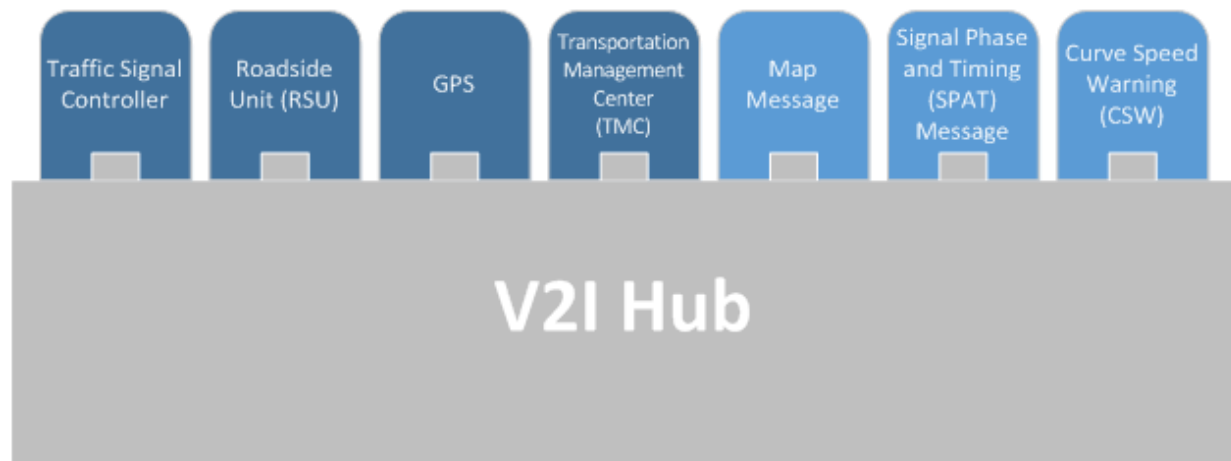


V2I Hub

Administration Portal User Guide

www.its.dot.gov/index.htm

Final Report – July 3, 2018
FHWA-JPO-18-646



U.S. Department of Transportation

Produced by Battelle Memorial Institute under DTFH61-12-D-00040
U.S. Department of Transportation
Office of the Assistant Secretary for Research and Technology
Joint Program Office

Notice

This document is disseminated under the sponsorship of the Department of Transportation in the interest of information exchange. The United States Government assumes no liability for its contents or use thereof.

The U.S. Government is not endorsing any manufacturers, products, or services cited herein and any trade name that may appear in the work has been included only because it is essential to the contents of the work.

Technical Report Documentation Page

1. Report No. FHWA-JPO-646	2. Government Accession No.	3. Recipient's Catalog No.	
4. Title and Subtitle V2I Hub Administration Portal User Guide		5. Report Date July 3, 2018	
		6. Performing Organization Code Battelle	
7. Author(s) William Gibbs, Veronica Hohe		8. Performing Organization Report No.	
9. Performing Organization Name and Address Battelle 505 King Ave Columbus, OH 43201-2693		10. Work Unit No. (TRAIS)	
		11. Contract or Grant No. DTFH61-12-D-00040	
12. Sponsoring Agency Name and Address Federal Highway Administration 1200 New Jersey Avenue, S.E. Washington, DC 20590		13. Type of Report and Period Covered Final	
		14. Sponsoring Agency Code FHWA	
15. Supplementary Notes			
16. Abstract <p>Connected and automated vehicle (CAV) technologies help reduce the number of driving-related injuries and fatalities by allowing road users to be aware of potential dangerous situations on the road. This user guide is intended for IT staff of State and local Departments of Transportation (DOT) and Metropolitan Planning Organization agencies and contractors responsible for deploying V2I Hub infrastructure connectivity equipment supporting CAV deployments. It provides an overview of operation and configuration of the Administration Portal used for the deployment of the V2I Hub.</p>			
17. Keywords CAV, V2I, safety, deployment, V2I Hub, SPaT, V2I Reference Implementation		18. Distribution Statement Unlimited	
19. Security Classif. (of this report) Unclassified	20. Security Classif. (of this page) Unclassified	21. No. of Pages 70	22. Price

Table of Contents

Executive Summary	1
Chapter 1. Administration Portal Overview	3
V2I Hub Software	3
Administration Portal Overview	4
Portal Header	4
Portal Display.....	5
Chapter 2. Administration Portal Installation	7
Administrator User Interface Installation	7
Chapter 3. Command Plugin	9
Description	9
Installation and Configuration	9
Configuration	10
Chapter 4. Administration Portal Guide.....	13
Login to Administration Portal	13
User Permissions	13
Initial Connection to a V2I Hub Unit	13
Successful Connection to a V2I Hub Unit	15
User's Login to the V2I Hub	16
"Plugins" Tab	19
Plugin Type.....	19
Plugin Filtering.....	20
Plugin Description	21
Plugin Messages.....	24
Plugin State	24
Plugin Configuration.....	25
Remove Plugin	29
File Upload.....	31
"Messages" Tab	42
Message Information	42
Message Filtering.....	42
"Event Log" Tab.....	45
Event Information	45

Event Log Filtering	46
Clear Event Log.....	47
“Users” Tab.....	48
Passwords	49
Add a New User	49
Reset a User’s Password	51
Change a User’s Access	52
Delete a User.....	55
Appendix A. SSL Certificate Exception	57
Appendix B. Acronyms.....	61

List of Tables

Table 1. Browser Compatibility.....	3
Table 2. Command Configuration Values.....	11
Table 3. Keys for Plugin Information’s Configurable Key-Value Pairs	23

List of Figures

Figure 1. V2I Hub Administration Portal, Plugins with Core.....	4
Figure 2. Portal Plugin Overview	5
Figure 3. Plugin Expandable Sections	6
Figure 4. Initial Connection to Default IP Address	14
Figure 5. Invalid IP Address for Connection Denoted by Red Background	14
Figure 6. Valid IP Address for Connection Denoted by White Background	15
Figure 7. Connection to New IP Address	15
Figure 8. Login Page after Successfully Connecting to V2I Hub	16
Figure 9. Login Attempt without Username Inputted.....	16
Figure 10. Login Attempt without Password Inputted	17
Figure 11. Login Attempt without Username and Password Inputted	17
Figure 12. Login Attempt with Invalid Information	18
Figure 13. Administration Portal after Successful Login	18
Figure 14. Plugin Expandable - Topmost Level	19
Figure 15. Enabled Plugin Expandable.....	19
Figure 16. Disabled Plugin Expandable.....	20
Figure 17. External Plugin Expandable.....	20
Figure 18. Multiple Plugin Filters Selected.....	21
Figure 19. Plugin with Topmost Level Expanded	21
Figure 20. Full Plugin Description Shown with ToolTip	22
Figure 21. Plugin Information Expanded.....	22
Figure 22. Configurable Plugin Information Key-Value Pair Input	23

Figure 23. Configurable Plugin Information Key-Value Pair Submitted and Waiting for New Value	23
Figure 24. Plugin Messages.....	24
Figure 25. Plugin State.....	24
Figure 26. Plugin Configuration Expanded	25
Figure 27. Waiting for New Value after Modifying a Configuration Parameter	26
Figure 28. Modified Configuration Parameter After Value was Accepted	27
Figure 29. New Configuration Parameter Dialog Window	28
Figure 30. New Configuration Parameter "Test Key" Added to Plugin	29
Figure 31. "Remove" Button to Remove a Plugin	29
Figure 32. "Remove Plugin?" User Confirmation Dialog Window.....	30
Figure 33. Plugin was Removed from the Plugin List	30
Figure 34. File with Invalid File Extension Selected for File Upload	31
Figure 35. File with Valid File Extension Selected for File Upload.....	32
Figure 36. File Exceeding Maximum File Size Selected for File Upload	32
Figure 37. File Violating Multiple Restrictions Selected for File Upload	32
Figure 38. "Upload File" Button to Select File Upload Information	33
Figure 39. "File Upload" Dialog Window	33
Figure 40. Application Administrator's File Upload Options	33
Figure 41. System Administrator's File Upload Options.....	34
Figure 42. File Upload Inputs Reset When a File Option is Selected	34
Figure 43. File Upload Option - "Upload Plugin"	35
Figure 44. File Upload Option - "Upload Map"	35
Figure 45. File Upload Option - "Upload Other"	35
Figure 46. Selecting an Upload Directory for File Upload Option "Upload Other"	36
Figure 47. File Upload Transfer Initiated	37
Figure 48. File Upload Transfer in Progress	38
Figure 49. "Command Error" Dialog Window with File Upload Failure Message	38
Figure 50. File Upload Transfer Completed	39
Figure 51. Notification Indicating Plugin Installation in Progress	40
Figure 52. Notification Indicating Plugin Installation is Complete	41
Figure 53. "Command Error" Dialog Window with Plugin Install Failure Message	41
Figure 54. Messages Table	42
Figure 55. Messages Table – Filter by Time Dropdown Menu.....	43
Figure 56. Messages Table – Hidden Keep Alive Messages.....	43
Figure 57. Messages Table - Shown Keep Alive Messages	44
Figure 58. Messages Table – Search Filter	44
Figure 59. Event Log Table	46
Figure 60. Event Log Table - Search Filter	47
Figure 61. Event Log Table - Cleared After Pressing "Clear Log" Button	48
Figure 62. Users List Table	48
Figure 63. "Add New User" Dialog Window	49
Figure 64. "Add New User" Dialog Window with "Select Access Level" Dropdown Menu Opened	50
Figure 65. "Add New User" Dialog Window with Mismatched Passwords	50

Figure 66. Command Error Dialog Window with an Add New User Failure Message	51
Figure 67. “Change User Password” Dialog Window	51
Figure 68. “Change User Password” Dialog Window with Mismatched Passwords.....	52
Figure 69. “Command Error” Dialog Window with User Update Failure Message for Changing a User's Password	52
Figure 70. Users List Table	53
Figure 71. “Change User Access” Dialog Window.....	53
Figure 72. “Change User Access” Dialog Window with Select New Access Dropdown Menu Open	54
Figure 73. Users List Table with an Updated Access Level	54
Figure 74. “Command Error” Window with a User Update Failure Message for Changing a User’s Access Level	55
Figure 75. “Delete User” Dialog Window	55
Figure 76. Users List Table with User Deleted	56
Figure 77. Insecure Connection Page for "https://<IP Address>:19760	57
Figure 78. Advanced Options for an Insecure Connection	58
Figure 79. Adding an Exception for an Insecure Connection.....	58
Figure 80. Exception Added for an Insecure Connection	59

Executive Summary

The Vehicle-to-Infrastructure (V2I) Reference Implementation Administration Portal User Guide was developed by Battelle on behalf of the Federal Highway Administration (FHWA) for IT staff of State and local Departments of Transportation and Metropolitan Planning Organization agencies and contractors responsible for deploying V2I Hub infrastructure connectivity equipment supporting connected and automated vehicle (CAV) communications. This user guide gives an overview of operation and configuration of the Administration Portal used for the deployment of the V2I Hub. The V2I Hub is a connectivity platform developed to be deployed at signalized intersections, and other infrastructure locations, with the intention of making roadways safer and smarter by reducing accidents and providing informational alerts to mobile users. This document is a part of the V2I Hub series of documents produced by the V2I Reference Implementation project. The rest of the documents are listed below. It is suggested to start with a review of the V2I Hub Guidebook.

- V2I Hub Guidebook
- V2I Hub Plugin Programming Guide
- V2I Hub Plugins
- V2I Hub Deployment Guide
- V2I Hub Software Configuration Guide

Chapter 1. Administration Portal Overview

V2I Hub Software

The V2I Hub software is a deployment-ready solution for implementing CAV applications at the roadside infrastructure. It was created and tested on Ubuntu 16.04 LTS but can run on most Linux operating systems. The V2I Hub architecture is modular, enabling different installed instances to be configured to run varied combinations of plugins and software applications. The V2I Hub software contains communication routing, plugin configuration, and plugin-monitoring to manage communication processes. Each plugin in the V2I Hub software is created to perform a function, such as communicate with a signal controller or produce Signal Phase and Timing (SPaT) messages. The Administration Portal allows users to install, configure, and control the plugins through a graphical interface implemented in Hypertext Markup Language (HTML) 5 and JavaScript. The Administration Portal has been tested with the latest version of Firefox and Chrome at the time of release (see Table 1). Compatibility with other browsers has not been verified.

Table 1. Browser Compatibility

Browser	Version
Firefox Quantum	58.0.2 (64-bit)
Google Chrome	64.0.xxx (64-bit and 32-bit)

The Administration Portal communicates to the V2I Hub Core (V2I Hub) through the CommandPlugin using Secure Sockets Layer (SSL) WebSockets. The V2I Hub architecture is shown in Figure 1.

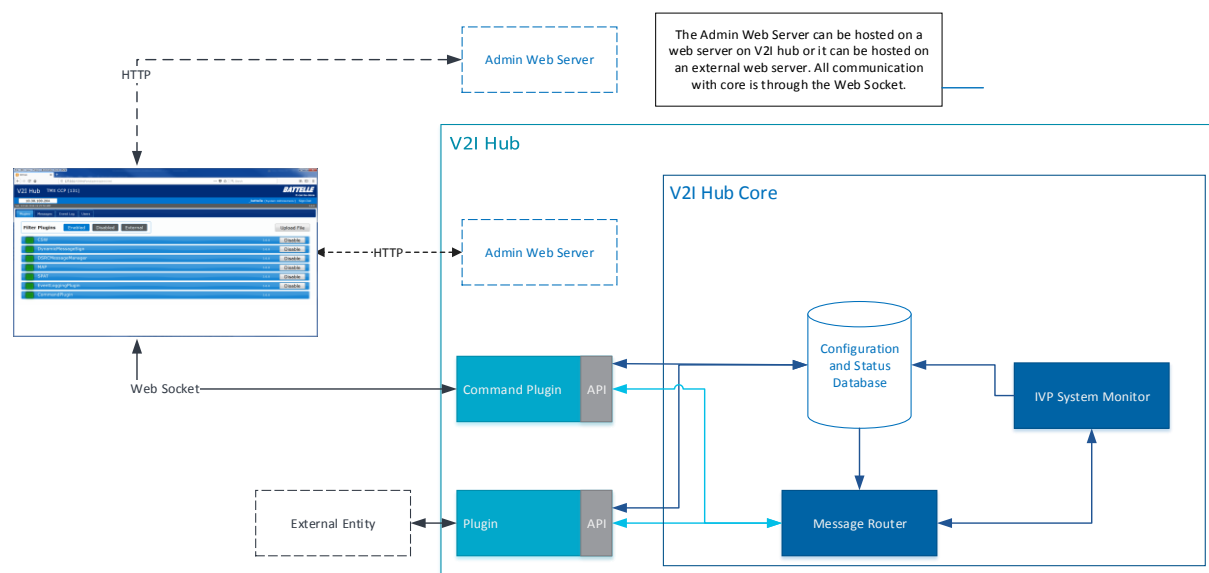


Figure 1. V2I Hub Administration Portal, Plugins with Core

Administration Portal Overview

This section provides a brief overview of the Administration Portal. More detailed descriptions and usage can be found in the Administration Portal Guide section of this document. The Administration Portal is a HTML-based user interface (UI) that allows users to install, configure, and monitor plugins. The portal uses WebSockets to communicate to the CommandPlugin, which executes commands from the user. The Administration Portal does not need to be hosted on the same machine as the V2I Hub as the connection is not based on the hosting server. This allows great flexibility in connecting to different V2I Hubs in one Administration Portal UI session. All WebSocket connections are SSL-encrypted.

The portal interface has two major sections consisting of a header and a tab-separated main display. A screen capture of the portal and short descriptions of the display areas can be found in the Portal Display section of this document.

Portal Header

The portal header contains the information relating to the user and the connection. On the left side of the header, the V2I Hub's instance name, Internet Protocol (IP) address, and time are shown. The connection status, user and access level and version are displayed on the right side of the header.

When the portal is not connected to the V2I Hub, the

- Battelle logo appears gray,
- Username and role are not visible,
- V2I Hub instance name is not visible, and
- Local time is reflected.

When a connection is made to the CommandPlugin and a user is not yet logged in, the

- Battelle logo turns white, and
- Login page opens

Upon successful login,

- V2I Instance name updates and becomes visible,
- Username and access level are populated,
- “Sign Out” button appears, and
- Time display transitions to the V2I Hub time.

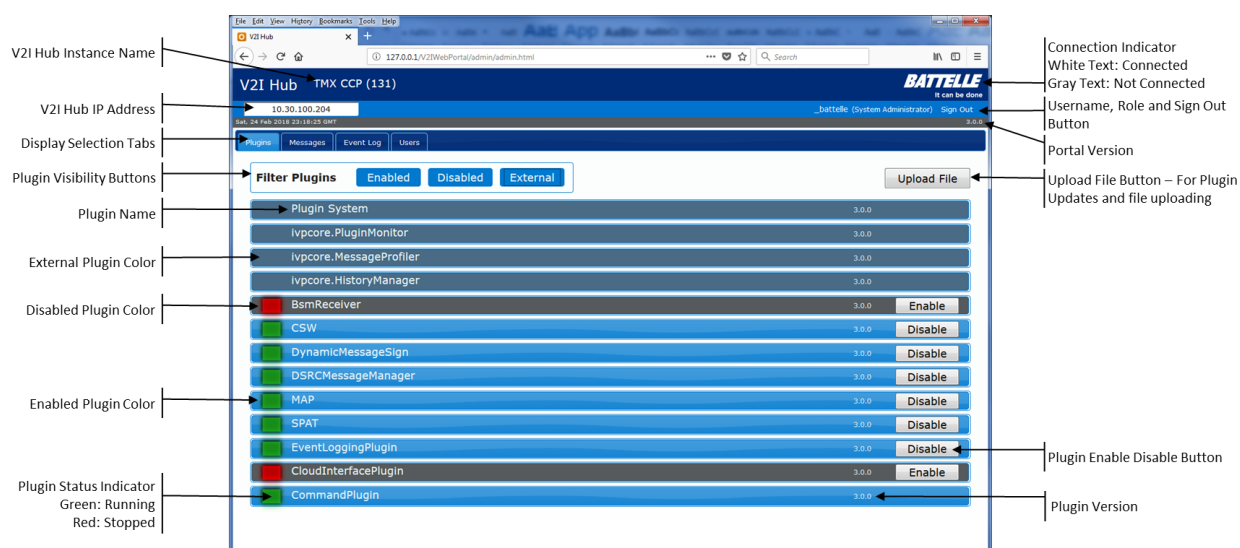


Figure 2. Portal Plugin Overview

Portal Display

The main display of the portal consists of tab-separated pages that contain the plugin information, V2I Hub messages, event log messages, and user administration. The different pages are selected by clicking on the appropriate display selection tab.

The Plugins tab contains a filterable list of currently installed and connected plugins. The plugin filters are “Enabled”, “Disabled”, and “External”. These plugins will be explained further in the Administration Portal Guide section, but external plugins are plugins that connect directly to the V2I Hub without being installed. The external plugins are comprised of some core plugins, including the PluginSystem which can set system-wide configuration items. Each plugin display contains multi-layered expandable sections that allow the user to drill down for more detailed information about the configuration and status of the plugin. The expandable sections can be seen in Figure 3.

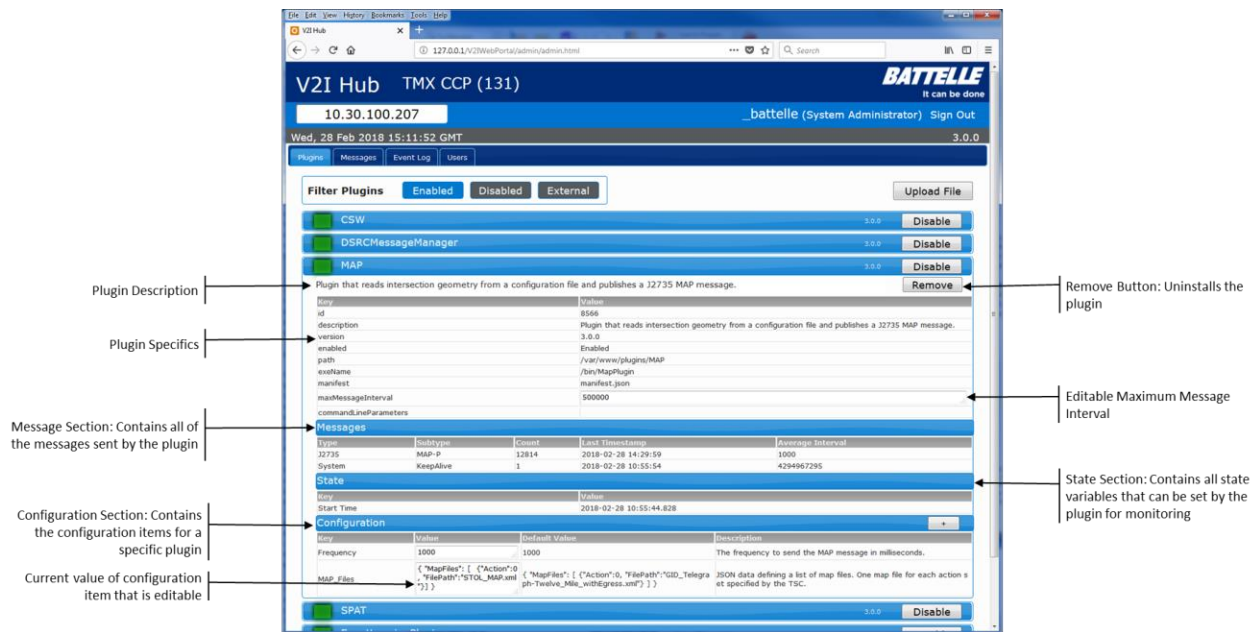


Figure 3. Plugin Expandable Sections

The Messages Tab contains a table of all message types being exchanged on the V2I Hub. These messages can be sorted by time and by a search filter.

The Event Log Tab contains a table with the most recent event log entries from the plugins along with a clear log functionality for System and Application Administrator users.

The Users Tab allows a System Administrator to add new users and to reset passwords, change access, and delete current users.

Chapter 2. Administration Portal Installation

The installation section details the process to install the Administration portal and support plugin for Operation. The HTML based User Interface and the V2I Hub Command Plugin must be installed and configured for the User Interface to operate correctly.

Administrator User Interface Installation

The user interface is an HTML based interface and can be deployed using any modern web server. This section will use the Apache Web Server installed on an Ubuntu 16.04 system. Once the web server is installed, the User Interface files are copied to the web directory.

1. Log in to the V2I Hub using the username and password provided by the owner of the V2I Hub
2. Update the apt-get system and install Apache

```
sudo apt-get update  
sudo apt-get install apache2
```

3. After Apache has installed successfully the default root for the web server will be /var/www/html
4. Copy all directories and files for the admin portal to the /var/www/html directory
5. The Administration Portal can then be reached by using the system's IP address. The index.html file will automatically forward the browser to the Administration Portal.

`http://<ip address>`

Chapter 3. Command Plugin

Description

The Command Plugin contains a websocket server that allows the Administration Portal to communicate to the V2I Hub system. The plugin also implements the ability to download files to the target system. The plugin sends the current status of the system to the UI and receives commands, files and configuration values from the UI. The websocket connection is SSL encrypted. The plugin is distributed without a SSL certificate but directions to create a self-signed certificate are included. A valid SSL certificate can be used.

NOTE: Instructions for adding an exception for the SSL certificate can be found in SSL Certificate Exception description in Appendix A.

Installation and Configuration

To install the plugin, you will need to obtain the plugin installation package for the Command plugin either from your hardware provider or by compiling the source code for the V2I Hub from the U.S. DOT's Open Source Application Development Portal. The package will either be a Debian installation package ending in .deb or a zip file ending in .zip. Once the installation packages have been obtained, install the plugin on the command line of the target system using the steps below. The V2I Hub must be installed to perform these steps.

1. Move the package to the target system
2. Open a terminal on the target system
3. Change to the directory that contains the package
4. Issue the following command to install the plugin. The package can be of type .deb, .tar.gz, or .zip.

```
tmxctl --plugin-install tmx-3.0.0-Linux-armhf-commandplugin.deb
```

5. The plugin must be configured
6. To generate a self-signed SSL certificate, issue the following commands. Substitute your information for the bold italic text including the brackets.

```
cd /var/www/plugins
sudo mkdir .ssl
sudo chown plugin .ssl
sudo chgrp www-data .ssl
cd .ssl
sudo openssl req -x509 -newkey rsa:4096 -sha256 -nodes -keyout tmxcmd.key -out
tmxcmd.crt -subj "/CN=<your website url>" -days 3650
sudo chown plugin *
sudo chgrp www-data *
```

7. Generate an administrator account for the Admin Portal user to login

```
mysql -uroot -p[your database root password here] -e "INSERT INTO IVP.user  
(IVP.user.username, IVP.user.password, IVP.user.accessLevel) VALUES ('<admin  
username>', '<admin password>', 3)"
```

8. Enable the plugin

```
tmxctl --plugin CommandPlugin --enable
```

The Command Plugin will be running now, and the Administrator Portal will be able to connect to the V2I Hub.

Configuration

The Command plugin has configurations to set the directories and other plugin parameters. Table 2 contains the configuration values for the Command plugin.

Table 2. Command Configuration Values

Key	Default Value	Description
DownloadPath	/var/www/download	The path to the directory where downloaded files will be saved on the target system. Any directory here must have write permissions for the www-data user,
EventRowLimit	50	The maximum number of rows returned for the initial Event Log query. This configuration item limits the number of previous log messages that are loaded on startup. Generally, keep this under 100 unless you are debugging an issue. Numbers above 100 cause delays in loading the initial page due to the volume of messages.
LogLevel	ERROR	The log level for this plugin. Keep this at ERROR unless an issue is being debugged.
SleepMS	100	The length of milliseconds to sleep between processing all messages. Recommend this value not be changed as it represents the amount of time for the plugin to wait between checks for incoming messages. Lower values increase CPU usage and higher values increase latency in message processing and responses.
SSLEnabled	true	Enables secure connection using SSL. Do not change this value. The Web Portal uses SSL certificates and the option cannot be changed there. If this is set to false, the Administration Portal will not be able to connect to the Command Plugin.
SSLPath	/var/www/plugins/.ssl	The path to the directory containing the SSL key and certificate files.

Chapter 4. Administration Portal Guide

Login to Administration Portal

To access information from the V2I Hub, a user must login to the V2I Administration Portal. Different permission levels provide different functions from within the Administration Portal. The Administration Portal must have an SSL exception to successfully connect to the V2I Hub. Once a persistent connection is opened, a user may login, review, and configure V2I Hub information. The SSL certificate verifies there is a secure connection to a trusted website. Since the website is local and known, the website is trusted and there is no challenge with adding an exception. The data will be encrypted between the Administration Portal UI and the V2I Hub and the exception will only apply to this specific website.

NOTE: Instructions for adding an exception for the SSL certificate can be found in SSL Certificate Exception description in Appendix A.

User Permissions

There are three levels of user permissions to a V2I Hub:

1. Read Only

A Read Only user can only view the V2I Hub information. This user can make no changes to plugins or users.

2. Application Administrator

An Application Administrator user can view V2I Hub information, change all plugin settings, and add new plugins.

3. System Administrator

A System Administrator user can view V2I Hub information, change all plugin settings, and add new plugins. This user can also add, remove, and modify other users.

Initial Connection to a V2I Hub Unit

When the V2I Administration Portal opens, a connecting page is displayed as shown in Figure 4. The “Connecting to wss://<IP address>:19760/...” text, spinning animation, and a gray Battelle logo indicate that the Administration Portal is waiting to connect to the CommandPlugin of a V2I Hub.

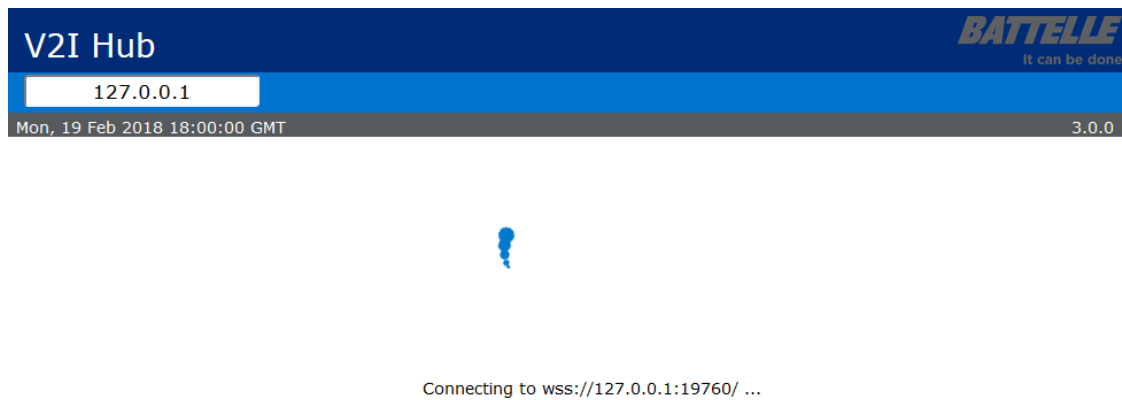


Figure 4. Initial Connection to Default IP Address

An operator can change the connection <IP address> to the V2I Hub's IP address by editing the white input text field below the "V2I Hub" header. The IP input text field's background color turns red, as shown in Figure 5, if its current value is an invalid IP address.

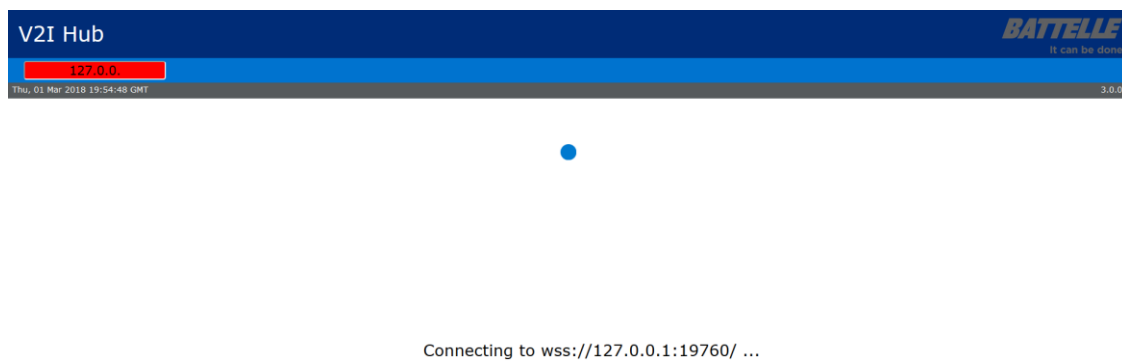


Figure 5. Invalid IP Address for Connection Denoted by Red Background

The IP input text field's background color turns white, as shown in Figure 6, if its current value is a valid IP address.

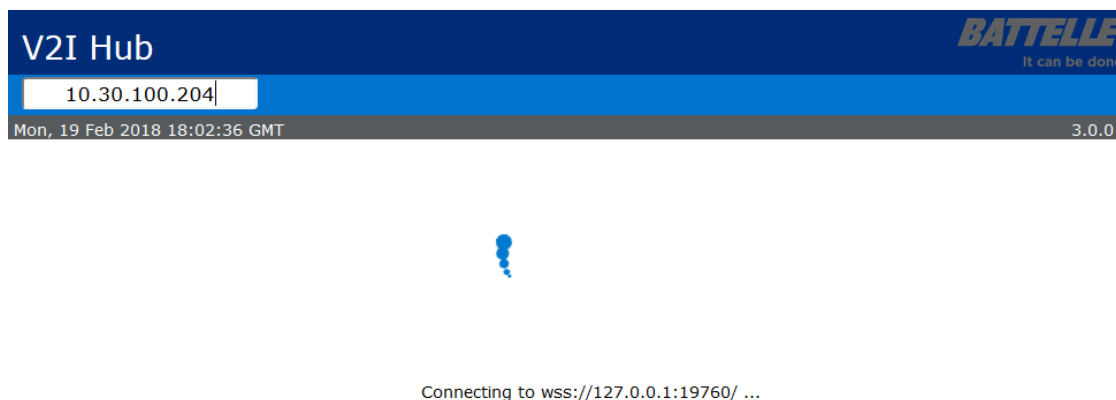


Figure 6. Valid IP Address for Connection Denoted by White Background

Once the ENTER key is pressed with a valid IP address entered in the input text field, the V2I Administration Portal will attempt to connect to this new address, as shown in Figure 7.

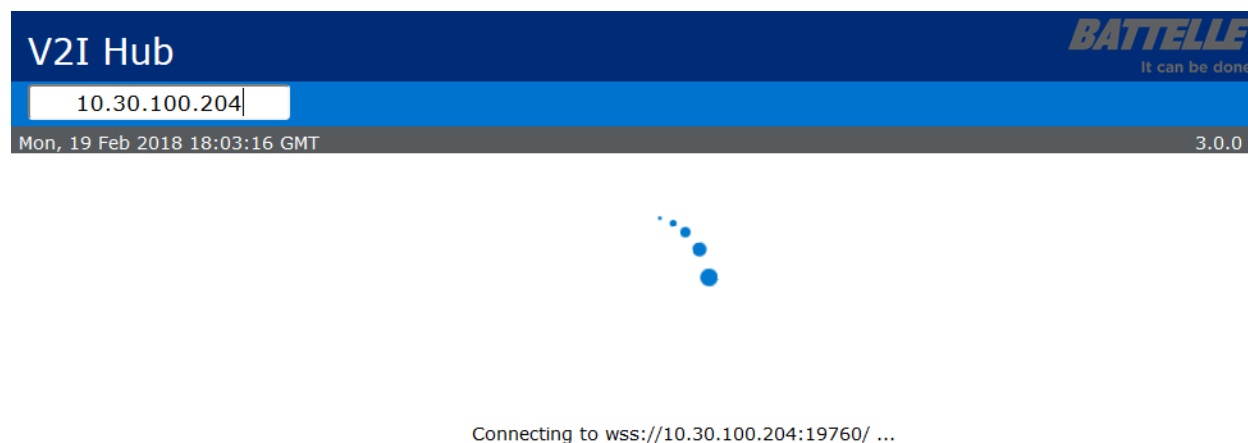


Figure 7. Connection to New IP Address

The CommandPlugin of a V2I Hub is designed to connect to multiple instances of the V2I Administration Portal over a SSL connection. The certificate, however, cannot be verified by the Firefox browser, causing the browser to choose to not connect to the CommandPlugin on the V2I Hub. Instructions for adding an exception for the SSL certificate can be found in SSL Certificate Exception description in Appendix A.

Successful Connection to a V2I Hub Unit

Upon successful connection to a V2I Hub, the Battelle logo updates from gray to white and a user login prompt appears as shown in Figure 8.

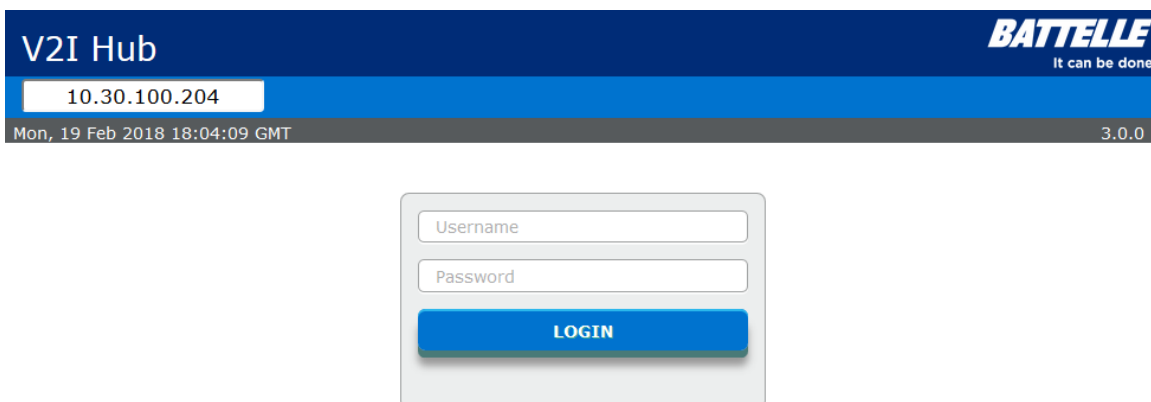


Figure 8. Login Page after Successfully Connecting to V2I Hub

Once a connection between the Administration Portal and the V2I Hub is established, the timestamp in the page header changes from the current date and time of the browser to a time that matches the time on the V2I Hub .

User's Login to the V2I Hub

The user must login to the V2I Hub to display and interact with the system and plugins. Input a valid username and password in the user login prompt and click the "LOGIN" button to initiate a connection to the V2I Hub via the CommandPlugin—the communicating plugin acting as the Administration Portal's server on the V2I Hub.

If the Username input text field is empty when the button is pressed, the field's background turns red and the Administration Portal indicates that a username is required, as shown in Figure 9.

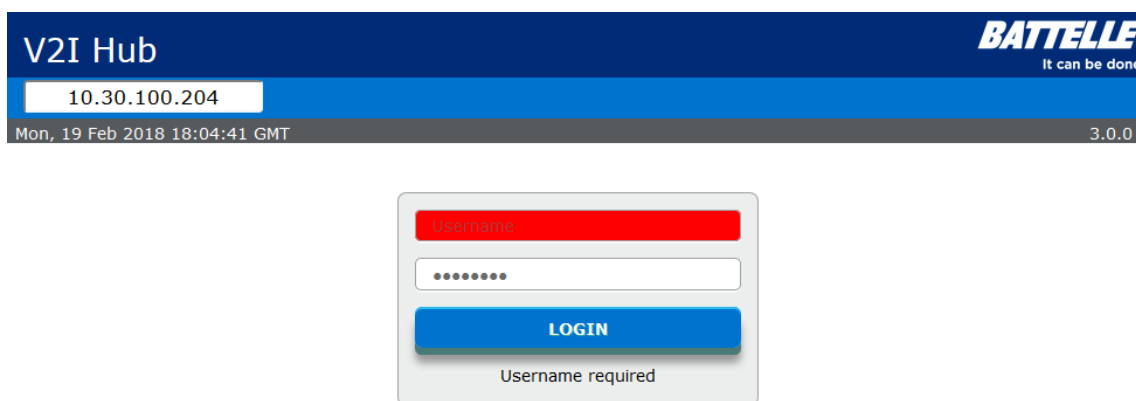


Figure 9. Login Attempt without Username Inputted

Likewise, if the Password input text field is empty when the “LOGIN” button is pressed, the field’s background turns red and the Administration Portal indicates that a password is required as shown in Figure 10.

A login form with a light grey border. It contains three main elements: a text input field at the top with the placeholder text "_battelle", a second text input field labeled "Password" in red text with a solid red background, and a blue button labeled "LOGIN" in white. Below the button, the text "Password required" is displayed in a small, grey font.

Figure 10. Login Attempt without Password Inputted

Note that if both Username and Password input text fields are empty when the “LOGIN” button is pressed, only the Username input text field turns red and the error message states that a username is required, as shown in Figure 11. This prioritization of feedback provides guidance on which field should be filled in first as the value that will be inputted in the Password input text field is dependent on the chosen username.

A login form with a light grey border. It contains three main elements: a text input field at the top labeled "Username" in red text with a solid red background, a second text input field labeled "Password" in grey text with a white background, and a blue button labeled "LOGIN" in white. Below the button, the text "Username required" is displayed in a small, grey font.

Figure 11. Login Attempt without Username and Password Inputted

The background colors of the Username and Password input text fields do not change from red to white when being edited with new values or by pressing the ENTER key. These input text fields’ background colors only update if filled when the “LOGIN” button is pressed.

A failed attempt, as shown in Figure 12, is presented if the Administration Portal does not recognize the username, an invalid password was entered, or the Administration Portal could not complete the login for any other reason.

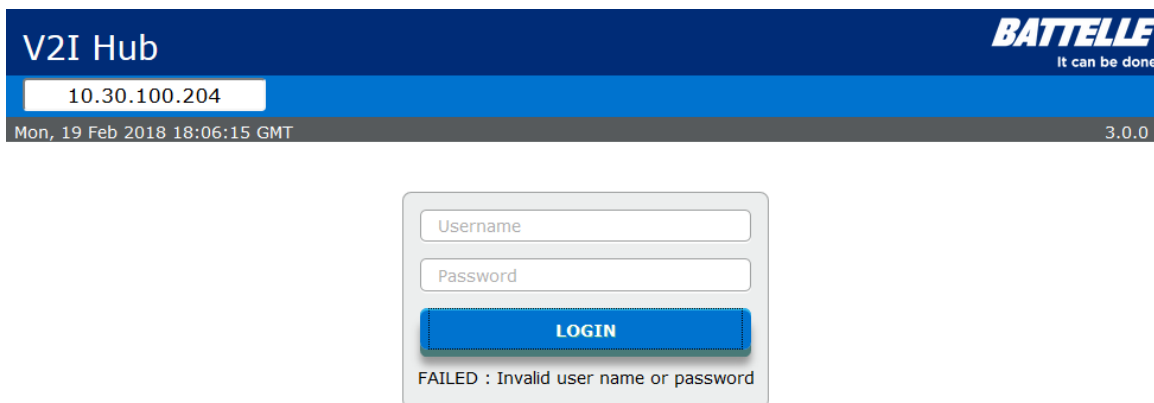


Figure 12. Login Attempt with Invalid Information

Displayed login feedback is removed from the display once the “LOGIN” button is pressed to provide space for any new feedback regarding the current login attempt.

If the Administration Portal accepts the user’s login information, the user login prompt disappears, and four navigation tabs appear beneath the header as shown in Figure 13. The header is also filled in with additional information from the V2I Hub, including the machine’s name, the currently logged in user, and the current permission level. A “Sign Out” button also appears to allow the user to log out of the V2I Hub.

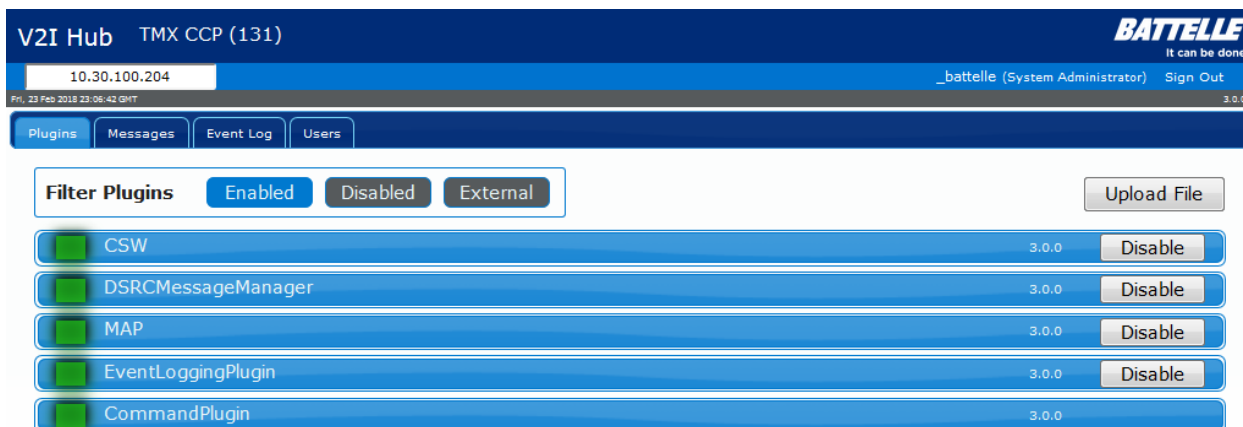


Figure 13. Administration Portal after Successful Login

“Plugins” Tab

The first tab, “Plugins”, opens by default upon successful connection to the V2I Hub. This tab displays the plugins registered in the V2I Hub as a list. The list of plugins can be filtered by selection of a button to see only enabled plugins, only disabled plugins, only external plugins, or a combination of these filters. Opening an individual plugin item in the list reveals detailed data associated with that plugin. A plugin can be removed by pressing the “Remove” button found within the plugin item (see Figure 19 below). Additional plugins or files can be uploaded via the “Upload File” button on the “Plugins” tab (see Figure 18 below).

Each plugin displayed onscreen is represented as a bar detailing basic information and actions. The bar is an expandable object containing more detailed information. When selected, the bar is expanded to reveal more actions and other expandable objects.

The topmost plugin level, as shown in Figure 14, contains the basic information associated with a plugin: the plugin’s name, version, and enabled status. The status indicator, plugin bar’s background color, and “Enable” / “Disable” button—a toggle that either displays and controls the enable state. The status indicator, background color, and button can vary depending on the type of plugin.



Figure 14. Plugin Expandable - Topmost Level

The CommandPlugin does not have an “Enable” / “Disable” button since it is acting as the server for the Administration Portal. Disabling this plugin means the Administration Portal would no longer have anything on that V2I Hub to communicate to until the CommandPlugin is re-enabled on the device, which can be done with the command-line.

Plugin Type

Plugins are categorized as three types:

1. Enabled

An enabled plugin is a plugin that is currently active and running on the V2I Hub. Bright blue bars with a green status indicator and “Disable” button on the topmost bar characterize an enabled plugin. The nested expandable bars below are also bright blue with the expandable description remaining white.

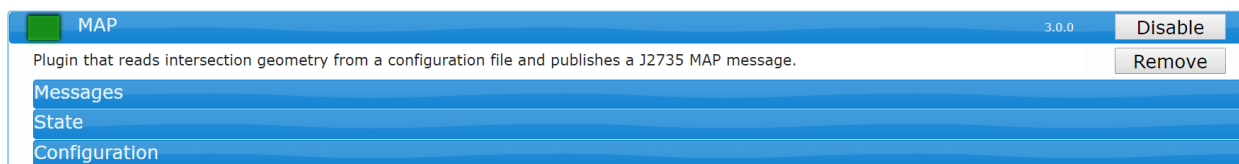


Figure 15. Enabled Plugin Expandable

2. Disabled

A disabled plugin is a plugin that is currently inactive on the V2I Hub. Gray bars with a red status indicator and an “Enable” button on the topmost bar characterize a disabled plugin. The nested expandable bars below are also gray with the expandable description remaining white.

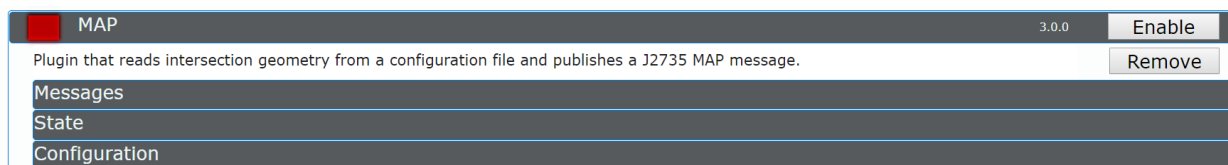


Figure 16. Disabled Plugin Expandable

3. External

An external plugin is a plugin that connects directly to the V2I Hub without being installed. Gray-blue bars with no status indicator or “Enable” / “Disable” button on the topmost bar characterize an external plugin. The nested expandable bars below are also gray-blue with the expandable description remaining white.

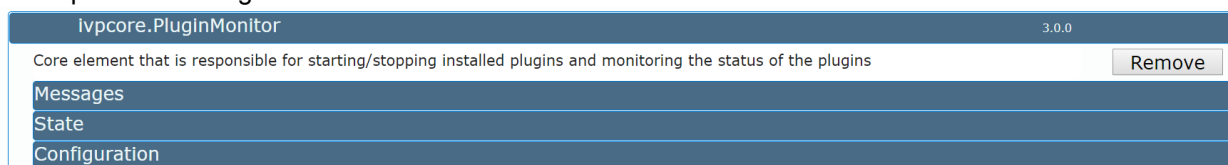


Figure 17. External Plugin Expandable

Plugin Filtering

The Administration Portal allows the user to filter the list of plugins based on plugin types. Filtering on plugin type is not mutually exclusive. Selecting multiple filter buttons presents the superset of selected plugin types rather than only those meeting all filters selected. Figure 18 exemplifies the selection of ‘Enabled’ and ‘External’ plugin filters.

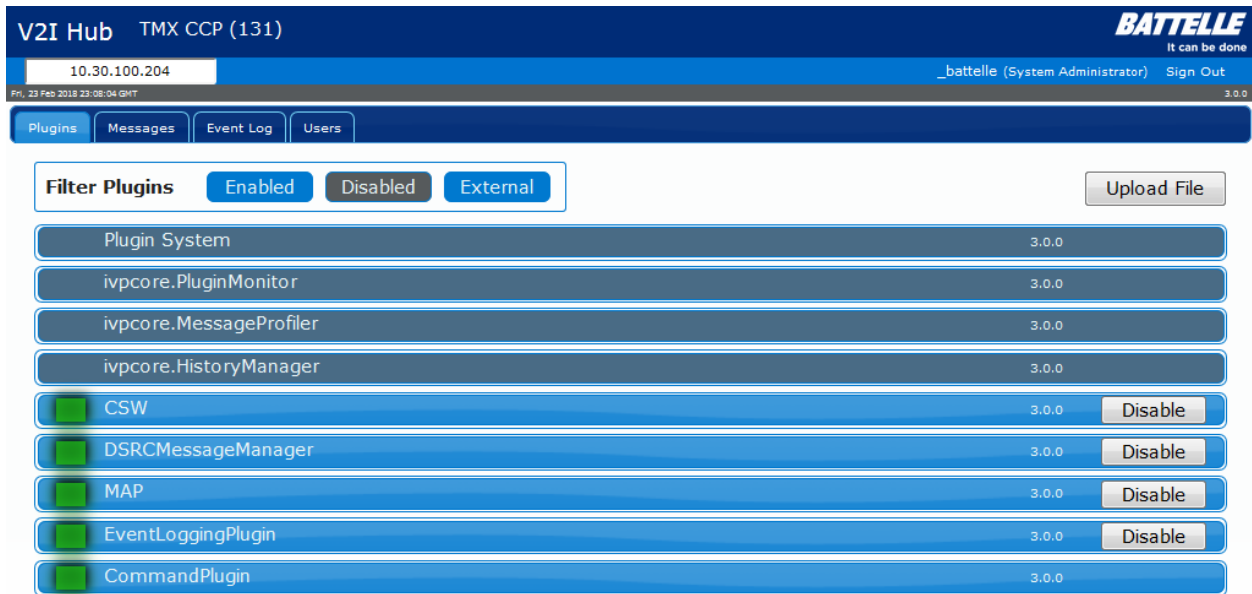


Figure 18. Multiple Plugin Filters Selected

Figure 19 shows an expanded view of the MAP plugin created when selecting the plugin bar, which includes a series of nested bars including a description of the plugin, a button to remove the plugin, and nested bars that can be selected to see additional details of the plugin including, message types, state, and configuration.

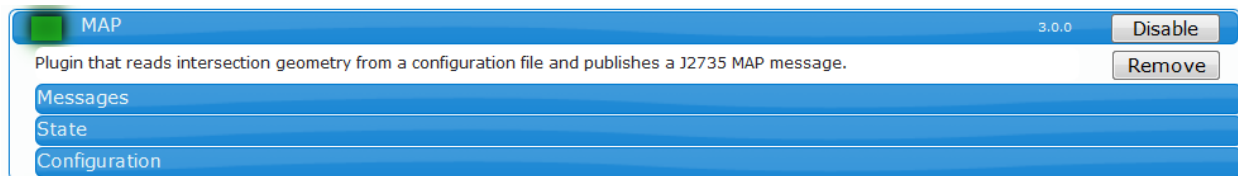


Figure 19. Plugin with Topmost Level Expanded

Plugin Description

The first nested bar is the plugin description and it provides the purpose of the plugin on a white background. If the length of the description exceeds the available space, the description is clipped using ellipsis. Hovering over this text opens a ToolTip with the complete plugin description, as shown in Figure 20.

V2I Hub TMX CCP (131) **BATTELLE** It can be done

10.30.100.207 _battelle (System Administrator) Sign Out

Tue, 27 Feb 2018 21:51:38 GMT 3.0.0

Plugins Messages Event Log Users

Filter Plugins Enabled Disabled External Upload File

Plugin Name	Version	Action
CSW	3.0.0	Disable
DSRCMessageManager	3.0.0	Disable
MAP	3.0.0	Disable
SPAT	3.0.0	Disable
Plugin that reads PTLM data from a configuration file, receives live data from the signal controller, and publishes a J2735 SPA...		Remove
Messages State Configuration		
EventLoggingPlugin	3.0.0	Disable
CommandPlugin	3.0.0	
BsmReceiver	3.0.0	Disable

Figure 20. Full Plugin Description Shown with ToolTip

Clicking on the plugin description opens a table of key-value pairs that convey the operational details of the plugin itself (see Figure 21). These key-value pairs can differ from plugin to plugin, but examples of these pairs include the plugin's description, version, executable path, and the command line parameters from which the plugin was called.

MAP 3.0.0 Disable

Plugin that reads intersection geometry from a configuration file and publishes a J2735 MAP message. Remove

Key	Value
id	8566
description	Plugin that reads intersection geometry from a configuration file and publishes a J2735 MAP message.
version	3.0.0
enabled	Enabled
path	/var/www/plugins/MAP
exeName	/bin/MapPlugin
manifest	manifest.json
maxMessageInterval	500000
commandLineParameters	

Messages
State
Configuration

Figure 21. Plugin Information Expanded

Modify Key-Value Pair of Plugin Information

Certain key-value pairs in this plugin description are configurable for Application and System Administrators (see Table 3).

Table 3. Keys for Plugin Information's Configurable Key-Value Pairs

Configurable Keys	
maxMessageInterval	

EventLoggingPlugin 3.0.0 [Disable] [Remove]

Logs events for the system.

Key	Value
id	8596
description	Logs events for the system.
version	3.0.0
enabled	Enabled
path	/var/www/plugins/EventLoggingPlugin
exeName	/bin/EventLoggingPlugin
manifest	manifest.json
maxMessageInterval	500000
commandLineParameters	

Messages
State
Configuration

Figure 22. Configurable Plugin Information Key-Value Pair Input

A user with either Application Administrator or System Administrator permissions can modify the value of configurable key-value pairs. The current value is modified by changing the value in the input text field of the "Value" column (see Figure 22) and pressing the ENTER key. If the ENTER key is not pressed, the change is not forwarded to the database. Instead, it is overwritten upon the next received message containing that configurable key-value pair or if the user clicks outside of the input. By pressing the ENTER key, the input text field's background and font colors change to gray and white respectively (see Figure 23) to indicate that a change in that configuration parameter was requested.

EventLoggingPlugin 3.0.0 [Disable] [Remove]

Logs events for the system.

Key	Value
id	8596
description	Logs events for the system.
version	3.0.0
enabled	Enabled
path	/var/www/plugins/EventLoggingPlugin
exeName	/bin/EventLoggingPlugin
manifest	manifest.json
maxMessageInterval	500000
commandLineParameters	

Messages
State
Configuration

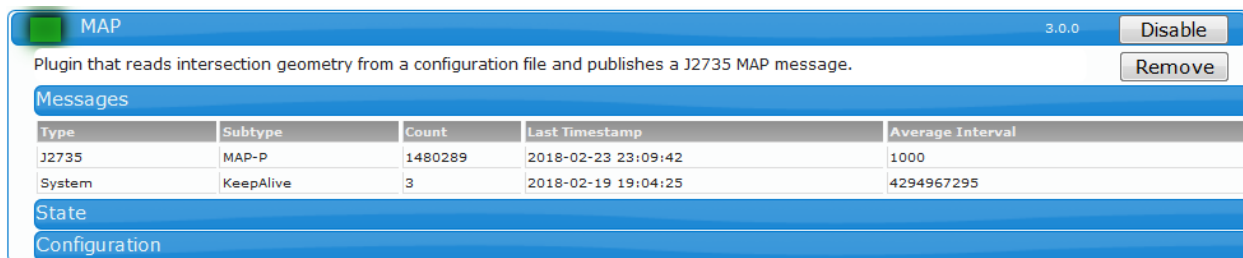
Figure 23. Configurable Plugin Information Key-Value Pair Submitted and Waiting for New Value

When the V2I Hub accepts the change for the value, a message containing that key-value pair's updated information is sent to the Administration Portal. The Administration Portal updates the input text field's value and the value input by the user is presented in black font on a white background.

The MaxMessageInterval key is the maximum number of milliseconds between messages received from a plugin. When the plugin has not sent a message in this amount of time the V2I Hub will restart the plugin. This is a watchdog timer that the V2I Hub uses to make sure the plugins are operating correctly. The plugins by default send a keep alive message every 470 seconds to keep the plugin from getting restarted. This number can be shortened for plugins that are expected to send messages at a higher frequency.

Plugin Messages

The second nested bar is labelled "Messages" and when expanded presents a table of the message types associated with that plugin, as shown in Figure 24. A subtype accompanies each message type to further differentiate the message from others of that same message type. The database maintains a count of the number of messages of that type/subtype that have been sent. The database also keeps track of when the last instance of the message type/subtype was sent. Using these pieces of information, the database can calculate the average interval of the message type/subtype to be displayed on the Administration Portal.

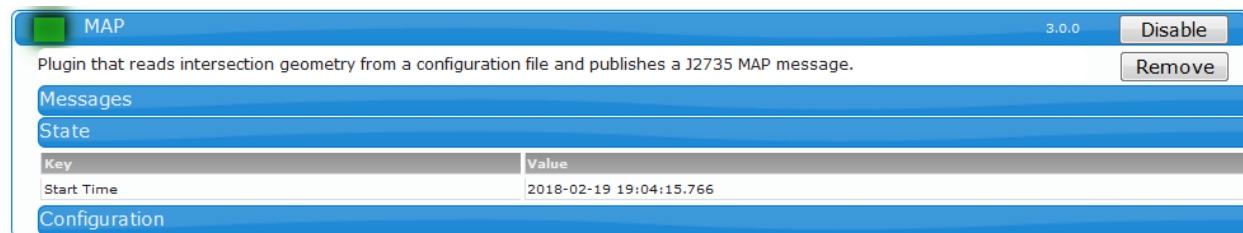


Type	Subtype	Count	Last Timestamp	Average Interval
J2735	MAP-P	1480289	2018-02-23 23:09:42	1000
System	KeepAlive	3	2018-02-19 19:04:25	4294967295

Figure 24. Plugin Messages

Plugin State

The third nested bar is labelled "State" and when expanded presents a table of key-value pairs that describe the state of the plugin, as shown in Figure 25. These key-value pairs can differ depending on the plugin.



Key	Value
Start Time	2018-02-19 19:04:15.766

Figure 25. Plugin State

Plugin Configuration

The fourth nested bar is labelled “Configuration” and when expanded presents a table of configuration parameters for the plugin, as shown in Figure 26. Each configuration parameter is sent with its identifier (“Key”), current and default values (“Value” and “Default Value”, respectively), and a description of what the parameter affects (“Description”).

Key	Value	Default Value	Description
Frequency	1000	1000	The frequency to send the MAP message in milliseconds.
MAP_Files	{ "MapFiles": [{ "Action": 0, "FilePath": "STOL_MAP.xml" }] }	{ "MapFiles": [{ "Action": 0, "FilePath": "GID_Telegraph-Twelve_Mile_withEgress.xml" }] }	JSON data defining a list of map files. One map file for each action set specified by the TSC.

Figure 26. Plugin Configuration Expanded

Modify a Plugin Configuration Parameter

A user with either Application or System Administrator permissions can modify the value of a configuration parameter. The current value of a configuration parameter is modified by changing the value in the input text field of the “Value” column and pressing the ENTER key. If the ENTER key is not pressed, the change is not forwarded to the database. Instead, it is overwritten upon the next received message containing that configuration parameter or if the user clicks outside of the input. By pressing the ENTER key, a message is sent to the CommandPlugin; the input text field’s background and font colors change to gray and white respectively to indicate that a change in that configuration parameter was requested, as shown in Figure 27.

CommandPlugin

3.0.0

Listens for websocket connections from the TMX admin portal and processes commands

Messages

State

Configuration

+

Key	Value	Default Value	Description
DownloadPath	<input type="text" value="/var/www/download"/>	/var/www/download	The path to the directory where downloaded files will be saved.
EventRowLimit	<input type="text" value="50"/>	50	The maximum number of rows returned for the initial Event Log query.
LogLevel	<input type="text" value="ERROR"/>	ERROR	The log level for this plugin
SleepMS	<input type="text" value="100"/>	100	The length of milliseconds to sleep between processing all messages.
SSLEnabled	<input type="text" value="true"/>	true	Enable secure connection using SSL.
SSLPath	<input type="text" value="/var/www/plugins/.ssl"/>	/var/www/plugins/.ssl	The path to the directory containing the SSL key and certificate files.

Figure 27. Waiting for New Value after Modifying a Configuration Parameter

When the V2I Hub accepts the change for the configuration value, a message containing that configuration parameter's updated information is sent to the Administration Portal. The input text field's value will be updated and the value input by the user is presented in black font on a white background, as shown in Figure 28.

CommandPlugin

3.0.0

Listens for websocket connections from the TMX admin portal and processes commands

Messages

State

Configuration

+

Key	Value	Default Value	Description
DownloadPath	<input type="text" value="/var/www/download"/>	/var/www/download	The path to the directory where downloaded files will be saved.
EventRowLimit	<input type="text" value="500"/>	50	The maximum number of rows returned for the initial Event Log query.
LogLevel	<input type="text" value="ERROR"/>	ERROR	The log level for this plugin
SleepMS	<input type="text" value="100"/>	100	The length of milliseconds to sleep between processing all messages.
SSLEnabled	<input type="text" value="true"/>	true	Enable secure connection using SSL.
SSLPath	<input type="text" value="/var/www/plugins/.ssl"/>	/var/www/plugins/.ssl	The path to the directory containing the SSL key and certificate files.

Figure 28. Modified Configuration Parameter After Value was Accepted

Add a New Configuration Parameter to Plugin

A user with either Application or System Administrator permissions can also add new configuration parameters to existing plugins by pressing the “+” button on the Configuration bar. This displays a dialog popup containing four labelled input text fields, an “Add” button, and a “Cancel” button (see Figure 29). The “+” button’s text also updates to “-” to indicate that pressing it will close this newly opened dialog.

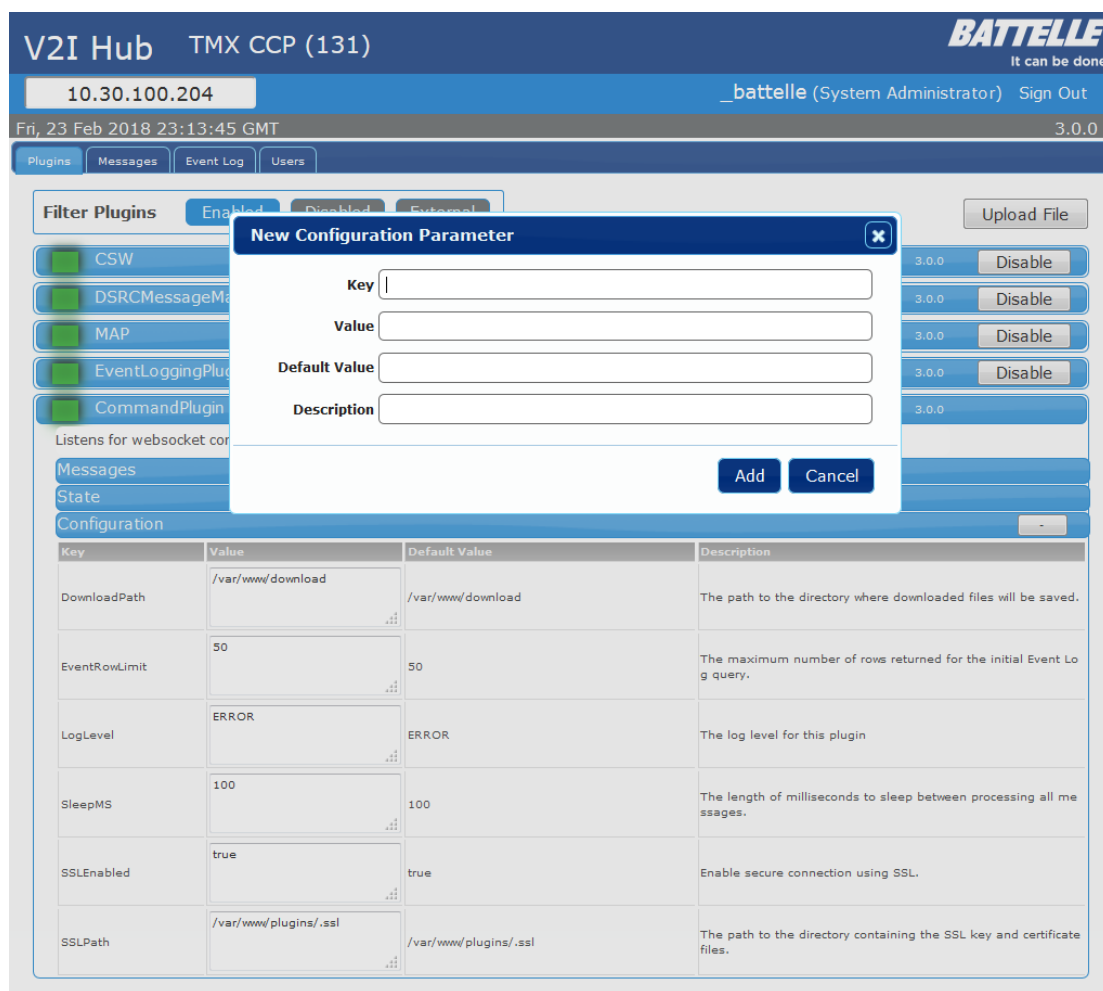
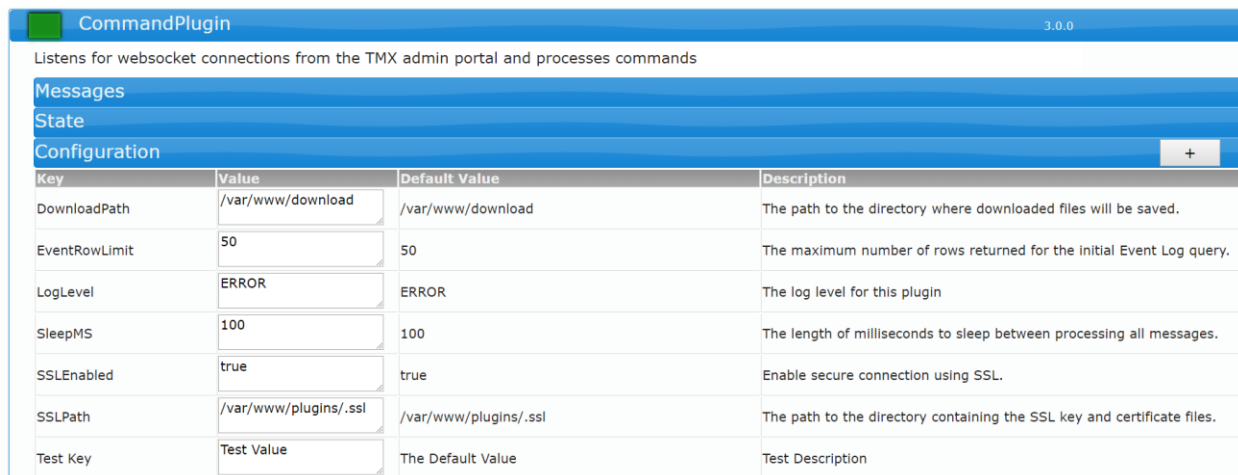


Figure 29. New Configuration Parameter Dialog Window

The Administration Portal does not check the validity of new entries. Responsibilities of error-checking and rejecting the entry are passed to the V2I Hub. Pressing the “Add” button forwards the values of the four input text fields. If accepted, the user-entered information comprises a new row in the configuration parameter table. The dialog then closes and hides the input text fields; the “-” button’s text reverts to “+” (see Figure 30).



Key	Value	Default Value	Description
DownloadPath	/var/www/download	/var/www/download	The path to the directory where downloaded files will be saved.
EventRowLimit	50	50	The maximum number of rows returned for the initial Event Log query.
LogLevel	ERROR	ERROR	The log level for this plugin
SleepMS	100	100	The length of milliseconds to sleep between processing all messages.
SSLEnabled	true	true	Enable secure connection using SSL.
SSLPath	/var/www/plugins/.ssl	/var/www/plugins/.ssl	The path to the directory containing the SSL key and certificate files.
Test Key	Test Value	The Default Value	Test Description

Figure 30. New Configuration Parameter "Test Key" Added to Plugin

Remove Plugin

Application and System Administrators can remove a plugin from the V2I Hub by expanding the plugin's nested bars to the first layer, clicking the "Remove" button (see Figure 31), and confirming the action in the resulting dialog window. Note that the CommandPlugin does not have a "Remove" button. Since the CommandPlugin acts as the Administration Portal's server, removal of this plugin would cause a loss of UI functionality and it is prohibited.

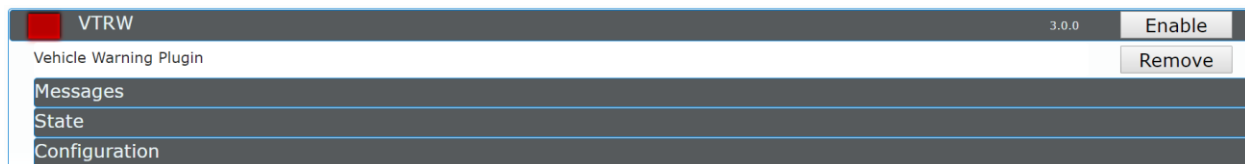


Figure 31. "Remove" Button to Remove a Plugin

Pressing the "Remove" button opens the "Remove Plugin?" dialog window shown in Figure 32 to ask for user confirmation of the action. This confirmation can be cancelled in three ways: pressing the "x" button in the upper right corner of the dialog window, pressing the "Cancel" button, or closing the UI session. The plugin is not removed if the action is cancelled.

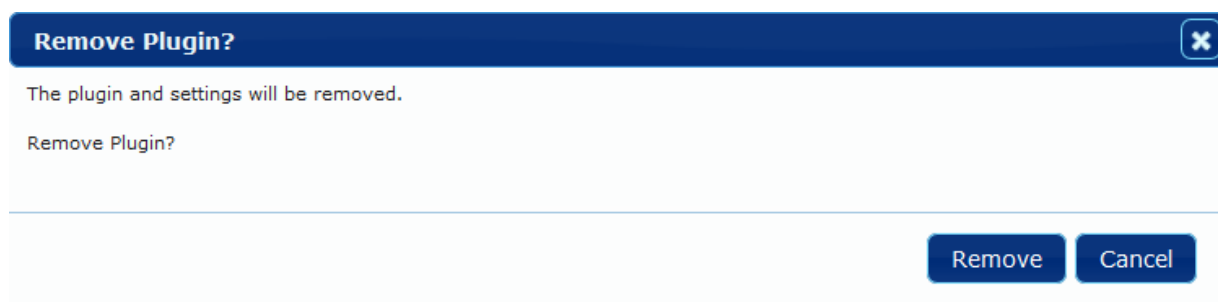


Figure 32. "Remove Plugin?" User Confirmation Dialog Window

To confirm removing the plugin, the Application or System Administrator must press the “Remove” button in the dialog window. After pressing this button, the dialog window closes and the plugin list updates to show the list without the plugin (e.g., Figure 33 does not contain the UI Proxy plugin). The plugin list may take a few seconds to update as the V2I Hub must remove all relevant files. Logging out and logging back in removes the plugin’s messages from the Messages table, but all events associated with the plugin remain.

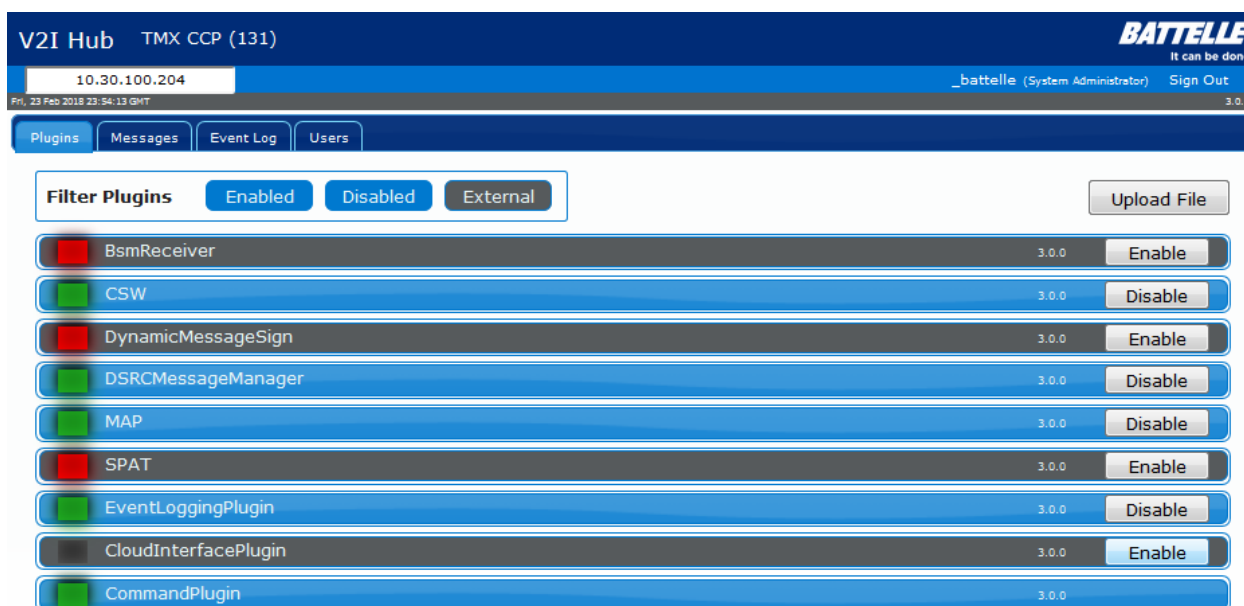


Figure 33. Plugin was Removed from the Plugin List

If the plugin fails to be removed, a “Command Error” dialog window opens to display the resulting error message. This dialog window specifically describes what command failed. The “PLUGINUNINSTALL” denotes remove plugin commands.

File Upload

A user with either Application or System Administrator permissions can upload new files to the V2I Hub. Using this functionality, a user can install new files or update existing ones. Plugin packages, MAP Extensible Markup Language (XML) files, and others can be uploaded on the V2I Hub.

A limitation of this file upload functionality is that only one session can upload a file at any given time. If a session is currently uploading a file and a second session starts a file upload, the first file upload terminates without any warning to the UI while the second one completes, as the first session believes that its file upload is still in progress.

File Restrictions for File Upload

Only one file can be selected for uploading at any given time. Each upload option has a different set of accepted file extensions:

1. Upload Plugin

Accepted file extensions for uploading a plugin file consist of .deb, .zip, .tar.gz, and .tgz. This option automatically initiates the installation process after the plugin was successfully uploaded. As a result, files for this option are expected to contain the necessary plugin files needed to install to work properly.

2. Upload MAP

The accepted file extension for uploading a MAP file is .xml. The file must follow the MAP XML conventions to operate as expected.

3. Upload Other

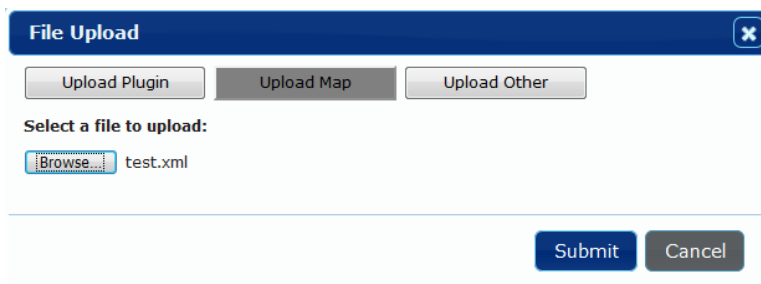
The Upload Other allows for a file of any type to be uploaded to the V2I Hub.

If an invalid file extension was chosen for an upload option, the file is deselected and an error message listing the allowed file extensions appears (see Figure 34). The “Submit” button remains disabled.

The screenshot shows a 'File Upload' dialog box with a title bar and a close button. Inside, there are three buttons: 'Upload Plugin', 'Upload Map', and 'Upload Other'. Below these is the text 'Select a file to upload:' followed by a 'Browse...' button and the text 'No file selected.' At the bottom, there is an error message: 'Error: test.txt does not have an accepted file type. The file extension must be .xml.' Below the error message are two buttons: 'Submit' and 'Cancel'.

Figure 34. File with Invalid File Extension Selected for File Upload

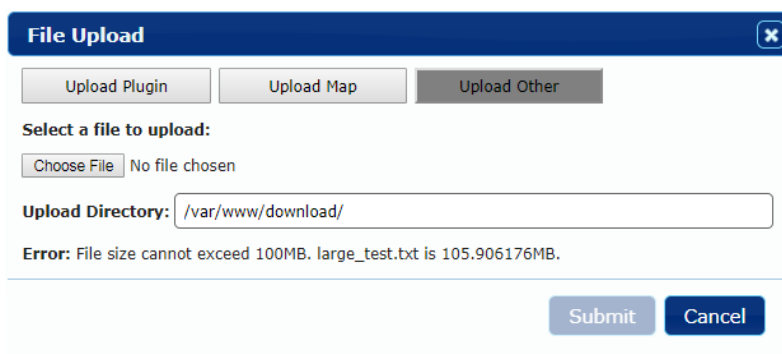
If a valid file extension was chosen for an upload option, the “Submit” button becomes enabled (see Figure 35). The Administration Portal removes any preexisting error messages in the dialog window.



The dialog box is titled "File Upload" with a close button (X) in the top right corner. It contains three tabs: "Upload Plugin", "Upload Map", and "Upload Other". Below the tabs, the text "Select a file to upload:" is followed by a "Browse..." button and the text "test.xml". At the bottom right, there are "Submit" and "Cancel" buttons.

Figure 35. File with Valid File Extension Selected for File Upload

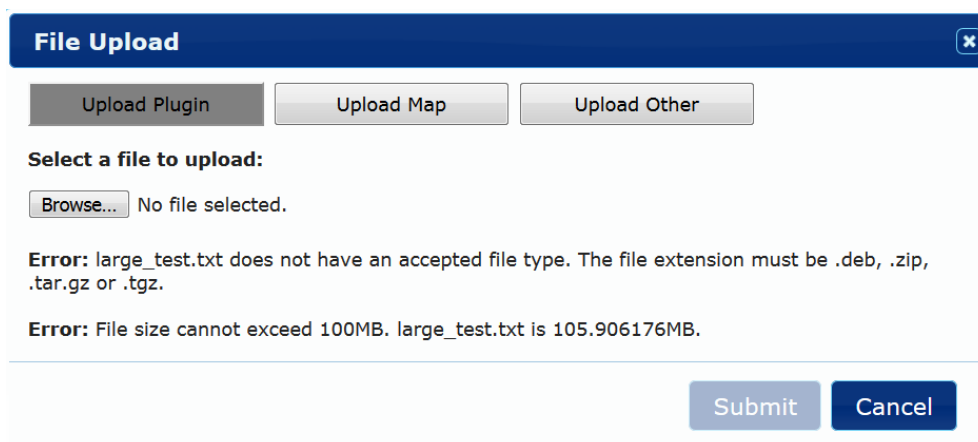
The size of a file to be uploaded is limited to 100MB. Most plugins will be less than 20 MB. Files exceeding this size produce an error message indicating how large the file is (see Figure 36).



The dialog box is titled "File Upload" with a close button (X) in the top right corner. It contains three tabs: "Upload Plugin", "Upload Map", and "Upload Other". Below the tabs, the text "Select a file to upload:" is followed by a "Choose File" button and the text "No file chosen". Below this, the "Upload Directory:" field contains the path "/var/www/download/". At the bottom, an error message states: "Error: File size cannot exceed 100MB. large_test.txt is 105.906176MB." At the bottom right, there are "Submit" and "Cancel" buttons.

Figure 36. File Exceeding Maximum File Size Selected for File Upload

Multiple error messages may be simultaneously displayed in the File Upload dialog (see Figure 37). All errors must be addressed to enable the "Submit" button.



The dialog box is titled "File Upload" with a close button (X) in the top right corner. It contains three tabs: "Upload Plugin", "Upload Map", and "Upload Other". Below the tabs, the text "Select a file to upload:" is followed by a "Browse..." button and the text "No file selected.". Below this, two error messages are displayed: "Error: large_test.txt does not have an accepted file type. The file extension must be .deb, .zip, .tar.gz or .tgz." and "Error: File size cannot exceed 100MB. large_test.txt is 105.906176MB." At the bottom right, there are "Submit" and "Cancel" buttons.

Figure 37. File Violating Multiple Restrictions Selected for File Upload

File Upload Options

The “Upload File” button is unavailable to Read Only users but appears under the “Plugins” tab for the other two access levels. Once the “Upload File” button is pressed, a dialog window appears with different options on this window for an Application and System Administrator (see Figure 39).

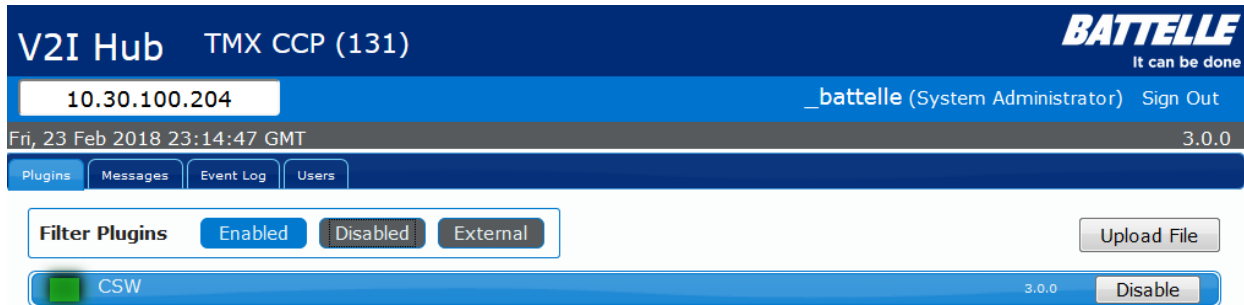


Figure 38. "Upload File" Button to Select File Upload Information

Before the “Submit” button is pressed, this action can be cancelled in three ways: pressing the “x” button in the upper right corner of the dialog window, pressing the “Cancel” button, or closing the UI session. After submitting the file, closing the UI session is the only way to terminate a file upload in progress, but this leaves an incomplete file on the V2I Hub.

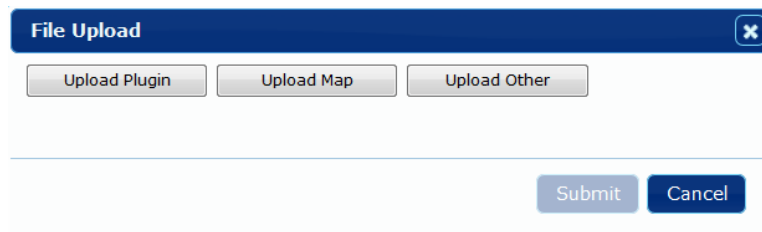


Figure 39. “File Upload” Dialog Window

As shown in Figure 40, Application Administrator users have two upload option buttons available, “Upload Plugin” and “Upload Map.”

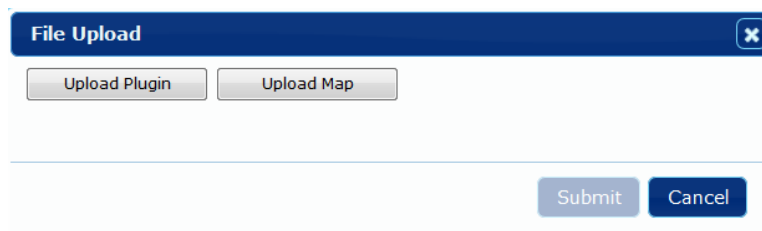


Figure 40. Application Administrator's File Upload Options

In addition to the “Upload Plugin” and “Upload Map,” the System Administrator users have an “Upload Other” button (see Figure 41).

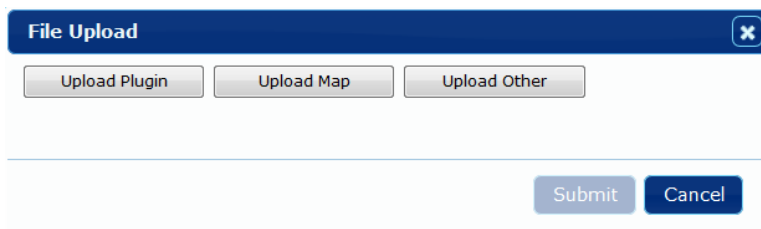


Figure 41. System Administrator's File Upload Options

Selecting a file upload option reveals the user inputs required to upload the appropriate file. Pressing a different upload option resets all user inputs, even those shared between upload options. Figure 42 illustrates how a selected MAP file (1st snapshot) is lost when the user chooses the Upload Plugin button (second snapshot) before returning to the Upload Map button third snapshot).

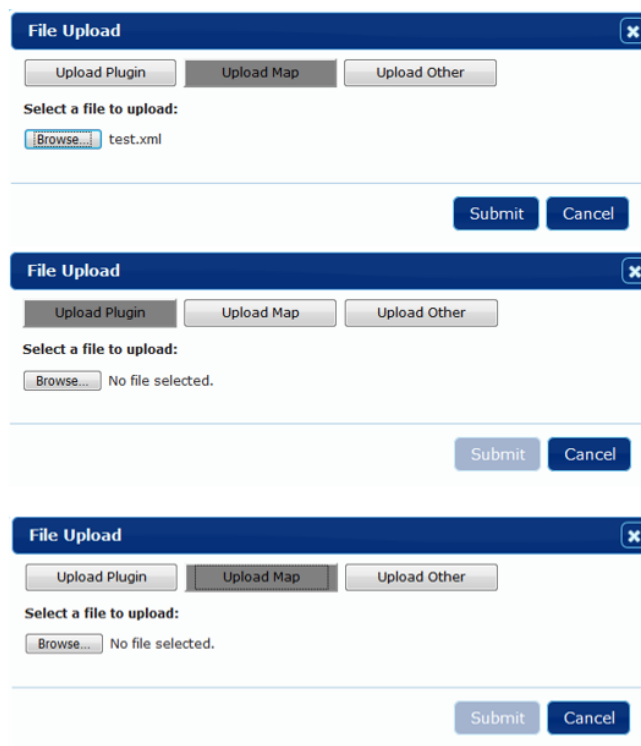


Figure 42. File Upload Inputs Reset When a File Option is Selected

Selecting a plugin, MAP, or other file for upload each works the same way in all three upload procedures. A user can select the desired file to upload by either pressing the “Browse” button, the “No file selected” text, or the name of an already selected file (depending on what stage of the process the user is on).

The “Upload Plugin” option (see Figure 43) only requires the file selection input. No additional inputs are required as the upload directory is selected in the code as “/var/www/download/”.

 A screenshot of a web interface titled "File Upload" with a close button (X) in the top right corner. Below the title bar are three buttons: "Upload Plugin" (which is highlighted with a dark border), "Upload Map", and "Upload Other". Underneath these buttons is the text "Select a file to upload:" followed by a "Browse..." button and the text "No file selected.". At the bottom right of the form are two buttons: "Submit" and "Cancel".

Figure 43. File Upload Option - "Upload Plugin"

Like the “Upload Plugin” option, the “Upload Map” option shown in Figure 44 only requires the file selection input. The upload directory defaults to “/var/www/plugins/MAP/”.

 A screenshot of a web interface titled "File Upload" with a close button (X) in the top right corner. Below the title bar are three buttons: "Upload Plugin", "Upload Map" (which is highlighted with a dark border), and "Upload Other". Underneath these buttons is the text "Select a file to upload:" followed by a "Browse..." button and the text "No file selected.". At the bottom right of the form are two buttons: "Submit" and "Cancel".

Figure 44. File Upload Option - "Upload Map"

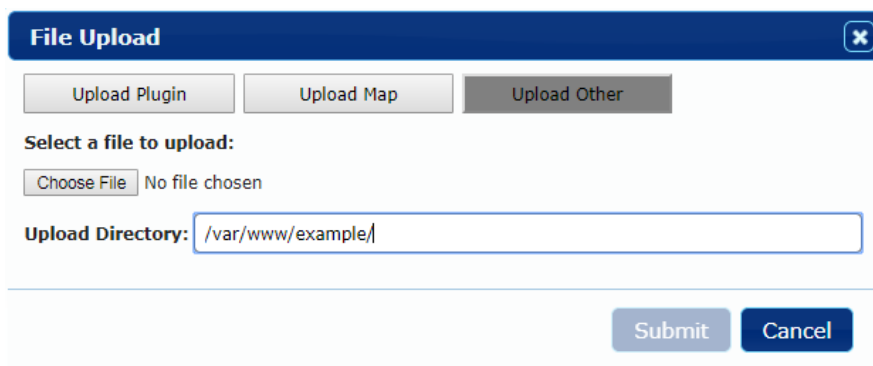
In addition to the file selection input, the “Upload Other” option shown in Figure 45 has a text input field that allows a user to choose an upload directory other than the default “/var/www/download/” (see Figure 46). This is an advanced option and it is the user’s responsibility to ensure the CommandPlugin has the appropriate permissions to write to the chosen directory.

 A screenshot of a web interface titled "File Upload" with a close button (X) in the top right corner. Below the title bar are three buttons: "Upload Plugin", "Upload Map", and "Upload Other" (which is highlighted with a dark border). Underneath these buttons is the text "Select a file to upload:" followed by a "Browse..." button and the text "No file selected.". Below this is a text input field labeled "Upload Directory:" containing the text "/var/www/download/". At the bottom right of the form are two buttons: "Submit" and "Cancel".

Figure 45. File Upload Option - "Upload Other"

Uploading a File

The “Submit” button becomes enabled after a valid file is selected. Pressing the “Submit” button uploads the file to the default directory “/var/www/download/”. Once the file successfully uploads to the default directory, the CommandPlugin then copies the file to the chosen directory. The CommandPlugin removes the file from the default directory regardless of whether the file succeeds or fails to be copied over to this new directory.



The screenshot shows a "File Upload" dialog box with a dark blue header and a close button (X) in the top right corner. Below the header are three buttons: "Upload Plugin", "Upload Map", and "Upload Other". The "Upload Other" button is highlighted with a dark grey background. Below these buttons is the text "Select a file to upload:" followed by a "Choose File" button and the text "No file chosen". Below that is a text input field labeled "Upload Directory:" containing the path "/var/www/example/". At the bottom right of the dialog are two buttons: "Submit" and "Cancel".

Figure 46. Selecting an Upload Directory for File Upload Option "Upload Other"

After submitting, the dialog window closes, and a notification opens with the filename and a progress completion status of 0% (see Figure 47). The “Upload File” button remains disabled until the CommandPlugin completes the file transfer, or the installation if the file option selected was “Upload Plugin”.

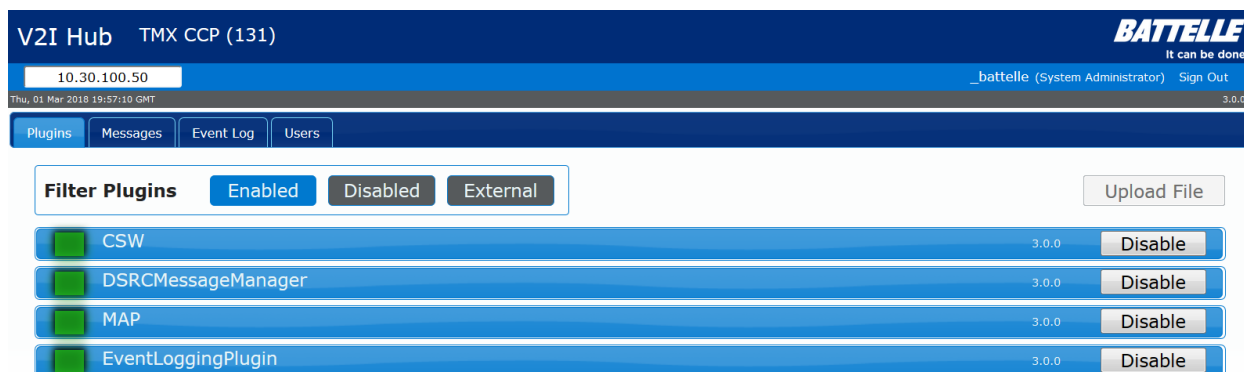


Figure 47. File Upload Transfer Initiated

Once the Administration Portal receives the CommandPlugin's confirmation for a file transfer, the File Upload dialog window closes. The "Upload File" button remains disabled until the file transfer is complete, and if the installation is complete if the file type is a plugin. A notification containing the filename and its upload progress status appears at the bottom of the Administration Portal (see Figure 48). This message continuously updates with progress messages until the file upload completes or an error message is returned.

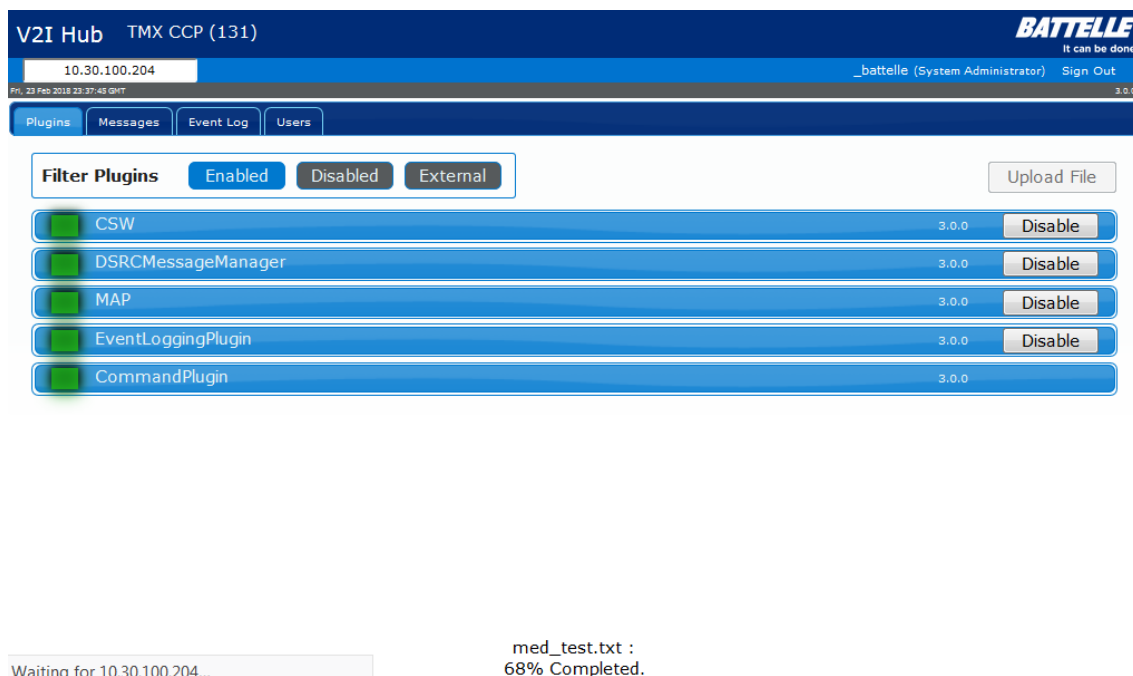


Figure 48. File Upload Transfer in Progress

If the file fails to upload for any reason, a “Command Error” dialog window replaces the notification onscreen (see Figure 49). This dialog window describes what command failed (the “UPLOADFILE” denotes file upload commands), and the reason it failed. The user must close the dialog window to enable the “Upload File” button, either by pressing the “OK” button or “x” button.

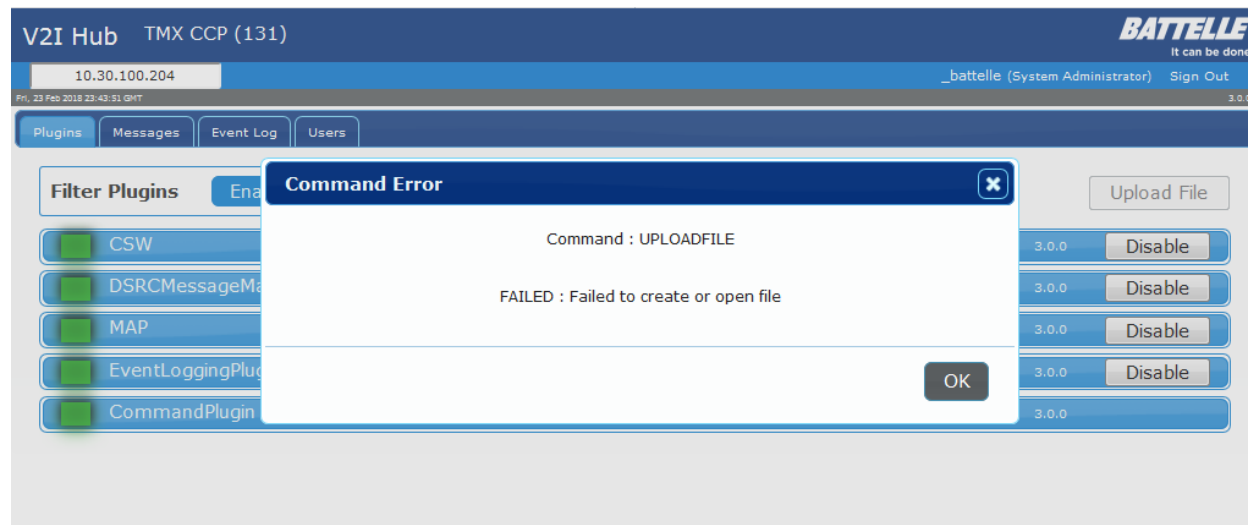


Figure 49. “Command Error” Dialog Window with File Upload Failure Message

Once the file upload successfully completes for a non-plugin file, the notification displays for an additional three seconds to indicate that progress reached 100% before disappearing (see Figure 50). During this time the “Upload File” button remains disabled. Once the notification disappears, the button reenables for the next file upload.

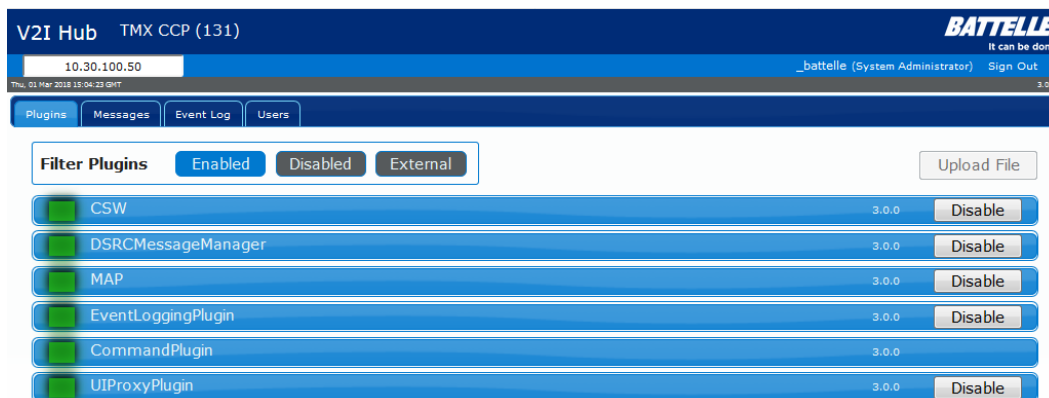


Figure 50. File Upload Transfer Completed

Plugin Install

If the file upload completed successfully for a plugin file, the Administration Portal initiates the installation process for the plugin. The notification that the file upload progress reached 100% will be replaced with an installing plugin message until the V2I Hub transmits a message saying it either succeeded or failed to install the plugin (see Figure 51). If successful, a new notification will appear, saying that the installation is complete. If the installation failed, a “Command Error” dialog window will open to convey the results.

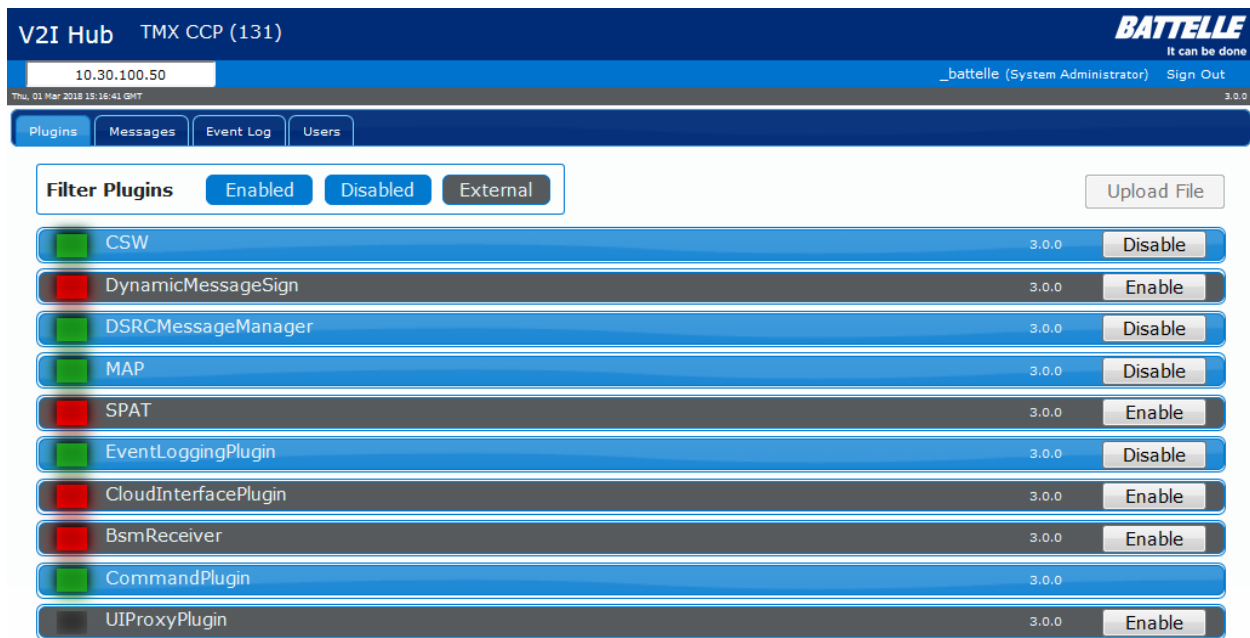
If the file upload completed successfully for a plugin file, the notification will display for an additional three seconds to indicate that progress reached 100% before disappearing. During this time, the Administration Portal initiates the installation process for the plugin. If the Administration Portal receives confirmation that the plugin installation process has started before the three second timeout, a notification with “Installing plugin...” text replaces the current notification.



Installing plugin...

Figure 51. Notification Indicating Plugin Installation in Progress

Upon successful installation, the notification text is replaced with “Plugin installation complete” (see Figure 52). This notification message stays on-screen for three seconds before disappearing.



Plugin installation complete.

Figure 52. Notification Indicating Plugin Installation is Complete

If the plugin fails to install, a “Command Error” dialog window will open to display the resulting error message (see Figure 53). This dialog window will specifically describe what command failed (the “PLUGININSTALL” denotes install plugin commands).

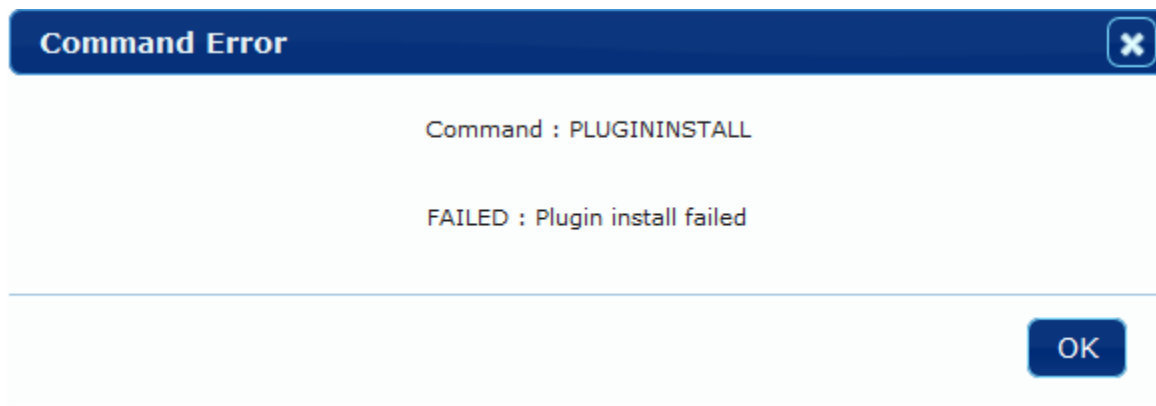


Figure 53. “Command Error” Dialog Window with Plugin Install Failure Message

The “Upload File” button remains disabled until the notification or dialog window disappears; at this point, the button reenables for the next file upload.

“Messages” Tab

The second available navigation tab, “Messages”, displays the message traffic as seen by the V2I Hub (see Figure 54). This consists of a table of the message types that have been sent through the V2I Hub. Filtering by time, message, and other fields provides a concentrated window of message traffic for a user to review. The number of total entries in the table displayed onscreen informs the user that more data is available when filtering.

Message Information

Type and subtype details categorize a message. These fields differentiate messages within a plugin. Since information from all plugins is available in this table and multiple plugins can use the same type/subtype, the database labels each message type/subtype instance with the plugin from which it originates.

The V2I Hub maintains relevant statistics regarding each plugin’s messages. One statistic is a count of the number of sent messages for a plugin’s type/subtype. V2I Hub also keeps track of when the last instance of the message type/subtype was sent for that plugin. Using these pieces of information, the V2I Hub can calculate the average interval of the message type/subtype for a plugin to be displayed on the Administration Portal.

Plugin	Type	Subtype	Count	Last Timestamp	Average Interval
MAP	J2735	MAP-P	1478325	2018-02-23 22:36:54	1000
CSW	J2735	TIM	1447248	2018-02-23 22:36:53	1052

Figure 54. Messages Table

Message Filtering

Message traffic can be filtered to show the messages that occurred during certain time intervals. These time intervals are predefined in a dropdown menu within the Filter by Time section of the page (see Figure 55). Selecting an option from this menu redraws the Messages table to display only the relevant information.

V2I Hub TMX CCP (131)

10.30.100.204 _battelle (System Administrator) Sign Out

Fri, 23 Feb 2018 22:37:17 GMT 3.0.0

Plugins Messages Event Log Users

Filter by Time 10 minutes Show Keep Alive

5 seconds
30 seconds
10 minutes
All

Plugin	Count	Last Timestamp	Average Interval
CSW	268	2018-02-23 22:37:14	1052
MAP	345	2018-02-23 22:37:14	1000

Showing 1 to 2 of 2 entries (filtered from 13 total entries)

Previous 1 Next

Figure 55. Messages Table – Filter by Time Dropdown Menu

While included in the total number of entries in the Messages table, Keep Alive messages are hidden by default. The color of the “Show Keep Alive” button indicates whether Keep Alive messages are shown or not. If the color is gray, Keep Alive messages are not shown (see Figure 56).

V2I Hub TMX CCP (131)

10.30.100.204 _battelle (System Administrator) Sign Out

Fri, 23 Feb 2018 22:36:57 GMT 3.0.0

Plugins Messages Event Log Users

Filter by Time 10 minutes Show Keep Alive

5 seconds
30 seconds
10 minutes
All

Plugin	Type	Subtype	Count	Last Timestamp	Average Interval
MAP	J2735	MAP-P	1478325	2018-02-23 22:36:54	1000
CSW	J2735	TIM	1447248	2018-02-23 22:36:53	1052

Showing 1 to 2 of 2 entries (filtered from 13 total entries)

Previous 1 Next

Figure 56. Messages Table – Hidden Keep Alive Messages

If the color of the “Show Keep Alive” button is blue, Keep Alive messages are shown (see Figure 57).

V2I Hub TMX CCP (131) **BATTELLE** It can be done

10.30.100.204 _battelle (System Administrator) Sign Out

Fri, 23 Feb 2018 22:42:20 GMT 3.0.0

Plugins Messages Event Log Users

Filter by Time 10 minutes Show Keep Alive

Search:

Plugin	Type	Subtype	Count	Last Timestamp	Average Interval
CSW	J2735	TIM	1447565	2018-02-23 22:42:18	1000
MAP	J2735	MAP-P	1478648	2018-02-23 22:42:18	1000
EventLoggingPlugin	System	KeepAlive	3152	2018-02-23 22:40:36	4294967295
DSRCMessageManager	System	KeepAlive	797	2018-02-23 22:39:14	4294967295
CommandPlugin	System	KeepAlive	2	2018-02-23 22:36:15	4294967295

Showing 1 to 5 of 5 entries (filtered from 13 total entries) Previous 1 Next

Figure 57. Messages Table - Shown Keep Alive Messages

Message traffic can also be filtered using the Search function above the upper right corner of the table. Figure 58 shows an example of searching for the “Keep” keyword and the rows that are shown. Searching for a keyword or phrase returns entries that match that search query. A user cannot search for multiple factors in a query. For example, searching for “CSW || MAP” returns “CSW || MAP” entries, not “CSW” or “MAP” entries.

V2I Hub TMX CCP (131) **BATTELLE** It can be done

10.30.100.204 _battelle (System Administrator) Sign Out

Fri, 23 Feb 2018 22:43:02 GMT 3.0.0

Plugins Messages Event Log Users

Filter by Time All Show Keep Alive

Search: Keep x

Plugin	Type	Subtype	Count	Last Timestamp	Average Interval
EventLoggingPlugin	System	KeepAlive	3152	2018-02-23 22:40:36	4294967295
DSRCMessageManager	System	KeepAlive	797	2018-02-23 22:39:14	4294967295
CommandPlugin	System	KeepAlive	2	2018-02-23 22:36:15	4294967295
UIProxyPlugin	System	KeepAlive	17	2018-02-21 21:32:44	4294967295
CSW	System	KeepAlive	8	2018-02-21 15:46:53	4294967295
SPAT	System	KeepAlive	2562	2018-02-20 17:38:46	4294967295
MAP	System	KeepAlive	3	2018-02-19 19:04:25	4294967295
DynamicMessageSign	System	KeepAlive	16	2018-02-19 16:49:54	4294967295
BsmReceiver	System	KeepAlive	8	2018-02-19 15:46:29	4294967295

Showing 1 to 9 of 9 entries (filtered from 13 total entries) Previous 1 Next

Figure 58. Messages Table – Search Filter

When the number of entries exceeds the Messages table's maximum page length (10 entries), additional pages are added to the table. The navigation buttons in the lower right corner of the table handle the traversal through these pages. Pressing a number button takes the user to that page of the table. The other buttons are enabled or disabled depending on the current page. If the Messages table is on the first page, the "Previous" button is disabled and only the "Next" button is enabled. Pressing the "Next" button takes a user to the next page. If the Messages table is on the last page, the "Next" button is disabled and only the "Previous" button is enabled. Pressing the "Previous" button takes the user to the page before the current page. If the Messages table is not on either the first or last pages, both buttons are enabled.


"Event Log" Tab

The third available navigation tab, "Event Log", displays plugin events that are logged to the database (see Figure 59). This consists of a table of events logged by all plugins. Filtering of these events can provide a concentrated window of the log. A "Clear Log" button is available to Application and System Administrators to clear all logged event messages from the database.

The CommandPlugin's configuration parameter "EventRowLimit" dictates the number of entries returned upon initial connection. Any entries after this connection will be appended to the beginning of the table. The number of entries does not reset to this initial number when switching users during a session

Event Information

Each event is logged into the database as a separate entity. If a subsequent event is the same as the previous one, each event is logged separately. To differentiate between the two events, a timestamp is logged with each event. Further information regarding the event includes the level of event severity, originating plugin, and a description of what occurred during the event.

V2I Hub TMX CCP (131)					
10.30.100.204		_battelle (System Administrator) Sign Out			
Fri, 23 Feb 2018 22:43:27 GMT				3.0.0	
Plugins	Messages	Event Log	Users		

Level	Source	Description	Timestamp
Info	CommandPlugin	Plugin registered	2018-02-23 22:28:15
Warning	CommandPlugin	Plugin deconstructing	2018-02-23 22:08:52
Info	CommandPlugin	Plugin registered	2018-02-23 21:48:18
Warning	CommandPlugin	Plugin deconstructing	2018-02-23 21:48:04
Info	ivpcore.PluginMonitor	Plugin 'CommandPlugin' (id: 14180) startup time: 626 milliseconds	2018-02-23 21:02:16
Info	CommandPlugin	Plugin registered	2018-02-23 21:02:12
Warning	CommandPlugin	Plugin deconstructing	2018-02-23 20:36:09
Info	CommandPlugin	Plugin registered	2018-02-23 20:29:38
Warning	CommandPlugin	Plugin deconstructing	2018-02-23 20:29:00
Info	CommandPlugin	Plugin registered	2018-02-23 20:27:42
Warning	CommandPlugin	Plugin deconstructing	2018-02-23 20:25:46
Info	ivpcore.PluginMonitor	Plugin 'CommandPlugin' (id: 14172) startup time: 380 milliseconds	2018-02-23 19:36:16
Info	CommandPlugin	Plugin registered	2018-02-23 19:36:11
Warning	CommandPlugin	Plugin deconstructing	2018-02-23 19:33:04

Showing 1 to 14 of 50 entries

Previous **1** 2 3 4 Next

Clear Log

Figure 59. Event Log Table

Event Log Filtering

Event logs can be filtered using the Search function above the upper right corner of the table (see Figure 60). Searching for a keyword or phrase returns entries that match the search query. A user cannot search for multiple factors in a query. For example, searching for “Info || Warning” returns “Info || Warning” entries, not “Info” or “Warning” entries.

The screenshot shows the V2I Hub Administration Portal interface. At the top, it displays 'V2I Hub TMX CCP (131)' and the IP address '10.30.100.204'. The user is logged in as '_battelle (System Administrator)' with a 'Sign Out' button. The 'Event Log' tab is selected. A search bar at the top right contains the text 'warning'. Below the search bar is a table with the following columns: Level, Source, Description, and Timestamp. The table contains 13 entries, all with a 'Warning' level and 'Plugin deconstructing' description. The sources are 'CommandPlugin' and 'UIProxyPlugin'. The timestamps range from 2018-02-21 to 2018-02-23. At the bottom of the table, it says 'Showing 1 to 12 of 13 entries (filtered from 50 total entries)'. Navigation buttons 'Previous', '1', '2', and 'Next' are visible. A 'Clear Log' button is located below the table.

Level	Source	Description	Timestamp
Warning	CommandPlugin	Plugin deconstructing	2018-02-23 22:44:01
Warning	CommandPlugin	Plugin deconstructing	2018-02-23 22:08:52
Warning	CommandPlugin	Plugin deconstructing	2018-02-23 21:48:04
Warning	CommandPlugin	Plugin deconstructing	2018-02-23 20:36:09
Warning	CommandPlugin	Plugin deconstructing	2018-02-23 20:29:00
Warning	CommandPlugin	Plugin deconstructing	2018-02-23 20:25:46
Warning	CommandPlugin	Plugin deconstructing	2018-02-23 19:33:04
Warning	UIProxyPlugin	Plugin deconstructing	2018-02-21 21:33:05
Warning	UIProxyPlugin	Plugin deconstructing	2018-02-21 21:32:58
Warning	UIProxyPlugin	Plugin deconstructing	2018-02-21 21:32:32
Warning	UIProxyPlugin	Plugin deconstructing	2018-02-21 21:32:07
Warning	UIProxyPlugin	Plugin deconstructing	2018-02-21 21:31:41

Showing 1 to 12 of 13 entries (filtered from 50 total entries)

Previous 1 2 Next

Clear Log

Figure 60. Event Log Table - Search Filter

When the number of entries exceeds the Event Log table's maximum page length (variable depending on row height and window size), additional pages are added to the table. The navigation buttons in the lower right corner of the table handle the traversal through these pages. Pressing a numbered navigation button takes the user to that page of the table. The other buttons are enabled or disabled depending on the current page. If the Event Log table is on the first page, the "Previous" button is disabled and only the "Next" button is enabled. Pressing the "Next" button takes a user to the next page. If the Event Log table is on the last page, the "Next" button is disabled and only the "Previous" button is enabled. Pressing the "Previous" button takes the user to the page before the current page. If the Event Log table is not on either the first or last pages, both buttons are enabled.

Clear Event Log

The "Clear Log" button is only available to Application and System Administrators. Pressing the "Clear Log" button sends a command to the connected V2I Hub to clear the database of all logged events. Upon success or failure, the database sends an indication of the status to the V2I Hub. If clearing the events succeeds, the table updates to show no entries (see Figure 61); if clearing the events fails, the table does not update, and the resulting error message is displayed in a dialog window.

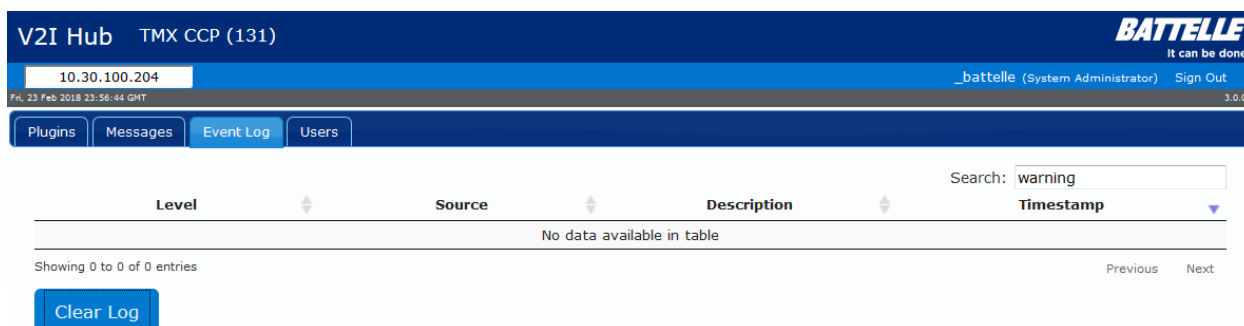


Figure 61. Event Log Table - Cleared After Pressing "Clear Log" Button

If clearing the event log failed, a Command Error dialog window opens to display the resulting error message. This dialog window specifically describes what type of command failed (the “CLEARLOG” denotes clearing the event log).

“Users” Tab

System Administrator users are the only users allowed to perform user administration, so the “Users” tab (see Figure 62) is only available for System Administrator users. This tab provides a record of all users and their access levels. Using this UI, a System Administrator user can add a new user, and set their access level and password in the process. A System Administrator can also reset a password for any. While a System Administrator can delete and change the access level of other users, these actions are not available to be taken for the session’s user to prevent a conflict in permissions.

The User List table details all users. For each user, the table lists the username, access level, and actions that can be taken regarding that user. Note that unlike the other users, the current user’s “Change Access” and “Delete User” buttons are not available. Changing the current user from a System Administrator to a lower permissions level or deleting the current user could leave the V2I Hub without a System Administrator, thus preventing further user management.

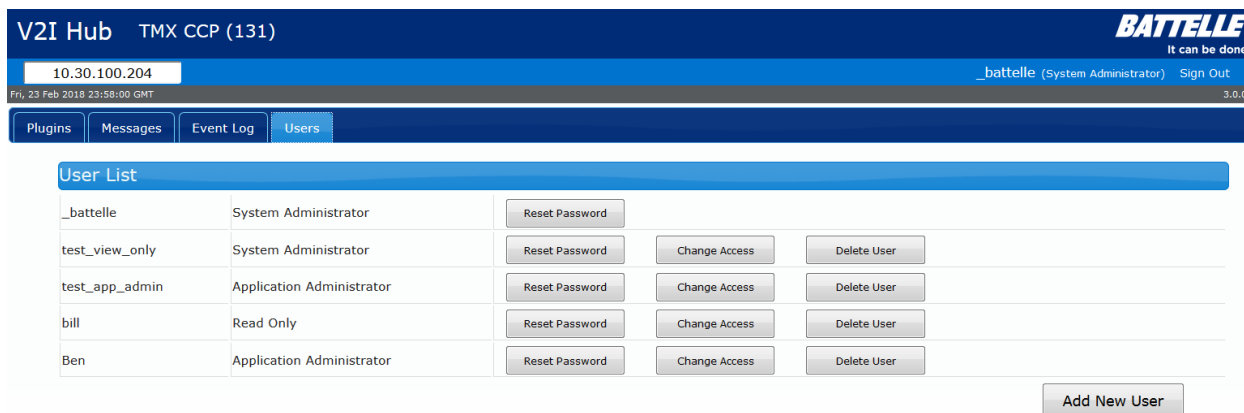


Figure 62. Users List Table

Passwords

Passwords must meet the requirement for a strong password. The following conditions must be met for a password to be accepted.

- Password length – At least 8 characters
- Combination of Uppercase and Lowercase
- At least one number
- At least one symbol ! @ # \$ % ^ & * - + = < > ?

Add a New User

Pressing the “Add New User” button opens a dialog window allowing the System Administrator to input relevant information regarding a new user (see Figure 63). Information needed to generate a new user includes a username, access level, and password.

The screenshot shows a dialog window titled "Add New User". It contains the following fields and controls:

- New Username:** A text input field.
- Select New Access:** A dropdown menu currently showing "Read Only".
- Enter New Password:** A password input field.
- Re-Enter New Password:** A password input field.
- Buttons:** "Add" and "Cancel" buttons at the bottom right.
- Close Button:** A small "X" button in the top right corner of the dialog header.

Figure 63. “Add New User” Dialog Window

The “Add New User” dialog window can be cancelled in three ways: pressing the “x” button in the upper right corner of the dialog window, pressing the “Cancel” button, or closing the UI session. A new user is not added if the dialog window is closed without pressing the “Add” button.

The username must be a unique identifier. Checks to determine the uniqueness of this username are made by the database upon submitting the information in the dialog window via the “Add” button. If the username is not considered unique by the database, an error message is returned.

The second piece of information required for a new user is the new user’s access level. The new user’s access level is chosen from the dropdown menu in the dialog window (see Figure 64). The “Read Only,” “Application Administrator,” and “System Administrator” levels are available to choose from for each new user.

Figure 64. “Add New User” Dialog Window with "Select Access Level" Dropdown Menu Opened

The “Add New User” dialog window has two input text fields for passwords. Requiring a user to input the password twice allows the user to confirm the inputted value since text for password inputs is hidden. When the form in the dialog window is submitted via the “Add” button, the Administration Portal checks if the passwords match. If the passwords do not match each other, the dialog window outputs an error message stating this and remains open for further action from the user (see Figure 65). No message is sent to add the new user to the V2I Hub.

Figure 65. “Add New User” Dialog Window with Mismatched Passwords

If the passwords do match each other when the “Add” button is pressed, the dialog window closes. A message is sent to add the new user to the database.

If adding a new user fails, a “Command Error” dialog window opens to display the resulting error message (see Figure 66). This dialog window specifically describes what command failed (the “USERADD” denotes adding a new user).

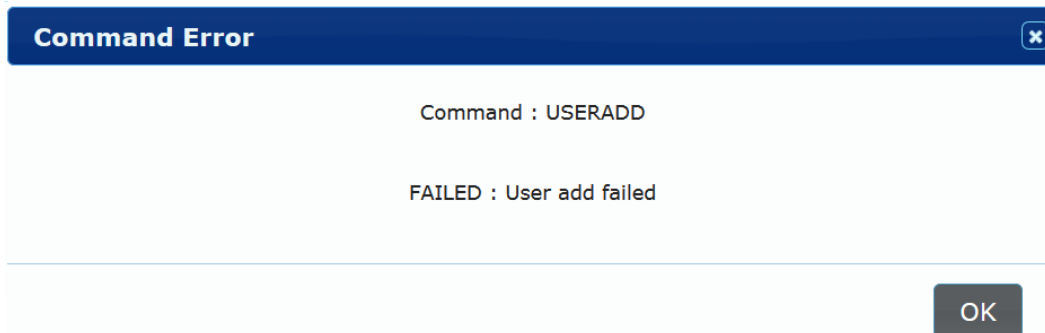


Figure 66. Command Error Dialog Window with an Add New User Failure Message

Reset a User’s Password

A System Administrator user can modify the password of any existing user by pressing the “Reset Password” button. Pressing this button opens a dialog window containing two input text fields for the System Administrator to input a new password and to confirm it (see Figure 67).

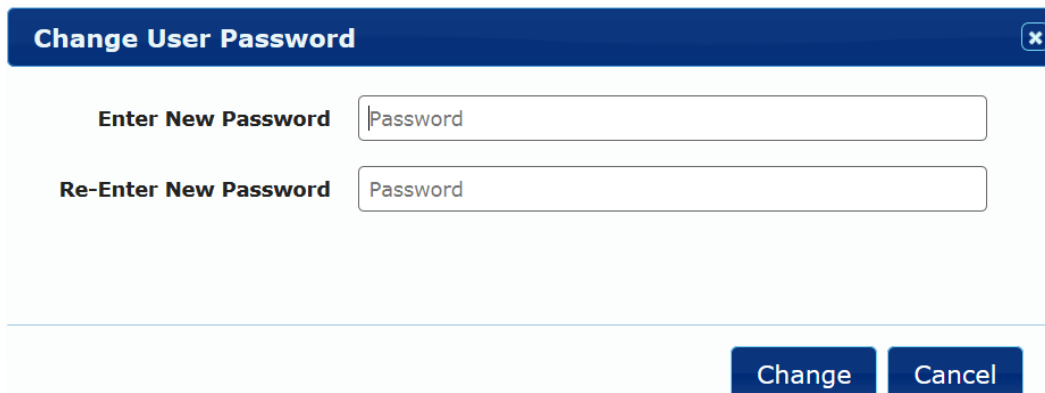
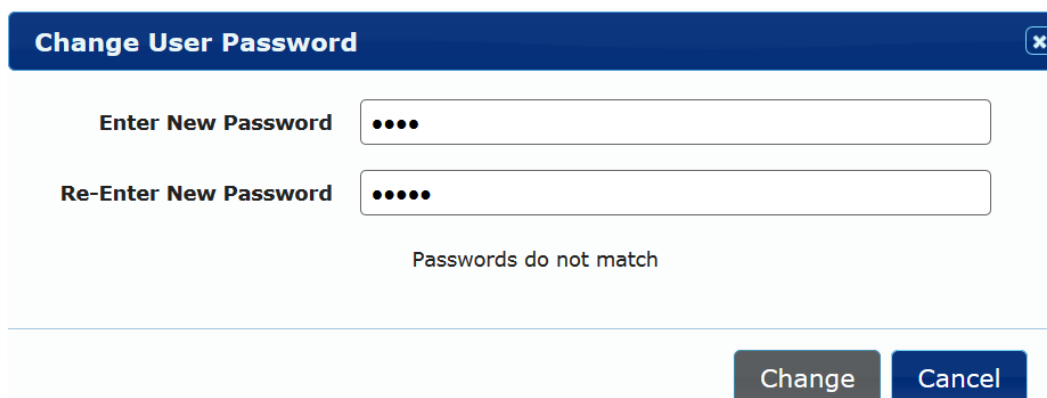


Figure 67. “Change User Password” Dialog Window

By clicking the “Change” button, the passwords are checked to see if they match.

If the passwords do not match each other, the dialog window outputs an error message (see Figure 68). No message will be sent to the V2I Hub to confirm the change in password. The dialog window remains open for further action from the user.



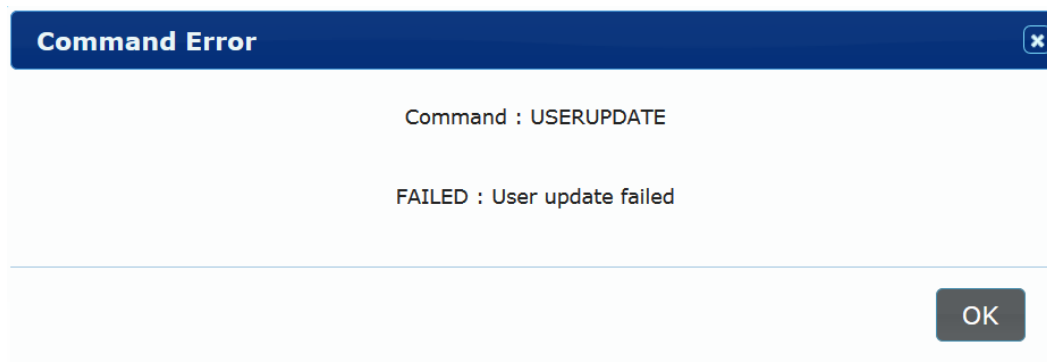
The dialog window has a dark blue header with the title "Change User Password" and a close button (X). Below the header, there are two input fields. The first is labeled "Enter New Password" and contains four black dots. The second is labeled "Re-Enter New Password" and contains five black dots. Below the input fields, the text "Passwords do not match" is displayed in a light gray font. At the bottom right, there are two buttons: "Change" (dark gray) and "Cancel" (dark blue).

Figure 68. “Change User Password” Dialog Window with Mismatched Passwords

If the passwords do match each other, a message is forwarded to the V2I Hub with this new information and the dialog window closes.

Once the V2I Hub completes the act of resetting the password, it sends a status message indicating whether it completed successfully or failed.

If resetting the password for a user failed, a “Command Error” dialog window opens to display the resulting error message (see Figure 69). This dialog window specifically describes what type of command failed (the “USERUPDATE” denotes user maintenance commands).



The dialog window has a dark blue header with the title "Command Error" and a close button (X). Below the header, the text "Command : USERUPDATE" is displayed. Below that, the text "FAILED : User update failed" is displayed. At the bottom right, there is an "OK" button (dark gray).

Figure 69. “Command Error” Dialog Window with User Update Failure Message for Changing a User’s Password

Change a User’s Access

A System Administrator user can change another user’s access level by pressing the associated “Change Access” button for that user (see Figure 70).

Note that if a session is already opened for a user whose access level is changed, the UI session for that user does not immediately update to reflect the changes. The user will be subjected to their new permissions once they log out and subsequently sign in.

The screenshot shows the V2I Hub Administration Portal interface. At the top, it displays 'V2I Hub TMX CCP (131)' and the Battelle logo with the tagline 'It can be done'. Below this is a status bar showing the IP address '10.30.100.204', the date and time 'Fri, 23 Feb 2018 23:58:00 GMT', the user '_battelle (System Administrator)', and a 'Sign Out' button. A navigation bar contains links for 'Plugins', 'Messages', 'Event Log', and 'Users'. The 'Users' section is active, displaying a 'User List' table.

User List		
_battelle	System Administrator	<button>Reset Password</button>
test_view_only	System Administrator	<button>Reset Password</button> <button>Change Access</button> <button>Delete User</button>
test_app_admin	Application Administrator	<button>Reset Password</button> <button>Change Access</button> <button>Delete User</button>
bill	Read Only	<button>Reset Password</button> <button>Change Access</button> <button>Delete User</button>
Ben	Application Administrator	<button>Reset Password</button> <button>Change Access</button> <button>Delete User</button>

At the bottom right of the table is an Add New User.

Figure 70. Users List Table

Pressing the “Change Access” button opens a dialog window containing a dropdown menu (see Figure 71).

The screenshot shows the 'Change User Access' dialog window. It has a dark blue header with the title 'Change User Access' and a close button (X). Below the header, there is a label 'Select New Access' followed by a dropdown menu currently showing 'Application Administrator'. At the bottom right, there are two buttons: 'Change' and 'Cancel'.

Figure 71. “Change User Access” Dialog Window

All access levels are available to choose from in this dropdown menu (see Figure 72).

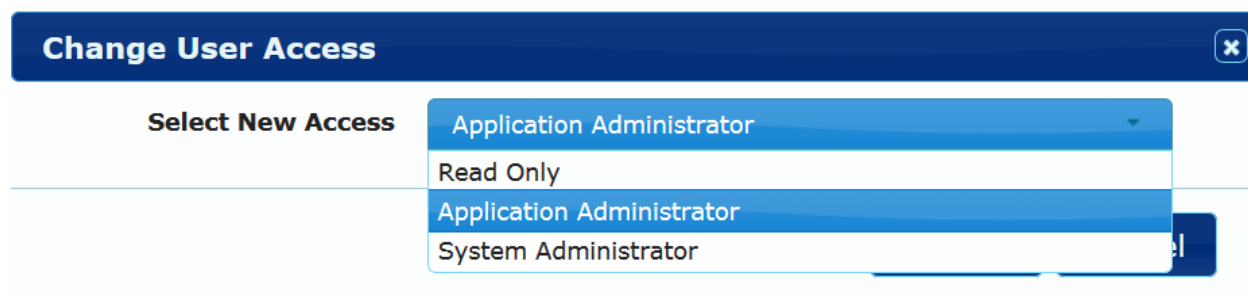


Figure 72. “Change User Access” Dialog Window with Select New Access Dropdown Menu Open

Changing a user’s access level can be cancelled in three ways: pressing the “x” button in the upper right corner of the dialog window, pressing the “Cancel” button, or closing the UI session. The access level is not changed if the action is cancelled.

To confirm the selection made in the dropdown menu, the System Administrator must press the “Change” button in the dialog window. The dialog window closes and the table updates to show the new access level if the action succeeded. Figure 73 shows Ben’s access changed from Application Administrator (in Figure 70) to Read Only.

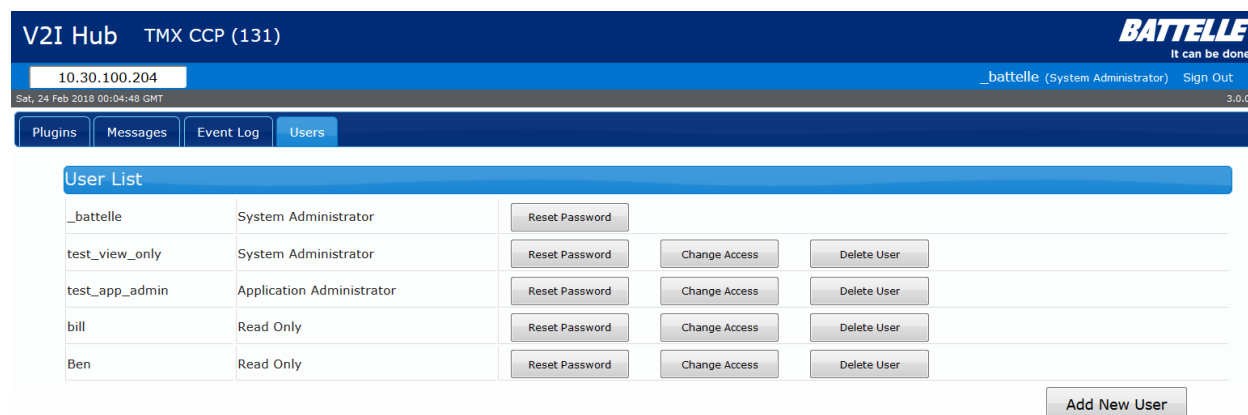


Figure 73. Users List Table with an Updated Access Level

Submitting the same access level currently assigned to a user results in an error message as the V2I Hub detects no change in permissions. If changing the access level fails, a “Command Error” dialog window opens to display the resulting error message (see Figure 74). This dialog window specifically describes what type of command failed (the “USERUPDATE” denotes user maintenance commands).

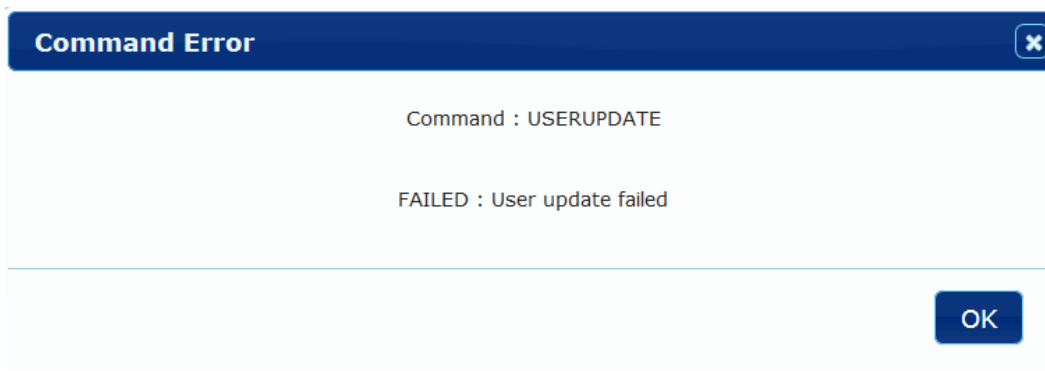


Figure 74. “Command Error” Window with a User Update Failure Message for Changing a User’s Access Level

Delete a User

A System Administrator user can delete a user from the V2I Hub by pressing the associated “Delete User” button for that user. Note that the System Administrator user cannot delete themselves to ensure that the V2I Hub will have at least one System Administrator user at any given time when operating via the UI. Furthermore, the UI assumes the access level of a user remains consistent from the time they logged in to when the session is either closed or the user is logged out. Preventing the System Administrator from deleting themselves while they are logged in also prevents a conflict of permission within the UI.

Pressing the “Delete User” button opens a dialog window asking for user confirmation of this action (see Figure 75). The System Administrator user can cancel this action by pressing either the “x” button on the upper right corner of the dialog window, pressing the “Cancel” button, or closing the UI session. No user is removed from the V2I Hub because of this action if cancelled. Pressing the “Delete” button confirms the action.

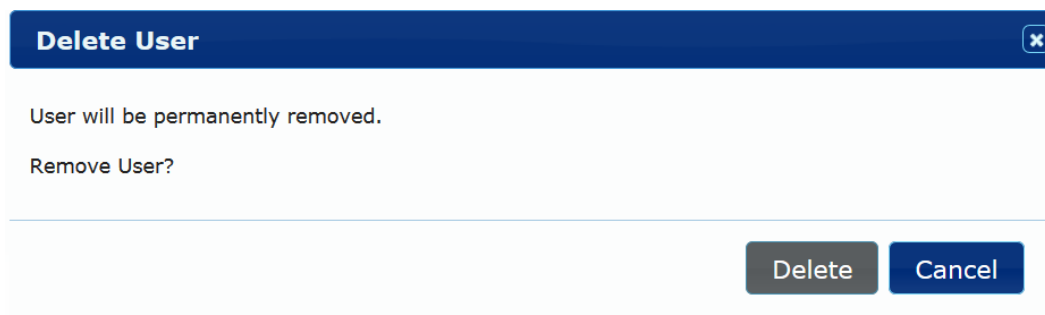


Figure 75. “Delete User” Dialog Window

Note that it may take a few seconds for the user to be removed from the V2I Hub and to send an updated list of users back to the UI. If the database successfully removes the user, the User List table updates to show that the table without the user (see Figure 76).

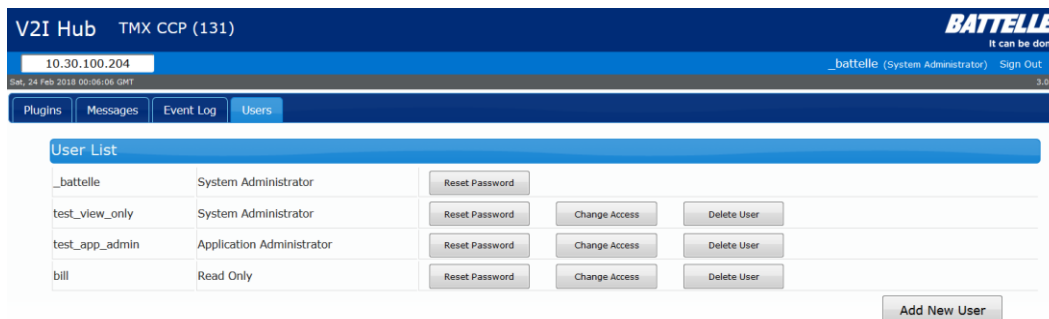


Figure 76. Users List Table with User Deleted

If deleting a user fails, a “Command Error” dialog window opens to display the resulting error message. This dialog window specifically describes what type of command failed (the “USERDELETE” denotes delete user commands).

Appendix A. SSL Certificate Exception

These instructions describe how to add an exception to the Firefox browser, so the Administration Portal can successfully connect.

1. Navigate to `https://<IP address>:19760`, where `<IP address>` will be the V2I Hub's IP address (see Figure 77).

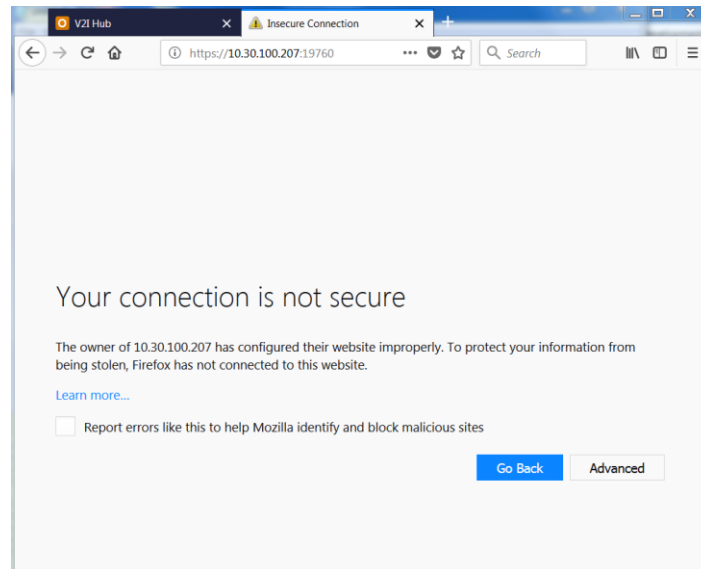


Figure 77. Insecure Connection Page for "https://<IP Address>:19760"

2. Click "Advanced" (see Figure 78).

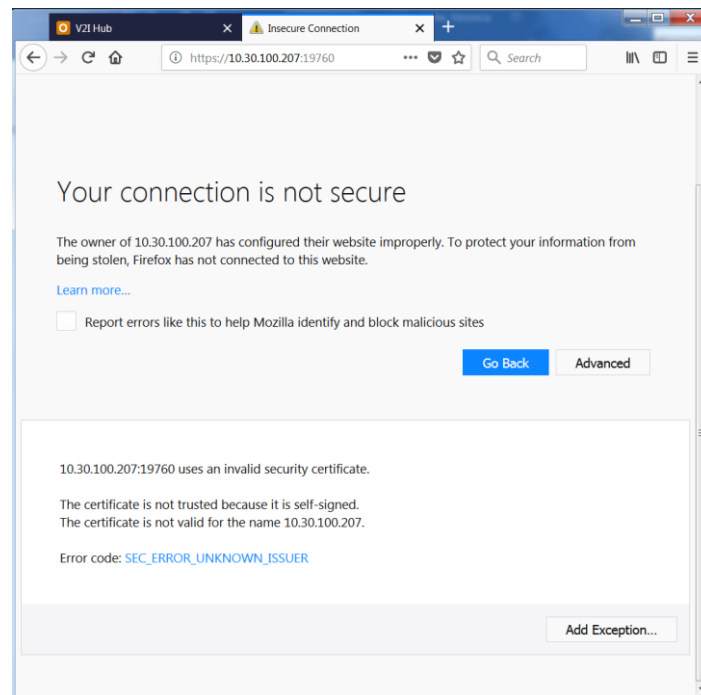


Figure 78. Advanced Options for an Insecure Connection

3. Click “Add Exception...” (see Figure 79).

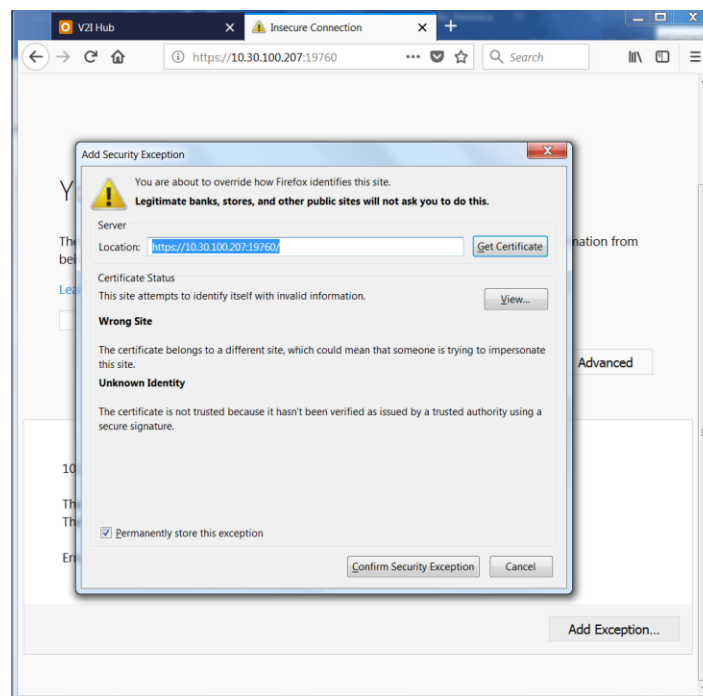


Figure 79. Adding an Exception for an Insecure Connection

4. Check “Permanently store this exception”, if not already checked.
5. Click “Confirm Security Exception” (see Figure 80).

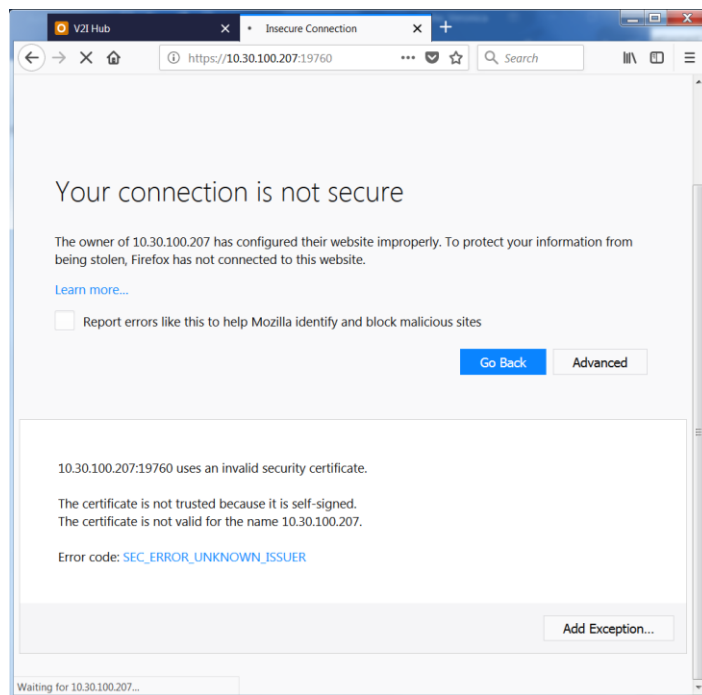


Figure 80. Exception Added for an Insecure Connection

6. Close “Insecure Connection” tab.

Appendix B. Acronyms

CAV	Connected and Automated Vehicles
FHWA	Federal Highway Administration
HTML	Hypertext Markup Language
IP	Internet Protocol
MAP	Roadway Geometry and Attribute Data (a.k.a. GID)
SCP	Secure Copy Protocol
SPaT	Signal, Phase, and Timing
SSL	Secure Sockets Layer
UI	User Interface
V2I	Vehicle-to-Infrastructure
XML	Extensible Markup Language

U.S. Department of Transportation
ITS Joint Program Office – HOIT
1200 New Jersey Avenue, SE
Washington, DC 20590

Toll-Free “Help Line” 866-367-7487

www.its.dot.gov

FHWA-JPO-18-646



U.S. Department of Transportation