Modernizing Meetings: Delivering Intel Unite® App Authentication with RFID

Intel Unite® Solution White Paper

June 2018

Revision 1.0

Legal Disclaimers and Copyrights

All information provided here is subject to change without notice. Contact your Intel representative to obtain the latest Intel product specifications and roadmaps.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software, or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at intel.com.

You may not use or facilitate the use of this document in connection with any infringement or other legal analysis concerning Intel products described herein. You agree to grant Intel a non-exclusive, royalty-free license to any patent claim thereafter drafted which includes subject matter disclosed herein.

No license (express or implied, by estoppel or otherwise) to any intellectual property rights is granted by this document.

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

Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

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

Contents

Figures

Tables

Revision History

Revision	Description	Date
1.0	Initial Document	June 2018

§

1 Introduction

This whitepaper provides information about planning, developing, and deploying an alternative method for allowing the Intel Unite® client app to join a meeting session. This solution can be implemented and deployed into any corporate or learning institution that has implemented RFID identification to authenticate employees or individuals in the organization.

The Intel Unite® solution is a collaboration and wireless screen sharing software suite developed by Intel.

1.1 Terminology

Table 1. Terminology

Term	Description
AD	Active Directory
AD DS	Active Directory Domain Services
Badge Information	26-bit numerical or alphanumeric data stored on an RFID badge
DNS	Domain Name Server
EID	Electronic Identity Card. A user's Active Directory Account identifier.
FQDN	Fully Qualified Domain Name
GPIO	General Purpose Input Output
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IDE	Integrated Development Environment
Intel Unite®	Screen sharing and collaboration software solution
IOT	Internet of Things
OS	Operating System
RFID	Radio-Frequency Identification
SDK	Software Development Kit
SID	Active Directory Security Identifier. The primary key for an Active Directory object.
SSO	Single Sign-On
TLS	Transport Layer Security

Term	Description
USB	Universal Serial Bus
URL	Uniform Resource Locator. Used to access a web service.
PIN	Personal Identification Number. A unique numeric code to authenticate users on the Intel Unite® app.
Token	A secret generated by client. It should be used only once and should expire periodically. This token provides exclusive read access to the web service.

1.2 Reference Documents

Table 2. Reference Documents

Document	Document No./Location
Intel Unite® Plugin Software Development Kit (SDK)	
Intel Unite® Solution Enterprise Deployment Guide	
Microsoft Active Directory Overview website	https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview
Intel Unite® App Plugin Software Developer Kit	https://downloadcenter.intel.com/download/25230/Intel-Unite-App-Plug-In-Software-Development-Kit
Remote Server Administration Tools (RSAT) for Windows 10*	https://www.microsoft.com/en-sg/download/details.aspx?id=45520&751be11f-ede8-5a0c-058c-2ee190a24fa6=True

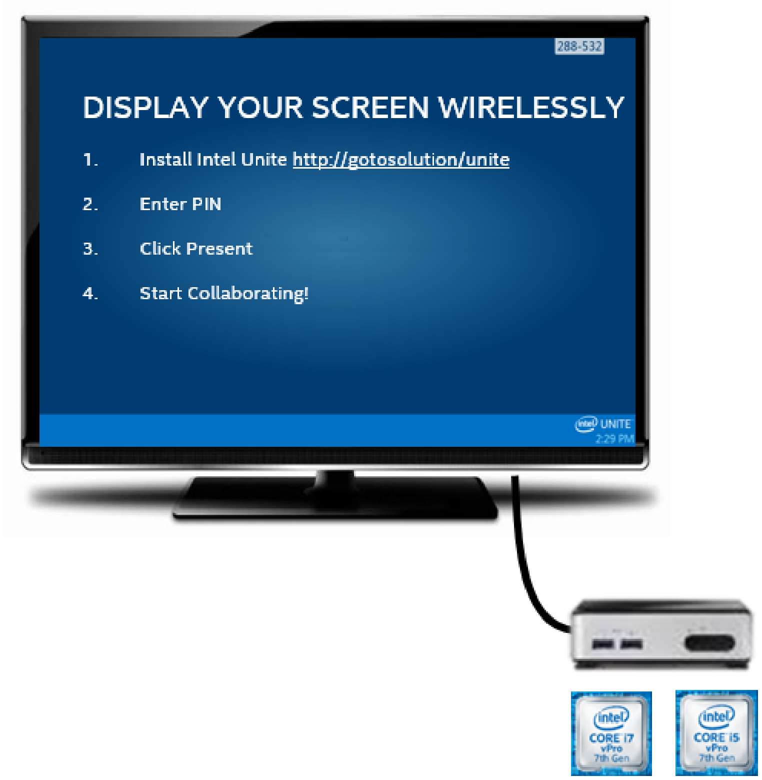
§

2 Business Challenge

The Intel Unite® solution utilizes a six-digit PIN, which users must enter to authenticate and join a meeting or collaboration session (refer to Figure 1). Some organizations are interested in enhanced solutions which integrate with existing controls or provide the identity of the participant.

One way to provide these types of enhancements to the Intel Unite® solution is described in the next section. The solution described involves integrating an existing card-based access control (RFID) with the Intel Unite solution to allow users to authenticate and join a meeting session without having to enter the six-digit PIN.

Figure 1. Intel Unite® Software Setup



DISPLAY YOUR SCREEN WIRELESSLY

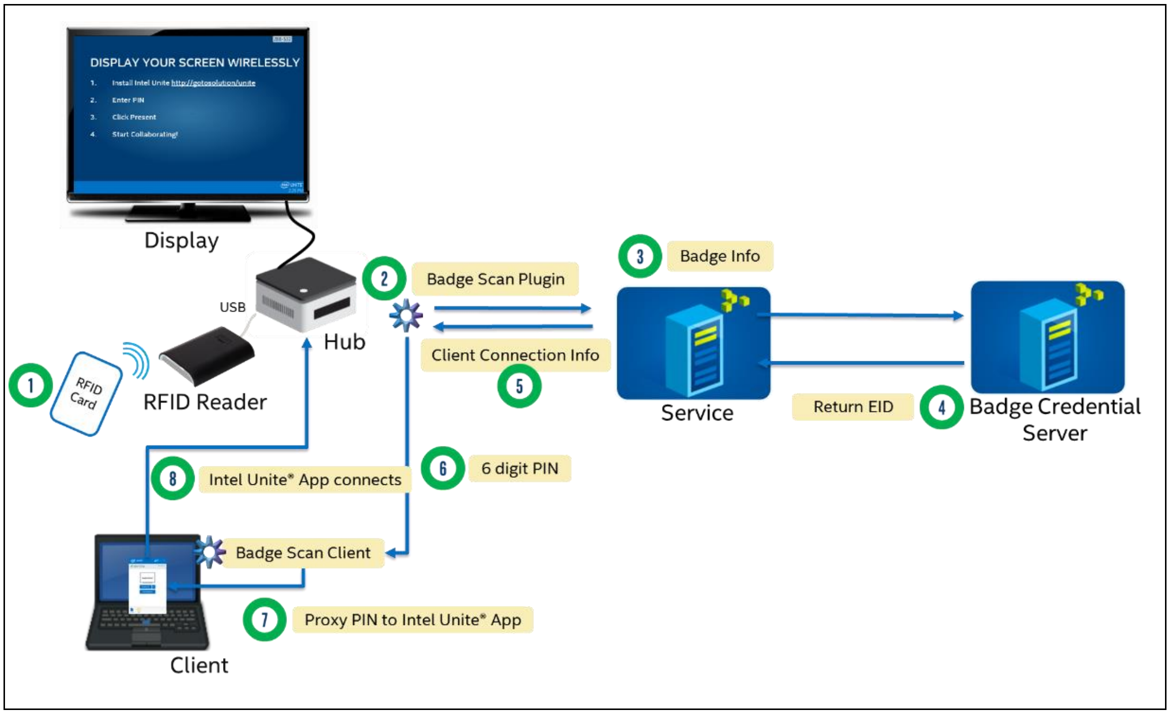
1. Install Intel Unite http://gotosolution/unite
2. Enter PIN
3. Click Present
4. Start Collaborating!

§

3 High-Level Solution Design

Before studying the solution design, let's assume the Intel Unite® solution is set up in an organization that shares the same enterprise network in all areas and has a unified card-based access control infrastructure, as shown in Figure 2.

Figure 2. Flow Diagram for Seamless Intel Unite® App Authentication via RFID



In this modern approach, an Intel Unite® app user walks into a meeting room and taps a valid employee RFID badge on an RFID reader connected to the hub (1).

The badge scan plugin (2) is a software runtime developed with the Intel Unite® SDK. It securely transmits the scanned badge information to the PIN server.

A *service* (3) picks up the badge information (a 26-bit unique badge identifier) and calls an API that exposes the employee ID (4) and retrieves the EID using Microsoft* Active Directory.

Note: The *service* is described in more detail in Section 3.3.3.

The service forwards the client connection information (5) to the badge scan plugin, and the badge scan plugin forwards the six-digit PIN (6) to the Intel Unite® app via the badge scan client (7) running in the client.

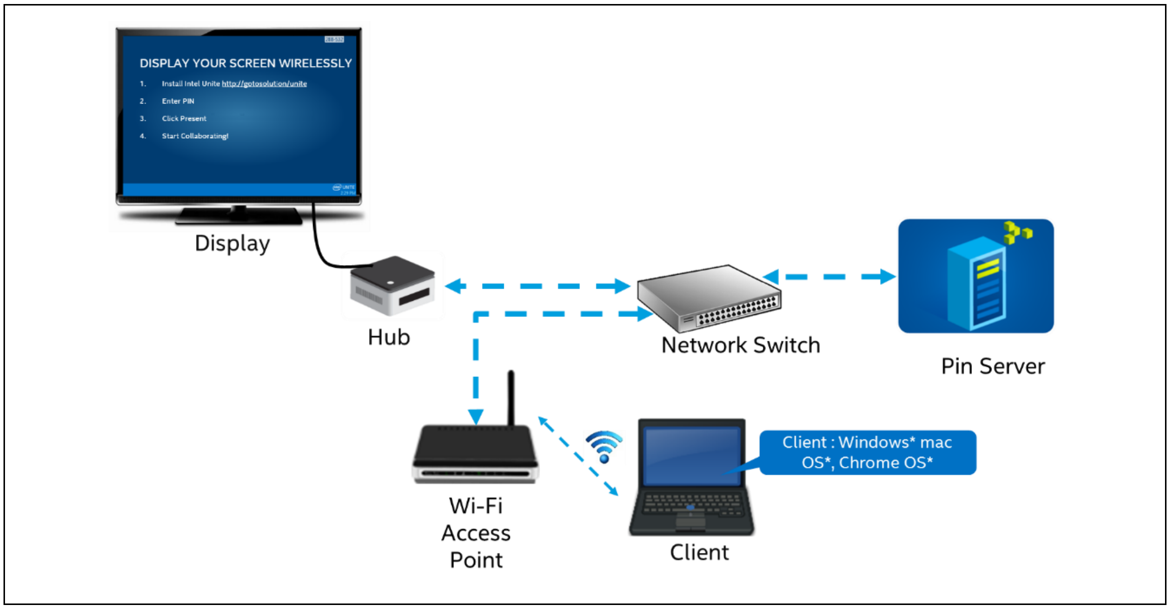
Finally, the Intel Unite® app connects with the hub (8). The client is ready for screen sharing or participating in an existing meeting session.

3.1 Environment Setup

A working solution for an enterprise network environment is shown in Figure 3 and requires the following components:

- Active Directory Domain Services (AD DS) to resolve computers and users' ID SIDs. The organization should have Microsoft* Active Directory established. To learn more about AD DS, visit the Microsoft Active Directory Configurations website (refer to Table 2).
- Conference rooms equipped with enterprise Intel Unite® software version 3.1 or later.
- Enterprise deployment of the Intel Unite® solution that includes:
  - A PIN server, which keeps track of hubs and clients, and periodically generates the six-digit PIN for clients to join a meeting session.
  - A hub that displays the six-digit PINs received from the PIN server and wirelessly presents content received from meeting participants connected to the hub.
  - Clients that allow meeting participants to become presenters or remote viewers.
- A badge scanner peripheral attached to the hub via a standard interface, such as USB or serial port. Because the market offers a wide range of badge scanners (such as HID* Badge Scanner from OMNIKEY 5427), contact the hardware vendor for an appropriate solution.

Figure 3. Enterprise Intel Unite® Solution Deployment



DISPLAY YOUR SCREEN WIRELESSLY

1. Install Intel Unite http://gotosolution/unite
2. Enter PIN
3. Click Present
4. Start Collaborating!

3.2 Development Prerequisites

Software prerequisites and setup configuration required include:

- MS Visual Studio* 2015.
- The *Intel Unite® App Plugin Software Developer Kit* (refer to Table 2).
- The *Remote Server Administration Tools (RSAT) for Windows* 10* (refer to Table 2).

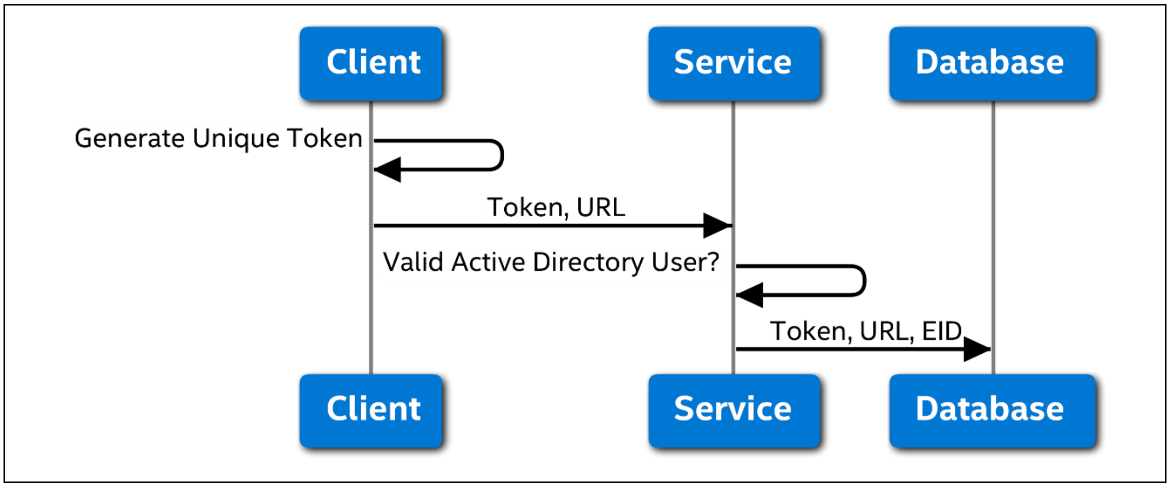
3.3 Badge Scan Client, Plugin, and Web Service Development

This section provides a high-level design for building and deploying a badge scan solution that is integrated with the Intel Unite® solution.

3.3.1 Badge Scan Client (Client)

The badge scan client is software that runs as a background service in the client PC where the Intel Unite® app is installed. This service scans incoming connections and automatically launches the Intel Unite® app if a valid token and PIN for Intel Unite® app is satisfied. Figure 4 shows how this process is accomplished.

Figure 4. Badge Scan Client Sequence Diagram



The following steps occur during a badge scan service check-in from the client:

1. A unique GUID (token) is generated and posted to a service running in the domain.

Note: The *service* is described in more detail in Section 3.3.3.

2. When the service returns a valid AD user, the service updates the database with a token hash, URL, and EID.
3. If any hub sends a valid token and PIN to the client, the client starts the Intel Unite® app and automatically join the meeting session with the PIN.

A developer could use pseudo-code to code the badge scan plugin service, as shown in the next two sections.

3.3.1.1 Periodic Check-In Unique GUID into Web Service Function

This function is an example of how to create a periodic check-in unique GUID in the web service:

```
while(true)
{
    // loop every 1 minute
    Guid = GenerateUniqueId;
    Checkin(Guid, webService.Url);
}
```

3.3.1.2 Token and PIN Validation before Joining a Meeting Session Function

This function is an example of how to execute token and PIN validation before joining a meeting session:

```
webService.OnConnect(token, pin)
{
    If (token.isValid())
    {
        Process.Start(unite.exe, pin);
    }
}
```

3.3.2 Badge Scan Plugin (Hub)

The developer needs to develop a plugin for the Intel Unite® app that runs on the hub. The plugin completes the badge scan, contacts the service, and triggers an Intel Unite® client to connect based on the badge scan action (refer to Figure 5).

When a badge is scanned, the following steps occur:

1. The plugin forwards the badge information to the service running on the domain to perform authentication and request the EID.

Note: The *service* is described in more detail in Section 3.3.3.

2. The EID received from the credential server is used by the service to request the token and URL from the database.
3. The database returns the previously stored token and URL to the plugin.
4. When the plugin receives the token and URL, it sends the token and PIN to the client PC. The client's badge scan service proxies the PIN received from the hub and starts the Intel Unite® app (refer to Figure 6).

Note: See the *Intel Unite® App Plugin SDK* for PIN retrieval methods (refer to Table 2).

Figure 5. Badge Scan Plugin Steps

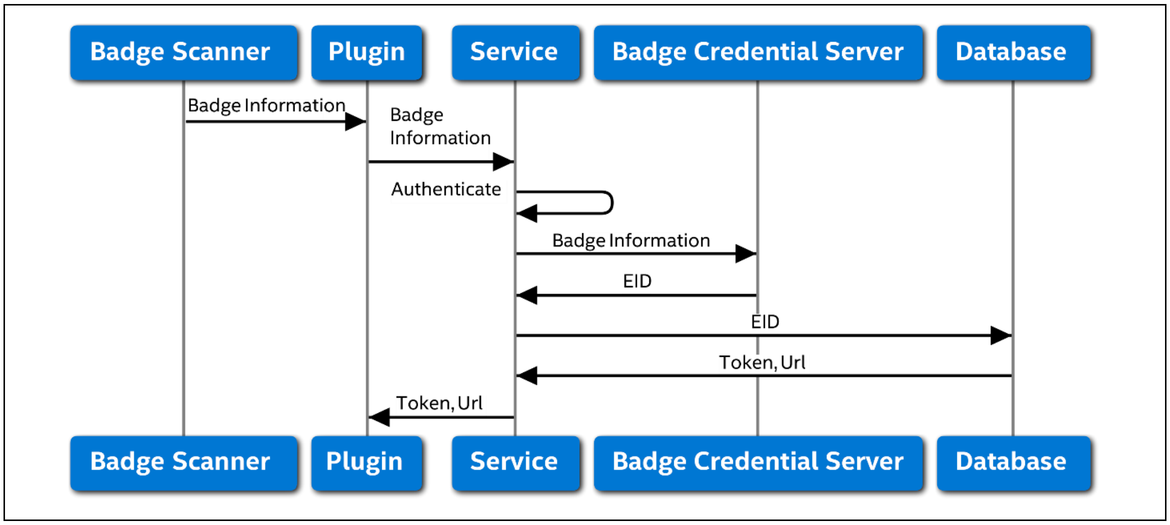
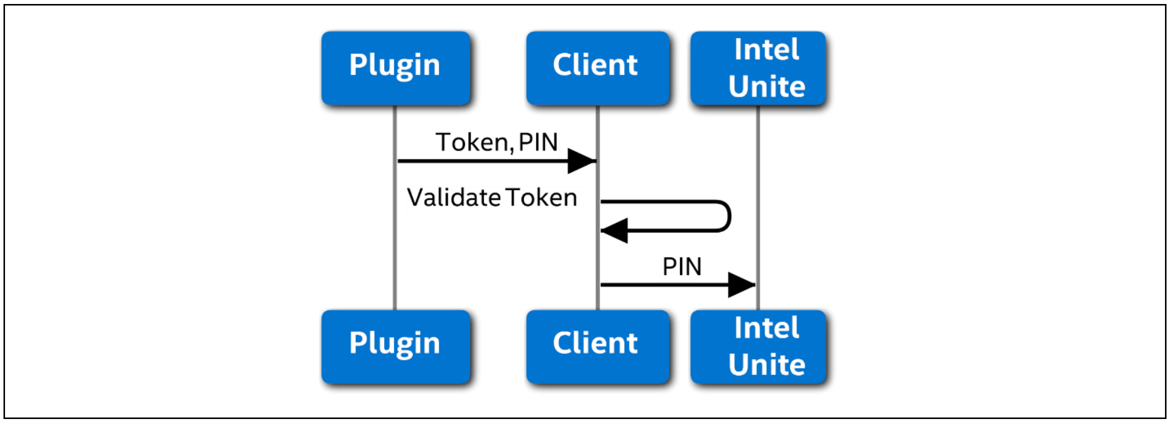


Figure 6. Client Badge Scan Service to Start the Intel Unite App



3.3.3 Badge Scan Service (PIN Server)

The badge scan service acts as a directory service. It tracks all clients connected to the domain that have the badge scan client installed. The traffic for these connections are encrypted with Transport Layer Security (TLS) and are authenticated via Active Directory.

The requests made to this service are client check-in and client lookup.

For client check-in, the token and URL are used as a requisite before the EID is generated and stored into the database, as shown in the following pseudo-code:

```
OnClientCheckin(Token, URL)
{
    EID = AuthenticateClientWithActiveDirectory();
    StoreInDatabase (Token, URL, EID)
}
```

For client lookup, the service uses the badge information received from the hub. It uses the information to search for the EID stored in the database. It retrieves and returns the token and URL value to the respective plugin running on the hub, as shown in the following pseudo-code.

```
OnClientLookup(BadgeId)
{
    EID = LookupEIDBasedOnbadgeInfoBadgeId);
    Token, Url = LookupConnectionInfoInDatabase(EID);
    Return (Token, URL);
}
```

§

4 Conclusion

The scalable Intel Unite® solution with the *Intel Unite® App Plugin SDK* provides a platform for system integrators and independent software vendors (ISV) on which they can integrate existing access management solutions. This enables developers to deliver seamless connectivity to users and support collaboration sessions in enterprise domains. This is one of the key values of the Intel Unite® solution—make meeting rooms intelligent.

§