Intel Unite® Cloud Service Version 4

Deployment Guide

Revision 1.9

October 2021

Legal Disclaimer

Performance varies by use, configuration and other factors. Learn more at www.intel.com/PerformanceIndex. Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure. Your costs and results may vary. Intel technologies may require enabled hardware, software or service activation. Check with your system manufacturer or retailer or learn more at intel.com.

Statements in this document that refer to future plans or expectations are forward-looking statements. These statements are based on current expectations and involve many risks and uncertainties that could cause actual results to differ materially from those expressed or implied in such statements. For more information on the factors that could cause actual results to differ materially, see our most recent earnings release and SEC filings at www.intc.com. All product plans and roadmaps are subject to change without notice.

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.

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.

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.

Copies of documents that have an order number and are referenced in this document may be obtained by calling 1-800-548-4725 or by visiting www.intel.com/design/literature.htm.

Contents

1 Introduction

The Intel Unite® Cloud Service powers secure, connected meeting spaces that simplify collaboration. It is designed to quickly and easily connect everyone in a session. The Intel Unite® Cloud Service 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 explains how to sign up for the Intel Unite® Cloud Service, install the Intel Unite® software, configure the Intel Unite® Cloud Service, and provides assistance for troubleshooting.

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

1.1 Audience

This document focuses on enabling users to setup and become familiar with the Intel Unite® Cloud Service. It is intended for users in an enterprise environment and anyone responsible for deploying the Intel Unite® Cloud Service.

1.2 Terminology

This section defines terms used in this document.

Table 1: Terminology

Term	Definition
Active Directory (AD)	A Microsoft developed directory service for the Windows domain network.
Active Directory Group	A container that contains user and computer objects within them as members.
Active Directory Organizational Unit (AD OU)	A subdivision within an Active Directory into which you can place users, groups, computers, and other organizational units.
Admin portal	The web interface that manages an organization and provides configuration settings for the Intel Unite® Cloud Service.
App	A software component that extends the functionality of the Intel Unite® Cloud Service.
Certificate Authority (CA)	An entity that issues digital certificates.
Certificate Revocation List (CRL)	A list of digital certificates that have been revoked by the issuing certificate authority (CA) before their scheduled expiration date and should no longer be trusted.
Client	A device (running Windows*, macOS*, iOS*, Android*, Chrome OS*, or Linux*) that connects to a hub.
Digital Certificate	An electronic document used to prove the ownership of a public key.
DNS TXT record	A type of resource record in the Domain Name System (DNS) used to provide the ability to associate arbitrary text with a host or other name, such as human readable information about a server, network, data center, or other accounting information.

Term	Definition
Domain Controller (DC)	A server computer that responds to security authentication requests (logging in, checking permissions, etc.) within a Windows domain.
Domain Name System (DNS)	A hierarchical decentralized naming system for computer, services, or other resources connected to the Internet or a private network.
Firewall	A network security system that monitors and controls incoming and outgoing network traffic based on predefined security rules.
Fully Qualified Domain Name (FQDN)	The complete domain name of a computer or host consisting of two parts: the host name and the domain name.
Hub	Mini form factor PCs, all-In-one PCs, and devices conforming to the Open Pluggable Specification (OPS) with Intel vPro® technology that is list on the support website for the Intel Unite® solution. The device is connected to a display in a conference room running the Intel Unite® application.
Information Technology (IT)	The usage of computers to store, retrieve, transmit, and manipulate data or information, often in the context of a business or other enterprise.
Lightweight Directory Access Protocol (LDAP)	An open, vendor-neutral, industry standard application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.
Secure Hash Algorithm (SHA)	A family of cryptographic hash functions published by the National Institute of Standard and Technology (NIST) as a U.S. Federal Information Processing Standard (FIPS).
Secure Sockets Layer (SSL)	A cryptographic protocol designed to provide communications security over a computer network.
Single Sign-On (SSO)	A property of access control of multiple related software systems, allowing a user to log in with a single ID and password to gain access to connected systems.
Unified Extensible Firmware Interface (UEFI)	A specification for a software program that connects a computer's firmware to its operating system.
Uniform Resource Identifier (URI)	A string of characters designed for unambiguous identification of resources and extensibility via the URI scheme.
Uniform Resource Locater (URL)	A reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it.
Virtual Private Network (VPN)	Extension of a private network across a public network, enabling users to send and receive data across a public network as if their computing devices were connected directly to the private network.

Term	Definition
Intel vPro® Technology	A set of security and manageability capabilities built into the processor aimed at addressing four critical areas of IT security: 1. Threat management, including protection from rootkits, viruses, and malware. 2. Identity and website access point protection. 3. Confidential personal and business data protection. 4. Remote and local monitoring, remediation, and repair of PCs and workstations.

2 Intel Unite® Solution Prerequisites

This section explains the hardware and software requirements for hub and client devices that are used with the Intel Unite® solution, along with some IT considerations and network requirements and mobile device considerations.

2.1 Hub Prerequisites

- A supported platform

  Note: Devices that are not explicitly approved by Intel but meet the remainder of the prerequisites may be used, but performance is not guaranteed.

- Microsoft Windows* 10 RS5, RS4, RS3, RS2 (64-bit only)
  - Recommended latest patch level
  - Microsoft .NET 4.8 or greater
- 4 GB RAM
- Network connection (wired or wireless)
- 32 GB available storage
- 7th gen Intel® Core™ i5 processor (or greater)

2.2 Client Prerequisites

- 32-bit or 64-bit Microsoft Windows* 10 RS5, RS4, RS3, or RS2
  - Recommended latest patch level
  - Microsoft .NET 4.8 or greater
- macOS* 10.12, 10.13, 10.14, or 10.15
- iOS* 13 or 14
- 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

2.3 4K Screen-Sharing Prerequisites

4K video is currently available only for Mac and Windows clients. The following are the prerequisites for 4K video.

2.3.1 Hub Prerequisites

- 7th gen Intel® Core™ i5 processor (or greater) with a 4K display

2.3.2 Client Prerequisites

- Windows* OS - 10th gen Intel® Core i5™ processor (or greater) with a 4K screen
- macOS - 7th gen Intel® Core i5™ processor (or greater) with a 4K screen

2.4 IT Considerations and Network Prerequisites

Primary IT considerations and network prerequisites include the following:

- Internet access to the Intel Unite® Cloud Service.
- 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 the 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 Intel Unite® Cloud Service. This provides the easiest method for hubs and clients to locate the Intel Unite® Cloud Service.
- For security purposes, the Intel Unite® application accepts only SHA-2 or greater certificates due to the end of life of SHA-1.

2.5 Mobile Client Devices

Some organizations deploy mobile client devices as part of the Intel Unite® solution. To connect to the Intel Unite® Cloud Service, all client devices (including iOS* and Android* devices) must be connected to the corporate network or use an appropriately configured VPN if Active Directory Federation Services is used to log into the admin portal for Intel Unite® Cloud Service. Mobile devices not connected to the corporate network (for example, personal laptops, tablets, and phones) may not be able to log into the admin portal. When enabling mobile client devices, IT administrators should do the following:

- If Intel Unite® app users are using personal mobile devices, require them to be on the same network as the hub to connect to Intel Unite® solution, or create another way to allow the connections.
- Utilize and adhere to your business' IT tools and strategies 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 strictly the company wants to apply protections.

3 Basic Setup

This section explains the basic setup for the Intel Unite® Cloud Service. The setup addresses the following:

- Creating a new account
- Creating a new organization
- Setting required organization configurations
- Pairing hubs
- Registering clients

After basic setup, clients can join Intel Unite® solution sessions hosted by hubs that have been paired with the organization.

3.1 New Account Creation

An Intel account is needed to use the Intel Unite® Cloud Service. If you already have an Intel account, skip to Section 3.2. Follow the steps below to create an account:

1. Open a browser, either Google Chrome or Microsoft Internet Explorer, and navigate to the login page of the Intel Unite® Cloud Service.
2. Click **Create your account** to display the account creation form.
3. Fill out the Personal Information form and click **Submit**.

3.2 Sign In

Follow the steps below to sign in:

1. Open a browser and navigate to the login page of the Intel Unite® Cloud Service.
2. Enter your username and password.
3. Click **Sign In**.

3.3 Setup Wizard

The setup wizard assists in the setup process. The setup wizard will start automatically when logging in if no organization currently exists. To start the setup wizard manually, click the **Configuration Assistant** icon at the upper-right corner of the window after signing in. The setup wizard facilitates the following:

- Organization creation
- Subscription acquisition
- Organization configuration
- Hub pairing
- Client pairing

If the setup wizard is exited before completion, the wizard will continue from the step where the wizard was last exited the next time the setup wizard is started.

3.3.1 Create an Organization

Upon starting the setup wizard, the Create an Organization page of the wizard will appear. An organization represents the business or a subgroup within a business that uses the Intel Unite® Cloud Service. Each organization has its own instance of the Intel Unite® Cloud Service. Follow the steps below to create an organization:

1. Enter Organization Name. The name must be at least four characters long. There are no restrictions as to which characters can be used.
2. Enter a description for the organization. The description must be at least four characters long.
3. Click **Next** to create the organization. A unique organization ID will be created for the new organization.

Once the organization has been created, the setup wizard will proceed to subscription and activation, described in Section 3.3.2.

3.3.2 Subscribe to and Activate the Intel Unite® Cloud Service

A subscription to the Intel Unite® Cloud Service is required to hub pair devices for use with the Intel Unite® Cloud Service. Multiple subscriptions can be activated for a single organization. If you already have an unactivated subscription, proceed to Section 3.3.2.1. Follow the steps below to add a subscription and activate it:

1. Click **SHOP SUBSCRIPTIONS**.
2. After obtaining a new subscription, the subscription will automatically be activated for the organization.
3. Once the display refreshes to show the activated subscription, click **Next** to continue.

Once a subscription has been acquired and activated, the setup wizard will proceed to configure settings, described in Section 3.3.3.

3.3.2.1 Activate an Unactivated Subscription

If you have an existing unactivated subscription, follow the steps below to activate it:

1. Enter the subscription ID into the Subscription ID field.
2. Click **ACTIVATE**.
3. Once the display refreshes to show the activated subscription, click **Next** to continue.

Once a subscription has been activated, the setup wizard will proceed to configure settings, described in Section 3.3.3.

3.3.3 Configure Settings

After obtaining a subscription, certain minimum settings must be configured. Follow the steps below to configure the minimum required settings:

1. Enter an email address for receiving notifications from the admin portal.
2. Choose the Privacy setting. Refer to Section 5.3.2.1 for available privacy setting values.
3. Click **Next** to continue.

Upon configuring the minimum settings, the setup wizard will proceed to hub pairing, described in Section 3.3.4.

3.3.4 Pair Hubs

At a minimum, one hub device must be paired with an organization through the admin portal for the Intel Unite® Cloud Service. After a hub is paired with an organization, it will receive PINs that allow registered clients to connect to sessions hosted by the hub. The instructions displayed in the wizard are for a hub device, except for step 4 in the list below, where the pairing code is entered on the system where the setup wizard is running. Follow the steps below to pair a hub device:

1. Follow the on-screen instruction prompts. If necessary, refer to Section 4.11.2 for detailed instructions on installing the hub software.

   Note: The provisioning URL must be activated on the hub device. Click the **copy to clipboard** icon to copy the provisioning URL, allowing the provisioning URL to be pasted into a text file to be transferred to the hub device via USB flash drive or a network share resource. Click the **email icon** to email the provisioning URL, allowing the hub device access to the URL through an email account.

2. On Windows* platforms, a Windows* Defender pop-up may appear requesting permission to allow network access for the Intel Unite® app. Until permission is given for the Intel Unite® app, the hub will not be able to connect to the Intel Unite® Cloud Service. In some cases, the hub application may hide the pop-up; to

resolve this issue, use Task Manager to close the Intel Unite® app, then click **Allow access** in the Windows Defender pop-up. Activate the URL referenced in the note from Step 1 to start the hub application.

3. The pairing code will appear on the hub display.
4. On the system where the setup wizard is running, enter the pairing code from the hub display and click the **PAIR HUB** button. If pairing more than one hub, enter the next hub's pairing code and click the PAIR HUB button again. Repeat this process until all desired hubs are paired. Click the **refresh** button to the right of the PAIR HUB button to refresh the list of paired hubs.
5. In the wizard, click **Next** to continue.

Once hub pairing is complete, the setup wizard will proceed to client pairing, explained in Section 3.3.5.

3.3.5 Pair Clients

In order for a client to connect to a session hosted by a hub, the client must be paired with the same organization that is paired with the hub. Follow the steps below to register a client with an organization:

1. Follow the on-screen instruction prompts. If necessary, refer to Section 4.12 for detailed instructions on installing the client software.

   Note: The provisioning URL must be activated on the client device. Click the **copy to clipboard icon** to copy the provisioning URL, allowing the provisioning URL to be pasted into a text file to be transferred to the client device via USB flash drive or a network share resource. Click the **email icon** to email the provisioning URL, allowing the client device access to the URL through an email account.
2. On Windows* platforms, a Windows* Defender pop-up may appear requesting permission to allow network access for the Intel Unite® application. Until permission is given for the Intel Unite® application, the client will not be able to connect to the Intel Unite® Cloud Service. In some cases, the client application may hide the pop-up; to resolve this issue, use Task Manager to close the Intel Unite® application, then click **Allow access** in the Windows Defender pop-up. Activate the URL referenced in the note from Step 1 to start the client application.
3. Click **Exit Setup** to complete the setup wizard.

3.3.6 Using the Setup Wizard after Setup Completion

After an organization is created from the completion of the setup wizard, the setup wizard can be used to change the admin e-mail address and the privacy policy setting, pair hubs, and register clients. From the Organizations page, select an organization that was created from a completed setup wizard, then click the **Configuration Assistant icon** to start the setup wizard to change the admin e-mail address, the privacy policy setting, pair hubs, or register clients.

4 Advanced Setup

This section provides greater details regarding the setup process and provides technical details for signing into the admin portal using Single-Sign On (SSO) authentication with Active Directory Federation Services (AD FS).

4.1 Deployment Overview

The Intel Unite® Cloud Service consists of four components:

- The **admin portal** for Intel Unite® Cloud Service – the web interface used to configure the Intel Unite® Cloud Service.
- **Hubs** – Intel® Core™ vPro® processor-based mini PCs that meets the hub requirements described in Section 2. The hub is typically connected to a display or a projector in a conference room. Refer to the display/projector user manual for instructions on how to properly connect it to the hub.
- **Clients** – systems that connect to a hub for collaboration in a session.
- Intel Unite® **apps** – software that extends the capability of the Intel Unite® solution. An example of an Intel Unite® app is Scratchpad*, which provides a virtual whiteboard for collaboration.

The steps for deploying the Intel Unite® solution using the Intel Unite® Cloud Service are listed below:

1. Sign in to the admin portal for the Intel Unite® Cloud Service.
2. Create an organization.
3. Subscribe to the Intel Unite® Cloud Service.
4. Activate the subscription.
5. Optional – Create custom group for hub and/or client devices.
6. Optional – Create and assign custom configurations for hubs and/or clients.
7. Pair hub(s).
8. Pair client(s).
9. Optional – Setup DNS TXT Record – Used to identify the Intel Unite® Cloud Service resource and provide organization information to hub and client devices.

4.1.1 Deployment Resources

Administrative rights on the hub are required to complete the installation. Requirements may also include the following:

- IT security administrator for setting firewall policies.
- IT administrator to create a DNS TXT record, which is used by hub and clients to locate the Intel Unite® Cloud Service (strongly recommended).

4.2 Single Sign On (SSO)

Single-Sign-On (SSO) allows a user to log in with a single ID and password to gain access to connected web resources. The Intel Unite® Cloud Service supports SSO using an Intel account and Active Directory Federation Services (AD FS) hosted by the customer.

4.2.1 Setup for SSO with Intel Accounts

A user with an Intel account can use the Intel account credentials to access the admin portal for the Intel Unite® Cloud Service. Follow the next steps to create an Intel account.

1. Open a browser and navigate to the login page of the Intel Unite® Cloud Service.
2. Select **Create your account**.
3. Enter your information and select **Submit**.

4. An Email Verification screen will be displayed. Check your email and follow the verification instructions contained within.
5. To confirm that Intel SSO is functional:
    a. Open a browser and navigate to the login page of the Intel Unite® Cloud Service.
    b. Enter your username and password, then click **Sign In**.
    c. After signing in, the Organizations page of the admin portal will be displayed..

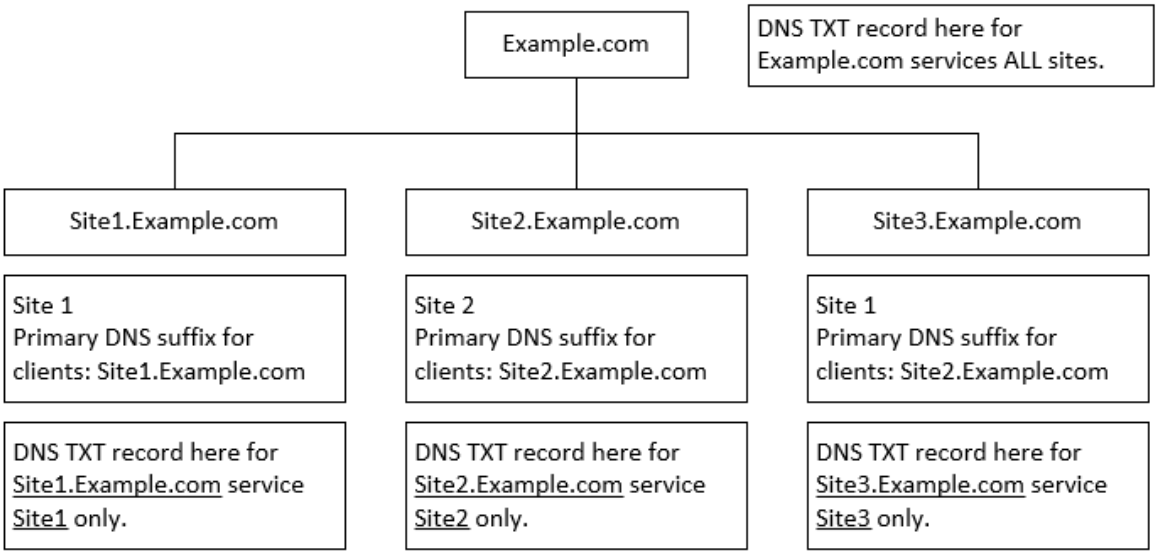
4.3 DNS TXT Record

The DNS TXT record is a resource record used to provide Intel Unite® clients with necessary information for the Intel Unite® Cloud Service. The specific information provided by the DNS TXT record is the URL of the server hosting the Intel Unite® Cloud Service and the organization ID.

4.3.1 DNS Hierarchy and Proper Placement of DNS TXT Record

The DNS TXT record facilitates the auto-discovery of the PIN service for Intel Unite® Cloud 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. Figure 1 and the examples below demonstrate the proper placement of the DNS TXT record.

Figure 1: DNS TXT Record Placement Example



The following examples are based on the diagram in Figure 1:

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

4.3.2 Create a DNS TXT Record

The hub and clients can locate the Intel Unite® Cloud Service by using a DNS TXT record during an automatic lookup for the Intel Unite® Cloud Service. The string in the DNS TXT record is not case-sensitive. Follow the steps below to add a DNS TXT record in Microsoft* Windows*:

1. Open **DNS Manager** on your DNS server.
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 will be filled in automatically.
8. The Text option should be automatically populated with `SERVICEURL=https://<admin portal for the Intel Unite® Cloud Service FQDN>/intelunite/api|ORGID=<Organization ID>|OrgName=<Organization Name>`, where `<Organization ID>` is the GUID for the organization, and `<Organization Name>` is the name of the organization. The OrgID is randomly generated, and the OrgName is set during creation of the organization. Both values can be found by browsing to the **Provision Device** page on the admin portal for Intel Unite® Cloud Service. Refer to Section 5.5 for additional details.
9. Click **OK** to create the record.
10. Click **Done** to close the Resource Record Type window.

4.3.3 Disable Use of the DNS TXT Record

The use of the DNS TXT Record for auto-discovery can be disabled. Below are the methods for disabling auto-discovery on Windows and macOS platforms.

Note: macOS and iOS platforms do not support auto-discovery with the `.local` domain.

Windows Platforms:

On Windows platforms, 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 the DNS TXT Record will not be used for auto-discovery. A DWORD value of 0 means, the DNS TXT Record will be used for auto-discovery. Any other value will result in the 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.

Below are the registry locations for the DisableAutoDiscovery key.

For 32bit Windows

- Hub Device: `HKLM\SOFTWARE\Intel\Intel Unite\Hub`
- Client Device: `HKLM\SOFTWARE\Intel\Intel Unite\Client`

For 64bit Windows

- Hub Device: `HKLM\SOFTWARE\{WOW6432Node}\Intel\Intel Unite\Hub`
- Client Device: `HKLM\SOFTWARE\{WOW6432Node}\Intel\Intel Unite\Client`

Once DNS TXT Record is disabled for auto-discovery, the use of the provision device page of the admin portal is needed to provide the information provided by the DNS TXT Record. On the Provision Device page, click the link that opens the Intel Unite® application on the device and set the registry keys with needed values.

macOS Platforms

There are several methods to disable auto-discovery on a macOS platform. Below are the methods for disabling auto-discovery:

Method 1 - Uncheck the Automatic checkbox next to Enterprise Server in the Configuration tab of the Intel Unite® application settings.

1. Open the Intel Unite® app.
2. Enter settings by clicking the **gear** icon in the upper right corner.
3. Click **Configuration**.

4. Uncheck the **Automatic** checkbox next to Enterprise Server.
5. Click **Save Settings** at the bottom.

Method 2 - Launch the Intel Unite® app from a terminal using the `disableautodiscovery` parameter.

1. Open a terminal. (Application -> Utilities -> Terminal)
2. Enter the following: `open -a "Intel Unite" disableautodiscovery`

Method 3 - Modify the plist to set `DisableAutoDiscovery` to `true`.

1. Open a terminal. (Application -> Utilities -> Terminal)
2. Enter the following: `defaults write com.intel.Intel-Unite DisableAutoDiscovery -bool true`

4.4 Sign in to the admin portal

Follow the below steps to sign in to the admin portal for the Intel Unite® Cloud Service.

1. Open a browser and navigate to the login page of the Intel Unite® Cloud Service.
2. Enter your username and password. For users that do not have an Intel account, refer to Section 4.2.1 for instructions on to create an Intel account.
3. Click **Sign In**.

4.5 Create an Organization

An organization represents the business or a unit within a business that uses the Intel Unite® Cloud Service. To create an organization without the Setup Wizard, refer to Section 5.3.1 to create an organization.

4.6 Subscribe to the Intel Unite® Cloud Service

An active subscription to the Intel Unite® Cloud Service is required to pair devices for use with the Intel Unite® Cloud Service.

Open a browser and navigate to https://www.intel.com/content/www/us/en/architecture-and-technology/unite/cloud-collaboration/options.html to subscribe.

4.7 Activate Subscription

An active subscription is required for pairing hubs for use with the Intel Unite® Cloud Service. Follow the steps below to activate a subscription:

1. After signing in, select the organization that the unused subscription will be applied to, by clicking on the organization name.
2. Open the **Subscription Management** menu.
3. Obtain the subscription ID from the e-mail received after signing up for the subscription.
4. Enter the subscription ID into the **Activate Subscription** text field.
5. Click the **Activate** button.
6. Confirm an activation success message pops up.

Note: If the user was sent to the Avnet website from clicking on a SHOP SUBSCRIPTIONS button and obtained a subscription, the subscription will automatically be activated and apply to the organization that the user was managing. The SHOP SUBSCRIPTIONS button can be found under the Subscription Management menu or within the second step of the setup wizard, refer to Section 3.3 for more information about the setup wizard.

4.8 Create Custom Group for Devices

Devices that have the same configuration are managed as a group. Upon the creation of an organization, a root group is created for the hub devices, and a root group is created for the client devices. By default, all hub devices are assigned to the root hub group when the hubs are paired with the organization, and all client devices are assigned to the root client group when the clients are registered.

Subgroups can be created to manage different configuration for hub and client devices. Follow the steps below to create a subgroup within the root group.

1. Open a browser and navigate to the login page of the Intel Unite® Cloud Service.
2. Enter your username and password. For users that do not have an Intel account, refer to Section 4.2.1 for instructions on to create an Intel account.
3. Click **Sign In**.
4. Select an organization by clicking the name of the organization on the Organizations page.
5. If creating a client subgroup, click **Clients** to display the client group(s) and devices.
6. Select the root client group.
7. Select **Create Group** from the select action drop-down menu located above the group and device lists.
8. Enter a name for the group.
9. Click **Create**.

4.9 Create Custom Configurations

A configuration defines the settings and apps for a hub or client device. A basic configuration for both hub and client is created for a new organization. A custom configuration can be created for hubs and clients. Follow the steps below to create a custom configuration:

1. Open a browser and navigate to the login page of the Intel Unite® Cloud Service.
2. Enter your username and password. For users that do not have an Intel account, refer to Section 4.2.1 for instructions on to create an Intel account.
3. Click **Sign In**.
4. Select an organization by clicking the name of the organization on the Organizations page.
5. Select **Configurations** from the Device Management menu.
6. On the Configurations page, click **Create Configuration**. The Create Configuration view will be displayed.
7. Replace configuration name with the name of the new configuration.
8. Select either **Hub** or **Client** next to the configuration name.
9. From the Intel Unite® Software drop-down menu, select a **version**.
10. To add features 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.
11. To remove a feature or an app, click the **white minus sign (-)** 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 will be moved to Available Features/Apps.
12. After adding the desired features and apps to the package, click the **Create Configuration** button.

4.10 Assign Custom Configurations

After a configuration is created, it must be assigned to a group. All devices in that group will use the same configuration. Follow the steps below to assign a configuration to a group.

1. Open a browser and navigate to the login page of the Intel Unite® Cloud Service.
2. Enter your username and password. For users that do not have an Intel account, refer to Section 4.2.1 for instructions on to create an Intel account.
3. Click **Sign In**.
4. Select an organization by clicking the name of the organization on the Organizations page.
5. Select **Hubs and Clients** from the Device Management menu.
6. If assigning a client custom configuration, click **Clients** to display the client group(s) and devices.
7. Select a group to assign the custom configuration.
8. Select **Assign Configuration** from the select action drop-down menu located above the group and device lists.
9. Select the custom configuration from the Select Configuration dialogue box.
10. Click the **Assign** button to assign the configuration to the selected group.

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

4.11 Pair a Hub

A hub device must be paired with an organization through the admin portal for Intel Unite® Cloud Service before clients can connect to it. Pairing a hub allows it to receive the PINs required for clients to join sessions hosted by the hub. Follow the steps in the subsections below to pair a hub device to the admin portal for Intel Unite® Cloud Service.

4.11.1 Hub Provisioning Considerations

Hub Requirements:

Refer to Section 2.1 for hub requirements.

Hub Preinstallation

A hub needs to be able to locate and pair with the admin portal for Intel Unite® Cloud Service. The Intel Unite® application needs an exemption in the hub firewall to communicate with the clients. By default, the port used by the Intel Unite® application is randomly set, but can be manually set through the admin portal for Intel Unite® Cloud Service under hub configuration properties. Additionally, complete the following verifications:

- Verify a network connection with the server by browsing to the Intel Unite® Cloud Service: https://admin.unitecloud.intel.com/.
- Verify a DNS TXT record has been created for the Intel Unite® Cloud Service. Refer to Section 4.3 for more information. If not using a DNS TXT record, confirm that the hub has access to the provisioning URL. Refer to Section 4.11.2.4.2 for more information.
- Verify that the hub meets the minimum software and hardware requirements specified in Section 2.1.

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 as follows:

- 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.

4.11.2 Hub Software Installation and Pairing

Follow the steps below to install the hub software:

1. Download the `Intel_Unite_Hub_vx.x.x.x_x86.mui.msi` file.
2. Locate and 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** checkbox.
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**.

4.11.2.1 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 "<.msi Installer Path>" /l*v "<Log Path>" /q HUBINSTALLFOLDER="<Value>"
ORGID="<Value>" PINSERVERURI="<Value>" ORGNAME="<Value>"
ACCEPTPRIVACYSTATEMENT="yes|no" REGISTRYMODE="HKCU|HKLM" OTP="<Value>"
```

4.11.2.1.1 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.

Table 2: Hub Installation Parameters

Parameter	Definition
`/i`	The switch for install.
`"<.msi Installer Path>"`	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 no user interaction.

Parameter	Definition
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 the following format: https://<FQDN of the admin portal for the Intel Unite® Cloud Service>/intelunite/api.
ORGNAME="<Value>"	The organization name; replace <Value> with the organization name.
ACCEPTPRIVACYSTATEMENT="yes|no"	Sets the accept privacy statement checkbox when set to "yes".
REGISTRYMODE="HKCU|HKLM"	Specify registry location where hub configuration is stored, either HKEY_CURRENT_USER or HKEY_LOCAL_MACHINE.
OTP="<Value>"	The OTP token used for registering a client; 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.

4.11.2.2 Configure Windows Firewall

The Windows firewall may prevent the hub from communicating with the Intel Unite® Cloud Service and client devices. This section explains how to configure the firewall to allow network access for the hub application for the Intel Unite® Cloud Service. Review and consult with your IT administrator prior to making any changes to the device.

4.11.2.2.1 Create Inbound Rule

Follow the steps below to create an inbound rule for the firewall:

1. Open the **Control Panel**.
2. Enter **Windows Defender Firewall** into the search box.
3. Click **Windows Defender Firewall** in the search results.
4. Click **Advanced settings**.
5. Click **Yes** on the User Account Control dialog box.
6. Select **Inbound Rules**.
7. Select **New Rule...** under the Actions pane.
8. Select **Program** and click **Next >**.
9. Select **This program path**, browse to the location of the hub application launcher, and select **Intel.Unite.HubLauncher.exe**. The 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 checkboxes for Domain, Private, and Public, then click **Next >**.
13. Enter a name and a description for this rule and click **Finish**.
14. Repeat Steps 6 through 13 to add a rule for `C:\ProgramData\Intel\Intel Unite\Hub\<version number>\Intel.Unite.Module.Process.exe`.
15. Repeat Steps 6 through 13 to add a rule for `C:\ProgramData\Intel\Intel Unite\Hub\<version number>\Intel Unite Hub.exe`.
16. Select **Inbound Rules**.
17. Select **New Rule…** under the Actions pane.
18. Select **Port** and click **Next >**.
19. Select **TCP** and **Specific local ports:**.
20. Enter `443` in the text field next to Specific local ports: and click **Next >**.
21. Select **Allow the connection** and click **Next >**.
22. Place a check in the checkboxes for Domain, Private, and Public, then click **Next >**.
23. Enter a name and a description for this rule and click **Finish**.

4.11.2.2.2 Create Outbound Rule

Follow the steps below to create an outbound rule for the firewall:

1. Open the **Control Panel**.
2. Enter **Windows Defender Firewall** into the search box.
3. Click **Windows Defender Firewall** in the search results.
4. Click **Advanced settings**.
5. Click **Yes** on the User Account Control dialog box.
6. Select **Outbound Rules**.
7. Select **New Rule…** under the Actions pane.
8. Select **Program** and click **Next >**.
9. Select **This program path**, browse to the location of the hub application launcher, and select **Intel.Unite.HubLauncher.exe**. The 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 checkboxes for Domain, Private, and Public, then click **Next >**.
13. Enter a name and a description for this rule and click **Finish**.
14. Repeat Steps 6 through 13 to add a rule for `C:\ProgramData\Intel\Intel Unite\Hub\<version number>\Intel.Unite.Module.Process.exe`.
15. Repeat Steps 6 through 13 to add a rule for `C:\ProgramData\Intel\Intel Unite\Hub\<version number>\Intel Unite Hub.exe`.
16. Select **Outbound Rules**.
17. Select **New Rule…** under the Actions pane.
18. Select **Port** and click **Next >**.
19. Select **TCP** and **Specific local ports:**.
20. Enter `443` in the text field next to Specific local ports: and click **Next >**.
21. Select **Allow the connection** and click **Next >**.
22. Place a check in the checkboxes for Domain, Private, and Public, then click **Next >**.
23. Enter a name and a description for this rule and click **Finish**.

4.11.2.3 Hub Privacy

Upon the first launch of the hub application, a privacy statement dialogue will be displayed if the Privacy Mode server property is set to **Prompt User**. To proceed, place a check in the checkbox next to **I consent to the collection of the information and would like to use the software**, then click the **Agree** button.

4.11.2.4 Hub Pairing

Before a hub can be used, it must be paired with an Organization on the admin portal. Part of the hub pairing process is hub configuration, which sets the `OrganizationID`, `OrganizationName`, and `ServerURL` values.

4.11.2.4.1 Hub Preconfig

The `OrganizationID`, `OrganizationName`, and `ServerURL` values must be set on the hub before it can be paired with an organization. These values can be obtained using DNS TXT record or URI.

DNS TXT Record

When a hub application 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`. Refer to Section 4.3 for instruction on creating a DNS TXT Record.

URI

On the hub, browse to the admin portal, go to the provision device page, and click the link. The following steps explain how to use a URI to set the `OrganizationID`, `OrganizationName`, and `ServerURL` values.

1. Sign in to the Intel Unite® Cloud Service on the hub. Use the following link to access the sign in page: https://www.intel.com/content/www/us/en/my-intel/intel-unite-sign-in.html?redirect=https://admin.unitecloud.intel.com/intelunite/admin.
2. Select the Organization this hub belongs to.
3. Click **Device Management** and select **Provision Device** to open the Provision Device page.
4. Click the link displayed on the Provision Device page (the link starts with intelunite4://) or copy and paste the link into a run command line on the hub.

   Note: If clicking on the link, a prompt may appear with a request to open the hub application for the Intel Unite® solution. If the prompt appears, click Open Intel Unite® Hub Launcher to open the hub application.
5. The hub application for the Intel Unite® solution will open to set the `OrganizationID`, `OrganizationName`, and `ServerURL` values. To continue with auto pairing, close the hub application and go to Section 5.5.2.2. To continue with manual pairing, refer to *Hub Manual Pairing Using the admin portal* in Section 4.11.2.4.2.

4.11.2.4.2 Hub Pairing Methods

Hubs can be paired automatically using a pairing token, or manually using the admin portal.

Note: Upon the first start of the hub application on Windows* platforms, a Windows* Defender pop-up may appear requesting permission to allow network access for the Intel Unite® application. Until permission is given for the Intel Unite® application, the hub will not be able to connect to the Intel Unite® Cloud Service. In some cases, the hub application may hide the pop-up; to resolve this issue, use Task Manager to close the Intel Unite® application, then click Allow access in the Windows Defender pop-up.

Hub Auto Pairing

The auto pairing steps are only applicable on hubs that have the OrganizationID, OrganizationName, and ServerURL set. If these values are not set, the hub will not be able to find the admin portal for pairing. Follow the steps below to use auto pairing:

1. Sign in to the Intel Unite® Cloud Service on the hub. Use the following link to access the sign in page: https://www.intel.com/content/www/us/en/my-intel/intel-unite-sign-in.html?redirect=https://admin.unitecloud.intel.com/intelunite/admin.
2. Select the Organization this hub belongs to.
3. Open the **Device Management** menu.
4. In the Duration (hours) text box, enter the number of hours the token will be valid.
5. Click the **Generate Token** button to generate a one-time pairing token.
6. 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 when the tokens will expire.

Hub Manual Pairing Using the Admin Portal

Follow the steps below to use manual pairing:

1. Sign in to the Intel Unite® Cloud Service on the hub. Use the following link to access the sign in page: https://www.intel.com/content/www/us/en/my-intel/intel-unite-sign-in.html?redirect=https://admin.unitecloud.intel.com/intelunite/admin.
2. Select the Organization this hub belongs to.
3. Click **Device Management** and select **Provision Device** to open the Provision Device page.
4. Click the link displayed on the Provision Device page (the link starts with intelunite4://) or copy and paste this link into a run command line on the hub. If clicking the link, a prompt may appear with a request to open the hub application for the Intel Unite® solution. If the prompt appears, click **Open Intel Unite® Hub Launcher** to open the hub application.
5. The hub application for the Intel Unite® solution will open and display a Ready to Pair prompt and a pairing code.
6. On a different device with access to the Internet, sign in to the Intel Unite® Cloud Service. Use the following link to access the sign in page: https://www.intel.com/content/www/us/en/my-intel/intel-unite-sign-in.html?redirect=https://admin.unitecloud.intel.com/intelunite/admin.
7. Select the same Organization that was selected in Step 2.
8. Click **Device Management**.
9. In the Pair Hub field, enter the pairing code displayed on the hub and click **Pair Hub**.
10. A Windows Defender Firewall dialog may appear on the hub. If the dialog appears, click **Allow Access**.
11. Once paired, the hub will download configuration settings and apps from the Intel Unite® Cloud Service.
12. After downloading, the hub will display a welcome screen with a PIN in the upper-right corner.

The hub is now configured and ready for use.

4.11.2.5 Uninstall Hub Software

Follow the steps below 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**, then click **Next**.

Note: 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.

4.11.2.5.1 Uninstall Hub Software by Command Line

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 "<.msi Installer Path>" /l*v "<Log Path>" /q
```

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.

Table 3: Hub Software Command-Line Uninstallation Parameters

Parameter	Definition
`/x`	The switch for uninstall.
`"<.msi Installer Path>"`	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.

4.11.2.6 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.

4.11.2.7 Hub Log File

The hub saves a log file in `%temp%\UniteLog\<yyyymmdd>_log.txt`, where `<yyyymmdd>` is the number of the year, month, and day of the log file.

Note: Log files are automatically deleted after 7 days.

4.12 Client Software Installation and Pairing

Clients must be registered with an organization through the admin portal before they join sessions hosted by hubs that are paired with the same organization.

4.12.1 Client Provisioning/Preinstallation Considerations

Refer to Section 2.2 for a detailed explanation of client requirements.

A client must be able to locate and communicate with the admin portal for Intel Unite® Cloud Service. The Intel Unite® application needs an exemption in the client firewall allowing the client application to communicate to the admin portal. The client port is the same as the hub port, which is randomly generated by default; the port number

can be manually set through the admin portal under the hub configuration properties. Refer to Appendix D for a detailed explanation of security considerations.

All client devices must be connected to the corporate network or must use an appropriately configured VPN, including Windows*, iOS*, macOS*, 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.

4.12.2 Windows* Client Software Installation

Only a single client application for Intel Unite® Cloud Service should be installed on a client device. Having more than a single client application for Intel Unite® Cloud Service installed on a client device is not supported and may result in inability to use the clients to connect to sessions.

Follow the steps below to install the Intel Unite® app on a Windows* client device:

1. Download the `Intel_Unite_Client_vx.x.x.x_x86.mui.msi` file.
2. Locate and launch the `Intel_Unite_Client_vx.x.x.x_x86.mui.msi` file, then click **Next**.
3. Accept the license agreement by checking the **I accept the terms of the License Agreement** box, then click **Next**.
4. 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**.
5. Click **Next**, then click **Install**.
6. When the installation completes, click **Finish**.

Note: Support for extended displays requires that the `Intel_Unite_Extended_Display_<x.x.x.x>.mui.msi` be installed.

4.12.2.1 Windows* Client Software Command Line Installation (Optional)

The Windows* client software 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.

Table 4: Windows* Client Software Command-Line Installation Parameters

Parameter	Definition
`/i`	The switch for install.
`"<.msi Installer Path>"`	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.
`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.

Parameter	Definition
PINSERVERURI="<Value>"	The PIN server URL, replace <Value> with the PIN server URL which has this format: https://<FQDN of the admin portal for the Intel Unite® Cloud Service>/intelunite/api.
ORGNAME="<Value>"	The organization name, replace <Value> with the organization name.
ACCEPTPRIVACYSTATEMENT="yes|no"	Sets the accept privacy statement checkbox when set to "yes".
REGISTRYMODE="HKCU|HKLM"	Specify registry location where client configuration is stored, either HKEY_CURRENT_USER or HKEY_LOCAL_MACHINE.
OTP="<Value>"	The OTP token used for registering a client, replace <Value> with the OTP token obtained from the admin portal.
USEREMAIL="<Value>"	The email of the user that uses this client, replace <Value> with the email 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.

4.12.3 macOS* Client Installation

It is possible to install the macOS* Intel Unite® client from both the macOS App Store* in addition to a direct download from Intel, resulting in two or more client applications for the Intel Unite® Cloud Service on the macOS device. Having multiple client applications for the Intel Unite® Cloud Service on a single device is not supported and may result in the malfunction of the Intel Unite® solution.

The macOS client supports connecting to 3.x and 4.x hubs. It is recommended that only a single 4.x version of the client application for the Intel Unite® Cloud Service be installed on a device allowing connection to both 3.x and 4.x hubs. Follow the steps below to identify if more than a single client application for the Intel Unite® Cloud Service is installed on a client:

1. Open **Finder**.
2. Type **Intel Unite** in the search box located at the upper right corner and press **return**.
3. Right-click or two-finger-tap on the results area and select **Arrange By->Kind**.
4. Confirm that there is only one Intel Unite® application present. If more than one Intel Unite® application is present, remove all but one of the Intel Unite® application.

Follow the steps below to install a macOS client:

1. Locate the Intel Unite macOS X.X.X.X.dmg file and download the software to the macOS* 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.
5. Go to the **Applications** folder, locate the application, and click it to launch it.

4.12.4 iOS* Client Installation

The app is compatible with all iPads* except the original 2010 iPad. Follow the steps below to install the Intel Unite® client on an iOS* device:

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 has been downloaded and installed, open the app.

4.12.5 Android* Client Installation

Follow the steps below to install the Intel Unite® client on an Android* device:

1. On an Android* device, go to the Google* app store and download the Intel Unite® software for the client.
2. Once the app has been downloaded and installed, open the app.

4.12.6 Chrome OS* Client Installation

Follow the steps below to install the Intel Unite® client on a Chrome OS* device:

1. On a Chromebook* device, go to the Google app store and download the Intel Unite® software for the client.
2. Once the app has been downloaded and installed, open the app.

4.12.7 Linux* OS Client Installation

Follow the steps below to install the Intel Unite® client on a Linux* OS device:

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

4.12.8 Configure Client Firewall

A firewall may prevent the client from communicating to the Intel Unite® Cloud Service and hub devices. The steps below explain how to configure the firewall to allow network access for the client application for the Intel Unite® Cloud Service. Review and consult with your IT administrator prior to making any changes to the device.

4.12.8.1 Windows Platform – Create Inbound Rule

Follow the steps below to create an inbound rule for Windows platform firewalls:

1. Open **Control Panel**.
2. Enter **Windows Defender Firewall** into the search box.
3. Click **Windows Defender Firewall** in the search results.
4. Click **Advanced settings**.
5. Click **Yes** on the User Account Control dialog box.
6. Select **Inbound Rules**.
7. Select **New Rule...** under the Actions pane.
8. Select **Program** and click **Next >**.
9. Select **This program path:** and browse to the location of the client application launcher. The 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 checkboxes for **Domain**, **Private**, and **Public**, then click **Next >**.
13. Enter a name and a description for this rule and click **Finish**.
14. Repeat Steps 6 through 13 to create an inbound rule for the client application located at the following path: `%program data%/Intel/Intel Unite/Client/Current/Intel Unite Client.exe`
15. Select **Inbound Rules**.
16. Select **Port** and click **Next >**.

17. Select **New Rule...** under the **Actions** pane.
18. Select **TCP** and select **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 checkboxes for **Domain**, **Private**, and **Public**, then click **Next >**.
22. Enter a name and a description for this rule and click **Finish**.

4.12.8.2 Windows Platform – Create Outbound Rule

Follow the steps below to create an outbound rule for Windows platform firewalls:

1. Open **Control Panel**.
2. Enter **Windows Defender Firewall** into the search box.
3. Click **Windows Defender Firewall** in the search results.
4. Click **Advanced settings**.
5. Click **Yes** on the User Account Control dialog box.
6. Select **Outbound Rules**.
7. Select **New Rule...** under the Actions pane.
8. Select **Program** and click **Next >**.
9. Select **This program path:** and browse to the location of the client application launcher. The 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 checkboxes for **Domain**, **Private**, and **Public**, then click **Next >**.
13. Enter a name and a description for this rule and click **Finish**.
14. Repeat Steps 6 through 13 to create an inbound rule for the client application located at the following path: `%program data%/Intel/Intel Unite/Client/Current/Intel Unite Client.exe`
15. Select **Outbound Rule**s.
16. Select **New Rule...** under the **Actions** pane.
17. Select **Port** and click **Next >**.
18. Select **TCP** and select **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 checkboxes for **Domain**, **Private**, and **Public**, then click **Next >**.
22. Enter a name and a description for this rule and click **Finish**.

4.12.8.3 macOS* Platforms

Follow the steps below to configure the firewall for macOS* 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.

9. Verify that port 443 is open 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.

4.12.8.4 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.

4.12.8.4.1 Define Network Port on the Admin Portal for Hubs

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

1. Sign in to the Intel Unite® Cloud Service on the hub. Use the following link to access the sign in page: https://www.intel.com/content/www/us/en/my-intel/intel-unite-sign-in.html?redirect=https://admin.unitecloud.intel.com/intelunite/admin.
2. Select the Organization that the client is registered with.
3. Select **Hubs and Clients** under the Device Management menu.
4. Click the **Hub** tab.
5. 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.
6. All groups are set to use the same network port.

4.12.8.4.2 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, replacing `<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
```

4.12.8.5 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.

4.12.8.6 Client Pairing

Before a client can be used to connect to a session hosted by a hub, it must be paired with the same organization that the hub is paired with through the admin portal. Part of the client registration process is client preconfiguration, which sets the `OrganizationID`, `OrganizationName`, and `ServerURL` values. Clients can be paired with multiple organizations.

4.12.8.6.1 Client Preconfiguration

The `OrganizationID`, `OrganizationName`, and `ServerURL` values must be set on the client before it can be registered with an organization. These values can be obtained in two ways – DNS TXT record and URI.

Support for DNS TXT record and custom URI depends on the OSs running on client platforms. Due to these differences, not all methods for client configuration are available on all client platforms. For Chrome OS, the URI support requires user to copy and paste the URI into the client application. Table 5 shows the configuration methods supported on each client OS.

Table 5: Client Preregistration Configuration Support per OS

Registration Method	Windows*	macOS*	Chrome OS*	Linux*	iOS*	Android*
DNS TXT Record	Supported	Supported	Not Supported	Supported	Supported	Supported
URI	Supported	Supported	Supported	Supported	Supported	Supported
Manual	Not Supported	Not Supported	Supported	Not Supported	Supported	Supported

DNS TXT Record

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`.

URI (Windows*, macOS* Linux*, Android*, and iOS*)

On the client, browse to the provision device page of the admin portal, and click the link. Follow the steps below to use an URI to set the `OrganizationID`, `OrganizationName`, and `ServerURL` values.

1. Sign in to the Intel Unite® admin portal on the client device.
2. Select the organization that this client device belongs to.
3. Click **Device Management** and select **Provision Device** to open the Provision Device page.
4. Click the link displayed on the Provision Device page (the link starts with intelunite4://) or copy and paste this link into a run command line on the hub. If clicking on the link, a prompt may appear with a request to open the hub application for the Intel Unite® solution. If the prompt appears, click Open Intel Unite® Hub Launcher to open the client application.
5. The client application for the Intel Unite® solution will open to set the `OrganizationID`, `OrganizationName`, and `ServerURL` values. To continue with auto pairing, close the client application and go to Section 5.5.2.2. To continue with enhanced pairing, go to *Hub Manual Pairing Using the admin portal* in Section 4.11.2.4.2.

URI (Chrome OS*)

The `OrganizationID`, `OrganizationName`, and `ServerURL` values can be set manually through the client settings. Follow the steps below to set them manually:

1. Sign in to the Intel Unite® application on the client.
2. Select the organization that this client device belongs to.
3. Click **Device Management** and select **Provision Device** to open the Provision Device page.
4. Copy the URL.
5. Launch the Intel Unite® client.
6. Click the **gear icon** in the upper-right corner to enter client settings.
7. Click **Update Server Information**, paste the URL from provision page of the admin portal into the text box, and click **Save Settings**.

Google* Admin Console (Chrome OS*)

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

Manual Client Provisioning (Android)

1. Launch the Intel Unite application and select the gear icon in the top right corner.
2. Select **Configuration**.
3. Select **Add Organization**.
4. Paste the provisioning URL from the Admin Portal (Device Management - Provision Device).
5. Select **Save Settings**.
6. If necessary, close and re-launch the application.

Confirming OrganizationID, OrganizationName, and ServerURL

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

Windows* Platforms

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

- `HKEY_CURRENT_USER\SOFTWARE\Intel\Intel Unite\Hub\OrganizationID`
- `HKEY_CURRENT_USER\SOFTWARE\Intel\Intel Unite\Hub\OrganizationName`
- `HKEY_CURRENT_USER\SOFTWARE\Intel\Intel Unite\Hub\ServerURL`

The `OrganizationID` is a `REG_SZ` value with the format XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX, where X is a hexadecimal value. This value can be found on the provision page of the admin portal.

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://<admin portal for the Intel Unite® Cloud Service FQDN>/intelunite/api`, where `<admin portal for the Intel Unite® Cloud Service FQDN>` is the fully qualified domain name of the server for the Intel Unite® Cloud Service.

Confirm that the three values match the values in the URI on the provision page of the admin portal (select Provision Device under the Device Management menu on the admin portal).

Non-Windows* Platforms

The `OrganizationID`, `OrganizationName`, and `ServerURL` values are shown in the client settings.

1. Open the client application and click on the **gear icon** in the upper-right corner.
2. Click **Configuration** to display the Configuration page.
3. If Automatic is selected, confirm the `OrganizationID`, `OrganizationName`, and `ServerURL` are populated with the values on the provision page of the admin portal (select Provision Device under the Device Management menu on the admin portal).

4. If Manual is selected, confirm the `OrganizationID`, `OrganizationName`, and `ServerURL` are entered with the values on the provision page of the admin portal (select Provision Device under the Device Management menu on the admin portal).

4.12.8.7 Pair a Client Device

There are three pairing modes that can be used to pair a client device:

- Standard Pairing Mode – This pairing mode does not require the user to click a verification token. If their email address is invalid or cannot be detected, they will be prompted to enter their email address manually.
- Auto Pairing Mode – This pairing mode does not require the user to click a verification token. If their email address is invalid or cannot be detected, an email address is automatically generated for them.
- Enhanced Pairing Mode – This pairing mode requires the user to click a token sent via email. If their email address is invalid or cannot be detected, they will be prompted to enter their email address manually.

The client pairing mode can be changed from the server properties in the admin portal. Follow the steps below to change the client pairing mode:

1. Sign in to the admin portal for the Intel Unite® Cloud Service.
2. Click **Server Management** and select **SERVER PROPERTIES** from the drop-down menu.
3. Click **Edit Properties**, then select properties for the desired pairing mode as described in Table 6 below:

Table 6: Client Pairing Mode Properties

Pairing Mode	Property	Value
Auto	Pairing Mode (Client) - Auto-Generate Email Address	True
	Pairing Mode (Client)	Standard Pairing Mode
Standard	Pairing Mode (Client) - Auto-Generate Email Address	False
	Pairing Mode (Client)	Standard Pairing Mode
Enhanced	Pairing Mode (Client) - Auto-Generate Email Address	False
	Pairing Mode (Client)	Enhanced Pairing Mode

4. Click **Save Changes**.

Note: The first time the client application is started on a Windows* platforms, a Windows* Defender pop-up may appear requesting permission to allow network access for the Intel Unite® application. Until permission is given for the Intel Unite® application, the hub will not be able to connect to the Intel Unite® Cloud Service. In some cases, the hub application may hide the pop-up; to resolve this issue, use Task Manager to close the Intel Unite® application, then click Allow access in the Windows Defender pop-up.

4.12.8.7.1 Standard Pairing Mode

Standard pairing mode requires the user to have a valid email address, but does not require the user to click a verification token. The Intel Unite® app will query the device for the user's email address. If the email address is invalid or cannot be found, the app will prompt the user to enter an email address manually.

Follow the steps below to pair a client device using standard pairing mode:

1. Open the Intel Unite® app on the client device.
    a. If the user's email address auto-populates correctly, click **Submit**.
    b. If the user's email address does not auto-populate correctly, enter the email address manually, then click **Submit**.
2. The device will now automatically pair.

4.12.8.7.2 Auto Pairing Mode

Auto pairing mode requires the user to have a valid email address, but does not require the user to click a verification token. If the email address is invalid or cannot be found, an email address will automatically generate.

Follow the steps below to pair a client device using auto pairing mode:

1. Open the Intel Unite® app on the client device.
2. The device will now automatically pair.

4.12.8.7.3 Enhanced Pairing Mode

Enhanced pairing mode requires the user to click a verification token sent to a valid email address. The Intel Unite® app will query the device for the user's email address. If the email address is invalid or cannot be found, the app will prompt the user to enter an email address manually.

Follow the steps below to pair a client device using enhanced pairing mode:

1. Open the Intel Unite® app on the client device.
    a. If the user's email address auto-populates correctly, click **Submit**.
    b. If the user's email address does not auto-populate correctly, enter the email address manually, then click **Submit**.
2. Open the verification email and click the link for the pairing token.
3. The device will now automatically pair.

4.12.9 Windows Client Software Uninstallation

Follow the steps below to uninstall the client application on a Windows* computer:

1. Locate and launch the `Intel_Unite_Client_vx.x.x.x_x86.mui.msi` file (either on local storage or network storage).
2. Click **Remove**, then click **Next**.

Note: Removing the client application does not remove the device from the admin portal. An administrator must 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.

4.12.9.1 Windows* Client Software Uninstallation – Command Line (Optional)

The Intel Unite® application installer for the client supports command-line uninstallations. The `Intel_Unite_Client_vx.x.x.x_x86.mui.msi`, where `X.X.X.X` is the version, 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 "<.msi Installer Path>" /l*V "<Log Path>" /q
```

4.12.9.2 Windows Client Software Uninstallation Command Line 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.

Table 7: Windows Client Software Uninstallation Command Line Parameters

Parameter	Definition
`/x`	The switch for uninstall.

Parameter	Definition
"<.msi Installer Path>"	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.

4.12.10 Linux Client Software Uninstallation

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`

4.12.11 Client Log File

The client saves a log file in `%temp%\UniteLog\<yyyymmdd>_log.txt`, where `<yyyymmdd>` is the number of the year, month, and day of the log file.

Note: Log files are automatically deleted after 7 days.

5 Admin Portal for the Intel Unite® Cloud Service

The admin portal for the Intel Unite® Cloud Service is the web interface for the Intel Unite® Cloud Service. It enables organization appointed administrators to view and manage the configuration of the Intel Unite® solution running on hub and client devices within an organization.

5.1 Access the Admin Portal

To access the admin portal for Intel Unite® Cloud Service, open a browser and navigate to https://www.intel.com/content/www/us/en/my-intel/intel-unite-sign-in.html?redirect=https://admin.unitecloud.intel.com/intelunite/admin. On the sign in page, enter your Username and Password, then click Sign In. For users without an Intel account, refer to Section 4.2.1 for instructions on how to create an account.

5.2 Admin Portal Common Controls

The banner at the top of the portal contains icons that are always available. These icons provide controls for the Configuration Assistant, logging out of the portal, accessing the help center, setting the display language, and displaying the About page.

5.2.1 Configuration Assistant

Clicking the Configuration Assistant wand icon starts the setup wizard. The setup wizard can be used to pair hub and client devices. Refer to Section 3.3 for more detailed information on how to use the setup wizard.

5.2.2 Log Out

Follow the steps below to log out of the admin portal:

1. Click the user icon from the common controls area of the admin portal.
2. Select **Logout** from the drop-down menu.

5.2.3 Change the Display Language

To change the display language, click the **language globe icon**, select a language, then click **Apply**.

Available languages:

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

5.2.4 Help Center

The Help Center provides documentation that assists in the use of the Intel Unite® Cloud Service. To access the Help Center, click the **Help Center question mark icon** at the top-right corner to open the Help Center panel,

which contains the following controls:

- Back arrow icon – Click the back arrow icon to scroll up one page.
- Forward arrow icon – Click the forward arrow icon to scroll down one page.
- Home icon – Click the Home icon to display the table of content for help.
- Link to Support – Click the Support link to navigate to the support website for the Intel Unite® Cloud Service.
- Link to About – Click the About link to display information about Intel Unite® Cloud Service.

5.2.5 Global Notifications

Global notifications appear in the banner at the top of the admin portal with the following color-coding:

- Red (error message)
- Yellow (warning message)
- Green (information message)

To dismiss a notification, click the circle x located at the right edge.

5.2.6 About

The **About** link in the admin portal displays the version and other information about the Intel Unite® Cloud Service. For users that are logged in, the About details will also include the Organization ID. Click **About** in the upper-right corner of the page to view details.

5.3 Organizations

After login, the Organizations page is displayed. The Organizations page displays a list of organization that the user belongs to. A user with the Edit Server Management permission can create a new organization, edit an existing organization, and delete an existing organization.

5.3.1 Create a New Organization

Follow the steps below to create a new organization:

1. Click the **Create New Organization** button.
2. Enter the **Organization Name**. The name must be at least 4 characters long.
3. Enter a **Description** for the organization. The description must be at least 4 characters long.
4. Click the **Save** button.

5.3.2 Select an Organization

To manage the configuration for an organization, it first has to be selected. To select an organization, click the name of the organization. After clicking on the name of the organization, the Portal will display the Hubs and Clients page for that organization.

Note: Once an organization has been selected, any changes made will only affect the selected organization.

5.3.2.1 Set Privacy Selection

Upon first selecting an organization that is not created using the setup wizard, the Privacy Selection dialogue will be displayed to configure the data collection policy for the organization. This can be changed by editing the **Privacy Mode** server property in the admin portal.

The available privacy policies are:

- **Share anonymous data with Intel** – Telemetry data is collected and forwarded to Intel.
- **Do not share anonymous data with Intel** – 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.

5.3.3 Edit an Existing Organization

Follow the steps below to edit an existing organization:

1. Identify the organization that needs to be updated and click the **Edit Organization** button for that organization.
2. Update the organization properties.
3. Click the **Save Changes** button.

5.3.4 Delete an Organization

Follow the steps below to delete an organization:

1. Identify the organization that needs to be deleted and click the **Delete Organization** button for that organization.
2. Confirm the deletion by clicking the **Delete** button in the Confirm Organization Deletion dialog box.

5.3.5 Find an Organization

For a user that belongs to many organizations, use the Search box to find organizations by string:

1. Enter a string in the search box at the top of the page.
2. Click the **Search** button to list all organizations that have the string in the name of the organization.

5.4 Intel Unite® Cloud Service Management

After selecting the organization from the Organizations page, the portal displays three main menus and the default page, which is the Hubs and Clients page. The three menus are:

- Device Management
- Server Management
- User Management

Click **Organizations** at the top of the page to return to the Organizations page.

5.5 Admin Portal Device Management Menu

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

The Device Management menu contains links to the following pages:

- **Hubs and Clients** – This is the default page after logging in. This page displays:
  - The hub or client groups.
  - Devices that are paired and registered with this organization.
- **Configurations** – This page provides the ability to create and make changes to hub and client configurations. These configurations will be assigned to device groups or to devices.
- **Features/Apps** – This page provides the ability to manage feature and app packages, allowing packages to be uploaded, approved, and to be deleted. As new version of feature and app packages are uploaded and approved, the old versions can be deleted.

- **Reserved PINs** – By default, the PIN for a hub will change after a period of time. This page allows assigning a static PIN to a hub, meaning the PIN will not change over time. If a hub is assigned a static PIN, this page allows the hub to be reset to use a changing PIN.
- **Custom Metadata** – This page provides the ability to create additional fields for devices. The fields are free form string fields. This is useful for adding more information for each device (for example, creating a field called “location” will allow recording the location of the hub for later reference).
- **Provision Device** – This page provides a URL that contains all the information needed for a hub or client device to contact the Intel Unite® Cloud Service to pair or register. This is the same page that is shown when clicking the Show provisioning URL link on the login page.
- **Auto Pairing Management** – This page provides the management of auto pairing tokens. These tokens are valid for a predefined period time, and this page shows when each token will expire. This page also provides the ability to delete expired tokens.

The device management menu contains the following Quick Actions:

- **Pair Hub** – This quick action is used when manually pairing a hub.
- **Auto Pairing** – This quick action displays a dialogue box of a randomly generated pairing token along with information on how to use the pairing token. The token and the time expiration are available on the Auto Pairing Management page.
- **Upload Package** – This quick action is used to upload feature/apps packages.
- **Create Meeting** – This quick action is used to display a page with a meeting URL. Send this URL to other users to allow them to join the same session for the Intel Unite® solution. This is the same page that is shown when clicking the Create Meeting link on the login page.

5.5.1 Device Management – Pages

The following subsections provide details for each page link that is available under the Device Management menu.

5.5.1.1 Hubs and Clients Page

The Hubs and Clients page is where hub and client devices are managed and is the page that is displayed after selecting an organization on the Organizations page.

Hub and client devices are organized in groups. A group of devices will be assigned the same configuration.

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 that are associated with an Active Directory group are denoted in the AD Organization Unit column by the icon shown below.

Hover over the icon to display the Active Directory group name.

Admin portal groups that have a configuration assigned are denoted by a gear icon in the configuration column. Hover over the icon to display the configuration name. In order for a device to function, it must be assigned to a group that have a configuration. A configuration is container that holds packages which are features, apps, and settings for devices.

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.

5.5.1.1.1 Select Action Menu

The Select Action menu on the Groups page provides actions that can be applied to a selected group. The list below describes 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. Available actions:
    - **Rename group**: To rename a group, click **Edit Group** next to the group name. The root group cannot be renamed.
    - **Add/Update AD OU association**: To add or update an AD OU association, click the **Assign** button, enter the distinguished name of the OU that contains the devices that will receive settings from the configuration that is assigned to this group, and click **Assign**. The distinguished name of an OU can be obtained by looking at the Attribute Editor tab of the OU property.
    - **Remove AD OU association**: 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 receive settings from the configuration assigned to the 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 group association. The configuration assigned to the admin portal group with the Active Directory group 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 configuration from a group, select the 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.

5.5.1.1.2 Move and Delete Devices

Follow the steps below to move a device from one group to another group:

1. Select a device by placing a check in the checkbox next to the device name.
2. Click the move group arrow icon.
3. Select a group.
4. Click **Move** in the Confirm Move dialogue box.

Follow the steps below to delete a device:

1. Select a device by placing a check in the checkbox next to the device name.
2. Click the trash can icon.

3. Click the **Delete** button in the Confirm Device Deletion dialogue box.

5.5.1.1.3 Configure Group Properties

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

Edit Hub Group Properties

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

Changes made using the steps above will apply to all devices in the group.

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. Follow the steps below to override the group configuration for a device:

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

Changes made using the steps above will apply to all devices in the group.

Hub Group Properties

Table 8 describes the hub properties that are in the hub packages. A dynamic value of "Yes" means the property value will be applied without restarting the device's Intel Unite® application. A dynamic value of "No" means the property value will be applied the next time the device's Intel Unite® application is restarted.

Table 8: Intel Unite® Solution Hub Properties

Property Name	Description	Dynamic	Value Type	Default Value
Allow Users to Reset Locked Sessions	Set to True, users should be able to reset a locked session when connecting to the hub.	No	Boolean	True
Available Displays	Set this property to specify the displays that are connected to the hub. 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 for Intel Unite® Cloud Service. Set the number of physical displays in which Intel Unite® solution will be displayed. Format: 1,2,3 or empty for all displays.	No	String	

Property Name	Description	Dynamic	Value Type	Default Value
Available Touch Displays	Set this property to specify the displays that are connected to the hub with touch support. 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.	No	String	
Background Color	Set this property to specify the background color displayed on the hub. Enter the palette number for the background color. The following website will convert a hexadecimal palette number into the corresponding color: https://www.w3schools.com/colors/colors_converter.asp.	Yes	HEX	#0071C5
Background Image URL	Set this property to specify a background image displayed on the hub. Enter the URL to the background image. It can be a local image.	Yes	String	
Background Instructions	Set this property to specify instructions for use to be displayed on the hub. Enter the instructions to be displayed on the hub display with the following reserved strings: • `{pin}` – replace with PIN • `{maxoccupancy}` – displays the calculated maximum occupancy for the hub. • `{n}` – new line For example: 1. Install Intel Unite® app`{n}`2. Enter PIN `{pin}{n}`3. Click Present`{n}`Maximum Occupancy:`{maxoccupancy}`	Yes	String	
Background Instructions Color	Set this property to specify background color for the instruction section that is displayed on the hub. Enter the palette number for the background color. The following website will convert a hexadecimal palette number into the corresponding color: https://www.w3schools.com/colors/colors_converter.asp.	Yes	HEX	#FFFFFF
Background Instructions Font	Set this property to specify the font that will be used to display the instructions displayed on the hub. Enter the font for the background instructions. Default font is Intel Clear. To identify the fonts installed on the hub, search for “Fonts” in the search box by the start menu, click on the “Fonts (Control Panel)” link to open the Fonts Manager displaying the fonts installed on the hub.	Yes	String	
Background Instructions Title	Set this property to specify a title to be displayed above the instructions on the hub. Enter a title. No reserved words.	Yes	String	Welcome
Disable Keyboard Command Keys	Set this property to disable keyboard entry on the hub. True: Disables keyboard commands. False: Enables keyboard commands.	Yes	Boolean	True
Enable Client Screen Preview	Allow moderators to preview client screens.		Boolean	True
Enable Hub as Presenter	Set this property to enable the hub as a presenter allowing the hub to present to remote users. 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	Set this property to enable the hub to check-in with the server, allowing the server to determine when a hub stops functioning. True: Enables hub check-in reporting. False: Disables hub check-in reporting.	Yes	Boolean	False
Enable PIN Refresh During Session	Set this property to allow the PIN to change while the hub is utilized in a session. True: Enables the PIN to change during a session. False: Disables the PIN from changing during a session.	Yes	Boolean	True
Enable TLS 1.1	Set this property to enable encryption using TLS 1.1. Recommend setting this property to True. True: Enables TLS 1.1. False: Disables TLS 1.1.	Yes	Boolean	True
Enable TLS 1.2	Set this property to enable encryption using TLS 1.2. Recommend setting this property to True. True: Enables TLS 1.2. False: Disables TLS 1.2.	Yes	Boolean	True
Make Background Clock Visible	Set this property to allow the clock to be visible in the lower right corner of the hub display. True: Shows background clock. False: Hides background clock.	Yes	Boolean	True
Make Background Visible	Set this property to display the background. True: Shows background. False: Hides background.	Yes	Boolean	True
Make Content Toolbar Visible	Set this property to display the content toolbar on the right side of the hub display. True: Shows content toolbar. False: Hides content toolbar.	Yes	Boolean	True
Make PIN Visible	Set this property to display the PIN in the upper right of the hub display. True: Shows PIN. False: Hides PIN.	Yes	Boolean	True
Maximum Occupancy	Set this property to specify the maximum occupancy of a room for a hub. Range: 1-2000	Yes	Integer	1
Moderator Mode	Set this property to allow sessions hosted by this hub to be moderated. 0 = No Moderation (default) 1 = Self-Promoted Moderation (first user to request to be moderator will become the moderator for the session) 2 = Strict Moderation mode (only a person on the moderator allow-list can be a moderator) Refer to Section 5.7.2.3 for details.	Yes	Integer	0
Moderator Mode - Screen Preview	0 = No preview 1 = Preview in strict moderation Refer to Section 5.7.2.3 for details.			
Network Port	Set this property to the network port to be used by the hub. Recommend setting to 0 unless a specific port is needed. Enter the port that the hub is listening to for clients. Default 0—random.	No	Integer	0
PIN Color	Set this property to change the color of the PIN that is displayed on the hub. Enter the palette number for the PIN. The following website will convert a hexadecimal palette number into the corresponding color: https://www.w3schools.com/colors/colors_converter.asp.	Yes	HEX	#FFFFFF

Property Name	Description	Dynamic	Value Type	Default Value
PIN Size	Set this property to change the font size of the PIN that is displayed on the hub. Enter an integer for the font size.	Yes	Integer	48
PIN Transparency	Set this property to change the transparency of the PIN that is displayed on the hub. Enter the opaqueness of the PIN with a range of 0 to 100 (default), where 0 is completely transparent and 100 is completely opaque.	Yes	Integer	100
QoS Maximum Message Size	Set this property to change the maximum message size that are sent to and from the hub and clients. Enter the maximum size in bytes of a message. Changing this property up or down may affect performance.	Yes	Integer	65535
QoS Message Queue Ratio	Set this property to change the message queue size ratio for different message priorities. Enter the message queue size. This ratio is used to determine when messages are handled based on message priority. A larger value will cause higher priority messages to be handled more often than lower priority messages. A smaller value will cause lower priority messages to be handled more often.	Yes	Integer	4
Password to close app	Set this property to allow the closure of the hub application when a password is entered. Enter a password. Only applicable if Disable Keyboard Command Keys is False.	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	Set this property to allow the background image to stretch to fill the hub display. True: Stretches the background image. False: Does not stretch the background image.	Yes	Boolean	True
Visibility Time for Notification Messages	Set this property to change the time that notification messages are displayed on the hub. Enter the time in seconds that the notification message is visible.	Yes	Integer	3

5.5.1.1.4 Hub Feature/App Properties

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

Table 9: File Sharing Module Properties

Property Name	Description	Dynamic	Value Type	Default Value
Allow Moderators to Receive Files	Set this property to allow moderators to receive files using the File Sharing app. True: Enables moderators to receive files. False: Does not allow moderators to receive files.	Yes	Boolean	True
Allow Moderators to Share Files	Set this property to allow moderators to share files using the File Sharing app. True: Enables moderators to share files. False: Does not allow moderators to share files.	Yes	Boolean	True

Property Name	Description	Dynamic	Value Type	Default Value
Allow presenters to Receive Files	Set this property to allow presenters to receive files using the File Sharing app. True: Enables presenters to receive files. False: Does not allow presenters to receive files.	Yes	Boolean	True
Allow presenters to Share Files	Set this property to allow presenters to share files using the File Sharing app. True: Enables presenters to share files. False: Does not allow presenters to share files.	Yes	Boolean	True
Allow viewers to Receive Files	Set this property to allow viewers to receive files using the File Sharing app. True: Enables viewers to receive files. False: Does not allow viewers to receive files.	Yes	Boolean	True
Allow viewers to Share Files	Set this property to allow viewers to share files using the File Sharing app. True: Enables viewers to share files. False: Does not allow viewers to share files.	Yes	Boolean	True

Table 10: Remote View Module (Hub) Properties

Property Name	Description	Dynamic	Value Type	Default Value
In-Room Experience Only	Set this property to allow or prevent remote users from viewing presentations. True: Disables remote viewing. False: Enables remote viewing.	Yes	Boolean	False
JPEG Compression	Set this property to change the compression ratio used for static content. Enter the compression ratio for non-AV content sharing. A higher value may result in lower quality of presentations but may improve sharing performance.	Yes	Integer	85
Tile Size	Set this property to change the tile size used for static content. Enter the tile size for non-AV content. A higher value may result in lower quality of presentations but may improve sharing performance.	Yes	Integer	128

Table 11: Screen Sharing Module (Hub) Properties

Property Name	Description	Dynamic	Value Type	Default Value
Audio Video Streaming Support	Set this property to allow or prevent AV streaming on the hub. 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

5.5.1.1.5 Edit Client Group Properties

Follow the steps below to edit client group properties:

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 as desired.
6. Click **Save Changes** to apply the modifications.

Changes made using the steps above will apply to all devices in the group.

5.5.1.1.6 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. Follow the steps below to override the group configuration for a device.

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.

Changes made using the steps above will only apply to the device.

5.5.1.1.7 Client Group Properties

The tables in this section describe the client properties that are in the client packages.

Table 12: Intel Unite® Client Version Properties

Property Name	Description	Value Type	Default Value
Allow Apps to Open Downloads folder	Set this property to allow or prevent apps access to the Download folder. Setting this property to False may cause some apps to not function properly. 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	Set this property to allow or prevent apps to save files. Setting this property to False may cause some apps to not function properly. True: Enables apps to save files. False: Disables apps from saving files.	Boolean	True
Allow Host from Your Device	Set this property to allow the client device to be a host of sessions for the Intel Unite® solution. Only applicable for devices that meet the Intel vPro® brand. 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	Set this property to filter which file extensions are available to the client. Enter the extensions that the File Manager will filter out. Multiple extensions can be defined, each separated with a comma. A blank value allows all file extensions.	String	
Disable User Profile Updates	If set to True, users will not be able to update their user profiles in the client app.	Boolean	False
Enable Client Screen Preview	Allow moderators to preview client screens.	Boolean	False

Property Name	Description	Value Type	Default Value
Enable PIN Refresh During Session	Set this property to allow the PIN to change while the hub is utilized in a session. True: Enables the PIN to change during a session. False: Disables the PIN from changing during a session.	Boolean	True
Enable TLS 1.1	Set this property to enable encryption using TLS 1.1. Recommend setting this property to True. True: Enables TLS 1.1. False: Disables TLS 1.1.	Boolean	True
Enable TLS 1.2	Set this property to enable encryption using TLS 1.2. Recommend setting this property to True. True: Enables TLS 1.2. False: Disables TLS 1.2.	Boolean	True
Host from Your Device Listen Port	Set this property to the network that is used when the client hosts a session. The port used for the peer-to-peer feature. Only applicable for devices that meet the Intel vPro® brand.	Integer	0
Maximum File Size	Set this property to limit the maximum size a file allowed. Enter the maximum file size allowed in bytes.	Integer	214783648
QoS Message Queue Ratio	Set this property to change the message queue size ratio for different message priorities. Enter the message queue size. This ratio is used to determine when messages are handled based on message priority. A larger value will cause higher priority messages to be handled more often than lower priority messages. A smaller value will cause lower priority messages to be handled more often.	Integer	4

Table 13: Remote View Module (Client) Properties

Property Name	Description	Value Type	Default Value
Currently, no properties are available for this module.	N/A	N/A	N/A

Table 14: Screen Sharing Module (Client) Properties

Property Name	Description	Value Type	Default Value
JPEG Compression	Set this property to change the compression ratio used for static content. Enter the compression ratio for non-AV content sharing. A higher value may result in lower quality of presentations but may improve sharing performance.	Integer	85
Tile Size	Set this property to change the tile size used for static content. Enter the tile size for non-AV content. A higher value may result in lower quality of presentations but may improve sharing performance.	Integer	128

5.5.1.1.8 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 session. Only plugins that have Disable plugin for non-moderators module property set to True will be hidden. The module property can be found in the Group Details of a configuration.

For non-moderated sessions, all participants will have access to plugins/apps, even when the Disable plugin for non-moderators is set to True for the plugins/apps.

Older plugins may not support moderation mode and will require the use of a newer version of those plugins. Follow these steps to install the new version.

Download the new plugin version before starting the steps below.

1. Remove the old plugin version from client configurations.
    a. Select **Configurations** from the Device Management menu.
    b. Click **Client Configurations** to display all client configurations.
    c. Click the **Edit** button assoicated with the configuration that has the old plugin version.
    d. Remove the plugin by clicking the **minus sign (-)** next to the old plugin.n.
    e. Click **Save Changes**.
    f. Repeat these steps for all configurations that has the old plugin version.
2. Delete the old plugin version.
    a. Select **Features/Apps** from the Device Management menu.
    b. Click **Client Features/Apps** to display all the client plugins.
    c. Click the **Delete** button associated with the old plugin version.
    d. Confirm the deletion by clicking **Delete** when the Confirm Delete Feature/App window pops up.
3. Upload and approve new plugin version.
    a. Click **Package Approval** on the Features/Apps page.
    b. Click **Upload Package** in the upper right corner.
    c. Browse to the location of the new plugin version and select the `.cab` file.
    d. Click **Open** to upload the plugin
    e. Confirm a Success message pops up and the plugin version is listed in the Package Approval tab.
    f. Click the **Approve** button associated with the new plugin version.
    g. Confirm a Success message pops up and the new plugin version is listed in the Client Features/Apps tab.
4. Add new plugin version to client configuration.
    a. Select **Configurations** from the Device Management menu.
    b. Click the **Client Configurations** to display all client configurations.
    c. Click the **Edit** button associated with the configuration that will have the new plugin version added.
    d. Add the plugin by clicking the **plus sign (+)** next to the new plugin version.
    e. Click **Save Changes**.
    f. Repeat these steps for all configurations that needs the new plugin version.

5.5.1.2 Configurations Page

Configurations are containers that holds packages which are features, apps, and settings for hub and client devices.

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 a container that holds packages which are features, apps, and settings for a device. Each configuration consists of packages. Most packages have properties that can be changed to alter the behavior of the device.

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.

5.5.1.2.1 Create Configuration

Follow the steps below to create a new configuration:

1. On the Configurations page, click **Create Configuration**. The Create Configuration view will be displayed.
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 features 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 features or an app, click the **white minus sign (-)** 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.

5.5.1.2.2 Edit Configuration

Follow the steps below 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, then select the desired version.
4. To add a features or an app, click the **white plus sign (+)** 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 features or apps, click the **white minus sign (-)** 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.

5.5.1.2.3 Delete a Configuration

Follow the steps below 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 Confirm Delete Configuration dialog box.
3. In the confirmation dialog box, click **Yes** to delete the configuration, or 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.

5.5.1.3 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.

5.5.1.3.1 Upload a Package

Features and apps for the Intel Unite® solution are distributed using Packages in cab file format. These apps packages can be downloaded from the Intel showcase website while feature packages are downloaded from the admin portal.

Follow the steps below to upload a package:

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

5.5.1.3.2 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.

5.5.1.3.3 View Hub/Client Features/Apps

To view a list of hub or client apps and features on the Features/Apps page, click the **Hub Features/Apps** tab or the **Client Features/Apps**tab. From that 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 module, click **Delete**. The Confirm Delete Module dialog box will open. Click **Yes** to delete the module. Click **No** to cancel the deletion. Only modules not in use can be deleted.

5.5.1.4 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.

5.5.1.4.1 Assign a Static PIN to a Hub

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

Method 1 – 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**.

5.5.1.4.2 Unassign a Static PIN for a Hub

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

Method 1 – Manually unassign each hub PIN

1. Find the hub with the static PIN assigned in the list of hubs on the Reserved PIN page.
2. 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 to *.
3. Save the .csv file.
4. Click the **Import Reserved PINs from CSV** 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**.

5.5.1.4.3 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**.

5.5.1.5 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.

5.5.1.5.1 Create or Delete Metadata

Follow the steps below 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.

Follow the steps below to delete metadata:

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

5.5.1.5.2 Edit Metadata Value

Follow the steps below 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.

5.5.1.6 Provision Device Page

The Provision Device page displays a URL. The URL can be used to pair hubs and register clients.

The URL contains three important pieces of information – the server URL, the organization ID, and the organization name. These values are needed to pair hubs and register clients. The organization ID and organization name are set during the creation of the organization. The URL string is not case-sensitive.

5.5.1.7 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.

Follow the steps below to generate a token:

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

Follow the steps below to delete a token:

1. Place a check in the checkbox next to the token. More than one token can be selected.
2. Click the **Delete Tokens** button in the upper-right corner. The Confirm Delete Token window will open.
3. Click the **Delete** button to delete the token or the **Cancel** button to keep the token.

5.5.2 Device Management – Quick Actions

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

5.5.2.1 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 4.11.2.4 for more information about hub pairing.

5.5.2.2 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.

Follow the steps below 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.

Follow the steps below 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=<machine name>`, where `<token>` is the value from Step 2, `<email address>` is the email address that will receive the registration email, and `<machine name>` is the name of the client system.
4. Click the **Close** button to close the Generate Auto Pairing Token dialog box.

5.5.2.3 Upload Package

Follow the steps below to use the Upload Package Quick Action:

1. On the Device Management menu, click the **Upload Package** button. An Open dialog box will be displayed.
2. Use the Open dialog box to select the file to upload, then 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.

5.5.2.4 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® Cloud Service add-in for Microsoft* Outlook.

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*, macOS*, and iOS* clients) or a web browser (Windows*, macOS*, and iOS* clients).

Follow the steps below to join a meeting using the Run command window on a Windows* device:

1. Copy the meeting 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**.

Follow the steps below to join a meeting using a web browser on a Windows* or macOS* device:

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

5.6 Admin Portal Server Management Menu

The Server Management menu includes the following menu items:

- Telemetry – This page displays telemetry data that are collected.
- Logs – This page displays the logs that have been generated, which can be used to debug unexpected behaviors.
- Server Properties – This page displays server properties and allows to edit them.
- Organizations – This page displays a list of organizations the user belongs to. A user with the Edit Server Management permission can create a new organization and edit existing organizations.

5.6.1 Telemetry Page

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

- Connections and presentations 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.
- Hubs Per OS – Operating systems running on the hubs associated with the server and the count of each operating system.
- Clients Per OS – Operating systems running on the clients paired with the server and the count of each operating system.
- Plugin Launches (Hub) – Names of the apps used on hubs, 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.

Telemetry data controls:

- Click the **Reset** button to reset the telemetry data and clear the graphs.
- Click the **Refresh** button to get the latest information and update the graphs.
- Click the **Export** button to export a .csv file of the telemetry data to the user's download directory.

5.6.2 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.

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.

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

5.6.3 Server Properties Page

The Server Properties page displays a list of server properties, the organization name, and the organization description. 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. Table 15 describes the server properties.

Table 15: Server Properties

Setting Name	Description	Value Type	Default Value
Admin Email	Set this property to receive email targeted for the organization administrator. The organization administrator can be setup to receive emails regarding notifications of hub failures, when a user request to be added to the moderator allowlist, and other administrator-specific emails. Enter the organization administrator email address.	String	Blank
Admin Portal Path	Overrides the default URL to the admin portal. User for URLs in admin portal emails. Useful when using a load-balanced server pool.	URL	
Allowlist	Set this property to change the email address domains that a user can use to register their devices. Enter the email addresses allowed to register clients with the server. The wildcard * is allowed (for example, *domain.com). Can enter multiple values separated by commas.	Array of Strings	*
Auto-Remove Inactive Clients	Days until an inactive client is automatically removed. Minimum 7 days, maximum 365 days.	Integer (days)	60
Configuration Cache Updates	Set this property to allow configuration cache updates. True: Allows configuration cache updates for device and groups. False: Prevents configuration cache updates for device and groups.	Boolean	False
Denylist	Email addresses not allowed to pair clients with the server. The wildcard * is allowed (for example, *@domain.com). Multiple addresses must be separated by commas.	List	
Maintenance Service Language	Set this property to change the language of the text that is sent to the Admin Email address due to maintenance service execution. Choose one of the languages listed below. Language options used for admin portal email notifications include: • zh-cn – Chinese (Simplified) • zh-tw – Chinese (Traditional) • de – German • en – English • es – Spanish • fr – French • it – Italian • ja – Japanese • ko – Korean • pt – Portuguese	String	en

Setting Name	Description	Value Type	Default Value
OTA Updates Enabled	Set this property to allow or prevent the update of clients and hubs automatically. 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 the installation msi on each device.	Boolean	True
Pairing Mode (Client)	Enhanced pairing mode requires users to verify their email address to pair. Standard pairing mode allows users to pair without email verification.	Pairing Mode	Standard Pairing Mode
Pairing Mode (Client) - Auto-Generate Email Address	Standard pairing mode requires client apps to provide an email address. The app will try to resolve the user's email address automatically. If the email address can't be resolved, setting this to false will prompt the user to enter their email address; setting this to true will auto-generate an email address without prompting the user.	Boolean	False
Pairing Mode (Hub)	Ehanced pairing mode requires hubs to verify to pair. Standard pairing mode allows hubs to pair without verification.	Pairing Mode	Standard Pairing Mode
Percent of Maximum Occupancy	Set this property to define a percentage of maximum occupancy. For example, if a hub is configured to have a maximum occupancy of 100, and Percent of Maximum Occupancy is set to 50, the max occupancy of that hub will be indicated as 50 instead of 100.	Integer	100
PIN Expiration Time	Set this property to change the time before a PIN is considered expired and is refreshed with a new one. Enter the minutes between PIN refreshes.	Integer	5
Privacy Mode	This is a read only property, showing the privacy mode set during the setup of the organization. Share anonymous data with Intel: Telemetry data is collected and forwarded to Intel. Do not share anonymous data with Intel: 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 selecting an organization from the admin portal during the creation of an organization using the Setup Wizard.
Protected Role List	Set this property to change which roles are protected from modification. Enter the admin portal user roles that cannot be edited or deleted for the Intel Unite® Cloud Service.	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

Setting Name	Description	Value Type	Default Value
Verify Plugins	Set this property to allow or prevent the verification of apps before loading. True: Verifies feature and apps modules before loading. False: Does not verify feature and apps modules before loading.	Boolean	True

In addition to the server properties, a button is available at the top the Server Properties page:

- Test AD connection – Click to verify AD FS settings are correctly set.

5.7 Admin Portal User Management Menu

The User Management menu groups all the pages that relates to user management.

The User Management menu includes the following pages:

- Users – This page provides the management of users in the organization that uses the Intel Unite® Cloud Service, allowing changing user properties, and deleting users.
- Moderators – This page provides the management of moderators. A moderator is a user that controls a moderated session. From this page, a user can be assigned to be a moderator or a user's moderator status can be revoked.
- Roles – This page provides the management of roles. Roles are a collection of specific permissions. Custom roles can be created or deleted.

5.7.1 Users Page

The Users page of the admin portal displays a list of all admin portal users. The Users page enables administrators to add, edit, delete, and reassign user roles, as described in the next sections. Use the Search boxes at the top of the 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.

5.7.1.1 Add a User

Follow the steps below to add a new user:

1. On the Users page of the admin portal, click the **Add User** button. The Add User page opens.
2. Complete the following options on the Add User page:
    - User Name – The user ID or the email address of the user to be added. The user to be added must have an account with Intel and have signed into the admin portal at least once.
    - Select Role – The user's role which determines the permissions for the user. The 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 to that role.
3. After filling in the user information click **Save** to add the user.

For Active Directory users, add the AD user to the appropriate AD OU that has the desired permissions defined by the corresponding role created for that AD OU. Refer to Section 5.7.3.1 for details about creating a role for an AD OU. AD users are not added to the admin portal for Intel Unite® Cloud Service and are managed through Active Directory.

5.7.1.2 User Actions

Users with User Management permissions can use the Users page to delete users and assign users to different roles:

- Delete User – Place a check in the box next to the username. 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 username. 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.

5.7.2 Moderators Page

The Moderators page displays a list of users who have moderator privileges. This page enables users with Moderator Management permissions to add, manage, and remove users from the moderator list. Use the Search boxes at the top of the page to find users in the moderator list. Enter a string and click **Search** to display a list of users who have the entered string in the user's name. Use the **Clear** button to clear the search results.

5.7.2.1 Add a Moderator

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

Follow the steps below to add a moderator individually:

1. Click **Add Moderator**.
2. Enter the moderator's name and email address.
3. Click **Save**.

Follow the steps below to add moderators as a group:

1. Click **Import Moderators from CSV**
2. Select the .csv file that contains the list of moderators.
3. Click **Open**.

5.7.2.2 Delete a Moderator

Follow the steps below to delete a moderator:

1. On the Moderators page, place a check in the box next to the username and select **Delete**. A confirmation dialog box will open.
2. Click **Yes** to delete the user or click **No** to close the confirmation dialog box without deleting the moderator.

5.7.2.3 Moderated Sessions

For a session to be moderated, the moderator functionality mode needs to be set for the hub device. To set the moderator functionality mode, modify the configuration hub properties Moderator Mode. Refer to Section 5.5.1.1.3 for more information about hub properties. The available Moderator Modes are:

0 – No Moderation

Default mode. No moderators are in the session, and all participants have equal rights to view and present.

1 – Self Promote

The session is unmanaged 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. Becoming a moderator during the session does not result in the user being added to the moderator allowlist.

2 – Strict

The session is managed only by the users that are on the moderator allowlist. 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 email to the administrator, who can add the participant to the moderator allowlist from the admin portal.

5.7.2.4 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 (preview in strict moderation).
- Moderator Mode - Screen Preview must be set to 1 (preview in strict moderation).

Client properties:

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

5.7.3 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
- Device Management

If a role is assigned with an AD OU, a URL will be shown at the top of the page. This URL is used to sign in to the admin portal.

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. Table 16 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.

Table 16: Built-In Roles Permissions

Permissions for Each Role	Administrator	Device Pairing Manager	Moderator Manager	No Permissions
Device Management Permission	Read and Write			
Device Pairing Management Permission	Read and Write	Read and Write		
Role Management Permission	Read and Write			Administrator
User Management Permission	Read and Write			Device Pairing Manager
Server Management Permission	Read and Write			Moderator Manager
Moderator Management Permission	Read and Write		Read and Write	No Permissions
Organization Management Permission	Read and Write			

Table 17: Device Management Permissions

Admin Portal Feature	View (View Devices, Groups, Features/Apps, Configurations, Device Properties)	Edit (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
Configurations, 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		
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

Admin Portal Feature	View (View Devices, Groups, Features/Apps, Configurations, Device Properties)	Edit (Read and Edit/Delete These Items, Upload Packages)
Create Organization		
Delete Organization		
Edit Organizations		
List Organization		

Table 18: Device Pairing Management Permissions

Admin Portal Feature	View (View Devices, Groups, Features/Apps, Configurations, Device Properties)	Edit (Read and Edit/Delete These Items, Upload Packages)
Login	x	x
Devices		
Configurations, 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		
Create Organization		
Delete Organization		
Edit Organizations		
List Organization		

Table 19: Role Management Permissions

Admin Portal Feature	View (View Devices, Groups, Features/Apps, Configurations, Device Properties)	Edit (Read and Edit/Delete These Items, Upload Packages)
Login	x	x
Devices		
Configurations, Features/Apps, Packages		
Reserved PINs		
Pair Hub		
Auto Pair		
Telemetry		
Logs		
Server Properties		
Users		
Moderators		

Admin Portal Feature	View (View Devices, Groups, Features/Apps, Configurations, Device Properties)	Edit (Read and Edit/Delete These Items, Upload Packages)
Roles	• Get role list • Get details of role • Get permission list	• Create role • Update role • Delete role • Bulk role deletion
Device Tree		
Create Organization		
Delete Organization		
Edit Organizations		
List Organization		

Table 20: User Management Permissions

Admin Portal Feature	View (View Devices, Groups, Features/Apps, Configurations, Device Properties)	Edit (Read and Edit/Delete These Items, Upload Packages)
Login	x	x
Devices		
Configurations, 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		
Create Organization		
Delete Organization		
Edit Organizations		
List Organization		

Table 21: Server Management Permissions

Admin Portal Feature	View (View Devices, Groups, Features/Apps, Configurations, Device Properties)	Edit (Read and Edit/Delete These Items, Upload Packages)
Login	x	x
Devices		
Configurations, Features/Apps, Packages		

Admin Portal Feature	View (View Devices, Groups, Features/Apps, Configurations, Device Properties)	Edit (Read and Edit/Delete These Items, Upload Packages)
Reserved PINs		
Pair Hub		
Auto Pair		
Telemetry	Get metrics reports Export metrics	
Logs	Get logs	
Server Properties	• Get server property list • Get list of organization the user belongs to	• Update server properties • Update and delete organization the user belongs to
Users		
Moderators		
Roles		
Device Tree		
Create Organization		
Delete Organization		
Edit Organizations		
List Organization		

Table 22: Moderator Management Permissions

Admin Portal Feature	View (View Devices, Groups, Features/Apps, Configurations, Device Properties)	Edit (Read and Edit/Delete These Items, Upload Packages)
Login	x	x
Devices		
Configurations, 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		
Create Organization		
Delete Organization		
Edit Organizations		
List Organization		

Table 23: Moderator Management Permissions

Admin Portal Feature	View (View Devices, Groups, Features/Apps, Configurations, Device Properties)	Edit (Read and Edit/Delete These Items, Upload Packages)
Login	x	x
Devices		
Configurations, Features/Apps, Packages		
Reserved PINs		
Pair Hub		
Auto Pair		
Telemetry		
Logs		
Server Properties		
Users		
Moderators		
Roles		
Device Tree		
Create Organization		x
Delete Organization		x
Edit Organizations		x
List Organization	x	x

5.7.3.1 Create a New Role

For users that require permissions that are not provided by the built-in roles, a new role with custom permissions can be created. 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 OU, meaning all domain users directly assigned to the Active Directory OU will have the same permissions. If an Active Directory OU contains subgroups, the users in the subgroups will not be recognized and will not have any permissions.
- 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 OU, click the **Assign** button next to the Active Directory Group text box. Enter the distinguished name of the OU that contains the users and click **Assign**. The Distinguished name of an OU can be obtained by looking at the Attribute Editor tab of the OU property.
   For example, enter `OU=unite_admin,CN=Users,DC=vprodemo,DC=com` as the distinguished name.

   Important Note: When an AD OU is assigned to a role, a URL will be shown at the top of the All Roles page. This URL is used to sign in to the admin portal for the Intel Unite® Cloud Service using AD FS.
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 Selected 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 Selected 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 OU and have different permissions. Users who are members of the Active Directory OU have a union of all the permissions from all roles linked to the Active Directory OU.

5.8 Admin Portal Subscription Management Menu

The subscription management menu groups all the pages and actions that relates to subscription management. It includes the following options:

- Subscriptions – This button takes the user to the Subscriptions page, which includes a list of subscriptions, hub devices, and for deactivation. For instructions on activation (pairing hubs), refer to Section 4.11.
- Shop Subscriptions – This button redirects the user to a website which provides different subscription options and allows administrators to manage their subscriptions.
- Activate Subscription – This quick action allows administrators to activate a subscription by entering it in the text field below and pressing the **ACTIVATE** button.

5.8.1 Subscriptions Page

The subscriptions page displays all current active/inactive subscriptions associated with the currently selected organization, lists devices, and provides tools for managing subscriptions. It provides the features described in Table 24. For additional details on subscriptions, refer to Section 5.8.2.

Table 24: Subscriptions Page Features

Subscriptions Page Feature	Description
Devices	This area shows how many hub devices are currently selected. The **Subscription** drop-down menu allows the currently displayed devices to be filtered to show only those activated with a specific subscription. The Deactivate button can be pressed to deactivate the selected devices when one or more are selected.

Subscriptions Page Feature	Description
Filters	This area provides the following additional ways to filter the results for which devices will be displayed: • **Add keyword (search by device or group name)** allows the device results to be filtered by the value entered in the text field. First enter the desired text, then click **Add keyword**. ◦ The results will display devices that contain the specified keyword in any part of the string. ◦ Multiple keywords can be entered. Once entered, they will be displayed below. Any undesired keywords can be removed by pressing the **X** button next to them. • The **Subscription** drop-down menu works similarly to the one above, filtering the device results by which subscription they're currently activated with. • The **Status** drop-down menu allows the device results to be filtered by whether they're currently enabled or disabled. • The **Clear filters** button removes all current filters so the results will include all devices associated with the currently selected organization.
Subscription Details	This area lists all subscriptions associated with the currently selected organization and includes the following details: • The name of each subscription. • The subscription's expiration date. • The number of devices currently activated under that subscription listed as X/Y, where X is the number of devices currently activated under that subscription, and Y is the total number of activations it accommodates. For example, a subscription with ten available hub activations and three in use will be displayed as "3/10". A blue utilization meter visually represents the portion of available activations currently in use for each subscription.
Device Results (table)	This table lists the device results from the filters listed above. If no filters are activated, all devices associated with the currently selected organization will be displayed. This table displays the following information: • Device Name – the name of the device. • Subscription – the name of the subscription that the device is currently activated with, if any. • Status – whether or not the device is currently enabled or disabled. • Group – the group the device is currently assigned to. To select a device, place a check in the checkbox on the left side of its row. To deselect it, remove the check. If no devices meet the filter criteria, a message reading "No matching records found" will be displayed.

5.8.2 Additional Subscription Details

Depending on the subscription options you have selected, there are limits to how many hubs can be activated. Multiple subscriptions may be required if the number of hubs used in your deployment exceeds the limit for a single subscription. When a hub device is paired and multiple subscriptions exist, it will automatically be activated with the subscription that was established earliest in chronological order. If all of that subscription's activations are currently in use, it will use the next subscription according to date established, and continue in that manner if it is also fully utilized. Further details are listed below:

- To use an existing subscription to pair a hub, refer to the instructions in Section 4.11.
- To review, manage, or shop for subscriptions, open a web browser and navigate to uat.shopcloudcollaboration.com/shop/intel.
- To see the requirements for hubs approved by Intel, refer to Section 2.1.
- While most deployments of the Intel Unite® Cloud Service use Intel-approved devices to operate as hubs, it is not an absolute requirement. Third-party devices can be used as hubs, so long as they meet the minimum requirements.

6 Alerts and Monitoring

The admin portal for Intel Unite® Cloud Service can be configured to notify the organization administrator when a certain number of hubs becomes unresponsive. The following server properties allow an organization 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 includes 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.

7 Security Controls

7.1 Minimum Security Standards (MSS)

Intel recommends that all devices running the Intel Unite® application meet the default organization Minimum Security Standards (MSS), 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).

7.2 Machine Hardening

The machine Unified Extensible Firmware Interface (UEFI) could be configured to only boot from the Windows* boot loader, ensuring that starting from a USB or DVD will not work. Other configurations can be set to enable the execute disable bit, enable Intel® Trusted Execution Technology, and require a password to change UEFI configurations.

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 usage of Alt + Tab, Ctrl + Shift + Esc, and the Charms bar.

7.3 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).

8 Maintenance Service

The Maintenance service is a Windows service responsible for supporting, cleaning, and maintaining server information. This section explains the functions and how to configure the various features of the maintenance service. The maintenance service is responsible for the following tasks:

- Cleaning expired data:
  - Pairing codes
  - PINs
  - OTP tokens
  - Meetings
  - Telemetry
  - Logging
- Updating device OUs
- Monitoring hub device health

8.1 Clean Expired Pairing Codes

This service is used to clean all rows in the pairing code table with expired pairing codes. It is configured using the properties listed in the table below.

Table 25: Clean Expired Pairing Codes Properties

Property Name	Description	Value Type	Default Value
Expired Paring Code Removal	This property sets the interval at which the Clean Expired Pairing Codes service is executed.	Minutes	1440

Follow the steps below to set up the Clean Expired Pairing Codes service:

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 for the **Expired Paring Code Removal** property.
5. Click **Save Changes**.

8.2 Clean Expired PINs

This service is used to clean all expired device PINs. It is configured using the properties listed in the table below.

Table 26: Clean Expired PINs Properties

Property Name	Description	Value Type	Default Value
Expired PIN Removal	This property sets the interval (in minutes) at which the Clean Expired PINs service is executed.	Minutes	5
PIN Expiration Time	This property sets the time (in minutes) before a PIN is considered expired.	N/A	None

Follow the steps below to set up the Clean Expired Pins service:

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 for the **Expired PIN Removal** property.

5. Enter a value for the **PIN Expiration Time** property.
6. Click **Save Changes**.

8.3 Clean Expired OTP Tokens

This service is used to clean all rows in the OTP token table with expired OTP tokens. It is configured using the properties listed in the table below.

Table 27: Clean Expired OTP Tokens Properties

Property Name	Description	Value Type	Default Value
Expired Auto Pairing Token Removal	This property sets the interval at which the Clean Expired OTP Tokens service is executed.	Minutes	1440

Follow the steps below to set up the Clean Expired OTP Tokens service:

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 for the **Expired Auto Pairing Token Removal** property.
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 expired meetings. It is configured using the properties listed in the table below.

Table 28: Clean Expired Meetings Properties

Property Name	Description	Value Type	Default Value
Expired Meeting Removal	This property sets the interval (in minutes) at which the Clean Expired Meetings service is executed.	Minutes	1440
Meeting Expiration	This property sets the time (in days) before a meeting is considered expired.	Days	1

Follow the steps below to set up the Clean Expired Meetings service:

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 for the **Expired Meeting Removal** property.
5. Enter a value for the **Meeting Expiration** property.
6. Click **Save Changes**.

8.5 Clean Telemetry Data

The Clean Telemetry Data service is used to clean all rows with expired telemetry data in the device metadata and device event tables. It is configured using the properties listed in the table below.

Table 29: Clean Telemetry Data Properties

Property Name	Description	Value Type	Default Value
Expired Telemetry Data Removal	This property sets the interval at which the Clean Telemetry Data service is executed.	Minutes	1449
Metrics Retention Policy	This property sets the time to retain telemetry data.	Days	365

Follow the steps below to set up the Clean Telemetry Data service:

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 for the **Expired Telemetry Data Removal** property.
5. Enter a value for the **Metrics Retention Policy** property.
6. Click **Save Changes**.

8.6 Clean Logging Data

The Clean Logging Data service is used to clean all rows in the logging table with expired telemetry data. It is configured using the properties listed in the table below.

Table 30: Clean Logging Data Properties

Property Name	Description	Value Type	Default Value
Expired Log Removal	This property sets the interval at which the Clean Logging Data service is executed.	Minutes	1440
Logs Retention Policy	This property sets the time to retain log data.	Days	30

Follow the steps below to set up the Clean Logging Data service:

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 for the **Expired Log Removal** property.
5. Enter a value for the **Logs Retention Policy** property.
6. Click **Save Changes**.

8.7 Update Device OU

The Update Device OU service is used to update the device table. It is configured using the properties listed in the table below.

Table 31: Update Device OU Properties

Property Name	Description	Value Type	Default Value
Maintenance Service AD OU Cache Generation	This property sets the interval at which the Update Device OU service is executed.	Minutes	1440

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

1. To set up the Update Device OU service, follow the steps below:
2. Log in to the admin portal.
3. Click **Server Management** from the navigation bar at the top of the screen and select **Server Properties**.
4. Click **Edit Properties**.
5. Enter a value for the **Maintenance Service AD OU Cache Generation** property.
6. Click **Save Changes**.
7. Go to the server where the Maintenance Service is running.
8. Using Task Manager, right-click `Intel Unite Maintenance Service` and select **Properties**.
9. Copy the path to the executable.
10. Open the `Intel.Unite.Server.Maintenance.exe.config` 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 watches to see if a set of hub devices becomes inactive (as determined by enabling a flag in reporting). If inactive, it will and an alert to admins listed in the admin portal. It is configured using the properties listed in the table below.

Table 32: Health Monitor Service Properties

Property Name	Description	Value Type	Default Value
Maintenance Service Interval	This property sets the interval at which the Health Monitor service is executed.	Minutes	`1440`
Inactive Hub Threshold	This property sets minimum number of inactive devices before a Health monitoring report is sent to all admins.	Number of inactive devices	`1`

Property Name	Description	Value Type	Default Value
Inactive Duration	This property sets the length of time before a hub device is considered inactive.	Minutes	70

The Health Monitor service scans the hubs and clients database where all the devices are stored and checks all the devices that have the configuration core property **Enable Reporting** set to **True**. Once all the clients with **Enable Reporting** set to **True** have been identified, the Health Monitor service checks the timestamp field. It then looks for devices where the difference in minutes between the actual time and the last update time is greater than the **Inactive Duration** key (as 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 greater than the number of devices set in the **Inactive Hub Threshold**, an email will be sent to all the users registered in the admin portal that have the Admin role. If the Health Monitor Service finds that the number of inactive devices is greater than it was in the previous scan, additional emails will be sent.

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 for the **Maintenance Service Interval**.
5. Enter a value for the **Inactive Hub Threshold** property.
6. Enter a value for the **Inactive Duration**.
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.config` file in Notepad and set the following properties:
    - `SMTP FROM`
    - `SMTP HOST`
    - `PORT`
    - `USERNAME`
    - `PASSWORD`

    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** button 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 you want to track, then click **Edit Device**.
18. Set Enable hub check-in reporting to **True**, then click **Save Changes**.

Each organization and the organization 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 (with no GUI prompts), preferably before the nightly reboot.
- **Reporting** – Logs are captured and can be accessed on the admin portal under the Server Management tab.
- **Backend Monitoring** – Use standard virtual server monitoring tools to generate and send alerts to second-level support.

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 server properties listed in Table 33 allow an IT administrator to customize the alert behavior. Refer to Section 5.6.3 for a detailed list of server properties.

Table 33: Alerts and Monitoring Properties

Property Name	Description
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.

Appendix A Provisioning for Google Admin*

A.1 Enforce Automatic Intel Unite® Application Install

Follow the steps below to configure the enforcement of automatic Intel Unite® application installation:

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-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 OS. 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 using the link above.
7. You will be sent to the management settings for the app. Click **User Settings**, then select your organization from the list of options.
8. Toggle Force Installation to **Enabled**.
9. Click **Save** when you are finished.

For a Chromebook to use these settings, it may have to be powerwashed. If your fleet is not joined to your enterprise account, then a powerwash may be necessary, except for brand new, out-of-box systems. If your fleet is already joined, powerwashing is not necessary. 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, then selecting Directory from the drop-down menu, then clicking Users.

A.2 Google Admin* Setup for Client Configuration

Follow the steps below to configure the Intel Unite® software using Google Admin* when Intel Unite® clients are under domain management.

1. Open a browser, navigate to https://admin.google.com, and log in 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**. The configuration file is in JSON* format. An example of what is in a configuration file is shown below:

```
{
"managedEnterpriseServer": {"Value" : "unite.example.com"},
"managedEnableWebrtc": {"Value" : true},
"managedLandingUrl": {"Value":
"intelunite4://localhost/register?serverUrl=https://unite4.example.com/intelunit
e/api&orgId=7A810B3F-0608-4A1C-BF42-C06A338EF877" },
```

```
"managedPairingUrl": {"Value":
"intelunite4://localhost/pair?otp=<token>&email=<email
address>&machineName=<machine name>" },
"managedOrganizationSecret": {"Value": "<this is your password>"}
}
```

9. The following settings can be set using the configuration file:
    a. managedEnterpriseServer – A text field labeled Enterprise Server. If set to anything other than blank, it is used as the Intel Unite® Cloud Service for the app, and it overrides and disables the Intel Unite® Cloud Service field in the settings.
    b. managedEnableWebrtc – A Boolean toggle labeled Enable WebRTC. If set to true, the app uses WebRTC (if available on the hub) rather than RFT.
    c. managedLandingUrl – If set, this is used as the Intel Unite® Cloud Service and organization ID for the associated Chromebooks*, overriding the local settings.The URL format is as follows: `intelunite4://localhost/register?serverUrl=<url>&orgId=<guid>`
    d. managedPairingUrl— This sets up the Email Address, Machine Name and Pairing Token for the associated Chromebooks, overriding the local settings.
    e. Note: If not set, the email address will not populate in the app; ensure that the managedPairingUrl is properly set in the configuration file.
    f. 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. Follow the steps below to obtain the `<OTP_GUID>`:
        i. Open a browser and navigate to the login page of the Intel Unite® Cloud Service.
        ii. Enter the username and password.
        iii. Click the **Sign In** button to sign in.
        iv. Select the organization being configured.
        v. Select **Auto Pairing Management** from the Device Management menu to display a list of token GUIDs.
    g. 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.
10. Click **Save**.

A.3 Grant the Intel Unite® App 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 allowlisted in your organizations Google Admin* account. Follow the steps below to grant the 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 plus button (+)** in the lower-right of this page, which will open the Add App To Trusted List dialog.
6. From the drop-down, 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-jvglhh0pen7vdjd96vr5g2g2dknfpf6.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**.
10. Paste the OAuth2 ID from above into the “Client Name” field
11. 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`
12. Click the **Authorize** button.

The Intel Unite® app will query Google* APIs 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.

Appendix B Error Codes

B.1 Client Error Codes

This section provides information about error codes that may occur on the client application. To contact Intel Unite® Cloud Service support, open a web browser and navigate to the support website for the Intel Unite® Cloud Service.

The client saves a log file at `C:\Users\<user>\AppData\Local\Temp`, where `<user>` is the logged in user

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

Table 34: Client Error Codes

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 following 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 the provision page of the admin portal 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: Remove all keys for organization id in the following 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 provision 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 a correct configuration (with https protocol). Confirm that the keys in the following registries are 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 the l provision page of the admin portal 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 for 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 the 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 the module assigned in the admin portal and upload again

B.2 Hub Error Codes

This section provides information about error codes that may occur on the hub application. To contact Intel Unite® Cloud Service support, open a web browser and navigate to the support website for the Intel Unite® Cloud Service.

The hub saves a log file at `C:\Users\<user>\AppData\Local\Temp`, where `<user>` is the logged in user.

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

Table 35: Hub Error Codes

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 a valid Keys in the following 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 provision page of the admin portal 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 provision 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

C.1 Slowness Accessing the 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, users may experience slowness when 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"
```

C.2 Hub Time Drift

Hub time might drift and be different than other hubs, which can cause confusion as to when a session ends or who owns the session. 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, follow the steps below 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` and press **Enter** or **Return**.
3. Confirm that the source is not set to Local CMOS Clock.

Appendix D Security Checklist

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

- Enable rate limiting in IIS: https://docs.microsoft.com/en-us/iis/configuration/system.webserver/security/dynamicipsecurity/denybyrequestrate

D.1 Hub

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

- Pin Intel Unite® Cloud Service 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.

D.2 Client

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

- Pin Intel Unite® Cloud Service certificate in registry. Refer to the Microsoft enterprise certificate pinning article.

Appendix E Considerations for Transitioning from a 4.x or 3.x Environment

This section describes some considerations for installing the Intel Unite® Cloud Service in an existing 4.x or 3.x environment.

- Cloud clients can connect to both 4.x and 3.x hubs.

  Note: For the Windows client to connect to a 3.x hub, the device must have a 3.x client installed as well as the client application for the Intel Unite® Cloud Service. The client application for the Intel Unite® Cloud Service must be installed after the 3.x client is already installed.

- Intel Unite® solution version 3.x uses DNS SRV record for autodiscovery, while Intel Unite® Cloud Service uses DNS TXT record. Both records can exist to support both solutions in an environment.

The install sequence when going from Intel Unite® solution 3.x or 4.x to Intel Unite® Cloud Service is as follows:

1. Throughout transition period, maintain 3.x or 4.x versions of the server.

   Note: You can run 3.x and 4.x Intel Unite® solution servers simultaneously while using the Intel Unite® Cloud Service.

2. Begin installing the client application for Intel Unite® Cloud Service on all of your Windows based devices while keeping the 3.x client application installed. Everything non-Windows can be upgraded to client applications for the Intel Unite® Cloud Service.
3. Once you have all the client devices on Intel Unite® Cloud Service then begin migrating hubs to Intel Unite® Cloud Service.