

Intel Unite[®] Solution

Intel Unite[®] Plugin for System Broadcast

Version 1.0



Legal Notices and Disclaimers

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

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

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

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

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

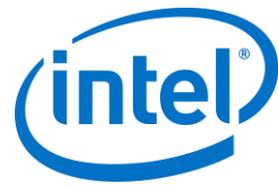
Intel disclaims all express and implied warranties, including without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement, as well as any warranty arising from course of performance, course of dealing, or usage in trade.

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

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

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

© 2018 Intel Corporation. All rights reserved.



Revision History

Revision	Date	Notes
1.0	June 2018	First Release



Contents

1.	Introduction.....	5
1.1	Audience.....	5
1.2	Intel Unite® Solution Terminology & Definitions	5
1.3	Overview	5
2.	Requirements	7
2.1	Server Requirements	7
2.1.1	Deployment Constraints.....	8
2.1.2	Authentication Modules	8
2.1.3	Installing IIS Extensions.....	8
2.1.4	Configure Application Request Routing Cache	8
2.2	Plugin Requirements.....	9
3.	Installation	10
3.1	Server Installation.....	10
3.2	Plugin Installation.....	11
3.3	Admin Portal Configuration.....	12
3.3.1	Obtaining Certificate Thumbprint	12
3.3.2	Admin Portal Configuration.....	13
4.	Features	15
4.1	Dashboard.....	15
4.2	Alerts	15
4.2.1	Send an Alert.....	15
4.2.2	Clear an Alert.....	16
4.3	Messages	16
4.4	Displays	17
4.5	Groups.....	17
4.6	Users.....	17
4.7	Tokens.....	18
4.8	System Configuration	18
5.	Programmer API.....	19
6.	Troubleshooting.....	20
6.1	Logging	20
6.2	Plugin Unable to Connect.....	20
6.3	Intel Unite® app crash	21



1. Introduction

Welcome to the Intel Unite® Plugin Guide for System Broadcast.

This guide contains detailed instructions on installing the server and plugin for System Broadcast, as well as information on the key features of this Intel Unite® plugin.

1.1 Audience

This document is designed for use by IT professionals operating within a corporate environment, who are responsible for installing the Intel Unite® software and adding optional features to the application.

1.2 Intel Unite® Solution Terminology & Definitions

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

Client – This term refers to a device (Windows*, macOS*, iOS*, Android* or Chromebook*) that will be used to connect to the Hub.

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

FQDN – This acronym stands for Fully Qualified Domain Name.

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

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

1.3 Overview

This plugin is a solution for broadcasting preset system messages to displays attached to hubs running the Intel Unite® app.

The solution contains a server component which includes an administrative portal for authorized individuals to create messages, push messages to multiple displays, and clear active alerts. The server also provides an API interface to automate and integrate the solution with existing systems that may be deployed in your environment.

Although the Intel Unite® application can be used to communicate broadcast messages (such as the availability of leftover food in a conference room) to participants when they are actively using the



application, it is not intended as the primary means of communicating emergency broadcast messages (such as a building evacuation order) and you should ensure there are alternate methods to communicating broadcast emergency messages.



2. Requirements

2.1 Server Requirements

The Intel Unite® Plugin for System Broadcast server component is designed to be installed on a server running IIS and Microsoft SQL.

You can install the server component on the same server as the Intel Unite® Enterprise PIN server, or you can install it on a separate server. The benefit of installing on the same server is that the plugin running on the hub will automatically find the server.

Software requirements:

- Windows* Server 2012 or greater
- Microsoft Visual C++ 2015 Redistributable Update 3 RC or later
 - <https://www.microsoft.com/en-us/download/details.aspx?id=52685>
- Microsoft Internet Information Services Requirements
 - IIS 7 or greater
 - SSL enabled
 - This will require a minimum SHA2 based web server certificate with an internal or public root of trust
 - Required IIS Features:
 - Microsoft .NET Framework 3.5 Features
 - ASP .NET 4.5
 - WCF Services
 - HTTP Activation enabled for both .NET 3.5 and 4.5
 - WebSocket Protocol
 - Security:
 - Windows, Digest, or Basic

Note: Anonymous authentication must be disabled for the System Broadcast site in IIS

- Required IIS Roles:
 - Common HTTP Features
 - Default Document
- IIS Extensions:
 - URL Rewrite Module
 - Request Route Module

Note: You may need to install the Web Platform Installer to install the IIS extensions:

- Microsoft SQL Server 2012 or greater
 - Recommended latest patch level
- Microsoft .NET* 4.5 or greater



- 4 GB RAM
- 32 GB available storage

NOTE: The IIS web server and Microsoft SQL database server can be installed on separate machines

2.1.1 Deployment Constraints

With this version, the server is not able to operate behind a load balanced environment due to the WebSocket server design.

This server has been validated up to 1,000 simultaneous connected hubs.

2.1.2 Authentication Modules

This server application will rely on your infrastructure to provide user authentication. This enables the server to integrate with many different environments. Window and Digest authentication are typically used in environments that are set up with Microsoft Active Directory, whereas Basic authentication does not require Active Directory.

For a full explanation of the authentication modules, their capabilities, and configuration options please refer to the IIS documentation provided by Microsoft:

<https://docs.microsoft.com/en-us/iis/configuration/system.webserver/security/authentication/>

2.1.3 Installing IIS Extensions

You can download the extensions from Microsoft and install them, or you can down the Web Platform Installer from Microsoft and use that tool to install the required extensions.

To use the Web Platform Installer:

1. Download and install the Web Platform Installer:
<https://www.microsoft.com/web/downloads/platform.aspx>
2. Start IIS Manager
3. Select your server in the left pane
4. Select **Microsoft Web Platform Installer** from the middle pane
5. Search for the desired extension and install the latest version

2.1.4 Configure Application Request Routing Cache

After you install the Application Request Routing Cache module, you must enable it before installing the server. To do this:

1. Start IIS Manager (Note: You may need to restart the IIS Manager App if you just installed this module)
2. Select your server in the left pane
3. Select **Application Request Routing Cache** in the **IIS** section in the middle pane



4. Select **Server Proxy Settings** in the right pane
5. Select the **Enable Proxy** checkbox.
6. Click "Apply" in the right pane

2.2 Plugin Requirements

The plugin component will be installed on a hub that is running the Intel Unite® app.

Software Requirements:

- Windows* 7, 8.1, or 10 64bit
- Intel Unite® software for the hub, version 3.0 or greater

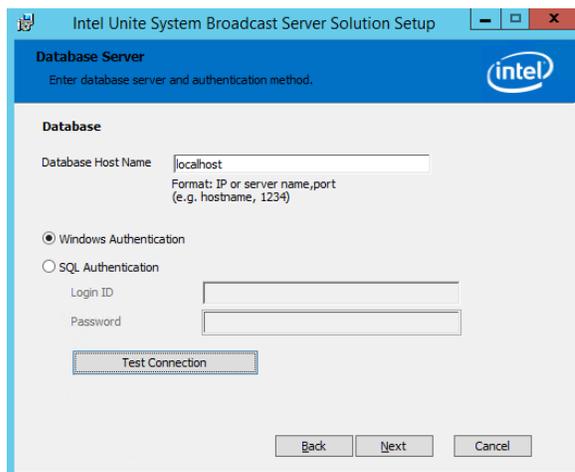


3. Installation

This section will guide you through the server and plugin installation. Please ensure that you have installed and configured all the required server and hub components before completing the installation.

3.1 Server Installation

1. On the server, launch **Intel Unite System Broadcast Server Solution Setup.msi**
2. Select **Next** on the Welcome screen
3. Review and accept the End-User License Agreement, then select **Next**
4. Enter credentials for your SQL Server and select **Test Connection**



5. After **Test Connection** succeeds, press **Next** to continue
6. Enter the server configuration in the next window:

- **HTTP Port:** This is the port the plugin will use to initiate a connection to the server.



- **Web Socket Port:** This is the port the plugin will use for continued communication to the server.
 - **Admin Username:** After installation, this is the login ID of the user that will have admin rights.
 - **Authentication Method:** This is the authenticate mode that IIS will be configured to use.
7. Select **Next** to start the installation
 8. Select **Finish** to complete the installation

To Log in, open a browser and navigate to <https://<server name>/systembroadcast/admin>.

Note: You must access the portal using https or you will get an “Access Denied” message.

Common Installation Issue:

If you run into an issue, please ensure

There is a known issue if you don't have the latest version of the Microsoft Visual C++ 2015 Redistributable where the installer will indicate that it failed, Windows Control Panel shows that it is installed, and when you load the admin web page you get the error, “You do not currently have access to this resource. Please contact the system administrator.”

To resolve this issue, you will need to uninstall System Broadcast from the control panel, delete the database that was created, update Microsoft Visual C++ 2015 Redistributable and re-run the installation.

3.2 Plugin Installation

On the hub running the Intel Unite® app:

1. Close the Intel Unite® application
2. Select **Next** on the Welcome screen
3. Review and accept the End-User License Agreement, then select **Next**
4. Select or enter your server:
 - Choose **Default Server** if the System Broadcast server is installed on the same server as the Intel Unite® PIN server
 - Choose **Enter Server Name** and enter the FQDN of the server where you installed System Broadcast if your server is not installed on the same server as the Intel Unite® PIN server
5. Select **Next** to start the installation
6. Select **Finish** to complete the installation



3.3 Admin Portal Configuration

For additional security, the Intel Unite® app on the hub will verify the digital signature of a plugin before it is loaded. The trust is configured per **Profile** on the **Admin Portal**.

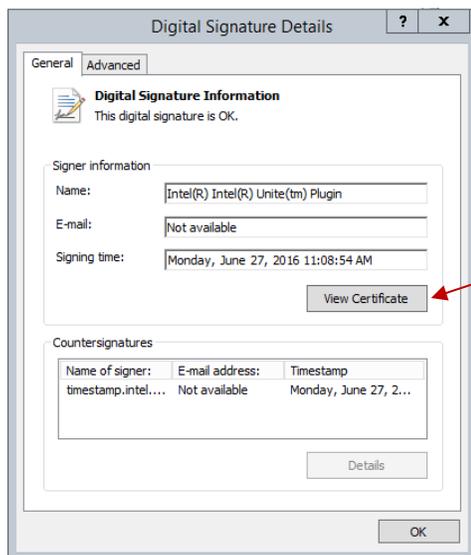
NOTE: For a test environment, you can disable the certificate verification. Refer to the **Enterprise Deployment Guide** for details.

To configure this, you will need to obtain the certificate thumbprint from the DLL and then log into the Admin Portal and add it to the profile the hub is assigned to.

3.3.1 Obtaining Certificate Thumbprint

On the hub:

1. Open the plugin installation folder (Default C:\Program Files (x86)\Intel\Intel Unite\Hub\Plugins)
2. Right click on **SystemBroadcast.Plugin.v3X.Plugin.dll** and choose **Properties**.
3. Select the **Digital Signatures** tab.
4. Select **Intel Unite Plugin** certificate in the **Signature List** and click on **Details**.
5. On the **Digital Signatures Details** window, click on **View Certificate**.



6. In the **Certificate** window, select the **Details** tab and scroll down until you see **Thumbprint**.
7. Select **Thumbprint**. Once the value is displayed, copy and paste it into a text file using a text editor (for example Notepad).
8. Remove the spaces and save it.



This information will be used when you update the profile for your plugin on the Admin Portal.

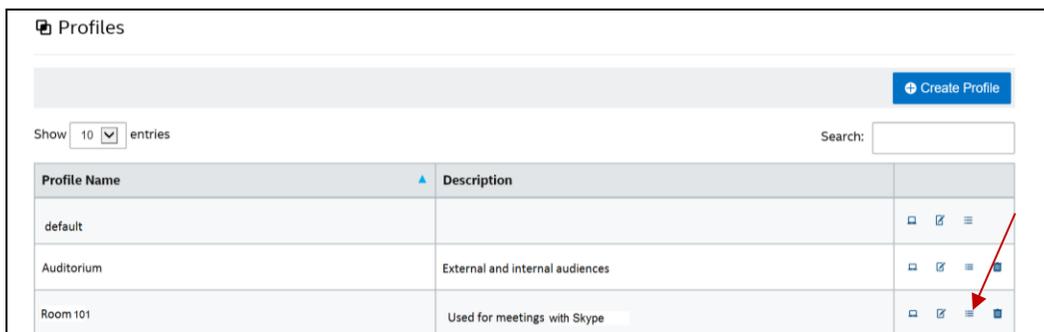
3.3.2 Admin Portal Configuration

Hubs running the Intel Unite® app are assigned to a profile using the Admin Portal. If a hub is not assigned to a profile, it inherits settings from the default profile.

You will need to determine which profiles the target hubs belong to and follow these steps to add a trusted certificate thumbprint. You may need to repeat these steps if you have hubs in different profiles that will run this plugin.

In the Admin Portal:

1. Log into the Admin Portal (<https://<servername>/admin>).
2. Select **Groups** then **Profiles**.
3. Under the **Profile Name** list, click the **View Details** icon (located in the last column on the right) for the profile that the hub will belong to. Alternatively, you may want to create a new Profile instead of using an existing one.



4. Click the **Add Profile Property** button.
5. This opens the **Add Profile Property** dialog. Enter the following information:



- **Key:** PluginCertificateHash_SystemBroadcastPlugin
- **Data Type:** String
- **Unit:** Text
- **Value:** Paste the thumbprint value saved in the text file from the **Obtaining Certificate Thumbprint** section of this guide.

6. Click on **Save**.

Alternately, for a test environment, you can also disable plugin certificate verification by setting **Verify Plugin Certificate Hash** key to **False** within the same profile. This is not recommended for a production environment as it is less secure.

Profile:Room101 | Used for meetings with Skype

← Back + Add Profile Property

Show 10 entries Search:

Key	Value	
PluginCertificateHash_LyncPlugin		<input type="checkbox"/>
Send Error Email Address		<input type="checkbox"/>
Service Listen Port	0	<input type="checkbox"/>
Tile Compression	85	<input type="checkbox"/>
Tile Size	128	<input type="checkbox"/>
Verify Plugin Certificate Hash	True	<input checked="" type="checkbox"/>

Showing 21 to 26 of 26 entries First Previous 1 2 3 Next Last

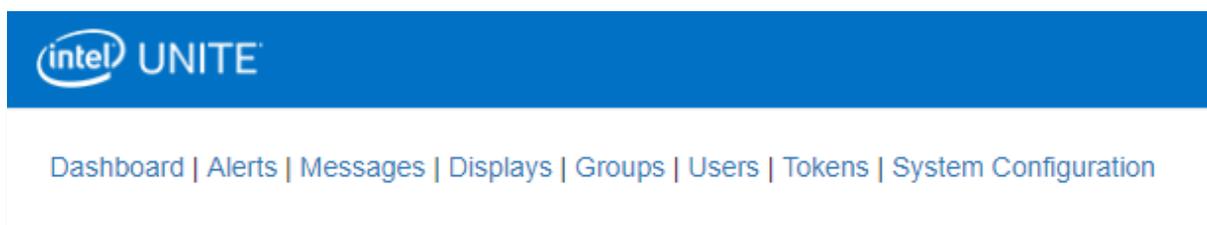


4. Features

This section will guide you through all the features of this solution.

This solution is used and managed through the System Broadcast server. To begin, log into the server: <https://<server name>/systembroadcast/admin>

You can access features and configure your solution using the navigation panel at the top of the page.



4.1 Dashboard

The Dashboard provides a quick view for connected displays and active alerts within your deployment.

When an alert is activated, an additional option appears at the top of the page which allows you to switch between **Display View** and **Alert View**.

You will have additional options to send or clear alerts based on the view you select.

4.2 Alerts

In this page, you can push pre-configured messages to groups or displays.

Note: Although the Intel Unite® application can be used to communicate broadcast messages (such as the availability of leftover food in a conference room) to participants when they are actively using the application, it is not intended as the primary means of communicating emergency broadcast messages (such as a building evacuation order) and you should ensure there are alternate methods to communicating broadcast emergency messages.

4.2.1 Send an Alert

1. Select the desired message in the **Select Message** dropdown
2. Select **Group(s)** or **Display(s)** – changing this selection will update the table below
3. Select the checkbox near the groups or displays you want to push the message to
 - a. Note: You can use the Filter at the top of the table to narrow your search



4. Select the **Send** button at the top

Additionally, you can activate alerts, per display, from the **Display View** on the **Dashboard**. To do this, click on the **Send Alert** link next to the display, select the message you want to send, and select **Send**.

4.2.2 Clear an Alert

When there are active alerts, an option will appear at the top of the page that will allow you to select **Send Alert** or **Clear Alert**. Selecting **Clear Alert** will update the options within the page.

Selecting the **Clear** button next to **Clear Active Alert(s)** will cause all active alerts to be cleared based on the options you select below.

The **Clear Alerts From** options must be selected before you select the **Clear** button. Select one of the options:

- **Group(s)** – This will allow you to clear alerts for a selected group of displays
- **Display(s)** – This will allow you to clear alerts for specific displays
- **Displays with Specified Active Alert** – This will allow you to clear an alert for a give message

Selecting one of these radio buttons will provide additional options for you to choose from. Make the specific selection based on the displays or alerts you want to clear, then select the **Clear** button.

You can also clear active alerts from the Dashboard.

In the **Display View** on the **Dashboard** you can clear an alert per display by selecting the Clear link in the row of the display.

In the **Active Alerts View** on the **Dashboard** you can, you can select the **Clear** link in the **Clear All** column in the same row as the message you want to clear.

4.3 Messages

This page will allow you to manage or create new messages.

Messages are divided in to 3 sections, a header, body, and footer. You can add text, configure the text color, and background color for each of these sections.

In addition, the Body will allow you to specify a URL to an image. The Image can be remote, or you can specify a local file by using [file:///](#) and specifying the path.

To create a new message:

1. Select **New Message** from the **Select Message** drop down
2. Enter a unique name for the message
3. Add text, images, and update the colors
4. Select the **Save** button at the bottom



To Modify a message, select the message from the **Select Message** drop down.

You can also delete a message by selecting it from the **Select Message** drop down and selecting the **Delete** button at the bottom of the page.

4.4 Displays

A display is the primary monitor attached to a hub running the Intel Unite® app with the plug-in installed. When the System Broadcast plugin is loaded on the hub, it will automatically show up in the table on the Displays page.

You can pre-add displays by entering the system name of the hub in the **Add New Display** area and selecting **Save**.

4.5 Groups

Groups provides a way for you to organize your displays and push/clear alerts to multiple displays at one time.

To add a group, enter a new group name in the **Add New Group** section and select **Save**.

Groups can be managed or deleted using the links within the table. Edit will allow you to rename the group, and modify hubs assigned to the group.

4.6 Users

Authentication and identity is managed by your organization. However, the Users page will allow you to set permissions for users you've configured to use the admin page.

To add a new user, enter their user ID in the **Add New User** section, select the desired permissions, and select **Save**.

The permissions are:

- **Read Permissions:** This will allow a user to view the dashboard, but the user will not be able to send alerts, add, update, or delete any entries on any page.
- **Write Permissions:** This will allow a user to push an alert and will also allow them to add an update displays, groups, and messages. The user will not be allowed to delete or modify user settings.
- **Delete Permissions:** The user will be allowed to push and clear permissions, read, add, update, and delete displays, groups, and messages. However, the user will not be allowed to modify user settings.
- **Admin Permissions:** This role provides all access and permissions. This is the only role that will be allowed to modify user permissions.



- **Inactive:** Checking this will remove all of the user's permissions until this is unchecked.

4.7 Tokens

This solution includes an API that allows IT to integrate this with an external system. You can read more in the API section of this guide.

This page provides a way for you to manage the API tokens for your deployment. You can create, extend, and de-active tokens.

To create a new token, click on the "Create New Token" button below the table. The token will be generated with a 1-month expiration by default. You can extend that by clicking on the "Extend" button in the "Expire Time" column.

You can revoke a token by marking it as Inactive. Marking a token as Inactive will disallow it, even if it hasn't expired.

4.8 System Configuration

This page will allow you to set some of the options you specified during installation.

Port 1 – The plugins running on the hub connect to the server via WebRTC using this port. Note: You may have to add firewall exceptions for these incoming ports on the server.

Port 2 – This is an internal port that is only used on localhost. This is the port that the server-side components will use to communicate.

Use SSL on localhost – This setting specifies if the server components, which communicate on localhost on the server, will use SSL to communicate. This is **Yes** by default. Setting this to **No** is less secure.

If set to **Yes**, a **Certificate** choose will appear. This option allows you to specify which certificate will be used.



5. Programmer API

This solution includes an API that will allow you to send and clear pre-configured messages. This will allow you to integrate it with existing systems and automate the key functions of sending and clearing an alert. To do this, you must first acquire an API token from the admin portal. See the Tokens section in this guide.

Note: These APIs can only send pre-configured messages. You will need access to the SQL database to retrieve the id of the message.

- **Parameters Object**
 - ApiKey (string)
 - This is the api token
 - Tokens are managed on the admin portal
 - Message (object)
 - ID_Message (int)
 - This is the ID_Message field from the Messages table in SQL for the alert being sent
 - ListID_Hub (Array<string>)
 - This is an array of Displays from the Displays tab on the admin portal
 - This parameter is optional. If it is not included, the alert/clear will be broadcasted to all displays.

```
{
  "ApiKey": "123456789abcdefg",
  "Message": {
    "ID_Message": 1
  },
  "ListID_Hub": [
    "some.hub.id",
    "some.other.hub.id"
  ]
}
```

- **Send Alert API**
 - URL: /systembroadcast/api/message/sendalert
 - HTTP Verb: POST
 - Body: Parameters Object
- **Clear Alert API**
 - URL: /systembroadcast/api/messag/clearalert
 - HTTP Verb: POST
 - Body: Parameters Object



6. Troubleshooting

This section will guide you through troubleshooting your installation by viewing the log files.

6.1 Logging

The System Broadcast server logs messages to the Windows Event Viewer:

1. Open Event Viewer
2. Expand **Application and Services Log**
3. Select **SystemBroadcastServerLog**

The Intel Unite® plugin will log messages to the Intel Unite® app log. You can access this log by starting the Intel Unite® app on the hub with the debug parameter:

1. Close the Intel Unite® app on the hub
2. Open **CMD**
3. Execute the Intel Unite® app using the debug flag:

```
"C:\Program Files (x86)\Intel\Intel Unite\Hub\Intel Unite.exe" /debug
```

You can also enable a persistent debug log by setting the **LogFile** registry key on the hub.

1. Close the Intel Unite® app on the hub
2. Open **RegEdit**
3. Expand this path: **HKEY_LOCAL_MACHINE\Software\Intel\Unite**
 - a. **Note:** You may need to create the **Unite** key
4. Right click on **Unite** and select **New**, then **String Value**
5. Enter **LogFile** for the name
6. Set the value to the full location where you want to store the log file
 - a. Example: "C:\temp\intelunite.log"
7. Start the Intel Unite® app

6.2 Plugin Unable to Connect

You may need to adjust the authentication settings in IIS on the System Broadcast server If the Intel Unite® plugin is unable to connect and you see this error in the Intel Unite® app log:

EXCEPTION: Web Socket ConnectAsync Error - The remote server returned an error: (401) Unauthorized.

To resolve this:

- 1) Open IIS Manager on the server
- 2) In the left pane, expand the server name



- 3) Expand: **Sites -> Default Web Site -> System Broadcast -> Server**
- 4) In the left pane, select **ws**
- 5) In the middle pane, select **Authentication**
- 6) Set **Anonymous Authentication** to **Enabled**
- 7) Set everything else to **Disabled**

Another reason a plugin may not be able to connect is that the server certificate isn't trusted. If you have used a self-signed certificate, you will need to add the self-signed certificate to the root of trust.

You must also ensure that the port you specified for incoming connections during installation of the server is allowed through the firewall.

6.3 Intel Unite® app crash

If you have multiple Intel Unite® plugins installed which utilize the Newtonsoft.Json library, you may encounter an unexpected crash due to incompatibility. To resolve this issue:

1. Exit the Intel Unite® app on the hub
2. Open Notepad as administrator
 - a. Enter **Notepad** into the Windows Search area
 - b. Right click on **Notepad** in the search results and select **Run as administrator**
3. Select **File** and **Open**
4. Select: **C:\Program Files (x86)\Intel\Intel Unite\Intel Unite.exe.config**
5. Add the following block of text in the **configuration\runtime\assemblyBinding** node

```
<dependentAssembly>
  <assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30ad4fe6b2a6aeed" culture="neutral" />
  <bindingRedirect oldVersion="0.0.0.0-10.0.0.0" newVersion="10.0.0.0" />
</dependentAssembly>
```

Example:

```
<configuration>
  <startup>
    <supportedRuntime version="v4.0" sku=".NETFramework,Version=v4.5"/>
  </startup>
  <runtime>
    <assemblyBinding xmlns="urn:schemas-microsoft-com:asm.v1">
      <probing privatePath="plugins"/>
      <dependentAssembly>
        <assemblyIdentity name="Newtonsoft.Json" publicKeyToken="30ad4fe6b2a6aeed"
culture="neutral" />
        <bindingRedirect oldVersion="0.0.0.0-10.0.0.0" newVersion="10.0.0.0" />
      </dependentAssembly>
    </assemblyBinding>
  </runtime>
```

6. Select **File** and **Save**



7. Restart the Intel Unite app