the same server as the database, as long as it has access to the database.

A default administrator account is created during the installation with the following username and password:

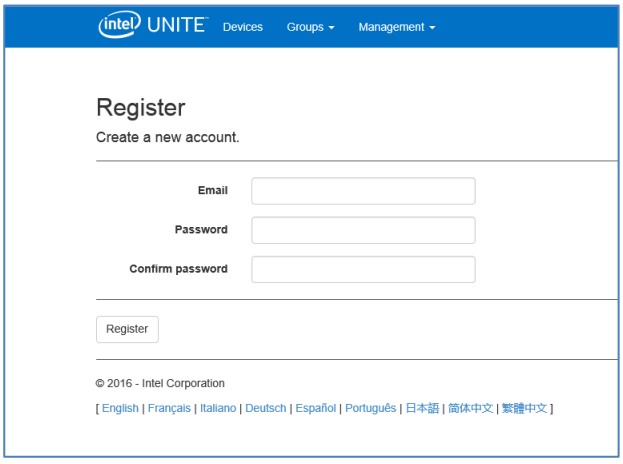
- User: admin@server.com
- Password: Admin@1

This account has complete access to the Admin Portal and it is recommended that you change the password or create a new account.



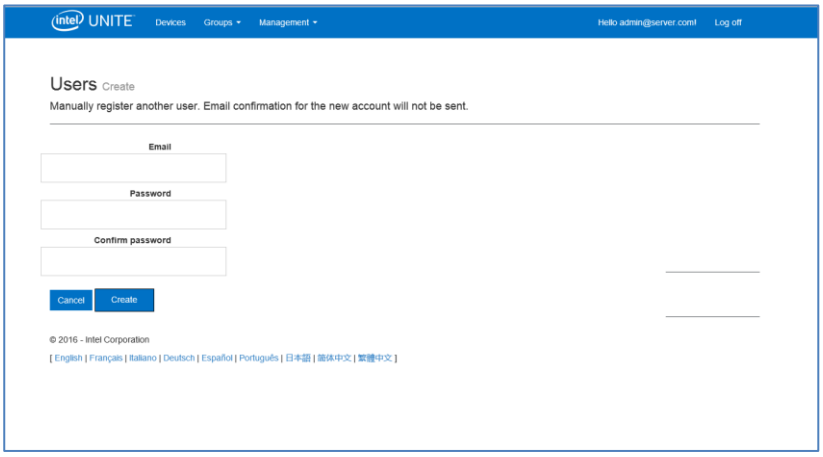

To create a new account

- Make sure you are logged out of the web portal.
- Click on the **Register** link at the top right of the navigation bar.
- Fill in the form with the desired email address and password and click **Register**.



Or alternatively, to add a new user account you can:

- Log in to the Admin Portal as admin@server.com.
- Click on the **Management** link in the navigation bar, and **Users** in the dropdown menu.
- Click **Create** and enter the desired email address and password.




**NOTE:** Adding a new user account by logging in with the default admin@server.com account will not automatically send an email verification. To manually verify the email address, log in to the new account, click the "Hello <your user name>!" in the top right of the navigation bar, and hit the "Send Email Verification" button at the bottom of the page. Before you do this, you will need to edit your server's mail settings in the web.config xml file. See section on Email Server Settings.

To assign access rights to the new user, you can define roles and assign the user to a role. See details under Roles and Role Assignments in the Management page.

## 8.1 The Admin Portal Navigation Bar

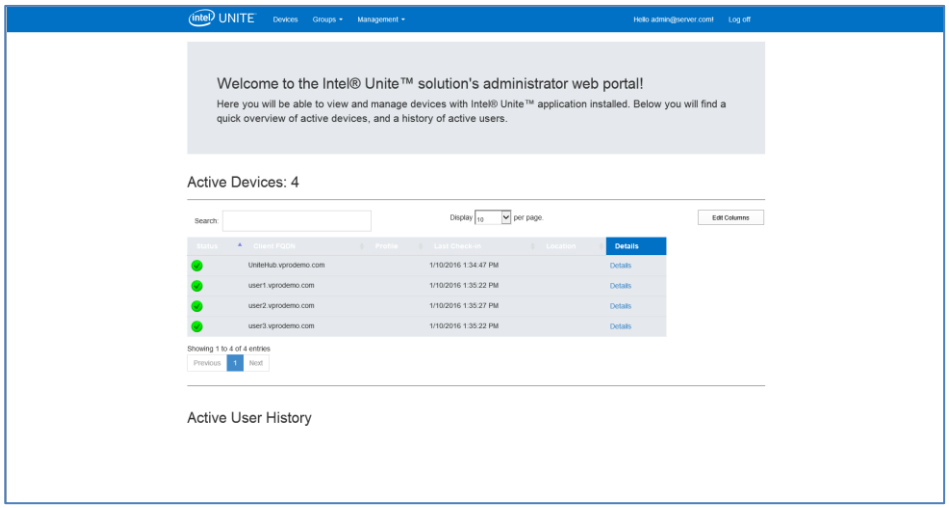
The navigation bar will direct you to the different areas of the web portal and also shows the currently logged in user or will show **Register** if no user is logged in. The web portal pages are:

- Admin Portal Home Page
- Devices
- Groups
- Management

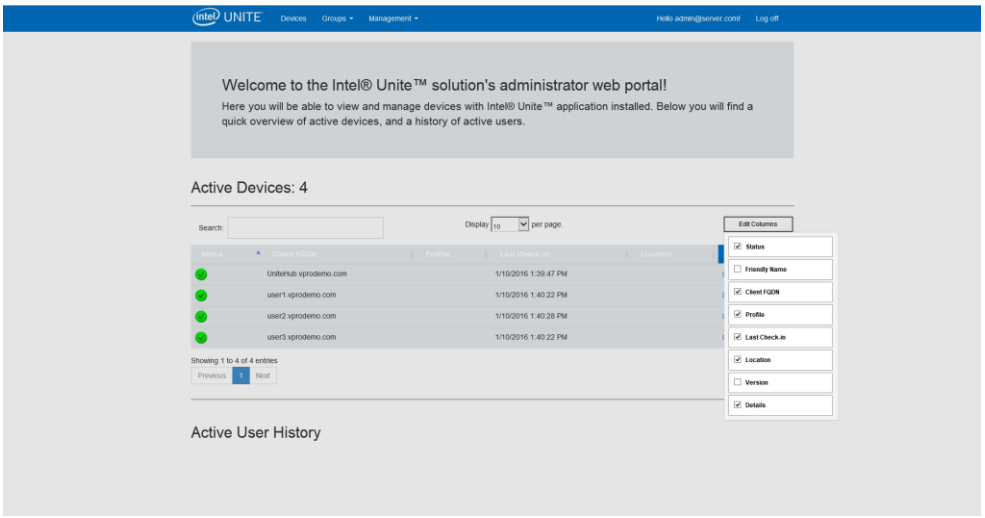
See the next section for details on each of these pages of the Admin Portal.


### 8.1.1 Admin Portal Home page

This page contains a welcome message and provides a quick overview of all active Clients and Hubs that have checked in with the server under Active Devices. The table displays the Status, Client Name and FQDN, Profile, last check-in time, location and details of each of the devices.




The entries of the table can be filtered using the search box with multiple Keywords and each keyword will search through all the columns. Columns in the table may be shown or hidden by clicking the **Edit Columns** button, but will be counted in the filtering regardless of visibility.



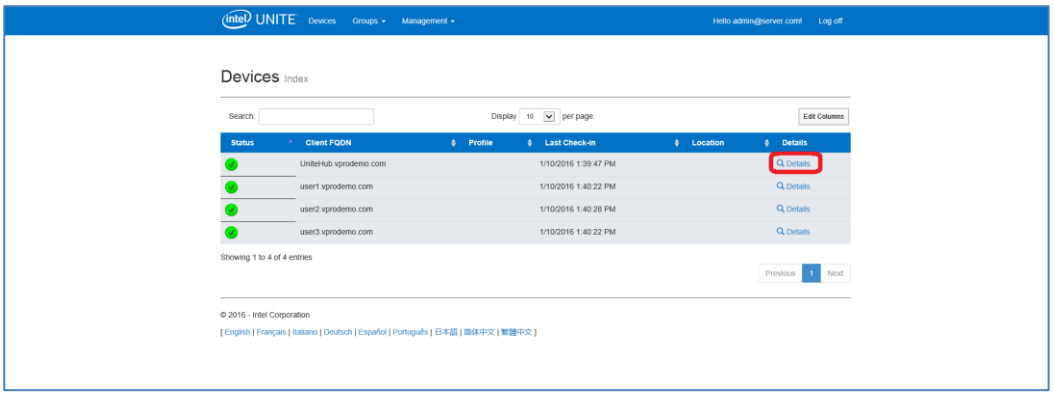

Additional properties of a device can be viewed by clicking on the Details link next to each device in the table. (For more information on **Details** link see section on Devices)

### 8.1.2 Devices

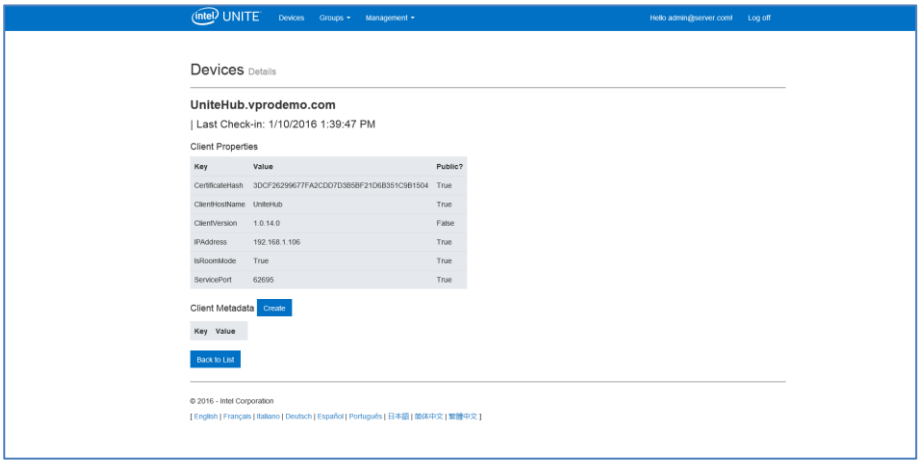
The Devices page contains all devices currently in the database. This page allows you to select device information you want to see in the table by clicking on **Edit Columns** to customize the table.

Available fields to display in this page are:

- Status – Shows if the client is active (green icon) or inactive (yellow icon) device
- Friendly Name – Is the customized device name
- Client FQDN – Is the Fully qualified domain name of the Client/Hub
- Profile – Has configuration settings that are applied to the devices
- Last Check-in – It is the last time the device checked in with the server
- Location – To view the device location (will be implemented in future versions)
- Version – Version number, (will be implemented in future versions)
- Details – Has detailed information on each device




Additional information on each device can be viewed by clicking on the Details link for each device.




You can create Client Metadata to view other client properties. There are several important metadata keys to note that the portal uses to populate certain tables.

- Location – text value, it is the location field of the device table
- ManagementLink – text value, will create a **Manage at ...** button on the details page of a device, which hyperlinks to the value. The value should be the full URL or the button may not work properly.
- FriendlyName – text value, it is the friendly name field of the device table

- EnableReporting – True or False value, if set to true the server will send out alerts to those with the notification role if the device goes inactive. If the key isn't present or the key is set to False, the client will not be monitored.

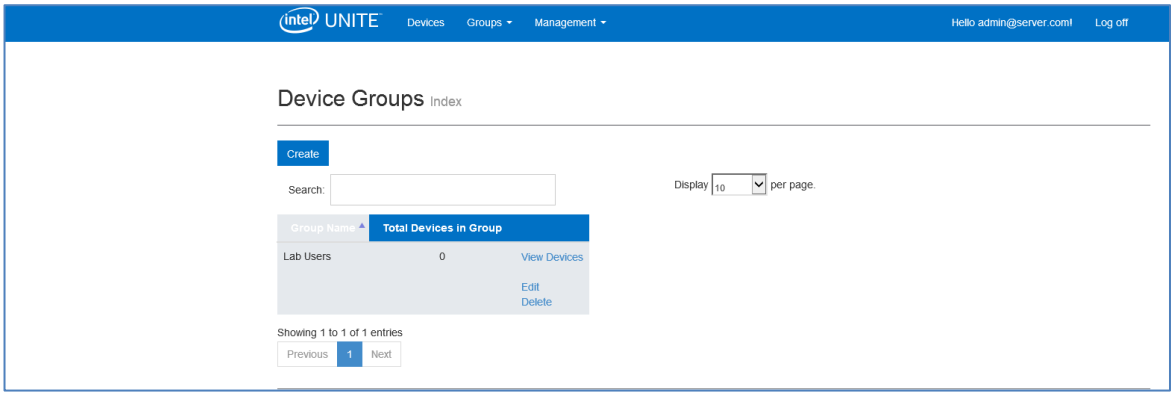
### 8.1.3 Groups

The Groups page gives you two options in the menu: Device Groups and Profiles


#### 8.1.3.1 Groups > Device Groups

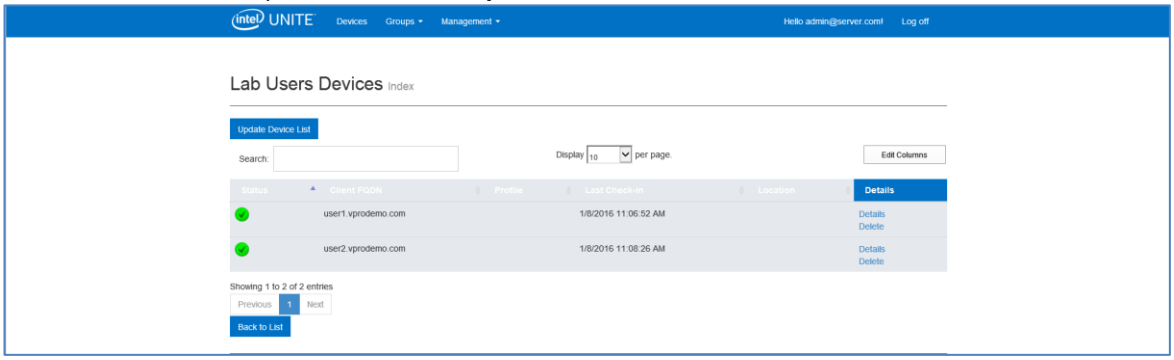
Device Groups provides a way for you to group devices together for monitoring. This page lets you create, view, edit and delete the groups and entries for each group.

In this page you can create a new group by clicking on **Create** and providing the name of the group.

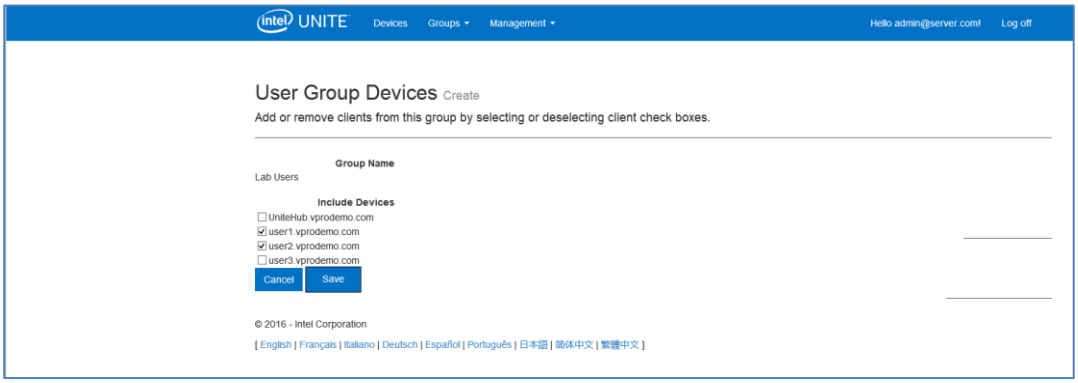



To add or remove devices in a group:

- Click on **View Devices**
- Under the Group Devices, click on **Update Device** List



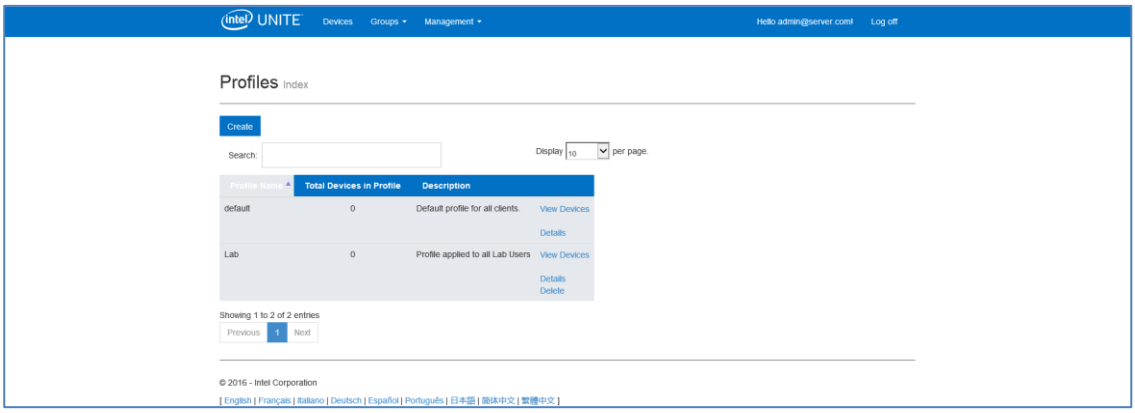
- Add or remove devices by selecting or deselecting the check boxes next to each device.




- Click on **Save** to save changes.

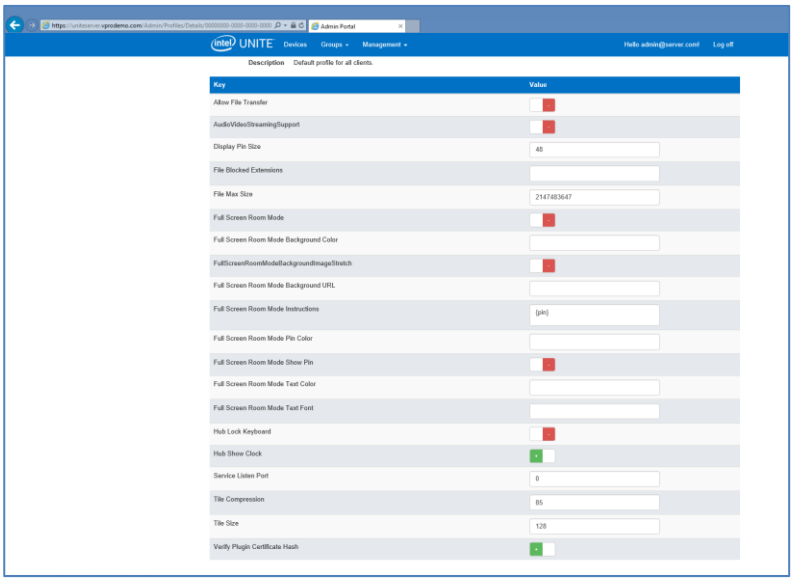
### 8.1.3.2 Groups > Profiles

This page allows you to create, view, delete and edit the profiles. It is similar in layout and function to **Device Groups**, but contains profiles. The difference between Profiles and Groups is that Profiles contain the configuration options for devices. Devices may only belong to one profile, while they can belong to many device groups.



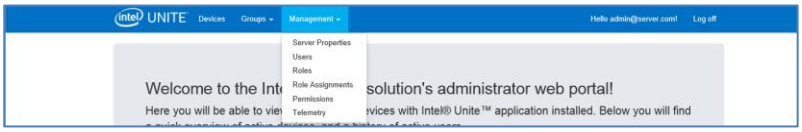

Profiles page displays the default profile that is applied to all devices checking in with the Enterprise Server for the first time.

To access and edit configuration settings of the default or newly created profile, click on **Details** of a particular profile. See section on Profile Configuration for more information editing the configuration settings.




## 8.1.4 Management

The Management page drops down into several sub-pages:

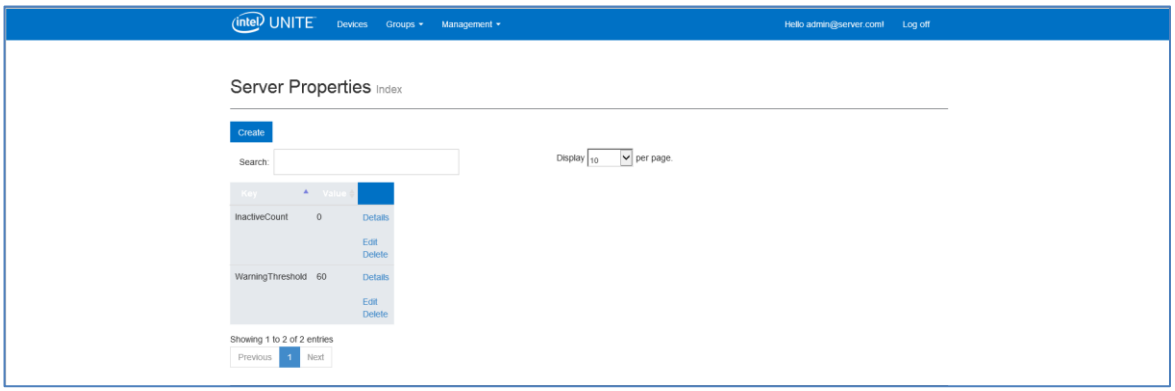



- Server Properties: is the interface for viewing and modifying server keys and values.
- Users: you may add, remove or manually edit any account on this page.
- Roles: will allow you to create new roles for user management.
- Role Assignments: will allow you to assign users to roles.
- Permissions: will allow you to edit access rights for actions on the portal.

For more information on these sub-pages, see sections below.

### 8.1.4.1 Management > Server Properties

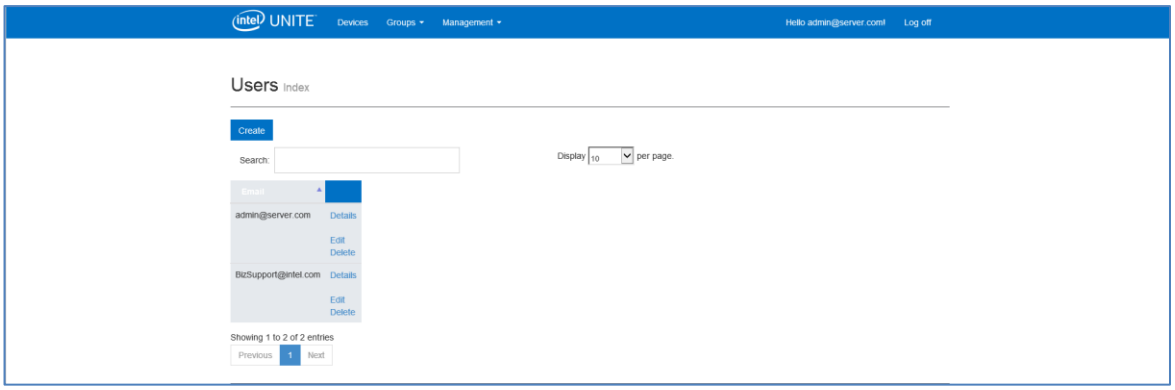
On this page you can view, create, edit and delete key-value pairs for the server.



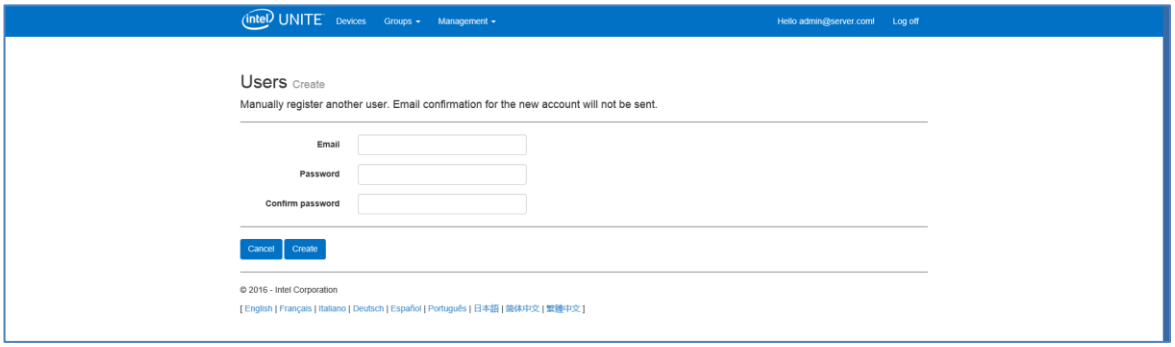

The two notable keys that the Admin Portal uses are **InactiveCount** and **WarningThreshold**. The first is used by the Intel Unite application's health monitoring tool that emails users that are assigned the **Notifications** role. The second is used to determine the threshold of when a device is considered to be inactive, in minutes. The default value for **WarningThreshold** is 60 minutes.

### 8.1.4.2 Management > Users

This page allows you to view the current users of the Admin Portal and user access details like password hash, access fail count etc.

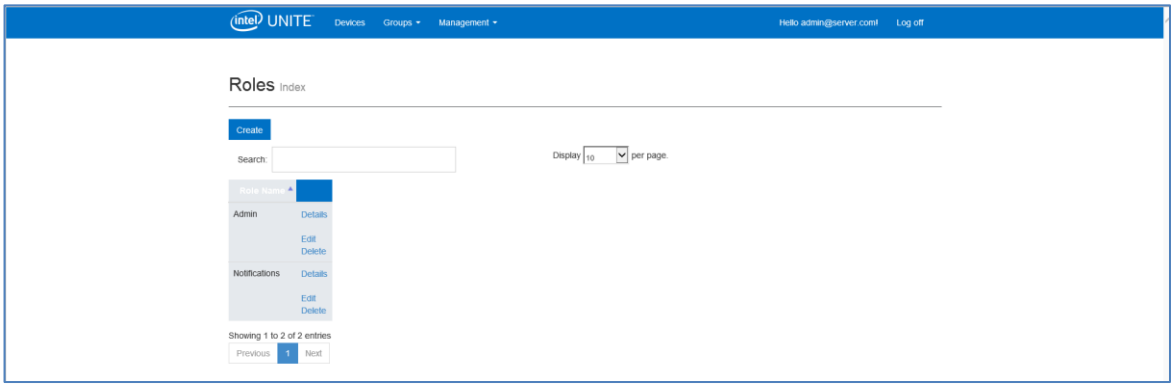



You can add a new user by clicking **Create** and providing an email and password for the user.



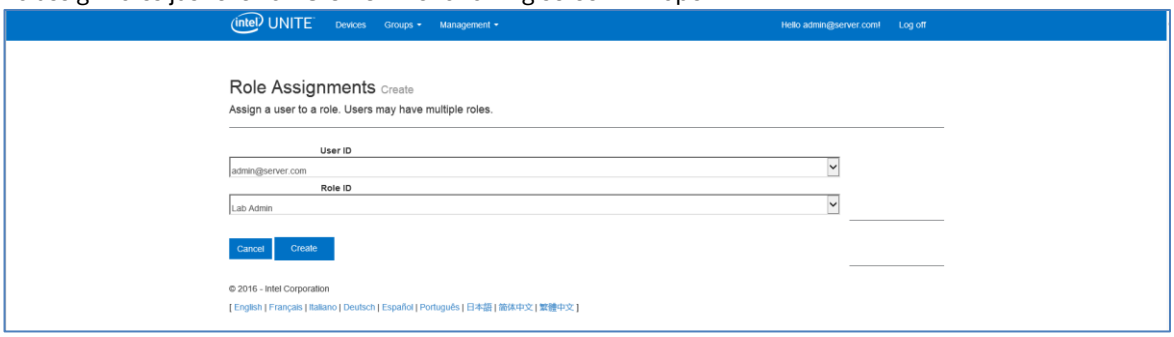
### 8.1.4.3 Management > Roles

This page shows the roles that are currently defined. You can add new roles and delete current roles. Roles alone do not regulate access to the portal, instead the actions on the portal (e.g. creating a user) are restricted to roles, which are associated with sets of users. By default, the roles **Admin** and **Notifications** are defined. The **Admin** role will have access to all actions on the portal. The **Notifications** role does not have any access, but is used for monitoring to determine which users to send email notifications.




### 8.1.4.4 Management > Role Assignments

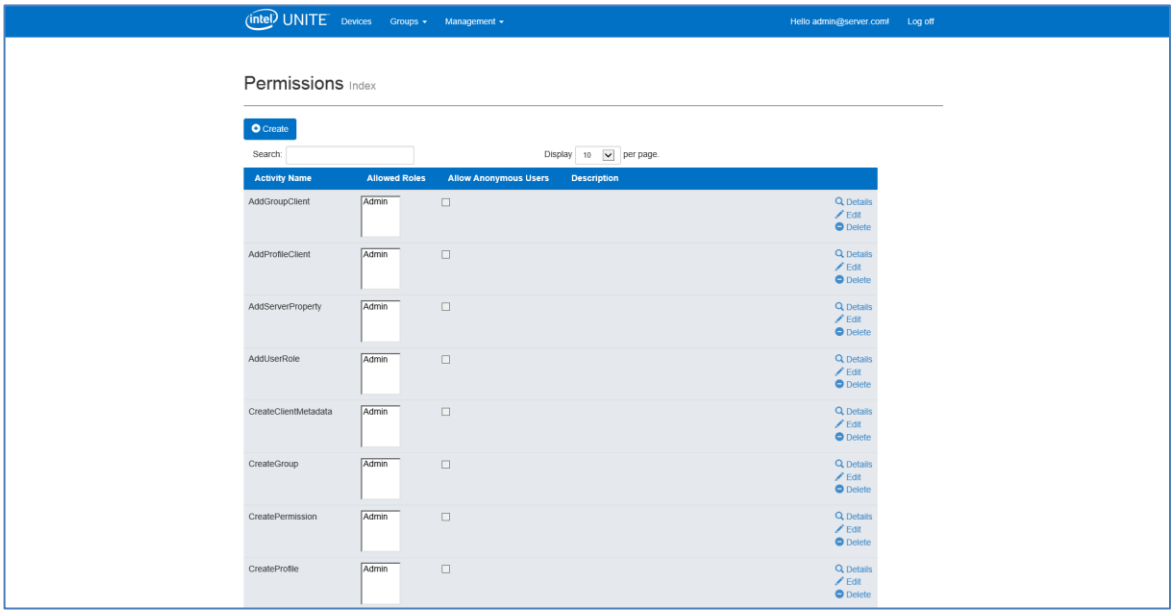
This page will allow you to assign users to roles. When a user is assigned a new role, they are notified via email. A user may be assigned to multiple Roles.
To assign roles just click on **Create**. The following screen will open:




To assign role to a new account, make sure you are logged in with admin@server.com and click on **Create** in the Role Assignments page.

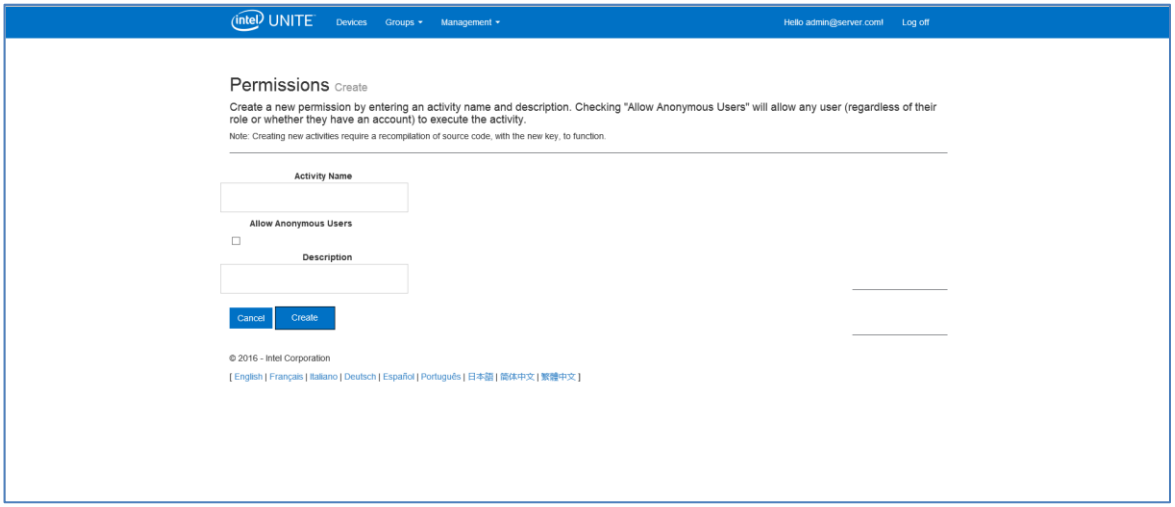
### 8.1.4.5 Management > Permissions

This page contains the definitions of all actions in the portal. These actions can be customized to allow a set of roles to perform the action. If **Allow Anonymous Users** is checked, then any user or visitor to the portal will be able to perform that action.




To create new permissions, click on **Create**. This will let you create new permissions by adding Activity Name, its Description and choosing to allow/disallow Anonymous Users.

Once a new **Permission** is created, you may add **Allowed Roles** to the **Permission** to regulate access to the portal.



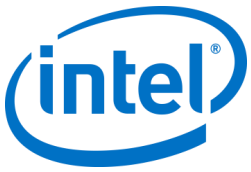
## 8.2 Other Configuration Options

### 8.2.1 Profile Configuration

Profiles can be configured by accessing **Groups** > **Profiles** and clicking on **Details** of the profile in the Admin Portal. This displays the configuration settings in the form of a "Key-value" pair. You can change the values to customize the application and the experience of the meeting space. For example, background image for Hub display, PIN size, font color and content are some of the settings that can be customized. After customizing the values in a profile, assign devices to the profile to apply the profile configuration settings. To apply the profile to devices, click on **View Devices** and then **Update Device List**. You will see the list of devices, click on the check box next to the device to apply the configuration settings.

The table below shows the available **Keys**, their description, data type and default values of the keys.

| Key | Description | Data Type | Default Value |
|---|---|---|---|
| Allow File Transfer | Flag to enable/disable the ability for a Hub or Client to transfer a file | Boolean | True |
| Audio Video Streaming Support | Flag to enable Windows users the ability to present their desktop with the full A/V experience (1080p at 20-30fps) | Boolean | True |
| Display PIN Size | 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 |
| File Blocked Extensions | Comma separated list of blocked file extensions | Integer | Blank |
| File Max Size | Max file size for file transfers | | 2147483647 Bytes<br><br>(valid range: 0-2147483647) |
| Full Screen Room Mode | Enable/disable Hub full screen<br>False: PIN in upper right only<br>True: PIN in upper right and a full screen background | Boolean | False |
| Full Screen Room Mode Background Color | Background color used on the Hub. HTML colors (Hexadecimal colors).<br><br>Examples of valid values (RGB values, format #000000 ) are:<br>Red: #FF0000<br>Yellow: #FFFF00<br>Green: #00FF00<br>Light Blue: #00FFFF<br>Dark Blue: #0000FF | String | Blank |



| | | | |
|---|---|---|---|
| | Black: #000000<br>White: #FFFFFF<br>Grey: #808080 | | |
| Full Screen Room Mode Background Image Stretch | Flag to set the background image to stretch across the entire screen | Boolean | False |
| Full Screen Room Mode Background URL | Sets the Hub background to the URL or image (jpg/png) specified. Set value to True if you want this feature<br><br>Example:<br>http://myserver.com/background.jpg | Boolean | Blank |
| Full Screen Room Mode Instructions | Text instructions to be displayed on Hub. Can use {pin} and {host} as replacements<br><br>URL for download of the Client. This item is displayed on the full screen room mode screen. | String | {pin} |
| Full Screen Room Mode Pin Color | Color of the PIN displayed | String | Blank |
| Full Screen Room Mode Show Pin | Show instructions. Set value to True if you want this feature | Boolean | False |
| Full Screen Room Mode Text Color | Color of the text displayed on Hub | String | Blank |
| Full Screen Room Mode Text Font | Name of font for instructions | Integer | Blank |
| Hub Lock Keyboard | Lock out the following: Ctrl-Esc, Alt-Tab, Charms bar, Windows keys and Alt-F4 in Hub<br>If set to True Hub lock out is enabled. Can override with password set in Reg Key Machine | Boolean | False |
| Hub Show Clock | Show clock in bottom right corner | Boolean | True |
| PLUGINCERTIFICATEHASH_GuestAccessPlugin | Certificate Hash value for the Guest Access plugin. Refer to Plugin Certificate Hash Value section for more details | String | Blank |
| Service Listen Port | The TCP port that the service should listen on | Integer | 0<br><br>(0 indicates OS assigned port) |
| Tile Compression | JPG compression level. % of compression to apply to a changed portion of the display (tile) being transmitted over the network | Integer | 85<br><br>(valid range: 5-100) |
| Tile Size | Tile size for breaking screen into chunks. The size, in pixels, for each | Integer | 128 |

| | | | |
|---|---|---|---|
| | tile. A tile is a section of the screen which is evaluated for change. Only changed tiles are transmitted | | (valid range: 32-512) |
| Verify Plugin Certificate Hash | | Boolean | True |

### 8.2.2 Pin Refresh Interval

The default pin refresh interval is 5 minutes, i.e. the PIN displayed on the hub changes every 5 minutes. This can be changed in 1 minute increments from 2 – 60 minutes by modifying the **web.config** file in the root of the web service site virtual directory. This can be accessed via the IIS manager. The file can also be accessed by navigating to the Intel Unite\PinServer directory. By default, this is installed under C:\Program Files (x86)\Intel\Intel Unite\PinServer.
Modify the value under <add key="**PinExpireTimeInMinutes**" value="5"></add> tag to the desired refresh interval.

### 8.2.3 Email Server Settings

The Admin Portal defines the SMTP server in web.config xml file that is created when the Intel Unite application is installed on the server. Depending on where your SMTP server is configured, **mailSettings** have to be modified in the web.config xml file so that "host" points to your SMTP server. (By default, the Web.config xml file is located in C:\Program Files (x86)\Intel\Intel Unite\PinServer.).

The settings in the file are as follows:

```
<mailSettings>

    <smtp from="noreply@uniteserver.com" deliveryMethod="Network">

        <network enableSsl="false" host="smtp.myco.com" port="25"
        userName="noreply@uniteserver.com" password="pass" />

    </smtp>

</mailSettings>
```

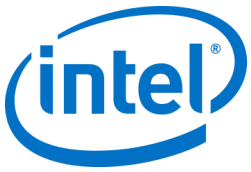
### 8.2.4 Alerting and Monitoring

The Enterprise Server offers Alerting and Monitoring services. This is an opt-in service and is configured in the Admin Portal.

Any device that is configured for alerts will be monitored and if it has not checked in within the warning threshold an email will be sent to specified users.

To opt in to receive emails about inactive devices, make sure that the **Notifications** role has been assigned to the user in Admin Portal. To opt a device into being monitored, add the key **EnableReporting** to its metadata and set the value to **True**.

The warning threshold is configured in **Management** > **Server Properties** and defaults to 60 minutes.



**InactiveCount:** If user wants to get an immediate email in the next check it should be set to a low number.

The email address (smtp from) and email server (host) must be specified in the **clocktower.exe.config** file, which is located in: /productfiles/release/clocktower.exe.config. (By default the location of the clocktower.exe xml config file is C:\Program Files (x86)\Intel\Intel Unite\ClockTower)

The settings in the file are as follows:

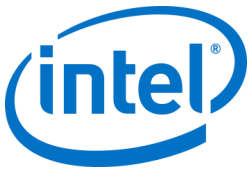
```
<mailSettings>

    <smtp from="noreply@uniteserver.com" deliveryMethod="Network">

        <network enableSsl="false" host="smtp.myco.com" port="25"
        userName="noreply@uniteserver.com" password="pass" />

    </smtp>

</mailSettings>
```



# 9 OS and PC Security Controls

### 9.1.1 Minimum Security Standards (MSS)

It is recommended that all devices running the Intel Unite application are met with your default organization MSS standards, have an agent installed for patching, and an antivirus / IPS / IDS and other necessary control as per the MSS specification (McAfee suite for Anti Malware, IPS, IDS was tested for compatibility).

### 9.1.2 Machine Hardening

Machine Unified Extensible Firmware Interface (UEFI) could be locked to boot the Windows boot loader only (so that boot from a USB disk / DVD will not work), Execute disable bit could be enabled, Intel® Trusted Execution Technology could be enabled, and settings can be locked with a password.

Windows OS Hardening: As a baseline, the system is running with non-elevated user rights. It is also recommended to remove unused software from the OS including unnecessary pre-installed software and Windows components (PowerShell, Print and Document services, Windows location provider, XPS services).

GUI subsystem lock: Since the systems uses a non-touch screen only without keyboard or mouse, it makes it harder to break out of the GUI subsystem. To prevent an attacker from attaching a HID device (USB keyboard/mouse) it is recommended to programmatically block **Alt+Tab**, **Ctrl+Shift+Esc**, and the **Charms** bar.

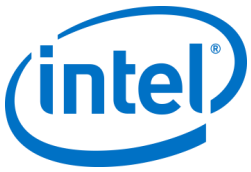
### 9.1.3 Other security controls

It is recommended to lock the machine user account per specific machine account in Active Directory. If the deployment includes a high number of units, user accounts can be locked per a designated floor of a specific building.

Machine ownership: Each machine is recommended to have an identified owner. In case the machine goes offline for an extended period the identified owner will get notified.

Beyond the security mechanisms provided by the Intel vPro platform and the Intel Unite software itself, it is recommended to harden the Microsoft* Windows* OS per Microsoft's guidelines for machine hardening, for reference, please consult the Microsoft Security Compliance Manager* (SCM) in the following link: https://technet.microsoft.com/en-us/solutionaccelerators/cc835245.aspx

**Note:** information in the link contains a wizard based hardening tool, including hardening best known methods and relevant documentation.



# 10 Maintenance

Your organization and IT administrator will decide a regular maintenance program. The following maintenance tasks are recommended:

## 10.1 Nightly reboot

It is recommended to reboot the Hubs on a daily base (preferably at night time) and prior to this reboot, run maintenance tasks such as: wiping cached temp files and initiating the standard patching procedure.

## 10.2 Patching strategy

If available, run your standard patching mechanism in an unattended mode (no GUI prompts) preferably before the above mentioned nightly reboot.

## 10.3 Reporting

Collect the machine uptime indicators and create a tailored report per your organization's needs.

## 10.4 Monitoring

Use a health tracking system based on machines heartbeat and do backend uptime analysis according to need.

### 10.4.1 Backend monitoring:

Use standard virtual server monitoring tools to generate and send alerts to second level support.

# 11 Intel Unite Solution for Mac OS X

## 11.1 Background

The Intel Unite software for OS X is packaged as a primary app package and can leverage IT specific preferences values. In this manner, the app supports a multitude of common deployments from general Mac management software and techniques, to manual installation and setting of preferences.

## 11.2 General Connection Workflow

By default, the app will use DNS Auto Discovery (e.g. DNS SRV records) to determine the proper Enterprise Server to connect to. The overall workflow is as follows:

- (Optional) Enterprise Server as defined in preferences
- Auto Discovery to the following domains:
  - _uniteservice._tcp
  - _uniteservice._tcp.yourSubDomain.yourDomain.yourTLD
    i. Example: _uniteservice._tcp.corp.acme.com
  - _uniteservice._tcp.yourDomain.yourTLD
    i. Example: _uniteservice._tcp.acme.com
  - Attempt connection to HTTPS followed by HTTP if failure
- uniteservice.yourDomain.yourTLD

## 11.3 Preferences Values

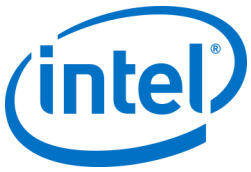
IT can modify and customize the Intel Unite app to meet their own infrastructure or security needs by setting the following settings to the com.intel.Intel-Unite.plist located in each user's ~/Library/Preferences folder:

- **Define a Default Enterprise Server**
  defaults write com.intel.Intel-Unite EnterpriseServer myServer.mydomain.myTLD

- **Define an Enterprise Server Public Key for Certificate Pinning**
  defaults write com.intel.Intel-Unite EnterpriseServerPublicKey "Public Key String"

- **Force a Client to Only Allow Trusted Server Certificates**
  defaults write com.intel.Intel-Unite ClientOnlyAllowsTrustedCertificates -bool true

- **Force a Client to Connect in Standalone Mode**
  defaults write com.intel.Intel-Unite Standalone -bool true



Each of these settings can be set or modified manually by opening the OS X Terminal (/Applications/Utilities) and entering the command followed by a return. Discussion and details of each command are as follows:

- **Define a Default Enterprise Server**
  Setting a Default Enterprise Server will stop the Auto Discovery process from taking place. If your Mac Clients live solely on your own network, this can be a useful setting to "pin" the Intel Unite app to your particular Enterprise Server for security reasons or troubleshooting.

- **Define an Enterprise Server Public Key for Certificate Pinning**
  If you wish to "pin" the Client application to your Enterprise Server, regardless of whether auto discovery is being used, you can do so by setting the “Public Key String” on each Client. To obtain this value:
  - Open Safari on any Mac on your corporate network
  - Go to the HTTPS address of your Enterprise Server
  - Click the lock icon in the Address Bar
  - Click the **Show Certificate** button in the certificate sheet
  - Click the **Details** disclosure triangle to expand it
  - Scroll down the certificate data until you find the **Public Key Info** > **Public Key** field
  - Click on the data field, which starts with "256 bytes:"
  - The data field will expand
  - Select all the data in this field via a mouse selection or CMD+A
  - Copy the data to your clipboard by selecting **Copy** from the context menu or **CMD+C**
  - In the defaults command, replace **Public Key String** with the data from your clipboard. Note: You will need to wrap the data in double quotes.

  Just as with defining a default Enterprise Server, setting this option will make it difficult for your user base to connect to other Intel Unite solution installations at other partners/locations.

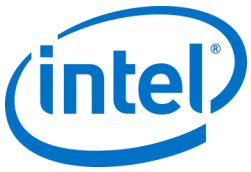
- **Force a Client to Only Allow Trusted Server Certificates**
  Beyond defining a specific Enterprise Server or pinning the certificate Public Key, you can also tell the Intel Unite app to only allow connections to servers/certificates that are fully allowed by your certificate trust chain. In doing so, you must ensure that your Enterprise Server certificate follows back to a public root server as defined by Apple in the keychain, or that you've installed your own root server certificate and any intermediate certificates necessary on each Client.

- **Force a Client to Connect in Standalone Mode**
  Setting this mode will change the connection workflow to perform a UDP Auto Discovery of a Hub that has generated a PIN in an environment without an Enterprise Server. In this scenario the Intel vPro processor-based system will act as the primary host and is useful in a small and medium business environment where there may not be an IT department to install the Enterprise Server infrastructure. This mode will only work across systems on the same subnet where UDP packets are not blocked.

## 11.4 Common Distribution Methodologies

If you are using Auto Discovery, distribution can be as easy as dragging the Intel Unite application to the Applications folder. In more complex environments, or those that require additional security settings, you may want to set specific preferences in conjunction with the app package distribution. There are numerous ways of doing this and here are some of the more common ones:

- Bash Script



- You can define your preference settings in a Bash script that can be distributed to your users in conjunction with the app package.

- Custom Installation Package via PackageMaker
  - You can define your preference settings via a pre or postflight script.
- Custom Installation via Apple Remote Desktop
  - Using Apple Remote Desktop, you can install the Intel Unite app package and define any preference settings via the **Send UNIX Command...** menu.
- Custom Installation via Enterprise Mac Management software
  - You can create a custom push or pull installation via most common Enterprise Mac Management solutions including:
    - Casper / Bushel
    - Puppet
    - Munki
    - Chef
    - Etc.

# 12 Troubleshooting

## 12.1 The Admin Portal page cannot be reached after installing the Intel Unite application on the server

**Workaround/Solution:** Make sure the necessary roles and features for Web Server have been added to the server.

- Add Roles and Features to the server using Server manager
  - Server Roles: Web Server
    - Include Management Tools
  - Add .NET Framework 3.5 features
  - Add .NET Framework 4 features
    - ASP .NET
      - WCF Services
      - HTTP Activation
    - Web Server Roles:
      - Web Server, Common HTTP features and Default Document.

## 12.2 Error when launching Hub application

A pop up window indicates the error ID. Based on the ID, the nature of the error can be determined.

### 12.2.1 Platform check fails with error ID333333

This error indicates that the Hub passed a platform check, but the code-signing certificate couldn't be validated. This is usually due to an OS that doesn't have an updated root certificate, so the public Intel Unite code signing certificate can't be validated.

Ensure the system is connected to the Internet, open a browser and navigate to https://www.microsoft.com (this forces the system to update root certificates).

### 12.2.2 Platform check fails with error ID666666

This error indicates that the platform is not compatible with the Intel Unite application. Check with the OEM vendor to make sure you have a supported platform to run the application.

## 12.3 Hub does not get a PIN from the PIN Server- Scrolling dashes displayed

Launch Intel Unite application on the Hub with a debug switch, i.e. from the command prompt navigate to the folder where the application is saved and run: **IntelUnite.exe** /debug

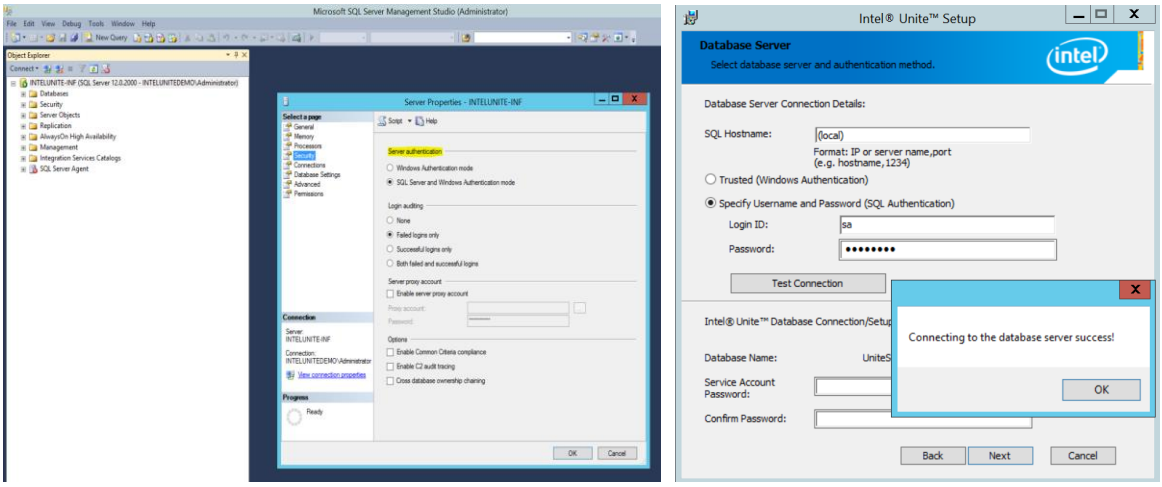
This will open a debug window and display the connection information. Some of the common errors and workarounds are listed below. If the debug information indicates any of these errors, follow the solution/workaround to resolve and get a PIN on the Hub.

### 12.3.1 Server unable to process request; Login failed for user "UniteServiceUser"

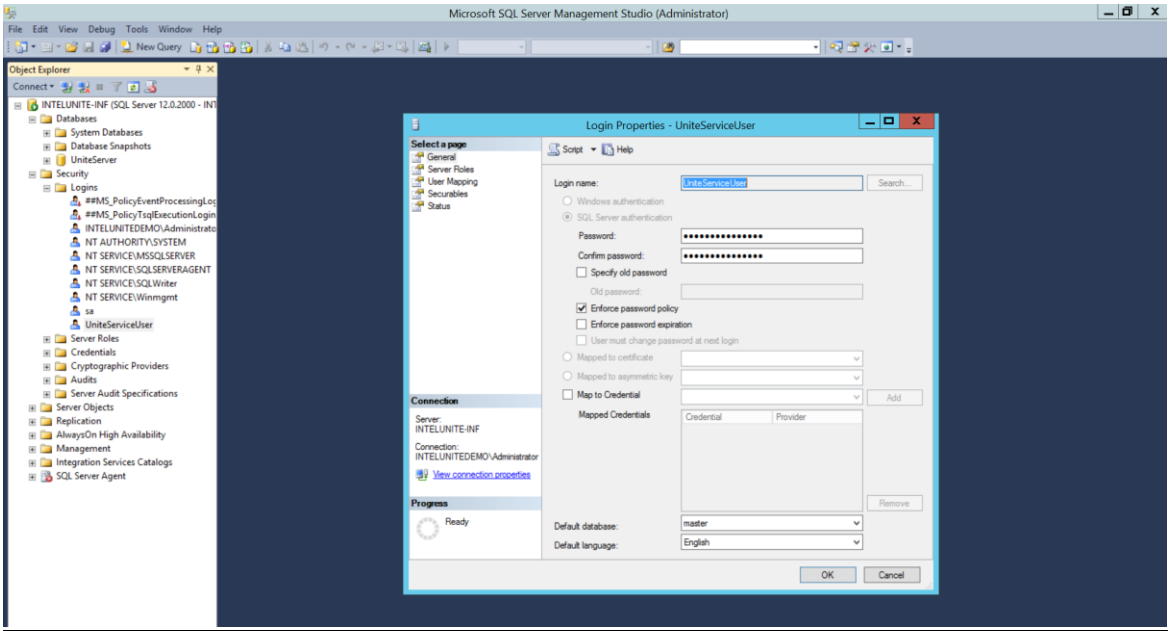
This could happen if there is a SQL login mismatch or if the database password gets corrupted because a user tries to install the Enterprise Server multiple times.

**Workaround/Solution:**

Verify the authentication modes used during MS SQL installation. To change login/authentication type go to Microsoft SQL Management Studio and connect to the SQL server, right click on the SQL server and select Properties. Select Security page and make sure **SQL Server and Windows authentication** mode is selected if SQL authentication is selected when installing Intel Unite application on the server.



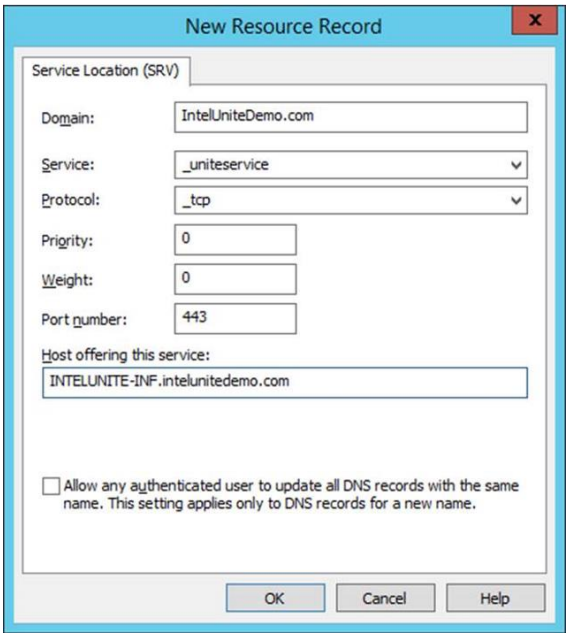

If you still see the error, reset the password for the **UniteServiceUser**. Use Microsoft SQL Management Studio and connect to your SQL server, go to **Security** > **Logins** and right click on **UniteServiceUser** to open a window for **Login Properties**. Enter a new password and click **OK** to save changes.



### 12.3.2 No Servers listed. Trying DNS service record: _uniteservice._tcp

**Workaround/Solution:**

This could happen if the Hub cannot find the DNS record. Make sure the Hub can ping the server on which DNS service is running and a DNS service record has been created for the Intel Unite solution. The service record must have the following values: **Service**: _uniteservice, **Protocol**: _tcp, **Port number**: 443 and **Host offering this service:** FQDN of the Enterprise Server.




### 12.3.3 Could not establish trust relationship for SSL/TLS secure channel with authority 'uniteserverfqdn'

The latest version of Intel Unite solution only accepts SHA-2 certificates or greater. You should work with your IT department to ensure the trusted web server certificate issued is a SHA-2 certificate and the certification path is valid.

For a test environment, obtain a SHA-2 certificate or disable encryption in your environment.

- To use Unite without encryption, skip the next steps that provide details on Site Bindings for secure port 443 and proceed to install MS SQL Server and prepare the DNS service record. You also need to make sure that the service is found on port 80 when a DNS service record is created.
- Another way to skip the certificate check is to add the registry in the machine account of the hub and client. HKEY_LOCAL_MACHINE\software\Intel\Unite\AllowInsecureCertificates (DWORD) [1 if certificate algorithm check should be skipped, 0 otherwise. (if value is 0, we force the enterprise certificate to use a SHA2 certificate)]

## 12.4 Client application crashes on launch/connect

Run the client application with a debug switch and save the information to a log file.

(Run Intel Unite.exe /debug >logfile.txt)

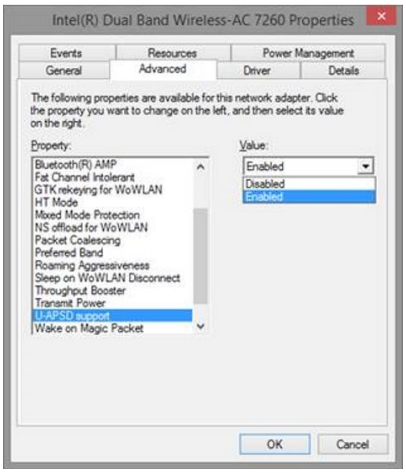
If the log file has the message “EXCEPTION:  - Key not valid for use in specified state.”, close the application and delete the file C:\Users\eaviles\AppData\Roaming\Microsoft\Crypto\RSA\[sid]\d046df

## 12.5 Caution Area: The user may see longer-than-usual connect times, or periodic slow screen updates.

**Root Cause:**

This is a bug with some wireless access points when U-APSD (Unscheduled Automatic Power Save Delivery) is enabled. Refer to http://www.intel.com/support/wireless/wlan/sb/CS-034875.htm.

**Workaround**: As the KB states, this can potentially be solved with an update to the firmware of the wireless access point. In most enterprises, this is not easy to do; as a last resort you can disable U-APSD on the Client in the advanced properties of the wireless driver.




## 12.6 Caution Area: Slowness on the PIN Server

**Workaround/Solution:** The Enterprise Server manages allocation of pins and looking up pins to connect to rooms. As a security feature the rate at which a user can request pins and query pins from the database is limited with an exponential back off algorithm. This back-off mechanism tracks attempts based on the user’s IP address and the number of attempts.

Production servers may utilize load balancers to help manage load and maintain redundancy in the environment. The load balancers redirect traffic to the appropriate web servers. So the web server may appear to be receiving all requests from the same IP address thus triggering the back off algorithms.

The database contains a stored procedure (*spGetPinBackoffTime*) that returns the calculated delay in seconds back to the web server. This functionality can been disabled, so the stored procedure always returns 0. This disables the security back off algorithm.

## 12.7 Mac Client troubleshooting

Launch the Intel Unite application (/Applications/Utilities) from the Terminal to see the debug messages.

/pathToUnite/Intel\ Unite.app/Contents/MacOS/Intel\ Unite

The application will start and you'll see all the debug information in the Terminal.

### 12.7.1 Enterprise Server Connection Error -1003: A server with the specified hostname could not be found.

**Workaround/Solution:** Make sure that the DNS Search Domain is defined correctly.

If a user defines a DNS server but does not specify any Search Domains, when the MAC tries to perform an Auto Discovery there is no DNS domain suffix to search through. If there's no DNS Search Domains defined, the Intel Unite application can't add them to either Auto Discovery or even the "static" entry of *uniteservice*. So unless Auto Discovery works on *_uniteservice._tcp*, the Client won't be able to find the Enterprise Server.

The easiest solution is simply to add a DNS Search Domain (which should match the DNS SRV record), but one could also define the Enterprise Server in the *plist* settings instead.

Use the Terminal command:

*defaults write com.intel.Intel-Unite EnterpriseServer myServer.mydomain.myTLD*

### 12.7.2 Enterprise Server Connection Error -1001: The request timed out

**Workaround/Solution:** This error could be because of the following two reasons.

1. There's potentially a problem with the Web Service on the Enterprise Server.
2. The Mac has a network issue connecting to the server.

The first step in addressing this would be to find the Web Service in the debug log. Look for https://yourserver/Unite/CCService.asmx.
Copy and paste this URL into Safari and confirm that the Mac can get to the Web Service. This will verify if there is a network issue connecting to the server and if the web service on Enterprise server is running.

### 12.7.3 Enterprise Server Connection Error -1200: An SSL error has occurred and a secure connection to the server cannot be made.

Work with your IT department to get valid SHA-2 certificates that are needed for the Intel Unite Solution.

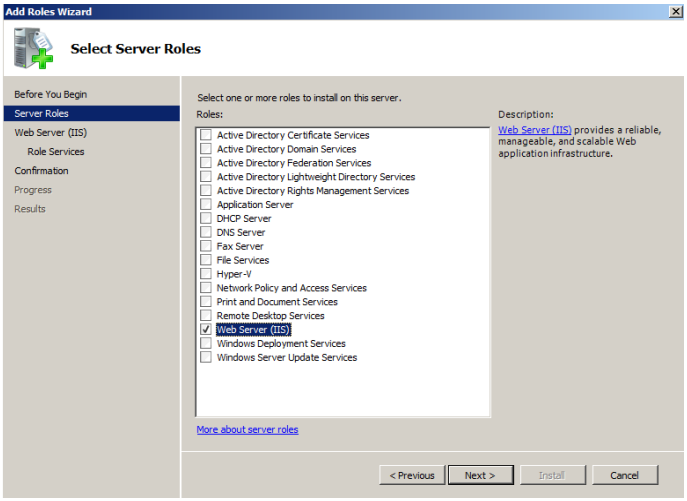
# Appendix A. Enterprise Server Preparation

## Enabling IIS

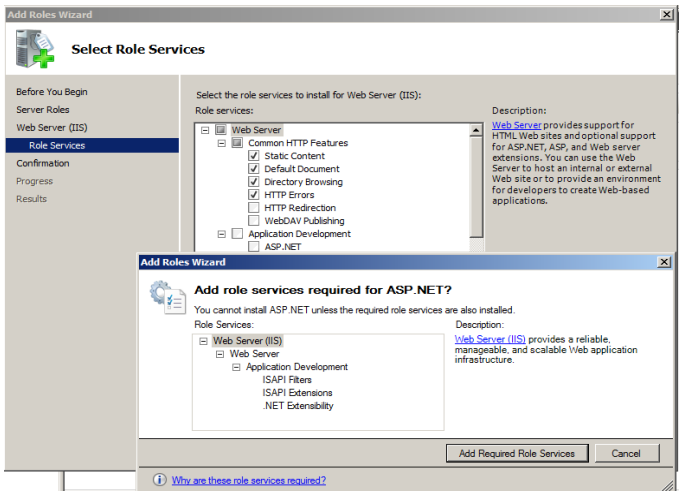
For Windows 2008:

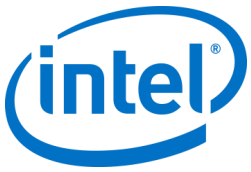
In Windows Server 2008, you would need to download the update for .NET Framework 4.5 (https://www.microsoft.com/en-us/download/details.aspx?id=40779)

- Click **Start**, point to **Administrative Tools** and then click **Server Manager**.
- In **Roles Summary**, click **Add Roles**.
- Use the **Add Roles Wizard** to add the **Web Server (IIS)** role (check this box).




- Click **Next** until you have the **Select Role Services** window.
- In the **Application Development** section, verify that ASP.NET is checked, if not, select it. Please note that ASP.NET will not be checked by default. **Add Required Role Services** for ASP.NET. You also need ASP.NET 4.5.





- Once the role is created, under the **Roles** menu, go to **Web Server (IIS)** - on the right side of the panel, go to **Internet Information Services (IIS) Manager** and select your server in the left **Connections** pane.

  Reference: Windows Server Library link Installing IIS on Windows Server 2008

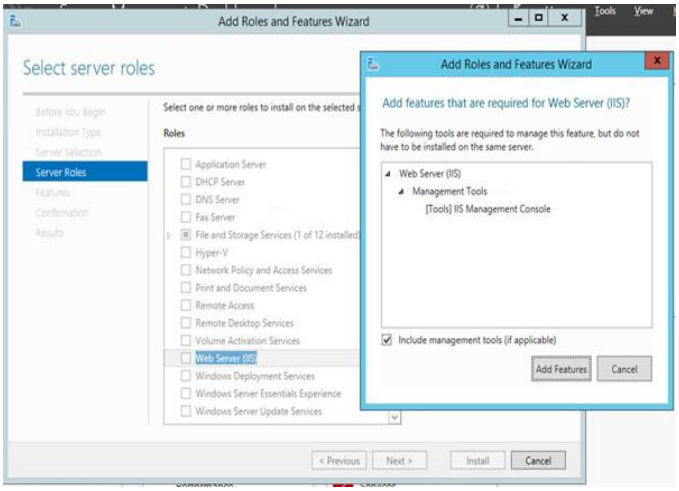
  **Note:** The latest version of Intel Unite solution only accepts SHA-2 certificates or greater. You should work with your IT department to ensure the trusted web server certificate issued is a SHA-2 certificate and the certification path is valid.

  For a test environment, either work with your Certificate Authority team to obtain a SHA-2 certificate or disable encryption.
  - To use Unite without encryption, skip the next steps that provide details on Site Bindings for secure port 443 and proceed to install MS SQL Server and prepare the DNS service record. You also need to make sure that the service is found on port 80 when a DNS service record is created.
  - Alternatively you may skip the certificate check by adding the registry key in the machine account of the hub and client.
    HKEY_LOCAL_MACHINE\software\Intel\Unite\AllowInsecureCertificates (DWORD) [1 if certificate algorithm check should be skipped, 0 otherwise. (if value is 0, we force the enterprise certificate to use a SHA2 certificate)]

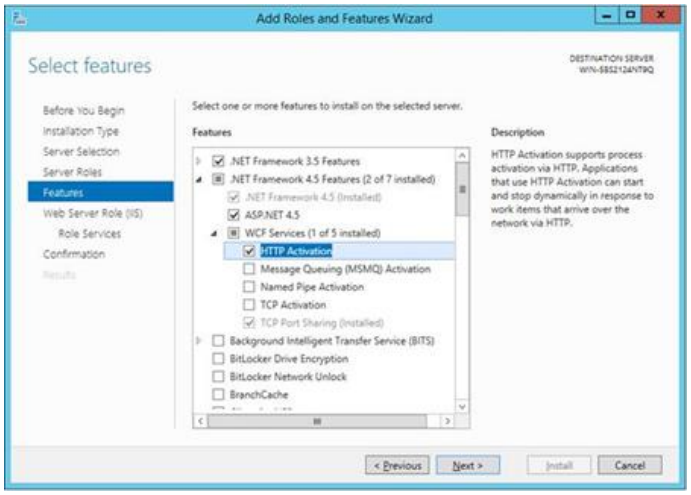
- To assign the certificate, in the left **Connections** pane, expand Sites and click on **Default Web Site**.
- In the right **Actions** pane, select **Bindings** (located under Edit Site).
- In the **Site Bindings** window, click on **Add**.
- Use the following information:
  - Type: https (Note: not http)
  - IP Address: All Unassigned
  - Port: 443
  - Hostname: (leave blank)
  - SSL Certificate: Use the SSL certificate that was installed in the previous steps.
  - Click **OK**.

For Windows 2012:

- Open **Server Manager**.
- Under **Manage** menu, select **Add Roles and Features**.
- Select **Role-based or Feature-based Installation**.
- Select the appropriate server (local is selected by default).
- Select **Web Server (IIS)** and **Add Features** that are required for Web Server (IIS) and click **Next**.

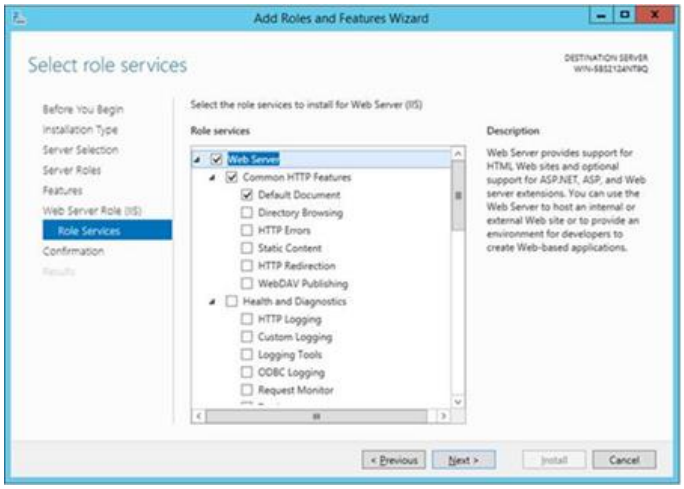



- In Features, add the following features for IIS (as they are not default options):
  - .NET Framework 3.5 Features
  - ASP.NET 4.5
  - WCF Services
  - HTTP Activation (Add features that are required for HTTP activation when prompted) and click **Next**.




**Note:** .NET 3.5 might give an error during installation. Provide an alternate source path if the target computer does not have access to Windows Update. Click on **Specify an alternate source path** link to specify the path to the **\sources\sxs** folder on the installation media.
Reference: https://technet.microsoft.com/en-us/library/dn482071.aspx

- In the Role Services page, add **Web Server (IIS)** as a role to your server or accept the default value.
- Select the following Role Services to install for the Web Server:
  - Common HTTP features
  - Default Document




- Click **Next** to continue and click **Install** on the next window to install the selected roles and features.
- Once the role is created, under the **Roles** menu, go to **Web Server (IIS)** - on the right side of the panel, go to **Internet Information Services (IIS) Manager** and select your server in the left **Connections** pane.

  **Note:** The latest version of the Intel Unite solution only accepts SHA-2 certificates or greater. You should work with your IT department to ensure the trusted web server certificate issued is a SHA-2 certificate and the certification path is valid.

  For a test environment, either disable encryption or create a self-signed SHA 2 certificate.
  - To use Unite without encryption, skip the next steps that provide details on Site Bindings for secure port 443 and proceed to install MS SQL Server and prepare the DNS service record. You also need to make sure that the service is found on port 80 when a DNS service record is created.
  - Run the following PowerShell command as an administrator.
    - New-SelfSignedCertificate –dnsname “yourservername” –CertStoreLocation cert:\LocalMachine\My ; where “yourservername” is the FQDN of the enterprise server.
  - Alternatively you may skip the certificate check by adding the registry key in the machine account of the hub and client.
    HKEY_LOCAL_MACHINE\software\Intel\Unite\AllowInsecureCertificates (DWORD) [1 if certificate algorithm check should be skipped, 0 otherwise. (if value is 0, we force the enterprise certificate to use a SHA2 certificate)]

- To assign the certificate, in the left **Connections** pane, expand Sites and click on **Default Web Site**.
- In the right **Actions** pane, select **Bindings** (located under Edit Site).
- In the **Site Bindings** window, click on **Add**.
- Use the following information:
  - Type: https (Note: not http)
  - IP Address: All Unassigned
  - Port: 443
  - Hostname: (leave blank)
  - SSL Certificate: (select the one you installed in the previous steps)
  - Click **OK**.
- Select **Close**.

Reference: Windows Server Library link [Installing IIS on Windows Server 2012]

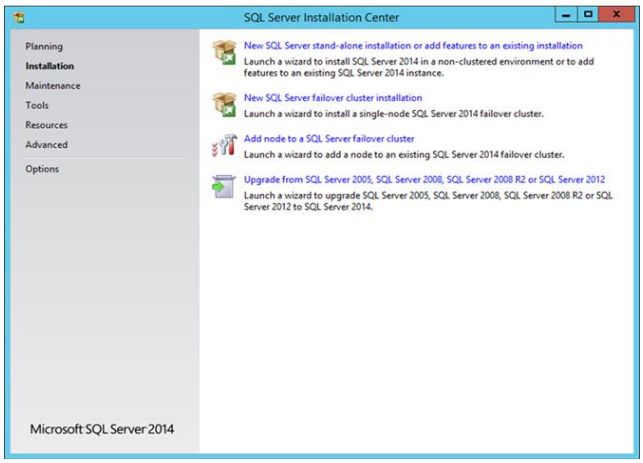
Note about port 443: The web service for Intel Unite application communicates with the Clients and Hubs using port 443 so make sure this port is enabled as mentioned above.

## Microsoft SQL Server Install

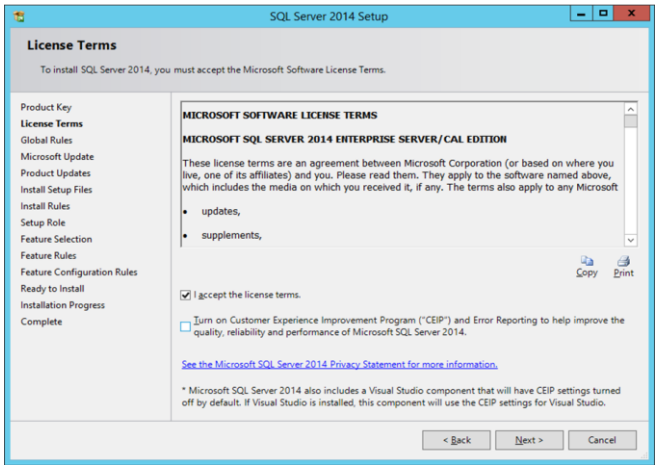
The Enterprise Server requires MS SQL to run, minimum requirements are version 2008 R2 or higher. You can install a new, dedicated SQL server if you wish to run a "test environment" and get comfortable with the application, however, it is not required. The Intel Unite application will create its own database, data tables and indexes in your existing database without interfering with other tables or existing data.

See below for installing MS SQL 2014

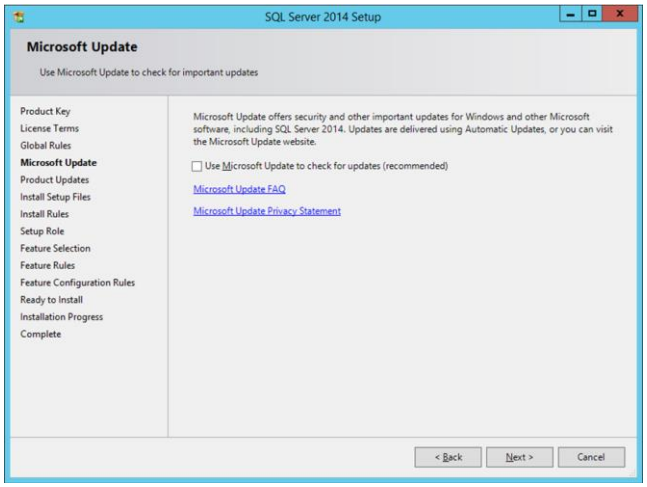
- Run the SQL server setup and open the SQL server installation Center. Click on **Installation** on the left pane and choose **New SQL Server stand-alone installation or add features to an existing installation**.



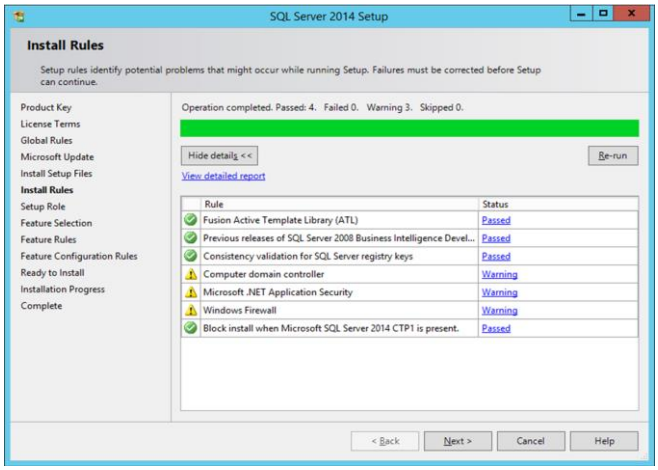

- Enter the product key, accept the license terms and click **Next**.



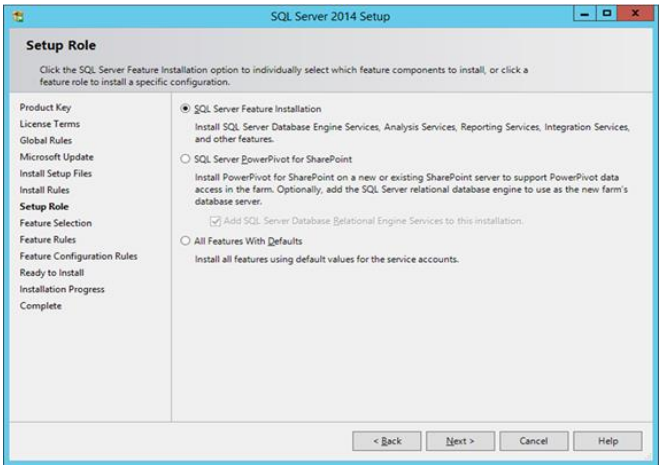

- Select **Use Microsoft Update to check for updates (recommended)** to check for updates and click **Next**. On the next window, the setup will look for Product Updates and install the necessary updates. To continue, click **Next**.


SQL Server 2014 Setup
Microsoft Update
Use Microsoft Update to check for important updates
Product Key
License Terms
Global Rules
Microsoft Update
Product Updates
Install Setup Files
Install Rules
Setup Role
Feature Selection
Feature Rules
Feature Configuration Rules
Ready to Install
Installation Progress
Complete
Microsoft Update offers security and other important updates for Windows and other Microsoft software, including SQL Server 2014. Updates are delivered using Automatic Updates, or you can visit the Microsoft Update website.
Use Microsoft Update to check for updates (recommended)
Microsoft Update FAQ
Microsoft Update Privacy Statement
< Back
Next >
Cancel

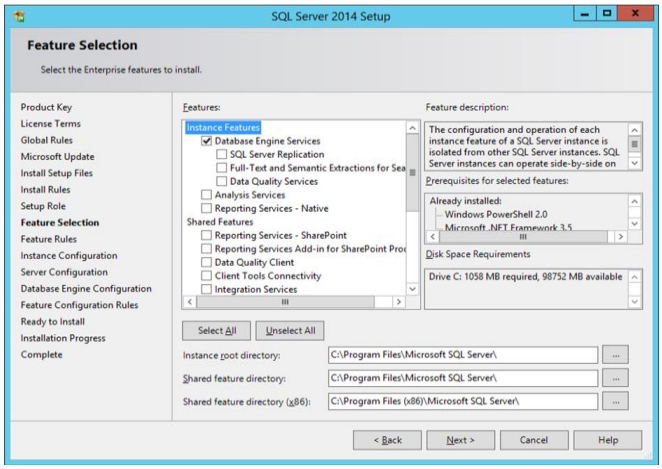
- SQL setup checks for potential failures and requirements to be met before the installation. Click **Next** to continue.



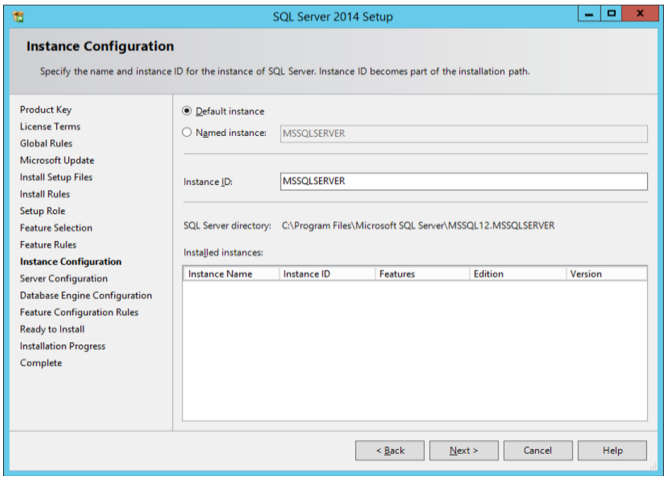

- Select **SQL Server Feature Installation** and click **Next**.



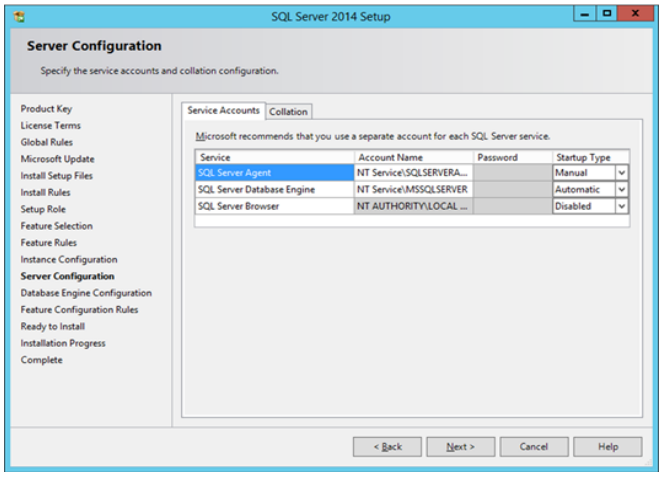

- Under the feature selection, select **Database Engine Services**, **Management tools- Complete** and click **Next**.



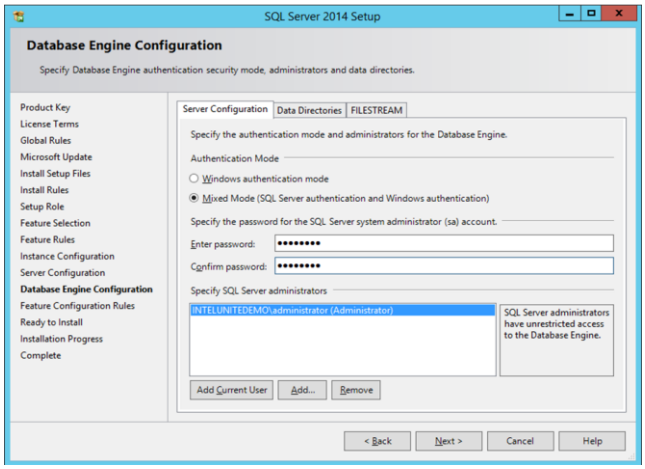
- Specify the name and instance ID for the SQL server and click **Next**.



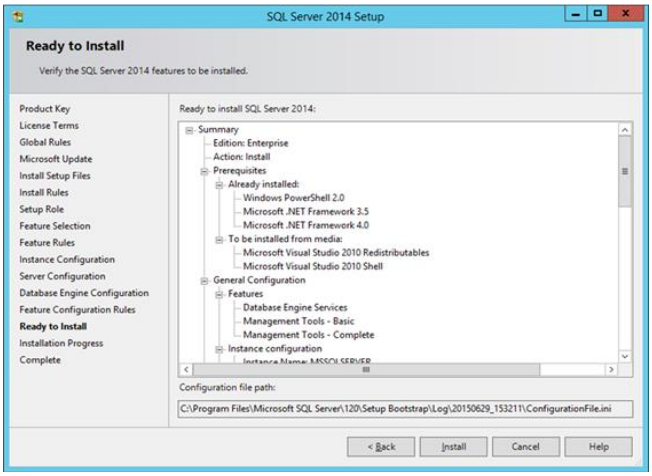

- Specify the service accounts for each service and click **Next** to continue.



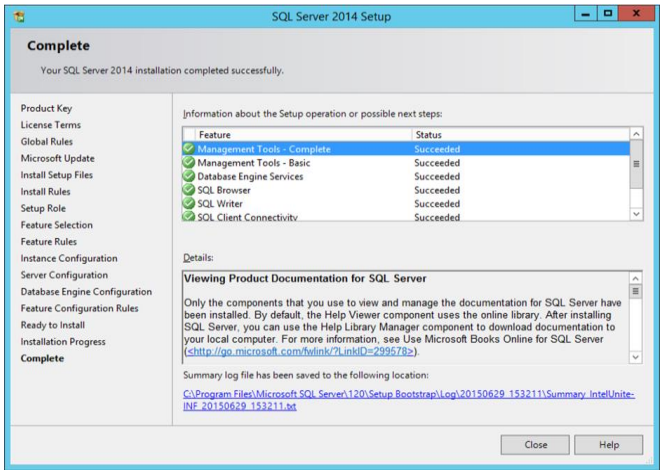
- Select Mixed Mode Authentication (which includes SQL server and Windows authentication), specify the SQL Server administrators and click **Next**.




- Verify the features to be installed and click on **Install**.




- Close the dialog box after the installation is complete.



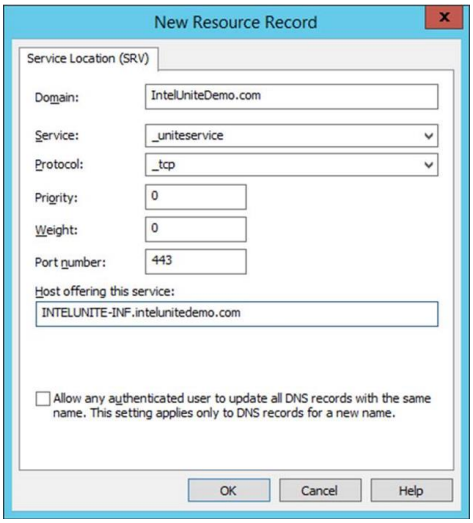
## Creating a DNS service record

The Hub or Clients will locate the Enterprise Server using DNS service during an automatic lookup for the Enterprise Server. You may also use the manual lookup but it is highly recommended that you use DNS. If you plan on providing the Enterprise Server hostname manually during Hub and Client installation, you can skip this section.

When a DNS service record is used, the Hub or Client will look for the service named _uniteservice._tcp within the DNS service records _uniteservice._tcp.example.com 86400 IN 0 5 443 uniteserver.example.com.

To add a DNS Service Record in Microsoft Windows:

- On your DNS server, open DNS Manager.
- Expand the Forward Lookup Zones (left pane).
- Right click on the zone and select "Other New Records..."
    - In **Select a resource record type:** select **Service Location (SRV)** and select **Create Record**.
    - For **Service** enter: _uniteservice
    - For **Protocol** enter: _tcp
    - For **Port** enter: 443
    - Host offering this service: Enter the hostname/IP of the Enterprise server(s).

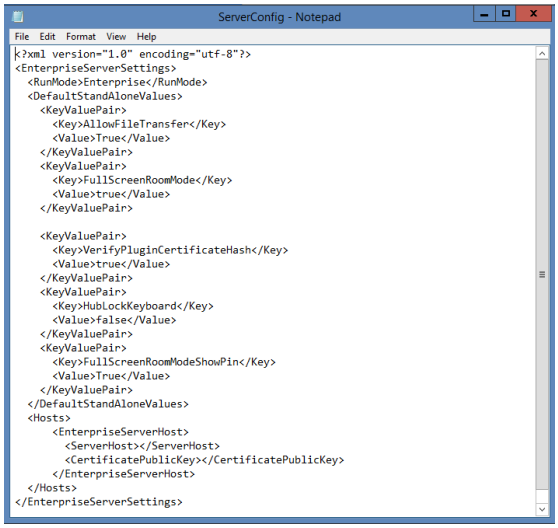


# Appendix B. Example of ServerConfig.xml

The ServerConfig.xml file gets created during the installation of hub and client components of the Intel Unite software. The default location of the xml file is C:\Program Files (x86)\Intel\Intel Unite\Hub or C:\Program Files (x86)\Intel\Intel Unite\Client for Hub and Client respectively.

This file gets edited when you choose to **Specify Server** and enter the server host name or when the **Public Key** is entered manually while installing Intel Unite software on the Hub or Client.

If you wish to edit the serverconfig.xml file after the installation, navigate to the folder where the file exists and make the necessary changes.




If a server is defined in the ServerConfig.xml, it will take precedence over the DNS Service Record.

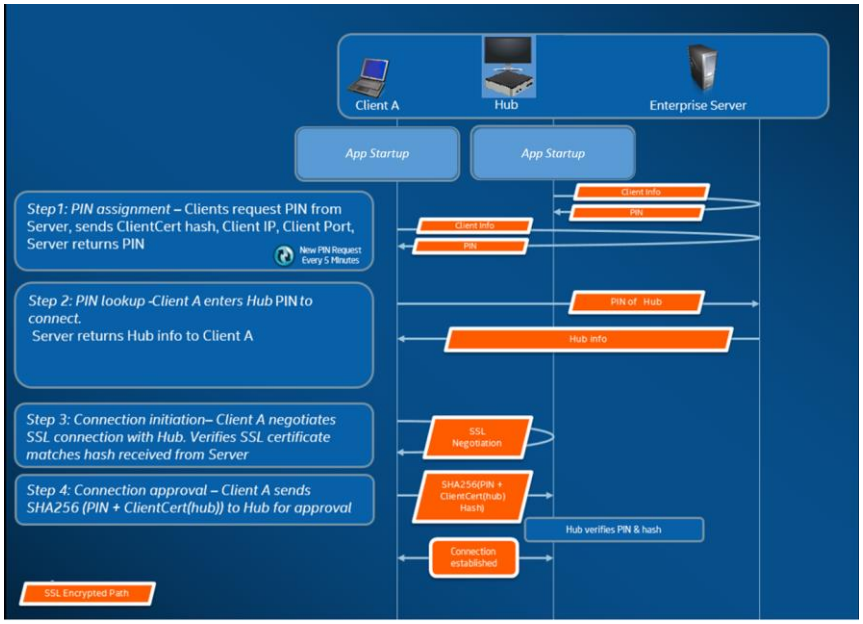
# Appendix C. Intel Unite Solution – Security Overview

## Intel Unite Software - Security Flow

This section briefly describes the security aspects of Intel Unite application. Security aspects of the connection are discussed for the following four steps:

1. PIN assignment
2. PIN lookup
3. Connection initiation
4. Connection approval

The following image contains a high level overview of how the Client (with Intel vPro technology) and Hub applications securely receive PINs from the Enterprise Server, resolve PINs, and establish a connection.



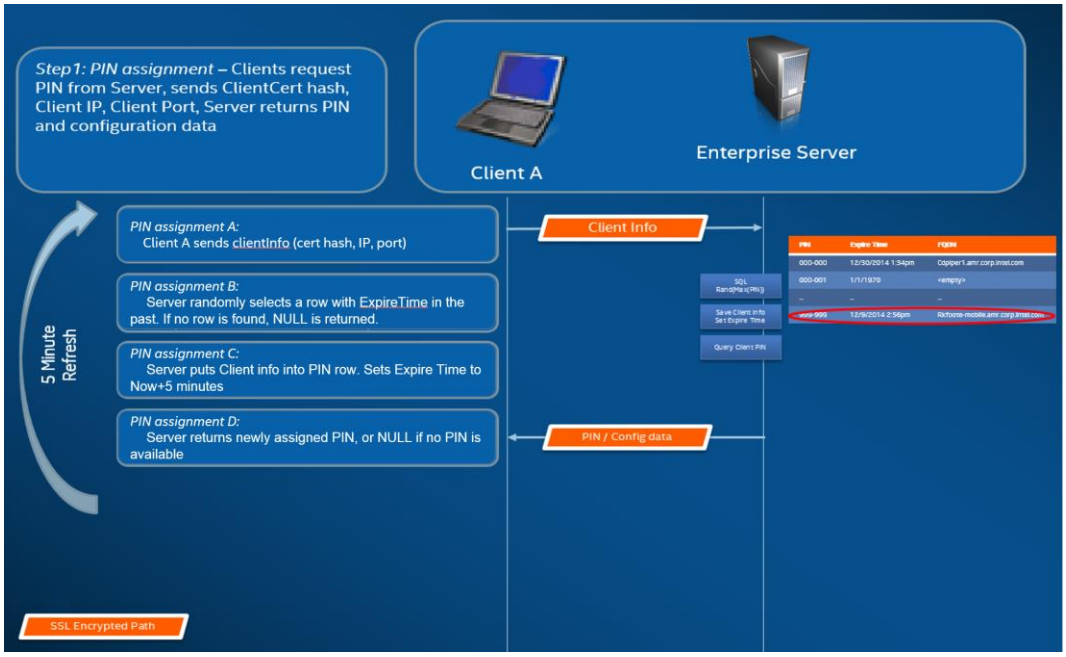
## Step 1: PIN Assignment

The image below shows how PINs are assigned. All network communication during this process is SSL encrypted over a web service (TCP 443).
In addition to receiving PINs, the Hub and Client also register their connection information and a public key to the server. The public key is used during connection to validate that each component is communicating with the intended target.

Note: PIN assignment for Client (with Intel vPro technology) and Hub follow the same flow.

Also note the following:

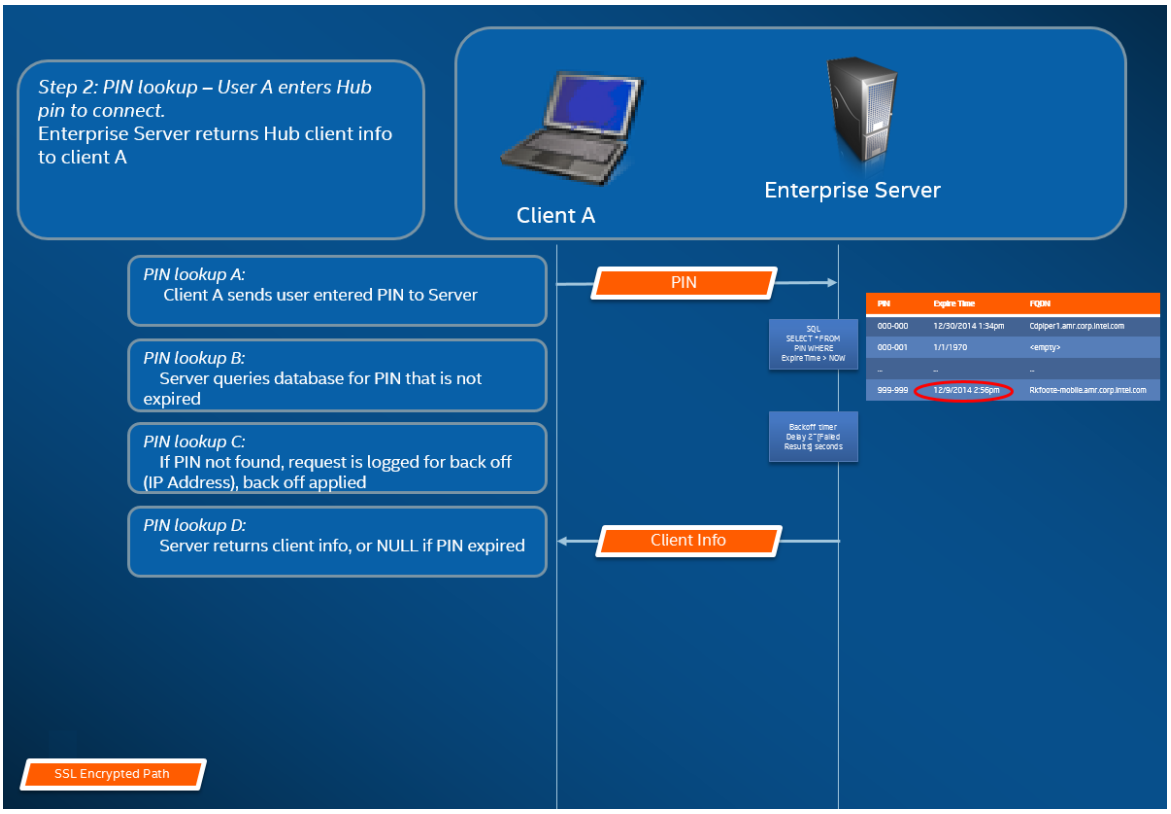
- The PIN refresh interval is configurable.
- When Hub or Client sends connection information, IP addresses in the local host (127.0.0.0/8) and 169.254.0.0/16 ranges are ignored.
- The TCP port can be configured per Client or Hub, or pushed via a profile from the Admin Portal. The default behavior is to let the operating system assign a port.
- Expired PINs will be allowed access for up to 15 seconds.
- Expired PINs will not be reassignment for up to 5 minutes after expiration to ensure that users don't accidentally connect to the wrong display.



## Step 2: PIN Lookup

The image below shows how PINs are resolved by the Enterprise Server. All network communication during the PIN lookup processes is SSL encrypted over a web service (TCP 443).
When a user enters a PIN of the target in the Client, the Client sends the PIN to the Enterprise Server to obtain the connection information. On a successful lookup, the Enterprise Server returns the valid connection information of the target. The target can either be a Hub or a Client (with Intel vPro technology) running the Intel Unite software.
In addition to receiving connection information, the public key of the target is also given, so that the Client application can validate that it is communicating with the correct target.

**NOTE:** Pin lookup for Hub and Clients follow the same flow.

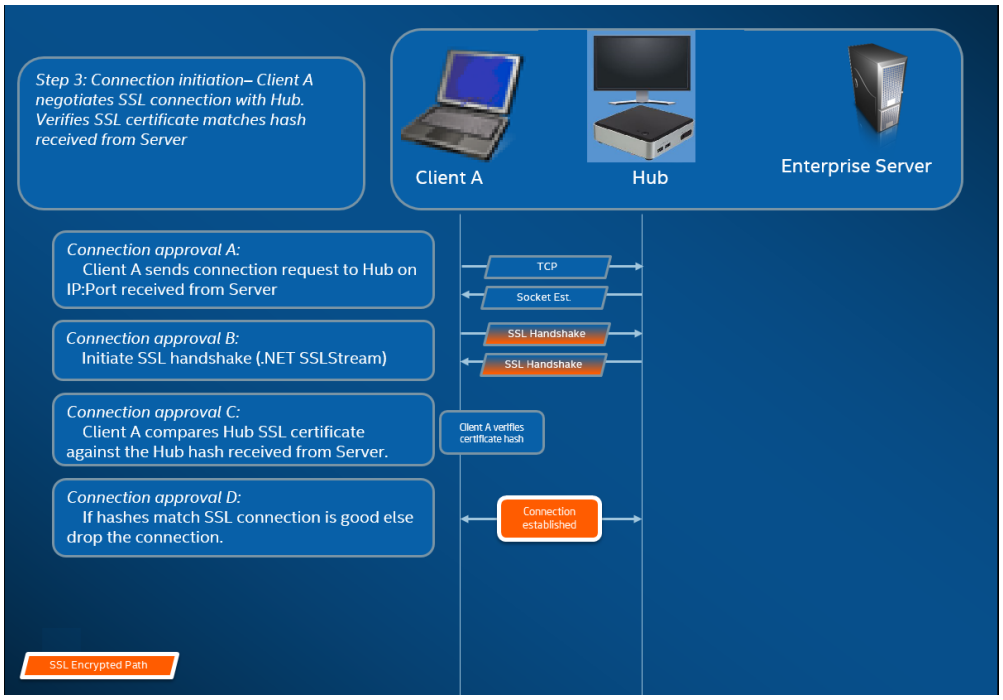



## PIN Lookup Back off

To prevent attackers from trying to harvest PINs from the Enterprise Server, failed attempts are logged. A user can have up to 3 failed attempts in a 10 second period before the back off mechanism begins enforcing a delay in responses (2^x seconds, where x=number of failed attempts within a 5 minute period).

## Step 3: Connection Initiation

The image below shows how a connection is initiated. The Client initiates a TCP peer-to-peer connection with the target (a Hub or a Client with Intel vPro technology running the Intel Unite software), and starts an SSL handshake. The certificate provided by the target is hashed and compared against the hash the Client received during step 2. This type of validation prevents attacks and also prevents situations where IP addresses of DHCP Clients may change.



## Step 4: Connection Approval

The image below shows how the connection is established between the client and the target, which could be a Hub or a Client (with Intel vPro technology) running the Intel Unite software. Once the target verifies the PIN and Client certificate, it accepts the connection and a connection is established between the client and the target.