Intel Unite® Solution

Version 4.0

Deployment Guide

Revision 1.5

October 2019

Legal Disclaimers and 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, Intel Unite, Intel Core, and Intel vPro are trademarks of Intel Corporation or its subsidiaries in the U.S. and/or other countries.

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

Table of Contents

Table of Tables

Table of Diagrams

Table of Figures

1 Introduction

The Intel Unite® solution powers secure connected meeting spaces that simplify collaboration. It is designed to quickly and easily connect everyone in a meeting. The Intel Unite solution is a simple and instant collaboration solution available today, and it serves as a foundation for additional capabilities and innovation in the future.

This document can be used to install the Intel Unite software, learn more about the application's features, and assist with troubleshooting.

This document is available in the following languages and can be downloaded from the support website for the Intel Unite solution: English, French, German, Spanish, Italian, Brazilian Portuguese, Korean, Japanese, Traditional Chinese, and Simplified Chinese.

1.1 Audience

This deployment guide focuses on enabling users to launch and become familiar with the Intel Unite application and its features. This guide is designed for IT professionals in an enterprise environment and any other people involved in deploying the Intel Unite solution.

1.2 Intel Unite® Solution Terminology and Definitions

Admin Portal—The web interface that manages hub and client configurations and provides configuration settings for the Intel Unite® solution.

Apps—A software component installed on a hub or client that extends the functionality of the Intel Unite solution.

Client—A device (Windows*, Mac OS*, iOS*, Android*, Chrome OS*, or Linux*) that connects to a hub.

Enterprise Server (Server)—The web server and the PIN service running on the server that assigns and resolves PINs. It provides a download page for the clients and the Admin Portal for configuration.

FQDN—Fully qualified domain name.

Hub—A mini form factor PC, All-In-One, compute stick, compute card, and devices conforming to the Open, Pluggable Specification with Intel® vPro™ technology that is connected to a display in a conference room running the Intel Unite application.

IIS—Internet Information Services*, which is a web server provided by Microsoft*.

2 Intel Unite® Solution Requirements

2.1 Enterprise Server Requirements

- Microsoft Windows Server* 2012 R2, 2016, or 2019
  - Recommended latest patch level
  - Microsoft* .NET Framework 4.8 or greater
- Microsoft Internet Information Services* (IIS) requirements:
  - IIS 7, 8, or 10
  - SSL enabled
    - At a minimum, SHA2-based web server certificate with an internal or public root of trust
  - Required IIS features:
    - ASP .NET 4.8
    - WCF services
    - HTTP activation enabled for .NET 4.8
  - Required IIS roles:
    - Common HTTP features
    - Default document
  - IIS extensions:
    - URL Rewrite* 2.1 (requires Microsoft Web Platform Installer*)
  - SMTP email server configured under Microsoft Internet Information Services
- SQL database (Microsoft SQL* or MySQL*): For full SQL support from the vendor, use the paid version of Microsoft SQL and MySQL. There is limited SQL support from the vendor and community when using the free versions (Microsoft SQL Express Edition and MySQL Community Edition).
  - Microsoft SQL Server 2012 SP4, 2014 SP2, 2016 SP1, or 2017 CU7
  - Database server running with mixed mode authentication (SQL Server and Windows Authentication mode)
  - MySQL 5.7
- 4 GB RAM
- 32 GB available storage

Note 1: The Intel Unite solution 3.x IIS components, the Intel Unite solution 4.0 IIS components, and the SQL database can coexist on the same server.

Note 2: For environments where the webservices and the database needs or is desired to be on separate servers, the IIS components and the SQL database can be installed on separate servers.

2.2 Hub Requirements

- A supported platform, as shown on the Intel Unite® solution overview web page
- Microsoft Windows* 7 latest or 10 RS4, RS3, RS2 (64 bit only)
  - Recommended latest patch level
  - Microsoft .NET 4.8 or greater
- 4 GB RAM

- Wired or wireless network connection
- 32 GB available storage

2.3 Client Requirements

- Microsoft Windows* 7 SP1, 8.1, or 10 (32 bit or 64 bit)
  - Recommended latest patch level
  - Microsoft .NET 4.8 or greater
- Mac OS* 10.12, 10.13, or 10.14
- iOS* 11 or 12
- Android* Version 6 (Marshmallow), Version 7 (Nougat), or Version 8 (Oreo)
- Chrome OS* Latest version
- Linux* Fedora* 27 or 28, Red Hat* Enterprise 7, Ubuntu* 16 LTS or 18 Non-LTS
- Wired or wireless network connection

2.4 IT Considerations and Network Requirements

Primary IT considerations and network requirements include the following:

- Hub and client installations should be managed using the IT department's established procedures.
- To ensure reliability, Intel strongly recommends that the hubs use wired network connections. This prevents wireless bandwidth saturation, especially in congested areas.
- The Intel Unite software must be allowed to accept incoming connections. This may require adding an exception to the firewall installed on the hub. Refer to firewall help guide for the Intel Unite® solution for more information. For other firewall vendors not in the help guide document, contact the firewall vendor for specific details on how to create application exceptions
- In production environments, Intel strongly recommends using fully qualified domain names (FQDNs) and setting up a DNS TXT record that points to the enterprise server. This provides the easiest method for hubs and clients to locate the enterprise server.
- As a security upgrade, the Intel Unite application accepts only SHA-2 or greater certificates due to the end of life of SHA-1. This may require upgrading the certificates on the web server. Work with the organization's IT security team to get SHA-2 certificates during setup.

2.5 Mobile Client Devices

Some organizations deploy mobile client devices as part of the Intel Unite solution. To connect to the Intel Unite solution, all client devices (including iOS* and Android* devices) must be connected to the corporate network or use an appropriately configured VPN. Mobile devices not connected to the corporate network—such as personal laptops, tablets, and phones—may not be able to connect to an Intel Unite app session if a corporate firewall does not allow the connections. When enabling mobile client devices, IT administrators should know the following:

- If Intel Unite app users are using personal mobile devices, require them to be on the company network to connect to Intel Unite, or create another way to allow the connections.
- Ensure the necessary tools and strategies are in place to manage devices and keep the network safe.
- Implement a *Mobile Device Management Policy* for personal and mobile devices used for work.

- Tailor security to provide the correct amount of protection in accordance with the sensitivity of the data to be protected. The amount of tailoring depends on the data the company considers critical and how far the company wants to drill down to apply protections.

3 Deployment Overview

The Intel Unite solution consists of four components—enterprise server, hub, clients, and SMTP mail server (or mail relay):

- The **enterprise server** is the first component that needs to be set up. When the hub and client applications are launched, they use the enterprise server to exchange connection information and receive connection information necessary to complete registration.
- The **hub** is an Intel® Core™ vPro™ processor-based mini PC that meets the hub requirements described in Section 2.2. The hub is typically connected to a display or a projector in a conference room. Consult the display's or projector's user manual for instruction on how to properly connect the display or projector to the hub.
- **Clients** are systems that connect to a hub for collaboration in a meeting.
- An **SMTP mail server** or mail relay is used to send users a link for client registration and to send alert messages to IT administrators.

3.1 Deployment Resources

The following resources are required to complete the installation:

- Administrative rights on the SQL database
- Administrative rights on the enterprise server
- Administrative rights on the hub
- Ability to send mail from the SMTP mail server

Requirements may also include the following:

- IT security administrator to issue the SHA-2 certificate
- IT security administrator for firewall policies
- IT administrator to create a DNS TXT record, which is used by hub and clients to locate the enterprise server (strongly recommended)
- Enterprise server configured with valid SMTP settings

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 consists of four components:

- **Microsoft* SQL or MySQL database**—Maintains all status information for the Intel Unite solution infrastructure.
- **IIS web service**—A standardized messaging service that communicates with the database, hubs, clients, and SMTP server.
- **Administration portal website**—Enables administrators to manage hubs and clients, generate statistics, and access monitoring and alerting features.
- **Client download landing webpage**—Contains the Intel Unite client software.

4.2 Enterprise Server Pre-Installation

The enterprise server pre-installation requirements include:

- Software requirements described Section 2.1.
- Additional security considerations (optional). Refer to Appendix D. Security Checklist.

4.2.1 SQL Server

A SQL database is required, and the Intel Unite® solution is designed to work with either Microsoft* SQL server or MySQL server. The SQL server can be on the same system as the Intel Unite solution server.

4.2.1.1 Microsoft* SQL Server Installation

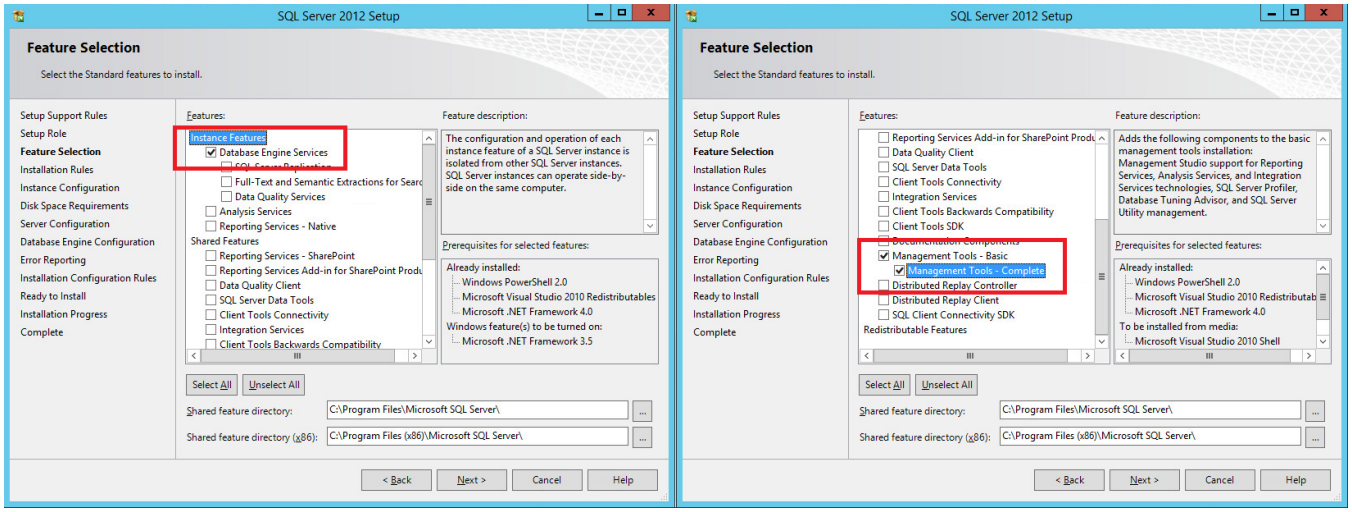
The enterprise server can be configured to work with MS SQL version 2012 or higher. Administrators can install a new, dedicated SQL server to run a test environment; however, it is not required. The Intel Unite application creates its own database, data tables, and indexes in an existing database without interfering with other tables or existing data.

The following steps describe how to install MS SQL2012:

1. Run the SQL server setup and open the SQL server installation center.
2. In the left pane, click **Installation**, and choose **New SQL Server stand-alone installation or add features to an existing installation**.
3. Enter the product key, accept the license terms, and click **Next**.
4. Select **Use Microsoft Update to check for updates (recommended)** to check for updates and click **Next**.
5. The setup looks for product updates and installs the necessary updates. To continue, click **Next**.
6. The setup checks for potential failures and requirements to be met before installation. To continue, click **Next**.
7. Select **SQL Server Feature Installation** and click **Next**.
8. Under the **Feature Selection**, select **Database Engine Services** and **Management Tools-Complete**, and

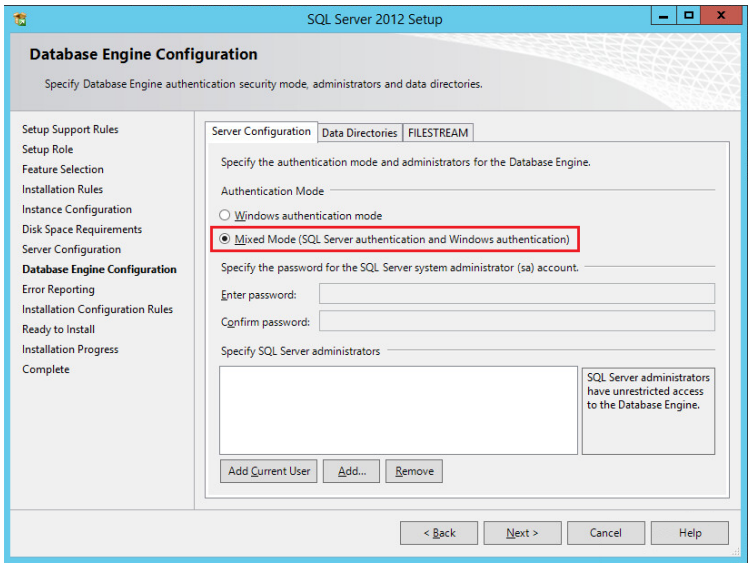
then click **Next**. (See Figure 1)

Figure 1. Microsoft SQL 2012 Feature Selection Screen



9. Specify the name and instance ID for the SQL server and click **Next**.
10. Specify the service accounts for each service, and click **Next**.
11. Select **Mixed Mode Authentication** (which includes SQL server and Windows* authentication), specify the SQL server administrators, and click **Next** on each screen until the verify features screen appears. (See Figure 2)

Figure 2. Mixed Mode Authentication Selection



12. Verify the features to be installed and click **Install**.
13. Close the dialog box after the installation completes.

4.2.1.2 MySQL Server Installation

The enterprise server can be configured to work with MySQL version 2008 R2 or higher. Administrators can install a new, dedicated MySQL server to run a test environment; however, it is not required. The Intel Unite application creates its own database, data tables, and indexes in an existing database without interfering with other tables or existing data. MySQL 5.7 have specific requirements:

- MySQL 5.7 requires Microsoft Visual C++ Redistributable Packages for Visual Studio 2013 (MySQL 5.7)

The following steps describe how to install MySQL 5.7:

1. Double-click the **.msi** file.
2. Click the **Run** button.
3. The User Account Control dialog box may display. If so, click **Yes** to continue.
4. On the License Agreement screen, place a check in the check box to accept the license terms, and click **Next**.
5. Select **Custom** and click **Next**.
6. On the next screen, expand **MySQL Server**, expand **MySQL Server *<version number>***, and then select **MySQL Server 5.7.22 – X64**, if installing on a 64-bit OS, or select **MySQL Server 5.7.22 – X86** , if installing on a 32-bit OS.
7. Click the green arrow to add the product to the **Products/Features To Be Installed** column and click **Next**.
8. Click **Execute** to install MySQL.
9. After installation, verify that a green check is next to **MySQL Server *<version number>***, which indicates a

successful installation, and then click **Next**.

10. Click **Next**, again.
11. For Group Replication, select **Standalone MySQL Server/Classic MySQL Replication**, and click **Next**.
12. Leave the **Type and Networking** default settings unchanged and click **Next**.
13. For **Accounts and Roles**, enter a password for the root account, and click **Next**.
14. Leave the **Windows* Service** default settings unchanged and click **Next**.
15. Leave the **Plugins and Extensions** default settings unchanged and click **Next**.
16. Leave the **Advanced Options** default settings unchanged and click **Next**.
17. For **Apply Configuration**, click **Execute**.
18. Click **Finish**, click **Next**, and then click **Finish**, again.

4.2.2 Verify .NET Framework 4.8 Installation

On the system targeted for the Intel Unite solution server installation, verify that .NET Framework 4.8 is installed. To verify your version, refer to How to: Determine which .NET versions are Installed. If the .NET Framework 4.8 is not installed, install .NET Framework 4.8 by referring to the Microsoft .NET Framework 4.8 website.

4.2.3 Enable IIS

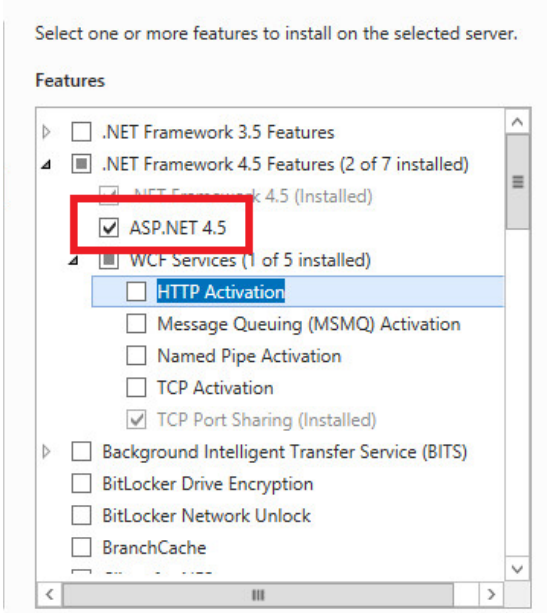
On the system targeted for the Intel Unite solution server installation, enable IIS. The following sections show the steps for enabling IIS on Windows Server* 2012, 2016, and 2019.

4.2.3.1 Windows Server* 2012

To enable IIS on Windows Server* 2012:

1. Open **Server Manager** and click **Manage > Add Roles and Features**.
2. In the Add Roles and Features Wizard, click **Next**.
3. On the Manage menu, select **Add Roles and Features**.
4. Select **Role-based or feature-based installation** and click **Next**.
5. Select the appropriate server (**local** is selected by default).
6. Select **Web Server (IIS)**.
7. In the Add features that are required for Web Server (IIS) dialog box, click **Add Features**.
8. Click **Next**.
9. On the Features page, add the following features for IIS:
    - .NET Framework 4.8 Features
        - ASP.NET 4.8 (refer to Figure 3)

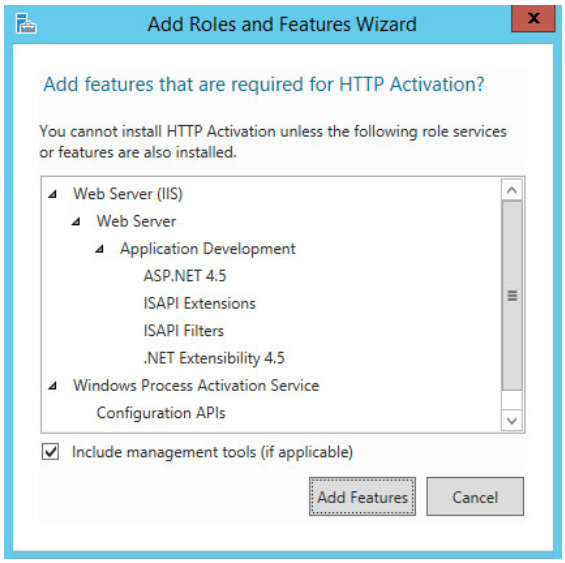
Figure 3. Server 2012 IIS Features to Install



Note: Some versions of Windows Server may not have .NET Framework version 4.8 available. To get hte latest version, go to the Microsoft .NET Framework 4.8 website.

- WCF Services
  - HTTP Activation (click **Add Features** in the **Add features that are required for HTTP Activation?** dialog box, refer to Figure 4)

Figure 4. Server 2012 IIS HTTP Activation Features to Install



10. Click **Next**.
11. On the Web Server Role (IIS) page, click **Next**.
12. On the Role Services page, click **Next**.
13. On the Confirm Installation Selections page, click **Install**.

4.2.3.2 Windows Server* 2016 and 2019

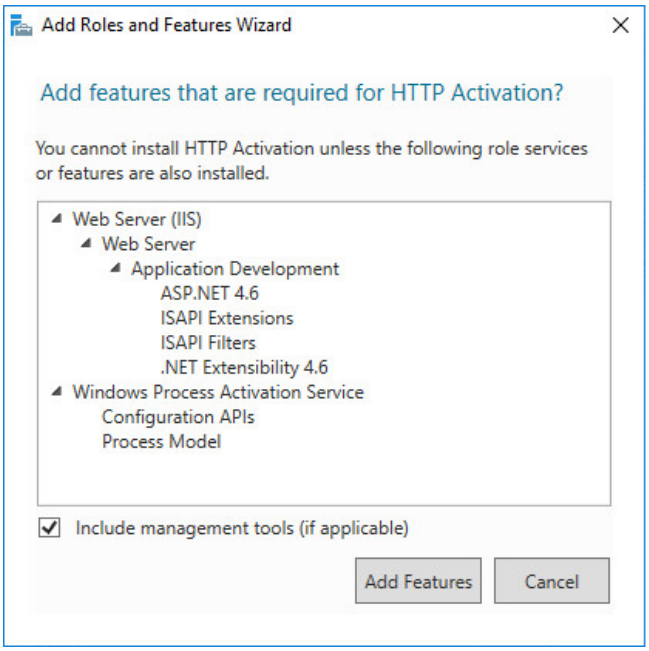
To enable IIS on Windows Server* 2016 and 2019

1. Open **Server Manager**.
2. On the Manage menu, select **Add Roles and Features**, and click **Next**.
3. In Installation Type, select **Role-based or feature-based Installation**, and click **Next**.
4. Select the appropriate server (**local** is selected by default) and click **Next**.
5. Select **Web Server (IIS)** and **Add Features that are required for Web Server (IIS)**, and click **Next**.
6. Add the following features for IIS:
   - .NET Framework 4.8 Features
     - ASP.NET 4.8
   - Windows Process Activation Service
     - Configurations APIs
     - Process Model
7. Click **Add Features** to continue, and add the following features:
   - .Net Framework 4.8 Features (2 of 7 installed)
     - .NET Framework 4.8
     - ASP.NET 4.8
       - WCF Services (1 of 5 installed)
         - HTTP Activation*
         - TCP Port Sharing (installed)

***Note:** Placing a check in the **HTTP Activation** check box opens a dialog box with the following features selected (See Figure 5):

- Web Server (IIS)
  - Web Server
    - Application Development
      - ASP.NET 4.8
      - ISAPI Filters
      - ISAPI Extensions
      - .NET Extensibility 4.8

Figure 5. Server 2016 IIS HTTP Activation Features



8. Click **Add Features** to continue.
9. Accept the default features on the Select Role Services page and click **Next**.
10. Read the information provided on the Web Server Role (IIS) page and click **Next**.
11. Click **Next** to continue.
12. Finally, on the Confirm Installation Selections page, review the items to be installed, and click **Install**.

4.2.4 Install URL Rewrite

On the system targeted for the Intel Unite solution server installation, install URL Rewrite. Two methods are available for installing URL Rewrite, as described in the next two sections.

4.2.4.1 URL Rewrite Installation – Method 1

1. Download and install the Web Platform Installer from this link.
2. Launch the **Web Platform Installer**.
3. Click the **Products** tab.
4. Search for **URL Rewrite**.
5. Select **URL Rewrite 2.1** from the list and click **Add**.
6. Click **Install**.
7. Review the license and accept it to begin the installation.
8. Click **Exit** to close the Web Platform Installer.

4.2.4.2 URL Rewrite Installation – Method 2

1. Download the URL Rewrite installer directly from this link.

2. Run the installer and follow the wizard.

4.3 Enterprise Server Installation

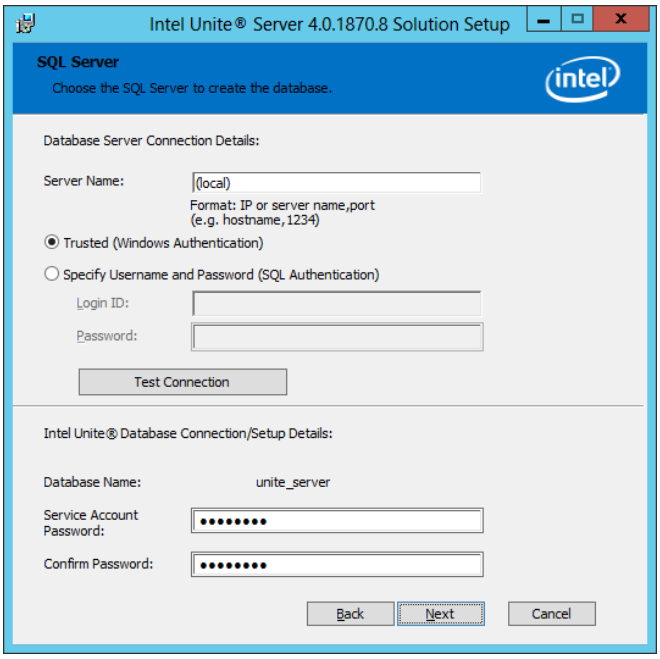
After completing all enterprise server pre-installation steps, the Intel Unite solution server software can be installed. This process must be run on the server that hosts the IIS environment.

4.3.1 Install the Enterprise Server Using the MSI

The following steps describe how to use the .msi file to install an enterprise server:

1. Locate the **Intel_Unite_Server_vx.x.x.x.mui.msi** file (either copied to local storage or on network storage).
2. After launching **Intel_Unite_Server_vx.x.x.x.mui.mui.msi**, check the **I accept the terms of the License Agreement** box.
3. Click **Next** to continue.
4. Choose the type of database—if using Microsoft SQL Server, select **Choose SQL**; if using MySQL, select **Choose MySQL**.
5. Click **Next** to continue.
6. In the Server Instance window, set the SQL database options. The available options are:

Figure 6. Server Installer Database Configuration Screen



- Database Server Connection Details section:
  - The **Server Name** default value is **(local)** for the SQL server. Replace the default with a hostname or leave the default value. If using MS SQL and MS SQL is installed on the same server, leave the **Server Name** as **(local)**. If using MySQL and MySQL is on the same server, the **Hostname** should be **localhost** instead of **(local)**
  - If MS SQL is selected, the default value for database server authentication is **Windows Authentication**. If SQL authentication is preferred, select **SQL Authentication**, and fill in the **Login ID** and **Password** of an MS SQL account that has create database and read/write access.

- If MySQL is selected, enter the account name in the **Login ID** text box and the account password in the **Password** text box. The account should have **create database** and **read/write** access.
- Click the **Test Connection** button to verify the account information.

- Database Server Connection/Setup Details section:
  - Create a password and enter the password into the **Service Account Password** text box. The password is for the **api_user**, which is used to access the database named *unite_server*.
  - Retype the password into the **Confirm Password** text box.

    Note: The password must contain at least eight characters, one uppercase character, one lowercase character, one digit, and one symbol.

7. Click **Next** to configure the installation path. The default path for the installation is **C:\Program Files (x86)\Intel\Intel Unite**. If a different location is preferred, enter the new location in the text box or click the **Change** button to use the Change Destination Folder dialog box to select the location. If using the Change Destination Folder dialog box, browse to the location, and click **OK**.
8. Click **Next**.
9. If you are using a load balancer, proceed to Appendix G. Load Balancing Configuration Options to complete the configuration. If you are not using a load balancer, click **Next** to accept the default settings.
10. Enter an organization name in the **Organization Name** text box, and enter a description in the **Organization Description** text box. The organization name is used to create a hub group and client group.
11. Select either **Enhanced Pairing Mode** or **Standard Pairing Mode**.
    - Enhanced Pairing Mode—This mode requires e-mail confirmation when registering a client device.
    - Standard Pairing Mode—This mode does not require e-mail confirmation when registering a client device.

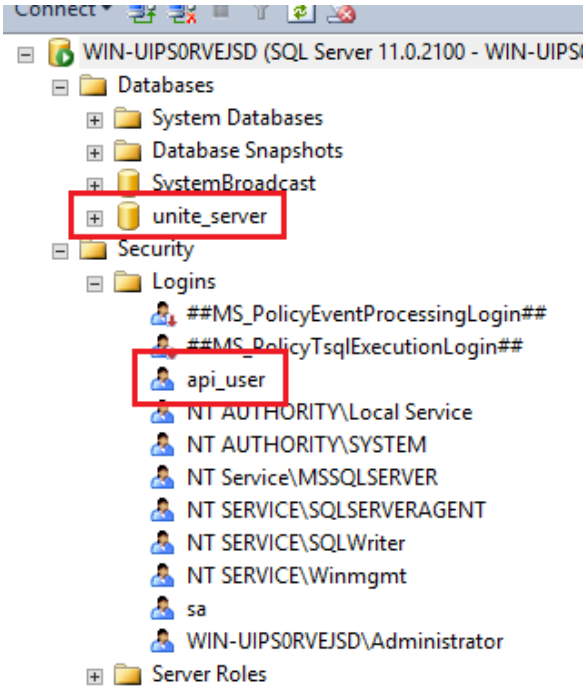
    Note: Pairing mode cannot be changed once it is set. It requires a re-installation of the server to change the pairing mode.
12. Click **Next**.
13. Click **Install** to start the installation. When the installation process completes, the enterprise server is installed.

4.3.2 Verify the Successful Creation of the database for the Intel Unite® solution (Optional)

To verify the successful creation of the database for the Intel Unite solution on MS SQL or MySQL, use one of the following procedures:

For MS SQL, open SQL Management Studio, and connect to the SQL server. Expand **Databases** on the left side pane and ensure the **unite_server** is listed. Confirm **api_user** exists under **Security->Logins**. See Figure 7.

Figure 7. Objects Created in Microsoft SQL



- For MySQL, open a command-line window on the MySQL server. Start the MySQL interpreter by typing **mysql -h *<host-name>* -u=*<your-user-name>* -p** at the command prompt, where ***<host-name>*** is **localhost**, since the command is running from the computer with My SQL, and ***<your-user-name>*** is the user name used during server installation. Enter the password for the user. Type **show databases;** and ensure the **unite_server** database is listed.

4.3.3 Install the Enterprise Server Using a Command Line

The Intel Unite application installer for the enterprise server supports command-line installations. The installer msi file must be in a known location, either on the local system or a network share. The command and parameters for installation are shown and must be executed as administrator:

msiexec /i "Installer_Path.msi" /l*v "Log_Path" /q INSTALLFOLDER="*Value*" DBTYPE="[1|0]" DBHOSTNAME=*Value* DBLOGONTYPE="[WinAccount|SqlAccount]" DBUSER=*Value* DBPASSWORD=*Value* DBLOGONPASSWORD=*Value* DBLOGONPASSWORDCONF=*Value* ORGNAMEPROPERTY=*Value* ORGDESCPROPERTY="*Value*" PUBLISH_WEBAPI_HELP=*Value* PAIRMODEPROPERTY="[0|1]" ADDLOCAL="*Value*"

4.3.3.1 Enterprise Server Command-Line Installation Parameters

The enterprise server installation parameters are case-sensitive. The result of the installation can be determined by parsing the log file. Double quotes are only required for input values that include one or more spaces. When in doubt, use double quotes to surround input values.

In the following list, names in caps are the supported properties. They can be combined depending on the setup. The values inside brackets are predefined options (choose one, and do not include brackets or the pipe character).

- **/i**—The switch for installation.

- **"Installer_Path.msi"**—The path including the filename of the msi file (for example, **"c:\my downloads\installer.msi"**).
- **/l*v**—The switch for generating a log file.
- **"Log_Path"**—The path including the log file name (for example, **"c:\my logs\serverinstallog.txt"**).
- **/q**—The switch for silent, no user interaction.
- **INSTALLFOLDER=*Value***—The location specifying where to install the server application. Replace ***Value*** with the full path, including the double quotes (for example, **"c:\my apps\unite server"**).
- **DBTYPE=[0|1]**—The switch for indicating which database is being used. A value of **0** means MySQL, and a value of **1** means MS SQL.
- **DBHOSTNAME=*Value***—The host name of the SQL server. Replace ***Value*** with the FQDN of the SQL server.
- **DBLOGONTYPE="[WinAccount|SqlAccount]"**—The switch indicating which type of login is used to access the SQL server. A value of **"WinAccount"** means using a Windows* account, and a value of **"SqlAccount"** means using a SQL server account. This parameter is only needed if **DBTYPE=1**.
- **DBUSER=*Value***—The user name of the account used to log in to the SQL database to create the database tables and create the service account. Replace ***Value*** with the database user name.
- **DBPASSWORD=*Value***—The password of the database account used to log in to the SQL database to create the database tables and create the service account. Replace ***Value*** with the password.
- **DBLOGONPASSWORD=*Value***—The password for the service account. Replace ***Value*** with the password.
- **DBLOGONPASSWORDCONF= *Value***—The confirmation of the password for the service account. Replace ***Value*** with the password. This must be the same as **DBLOGONPASSWORD**.
- **ORGNAMEPROPERTY=*Value***—The organization name, which is used to create a hub group and a client group. Replace ***Value*** with the organization name.
- **ORGDESCPROPERTY= "*Value*"**—A detailed description for the organization. Replace ***Value*** with the description in double quotes.
- **PUBLISH_WEBAPI_HELP=[0|1]**—The switch to install the help webapi. A **Value** of **1** means to install the help webapi, and a **Value** of **0** means to not install the help webapi.
- **PAIRMODEPROPERTY=[0|1]**—The switch to set the pairing mode. A **Value** of **1** means Standard Pairing Mode, and a **Value** of **0** means Enhanced Pairing Mode.
- **ADDLOCAL="*Value*"**—The list of server component features to install on this server. Replace ***Value*** with a server component feature or a list of server component features separated with commas. Following is a list of server component features:
    - DatabaseFeature — Install the database on this server.
    - WebApiFeature — Install the WebAPI on this server.
    - AdminPortalFeature — Install the Admin Portal on this server.
    - TelemetryFeature — Install the Telemetry service on this server.
    - MaintenanceFeature — Install the Maintenance service on this server.
    - ALL — Install all the above features on this server.

4.4 Configure IIS for the Admin Portal Website (Quick Start)

This section describes the basic configuration needed for the Admin Portal to be set up to pair with hubs and client registrations, which enables clients to connect to the hubs. Refer to Section 7 for a complete set of Admin Portal configuration options.

4.4.1 Obtaining a Certificate

Intel Unite® solution can be configured to work with SHA-2 certificates from public root of trust certificate authorities or self-signed certificates.

4.4.1.1 Option 1: Obtain a Certificate from a public root of trust certificate authority

Using a public root of trust or external certificates authority allows Intel Unite® clients and hubs to establish a reliable, secure connection to the enterprise server. Major operating systems inherently trust these certificate authorities as part of normal operating system process. This link defines the process for creating a certificate signing request and submitting the request to a certificate authority.

Below are a couple of examples of certificate authorities that can provide SHA-2 certificates:

www.godaddy.com

www.verisign.com

4.4.1.2 Option 2: Create a self-signed Web Server Certificate

For test environment, a self-signed certificate can work well. However, attempting to use self-signed certificates in a production environment can limit connectivity of some platforms. Not all platforms are capable of trusting self-signed certificates, such as iOS and Chrome OS.

With the end of life of SHA-1 certificates, the latest version of the Intel Unite solution only accepts SHA-2 certificates or greater. The organization's IT department should ensure the trusted web server certificate issued is a SHA-2 certificate and the certification path is valid.

For a test environment, a self-signed SHA 2 certificate can be created, as follows:

1. Run PowerShell as administrator.

2. Run the following command:

   New-SelfSignedCertificate -DnsName <*Computer Name*> -CertStoreLocation "cert:\ LocalMachine\My"

   Replace ***<Computer Name>*** with the FQDN used to access the enterprise server. For example, **mytestserver.mycompany.com**.

3. To run MMC as an administrator, click the **Search** icon on the Windows* task bar, type **Run**, press **Enter** or **Return**, and type **mmc**.
4. In the Console window, click **File**, and select **Add or Remove Snap-ins**.
5. Select **Certificates** and click **Add**.
6. Select **Computer Account**.
7. Select **Local Computer**.
8. Click **Finish**, and then click **OK**.
9. In the left pane, click **Expand Certificate (Local Computer)**, select **Personal**, and select **Certificates**.
10. In the middle pane, right-click the certificate created previously, and enter a **Friendly Name** (this name is used in a later step).
11. Right-click the certificate again and click **Copy**.
12. In the left pane, click **Trusted Root Certification Authorities**.
13. In the center pane, right-click anywhere, and click **Paste**.
14. To close the mmc, click **File**, and click **Exit**. On exit, a prompt to save may be displayed. Saving the settings enables loading the settings later, including the certificate snap-in. If the settings are not saved, the certificate snap-in will have to be added again.

4.4.2 Install the Web Server Certificate and Configure Web Server Bindings

This section describes how to open the Internet Information Services (IIS) Manager, expand the server name, and remove a port binding.

4.4.2.1 Open IIS Manager

The following steps describe how to open the IIS Manager;

1. On the Start menu, click **All Programs**, click **Accessories**, and then click **Run**.
2. In the Run text box, type **control panel**, and then click **OK**.
3. In the Control Panel window, click **Classic View**, and then double-click **Administrative Tools**.
4. In the Administrative Tools window, double-click **Internet Information Services (IIS)**.

4.4.2.2 Expand the Server Name

To expand the server name:

1. In the left Connections pane, expand **Sites**, and click **Default Web Site**.
2. In the right Actions pane, find **Edit Site**, and select **Bindings**.
3. In the Site Bindings window, click **Add**.
4. Configure the following settings:
   - **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)

5. Click **OK**.
6. Click **Close**.

Note that the web service for the Intel Unite application communicates with the clients and hubs using port 443.

4.4.2.3 Remove Port 80 Binding

The following steps describe how to remove the port 80 binding:

1. In the left navigation pane, find Sites, and then select **Default Web Site**.
2. In the right Actions pane, find Edit Site, and then select **Bindings**.
3. Select the item with **Port** equal to **80**.
4. Click the **Remove** button and click **Close**.

4.4.3 Enable Anonymous Authentication

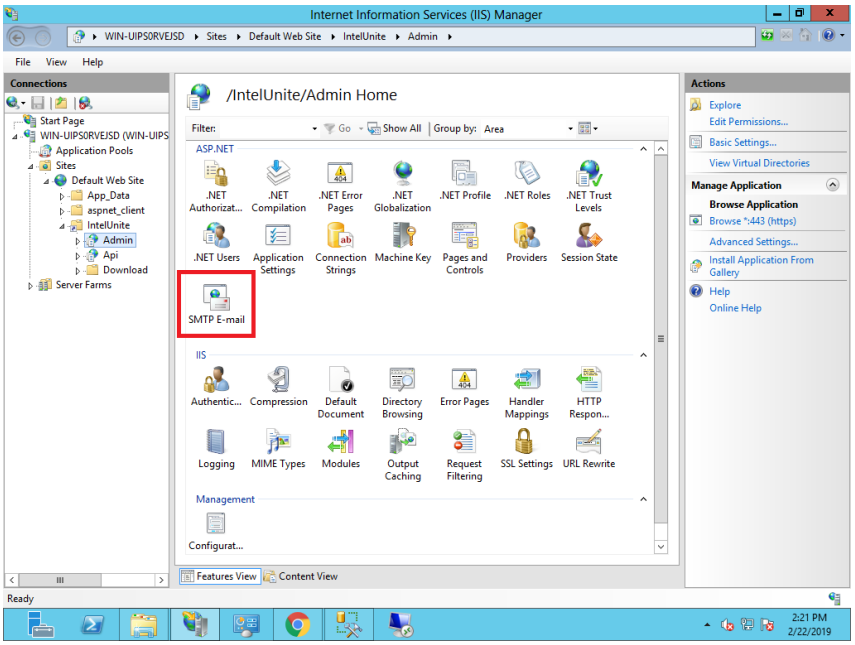
Anonymous Authentication **MUST** be enabled for the Intel Unite solution to work properly. The following steps describe how to enable Anonymous Authentication:

1. In the left navigation pane, find Sites, and then select **Default Web Site**.
2. In the middle pane, double click **Authentication**.
3. Select **Anonymous Authentication**.
4. In the Actions pane, select **Edit**.
5. Select **Specific user.**
6. Click **Set**.
7. Enter **IUSR** for the User name and leave the Password Confirm password fields blank.
8. Click **OK**.

4.4.4 Configure IIS SMTP Email Settings

To configure IIS SMTP email settings:

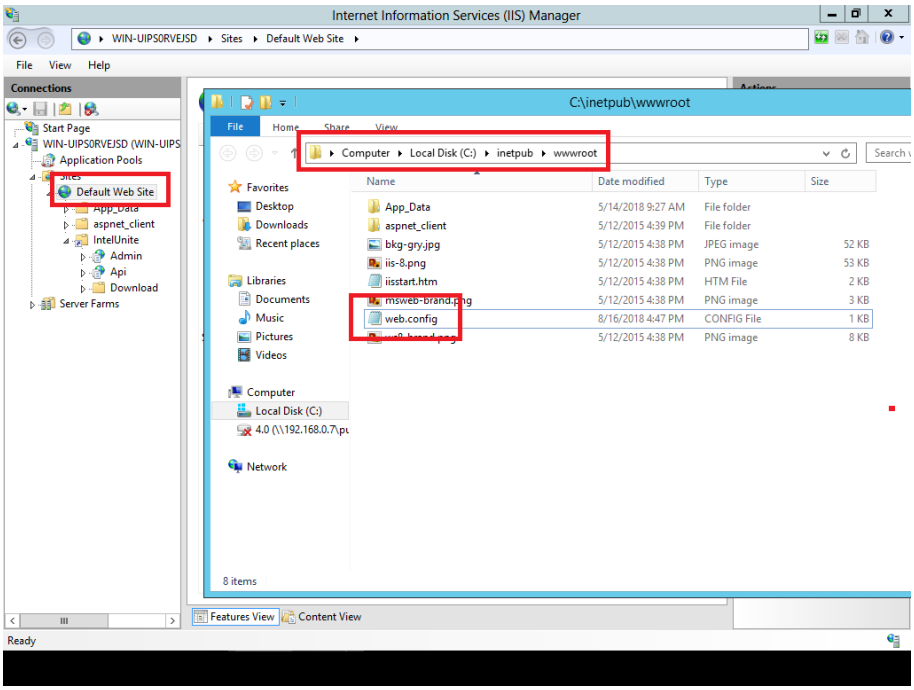
Figure 8. IIS Default Web Site SMTP Email Icon



1. In the left navigation pane, find **Sites**, and select **Default Web Site**.
2. Double-click the **SMTP Email** icon. Refer to Figure 8.
3. On the SMTP Email page, type the sender's email address in the **Email address** text box.
4. Select **Deliver email to SMTP server**. (This delivers email messages immediately. This requires an operational SMTP server for which the user has credentials.)
5. In the SMTP Server text box, type the SMTP server's unique FQDN, or select the **Use localhost** check box to set the name to **LocalHost**. Setting the name to LocalHost means ASP.NET uses an SMTP server on the local computer. Typically, this is the default SMTP virtual server.
6. In the Port text box, enter a TCP port. Port 25 is the SMTP standard TCP port and is the default setting. More than one virtual server can use the same TCP port if all servers use different IP addresses.
7. Under Authentication Settings, specify the authentication mode and credentials, if your SMTP server requires these.
8. If the SMTP server is set up for email relaying, find **Authentication Settings**, and choose **Not required**.
9. Click **Apply** in the Actions pane.

Note: For third-party SMTP servers that have SSL enabled, add **enableSsl="true"** between the SMTP tags to the web.config file, refer to Figure 9 for web.config location.

Figure 9. IIS Web.config Location



Example: Web.config - SMTP with SSL Enabled

```
<system.net>

   <mailSettings>

      <smtp from="water@test.com">

          <network host="mail.test.com" port="25" userName="tester@test.com"
          password="xxxxx" defaultCredentials="false" enableSsl="true"/>

      </smtp>

   </mailSettings>

</system.net>
```

4.4.5 Configure IIS with Active Directory for the Admin Portal (Optional)

An Intel Unite solution server running the Admin Portal can use Active Directory to manage hub settings and user permissions. To do so, the following configurations are needed:

- Enterprise server and hubs must be joined to the Active Directory domain.
- The enterprise server's IIS settings must be configured with an identity that has "read" access to Active Directory groups containing the hub and/or user objects. By default, IIS uses the server's machine identity to access Active Directory. The identity used to access Active Directory can be changed, if desired.
- Active Directory groups must exist (or be created) that contain the hub and/or user objects to be used with the Intel Unite solution. In addition, read permissions must be granted on the groups to the enterprise server's identity so it can access them. Creating and maintaining the Active Directory groups is beyond the scope of this document. Consult the organization's IT department for help, if needed.

Note: The Active Directory identity used by the enterprise server to access Active Directory should be limited to "read only" for additional security.

4.4.5.1 Configure IIS for Active Directory Access

Once read permissions are granted for the enterprise server to the Active Directory hub and user groups, the enterprise server's IIS needs to be configured with the desired identity.

1. Open Internet Information Services (IIS) manager on the enterprise server.
2. In the left navigation pane, expand the server name, and then expand **Sites**.
3. Select **Default Web Sites**.
4. In the middle pane, double-click **Application Settings**.
5. In the right Actions pane, click **Add**.
6. Add the following Application Settings:
   - **ActiveDirectoryServer**
     - **Name:** ActiveDirectoryServer
     - **Value:** Enter the domain controller's FQDN. If there are multiple domains, enter each domain controller separated by a pipe. The port number can be appended to the FQDN (for example, **DC1.abc.corp.mycompany.com|DC1.xyz.corp.mycompany.com:1234**).
7. Click **OK**.
8. Repeat Steps 6 and 7 for each of the following entries:
   - **ActiveDirectoryGlobalCatalog**
     - **Name:** ActiveDirectoryGlobalCatalog
     - **Value:** Enter the forest (for example, **corp.mycompany.com**).
   - **ActiveDirectoryServerUseSSL**
     - **Name:** ActiveDirectoryServerUseSSL
     - **Value:** Enter **True** if SSL is used. Enter **False** if SSL is not used. By default, this value is False.
   - **ActiveDirectoryGroupsCacheLifeSpan**
     - **Name:** ActiveDirectoryGroupsCacheLifeSpan
     - **Value:** Enter the number of hours between group cache refresh. By default, this value is 24 hours.
   - **ActiveDirectoryServerUsername**
     - **Name:** ActiveDirectoryServerUsername
     - **Value:** Enter a valid user name with read permission to the Active Directory hub and user group(s).
   - **ActiveDirectoryServerPassword**
     - **Name:** ActiveDirectoryServerPassword
     - **Value:** Enter the password for the account.

If the AD machine account that hosts the Admin Portal has read access to the Active Directory groups, the **ActiveDirectoryServerUsername** and **ActiveDirectoryServerPassword** values are not needed.

Reference: Microsoft Windows server* library article for installing IIS on Windows Server* 2012

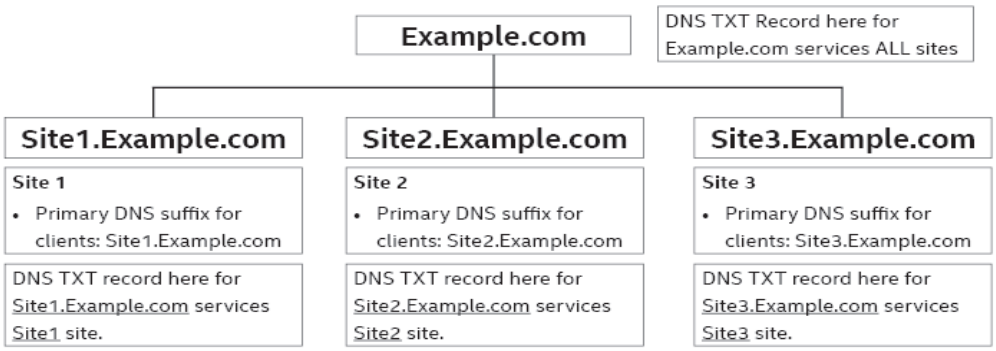
4.5 DNS TXT Record

The DNS TXT record is a resource record used to provide information needed for the Intel Unite solution. The specific information provided by the DNS TXT record is the URL of the server hosting the Web API component of the Intel Unite software and the organization ID.

4.5.1 DNS Hierarchy and Proper Placement of DNS TXT Record

The DNS TXT record facilitates the auto-discovery of the Intel Unite solution's PIN service. The DNS TXT record placement must match the primary DNS suffix or parent zone suffix of the hubs and clients. A PIN service can reside in any site if network traffic is permitted between sites. The following diagram and examples show the proper placement of the DNS TXT record.

Diagram 1. DNS TXT Record Placement Example



Examples based on the diagram:

Option 1: The DNS TXT record is created in example.com, and the PIN service resides in Site1. Clients from any site can auto-discover the service.

Option 2: Three DNS TXT records are created in Sites 1, 2, and 3 in example.com, and the PIN service resides in Site1. Clients from any site can auto-discover the service.

4.5.2 Create a DNS TXT Record

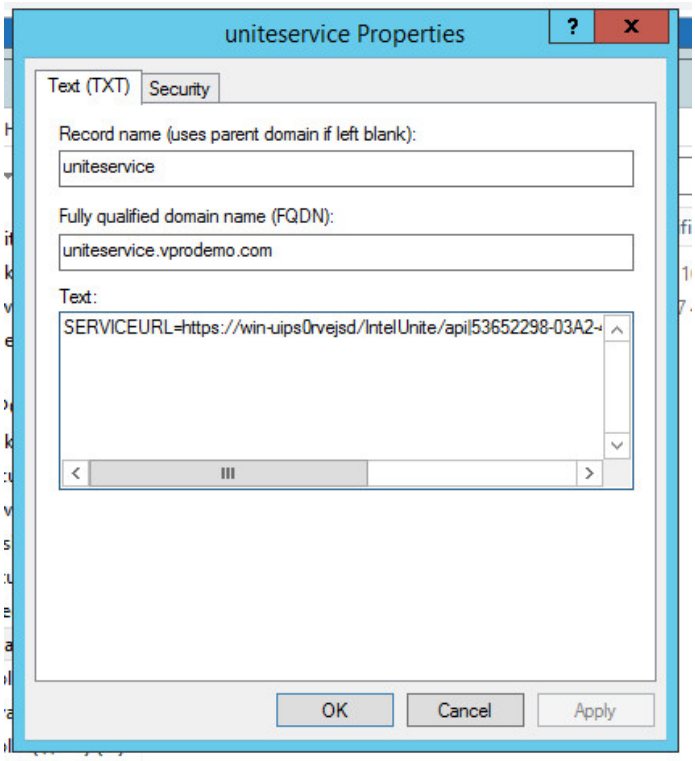
The hub and clients can locate the enterprise server by using a DNS TXT record during an automatic lookup for the enterprise server. The string in the DNS TXT record is not case-sensitive. To add a DNS TXT record in Microsoft* Windows*, complete the following steps:

1. On your DNS server, open **DNS Manager**.
2. In the left pane, expand **Forward Lookup Zones**.
3. Right-click the zone that contains the systems used for the Intel Unite solution. For a DNS setup that contains multiple forward lookup zones, select the zone that matches the primary DNS suffix for devices

that will be used with the Intel Unite solution.

4. Select **Other New Records**.
5. In the Select a Resource Record Type area, select **Text (TXT)**.
6. Click **Create Record**.
7. For **Record Name**, enter ***uniteservice***. The FQDN is filled in automatically.
8. For the Text option, enter **`SERVICEURL=https://<FQDN of the Admin Portal Server>/intelunite/api|ORGID=<OrgID>|OrgName=<OrgName>`**, where **`<OrgID>`** is the GUID for the organization and **`<OrgName>`** is the name of the organization. The OrgID is randomly generated, and the OrgName is set during installation of the Intel Unite® solution. Both values can be found by browsing to **https://*<yourserverfqdn>*/intelunite/admin/landing**. See Figure 10.

   Figure 10. DNS TXT Record Properties



9. Click **OK** to create the record.
10. Click **Done** to close the Resource Record Type window.

4.5.3 Disable Use of the DNS TXT Record

The use of the DNS TXT Record for auto discovery can be disabled by adding the registry key **DisableAutoDiscovery** of the type DWORD to the following registry paths. A DWORD value of 1 means do not use DNS TXT Record for auto discovery. A DWORD value of 0 means, use the DNS TXT Record for auto discovery. Any other value will result in default behavior of using the DNS TXT Record for auto discovery. If the key is not present, the device will use the DNS TXT Record for auto discovery.

32bit Windows

Hub

HKLM\SOFTWARE\Intel\Intel Unite\Hub

Client

HKLM\SOFTWARE\Intel\Intel Unite\Client

64bit Windows

Hub

HKLM\SOFTWARE\{WOW6432Node}\Intel\Intel Unite\Hub

Client

HKLM\SOFTWARE\{WOW6432Node}\Intel\Intel Unite\Client

Once DNS TXT Record is disabled for auto discovery, the use of the Intel Unite solution landing page is needed to provide the information provided by the DNS TXT Record. To access the landing page, browse to the following URL: **https://*<Intel Unite solution portal FQDN>*/intelunite/admin/landing**. On the landing page, click the link which will set the registry keys with needed values and open the Intel Unite application on the device.

4.6 Configure the Enterprise Server for Intel Unite® Solution

This section describes how to use the Admin Portal to configure the enterprise server for the Intel Unite solution.

4.6.1 Log in to the Admin Portal

The following steps describe how to connect to the Admin Portal.

1. Open a web browser. Internet Explorer* may not work. If that occurs, Intel recommends using Chrome*.
2. Go to **https://*<yourserverfdqn>*/intelunite/admin**.
3. In the User Name text box, enter **admin**.
4. In the Password text box, enter **Admin@1**.

The first time the built-in admin account is used to log in to the Admin Portal, the Admin Portal prompts for a change of the **admin** password. Set a new password, and use the new password to log in to the Admin Portal. Click the *i* in a gray circle next to **password rule** to see more information about the password requirements.

4.6.2 Set Privacy Policy

After logging into the Admin Portal for the first time, a dialogue displays the available privacy policies. Select one of these options to continue.

Available privacy policies include:

- **Collect locally and share anonymous data with Intel** — Telemetry data is collected and forwarded to Intel.
- **Collect locally and DO NOT share anonymous data with Intel** — Telemetry data is collected and stored on the Admin Portal, but not forwarded to Intel.
- **Do not collect** — No telemetry data is collected.

- **Prompt user to potentially share anonymous data with Intel** — Asks the user to opt-in or opt-out of telemetry data collection and the forwarding of the telemetry data to Intel.

4.6.3 Upload the Hub and Client Package Files to the Admin Portal

Packages contain the core configuration and feature/apps modules use to configure and extend the capabilities of the hubs and clients. If packages are not uploaded to the server, the hubs and clients will not be configured, and they will not be functional.

Core client and hub packages, along with the file transfer package, are included in the Intel Unite® solution installer ZIP file. The following packages are included in the installer ZIP file:

- **Unite_Client_vXXX.cab**—The core module needed by the client devices.
- **Unite_ClientRemoteView_vXXX.cab**—The module that allows clients to view remotely.
- **Unite_ClientScreenSharing_vXXX.cab**—The module that allows clients to share.
- **Unite_Hub_vXXX.enabled.cab**—The core module needed by the hub devices.
- **Unite_HubRemoteView_vXXX.cab**—The module that allows hubs to view remotely.
- **Unite_HubScreenSharing_vXXX.cab**—The module that allows hubs to share.
- **Unite_FileTransfer_vXXX.cab**—The module that allows file transfers between clients.

To obtain other app packages, visit the Intel Unite® App Showcase website. Refer to the Intel Unite® Solution 4.0 SDK documentation for package creation.

To upload packages.

1. Log in to the Admin Portal.
2. Open the **Device Management** menu and click **Upload Package**.
3. Browse to the installation files for Intel Unite solution and open the **Manifests** directory.
4. Select **Unite_Client_vXXX.cab** and click **Open**. A Success message should appear temporarily to indicate a successful upload.
5. Click **Upload Package** again.
6. Browse to the Installation files for Intel Unite solution, and open the **Manifests** directory.
7. Select **Unite_ClientRemoteView_vXXX.cab** and click **Open**. A Success message should appear temporarily to indicate a successful upload.
8. Click **Upload Package** again.
9. Browse to the Installation files for Intel Unite solution and open the **Manifests** directory.
10. Select **Unite_ClientScreenSharing_vXXX.cab** and click **Open**. A Success message should appear temporarily to indicate a successful upload.
11. Click **Upload Package** again.
12. Browse to the Installation files for Intel Unite solution and open the **Manifests** directory.
13. Select **Unite_Hub_vXXX._enabled.cab** and click **Open**. A Success message should appear temporarily to indicate a successful upload.
14. Click **Upload Package** again.
15. Browse to the Installation files for Intel Unite solution and open the **Manifests** directory.
16. Select **Unite_HubRemoteView_vXXX.cab** and click **Open**. A Success message should appear temporarily

to indicate a successful upload.

17. Click **Upload Package** again.
18. Browse to the Installation files for Intel Unite solution and open the **Manifests** directory.
19. Select **Unite_HubScreenSharing_vXXX.cab** and click **Open**. A Success message should appear temporarily to indicate a successful upload.
20. (Steps 20–22 are optional) If the file transfer feature is needed click **Upload Package** again.
21. Browse to the Installation files for Intel Unite solution and open the **Manifests** directory.
22. Select **Unite_FileTransfer_vXXX.cab** and click **Open**. A Success message should appear temporarily to indicate a successful upload.

4.6.4 Approve Packages for Deployment

Configuration of core components, apps, and features in a package is not available for assignment until the package is approved. These components are needed for hub and client configurations. To approve packages:

1. Log in to the Admin Portal.
2. Open the **Device Management** menu and click **Features/Apps**.
3. Click the **Package Approval** tab.
4. For each package shown, click the **Approve** button to approve the package.

4.6.5 Create a Hub Configuration

To create a hub configuration:

1. Log in to the Admin Portal.
2. Open the **Device Management** menu and click **Configurations**.
3. Click the **Create Configuration** button.
4. In the Configuration Name text field, enter a name for the configuration.
5. Open the **Intel Unite® Software Version** menu, and select **Intel Unite® Solution Hub - x.x.x.x**, where ***x.x.x.x*** is the release version number.
6. To add features or apps to the configuration, click the white plus sign with the blue background ( ) icon associated with the feature or app.
7. Click **Create Configuration** to save the new configuration.

4.6.6 Create a Client Configuration

To create a client configuration:

1. Log in to the Admin Portal.
2. Open the **Device Management** menu and click **Configurations**.
3. Click the **Create Configuration** button.
4. Click the **Client Configuration** check box.
5. In the Configuration Name text box, enter a name for the configuration.
6. Open the **Intel Unite® Software Version** menu, and select **Intel Unite(R) Client version - x.x.x.x**, where ***x.x.x.x*** is the release version number.
7. To add features or apps to the configuration, click the white plus sign with the blue background ( ) icon

associated with the feature or app.

8. Click the **Create Configuration** button to save the new configuration.

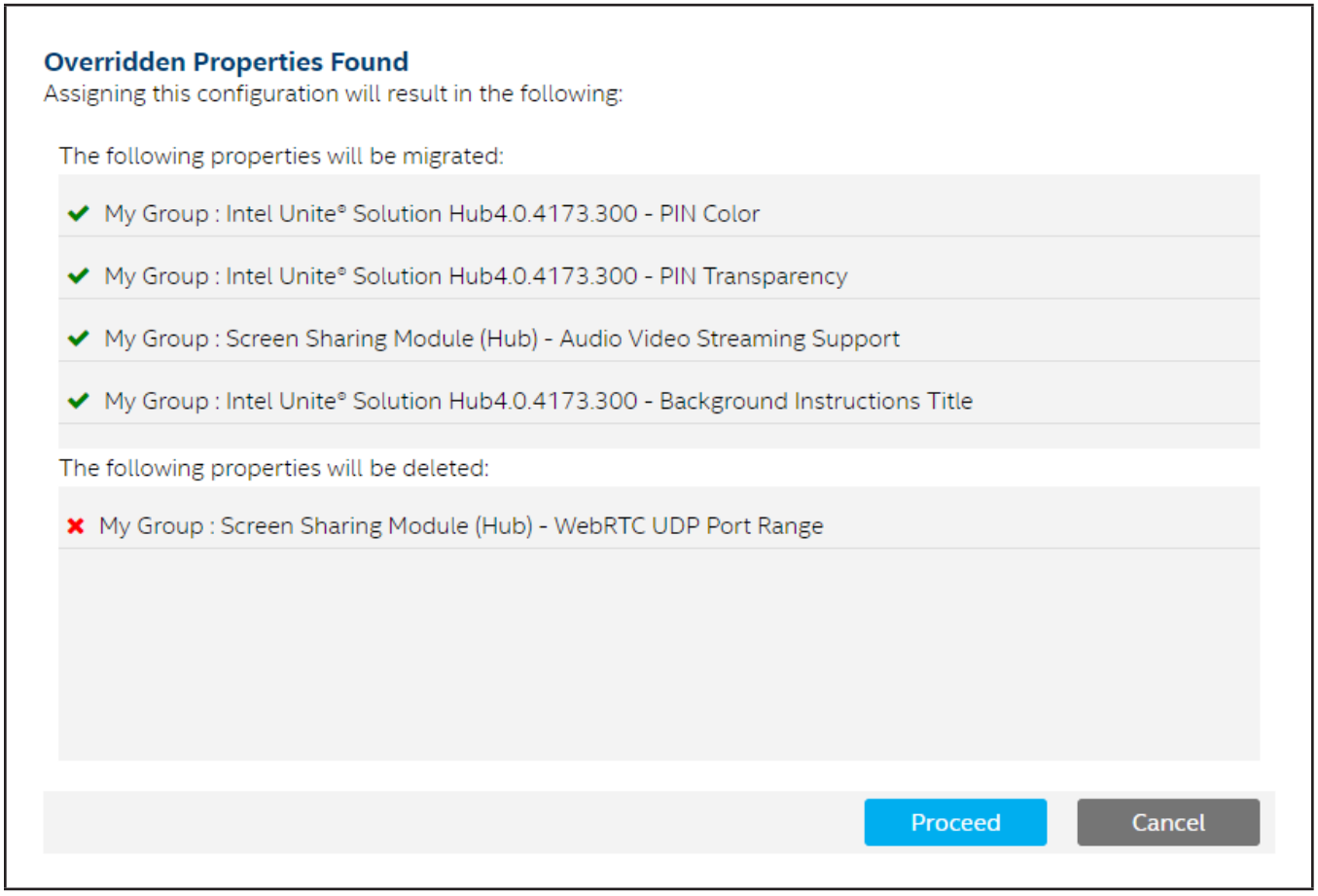
4.6.7 Assign Configurations to Hubs

To view defined hub configurations, open the **Device Management** menu, and click **Configurations**. To view a list of hub configurations, click the **Hub Configurations** tab. Follow the steps below to assign configurations to hubs:

1. Log in to the Admin Portal.
2. Open the **Device Management** menu and click **Hubs and Clients**.
3. Click the **Hubs** tab.
4. Click the group with the name that contains the organization name used during server installation. **Note:** Subgroups can be created, and configurations can be assigned to them. When assigning a configuration to a subgroup, expand the subgroup and click the group name under the subgroup.
5. Open the **Select Action** menu and select **Assign Configuration**.
6. Choose the hub configuration created in the previous steps.
7. Click **Assign**.

Note: If a group has custom/overridden properties configured, their values will retained when the new configuration is assigned, if possible. As shown in Figure 11, a confirmation dialog will appear that list custom/overridden properties and indicate whether or not they will be retained.

Figure 11. Custom/Overridden Properties Confirmation Dialog



If a group has custom/overridden properties, this confirmation dialog will be shown in the following events:

- A new configuration is assigned to the group.
- The version of a module of the configuration assigned to the group is changed.
- The group is moved or deleted.
- Device(s) are moved from/to the group.

4.6.8 Assign Configurations to Client Groups

To assign configurations to clients:

1. Log in to the Admin Portal.
2. Open the **Device Management** menu and click **Hubs and Clients**.
3. Click the **Clients** tab.
4. Click the group with the name that contains the organization name used during server installation.

   Note: Subgroups can be created, and configurations can be assigned to them. When assigning a configuration to a subgroup, expand the subgroup, and click the group name under the subgroup.
5. Open the **Select Action** menu and select **Assign Configuration**.
6. Choose the client configuration created in the previous steps.
7. Click **Assign**.

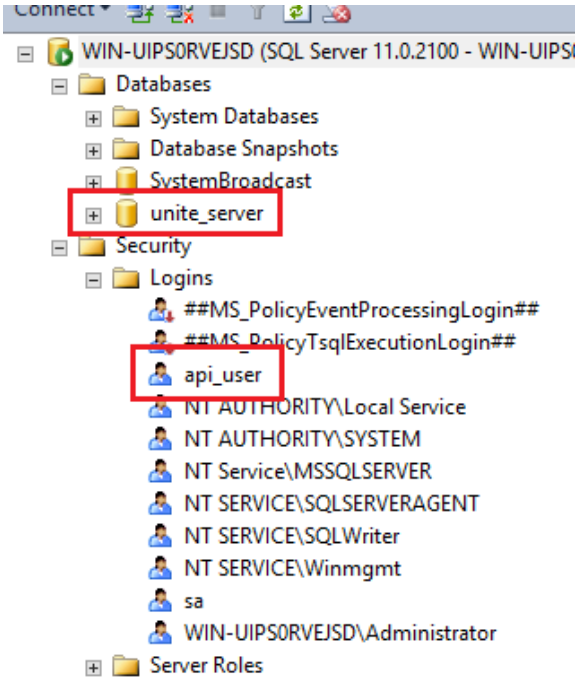
Note: To view defined client configurations, open the **Device Management** menu, and click **Configurations**. To view a list of client configurations, click the **Client Configurations** tab.

4.7 Enterprise Server Software Uninstallation

If the server application needs to be uninstalled, the **unite_server** database also needs to be deleted. Before uninstalling, back up the database.

1. Locate the **Intel_Unite_Server_vx.x.x.x_x86.mui.msi** file (copied to local storage or on network storage).
2. Launch the **Intel_Unite_Server_vx.x.x.x_x86.mui.msi** installer.
3. Click **Remove** and click **Next** to uninstall the Intel Unite solution server application.
4. Delete the SQL database using of the following procedures:
   - **Microsoft SQL**—Go to Microsoft SQL Server Management Studio, and manually delete the **unite_server** SQL database and the **api_user**, See Figure 12.

Figure 12. Objects to Delete from Microsoft SQL



- **MySQL**—Open a command-line window on the MySQL server. Start the MySQL interpreter by typing **mysql -h *<host-name>* -u=*<your-user-name>* -p** at the command prompt, where ***<host-name>*** is **localhost**, and ***<your-user-name>*** is the user name used during server installation. Enter the password. Type **drop databases unite_server;** to delete the database. Type **show databases;** to verify that the **unite_server** database is deleted. Type **drop user api_user**, to delete the **api_user**.

4.7.1 Enterprise Server Command-Line Uninstallation

The Intel Unite application installer for the enterprise server supports command-line uninstallation. The installer msi file must be in a known location on the local system or network share. The following command and parameters for uninstallation must be executed as an administrator:

msiexec /x "Installer_Path.msi" /l*v "Log_Path" /q

4.7.1.1 Enterprise Server Command-Line Uninstallation Parameters

The uninstallation parameters are case-sensitive. The result of an uninstallation can be determined by parsing the log file. Double quotes are only required for input values that include one or more spaces. When in doubt, use double quotes to surround input values.

/x—The switch for uninstall.

"Installer_Path.msi"—The path and filename of the msi file, including double quotes.

/l*v—The switch for generating a log file (for example, **"c:\my logs\serveruninstallog.txt"**).

"Log_Path"—The path including the log filename, with double quotes (for example, **"c:\my downloads\installer.msi"**).

/q—The switch for silent, no user interaction.

4.8 Enterprise Server Log Files

The server saves log files at the following path:

```
C:\Users\IntelUniteWebApiPool\AppData\Local\Temp
```

The following log files are found in the above path:

- IntelUniteServerLog.txt
- IntelUniteTransactionLog.txt
- UniteServerLog.txt

5 Hub Installation

5.1 Hub Pre-Installation

A hub needs to be able to locate and pair with the enterprise server. The Intel Unite® application needs an exemption in the hub firewall to communicate with the enterprise server. The port used by the Intel Unite application is randomly set by default; however, the port value can be set through the Admin Portal under hub configuration properties. In addition, complete the following verifications:

- Verify a network connection with the server by pinging to the server from the hub using the FQDN of the server and pinging from the server to the hub using the FQDN of the hub.
- Verify a DNS TXT record has been created for the Intel Unite solution service (refer to Section 4.5 for more information).
- Verify that the hub meets the minimum software and hardware requirements specified in Section 2.2.

5.1.1 Use Self-Signed Certificates

If the server uses a self-signed certificate, the certificate needs to be imported into the Trusted Root of the hub's certificate store. To do this, the certificate must be exported from the Admin Portal, saved locally, and then imported on a hub. This section describes how to export, save, and import self-signed certificates on Windows* and Mac* clients.

5.1.1.1 Import Certificates on Windows* Clients

To import a self-signed certificate for a Windows* client:

1. Export certificate:
   - For Chrome:
     a. Open Chrome and browse to the Admin Portal (**https://<FQDN of the Server>/intelunite/admin**).
     b. Right-click the red lock icon in the address bar and click **Certificate**.
     c. Click the **Details** tab and click **Copy to File**. The Certificate Export Wizard opens.
     d. In the Certificate Export Wizard, click **Next** to go to the Export File Format screen.
     e. Choose **DER encoded binary X.509 (.CER)** and click **Next**.
     f. Click **Browse** and save the file to the computer using a descriptive name.
     g. Click **Next**, and then click **Finish** to close the wizard.
   - For Internet Explorer:
     a. Open Internet Explorer and browse to the Admin Portal (**https://<FQDN of the Server>/intelunite/admin**).
     b. Click the lock icon in the address bar and click **View Certificate**.
     c. Click the **Details** tab and click **Copy to File**. The Certificate Export Wizard opens.
     d. In the Certificate Export Wizard, click **Next** to go to the Export File Format screen.
     e. Choose **DER encoded binary X.509 (.CER)** and click **Next**.
     f. Click **Browse** and save the file to the computer using a descriptive name.
     g. Click **Next** and then click **Finish** to close the wizard.
2. Import certificate.
   - For Chrome:

a. Open Chrome settings, scroll to the bottom, and click **Advanced**.
a. Under Privacy and Security, click **Manage certificates**.
b. Click the **Trusted Root Certification Authorities** tab, and then click the **Import** button. The Certificate Import Wizard opens.
c. In the Certificate Import Wizard, click **Next** to go to the File to Import screen.
d. Click **Browse**, select the certificate file saved earlier, and then click **Next**.
e. Select **Place all certificates in the following store**. The selected store should be Trusted Root Certification Authorities. If it isn't, click **Browse**, and select it.
f. Click **Next**, and then click **Finish**.
g. Click **Yes** on the security warning.

- For Internet Explorer:
  a. Open Internet Explorer Internet Options.
  b. Click the **Content** tab.
  c. Click the **Certificates** button.
  d. Click the **Import** button to open the Certificate Import Wizard and click **Next**.
  e. Click **Browse**, select the certificate file saved earlier, and then click **Next**.
  f. Select **Place all certificates in the following store**. The selected store should be Trusted Root Certification Authorities. If it isn't, click **Browse**, and select it.
  g. Click **Next**, and then click **Finish**.
  h. Click **Yes** on the security warning.

5.1.2 Certificate Verification

In certain scenarios, such as no access to the internet, it is desirable to disable or limit the verification of certificates.

To disable certificate verification, set the following registry key to a REG_DWORD value of 1.

HKLM\SOFTWARE\Wow6432Node\Intel\Intel Unite\DisableCertificateChainVerification

Value meaning:

1 = Disables certificate chain verification

0 = Enables certificate chain verification (default behavior/also when key is not present)

To ensure that SSL certificates being used are verified, set the following registry key to a REG_DWORD value of 1.

HKLM\SOFTWARE\Wow6432Node\Intel\Intel Unite\EnforceSslCrlCheck

Value meaning:

1 = Enforces SSL CRL check

0 = Doe not enforce SSL CRL check (default behavior/also when key is not present)

5.2 Recommended Hub System Settings

To ensure the best possible end user experience, the hub should be configured so it is always ready to be used, and system alerts or pop-ups are suppressed. The recommended system settings are:

- Windows* automatically logs in with the account that executes the Intel Unite application.
- Screen savers are disabled.
- The system is set to never go into standby mode.
- The system is set to never log out.
- The display is set to never turn off.
- System alerts are suppressed.

5.3 Hub Software Installation

The following steps describe how to install the hub software:

1. Locate the **Intel_Unite_Hub_vx.x.x.x_x86.mui.msi** file (either copied to local storage or on network storage).
2. Launch the **Intel_Unite_Hub_vx.x.x.x_x86.mui.msi** file.
3. Click **Next**.
4. Accept the license agreement by checking the **I accept the terms of the License Agreement** box.
5. Click **Next**.
6. The default path for the installation is **C:\Program Files (x86)\Intel\Intel Unite\Hub *<version number>***, where ***<version number>*** is the version number of the hub software. If a different location is preferred, enter the new location into the text box or click the **Change** button to use the **Change destination folder** dialog box to select the installation location. If using the **Change destination folder** dialog box, browse to the install location, and click **OK**.
7. Click **Next**.
8. Click **Install** to start the installation.
9. When the installation completes, leave the box for launching the application unchecked, and click **Finish**.

5.3.1 File Sharing App Installation (Optional)

The following steps are optional and are for the installation of the File Sharing App:

1. Locate the **Intel_Unite_FileTransfer_x86.mui.msi** and launch it.
2. Click **Next**.
3. Accept the license agreement by checking the **I accept the terms of the License Agreement** box.
4. Click **Next**.
5. Click **Install** to install the module.
6. Click **Finish**.

5.3.2 Hub Software Command-Line Installation (Optional)

The Intel Unite application installer for the hub supports command-line installations. The installer msi file must be in a known location on the local system or network share. The following command and parameters for a hub software command-line installation must be executed as an administrator:

msiexec /i "Installer_Path.msi" /l*v "Log_Path" /q HUBINSTALLFOLDER="*Value*" ORGID="Value" PINSERVERURI="Value" ORGNAME="Value" ACCEPTPRIVACYSTATEMENT="yes|no" REGISTRYMODE="HKCU|HKLM" OTP="Value"

5.3.2.1 Hub Installation Parameters

The hub installation parameters are case-sensitive. The result of the installation can be determined by parsing the log file. Double quotes are only required for input values that include one or more spaces. When in doubt, use double quotes to surround input values.

/i—The switch for install.

"Installer_Path.msi"—The path and filename of the msi file, with double quotes (for example, **"c:\my downloads\installer.msi"**).

/l*v—The switch for generating a log file.

"Log_Path"—The path including the log filename, with double quotes (for example, **"c:\my logs\ hubinstallog.txt"**).

/q—The switch for silent, no user interaction.

HUBINSTALLFOLDER="*Value*"—The location specifying where to install the hub application, replace ***Value*** with the full path, with double quotes (for example, **"c:\my apps\unite hub"**).

ORGID="Value"—The organization ID, replace ***Value*** with the organization ID.

PINSERVERURI="Value"—The PIN server URL, replace ***Value*** with the PIN server URL which has this format: **https://*<FQDN of the server hosting the Admin Portal>***/intelunite/api.

ORGNAME="Value"—The organization name, replace ***Value*** with the organization name.

ACCEPTPRIVACYSTATEMENT="yes"—Sets the accept privacy statement checkbox.

REGISTRYMODE="HKCU|HKLM"—Stores the client configuration

OTP="Value"—The OTP token used for pairing a hub, replace ***Value*** with the OTP token obtained from the Admin Portal.

DISABLEAUTODISCOVERY="<yes|no>"—Enable or disable automatic discovery of the Intel Unite® Cloud Service server. Set to “yes” to disable automatic discovery. Set to “no” to enable automatic discovery.

5.4 Configure Hub Firewall

A firewall may prevent the hub from communicating to the Intel Unite solution server and client devices. Below are steps to configure the firewall to allow network access for the hub application for the Intel Unite solution. Review and consult with the IT administrator prior to making any changes to the device.

5.4.1 Create Inbound Rule

1. Open Control Panel.

2. Enter **Windows Defender Firewall** into the search box.
3. Click on **Windows Defender Firewall** in the search results.
4. Click on **Advanced settings**.
5. Click **Yes** on the User Account Control dialog box.
6. Select **Inbound Rules**.
7. Select **New Rule...** under Actions pane.
8. Select **Program** and click **Next >**.
9. Select **This program path:** and browse to the location of the hub application launcher. **Note:** Default path of the hub application launcher is C:\Program Files (x86)\Intel\Intel Unite\Hub <version number>\Intel.Unite.HubLauncher.exe.
10. Click **Next >** once the program path is set.
11. Select **Allow the connection** and click **Next >**.
12. Place a check in the box for **Domain**, **Private**, and **Public** and click **Next >**.
13. Enter a name and a description for this rule and click **Finish**.
14. Select **Inbound Rules**.
15. Select **New Rule...** under Actions pane.
16. Select **Port** and click **Next >**.
17. Select **TCP** and **Specific local ports:**.
18. Enter "443" in the text field next to **Specific local ports:** and click **Next >**.
19. Select **Allow the connection** and click **Next >**.
20. Place a check in the box for **Domain**, **Private**, and **Public** and click **Next >**.
21. Enter a name and a description for this rule and click **Finish**.

5.4.2 Create Outbound Rule

1. Open Control Panel.
2. Enter **Windows Defender Firewall** into the search box.
3. Click on **Windows Defender Firewall** in the search results.
4. Click on **Advanced settings**.
5. Click **Yes** on the User Account Control dialog box.
6. Select **Outbound Rules**.
7. Select **New Rule...** under Actions pane.
8. Select **Program** and click **Next >**.
9. Select **This program path:** and browse to the location of the hub application launcher. **Note:** Default path of the hub application launcher is C:\Program Files (x86)\Intel\Intel Unite\Hub <version number>\Intel.

Unite.HubLauncher.exe.

10. Click **Next >** once the program path is set.
11. Select **Allow the connection** and click **Next >**.
12. Place a check in the box for **Domain**, **Private**, and **Public** and click **Next >**.
13. Enter a name and a description for this rule and click **Finish**.
14. Select **Outbound Rules**.
15. Select **New Rule...** under Actions pane.
16. Select **Port** and click **Next >**.
17. Select **TCP** and **Specific local ports:**.
18. Enter "443" in the text field next to **Specific local ports:** and click **Next >**.
19. Select **Allow the connection** and click **Next >**.
20. Place a check in the box for **Domain**, **Private**, and **Public** and click **Next >**.
21. Enter a name and a description for this rule and click **Finish**.

5.5 Hub Privacy

Upon the first launch of hub application, a privacy statement dialogue reading "Can the Intel Unite® application collect and send anonymous usage data?" will be displayed if the **Privacy Mode** server property is set to **Prompt User**. To proceed, click the **Yes** button.

5.6 Hub Pairing

Before a hub can be used, it must be paired with an Admin Portal. Part of the hub pairing process is hub configuration, which sets the **OrganizationID, OrganizationName,** and **ServerURL** values.

5.6.1 Hub Configuration

The **OrganizationID, OrganizationName,** and **ServerURL** values can be obtained in two ways—DNS TXT record and URL.

5.6.1.1 DNS TXT Record

When a hub first starts, it checks to see if the **OrganizationID**, **OrganizationName**, and **ServerURL** are set. If the values are not set, the hub attempts to obtain the values by looking for the DNS TXT record. Once the hub finds the DNS TXT record, it parses the text string to set the **OrganizationID**, **OrganizationName**, and **ServerURL**.

5.6.1.2 URL

During installation of the hub a custom URL protocol handler for **intelunite4** is installed. This handler launches the hub application with the URL as an argument, allowing the hub to parse the URL to obtain the **OrganizationID**, **OrganizationName**, and **ServerURL**. To use this handler, browse to the Admin Portal landing page (**https://<FQDN of the server hosting the Admin Portal>/intelunite/admin/landing**) on the hub, and click the link.

5.6.2 Hub Pairing Methods

Pairing a hub can be done in the following two ways:

- **Method 1**—Auto Pairing

- **Method 2**—Manually through the Admin Portal

5.6.2.1 Auto Pairing

The auto pairing steps are applicable on hubs that have the **OrganizationID**, **OrganizationName**, and **ServerURL** set. If the values are not set, the hub will not be able to find the Admin Portal for pairing. To use auto pairing:

1. Log in to the Admin Portal.
2. Open the **Device Management** menu.
3. In the **Duration (hours)** text box, enter the number of hours the token will be valid.
4. Click the **Generate Token** button to generate a one-time pairing token.
5. From the hub device, open a web browser, and browse to the URI **intelunite4://localhost/pair?otp=*<token>***, where ***<token>*** is the value from Step 4.

The token is saved to the Auto Pairing Management page. To access the token at a later time, log in to the Admin Portal, open the **Device Management** menu, and select **Auto Pairing Management**. The Auto Pairing Management page displays a list of pairing tokens, along with the date and time of when the tokens expire.

5.6.2.2 Manual Pairing Using the Admin Portal

The manual pairing steps are applicable on hubs that have the **OrganizationID**, **OrganizationName**, and **ServerURL** set. If the values are not set, the hub will not be able to find the Admin Portal for pairing. To use manual pairing:

1. Launch the hub software.
2. When the hub software launches, a privacy statement displays. To continue, click **Agree** to consent to the privacy statement.
3. Confirm the hub displays the instruction for pairing with a six-digit PIN.
4. Browse to the Admin Portal. If the hub software prevents the browser from launching, use another system on the same network.
5. Log in using the built-in admin user account:
   - **User Name:** admin
   - **Password:** Admin@1

   The first time the built-in admin account is used to log in to the Admin Portal, the Admin Portal prompts for a change of the **admin** password. Set a new password and use the new password to log in to the Admin Portal. Click the *i* in a gray circle next to **password rule** to see more information about the password requirements.
6. Open the **Device Management** menu.
7. Click in the **Pair Hub** text box, enter the six-digit PIN from the hub, and click the **Pair Hub** button.
8. The hub launcher downloads the components from the Admin Portal, and then displays the instructions on how to join a meeting.

Note: If the hub reports that the required hub version is missing, verify that the steps in the server configuration portion of this document have been completed.

5.7 Hub Software Uninstallation

The following steps describe how to uninstall the hub application:

1. Locate the **Intel_Unite_Hub_vx.x.x.x_x86.mui.msi** file (either on local storage or network storage).
2. Launch the **Intel_Unite_Hub_vx.x.x.x_x86.mui.msi** client installer.
3. Click **Remove** and click **Next**.

Removing the hub application does not remove the device from the Admin Portal. An administrator needs to manually delete the device from the Admin Portal. Until removed, a paired hub with an identical machine name is tagged as a "duplicate" entry.

5.7.1 Hub Software Command-Line Uninstallation (Optional)

The Intel Unite application installer for the hub supports command-line uninstallations. The installer msi file must be in a known location on the local system or network share. The following command and parameters for uninstallation must be executed as an administrator:

msiexec /x "Installer_Path.msi" /l*v "Log_Path" /q

5.7.1.1 Hub Software Command-Line Uninstallation Parameters

The hub command-line uninstallation parameters are case-sensitive. The result of the uninstallation can be determined by parsing the log file. Double quotes are only required for input values that include one or more spaces. When in doubt, use double quotes to surround input values.

/x—The switch for uninstall.

"Installer_Path.msi"—The path and filename of the msi file, with double quotes (for example, **"c:\my downloads\installer.msi"**).

/l*v—The switch for generating a log file (for example, **"c:\my logs\hubuninstallog.txt"**).

"Log_Path"—The path including the log filename, with double quotes.

/q—The switch for silent, no user interaction.

5.8 Hub Security

The hub administrator should ensure that recommended security practices are followed for each hub. If the local user is logged on automatically, ensure that the user does not run with administrative privileges. For additional security considerations, refer to Appendix D.

5.9 Hub Log File

The hub saves a log file at the following path:

`C:\Users\<user>\AppData\Local\Temp`, where `<user>` is the logged in user

The name of the log file is **Unite.sql**.

6 Client Installation

6.1 Client Pre-Installation

A client must be able to locate and check in with the enterprise server. The Intel Unite application needs an exemption in the client firewall to communicate with the enterprise server. The client port is the same as the hub port, which is by default randomly generated. However, the port number can be set through the Admin Portal hub configuration properties. For security considerations, refer to Appendix D.

All client devices must be connected to the corporate network or must use an appropriately configured VPN, including Windows*, iOS*, Mac*, Linux*, Chrome OS*, and Android* devices. Tablets and phones connected to their own carrier provider may not be able to connect to an Intel Unite app session due to corporate firewall configurations. Refer to the specific mobile device sections for more information.

Lastly, ensure each client meets the minimum software and hardware requirements, as specified in Section 2.3.

6.1.1 Use Self-Signed Certificates

If the server uses a self-signed certificate, the certificate needs to be imported into the Trusted Root of the client's certificate store. To do this, the certificate must be exported from the Admin Portal, saved locally, and then imported on a client. This section describes how to export, save, and import self-signed certificates on supported clients.

6.1.1.1 Export a Certificate

The steps to export certificates varies among browsers. This section describes how to export certificates in Chrome and Internet Explorer.

6.1.1.1.1 Export a Certificate Using Chrome

To export a certificate using Chrome:

1. Open Chrome and browse to the Admin Portal (**https://<FQDN of the Server>/intelunite/admin**).
2. Right-click the red lock icon in the address bar and click **Certificate**.
3. Click the **Details** tab and click **Copy to File**. The Certificate Export Wizard opens.
4. In the Certificate Export Wizard, click **Next** to go to the Export File Format screen.
5. Choose **DER encoded binary X.509 (.CER)** and click **Next**.
6. Click **Browse** and save the file to the computer using a descriptive name.
7. Click **Next**, and then click **Finish** to close the wizard.

6.1.1.1.2 Export a Certificate Using Internet Explorer

To export a certificate using Internet Explorer:

1. Open Internet Explorer and browse to the Admin Portal (**https://<FQDN of the Server>/intelunite/admin**).

2. Click the lock icon in the address bar and click **View Certificate**.
3. Click the **Details** tab and click **Copy to File**. The Certificate Export Wizard opens.
4. In the Certificate Export Wizard, click **Next** to go to the Export File Format screen.
5. Choose **DER encoded binary X.509 (.CER)** and click **Next**.
6. Click **Browse** and save the file to the computer using a descriptive name.
7. Click **Next** and then click **Finish** to close the wizard.

6.1.1.2 Import Certificates on Windows* Clients

Importing certificates on Chrome and Internet Explorer for Windows clients varies, as described in this section.

6.1.1.2.1 Import a Certificate for a Windows Client Using Chrome

To import a certificate on a Windows client using Chrome:

1. Open Chrome settings, scroll to the bottom, and click **Advanced**.
2. Under Privacy and Security, click **Manage certificates**.
3. Click the **Trusted Root Certification Authorities** tab and then click the **Import** button. The Certificate Import Wizard opens.
4. In the Certificate Import Wizard, click **Next** to go to the File to Import screen.
5. Click **Browse**, select the certificate file saved earlier, and then click **Next**.
6. Select **Place all certificates in the following store**. The selected store should be Trusted Root Certification Authorities. If it isn't, click **Browse** and select it.
7. Click **Next** and then click **Finish**.
8. Click **Yes** on the security warning.

6.1.1.2.2 Import a Certificate for a Windows Client Using Internet Explorer

To import a certificate on a Windows client using Internet Explorer:

1. Open the Internet Explorer Internet Options.
2. Click the **Content** tab.
3. Click the **Certificates** button.
4. Click the **Import** button to open the Certificate Import Wizard and click **Next**.
5. Click **Browse**, select the certificate file saved earlier, and then click **Next**.
6. Select **Place all certificates in the following store**. The selected store should be Trusted Root Certification Authorities. If it isn't, click **Browse** and select it.
7. Click **Next** and then click **Finish**.
8. Click **Yes** on the security warning.

6.1.1.3 Import Certificates on Mac* Clients

To import a self-signed certificate on a Mac* client:

1. Copy the self-signed certificate to the Mac.
2. Double-click the self-signed certificate to open it in Keychain Access.
3. The self-signed certificate appears in login. Copy the self-signed certificate to System. The certificate must

be copied to System to ensure it is trusted by all users and local system processes, including the virtual machine (.vmx) processes in Fusion Pro*.

4. Open the self-signed certificate in System, click to expand **Trust**, select **Use System Default**, and click **Save**.
5. Reopen the self-signed certificate in System, click to expand **Trust**, select **Always Trust**, and click **Save**.
6. Delete the self-signed certificate from login.

6.1.1.4 Import Certificates on Linux* Clients

To import a self-signed certificate on a Linux client using Fedora/Red Hat, open a terminal, and run the following commands:

- sudo cp <the certificate filename> /etc/pki/ca-trust/source/anchors/
- sudo update-ca-trust extract.

To import a self-signed certificate on a Linux client using Ubuntu, open a terminal, and run the following commands:

- sudo cp <the certificate filename> /usr/local/share/ca-certificates/
- sudo update-ca-certificates.

6.1.1.5 Import Certificates on Chrome OS* Clients

To import a self-signed certificate on a Chrome OS* client:

1. Open Chrome settings, scroll to the bottom, and click **Advanced**.
2. Under Privacy and Security, click **Manage certificates**.
3. Click the **Trusted Root Certification Authorities** tab and then click the **Import** button. The Certificate Import Wizard opens.
4. In the Certificate Import Wizard, click **Next** to go to the File to Import screen.
5. Click **Browse**, select the certificate file saved earlier, and then click **Next**.
6. Select **Place all certificates in the following store**. The selected store should be Trusted Root Certification Authorities. If it isn't, click **Browse** and select it.
7. Click **Next** and then click **Finish**.
8. Click **Yes** on the security warning.

6.1.1.6 Import Certificates on iOS* Clients

To import a self-signed certificate on an iOS* client:

1. Email the certificate to an account that can be accessed by the iOS client.
2. Open the email and select the certificate file.
3. Click **Install**.

6.1.1.7 Import Certificates on Android* Clients

To import a self-signed certificate on an Android* client:

1. Put the certificate onto the SD card of your Android device (usually to internal one). It should be in the root directory.

2. Click **Settings**, click **Security**, click **Credential storage**, and select **Install from device storage**.
3. When the .crt file is detected, enter a certificate name.
4. To find the certificate after importing it, click **Settings**, click **Security**, click **Credential storage**, click **Trusted credentials**, and then click **User**.

6.1.2 Certificate Validation

In certain scenarios, such as no access to the internet, it is desirable to disable or limit the validation of certificates.

To disable certificate validation, set the following registry key to a REG_DWORD value of 1.

HKLM\SOFTWARE\Wow6432Node\Intel\Intel Unite\Client\DisableCertificateChainValidation

Value meaning:

1 = Disables certificate chain validation

0 = Enables certificate chain validation (default behavior/also when key is not present)

To ensure that SSL certificates being used are validate, set the following registry key to a REG_DWORD value of 1.

HKLM\SOFTWARE\Wow6432Node\Intel\Intel Unite\Client\EnforceSslCrlCheck

Value meaning:

1 = Enforces SSL CRL check

0 = Doe not enforce SSL CRL check (default behavior/also when key is not present)

6.2 Client Download

The Windows* and Mac* client installer can be downloaded from the Admin Portal. To download the client application from the Admin Portal, browse to **https://<FQDN of the server>/intelunite/download**. To download the Windows* client, click the **Intel Unite® 4.0 for Microsoft® Windows®** link. To download the Mac* OS X client, click the **Intel Unite® for Apple® Mac® OS X®** link.

6.3 Client Install

Only a single Intel Unite solution version 4.0 client should be installed on a client device. Having more than a single client installed on a device is not supported.

6.3.1 Install Windows* Client

To install a Windows* client:

1. Locate the **Intel_Unite_Client_vx.x.x.x_x86.mui.msi** file (copied to local storage or network storage).
2. Launch the **Intel_Unite_Client_vx.x.x.x_x86.mui.msi** file.
3. Click **Next**.
4. Accept the license agreement by checking the **I accept the terms of the License Agreement** box.
5. Click **Next**.
6. The default path for the installation is **C:\Program Files (x86)\Intel\Intel Unite\Client *<version number>***, where ***<version number>*** is the version number of the client software. If a different location is preferred,

enter the new location into the text box or click the **Change** button to use the Change Destination Folder dialog box to select the install location. If using the Change Destination Folder dialog box, browse to the install location, and click **OK**.

7. Click **Next**.
8. Click **Install** to start other installation.
9. When the installation completes, click **Finish**.

Note: The support for extended display requires installing the Intel_Unite_Extended_Display_<x.x.x.x>.mui.msi.

6.3.1.1 Windows* Client Command-Line Installation (Optional)

The Intel Unite application installer for the client supports command-line installations. The installer msi file must be in a known location on the local system or network share. The following command and parameters for a Windows* client command-line installation must be executed as administrator:

msiexec /i "Installer_Path.msi" /l*v "Log_Path" /q CLIENTINSTALLFOLDER="Value" ORGID="Value" PINSERVERURI="Value" ORGNAME="Value" ACCEPTPRIVACYSTATEMENT="yes|no" REGISTRYMODE="HKCU|HKLM" OTP="Value" USEREMAIL="Value"

6.3.1.1.1 Windows* Client Command-Line Installation Parameters

The Windows* client command-line installation parameters are case-sensitive. The result of the installation can be determined by parsing the log file. Double quotes are only required for input values that include one or more spaces. When in doubt, use double quotes to surround input values.

/i—The switch for install.

"Installer_Path.msi"—The path and filename of the msi file, with double quotes.

/l*v—The switch for generating a log file (for example, **"c:\my logs\clientinstallog.txt"**).

"Log_Path"—The path including the log filename, with double quotes (for example, **"c:\my downloads\installer.msi"**).

/q—The switch for silent, no user interaction.

CLIENTINSTALLFOLDER="*Value*"—The location specifying where to install the client application. Replace ***Value*** with the full path (for example, **"c:\my apps\unite client"**).

ORGID="Value"—The organization ID, replace ***Value*** with the organization ID.

PINSERVERURI="Value"—The PIN server URL, replace ***Value*** with the PIN server URL which has this format: **https://*<FQDN of the server hosting the Admin Portal>***/intelunite/api.

ORGNAME="Value"—The organization name, replace ***Value*** with the organization name.

ACCEPTPRIVACYSTATEMENT="yes"—Sets the accept privacy statement checkbox.

REGISTRYMODE="HKCU|HKLM"—Stores the client configuration

OTP="Value"—The OTP token used for registering a client, replace ***Value*** with the OTP token obtained from the Admin Portal.

USEREMAIL="Value"—The e-mail of the user that uses this client, replace ***Value*** with the e-mail of the user that uses this client.

DISABLEAUTODISCOVERY="<yes|no>"—Enable or disable automatic discovery of the Intel Unite® Cloud Service server. Set to "yes" to disable automatic discovery. Set to "no" to enable automatic discovery.

6.3.2 Install Mac OS Client

It is possible to install the Mac OS Intel Unite client from both the Mac App Store and direct download from Intel, resulting in two or more Intel Unite clients 4.0 on the Mac OS device. Having multiple Intel Unite clients 4.0 on a single device is not supported and may result in the malfunction of the Intel Unite solution.

The Mac OS client supports connecting to 3.x and 4.0 hubs. It is recommended that only the Intel Unite client 4.0 is installed on a device that needs to connect to both 3.x and 4.0 hubs. To identify if more than a single Intel Unite client is installed on a client, follow these steps:

1. Open **Finder**.
2. Type **Intel Unite** in the search box located at the upper right corner and hit **return**.
3. Two fingers tap on the results area and select **Arrange By->Kind**.
4. Confirm that there is only one Intel Unite application. If more than one Intel Unite application is shown, remove all but one of the Intel Unite application.

To install a Mac OS client:

1. Locate the **Intel Unite macOS X.X.X.X.dmg** file and download the software to the Mac OS* client.
2. Double-click the file to extract the application.
3. After reviewing the End User License Agreement, click **Agree** to continue.
4. Drag the extracted file to the **Applications** folder. If prompted to replace an existing installed version of the Intel Unite client 4.0, click the **Replace** button.
5. Go to the **Applications** folder, locate the application, and click it to launch it.

6.3.3 Install iOS* Client

The app is compatible with all iPads* except the original 2010 iPad. To install an iOS* client:

1. On an iOS* client (such as an iPad), go to the Apple app store, and download the Intel Unite software for the client.
2. Once the app is downloaded, open the app.
3. Click the **Settings** gear (the gear icon in the upper-right corner) and enter the information requested.
4. On Settings, complete the **User Name** and **Server** information. Select **Automatic** to find the server, or to connect to a specific server, click **Manual**, and enter the server information. Click **Save**.
5. To connect to the hub, enter the PIN displayed on the monitor or screen, and start sharing.
6. Refer to the *Intel Unite® Solution User Guide* to learn about features and user information.

6.3.4 Install Android* Client

To install an Android* client:

1. On the Android* device, go to the Google app store, and download the Intel Unite software for the client.

2. Once the app is downloaded, open the app.
3. Click the **Settings** gear (the gear icon) and enter the information requested.
4. On Settings, complete the User Name and Server information. Select **Automatic** to find the server, or to connect to a specific server, click **Manual**, and enter the server information. Click **Save Settings**.
5. To connect to the hub, enter the PIN displayed on the monitor or screen, and start sharing.
6. Refer to the *Intel Unite® Solution User Guide* to learn about features and user information.

6.3.5 Install Chrome OS* Client

To install a Chrome OS* client:

1. On a Chromebook* device, go to the Google app store, and download the Intel Unite software for the client.
2. Once the app is downloaded, open the app.
3. Click the **Settings** gear (the gear icon in the upper-right corner) and enter the information requested.
4. On Settings, complete the User Name and Server information. Select **Automatic** to find the server, or to connect to a specific server, click **Manual**, and enter the server information. Click **Save Settings**.
5. To connect to the hub, enter the PIN displayed on the monitor or screen, and start sharing.
6. Refer to the *Intel Unite® Solution User Guide* to learn about features and user information.

6.3.6 Install Linux* OS Client

To install a Linux* OS client:

1. Obtain the corresponding Linux* client binary from the Intel Unite® solution support site:
   - Fedora*/Red Hat*—.rpm
   - Ubuntu*—.deb
   - Manual (advanced users)—.bz2
2. Install the client using the following commands:
   - Red Hat Enterprise and Fedora:

     sudo yum install /<rpm path>/<unite_pack.rpm>
   - Ubuntu

     sudo apt-get install ./<unite_pack.deb>
   - Manual (advanced users)

     Unpack the .bz2 file to a specified location
3. Click the **Settings** gear (the gear icon in the upper-right corner), complete the **User Name**, **Email**, and **Server** information. In the **Enterprise Server** text box, enter the server to connect to (for example, **https://**

unite.yourorganization.com).

4. Click **Save Settings**.
5. To connect to the hub, enter the PIN displayed on the monitor or screen, and start sharing.
6. Refer to the *Intel Unite® Solution User Guide* to learn about features and user information.

6.4 Configure Client Firewall

A firewall may prevent the client from communicating to the Intel Unite solution server and hub devices. Below are steps to configure the firewall to allow network access for the client application for the Intel Unite solution. Review and consult with the IT administrator prior to making any changes to the device.

6.4.1 Windows* Platforms

Below are the steps for configuring the firewall for Windows* platforms.

6.4.1.1 Create Inbound Rule

1. Open Control Panel.
2. Enter **Windows Defender Firewall** into the search box.
3. Click on **Windows Defender Firewall** in the search results.
4. Click on **Advanced settings**.
5. Click **Yes** on the User Account Control dialog box.
6. Select **Inbound Rules**.
7. Select **New Rule...** under Actions pane.
8. Select **Program** and click **Next >**.
9. Select **This program path:** and browse to the location of the client application launcher. **Note:** Default path of the client application launcher is `C:\Program Files (x86)\Intel\Intel Unite\Client <version number>\Intel.Unite.ClientLauncher.exe`.
10. Click **Next >** once the program path is set.
11. Select **Allow the connection** and click **Next >**.
12. Place a check in the box for **Domain**, **Private**, and **Public** and click **Next >**.
13. Enter a name and a description for this rule and click **Finish**.
14. Repeat Steps 6 through 13 to add an inbound rule for the add client application located at the following path: `%program data%/Intel/Intel Unite/Client/Current/Intel Unite Client.exe`.
15. Select **Inbound Rules**.
16. Select **New Rule...** under Actions pane.
17. Select **Port** and click **Next >**.
18. Select **TCP** and **Specific local ports:**.
19. Enter "443" in the text field next to **Specific local ports:** and click **Next >**.
20. Select **Allow the connection** and click **Next >**.
21. Place a check in the box for **Domain**, **Private**, and **Public** and click **Next >**.
22. Enter a name and a description for this rule and click **Finish**.

6.4.1.2 Create Outbound Rule

1. Open Control Panel.
2. Enter **Windows Defender Firewall** into the search box.
3. Click on **Windows Defender Firewall** in the search results.
4. Click on **Advanced settings**.
5. Click **Yes** on the User Account Control dialog box.
6. Select **Outbound Rules**.

7. Select **New Rule...** under Actions pane.
8. Select **Program** and click **Next >**.
9. Select **This program path:** and browse to the location of the hub application launcher. **Note:** Default path of the hub application launcher is C:\Program Files (x86)\Intel\Intel Unite\Client <version number>\Intel.Unite.ClientLauncher.exe.
10. Click **Next >** once the program path is set.
11. Select **Allow the connection** and click **Next >**.
12. Place a check in the box for **Domain**, **Private**, and **Public** and click **Next >**.
13. Enter a name and a description for this rule and click **Finish**.
14. Repeat Steps 6 through 13 to add an outbound rule for the add client application located at the following path: `%program data%/Intel/Intel Unite/Client/Current/Intel Unite Client.exe`.
15. Select **Outbound Rules**.
16. Select **New Rule...** under Actions pane.
17. Select **Port** and click **Next >**.
18. Select **TCP** and **Specific local ports:**.
19. Enter "443" in the text field next to **Specific local ports:** and click **Next >**.
20. Select **Allow the connection** and click **Next >**.
21. Place a check in the box for **Domain**, **Private**, and **Public** and click **Next >**.
22. Enter a name and a description for this rule and click **Finish**.

6.4.2 MacOS* Platforms

Below are the steps for configuring the firewall for Mac OS* platforms.

1. Choose **System Preferences** from the Apple menu.
2. Click **Security**.
3. Click the **Firewall** tab.
4. Click the **Firewall Options...** button.
5. Click the button with the plus symbol to add an application.
6. Select Intel Unite and click the **Add** button.
7. Click the **OK** button.
8. Close the System Preferences window.

Port 443 is usually open by default. Verify by opening a browser and navigating to https://www.intel.com. If the browser does not load the webpage, contact IT support to open port 443 on the device.

6.4.3 Linux* Platforms

On Linux platforms, the network port used by hubs and clients must be set before configuring the clients' firewall to allow traffic through that port.

6.4.3.1 Define Network Port on the Admin Portal for Hubs

The network port used by a client is communicated by the hub. To configure the network port that is used by the Intel Unite app running on a hub (which will be communicated to clients), follow the steps below.

1. Log into the Admin Portal.
2. Select Hubs and Clients under Device Management menu.
3. Click on the Hub tab.
4. For each group, set the Network Port property to the same value. This is the value that will be used to configure the client firewall.
   a. Select a group.
   b. Select Group Details from the select action drop-down menu.

c. Click the Edit Properties button.
d. Enter a number for the Network Port property and click the Save Changes button.

5. All groups are set to use the same network port

6.4.3.2 Configure Firewall with Network Port Value

Once the network port is set for the hubs on the Admin Portal, the client firewall can be configured to allow network traffic through that port.

1. On the Linux client device open a command terminal.
2. Type the following commands to allow network traffic through a port for the internal, external, public, trusted, and work zones (replace <network port> with the value set on the Admin Portal):

```
firewall-cmd --permanent --zone=internal --add-port=<network port>/tcp
firewall-cmd --permanent --zone=external --add-port=<network port>/tcp
firewall-cmd --permanent --zone=public --add-port=<network port>/tcp
firewall-cmd --permanent --zone=trusted --add-port=<network port>/tcp
firewall-cmd --permanent --zone=work --add-port=<network port>/tcp
firewall-cmd --permanent --zone=internal --add-port=443/tcp
firewall-cmd --permanent --zone=external --add-port=443/tcp
firewall-cmd --permanent --zone=public --add-port=443/tcp
firewall-cmd --permanent --zone=trusted --add-port=443/tcp
firewall-cmd --permanent --zone=work --add-port=443/tcp
```

6.4.4 Alternative Firewall Configurations

IT security policies may result in unique firewall configurations. Contact the IT administrator for assistance in allowing internal and external network traffic for the Intel Unite application or with setting specific ports that can be used by the Intel Unite application for network traffic.

6.5 Client Registration

Before a client can be used, it must be registered with an Admin Portal. Part of the client registration process is client preregistration configuration, which sets the **OrganizationID, OrganizationName,** and **ServerURL** values.

6.5.1 Client Preregistration Configuration

The **OrganizationID, OrganizationName,** and **ServerURL** values can be obtained in three ways—DNS TXT record, URL, and client settings.

Support for DNS TXT record and custom URL varies on OSs running on client platforms. Due to these differences, not all methods for client configuration are available on all client platforms. The following table shows the configuration methods supported on each client OS.

Client Preregistration Configuration Support per OS

Registration Method	Windows*	Mac*	Chrome OS*	Linux*	iOS*	Android*
DNS TXT Record	Supported	Supported	**Not Supported**	Supported	Supported	Supported
URL	Supported	Supported	**Not Supported**	Supported	Supported	**Not Supported**

Registration Method	Windows*	Mac*	Chrome OS*	Linux*	iOS*	Android*
Manual	Not Supported	Not Supported	Supported	Not Supported	Not Supported	Supported

6.5.1.1 DNS TXT Record (Windows*, mac OS*, Linux*, Android, and iOS)

When a client first starts, it checks to see if the **OrganizationID**, **OrganizationName**, and **ServerURL** are set. If the values are not set, the client attempts to obtain the values by looking for the DNS TXT record. Once the client finds the DNS TXT record, it parses the text string to set the **OrganizationID**, **OrganizationName**, and **ServerURL**.

6.5.1.2 URL (Windows, mac OS, Linux, and iOS)

During installation of the client on Windows*, Mac*, Linux*, and iOS*, a custom URL protocol handler for **intelunite4** is installed. This handler launches the client application with the URL as an argument, allowing the client to parse the URL to obtain the **OrganizationID**, **OrganizationName**, and **ServerURL**. To use this handler, browse to the Admin Portal landing page (**https://*<FQDN of the server hosting the Admin Portal>*/intelunite/admin/landing**) on the client, and click the link.

6.5.1.3 Client Settings (Chrome OS*)

The **OrganizationID, OrganizationName,** and **ServerURL** values can be set manually through the client settings. To use this method:

1. Copy the URL from the Admin Portal landing page (**https://*<FQDN of the server hosting the Admin Portal>*/intelunite/admin/landing**).
2. Launch the Intel Unite client.
3. Paste the URL when prompted to provide the provisioning URL.
4. Click OK.

6.5.1.4 Google* Admin Console (Chrome OS*)

The **ServerURL** value can be set for Chrome OS* platforms through the Google Admin console. Refer to Appendix A for details about using the Google Admin console.

6.5.1.5 Confirming OrganizationID, OrganizationName, and ServerURL

The process to confirm the values set for **OrganizationID**, **OrganizationName**, and **ServerURL** are different based on OS running on the client platform.

6.5.1.5.1 Windows* Platforms

The **OrganizationID**, **OrganizationName**, and the **ServerURL** values are stored in the following registry keys on Windows* platforms:

HKEY_CURRENT_USER\SOFTWARE\Intel\Intel Unite\Client\OrganizationID

HKEY_CURRENT_USER\SOFTWARE\Intel\Intel Unite\Client\OrganizationName

HKEY_CURRENT_USER\SOFTWARE\Intel\Intel Unite\Client\ServerURL

The **OrganizationID** is a **REG_SZ** value with the following format:

XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX

where ***X*** is a hexadecimal value. This value can be found on the Admin Portal landing page.

The **OrganizationName** is a **REG_SZ** with a string value that is determined during the server install.

The **ServerURL** is a **REG_SZ** with a string value of **https://*<FQDN of the Admin Portal Server>*/intelunite/api**, where ***<FQDN of the Admin Portal Server>*** is the fully qualified domain name of the server hosting the Admin Portal website.

Confirm that the three values match the values in the URL of the Admin Portal landing page (**https://*<FQDN of the server hosting the Admin Portal>*/intelunite/admin/landing**).

6.5.1.5.2 Mac OS*, iOS*, Linux*, Android*, and Chrome OS*

The **OrganizationID**, **OrganizationName**, and **ServerURL** are displayed in the client settings. Launch the client, click the gear icon in the upper-right corner, click **Configurations**, and the **OrganizationID**, **OrganizationName**, and **ServerURL** are shown on the Configurations page.

Confirm that these three values match the values in the URL of the Admin Portal landing page (**https://*<FQDN of the server hosting the Admin Portal>*/intelunite/admin/landing**).

6.5.2 Client Registration Methods

Registering a client can be done in three ways:

- **Method 1**—Auto Pairing Mode
- **Method 2**—Standard Pairing Mode (no email confirmation)
- **Method 3**—Enhanced Pairing Mode (email confirmation)

Note: The pairing mode is set during server installation. The value of this setting can be viewed from the Server Properties page of the Admin Portal.

6.5.2.1 Method 1 – Auto Pairing Mode

The steps for the Auto Pairing Mode method vary among the supported operating systems due to different levels of support for custom URL handlers. Only supported on Windows and mac OS platforms.

6.5.2.1.1 Windows* and mac OS*

These steps are applicable on clients that have the **OrganizationID**, **OrganizationName**, and **ServerURL** already set. Confirm that the three values are set on the platform prior to executing the following steps:

1. Log in to the Admin Portal.
2. Click **Device Management** to open the Device Management menu.
3. In the **Auto Pairing** section, click in the **Duration (hours)** text box, and enter the number of hours the token will be valid.
4. Click the **Generate Token** button to display the Generate Token dialog box.
5. On the Client device, open a web browser, and browse to the URI **intelunite4://localhost/pair?otp=*<token>*&email=*<email address>*&machineName=*<machinename>***, where ***<token>*** is the value from Step 4, ***<email address>*** is the email address that receives the registration email, and

<machinename> is the name of the system.

6.5.2.1.2 Chrome OS*

These steps are applicable on clients that have the **OrganizationID**, **OrganizationName**, and **ServerURL** already set. Confirm that the three values are set on the platform prior to executing the following steps:

1. Log in to the Admin Portal.
2. Click **Device Management** to open the Device Management menu.
3. In the **Auto Pairing** section, click in the **Duration (hours)** text box, and enter the number of hours the token will be valid.
4. Click the **Generate Token** button to display the Generate Token dialog box.
5. On the Client device, start the Intel Unite® client application.
6. Click on **Use an Auto Pairing URL** at the bottom to display a text box.
7. Copy and paste the URI from the Generate Token dialog box into the text box and replace the machinename and the e-mail address with the appropriate values. The URI from the Generate Token dialog box is in the following format: **intelunite4://localhost/pair?otp=*<token>*&email=*<email address>*&machineName=*<machinename>***, where ***<token>*** is the value from Step 4, ***<email address>*** is the email address that receives the registration email, and ***<machinename>*** is the name of the system.

6.5.2.2 Method 2 – Standard Pairing Mode (No Email Confirmation)

These steps are applicable on clients that have the **OrganizationID**, **OrganizationName**, and **ServerURL** already set. Confirm that the three values are set on the platform prior to executing the following steps:

1. Launch the client application.
2. When the client software launches, a privacy statement may be displayed. To continue, click **Agree** to consent to the privacy statement.

   A privacy statement only appears if the server property for data collection is set to **Prompt user to potentially share anonymous data with Intel** on the Admin Portal.

   Make sure there is a DNS entry for the email server in the DNS lookup table and that pinging from the server to the email server using the FQDN and IP address is successful. This might require flushing DNS if a DNS entry is created after attempting to go to a URL.
3. After launching the client, the client software asks for an email address. Enter an email address for the user. This email address is used to enable the moderator feature for user devices when Standard Pairing Mode is set.

The client is now ready to connect to a hub running the Intel Unite® software.

6.5.2.3 Method 3 – Enhanced Pairing Mode (Email Confirmation)

These steps are applicable on clients that have the **OrganizationID**, **OrganizationName**, and **ServerURL** already set. Confirm that the three values are set on the platform prior to executing the following steps:

1. Launch the client.
2. When the client software launches, a privacy statement may be displayed. To continue, click **Agree** to consent to the privacy statement.

   A privacy statement only appears if the server property for data collection is set to **Prompt user to potentially share anonymous data with Intel** on the Admin Portal.

Make sure there is a DNS entry for the email server in the DNS lookup table and that pinging from the server to the email server using the FQDN and IP address is successful. This might require flushing DNS if a DNS entry is created after attempting to go to a URL.

3. After launching the client, the client software asks for an email address. Enter an email address that can receive the registration email from the Admin Portal.
4. Click **Submit** and verify that the **Submit** button is replaced by a **Resend** button.
5. Go to the email account and open the email from the Admin Portal. Check the Junk folder if the email is not in the inbox.
6. Click the link in the email to register the client.

The client is now ready to connect to a hub running the Intel Unite® software.

6.5.3 Multiple Organization Support

Intel Unite® client devices can be registered with more than one server. Usually, each organization will have a server supporting the Intel Unite solution. For users that travel to different organizations that implement Intel Unite solution, the client device can join Intel Unite solution sessions in these different organizations if the client device is resisted with the server for the Intel Unite solution for each organization.

When the Intel Unite client application starts, it will look for a DNS TXT Record to determine the server for the Intel Unite solution, the Organization ID, and the Organization Name. If there is no DNS TXT Record or if the use of DNS TXT Record for auto discovery is disabled, and the device has registered with more than one server for the Intel Unite solution, then the client will display a list of Organization Names that corresponds to the servers that the client device has registered with. Choosing an Organization Name will allow the client device to connect to all the hubs that are paired with that organization's server for the Intel Unite solution.

6.6 Client Software Uninstallation

This section provides information about uninstalling the client software on Windows* and Linux*.

6.6.1 Windows*

To uninstall the client application on a Windows* computer:

1. Locate the **Intel_Unite_Client_vx.x.x.x_x86.mui.msi** file (either on local storage or network storage).
2. Launch the client installer **Intel_Unite_Client_vx.x.x.x_x86.mui.msi**.
3. Click **Remove** and click **Next**.

Removing the client application does not remove the device from the Admin Portal. An administrator needs to manually delete the device from the Admin Portal. Until removed, a paired client with an identical machine name will be tagged as a "duplicate" entry.

6.6.1.1 Client Software Command-Line Uninstallation (Optional)

The Intel Unite application installer for the client supports command-line uninstallations. The installer msi file must be in a known location on the local system or network share. The following command and parameters for uninstallation must be executed as an administrator:

msiexec /x "Installer_Path.msi" /l*V "Log_Path" /q

6.6.1.2 Client Software Command-Line Uninstallation Parameters

The client command-line uninstallation parameters are case-sensitive. The result of the uninstallation can be determined by parsing the log file. Double quotes are only required for input values that include one or more spaces. When in doubt, use double quotes to surround input values.

/x—The switch for uninstall.

"Installer_Path.msi"—The path and filename of the msi file, with double quotes (for example, **"c:\my downloads\installer.msi"**).

/l*v—The switch for generating a log file (for example, **"c:\my logs\hubuninstallog.txt"**).

"Log_Path"—The path including the log filename, with double quotes.

/q—The switch for silent, no user interaction.

6.6.2 Linux*

To uninstall the client application on Red Hat Enterprise, Fedora, or Ubuntu, use the following commands:

- Red Hat Enterprise and Fedora

  sudo yum remove intel-unite-client, sudo dnf remove intel-unite-client

- Ubuntu

  sudo apt-get remove intel-unite-client

6.7 Client Log File

The client saves a log file at the following path:

`C:\Users\<user>\AppData\Local\Temp`, where `<user>` is the logged in user

The name of the log file is **Unite.sql**.

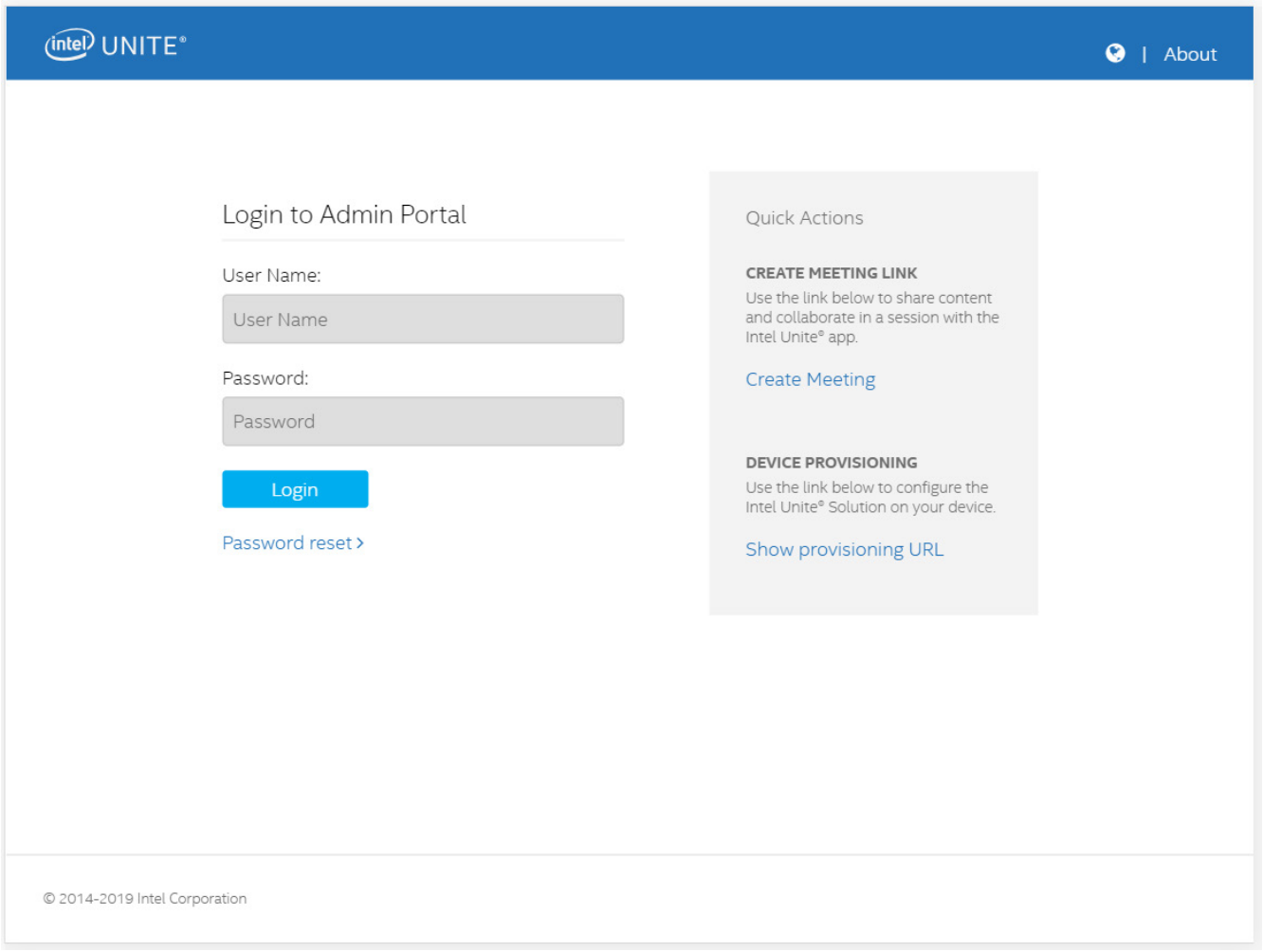
7 Admin Portal Guide

The Admin Portal is the administrator web portal for the Intel Unite application. It enables administrators to view and manage the devices using the Intel Unite application. The Admin Portal is one of the components installed on the enterprise server during installation, along with the PIN service and web server (for more information about the enterprise server installation, refer to Section 4.3). The Admin Portal must be able to access the database, although it does not need to be on the same server as the database.

7.1 Admin Portal Login Page

The login page consists of the login area, password reset link, and quick action links. See Figure 13.

Figure 13. Admin Portal Login Page



7.1.1 Access the Admin Portal

To access the Admin Portal:

1. Open a browser, and enter **https://*<yourserverFQDN>*/intelunite/admin**, where ***<yourserverFQDN>*** is the FQDN of the Intel Unite application's server.

2. On the login page, enter a user name and password, and click **Login**. Active Directory users should not include *domain*\ in the user name text box.

Note: When the IT administrator runs the server software installer, a default administrator account is created with the following user name and password:

- **User Name:** admin
- **Password:** Admin@1

The first time the built-in admin account is used to log in to the Admin Portal, the Admin Portal prompts for a change of the **admin** password. Set a new password and use the new password to log in to the Admin Portal. Click the *i* in a gray circle next to **password rule** to see more information about the password requirements.

After logging into the Admin Portal, if there is no activity for 30 minutes, the user is automatically logged out, and the login page is displayed with a message indicating that the user has been logged out due to inactivity.

7.1.1.1 Active Directory Users

For AD users, Intel recommends using the following format for logging in:

<username>@<domain>

Example: joe@company.com.

7.1.2 Reset User Passwords

A password reset link is provided on the Login page of the Admin Portal. To reset a user's password:

1. Click the **Password reset** link on the Admin Portal login page.
2. In the dialog box, enter the email address of the user that needs a password reset, and click **Send**.
3. Check the email address inbox for a reset email from the server for the Intel Unite solution.
4. Follow the instruction in the email to reset the user's password.

7.1.3 Quick Actions Links

Two Quick Actions links are on the Login page:

- **Create meeting**—Clicking this link displays the Join: dialog box, which includes a URL. Send the URL to participants so they can join a session. All participants who use the URL will join the same session. Participants must already have the Intel Unite® application installed on their registered client. Click the **Close** button to close the dialog box.
- **Get provisioning URL**—Clicking this link displays the Provision Device dialog box, which includes URL. The URL contains the **ServerURL** and the **OrganizationID**. This URL is used to start the Intel Unite application on a hub or a client prior to hub pairing or client registration. This URL is the same as the URL that is displayed on the Admin Portal landing page (**https://<FQDN of the server>/intelunite/admin/landing**).

7.2 Admin Portal

After login, the Admin Portal displays three main menus, three links, and the default view, which is the Groups page. The three menus are:

- Device Management

- Server Management
- User Management

The Admin Portal links, located in the upper-right corner, are the user icon (), the language icon (), and the About link. The user icon displays the user name and two options—**Logout** and **Edit Profile**.

7.2.1 Logout

To log out of the Admin Portal:

1. Click the user icon ().
2. Click **Logout** on the menu.

7.2.2 View and Edit a User Profile

To view and edit the user profile for a user who is currently logged in:

1. Click the user icon ().
2. Click **Edit Profile**, which opens the Account page.
3. On the Account page, update or change the user profile or password:
   - To update the user profile, make changes to the profile, and click **Update Profile**.
   - To change the user password, complete the **Current Password**, **New Password**, and **Confirm New Password** text boxes, and then click **Change Password**.

Note: The default Admin user account name cannot be changed.

7.2.3 Change the Display Language

The language icon () enables changing the language displayed in the Admin Portal. Available languages are:

- English
- German
- Spanish
- French
- Italian
- Japanese
- Korean
- Portuguese
- Chinese (Simplified)
- Chinese (Traditional)

To change the language:

1. Click the language icon ().

2. Choose a language and click **Apply**.

7.2.4 Admin Portal About Link

The About link in the Admin Portal displays the version and other information about the Intel Unite application. Click **About** in the upper-right corner of the page to view Intel Unite application details.

After logging in, the About detail includes the Organization ID.

7.3 Admin Portal – Device Management Menu

The Device Management menu provides links to device management pages and Quick Actions, which are described in this section.

The device management pages include:

- Hubs and Clients
- Configurations
- Features/Apps
- Reserved PINs
- Custom Metadata
- Provision Device
- Auto Pairing Management

The available Quick Actions are:

- Pair Hub
- Auto Pairing
- Upload Package
- Create Meeting

7.3.1 Device Management – Pages

In addition to the Quick Actions tools, the Device Management menu provides access to the following pages:

- Hubs and Clients
- Configurations
- Features/Apps
- Reserved PINs
- Custom Metadata
- Provision Device
- Auto Pairing Management

The following subsections describe the Device Management pages.

7.3.1.1 Hubs and Clients Page

The Hubs and Clients page displays the Device Groups view, which is the default view after logging into the Admin Portal. A *group* provides a way to organize devices that have the same configuration.

The Device Groups page lists groups and devices. By default, hub groups and devices are displayed. Click **Clients** to display the client groups and devices. To display the hub groups and devices, click **Hubs**.

Admin Portal groups associated with an Active Directory group are denoted by this  icon in the **AD Organization Unit** column. Hover over the icon to display the AD OU name.

Admin Portal groups that have a configuration assigned are denoted by this  icon in the **Configuration** column. Hover over the icon to display the configuration name.

Use the search box at the top of the page to quickly find devices. Enter a string in the search box and click the **Search** button to find devices that contains the string in the name. Use the **Clear** button to clear the search results.

7.3.1.1.1 Select Action Menu

The Select Action menu on the Groups page provides actions that can be applied to a selected group. Following are the descriptions of the available actions:

- **Group Details**—View and modify a group's details. To access a group's details page, select a group by clicking the group name, open the **Select Action** menu, and select **Group Details**. The group details page displays the group name and the Active Directory OU associated with the group. Groups can be renamed, added, and updated on this page, as follows:
  - To rename a group, click **Edit Group** next to the group name. The root group cannot be renamed.
  - To add or update an Active Directory OU association, click the **Assign** button, use the search box to list Active Directory OUs that contain the string in the name, select the desired Active Directory OU, and click **Assign**. When a group is associated with an Active Directory OU, the computers in the Active Directory OU are added to the Admin Portal group.
  - To remove an association with an Active Directory OU, click the **Unassign** button.
    - If an Active Directory OU contains subgroups, the computers in a subgroup will not be recognized and will not be added to the Admin Portal group.
    - Some devices may belong to two Admin Portal groups—a group *without* an Active Directory OU association and a group *with* an Active Directory OU association. The configuration assigned to the Admin Portal group with the Active Directory OU association is applied to the device.
- **Assign Devices**—Assign devices to a selected group. To assign devices to a group, select a group, open the **Select Action** menu, select **Assign Devices**, select devices to add to the group by placing a check next to each device to be added to the selected group, and click the **Assign Device** button at the top of the page to assign devices to the selected group.
- **Assign Configuration**—Assign a configuration to the selected group. To assign a configuration to a group, select a group, open the **Select Action** menu, select **Assign Configuration**, select a configuration, and click the **Assign** button to assign the configuration to the selected group.
- **Remove Configuration**—Remove a configuration from a selected group. To remove a group, select a group, open the **Select Action** menu, select **Remove Configuration**, and click **Remove** to confirm removal of the configuration from the selected group.

- **Create Group**—Create a new group under the selected group. The new group will become the child and the selected group will become the parent. Child groups inherit the configuration assigned to the parent group by default. The configuration of a child can be different than the one assigned to the parent. Use the Assign Configuration action to assign a configuration to a child group. To create group, select a group, open the **Select Action** menu, select **Create Group**, enter a name for the new group, and click the **Create** button to create the group.
- **Delete Group**—Delete a selected group. When this action is selected, a Confirm Delete Group(s) dialog box opens to confirm the deletion of the selected group and all child groups. The root group cannot be deleted.
- **Move Group**—Move a group. To move a group, select a group, open the **Select Action** menu, select **Move Group**, select a parent group, and click **Move** to confirm moving the selected group to the new parent group.

7.3.1.1.2 Move and Delete Devices

Devices can be moved from one group to another group. To move a device, select a device by placing a check in the box next to the device name, click  , select a group, and click **Move** in the Confirm Move dialogue box.

Devices can be deleted. To delete a device, select a device by placing a check in the box next to the device name, click  , and click the **Delete** button in the Confirm Device Deletion dialogue box.

7.3.1.1.3 Configure Group Properties

To assist in the configuration of hubs and clients that have the same settings, hubs and clients can be put into groups. Each device in a group inherits the settings from the group configuration.

7.3.1.1.3.1 Edit Hub Group Properties

Hub group properties can be edited by following these steps.

1. On the **Groups** page, click the **Hubs** tab.
2. Select a hub group by clicking the group name.
3. Select **Group Details** from the drop-down menu at the top.
4. On the group details page, click the **Edit Properties** button.
5. Modify the properties.
6. Click **Save Changes** to apply the modifications.

7.3.1.1.3.2 Override Hub Group Configuration

At times, a hub device in a hub group requires a different set of configurations than those inherited from the group. To override the group configuration for a device, follow these steps.

1. On the **Groups** page, click on the **Hubs** tab.

2. Select the hub group that contains the hub device by clicking the group name.
3. Click the device name to display the detail page.
4. Click the **Edit Device** button.
5. Modify the properties.
6. Click **Save Changes** to apply the modifications.

7.3.1.1.3.3 Hub Group Properties

The table in this section describes the hub group properties. Properties that have a dynamic value of **Yes** means the property value will be applied the next time the device connects to the server. A dynamic value of **No** means the property value will be applied the next time the device's Intel Unite® application is restarted.

Intel Unite® Solution Hub Properties

Property Name	Description	Dynamic	Value Type	Default Value
Available Displays	Numbers separated by commas, from 1 through x, where the administrator can specify which display is available to be used by Intel Unite® solution. The first number is the main display. Set the number of physical displays in which Intel Unite solution will be executed. Format: 1,2,3 or empty for all displays.	No	String	
Available Touch Display	Numbers separated by commas, from 1 through x, where the administrator can specify which displays are touch capable. The first number, 1, is the main display. A value of 0 indicates that no displays are capable and an empty value indicates that all displays are touch capable.	Yes	String	
Background Color	Color of the background palette number.	Yes	HEX	#0071C5
Background Image URL	The URL to the background image. It can be a local image.	Yes	String	
Background Instructions	The instructions displayed on the Intel Unite solution's display with the following reserved words: {PIN}—replace with PIN {n}—new line {rn}—new line	Yes	String	Refer to the table note.
Background Instructions Color	Color of the background instructions palette number.	Yes	HEX	#FFFFFF
Background Instructions Font	The font of the background instructions. Default font is Intel Clear.	Yes	String	
Background Instructions Title	Title to the background instructions. No reserved words.	Yes	String	Welcome
Disable Keyboard Command Keys	TRUE: Disables keyboard commands. FALSE: Enables keyboard commands.	Yes	Boolean	TRUE
Enable Hub as Presenter	TRUE: Enables the hub to be a presenter. FALSE: Disables the hub from being a presenter.	Yes	Boolean	FALSE

Property Name	Description	Dynamic	Value Type	Default Value
Enable hub check-in reporting	TRUE: Enables hub check-in reporting. FALSE: Disables hub check-in reporting.	Yes	Boolean	FALSE
Enable PIN Refresh During Session	TRUE: Enables the PIN to refresh during a session. FALSE: Disables the PIN from refreshing during a session.	Yes	Boolean	TRUE
Enable TLS 1.1	TRUE: Enables TLS 1.1. FALSE: Disables TLS 1.1.	Yes	Boolean	TRUE
Enable TLS 1.2	TRUE: Enables TLS 1.2. FALSE: Disables TLS 1.2.	Yes	Boolean	TRUE
Make Background Clock Visible	TRUE: Shows background clock. FALSE: Hides background clock.	Yes	Boolean	TRUE
Make Background Visible	TRUE: Shows background. FALSE: Hides background.	Yes	Boolean	TRUE
Make Content Toolbar Visible	TRUE: Shows content toolbar. FALSE: Hides content toolbar.	Yes	Boolean	TRUE
Make PIN Visible	TRUE: Shows PIN. FALSE: Hides PIN.	Yes	Boolean	TRUE
Moderator Mode	0—No Moderation (default) 1—Self-Promoted Moderation 2—Strict Moderation mode (only a person on the whitelist can be a moderator)	Yes	Integer	0
Network Port	The port that the hub is listening to for clients. Default 0—random.	No	Integer	0
PIN Color	Color of the PIN palette number.	Yes	HEX	#FFFFFF
PIN Size	Font size of the PIN with a range of x and y.	Yes	Integer	48
PIN Transparency	The opaqueness of the PIN with a range of 0 to 100 (default), where *0* is transparent and *100* is solid.	Yes	Integer	100
QoS Maximum Message Size	Maximum size in bytes of a message.	Yes	Integer	65535
QoS Message Queue Ratio	Message queue size.	Yes	Integer	4
Set password to close the app.	Close the hub application when this password is entered.	Yes	String	
Show Toggle Desktop Button	Shows a toggle button next to the hub PIN that allows access to the hub desktop while presenting. Requires that the **Make Background Visible** hub property be set to **FALSE**, otherwise the button will not be shown.	Yes	Boolean	FALSE
Stretch Background Image	TRUE: Stretches the background image. FALSE: Does not stretch the background image.	Yes	Boolean	TRUE
Visibility Time for Notification Messages	Time in seconds that the notification message is visible.	Yes	Integer	3

Table Notes: 1. Install Intel Unite® app{n}.2. Enter PIN {pin}{n}.3. Click Present.

Hub Features/Apps Properties

The tables in this section describe the properties of the hub features and hub apps.

File Sharing Module Properties

Property Name	Description	Dynamic	Value Type	Default Value
Allow Moderators to Receive Files	TRUE: Enables moderators to receive files. FALSE: Does not allow moderators to receive files.	Yes	Boolean	TRUE
Allow Moderators to Share Files	TRUE: Enables moderators to share files. FALSE: Does not allow moderators to share files.	Yes	Boolean	TRUE
Allow presenters to Receive Files	TRUE: Enables presenters to receive files. FALSE: Does not allow presenters to receive files.	Yes	Boolean	TRUE
Allow presenters to Share Files	TRUE: Enables presenters to share files. FALSE: Does not allow presenters to share files.	Yes	Boolean	TRUE
Allow viewers to Receive Files	TRUE: Enables viewers to receive files. FALSE: Does not allow viewers to receive files.	Yes	Boolean	TRUE
Allow viewers to Share Files	TRUE: Enables viewers to share files. FALSE: Does not allow viewers to share files.	Yes	Boolean	TRUE

Remote View Module (Hub) Properties

Property Name	Description	Dynamic	Value Type	Default Value
In-Room Experience Only	TRUE: Disables remote viewing. FALSE: Enables remote viewing.	Yes	Boolean	FALSE
JPEG Compression	Enables adjusting the compression ratio for non-AV content sharing.	Yes	Integer	85
Tile Size	Enables adjusting the tile size for non-AV content sharing.	Yes	Integer	128

Screen Sharing Module (Hub) Properties

Property Name	Description	Dynamic	Value Type	Default Value
Audio Video Streaming Support	TRUE: Enables AV presentation on the hub. FALSE: Disables AV presentation on the hub.	Yes	Boolean	TRUE
WebRTC UDP Ports Range	Sets the range of available ports. **Note:** Only use ports 1025-49151, as ports 0-1024 are reserved by the OS and 49152-65535 are for dynamic port use. The minimum and maximum values must be entered as numbers separated by a hyphen.	No	Range	0-0

7.3.1.1.3.4 Edit Client Group Properties

Client group properties can be edited by following these steps.

1. On the **Groups** page, click the **Client** tab.

2. Select a client group by clicking the group name.
3. Select **Group Details** from the drop-down menu at the top.
4. On the group details page, click the **Edit Properties** button.
5. Modify the properties.
6. Click **Save Changes** to apply the modifications.

7.3.1.1.3.5 Override Client Group Configuration

At times, a client device in a client group requires a different set of configurations than those inherited from the group. To override the group configuration for a device, follow these steps.

1. On the **Groups** page, click the **Client** tab.
2. Select the client group that contains the client device by clicking the group name.
3. Click the device name to display the detail page for that device.
4. On the device details page, click the **Edit Device** button.
5. Modify the properties.
6. Click **Save Changes** to apply the modifications.

7.3.1.1.3.6 Client Group Properties

The table describe the client group properties.

Intel Unite® Client Version Properties

Property Name	Description	Value Type	Default Value
Allow apps to open Download folder	TRUE: Enables apps to open the user's Download folder. FALSE: Disables apps from opening the user's Download folder.	Boolean	TRUE
Allow apps to save files	TRUE: Enables apps to save files. FALSE: Disables apps from saving files.	Boolean	TRUE
Allow host from your device	TRUE: Enables an Intel Unite client to host a peer-to-peer session. FALSE: Disables an Intel Unite client to host a peer-to-peer session.	Boolean	TRUE
Blocked file extensions	The extensions that the File Manager will filter out. Multiple extensions can be defined, each separated with a comma.	String	
Enable PIN refresh during hosted session	TRUE: Allow the PIN to change during a hosted session. FALSE: Prevent the changing of the PIN during a hosted session.	Boolean	TRUE
Enable TLS 1.1	TRUE: Enables TLS 1.1. FALSE: Disables TLS 1.1.	Boolean	TRUE
Enable TLS 1.2	TRUE: Enables TLS 1.2. FALSE: Disables TLS 1.2.	Boolean	TRUE
Host from your device listen port	The port used for the peer-to-peer feature.	Integer	0
Maximum file size	The maximum file size allowed in bytes.	Integer	214783648
QoS message Queue Ratio	Sets the number of messages to be dequeued from a particular queue before moving to processing messages in the next queue.	Integer	4

7.3.1.1.3.7 Client Features/Apps Properties

The tables in this section describe the properties of the client features and client apps.

Remote View Module (Client) Properties Table

Currently, no properties are available for this module.

Screen Sharing Module (Client) Properties

Property Name	Description	Value Type	Default Value
JPEG compression	Enables adjusting the compression ratio for non-AV content sharing.	Integer	85
Tile size	Enables adjusting the tile size for non-AV content sharing.	Integer	128

7.3.1.1.3.8 Client Plugin Moderation Mode

Some plugins /Apps can be configured to only show on moderator clients and be hidden for viewers and presenters in a moderated meeting. Only plugins that have **Disable plugin for non-moderators** module property set to **TRUE** can be hidden. The module property can be found in the Group Details of a configuration.

For non-moderated meetings, all participants will have access to plugins/Apps, even when the Disable plugin for non-moderators is set to TRUE for the plugins/Apps.

7.3.1.2 Configurations Page

On the Device Management menu, click **Configurations** to navigate to the Configurations page. The Configurations page lists the hub and client configurations. A *configuration* is the settings for a device. Each configuration consists of packages.

When a hub is paired or a client is registered, the assigned configuration determines how the device is configured, and what features and apps are loaded on the device.

The Configurations page displays a list of configurations. By default, the list displays hub configurations. To display a list of client configurations, click **Client Configurations**. To switch to a list of hub configurations, click **Hub Configurations**. Click the right-pointing chevron (›) icon to see a package's details. Click the down- pointing chevron (⌄) icon to hide a package's details.

Use the Search boxes at the top of the Configurations page to find configurations. Enter a string and click **Search** to display a list of configurations that have the string in its name. Use the **Clear** button to clear the search results.

7.3.1.2.1 Create Configuration

The following steps describe how to create a new configuration:

1. On the Configurations page, click **Create Configuration**. The Create Configuration view displays.
2. Replace **configuration name** with the name of the new configuration.
3. Select either **Hub** or **Client** next to the configuration name.
4. From the **Intel Unite® Software** drop-down menu, select a version.
5. To add a feature or an app, click the white plus sign with the blue background (⊕) associated with the feature or app under Available Features/Apps. Use the **Filter** field to find features and apps. Once feature or app is added, it's moved under Selected Features/Apps.
6. To remove a feature or an app, click the white minus symbol with the blue background (⊖) associated with the feature or app under Selected Features/Apps. After removing a feature or an app, the feature or

app moves under Available Features/Apps.

7. After adding the desired features and apps to the package, click the **Create Configuration** button.

Note: Clicking **Cancel** before clicking **Create Configuration** terminates the configuration creation process without saving the changes and returns to the Configurations page.

7.3.1.2.2 Edit Configuration

To edit a configuration:

1. On the Configurations page, click the **Edit** button associated with a configuration to bring up the Edit Configuration page. On this page, features and apps can be added or removed.
2. To change the name of the configuration, highlight the name in the **Edit Configuration** text box, and type the new name.
3. To select a new version, open the **Intel Unite® Software** menu by clicking the white down arrow with the blue background icon ( ), and then select the desired version.
4. To add a feature or an app, click the white plus symbol with the blue background ( ) associated with the feature or app under Available Features/Apps. After adding, the feature or app, it moves under Selected Features/Apps. Use the **Filter** field to help find features or apps.
5. To remove a feature or an apps, click the white minus symbol with the blue background ( ) associated with the feature or app under Selected Features/Apps. After removing, the feature or app moves under Available Features/Apps. Use the **Filter** field to help find features or apps.
6. Click the **Save Changes** button to save changes.

Note: Clicking **Cancel** before clicking **Save Changes** terminates the process without saving changes and returns to the Configurations page.

7.3.1.2.3 Delete Configuration

To delete a configuration:

1. On the Configurations page, identify the configuration to be deleted.
2. For the configuration to be deleted, click the **Delete** button ( ) to open the **Confirmation Delete Configuration** dialog box.
3. In the confirmation dialog box, click **Yes** to delete the configuration. Click **No** to cancel the deletion.

Note: Only configurations that are not in use can be deleted. When a configuration is not assigned to any group, it is not in use. If a configuration is in use, the **Delete** button ( ) is not available.

7.3.1.3 Features/Apps Page

To access the Features/Apps page, click **Features/Apps** on the Device Management menu. The Package Approval page shows the uploaded packages that have not been approved. The contents of the package will not be available for use in a configuration until the package is approved. After a package is approved, the contents are listed under either **Hub Features/Apps** or **Client Features/Apps**. Click the **Hub Features/Apps** tab to display a list of hub modules. Click the **Client Features/Apps** tab to display a list of client modules.

Features/App are modules that provide core functionality or enhanced capabilities for the hub and/or client. An example of a core functionality is the ability to view presentations remotely. An example of an enhanced capability is the ability to set a customized background. To create modules and packages, refer to the SDK documentation.

7.3.1.3.1 Upload a Package

Features and apps are distributed using packages in cab file format. These apps packages can be downloaded from Intel showcase website while feature packages are downloaded from the Intel Unite solution Admin Portal.

To upload a package, click the **Upload Package** button in the upper right corner. Browse to the location of the manifests or Apps directory. Select the cab file and click the **Open** button. A successful upload will be indicated by a green pop up box with the word **Success**.

7.3.1.3.2 Approve a Package

To approve a package on the **Features/Apps** page, click the **Approve** button associated with the package. Clicking the **Reject** button results in the package being unavailable.

7.3.1.3.3 View Hub Features/Apps

To view a list of hub apps and features on the Features/Apps page, click the **Hub Features/Apps** tab. On the Hub Features/Apps tab page, click the right-pointing chevron (›) icon to see a module's details. Click the down-pointing chevron (⌄) icon to hide a module's details.

To delete a hub module, click **Delete** (🗑). The Confirmation Delete Module dialog box opens. Click **Yes** to delete the module. Click **No** to cancel the deletion. Only modules not in use can be deleted.

7.3.1.3.4 View Client Features/Apps

To view client apps and features on the Features/Apps page, click the **Client Features/Apps** tab. To see a module's details, click the right-pointing chevron (›). To hide a module's details, click the down-pointing chevron (⌄).

To delete a client module, click **Delete** (🗑). The Confirmation Delete Module dialog box opens. Click **Yes** to delete the module. Click **No** to cancel the deletion. Only modules not in use can be deleted.

7.3.1.4 Reserved PINs Page

Selecting the Reserved PINs menu item on the Device Management menu opens the Reserved PIN page. On the Reserved PIN page, a list of hubs is displayed, and a static PIN can be assigned to a hub.

Use the Search boxes at the top of the **Hubs with Reserved PIN** and the **Hubs** section to find hubs. Enter a string and click **Search** to display a list of hubs that have the string in its device name. Use the **Clear** button to clear the search results.

7.3.1.4.1 Assign a Static PIN to a Hub

A static PIN can be assigned to a hub in two ways:

Method 1

To manually set each hub PIN:

1. Find the hub in the list that is to be assigned a static PIN and enter a six-digit number in the PIN field. The six-digit number can be randomly generated or defined specifically by the person entering the static PIN.

2. Click **Save**.

Method 2

Assign PINs to one or more hubs using a csv file:

1. Download the csv template by clicking the **Download Template** link in the upper-right corner of the page.
2. Fill in the csv template with the hub FQDN and PIN.
3. Save the csv file.
4. Click the **Import Reserved PINs** button at the top of the page.
5. In the Open dialog box, browse to the location of the csv file, select it and click **Open**.

7.3.1.4.2 Unassign a Static PIN for a Hub

A static PIN can be unassigned for a hub in two ways:

Method 1

To manually unassign each hub PIN, find the hub with the static PIN assigned in the list of hubs on the Reserved PIN page and click **Unreserve**.

Method 2

Unassign PINs to one or more hubs using a csv file.

1. Download the csv template by clicking the **Download Template** link in the upper-right corner of the page.
2. Fill in the csv template with the hub FQDN and set the value for PIN.
3. Save the csv file.
4. Click the **Import Reserved PINs** button at the top of the page.
5. In the Open dialog box, browse to the location of the csv file select the csv file, and click **Open**.

7.3.1.4.3 Use a Random PIN as a Static PIN

To assign a randomly generated PIN as a static PIN for a hub:

1. On the Reserved PIN page, find the hub in the list that is to be assigned the static PIN, and click the **Auto Generate** button.
2. Click **Save**.

7.3.1.5 Custom Metadata Page

The Metadata Page displays a list of user-defined metadata. The properties defined on this page become properties of all hub and client devices, allowing each device to be assigned a different value for each property.

Use the Search box at the top of the Custom Metadata page to find defined metadata properties. Enter a string and click **Search** to display a list of metadata properties that have the string in its name. Use the **Clear** button to clear the search results.

7.3.1.5.1 Create Metadata

To create metadata.

1. Click the **Add Item** button at the top of the page.

2. Enter a name for the metadata.
3. Click the **Save** button at the top of the page.

7.3.1.5.2 Delete Metadata

To delete metadata.

1. Place a check in the box next to the metadata to be deleted.
2. Click the **Delete** button at the top of the page.
3. Click **Delete** to confirm deletion.

7.3.1.5.3 Edit Metadata Value

To edit a metadata property.

1. Navigate to the Hubs and Clients page by selecting **Hubs and Clients** on the **Device Management** menu.
2. Click a device name to open the device details.
3. Click the **Edit Device** button at the top of the page.
4. Enter a string value into the text box for the metadata property.
5. Click **Save Changes** at the top of the page.

7.3.1.6 Provision Device Page

The Provision Device page displays a URL. This is the Admin Portal landing page. The URL can be used to pair hubs and register clients.

The URL contains two important pieces of information—the server URL and the OrgID. Both of these are needed to pair hubs and register clients, and they are determined during the server software installation. The OrgID is randomly generated. Both the server URL and the OrgID values can be found by browsing to **https://*<yourserverfqdn>*/intelunite/admin/landing**. The URL string is not case-sensitive.

7.3.1.7 Auto Pairing Management Page

The Auto Pairing Management page displays a list of auto pairing tokens and their time of expiration. From this page, tokens can be generated and deleted.

7.3.1.7.1 Generate Token

Enter the number of hours that the token will be valid into the **duration (hours)** text box in the upper-right corner. Click the **Generate Token** button. The **Generate Auto Pairing Token** window opens with instruction on how to use the token. Click the **Close** button to dismiss the window. The new token is added to the token list.

7.3.1.7.2 Delete Token

To delete a toke, place a check in the box next to the token. Click the **Delete Tokens** button in the upper-right corner. The **Confirm Delete Token** window opens, click the **Delete** button to delete the token or the **Cancel** button

to keep the token. More than one token can be deleted by placing a check in the boxes for all the tokens to be deleted prior to clicking the **Delete Tokens** button.

7.3.2 Device Management – Quick Actions

This section provides information about the Pair Hub, Auto Pairing, Upload Package, and Meeting Link Quick Actions located on the Device Management menu.

7.3.2.1 Pair Hub

The Pair Hub Quick Action is used during the hub setup procedures. A hub must be paired with the Admin Portal before it can be used. Refer to Section 5.4 for more information about hub pairing.

7.3.2.2 Auto Pairing

The Auto Pairing Quick Action enables the generation of a token that can be used to pair multiple hub devices and register multiple client devices. The next two sections describe the Auto Pairing processes.

7.3.2.2.1 Hub Pairing

To pair devices using the auto pairing token:

1. On the Device Management menu, click in the **duration (hours)** text box, and enter the number of hours the token will be valid.
2. Click the **Generate Token** button to display the Generate Auto Pairing Token dialog box, which contains the pairing token and instructions on how to use the token.
3. On the hub device, open a web browser, and browse to the URI **intelunite4://localhost/pair?otp=*<token>***, where ***<token>*** is the value from Step 2.
4. Click **Close** to close the Generate Auto Pairing Token dialog box.

7.3.2.2.2 Client Registration

To register client devices using the auto pair token:

1. On the Device Management menu, click in the **duration (hours)** text box, and enter the number of hours the token will be valid.
2. Click the **Generate Token** button to display the Generate Auto Pairing Token dialog box, which contains the pairing token and instructions on how to use the token.
3. On the client device, open a web browser, browse to the URI **intelunite4://localhost/pair?otp=*<token>*&email=*<email address>*&machineName=*<machinename>***, where ***<token>*** is the value from Step 2, ***<email address>*** is the email address that will receive the registration email, and ***<machinename>*** is the name of the client system.
4. Click the **Close** button to close the Generate Auto Pairing Token dialog box.

7.3.2.3 Upload Package

To use the Upload Package Quick Action:

1. On the Device Management menu, click the **Upload Package** button. An Open dialog box displays.
2. Use the Open dialog box to select the file to upload and click **Open**. The package file must be in .cab

format.

Once a package is uploaded, the package contents are not available. The package requires approval before the package contents can be used in a configuration.

7.3.2.4 Create Meeting

The Create Meeting Quick Access tool on the Device Management menu displays the Join dialog box. This tool creates a meeting URL for participants who are unable to install or use the existing Intel Unite solution's add-in for Microsoft* Office.

The meeting URL can be sent to users who will join a session using the Intel Unite solution. Recipients can join a meeting by using the Run command window (Windows*, Mac*, and iOS* clients) or a web browser (Windows*, Mac*, and iOS* clients).

7.3.2.4.1 Join a Meeting Using the Run Command Window (Windows*, Mac*, and iOS*)

To join a meeting using the Run command window on a Windows* device:

1. Copy the URL.
2. Open a Run command window or terminal window.
3. Paste the URL in the Run command text box or terminal window and press **Enter**.

7.3.2.4.2 Join a Meeting Using a Web Browser (Windows*, Mac*, and iOS*)

To join a meeting using a web browser on a Windows* or Mac* device:

1. Copy the URL.
2. Open a web browser.
3. Paste the URL in the address bar and press **Enter**.

7.4 Admin Portal – Server Management Menu

The Server Management menu includes the following menu items:

- Telemetry
- Logs
- Server Properties

7.4.1 Telemetry Page

The Telemetry page includes graphs showing telemetry information. The following information types are displayed as telemetry data:

- **Connections per Day (All Rooms)**—Connection events per day.
- **Seconds in Use per Day (All Rooms)**—Usage time per day.
- **Participant Count per Session**—The number of participants per session.
- **Participant Connected Duration (Seconds)**—Participant connection time per session.
- **CPU Information (Hub)**—CPUs running in hubs associated with the server and the count of each CPU.

- **OS Count (Hub)**—Operating systems running on the hubs associated with the server and the count of each operating system.
- **OS Count (Client)**—Operating systems running on the clients paired with the server and the count of each operating system.
- **Plugins Usage (Hub)**—Names of the apps used on hubs and the count of each app.
- **Plugin Usage (Client)**—Names of the apps used on clients and the count of each app.

  The range can be modified by changing the **Start Date** and/or the **End Date** fields. This range applies to all telemetry data.

7.4.1.1 Reset Data

At the top of the Telemetry page, click the **Reset** button to reset the telemetry data and clear the graphs.

7.4.1.2 Refresh Data

At the top of the Telemetry page, click the **Refresh** button to get the latest information and update the graphs.

7.4.1.3 Export Data

The telemetry data can be exported to a comma-separated formatted file (.csv). To export telemetry data, click the **Export** button at the top of the Telemetry page. The file is saved to the user's download directory.

7.4.2 Logs Page

The Logs page displays a list of logs. Each log entry includes the following information:

- **Device Name**—The fully qualified domain name of the device that generated the log entry.
- **Level**—The severity of the log entry. The following table describes the severity levels.
- **Source**—The originator of a log entry.
- **Timestamp**—The time a log entry was generated.
- **Message**—Information specific to the log entry.

The **Reset** button clears the logs.

Use the Search box at the top of the Logs page to find log entries. Enter a string and click **Search** to display a list of logs that have the string associated with the device name. Use the **Clear** button to clear the search results.

Log Severity Level

Log Severity Level	Severity Name	Description
1	Critical	Critical errors that cannot be recovered. This results in program crash, data loss, and so forth.
2	Error	Major error that is still recoverable.
3	Warning	Event that is handled but should still have some type of review for ongoing occurrences.
4	Info	Informational status.
5	Debug	Lower-level debug messages that can help diagnose an issue.
6	Trace	Lowest-level logging, may include all function enter/exit as well as internal states for various modules.

Change the Start Date and End Date to widen or narrow the list of logs generated between the two dates inclusive.

7.4.3 Server Properties Page

The Server Properties page displays a list of server properties, the organization name, and the organization description. The total number of properties is displayed in the lower-left corner. At the center bottom of the page are navigation controls to the different pages, forward arrow, and backward arrow.

To edit and change the server properties, organization name, or organization description, click the **Edit Properties** button. After a change is made, click **Save Changes** to apply the change. The following table describes the server properties.

Server Properties

Setting Name	Description	Value Type	Default Value
Admin Email	The administrator email address.	String	Blank
Admin Portal Path	The URL to the Admin Portal.	String	Blank
Black List	List of email addresses that are not allow to pair with the server. Email addresses are separated by commas. The wildcard character * matches any string. (Example: *@acme.com,@danger.com will prevent all email addresses from acme.com and danger.com from pairing.)	String	Blank
Configuration Cache Updates	TRUE: Allows configuration cache updates for device and groups. FALSE: Prevents configuration cache updates for device and groups.	Boolean	FALSE
Expired Auto Pairing Token Removal	The number of minutes past the expiration time before expired Auto Pairing Tokens are cleared.	Integer	1440
Expired Log Removal	The number of minutes past the expiration time before logs are cleared	Integer	1440
Expired Meeting Removal	The number of minutes past the expiration time before expired meetings are cleared.	Integer	1440
Expired Pairing Code Removal	The number of minutes past the expiration time before expired pairing codes are cleared.	Integer	1440
Expired PIN Removal	The number of minutes past the expiration time before expired PINs are cleared.	Integer	1440
Expired Telemetry Data Removal	The number of minutes past the expiration time before telemetry data is cleared.	Integer	1440
Inactive Hub Threshold	Maximum number of concurrent inactive devices before a warning email is sent to the email address specified by the Admin Email server property.	Integer	1
Inactive Notification Interval	Time interval in minutes for sending repeated inactive hub notification emails.	Integer	1440
Inactivity Duration	Maximum number of minutes since the last check-in before a hub is considered inactive.	Integer	60
Logs Retention Policy	Number of days logs are kept in the Admin Portal log collection.	Integer	30
Maintenance Service AD OU Cache Generation	Minutes between Active Directory cache refreshes.	Integer	5
Maintenance Service Interval	Time interval for maintenance services runs.	Integer	5

Setting Name	Description	Value Type	Default Value
Maintenance Service Language	Language used for Admin Portal email notifications. Options include: • ch—Chinese (Simplified) • ch—Chinese (Traditional) • de—German • en—English • es—Spanish • fr—French • it—Italian • jp—Japanese • ko—Korean • pt—Portuguese	String	en
Meeting Expiration	A meeting is set to expired when the number of minutes set here has elapsed.	Integer	5
Metrics Retention Policy	Number of days telemetry data is kept on the server.	Integer	365
OTA Updates Enabled	TRUE: Allows automatic updates of client and hub devices. FALSE: Client and hub devices require manual updates and all feature and apps (plugins) must be installed using installation msi on each device.	Boolean	TRUE
Pairing Mode	Enhanced Pairing Mode: Requires confirmation of client registration through user email. Standard Pairing Mode: Does not require confirmation of client registration through user email and does not require pairing of hubs. Require user email to enable moderator feature on user devices.	String	This value is set during server installation.
Password Reset HTML Message	Email text sent to an Admin Portal user with instructions on how to reset the password.	String	Here is your password reset link {0}. There you can create your new password.
PIN Expiration Time	Minutes between PIN refreshes.	Integer	5
Privacy Mode	**Collect locally and share anonymous data with Intel:** Telemetry data is collected and forwarded to Intel. **Collect locally and DO NOT share anonymous data with Intel:** Telemetry data is collected and stored on the Admin Portal, but not forwarded to Intel. **Do not collect:** No telemetry data is collected. **Prompt user to potentially share anonymous data with Intel:** Asks the user to opt-in or opt-out of telemetry data collection and the forwarding of the telemetry data to Intel.	String	This value is set after the first time log into the Admin Portal.

Setting Name	Description	Value Type	Default Value
Protected Role List	The Admin Portal user roles that cannot be edited or deleted.	String	Administrator, Device Pairing Manager, Moderator Manager, No Permissions
Support Link	Set the support website URL. If left blank, the user is directed to https://www.intel.com/support/uniteappsupport when the support link within the client Settings' page is clicked.	String	Blank
User Account Activation HTML Message	Email text sent to a new Admin Portal user with instructions on how to complete account activation.	String	Activation Link Activate your account
Verify Plugins	TRUE: Verifies feature and apps modules before loading. FALSE: Does not verify feature and apps modules before loading.	Boolean	TRUE
White List	Email addresses allowed to pair Intel Unite clients with the server. The wildcard '*' is allowed (for example, *domain.com). Can enter multiple values separated by a comma.	Array of Strings	*

In addition to the server properties, two buttons are available at the top the Server Properties page:

- **Test AD connection**—Click to verify Active Directory settings are correctly set in IIS. A success message displays when the settings are correct.
- **Clear AD user role cache**—Click to refresh the Active Directory user data immediately. When changes are made to Active Directory (such as adding a user to an AD group), the changes do not take effect immediately. The Active Directory data refresh time is based on the Maintenance Service AD OU Cache Generation server property.

7.5 Admin Portal – User Management Menu

The User Management menu includes the following pages:

- Users
- Moderators
- Roles

7.5.1 Users Page

The Admin Portal Users page displays a list of all Admin Portal users. The Admin Portal Users page enables administrators to add, edit, delete, and reassign user role, as describe in the next sections. Use the Search boxes at the top of the Admin Portal Users page to find users. Enter a string and click **Search** to display a list of users that have the string in its name. Use the **Clear** button to clear the search results.

7.5.1.1 Add a User

To add a new user:

1. On the Admin Portal Users page, click the **Add User** button. The Add User page opens.

2. Complete the following options on the Add User page:
   - **User Name**—The user's name. Intel recommends using only alphanumeric characters.
   - **Email Address**—The user's email address.
   - **Phone Number**—The user's phone number.
   - **Password**—The user's password. The password must have at least one number (0–9), at least one uppercase letter, at least one lowercase letter, at least one special character (such as !@#$%^&*._+), and at least eight characters.
   - **Select Role**—The user's role. The Local Admin Portal user can be assigned a role that is linked to an Active Directory user group. Linking an Active Directory user group to a role does not restrict which user can be assigned that role.
3. After filling in the user information, click **Save** to add the user.

Note: For Active Directory users, add the AD user to the appropriate AD group that has the desired permissions defined by the corresponding role created for that AD group. See Section 7.5.3.1 for details about creating a role for an AD group. AD users are not added to the Admin Portal and are managed through Active Directory.

7.5.1.2 Edit User Properties

Existing user properties can be edited on the User Details page. To edit a user's details:

1. On the Admin Portal Users page, click the **Edit** button, or click a name. The User Details page for the user displays. The right side of the User Details page displays the current role assigned to the user and the permissions associated with the role.
2. Change any of the following properties on the **User Details** page:
   - **Email**—To change the email address, highlight the email address, and type another email address.
   - **Phone Number**—To change the phone number, highlight the phone number, and type another phone number.
   - **Role**—To set a new role for the user, click the white down arrow with blue background icon ( ) to display a list of roles available. Select a role on the list and click **Save**.
   - **User Account Status**—If the status is set to Disabled, the account is not active. To disable the account, place a check in the Disabled box. To enable the account, clear the check from the Disabled box.
   - **Delete User**—Opens the delete user confirmation box. Click **Yes** to delete or click **No** to cancel the deletion. Users can also be deleted from the Admin Portal Users page, as described in the next section.
3. Click **Save**.

7.5.1.3 User Actions

Administrators can use the Admin Portal Users page to delete users and assign users to different roles:

- **Delete User**—Place a check in the box next to the user name. On the Select Action menu at the top of the page, click **Delete**. A confirmation dialog box opens. Click **Yes** to delete the user or click **No** to close the confirmation dialog box without deleting the user.
- **Assign Different Role**—Place a check in the box next to the user name. On the Select Action menu at the top of the page, select **Assign Different Role**. The Select Role dialog box opens. Choose the new role and click **Assign**.

7.5.2 Moderators Page

The Moderators page displays a list of users who have moderator privileges. This page enables administrators to add, manage, and delete moderators.

Administrators manage the list of the moderators through the Admin Portal. Moderators are authenticated using a key associated with their email address.

For environments where Standard Pairing Mode is enabled, when a user is promoted to moderator, the Admin Portal sends an email that contains a URL to the moderator's email address. The moderator opens the email on the client that is used to connect to a moderated session. The moderator clicks the link in the email to install a token on the client, allowing the moderator to use the client to moderate session using the Intel Unite solution. If a moderator has multiple client devices and wants to moderate sessions using the devices, the moderator token must be installed on all the client devices.

For environments where Enhanced Pairing Mode is enabled, moderator tokens are not used.

To send registration emails to moderators, IT needs to configure an SMTP relay. Refer to Section 4.4.3 for more details on SMTP setup.

Use the Search boxes at the top of the page to find users that have moderator privilege. Enter a string and click **Search** to display a list of users who have the string in its name. Use the **Clear** button to clear the search results.

7.5.2.1 Add a Moderator

On the Moderators page, moderators can be added in two ways—individually or as a group:

- **Add a moderator individually**—Click **Add Moderator**, enter the moderator's name and email address, and click **Save**.
- **Import moderators as a group**—Click **Import Moderators**, select the CSV file that contains the list of moderators, and click **Open**.

7.5.2.2 Delete a Moderator

On the Moderators page, place a check in the box next to the user name, and select **Delete**. A confirmation dialog box opens. Click **Yes** to delete the user. Click **No** to close the confirmation dialog box without deleting the moderator.

7.5.2.3 Send Token

For environments that enables Standard Pairing Mode, in order for user to be recognized as a moderator in a moderated session, the device the user uses to join the session must have a moderator token installed.

To install a moderator token on a device.

1. Place a check in the box next to the user to send the moderator token.
2. Click **Send Token** to send an email to the user with an URL that installs the moderator token.
3. On the user's device, install the Intel Unite® client software.
4. On the user's device, open the email, and click the link. The link will launch the Intel Unite client to install

the moderator token on the device.

7.5.2.4 Moderated Sessions

For a session to be moderated, the moderator functionality mode needs to be set in the hub group or hub device configuration. Refer to Section 7.3.1.1.3.3 for more information about group properties. Moderator modes are:

- **0-No Moderation**—Default mode. No moderators are in the meeting/session and all participants have equal rights to view and present.
- **1-Self Promote**—The meeting/session is not moderated until someone promotes themselves to be the moderator. The moderator designates who presents during the session and have the ability to promote other participants to be moderators. **Note:** Becoming a moderator during the meeting does not result in the user being added to the moderator whitelist.
- **2-Strict**—The meeting/session is moderated only by the users that are on the moderator whitelist. When the moderator joins the session, they are automatically promoted to the moderator role. A participant can request to become a moderator, which results in an e-mail to the administrator, who can add the participant to the moderator whitelist from the Admin Portal.

7.5.2.4.1 Enhanced Moderation

Enhanced Moderation is a feature that provides the ability for session moderators to preview a participant's screen and invite them to start presenting. To use Enhanced Moderation, the following properties must be configured

Hub properties:

- Moderator Mode must be set to **2** (strict moderation).
- Screen Preview must be set to **1** (strict moderation).

Client properties:

- Enable Client Screen Preview must be set to **True**.
  Note: This setting will apply to all devices in the group, but it can be overridden per device if required.

7.5.3 Roles Page

Clicking **Roles** on the User Management menu opens the All Roles Page. The All Roles page displays a list of roles and the number of users who are assigned to each role. By default, five roles are listed—Admin, Pairing, Role Management, User Management, and Device Management. Each built-in role has a specific set of permissions. Permissions are allowed actions/access to the Admin Portal.

To show permissions for a role, click the right-pointing chevron (›). Click the down-pointing chevron (⌄) to hide the permissions. The following table shows the built-in permissions for each role. Write permissions have all the permissions of read with additional capabilities. The subsequent tables show the allowed actions and access for the defined permissions.

Built-In Roles Permissions

Role	Device Management Permission	Device Pairing Management Permission	Role Management Permission	User Management Permission	Server Management Permission	Moderator Management Permission
Administrator	Read and Write	Read and Write	Read and Write	Read and Write	Read and Write	Read and Write
Device Pairing Manager		Read and Write				
Moderator Manager						Read and Write

Device Management Permissions

Admin Portal Feature	Read (View Devices, Groups, Features/ Apps, Configs, Device Properties)	Write (Read and Edit/Delete These Items, Upload Packages)
Login	x	x
Devices	• Search OUs (AD) • Get all child OUs from a parent OU (AD) • Test AD connection • Get all configuration and device details • Get details about a selected configuration or device	• Flush AD cache • Get AD domains • Delete a configuration • Assign modules to configuration • Create configurations and assign modules • Enable/disable device • Delete device • Get properties of device • Get configuration assigned to chosen device
Configs, Features/ Apps, Packages	• Get Features/Apps list • Delete Features/Apps	• Install package • Get unapproved Features/Apps • Approve Features/Apps • Delete unapproved Features/Apps
Reserved PINs	Get devices with reserved PIN	• PIN reservation • Bulk PIN reservation • Get random free device PIN • Unreserve pin
Pair Hub		
Auto Pair		
Telemetry		
Logs		
Server Properties		
Users		
Moderators		
Roles		

Admin Portal Feature	Read (View Devices, Groups, Features/ Apps, Configs, Device Properties)	Write (Read and Edit/Delete These Items, Upload Packages)
Device Tree	• Get device tree • Get devices of each tree group • Get properties of each tree group	• Create a tree group • Update a tree group • Move a tree group • Bulk tree group deletion • Assign devices to a tree group • Assign configuration to a tree group • Remove configuration from a tree group • Overwrite properties for a child tree group

Device Pairing Management Permissions

Admin Portal Feature	Read (Only Login Rights)	Write (Pair Hub, Create/Manage Auto Pairing Tokens)
Login	x	x
Devices		
Configs, Features/ Apps, Packages		
Reserved PINs		
Pair Hub		Approve hub for pairing
Auto Pair		Create otp tokens
Telemetry		
Logs		
Server Properties		
Users		
Moderators		
Roles		
Device Tree		

Role Management Permissions

Admin Portal Feature	Read (View Roles and Permissions)	Write (Create/Manage Roles)
Login	x	x
Devices		
Configs, Features/ Apps, Packages		
Reserved PINs		
Pair Hub		
Auto Pair		
Telemetry		
Logs		
Server Properties		
Users		
Moderators		

Admin Portal Feature	Read (View Roles and Permissions)	Write (Create/Manage Roles)
Roles	• Get role list • Get details of role • Get permission list	• Create role • Update role • Delete role • Bulk role deletion
Device Tree		

User Management Permissions

Admin Portal Feature	Read (View Users)	Write (Create/Manage Users)
Login	x	x
Devices		
Configs, Features/ Apps, Packages		
Reserved PINs		
Pair Hub		
Auto Pair		
Telemetry		
Logs		
Server Properties		
Users	• Get a list of users • Get details of user	• Register user • Update user • Delete user • Bulk user deletion • Bulk assigning of role to users • Change user password
Moderators		
Roles		
Device Tree		

Server Management Permissions

Admin Portal Feature	Read (View Logs, Telemetry, and Server Properties)	Write (Edit Server Properties)
Login	x	x
Devices		
Configs, Features/Apps, Packages		
Reserved PINs		
Pair Hub		
Auto Pair		
Telemetry	• Get metrics reports • Export metrics	
Logs	Get logs	
Server Properties	Get server property list	Update server properties

Admin Portal Feature	Read (View Logs, Telemetry, and Server Properties)	Write (Edit Server Properties)
Users		
Moderators		
Roles		
Device Tree		

Moderator Management Permissions

Admin Portal Feature	Read (View Moderators)	Write (Create/Manage Moderators)
Login	x	x
Devices		
Configs, Features/Apps, Packages		
Reserved PINs		
Pair Hub		
Auto Pair		
Telemetry		
Logs		
Server Properties		
Users		
Moderators	Get list of moderators and details	• Create and delete moderators • Import from CSV
Roles		
Device Tree		

7.5.3.1 Create a New Role

When creating a new role, the following are defined:

- **Role Name**—The name of the new role.
- **Active Directory Group**—Links the role to an Active Directory user group. If an Active Directory group contains subgroups, the users in the subgroups are not recognized by the Admin Portal.
- **Permissions**—Permissions applied to a new role. Multiple or all permissions can be applied.

The following steps describe how to create a new role:

1. On the Roles page, click the **Create New Role** button.
2. Replace the Role Name with the name of the new role.
3. If creating a new role for an AD user group, click the **Assign** button next to the Active Directory Group text box. To find the AD user group, use the **Search Active Directory** dialog box by entering the full name or partial name of the AD group in the **Enter AD group search strings** text box and clicking **Search**. Pick the AD group from the groups found list.
4. Add and remove permissions as needed:
   - **Add permissions**—Click the white plus sign with blue background (⊕) associated with the permission under Available Permissions. After adding, the permission is displayed under Applied Permissions. To add all available permissions, click the blue plus sign with the white background (⊕) next to Available Permissions. Use the **Filter** field to help find permissions.

- **Remove permissions**—Click the white minus sign with blue background ( ) associated with the permission under Applied Permissions. After removing, the permission is displayed under Available Permissions. To remove all available permissions, click the blue minus sign with the white background ( ) next to Applied Permissions. Use the **Filter** field to help find permissions.

5. After adding the desired permissions, click **Create New Role**. The newly created role is listed under All Roles on the Roles page.

Multiple roles can be created that are linked to the same Active Directory user group and have different permissions. Users who are members of the Active Directory user group have a union of all the permissions from all roles linked to the Active Directory user group.

8 Maintenance Service

The Maintenance service is a Windows service responsible for supporting, cleaning, and maintaining the server information (database). This section explains the functions and how to configure the various features of the maintenance service responsible for cleaning expired data from pairing codes, PINs, OTP tokens, meetings, telemetry, and logging, as well as updating device OUs and monitoring hub device health.

8.1 Clean Expired Pairing Codes

This service is used to clean all rows in the pairing code table with an expired date/time. It has 1 property to configure; `Expired Paring Code Removal`, which sets the interval at which the Clean Expired Pairing Codes service is executed. To set up the Clean Expired Pairing Codes service, follow the steps below:

1. Log in to the admin portal.
2. Click **Server Management** from the navigation bar at the top of the screen and select **Server Properties**.
3. Click **Edit Properties**.
4. Enter a value (in minutes) for the `Expired Paring Code Removal` property; the default value is 1440.
5. Click **Save Changes**.

8.2 Clean Expired PINs

This service is used to clean all expired device PINs. It has 2 properties to configure; `Expired PIN Removal` sets the interval (in minutes) at which the Clean Expired PINs service is executed, and `Pin Expiration Time` sets the time (in minutes) before a PIN is considered expired.

To set up the Clean Expired PINs service, follow the steps below:

1. Log in to the admin portal.
2. Click **Server Management** from the navigation bar at the top of the screen and select **Server Properties**.
3. Click **Edit Properties**.
4. Enter a value (in minutes) for the `Expired PIN Removal` property; the default value is 5.
5. Enter a value for the `Pin Expiration Time` property; there is no default value.
6. Click **Save Changes**.

8.3 Clean Expired OTP Tokens

This service is used to clean all expired rows in the OTP token table with an expired date/time. It has 2 properties to configure; `Expired PIN Removal` sets the interval (in minutes) at which the Clean Expired OTP Tokens service is executed, and `Pin Expiration Time` sets the time (in minutes) before an OTP is considered expired.

To set up the Clean Expired OTP Tokens service, follow the steps below:

1. Log in to the admin portal.
2. Click **Server Management** from the navigation bar at the top of the screen and select **Server Properties**.
3. Click **Edit Properties**.
4. Enter a value (in minutes) for the `Expired Auto Paring Token Removal` property; the default value is 1440.
5. Click **Save Changes**.

8.4 Clean Expired Meetings

The Clean Expired Meetings service is used to clean all rows in meeting and meeting device tables with an expired date/time. It has 2 properties to configure; `Expire Meeting Removal Token Removal` sets the interval (in minutes) at which the

Clean Expired Meetings service is executed, and `Meeting Expiration` sets the time (in days) before a meeting is considered expired.

To set up the Clean Expired Meetings service, follow the steps below:

1. Log in to the admin portal.
2. Click **Server Management** from the navigation bar at the top of the screen and select **Server Properties**.
3. Click **Edit Properties**.
4. Enter a value (in minutes) for the `Expired Meeting Removal Token Removal` property; the default value is 1440.
5. Enter a value (in days) for the `Meeting Expiration` property; the default value is 1.
6. Click **Save Changes**.

8.5 Clean Telemetry Data

The Clean Telemetry Data service is used to clean all rows in device metadata and device event tables already uploaded to telemetry. It has 2 properties to configure; `Expired Telemetry Data Removal` sets the interval (in minutes) at which the Clean Telemetry Data service is executed, and `Metrics Retention Policy` sets the time (in days) to retain the data.

To set up the Clean Expired Meetings service, follow the steps below:

1. Log in to the admin portal.
2. Click **Server Management** from the navigation bar at the top of the screen and select **Server Properties**.
3. Click **Edit Properties**.
4. Enter a value (in minutes) for the `Expired Telemetry Data Removal` property; the default value is 1440.
5. Enter a value (in days) for the `Metrics Retention Policy` property; the default value is 365.
6. Click **Save Changes**.

8.6 Clean Logging Data

The Clean Logging Data service is used to clean all rows in the logging table already with expired data uploaded to telemetry. It has 2 properties to configure; `Expired Log Removal` sets the interval (in minutes) at which the Clean Logging Data service is executed, and `Logs Retention Policy` sets the time (in days) to retain the data.

To set up the Clean Expired Meetings service, follow the steps below:

1. Log in to the admin portal.
2. Click **Server Management** from the navigation bar at the top of the screen and select **Server Properties**.
3. Click **Edit Properties**.
4. Enter a value (in minutes) for the `Expired Log Removal` property; the default value is 1440.
5. Enter a value (in days) for the `Logs Retention Policy` property; the default value is 30.
6. Click **Save Changes**.

8.7 Update Device OU

The Update Device OU service is used to update the device table. It has 1 properties to configure; `Maintenance Service AD OU Cache Generation` sets the interval at which the Update Device OU service is executed. In addition to this property, configuring the Update Device OU service requires changes to the following Active Directory properties in the configuration file:

- `ActiveDirectoryServer`
- `ActiveDirectoryGlobalCatalog`
- `ActiveDirectoryServerUsername`
- `ActiveDirectoryServerPassword`
- `ActiveDirectoryServerUseSSL`

To set up the Update Device OU service, follow the steps below:

1. Log in to the admin portal.
2. Click **Server Management** from the navigation bar at the top of the screen and select **Server Properties**.
3. Click **Edit Properties**.
4. Enter a value (in minutes) for the `Maintenance Service AD OU Cache Generation` property; the default value is 1440.
5. Click **Save Changes**.
6. Go to the server where the Maintenance Service is running.
7. Using Task Manager, right-click "Intel Unite Maintenance Service" and select **Properties**.
8. Copy the path to the executable.
9. Open the `Intel.Unite.Server.Maintenance.exe` file in notepad and set the following properties:
   - ActiveDirectoryServer
   - ActiveDirectoryGlobalCatalog
   - ActiveDirectoryServerUsername
   - ActiveDirectoryServerPassword
   - ActiveDirectoryServerUseSSL

   For example:

```
<add key="ActiveDirectoryServer" value="1440"/> <!-- In Minutes -->
<add key="ActiveDirectoryGlobalCatalog" value=""/>
<add key="ActiveDirectoryServerUsername" value=""/>
<add key="ActiveDirectoryServerPassword" value=""/>
<add key="ActiveDirectoryServerUseSSL" value=""/>
<add key="ActiveDirectoryServerGroupsCacheLifespan" value="1"/>
<add key="ActiveDirectoryServerUnitInterval" value="5"/>
```

8.8 Health Monitor Service

The Health Monitor service is used to monitoring if a set of hub devices chosen by a flag enable reporting are inactive and send alerts to the list of admins in the admin portal. It has 3 properties to configure; `Maintenance Service Interval` sets the interval at which the Health Monitor service is executed, `Inactive Hub Threshold` sets minimum number of inactive devices before a Health monitoring report is sent to all admins, and `Inactive Duration` sets the length of time before a hub device is considered inactive.

The Health Monitor service scans the hubs and clients database where all the devices (Hubs mostly) are stored and checks all the devices that have a configuration core property Enable Reporting in true. Once all the clients that have the core property have been identified, the Health Monitor service checks the timestamp field and gets all the devices for which the difference in minutes between the actual time and last update is bigger than the “Inactive Duration” key set in the Server Properties section of the admin portal.

After the Health Monitor service gets the number of devices that meet these criteria it compares that number against the “Inactive Hub Threshold” key. If the number of devices that exceed the “Inactive Duration” is bigger than the number of devices set in the “Inactive Hub Threshold” and email will be sent to all the users register in the Admin Portal that have the Admin Role. More emails could be send out if in the next check the health monitor finds that the number of inactive devices is more than here were in the previous scan.

To set up the Clean Expired Meetings service, follow the steps below:

1. Log in to the admin portal.
2. Click **Server Management** from the navigation bar at the top of the screen and select **Server Properties**.
3. Click **Edit Properties** and find the `Maintenance Service AD OU Cache Generation` property.
4. Enter a value (in minutes) for the `Maintenance Service Interval`; the default value is 1440.
5. Enter a value (in number of inactive devices) for the `Inactive Hub Threshold` property; the default value is 1.
6. Enter a value (in minutes) for the `Inactive Duration`; the default value is 60.

7. Click **Save Changes**.
8. Go to the server where the Maintenance Service is running.
9. Using Task Manager, right-click "Intel Unite Maintenance Service" and select **Properties**.
10. Copy the path to the executable.
11. Open the `Intel.Unite.Server.Maintenance.exe` file in notepad and set the following properties:
    - `SMTP FROM`
    - `SMTP HOST`
    - `PORT`
    - `USERNAME`
    - `PASSWRORD`

    For example:

```
<mailSettings>
<smtp from="noreply@intel.com">
<network host="smtp.intel.com" port="25" userName="noreply@intel.com" password="pass"/>
</smtp?
</mailSettings>
```

12. Return to the admin portal.
13. Click **User Management** from the navigation bar at the top of the screen and select **Users**.
14. Find the email address of the account that should become the admin and click the edit icon ( ) next to it.
15. Set the Role of that user to "Admin", then click **Save**.
16. Click **Device Management** from the navigation bar at the top of the screen, then click **Hubs and Clients**.
17. Click the hub or client you want to track, then click **Edit Device**.
18. Set Enable hub check-in reporting to **True**, then click **Save Changes**.

8.9 Alerts and Monitoring

The Admin Portal can be configured to notify the IT administrator when a certain number of hubs becomes non-responsive. The following server properties allow an IT administrator to customize the alert behavior:

- **Admin Email**—The email address where alert messages are sent.
- **Maintenance Service Interval**—The number of minutes between maintenance service events, which include checking for inactive devices.
- **Inactive Hub Threshold**—The number of concurrent inactive hubs before an email is sent to the admin email address.
- **Inactive Notification Interval**—Time interval for sending repeated inactive hub notification emails.
- **Inactivity Duration**—The number of minutes since the last check-in from a hub before it is considered inactive.

9 Security Controls

9.1 Minimum Security Standards (MSS)

Intel recommends that all devices running the Intel Unite application meet the default organization MSS standards, have an agent installed for patching, and have an antivirus/IPS/IDS and other necessary controls as per the MSS specification (McAfee* suite for Anti Malware, IPS, and IDS were tested for compatibility).

9.2 Machine Hardening

Machine Unified Extensible Firmware Interface (UEFI) could be locked to boot the Windows* boot loader only (ensuring that starting from a USB or 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.

For Windows* OS hardening, as a baseline, the system runs with non-elevated user rights. Intel also recommends removing unused software from the OS, including unnecessary preinstalled software and Windows* components (PowerShell, Print and Document services, Windows* location provider, XPS services, and so forth). Apply group policies that are reminiscent of kiosks or digital signage.

Regarding GUI subsystem lock, for systems that use non-touch screens without a keyboard or mouse, breaking out of the GUI subsystem is harder. To prevent an attacker from attacking using an HID device (USB keyboard/mouse), Intel recommends to programmatically block using **Alt + Tab, Ctrl + Shift + Esc,** and the **Charms** bar.

9.3 Other Security Controls

Intel recommends locking 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.

Each machine is recommended to have an identified owner. If a machine goes offline for an extended period, the identified owner is notified.

Beyond the security mechanisms provided by the Intel® vPro™ platform and the Intel Unite® software, Intel recommends to harden the Microsoft* Windows* OS per Microsoft's guidelines for machine hardening. For reference, consult the Microsoft Security Compliance Manager* (SCM) (includes a wizard-based hardening tool, including hardening best known methods (BKMs) and relevant documentation).

10 Maintenance

Each organization and the IT administrators determine a regular maintenance program. In addition, the following maintenance tasks are recommended:

- **Nightly Reboot**—Reboot the hubs on a daily base (preferably at night). Prior to reboot, run maintenance tasks, such as wiping cached temp files and initiating the standard patching procedure.
- **Patching Strategy**—If available, run the standard patching mechanism in an unattended mode (no GUI prompts), preferably before the nightly reboot.
- **Reporting**—Logs are captured and can be accessed on the Admin Portal under on the System Management tab.
- **Backend Monitoring**—Use standard virtual server monitoring tools to generate and send alerts to second-level support.

Appendix A. Provisioning Guide for Google Admin*

Enforce Automatic Intel Unite Application Install

The following steps describe how to configure the enforcement of automatic Intel Unite application installation.

1. Open a browser and navigate to https://admin.google.com and login to the Google Admin Console.
2. From the menu in the upper left hand corner of the Admin dashboard, choose Devices > Chrome Management from the slide out menu.
3. Scroll down and click App Management.
4. Click on the three dots Settings menu just below the header bar in the upper right corner.
5. Choose Add Custom App.
6. Enter the ID and URL of the Intel Unite app for Chrome*. These values are currently:
   - cphbmldgllfddfdnjgfclcpckpbcliai
   - https://chrome.google.com/webstore/detail/intel-unite%C2%AE/cphbmldgllfddfdnjgfclcpckpbcliai

   Note: Intel Unite application is hidden on desktop browsers due to Google's new policies regarding Chrome Browser no longer supporting Chrome Applications. You can still access the store page with the link above.
7. You will be sent to the management settings for the app. Click on User Settings and then your Org from the list of options.
8. Toggle Force Installation to Enabled.
9. Click Save when you are finished.

In order for Chromebooks to use these Settings, it may have to be Powerwashed. If your fleet are not joined to your Enterprise Account, then a Powerwash may be necessary (except for brand new OOB systems). Otherwise if your fleet is already joined, there is no need to Powerwash. The first User Account used on the device must be a User from your Organization's User Directory. These Users can be found by clicking the menu button » Directory » Users.

Google Admin* Setup for Client Configuration

The following steps describe how to configure the Intel Unite® software using Google Admin* when Intel Unite® clients are under domain management.

1. Open a browser and navigate to https://admin.google.com and login to the Google Admin Console.

2. From Google Admin, click Device Management.
3. Click Chrome Management.
4. Click App Management.
5. Select the Intel Unite® software icon.
6. Select User Settings.
7. Select the organization from the Orgs list.
8. Make desired configuration changes, or to upload a configuration file, click Upload Configuration File.
9. The configuration file is in JSON* format. An example of what is in a configuration file is shown below:

```
{

"managedEnterpriseServer": {"Value" : "unite.parthenonsoftware.com"},

"managedEnableWebrtc": {"Value" : true},

"managedLandingUrl": {"Value": "intelunite4://localhost/register?serverUrl=https://unite4.
parthenonsoftware.com/intelunite/api&orgId=7A810B3F-0608-4A1C-BF42-C06A338EF877" },

"managedPairingUrl": {"Value": "intelunite4://localhost/
pair?otp=<token>&email=<email>&machineName=<name>" },

"managedOrganizationSecret": {"Value": "thisisyourpassword"}

}
```

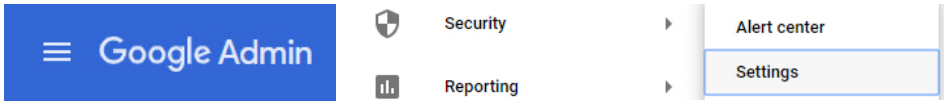
10. The following settings can be set using the configuration file:
    - **managedEnterpriseServer** – A text field labeled Enterprise Server. If set to anything other than blank, it is used as the server for the Intel Unite® solution for the app, and it overrides and disables the Enterprise Server field in the settings.
    - **managedEnableWebrtc** – A Boolean toggle labeled Enable WebRTC. If set to true, the app uses WebRTC (if available on the hub) rather than RFT.
    - **managedLandingUrl** – If set, this is used as the server for the Intel Unite® solution and organization ID for the associated Chromebooks*, overriding the local settings. The URL format is as follows: intelunite4://localhost/register?serverUrl=<url>&orgId=<guid>
    - **managedPairingUrl**— This sets up the Email Address, Machine Name and Pairing Token for the associated Chromebooks, overriding the local settings.
      Note: If not set, the email address will not populate in the app; ensure that the managedPairingUrl is properly set in the configuration file.
      The URL format is as follows: intelunite4://localhost/pair?otp=<OTP_GUID>&email=<EMAIL>&machineName=<NAME>, where the <EMAIL> and <NAME> will be filled in automatically, while the <OTP_GUID> is the token created on the admin portal for the Intel Unite solution. Below are the steps for obtaining the <OTP_GUID>:
      i. Open a browser, either Google Chrome or Microsoft Internet Explorer, and navigate to the Intel Unite® solution admin portal.
      ii. Enter the user name and password to log in.
      iii. Select **Auto Pairing Management** from the **Device Management** menu to display a list of OTP GUIDs.
    - **managedOrganizationSecret** — A string value that acts as a unique password that encrypts each client app data stored inside Google's Sync storage. Any string value will work and there are no requirements for length or complexity.

11. Click Save.

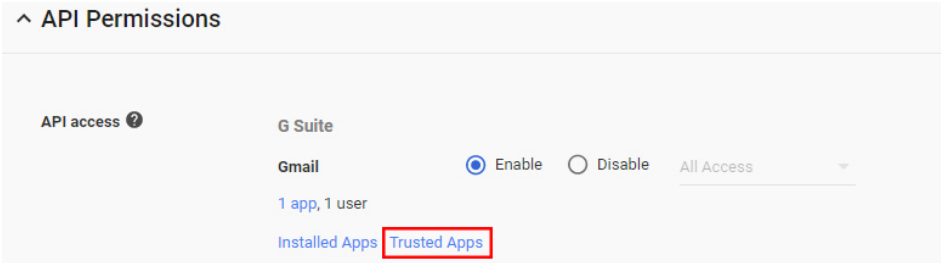
Grant Intel Unite Solution Trusted User Information Access

Intel Unite application queries the User's Google Plus Account for their Email, Name, and Avatar with no User input required, if the app has been whitelisted in your organizations Google Admin account. The following steps describe how to configure the granting of Intel Unite application trusted user information access.

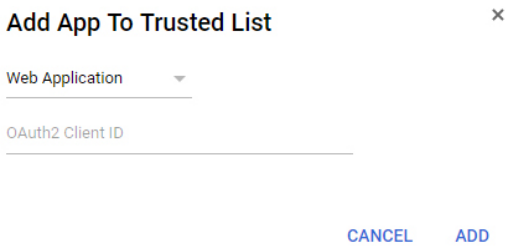
1. Open a browser, navigate to https://admin.google.com, and login to the Google Admin Console.
2. From the menu in the upper-left corner of the admin dashboard, choose **Security > Settings**.



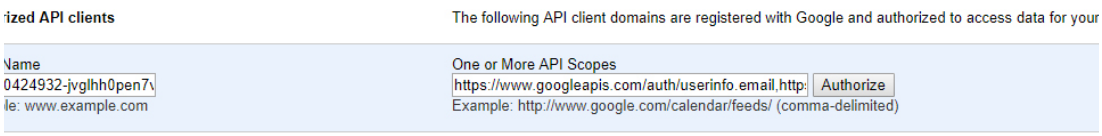
3. Scroll to the bottom of the Security page and click **API Permissions**.
4. Under the API Access subsection you will see a list of Apps. Scroll to the bottom of this list where you will see two links: "Installed Apps" and "Trusted Apps". Click **Trusted Apps**.



5. Click the yellow "**+**" button (+) in the lower right of this page, which will open the Add App To Trusted List dialog.



6. From the drop-down menu, select **Web Application**. Since the Chrome App uses a Google API key, it is treated as any other website.
7. Paste the OAuth2 "client_id" into the OAuth2 Client ID input; this value is as follows:
   `401030424932-jvglhh0pen7vdjd96vr5g2g2dnknfpf6.apps.googleusercontent.com`
8. Click **Security** in the upper-left corner of the browser to navigate back to the security settings page.
9. Click **Advanced Settings**, then click **Manage API client access**.
   Paste the OAuth2 ID from above into the "Client Name" field
10. Paste the following string into the "One or More API Scopes" field:
    `https://www.googleapis.com/auth/userinfo.email,https://www.googleapis.com/auth/userinfo.profile`



11. Click the **Authorize** button.

The Intel Unite app will query googleapis to retrieve each user's Google Plus profile and receive a unique Email Address, Name, and Profile Image. These will be used to replace the generate values in the Pairing URL and to configure the User's Email, Name, Initials and Avatar Image automatically, without user input.

Self-Signed Pin Server Certificate Support

The following steps describe how to configure the PIN server for Intel Unite Solution to use self-signed certificates.

1. Using a browser, make a copy of the pin server self-signed certificate.
   - In Chrome click on the Secure lock icon that appears next to https URLs. Click Certificate and then choose the Details tab and click the Export button on the lower right.
   - In Firefox click the lock icon next to https URLs. Click the ">" button to the right of the Secure Connection area of the menu. Click More Information. Click the View Certificate button and then switch to the Details tab of the popup window. Click Export to save a copy of the certificate.
2. Open a browser and navigate to https://admin.google.com and login to the Google Admin Console.
3. From the Google Admin Menu in the upper right of the dashboard, choose Device Management > Networks.
4. From the Networks page, choose Certificates.
5. Click Add Certificate and choose the certificate saved in Step 1.

Appendix B. Error Codes

Client Error Codes

The following list provides information about error codes that may occur on the client application. To contact Intel Unite® solution's support, click this link.

The client saves a log file at the following path:

`C:\Users\<user>\AppData\Local\Temp`, where `<user>` is the logged in user

The name of the log file is **Unite.sql**.

Error Code: **0x00000** Error Text: Empty server response. Error Description: This error appears when a response from the server side is wrong. Error Remediation: Internal error, contact support and provide Unite.sql file.
Error Code: **0x00001** Error Text: Missing parameter server response. Error Description: This error appears when a bad request is made Error Remediation: Internal error, contact support and provide Unite.sql file.
Error Code: **0x00002** Error Text: Invalid OrganizationId server response. Error Description: OrganizationId is not found in the API DataBase. Error Remediation: Verify valid Keys in the registry paths: Computer\HKEY_CURRENT_USER\Software\Intel\Intel Unite Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Intel\Intel Unite Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Intel\Intel Unite Delete incorrect or corrupted keys and go to admin portal landing page to create new keys.
Error Code: **0x00535** Error Text: Error while attempting to get request. Error Description: The server instance is wrong. Error Remediation: Internal error, contact support and provide Unite.sql file.

Error Code: **0x00536** Error Text: Unknown server response. Error Description: Response not supported. Error Remediation: Internal error, contact support and provide Unite.sql file.
Error Code: **0x00537** Error Text: Unknown state of GetAuthorizationToken. Error Description: Server responded with code unknown for authorization token. Error Remediation: Please remove all keys for organization id in registry paths: Computer\HKEY_CURRENT_USER\Software\Intel\Intel Unite Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Intel\Intel Unite Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Intel\Intel Unite Go to Admin portal and check if the device with the host name exist, if exist remove it, afterwards go to landing page to create new keys. If the problem persists, contact support and provide Unite.sql file.
Error Code: **0x00538** Error Text: Error while attempting to set version. Error Description: Error while attempting to set version or configuration is empty. Error Remediation: Verify root node has a configuration assigned on the admin portal. Verify configuration is valid with correct core and app modules.
Error Code: **0x0053A** Error Text: Error in PairingManagerOnPairingProcessFinished. Error Description: Error installing current app. Error Remediation: Uninstall and delete device on the admin portal and try installing the app and registering the client again. If the problem persists, contact support and provide Unite.sql file.

Error Code: **0x0053B** Error Text: Pre-requirements OrganizationId and/or ServerUrl and/or OrganizationName are missing. Error Description: Keys or values in DNS TXT record missing. Error Remediation: Verify DNS TXT record have the correct configuration (with https protocol). Confirm keys in registry is correct: Computer\HKEY_CURRENT_USER\Software\Intel\Intel Unite Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Intel\Intel Unite Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Intel\Intel Unite Make sure you have the necessary properties, be aware if these keys are incorrect or corrupted, delete them and go to admin portal landing page to create new keys.
Error Code: **0x0053D** Error Text: Unable to launch client app because the file was not found. Error Description: Unable to find app core file. Error Remediation: Check if path exist in program data, if exist check permissions.
Error Code: **0x0053E** Error Text: Unable to launch client app. Error Description: Unable to launch client app. Error Remediation: Uninstall and delete device on the admin portal and try installing the app and registering the client again. If the problem persists, contact support and provide Unite.sql file.
Error Code: **0x0053F** Error Text: Error downloading client core file. Error Description: Error downloading/decompressing client core file. Error Remediation: Delete core app assigned in admin portal and upload again.
Error Code: **0x00540** Error Text: Error downloading client module file. Error Description: Error downloading/decompressing client module file. Error Remediation: Delete module assigned in admin portal and upload again.

Hub Error Codes

The following list provides information about error codes that may occur on the hub application: To contact Intel Unite® solution's support, click this link.

The hub saves a log file at the following path:

`C:\Users\<user>\AppData\Local\Temp`, where `<user>` is the logged in user

The name of the log file is **Unite.sql**.

Error Code: **0x0053B** Error Text: Pre-requirements OrganizationId and/or ServerUrl and/or OrganizationName are missing. Error Description: Keys missing in registry or wrong values in DNS TXT record. Error Remediation: Go to admin portal and make sure to create ServerUrl key with https protocol (similar to the DNS TXT record).
Error Code: **0x00002** Error Text: OrganizationId does not exist server response Error Description: OrganizationId is not found in API DataBase. Error Remediation: Verify you have valid Keys in the registry paths: Computer\HKEY_CURRENT_USER\Software\Intel\Intel Unite Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Intel\Intel Unite Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Intel\Intel Unite Delete incorrect or corrupted keys and go to admin portal landing page to create new keys.
Error Code: **0x00536** Error Text: Unknown server response. Error Description: Response not supported. Error Remediation: Internal error, contact support and provide Unite.sql file.
Error Code: **0x00541** Error Text: UnknownResponse on CheckShortCodeTokenStatus procedure. Error Description: Error while attempting to get short code status. Error Remediation: Remove all keys for organization id in registry paths: Computer\HKEY_CURRENT_USER\Software\Intel\Intel Unite Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Intel\Intel Unite Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Intel\Intel Unite Go to Admin portal and check if the device with the host name exist, if exist remove it, afterwards go to landing page to create new keys. If the problem persists, contact support and provide Unite.sql file.

Error Code: **0x00542** Error Text: Error at looking manifest assigned in the admin portal. Error Description: Error while attempting to set version or configuration is empty. Error Remediation: Verify root node has a configuration assigned on the admin portal. Verify configuration is valid with correct core and app modules.
Error Code: **0x00544** Error Text: Error updating manifest progress bar. Error Description: Error in UI thread Check. Error Remediation: Internal error, contact support and provide Unite.sql file.
Error Code: **00x00545** Error Text: Error downloading core Manifest. Error Description: Error downloading/decompressing Hub module file. Error Remediation: Delete core app assigned in admin portal and upload again.
Error Code: **0x00546** Error Text: Error downloading module Manifest. Error Description: Error downloading/decompressing Hub core file. Error Remediation: Delete module assigned in admin portal and upload again.
Error Code: **0x00547** Error Text: Error launching app, the file was not found. Error Description: Unable to find app core file. Error Remediation: Check if path exist in program data, if exist check permissions.
Error Code: **0x00548** Error Text: Exception launching app. Error Description: Unable to launch client app. Error Remediation: Uninstall and delete device on the admin portal and try installing the app and registering the client again. If the problem persists, contact support and provide Unite.sql file.
Error Code: **0x0054A** Error Text: Exception while attempting to CheckLongPairingTokenStatus / Unable to connect to server. Error Description: Cannot connect with server. Error Remediation: This occurs when the server cannot response or socket exception occurs. Attempt pairing again, if problem persists, contact support and provide Unite.sql file.

Error Code: **0x0054B**

Error Text: Exception while attempting to CheckLongPairingTokenStatus SMTP server configuration missing.

Error Description: IIS SMTP send email setting not set.

Error Remediation: Configure IIS SMTP server property on the admin portal.

Appendix C. Troubleshooting

Slowness Accessing Admin Portal or Launching Client/Hub Software When Not Connected to the Internet

Due to timeouts when the operating system attempts to verify certificate revocation, which requires Internet access, slowness may result in accessing the Admin Portal or launching the client/hub software. To prevent this behavior, set the following registry keys on your client/hub.

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings]

"CertificateRevocation"=dword:00000000

[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\WinTrust\Trust Providers\Software Publishing]

"State"=dword:00023e00

[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Download]

"CheckExeSignatures"="no"

Hub Time Drift

Hub time might drift and be different than other hubs, which can cause confusion as to when a meeting ends or who owns the meeting. To resolve this, configure the hubs sync time with the domain on a regular basis. Use a search engine in a web browser to search for how to configure a domain system to sync time with the domain controller.

After configuring the hub to sync time with the domain controller on a regular basis, use the following steps to confirm the setting:

1. Open a command-line window (press **Windows Key + R**, type **cmd**, and press **Enter** or **Return**).
2. Type **w32tm.exe /query /status**.
3. Confirm that the source is not set to **Local CMOS Clock**.

Client Error 0x00535 – Unable to Connect to Server

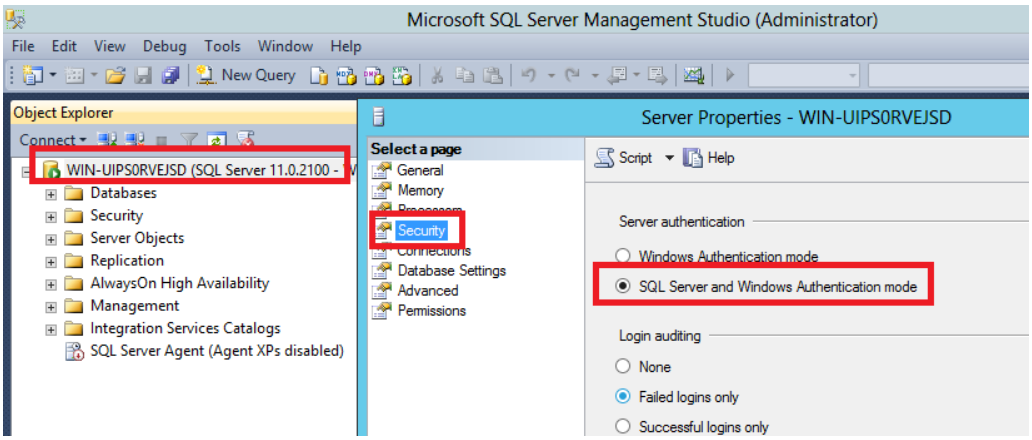
Client Error 0x00535 - Unable to connect to Server may result due to not having the SHA2 certificate installed on the client system.

To resolve this issue, import the SHA2 certificate from the Admin Portal to the trusted root of the client system. Refer to Section 6.1.1 for details about importing a certificate on the client.

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. The workaround/solution is to verify the authentication modes used during Microsoft 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. See Figure 14.

Figure 14. Microsoft SQL Server Security Properties

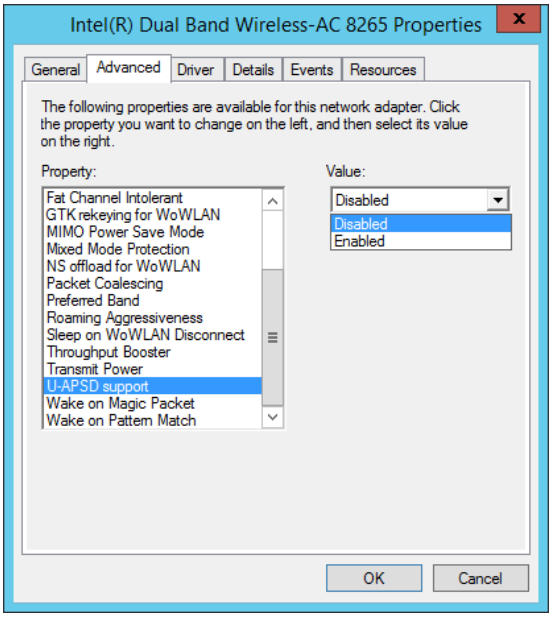


If error continues to occur, reset the password for the **api_user**. Use Microsoft SQL Management Studio and connect to your SQL server, go to Security > Logins and right click on **api_user** to open a window for Login Properties. Enter a new password and click OK to save changes.

The user may see longer-than-usual connect times, or periodic slow screen updates

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

Figure 15. Wireless Driver Properties



Appendix D. Security Checklist

Intel recommends a number of server, hub, and client security settings.

Server

Intel recommends the following settings to enhance the server security being used with the Intel Unite® solution:

- Ensure SSL is enabled in IIS (https sites should work). This might require working with the organization's IT department to install an SHA-2 certificate with a valid root of trust. **(Strongly Recommended)**

  Note: The hub can pin the certificate hash in the registry to simplify certificate checking.

- Encrypt connection strings. For details refer to the Microsoft Developer Network* (MSDN) documentation.
- Encrypt communication between the web portal and SQL DB.
- If using SQL authentication, protect the SQL credentials. For more information, refer to the MSDN webpage How To: Connect to SQL Server Using SQL Authentication in ASP.NET 2.0.
- Remove Port 80 binding for Default Web Site in IIS.

Hub

Intel recommends the following settings to enhance security for hub devices being used with the Intel Unite solution:

- Pin enterprise server certificate in registry. Refer to the Microsoft enterprise certificate pinning article.
- Physically secure the hub to prevent unauthorized access or theft.
- Disable unused or unnecessary input/output ports to prevent unauthorized access or alteration of hub behavior.
- Consult with IT security experts for any other security recommendations.

Client

Intel recommends the following setting to enhance security for client devices being used with the Intel Unite solution:

- Pin enterprise server certificate in the registry. Refer to the Microsoft enterprise certificate pinning article.

Appendix E. Considerations for Transitioning from a 3.x Environment

This section describes some considerations for installing Intel Unite® solution 4.0 in an existing 3.x environment.

- Intel Unite solution 4.0 server components can be installed on a server that already has Intel Unite solution 3.x server components installed.
  - 4.0 server database components can be installed on the same server that has 3.x server database components installed. This is because 4.0 and 3.x create different database tables.
  - 4.0 Admin Web Portal can be installed on the same server that has a 3.x Admin Web Portal installed. The web resources for the 4.0 Admin Web Portal are installed to a different path than the 3.x Admin Web Portal.
  - The 4.0 server components Admin API, Telemetry Service, and Maintenance Service can be installed on a server that has 3.x server components installed.
- 4.0 clients can connect to both 4.0 and 3.x hubs. **Note:** In order for the Windows 4.0 client to connect to a 3.x hub, the device must have a 3.x client installed as well as the 4.0 client. The 4.0 Client must be installed **after** the 3.x client is already installed.
- Intel Unite solution 3.x uses a DNS SRV record for Autodiscover, while Intel Unite solution 4.0 uses a DNS TXT record. This allows both to run within an organization.

Install sequence when going from Intel Unite solution 3.x to 4.0:

1. First install 4.0 Intel Unite software on the PIN server and create the DNS TXT record.
2. Throughout transition period, maintain 3.x and 4.0 versions of the server. Note: You can run Intel Unite solution 3.x and 4.0 servers simultaneously on the same OS.
3. Begin installing 4.0 client application on all of your Windows based devices while keeping the 3.x client application installed. Everything non-Windows can be upgraded to 4.0. When the application starts up the 4.0 client will attempt to connect to a 4.0 hub and fall back to a 3.x connection as needed.
4. Once you have all the client devices on 4.0 then begin migrating hubs to 4.0.

Appendix F. Backup and Restore of the PIN Server for Intel Unite® Solution 4.0

Use the steps shown for backing up and restoring a PIN Server for Intel Unite® solution 4.0.

Minimum Backup Steps:

1. Back up the SQL database 'unite_server' using your preferred backup method.
2. Back up the following directories as part of your normal backup routine:
   - C:\Intel\Manifests
   - C:\Intel\TempManifest

Restore Steps:

1. Rebuild the server or restore the VM and install all prerequisites for server of the Intel Unite solution.
2. Install the server for the Intel Unite solution, let it create the DB. On the Custom Setup page, select **Will be installed on local hard drive** for the Database item.
3. After the server for the Intel Unite solution is installed, stop the following Services in the order listed:
   - Unite Maintenance
   - Unite Telemetry
   - WWW
4. Restore manifest backups to **C:\Intel\TempManifests** and **C:\Intel\Manifests** respectively.

   Note: Target directory does not exist at this time.
5. Use your preferred method to restore the 'unite_server' database and associate the 'api_user' to the 'unite_server' database.

   Sample code to associate user:

   USE unite_server

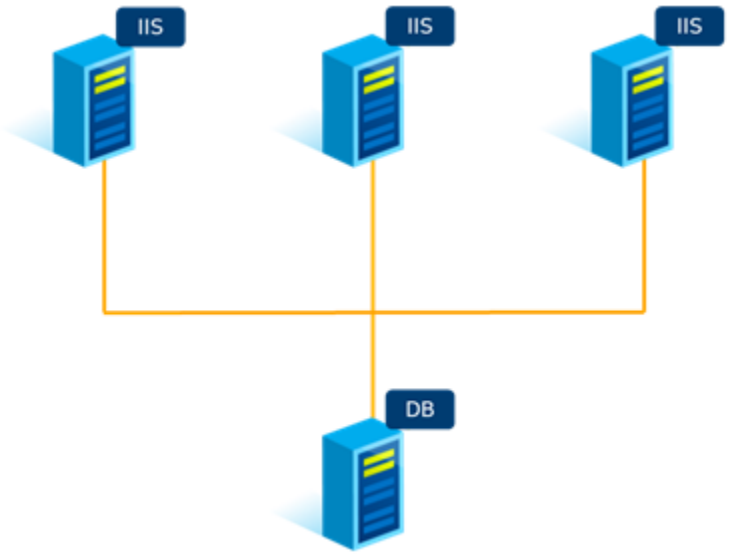
   GO

   sp_change_users_login 'AUTO_FIX', 'api_user'
6. Start the following Services in the order listed:
   - Unite Maintenance
   - Unite Telemetry
   - WWW
7. Confirm that the server is functioning by logging in to the Admin Portal

Appendix G. Load Balancing Configuration Options

The Intel Unite solution supports a number of load balancing configurations. An example that would use DNS Round Robin load balancing is depicted below:

Diagram 2. Load Balanced Configuration



This example shows multiple IIS front-end servers all connecting to a DB hosted on an existing SQL infrastructure such as a SQL farm, etc.

The installation components will be distributed in an architecture such as this. The section below defines how to select individual components to install using the server for the Intel Unite solution installer.

Distributing the enterprise server components in a load balancing configuration

For an enterprise server installation in a load balanced configuration, the Database feature should be installed on one server, while the Web API, Admin Portal, Telemetry Service, and Maintenance Service can be installed on multiple servers:

Figure 16. Server Features

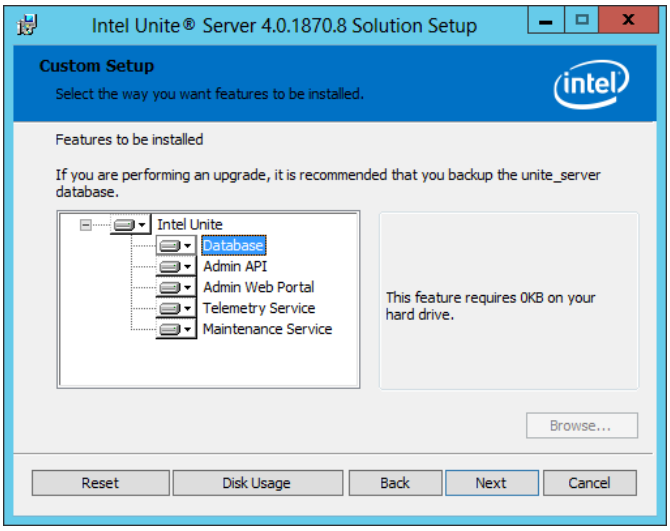
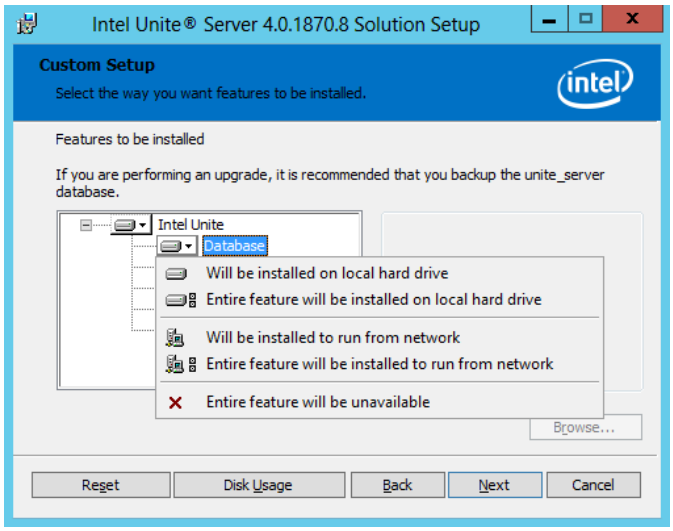


Figure 17. Server Feature Installation Options



The following steps describe how to configure the installation of the enterprise server software for use with a load balancer Refer to Figure 16 and Figure 17:

1. After completing the procedure in Section 4.3.1 through Step 9, configure the following install options for Database, Web API, Admin Portal, Telemetry Service, and Maintenance Service features to set up the enterprise server with a load balancer:
   - To install the Database on the server, choose **Will be installed on local hard drive** or **Entire feature will be installed on local hard drive**.
   - To not install the Database on the server, choose **Entire feature will be unavailable**.
   - To install the Web API on the server, choose **Will be installed on local hard drive** or **Entire feature will be installed on local hard drive**.
   - To not install the Web API on the server, choose **Entire feature will be unavailable**.
   - To install the Admin Portal on the server, choose **Will be installed on local hard drive** or **Entire feature will be installed on local hard drive**.

- To not install the Admin Portal on the server, choose **Entire feature will be unavailable**.
- To install the Telemetry Service on the server, choose **Will be installed on local hard drive** or **Entire feature will be installed on local hard drive**.
- To not install the Telemetry Service on the server, choose **Entire feature will be unavailable**.
- To install the Maintenance Service on the server, choose **Will be installed on local hard drive** or **Entire feature will be installed on local hard drive**.
- To not install the Maintenance Service on the server, choose **Entire feature will be unavailable**.

Note: Currently, the options **Will be installed to run from network** and **Entire feature will be installed to run from network** are not supported. Choosing these options results in the feature not being installed on the server.

2. After selecting the features to install, click **Next**.
3. In the **Organization Name** text box, enter an organization name, and in the **Organization Description** text box, enter a description. The organization name is used to create the root hub group and the root client group.
4. Select either **Enhanced Pairing Mode** or **Standard Pairing Mode**.
   - Enhanced Pairing Mode—This mode requires e-mail confirmation when registering a client device.
   - Standard Pairing Mode—This mode does not require e-mail confirmation when registering a client device.

   Note: Pairing mode cannot be changed once it is set. It requires a re-installation of the server to change the pairing mode.
5. Click **Next**.
6. Click **Install** to start the installation. When the installation process completes, the enterprise server is installed.

Additionally, the enterprise server distributes the manifest files and they will need to reside in a common location to all of the front-end IIS servers. The web.config files specify the locations of the Manifest and TempManifest directories that host these files. Re-locate the files from these directories to a central location such as a Windows share and edit the web.config files to reflect the new location. Perform the followings steps to edit the configuration to reflect the new locations:

Option 1: Manually Edit Web.config

1. Using a text editor, open web.confg located at c:\Program Files (x86)\Intel\Intel Unite\IntelUnite\Api.
2. Add the following two lines to the <AppSettings> section (replace "server" and "share" with appropriate values):
   a. <add key="ManifestFolder" value="\\\\server\\share\\Manifests" />
   b. <add key="UnapprovedManifestFolder" value="\\\\server\\share\\TempManifests" />
3. Save the modified web.confg file.

Option 2: IIS Manager

1. Open IIS Manager.
2. Browse to Default Web Site in the Connection pane.
3. Open Application Settings in the middle pane.
4. If ManifestFolder and UnapprovedManifestFolder are not listed, create them using the following steps:
   a. Click Add in the Actions pane.

b. Enter ManifestFolder for the name.
c. For the value, enter the UNC path for the manifest files (\\\\server\\share\\Manifests)
d. Click OK.
e. Click Add in the Actions pane.
f. Enter UnapprovedManifestFolder for the name.
g. For the value, enter the UNC path for the unapproved manifest files (\\\\server\\share\\TempManifests)
h. Click OK.

5. If ManifestFolder and UnapprovedManifestFolder already exists, update the values using the following steps:
   a. Double click on the name ManifestFolder.
   b. Modify the value by entering the UNC path for the manifest files (\\\\server\\share\\Manifests)
   c. Click OK.
   d. Double click on the name UnapprovedManifestFolder.
   e. Modify the value by entering the UNC path for the unapproved manifest files (\\\\server\\share\\TempManifests)
   f. Click OK.