

Version 25



Trapeze

Enterprise Asset Management

KeyValet

Administrator Guide

Trade Secret | February 2025

© 2025 Trapeze Software ULC, its subsidiaries and affiliates (collectively “TSU”). All rights reserved.

Trapeze Software ULC (“TSU”) Proprietary and Confidential: Information contained in this document is proprietary to TSU and its subsidiaries and may be used or disclosed only with written permission from TSU. This guide, or any part thereof, may not be reproduced without the prior written permission of TSU. The recipient acknowledges and agrees that disclosure of this document to recipient, and its use, are subject to the terms and conditions specified in their relevant software license agreement, software maintenance agreement, and/or non-disclosure agreement (“Governing Agreement”) under which this document was disclosed. This document is for internal use only in conjunction with TSU products. This document may not be modified in any way.

All other trademarks, registered trademarks, product names and company names or logos mentioned are the property of their respective owners.

Except as may be provided in the Governing Agreement, TSU and its affiliates, subsidiaries, officers, directors, employees, and agents provide the information contained in this manual on an “as-is” basis and do not make any express or implied warranties or representations with respect to such information including, without limitation, warranties as to non-infringement, reliability, fitness for a particular purpose, usefulness, completeness, accuracy or currentness. TSU shall not in any circumstances be liable to any person for any special, incidental, indirect or consequential damages, including without limitation, damages resulting from use of or reliance on information presented herein, or loss of profits or revenues or costs of replacement goods, even if informed in advance of the possibility of such damages.

TSU reserves the right, to be exercised at its sole discretion and without notice, to change, modify or adapt the contents of this edition in order to accurately reflect any future upgrades to the TSU proprietary software and/or hardware. In the event of such changes, TSU expects, but does not represent or guarantee, that this current edition will continue to remain reasonably accurate insofar as it describes the basic functions of the TSU proprietary software and/or hardware. Furthermore, based on your system settings, certain functionality, such as application screens, may not function exactly as shown or described in this guide.

Technical Support

Trapeze provides several ways to connect with the Customer Care team. Please provide detailed information to the representative. If you are reporting an issue by e-mail, include any error messages, screen shots of your problem, and steps to replicate the issue.

Customer Care is available Monday through Friday, 8:00 a.m. to 8:00 p.m., Eastern Standard Time.

Toll-Free Telephone: 1-877-411-8727

E-mail: cc@trapezegroup.com

FTP Site: <https://ftps.trapezegroup.com/>

Web Site: <https://collaborate.trapezegroup.com>

The website provides access to Trapeze Collaborate which offers resources to implement and operate the software, search knowledge, participate in communities, log/track service requests, sign-up for release alerts, view product health recommendations, and download updates or documentation. For secure access to Collaborate, contact Customer Care through the website or by calling the number above.

Product Compatibility

Refer to the latest [Product Compatibility](#) information on Trapeze Collaborate for requirements including operating system information, databases, Crystal reports, network protocol, HTTP servers and browsers that are supported.

KeyValet - Administrator Guide

Version 25.x

February 2025

Contents

1. Overview.....	1
Requirements.....	2
Hardware Options	2
Assumptions	2
2. Installation.....	3
KeyValet Setup	3
KeyBox Configuration.....	3
Editing the .XML File.....	3
KeyBox Manager.....	6
General Settings	7
Main KeyBox Manager Window.....	19
3. KeyValet MAXQueue Setup.....	27
4. Understanding KeyValet.....	28
How It Works.....	28
Using KeyValet and Reservations.....	29
5. SSL Setup.....	32
Changing Bindings to Support HTTPS in IIS.....	32
Export SSL Certificate	33
Import the SSL Certificate to the KeyValet.....	39
Configure KeyBoxManager.exe.config for SSL	48
Configure KeyBoxKiosk.exe.config for SSL.....	49
Verify Connectivity.....	51
Appendix A. Additional Information	53
A.1 Notes and Assumptions	53
A.2 KeyValet Ready Checklist.....	54
A.3 Site Layout Diagram	55
A.4 Antenna Diagrams for Wiring to KeyValet Controller.....	56
Location Criteria.....	57
System Components.....	57
Vehicle List	57
A.5 Keybox Diagrams.....	58
Keybox Mounting Diagram	58

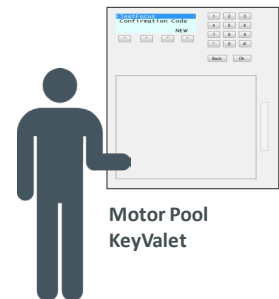
	KeyBox Power Box	59
	Circuitry and Cable Connections	60
	Keybox Schematics for Various Keybox Sizes.....	60
A.6	Module Config.....	65
	MAXQueueDesigner Settings Tab.....	65
	Services to enable	65
	Data Events enabled.....	66
	Module Dependencies	66
	Services to configure.....	66
A.7	KeyValet Upgrade.....	67
	Packaged folders	67
	Steps to perform KeyValet upgrade.....	67

1. Overview

Motor pools allow fleet managers to make their fleet more right-sized by reducing fleet size while increasing use. Successfully managing a motor pool involves many components including customer reservations, vehicle check-out, billing, and maintaining the motor pool vehicles. KeyValet is a comprehensive solution for successfully running a motor pool.

KeyValet integrates with FleetFocus motor pool software which manages every aspect of the motor pool fleet and allows fleet managers to deploy an unmanned motor pool in an efficient, secure, and cost-effective manner. This product also provides 24/7 access through an online portal for your customers to reserve their vehicles along with a secure automated keybox with radio frequency connectivity to record trip data and provide accurate odometer updates. These features, coupled with reporting and integrated customer billing, make KeyValet the only motor pool solution you need.

- A single software solution to handle all aspects of your motor pool including reservations, availability management, customer notifications, dispatch, and billing.
- Online access for customers to reserve motor pool vehicles 24/7. Automated confirmation emails are sent directly to the customer with a reservation-specific confirmation code.
- Real-time odometer readings from motor pool vehicles at the start/end of the trip automatically updating FleetFocus thereby reducing data entry time and errors.
- Secure key storage for unmanned motor pool with smart-card options.
- A radio-frequency identification device (RF ID) installed in every vehicle that also works with FuelFocus, thus, reducing additional hardware. (As an option, KeyValet can also be used without RF ID boxes in each vehicle. However, in this case, customers are required to manually key in their vehicle's mileage.)
- Integrated billing and reporting using FleetFocus.



Requirements

Application 25.x

Web Modules 25.x

- Motor Pool module
- Reservations module
- Notifications module
- MAXQueue server with KeyValet services
- Reporting module (recommended)
- Dashboards module (recommended)

Hardware Options

- KeyValet boxes: Sized according to requirements.

Latched Assets						
Standard Configuration	3 Key	8 Key	16 Key	32 Key	64 Key	96 Key
Dimensions						
Weight*	15 lbs.	20 lbs.	45 lbs.	65 lbs.	95 lbs.	130 lbs.

- HID option: Available if User ID is required for reservations.
- Keycode on key ring: Provides cross index to Equipment ID.

Assumptions

This guide assumes familiarity with workflows and configuration of the application.

- ❗ User defined required fields that do not appear in the Web Modules will return validation messages.
- ❗ Special characters cannot be placed into the Web Modules fields or unanticipated results may occur. This would include any character that cannot be typed with a standard keyboard.
- ❗ Do not use the browser's **Back** button in the Web Modules as unanticipated results may occur.
- ❗ Do not open or use the same instance of the Web Modules in multiple browser windows or tabs. This can cause errors or unexpected performance issues.

2. Installation

KeyValet Setup

Prior to installing KeyValet, it is necessary to setup the system as indicated below.

- To allow drivers to swipe their personal HID card to conveniently open the Keybox door, go to the **Authority** tab of the **Operator Primary** screen and populate the **Access Card ID** and **Facility ID** fields.
- Per standard FuelFocus setup, enter the vehicle VIB (Vehicle Integration Box) number/address in the **Fuel Card** field on the **Authorization** tab of the **Fleet Equipment** screen.

KeyBox Configuration

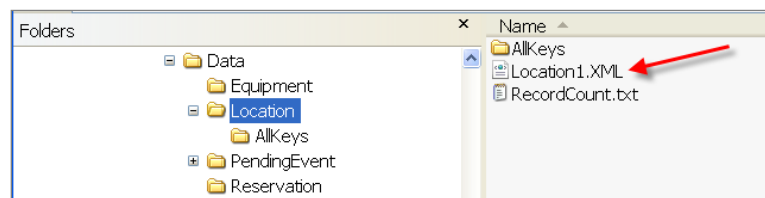
To configure the Keybox, it is necessary to manually edit the Location1.xml file as indicated below, and configure the General Settings page for KeyValet.

Editing the .XML File



The .xml file must be manually edited.

- On the KeyValet server, navigate to the Data – Location folder and manually edit the Location1.XML file (using a text editor) in order to define:
 - **Global settings:** Including the Equipment Selection Method, and
 - **Key-specific configurations:** Such as which key maps to each vehicle



- Manually edit the parameters, as needed, as described in the sample and definitions provided on the following page.
- Carefully edit the .xml file making sure all of the beginning and ending tags remain in their correct location. When you are done with your edits, save it and try double-clicking on the file using Windows Explorer. Internet Explorer will launch and attempt to open the file. If the syntax is correct, the file contents will display. If the syntax is incorrect, it will generate the following error: “The XML page cannot be displayed.”

Sample Location1.XML file:

```
<?xml version="1.0" encoding="utf-8" ?>

<Location xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <SystemName>YourCompany KeyValet</SystemName>
  <LocationID>MHQ</LocationID>
  <MeterRecentMinutes>5</MeterRecentMinutes>
  <KeyBoxAddress>localhost</KeyBoxAddress>
  <DataRefreshMinutes>2</DataRefreshMinutes>
  <CommittedRefreshMinutes>1</CommittedRefreshMinutes>
  <EquipmentSelectionMethod>RANDOM</EquipmentSelectionMethod>
  <VDCListener>true</VDCListener>
  <VDCPath>D:\KeyValetServer\FASuite\VDC</VDCPath>
  <LiveData>true</LiveData>
  <PromptParkingStall>false</PromptParkingStall>
  <PromptDriverLicense>true</PromptDriverLicense>

  <Keys>
    <Key>
      <KeyID>0001</KeyID>
      <EquipmentID>901</EquipmentID>
      <Panel>1</Panel>
      <Position>1</Position>
      <AccessKey>
        <FacilityCode>113</FacilityCode>
        <CardID>10605</CardID>
      </AccessKey>
    </Key>
    <Key>
      <KeyID>0002</KeyID>
      <EquipmentID>902</EquipmentID>
      <Panel>1</Panel>
      <Position>2</Position>
      <AccessKey>
        <FacilityCode>113</FacilityCode>
        <CardID>10601</CardID>
      </AccessKey>
    </Key>
  </Keys>
</Location>

—End of Document —
```

Header Parameter Definitions:

- **<System Name>**: Name that shows at the top of the Keybox display.
- **<LocationID>**: Motorpool Location in the system.
- **<MeterRecentMinutes>**: Number of minutes allowed before the keybox prompts for odometer. If the reservation does not receive a Return meter reading (e.g., from a VIB

unit) within that number of minutes, the keybox prompts the user to manually enter the odometer reading.

- **<EquipmentSelectionMethod>**: Options are: RANDOM, LEASTMILES, MOSTMILES, or ALL (allows driver to select any key of that pooltype). Recommend using: RANDOM. Be sure to use all capital letters.
- **<VDCListener>**: Enables or disables the vehicle VIB boxes for data collection. Set to True if using VIBs.
- **<PromptParkingStall>**: Option to ask driver to enter parking stall upon return. Writes to the Fleet Equipment and Motor Pool center screens.
- **<PromptDriverLicense>**: Option to prompt operator if they have valid driver's license. Keybox door will not open unless they respond (Y)es.
- **<EquipmentSelectionPriority>**: Set to LEASTUSED. When EquipmentSelectMethod is RANDOM, out of all available type, raises priority of the vehicle to be randomly chosen based on which vehicles have not been recently used on a reservation.

Settings not normally changed:

- **<DataRefreshMinutes>**: How often the server is queried for updates to MP reservations.
- **<VDCPath>**: This should never change.
- **<EquipmentRefreshMinutes>**: How often the server is queried for pool equipment information.

Future Settings Enhancements:

- **<EmergencyKeys>**: HID cards that allow full access to retrieve any keys from the keybox.
- **<AllowLatePickup>**: Option to allow pickups well beyond the reservation start. Operator will be prompted to confirm that vehicle will still be returned at original return time.

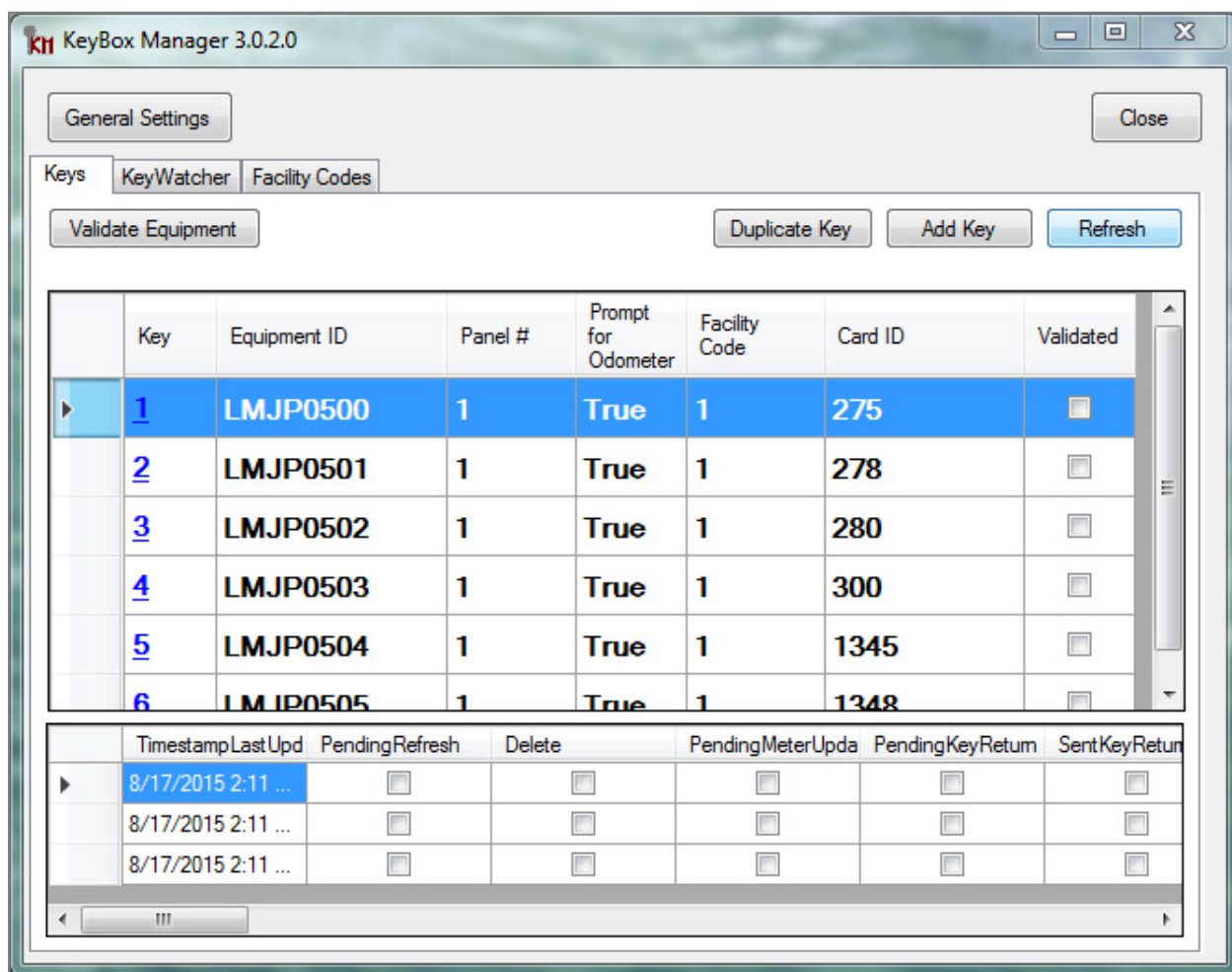
Key Parameter Definitions:

- **<Key ID>**: Unique ID for the key on this box/panel.
- **<EquipmentID>**: The equipment ID that has a key in this position/slot.
- **<Panel>**: Will always be '1'. Unique ID for this keybox.
- **<Position>**: Slot number for this key in the box.
- **<FacilityCode>**: Customers are informed of their facility code.
- **<CardID>**: (Optional) This is only used for key fobs. The ID is on the key fob itself.

KeyBox Manager

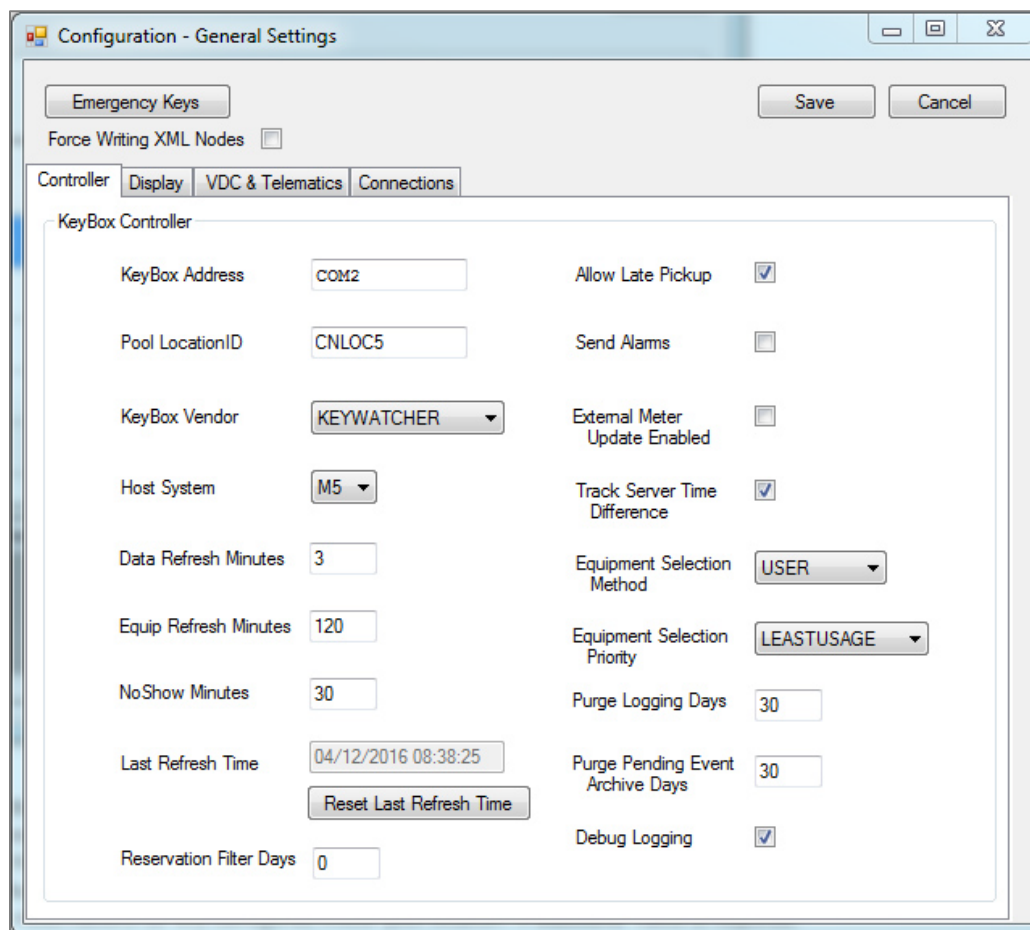
The KeyBoxManager.exe configuration utility was designed to be an interface with KeyValet's Location1.xml and parking.xml files. When you start the KeyBoxManager.exe file, you can configure many settings.

When you open the KeyBoxManager.exe program, the Keys tab displays by default. The bottom section of this tab contains a list of current reservations.



General Settings

Use the General Settings button to edit application settings relevant to all versions of KeyValet (Key Systems, Key Watcher, and SafePack). There are a number of tabs and settings to configure for KeyValet.



 When entering text for the system, The maximum number of characters for Key Systems is 20 characters, for KeyWatcher is 35 characters.

Emergency Keys Button

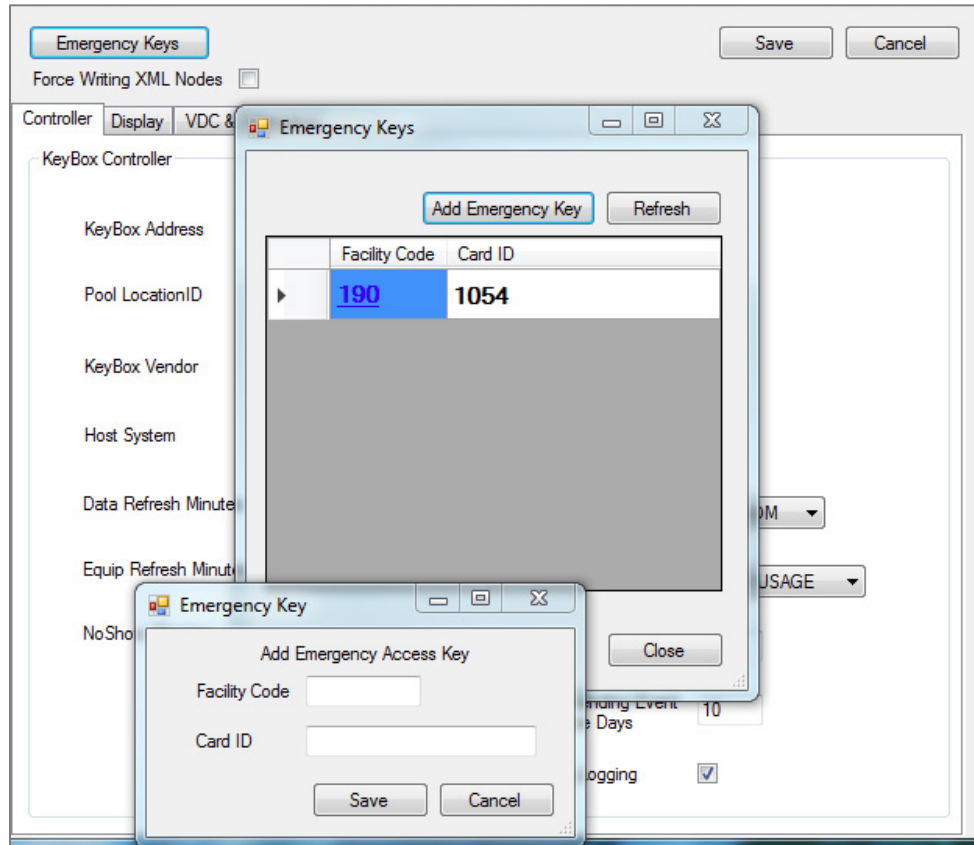
Use the Emergency Keys button to add, edit, or delete HID security cards (facility code or card IDs) from a list of emergency keys. Emergency keys can be used to access the Remove Key screen on the kiosk program running on the KeyWatcher program. When pushed, the Emergency Keys button will display a dialog with a list of configured HID cards.

 Note: For the HID reader to successfully read a swiped card, the HID settings must be configured correctly in the KeyWatcher tab or in the Key Systems web application.

To add or edit an emergency key:

1. Click **Emergency Keys**.

The Emergency Keys window displays.



2. Click **Add Emergency Key**.

This displays the window to add an emergency key. Here you can enter individual HID card values (Facility Code, Card ID). The card ID is generally marked on the HID card or fob.

3. Enter the information into the fields.

The facility codes must be obtained from the HID security card provider (or by viewing the Access.log which records all HID cards swiped over a HID reader).

4. Click **Save** to save the newly entered information, or click **Delete** to delete the key. If you click **Cancel**, you will exit the Emergency Keys window and nothing changes.

Force Writing XML Nodes

It is important to note the KeyBoxManager does not add new XML nodes into the Location1.xml file if they do not already exist, it will only update existing nodes. If you need to force writing out

all xml nodes to the Location1.xml file for a given screen, you need to check the **Force Writing XML Nodes** check box, and then click **Save**. All general settings are written into the Location1.xml file. For further information go [here](#).

Controller Tab

Settings on the **Controller** tab are essential for the keybox to work correctly.

KeyBox Address: Defines the IP address for the key systems keybox (for example: 172.22.1.100), or the COM port for communication to the KeyWatcher keybox. (for example: COM2).

Important: Set this setting first.

Pool Location ID: The Motor Pool location ID as set in FA or M5. Use all caps.

Important: You must set this correctly.

KeyBox Vendor: For KeyValet v3.0.0 and above, the two available options are as follows:

- KEYSYSTEMS
- KEYWATCHER

 Important: You must set this correctly.

Host System: Defines the destination hosting system. Possible options are FA and M5.

 Important: You must set this correctly.

Data Refresh Minutes: The number of minutes KeyValet will query the application server for updates on reservations for the configured motor pool location.

Equip Refresh Minutes: The number of minutes KeyValet will query the application server for updates on equipment data. A numeric value is required.

NoShow Minutes: The number of minutes beyond the scheduled pickup time when the reservation status will be changed to **NO SHOW** if the key is not retrieved from the keybox. A numeric value is required.

Reservations Filter Days: The number of days window (current date/time to future number of days) to download reservations from the server. 0 days will disable the filter.

 Note: FA Suite also uses download optimization, M5 only uses this setting to limit reservation downloads.

Last Refresh Time: The last successful download of reservations from server onto a controller. A date/time of 01/01/0001 00:00:00 indicates the next download will retrieve all reservations from the server which meet the necessary criteria (locationID, correct status).

Reset Last Refresh Time: Updates the last refresh time to 01/01/0001 00:00:00, thus resulting in all applicable reservation download at next collect data cycle.

Reservation Optimization: If this option is unchecked, the controller will download all reservations every time it requests a reservation from the server through the MAXQueue GetReservations interface. If this option is checked, the reservation is only downloaded once.

Allow Late Pickup: Enable or disable late reservation pickups. If checked, the keybox will allow late pickups up to the expected return date/time. Currently, only on Key Systems keyboxes, the operator is prompted to confirm the vehicle will be returned at or before the original reservation return time.

Send Alarm: Enable or disable sending alert messages if the user does not return a key properly. The user that will be alerted is configured on the MAXQueue server setting: vars.KeyValetAlarmUserId.

External Meter Update Enabled: This setting identifies whether the equipment meter readings will be provided by third party processes such as Network Fleet, etc. at the application server. When this setting is enabled, the equipment's meter reading is first retrieved before sending

motor pool transactions back to the user server. This option should be disabled if the PromptOdometer option is set to true or if VDC is being used.

Track Server Time Difference: This setting should always be enabled. When enabled, the controller requests the current date/time from the server and compares it with the PC controller's system time. If the difference is greater than one minute, the controller stores the time difference and adjusts the time when sending any date/time values to the MAXQueue server in data transmissions.

Equipment Selection Method: Defines the rules used to select from available motor pool equipment types. The options are as follows:

- Random: This is the recommended setting
- Leastmiles
- Mostmiles
- Ordered: This selects the oldest last date/time returned vehicle for dispatching
- User (prompts user to select from available vehicles)

Equipment Selection Priority: There are two options; LEASTUSAGE and NOPRIORITY.

- **LEASTUSAGE:** When the equipment select method is random, this raises the priority (out of all available vehicles) of the vehicle to be randomly chosen based on which vehicles have not been recently used on a reservation.
- **NOPRIORITY:** Leaves the priority as regularly listed.

Purge Logging Days: Defines the number of days log files are kept. Any log folders that are older will be deleted. The minimum days allowed are 30. If a value less than this is entered, the system ignores the value and uses 30. A numeric value is required.

Purge Pending Event Archive Days: Defines the number of days files are kept in the \Data\PendingEvent\Purge directory. A numeric value is required.

Debug Logging: Enable or disable extensive logging in LogDir directory.

 **Caution:** Enabling logging can result in large log files from controller activities.

Tablet Support: Check this box to enable tablet support. This option defaults to unchecked, or disabled.

Get Alternate Pool Types: Check this box to enable users to get pool types other than the one selected on the reservation if the type on the reservation is not available.

Display 1 Tab

Settings on the **Display** tab affect what is displayed and prompted for on the KeyValet key box.

Display Name: This is the text that shows at the top of the KeyBox console or touch screen display.

KeyBox Date Format: The format of the date time at the bottom of the console or touch screen display.

KeyBox Time Display Offset Hours: Defines the number of hours to offset from the controller/keybox system datetime, this also displayed at the bottom of the console or touch screen display.

 Important: the controller/keybox datetime must be set to the same as application/database server system date/time.

Prompt Personal Items: Enable or disable the prompt for personal items question. The wording for this prompt is entered in **Personal Items Line1** and **Personal Items Line2**.

Personal Items Line1: This text is used on first line of question **Prompt Personal Items**.

Personal Items Line2: This text is used on the second line of question **Prompt Personal Items**.

Prompt Service Request: Enable or disable the prompt for creating a service request. The wording for this prompt is entered in **Service Request Line 1** and **Service Request Line 2**.

Service Request Line 1: This text is used on first line of question **Prompt Service Request**.

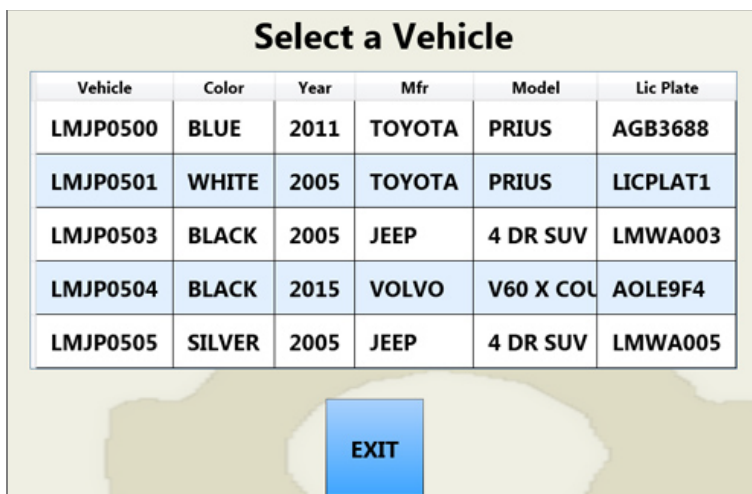
Service Request Line 2: This text is used on second line of question **Prompt Service Request**.

Confirm Create Service Request: Enter text to display when confirming the creation of a service request.

Prompt on Start Screen: Enter the text to show on the start screen.

Prompt Equipment: This text is used when the user is selecting a vehicle and the equipment selection method is set as **USER**. Vehicle is the default. The prompt will be **Select a [prompt equipment value]**.

For example, the below screen shot shows where this field displays. The word *vehicle* in **Select a Vehicle** and the first column labeled **Vehicle** are where the **Prompt Equipment** field displays.



The screenshot shows a screen titled "Select a Vehicle". Below the title is a table with the following columns: Vehicle, Color, Year, Mfr, Model, and Lic Plate. The table contains five rows of vehicle data. Below the table is a blue button labeled "EXIT".

Vehicle	Color	Year	Mfr	Model	Lic Plate
LMJP0500	BLUE	2011	TOYOTA	PRIUS	AGB3688
LMJP0501	WHITE	2005	TOYOTA	PRIUS	LICPLAT1
LMJP0503	BLACK	2005	JEEP	4 DR SUV	LMWA003
LMJP0504	BLACK	2015	VOLVO	V60 X COL	AOLE9F4
LMJP0505	SILVER	2005	JEEP	4 DR SUV	LMWA005

EXIT

Prompt Destination: Enable or disable the display of **prompt for destination** screen when doing an on-the-fly reservation. This screen is only available for FA host system only.

Prompt Parking Stall: Enable or Disable the screen to prompt for parking stall when returning the key.

Filter Parking Stalls: Check this box to filter out parking stalls that already have vehicles parked in them. Leave this option unchecked

Prompt Driver's License: Enable or disable the prompt for driver license during key pick up. The key box door will not open unless the user responds to this screen.

Allow ROTF: Check this box to enable on-the-fly reservations to be created.

Display 2 Tab

Emergency Keys Save Cancel

Force Writing XML Nodes ☐

Controller Display 1 Display 2 VDC & Telematics Connections

KeyBox Display (Cont.)

Prompt Fuel Level Line 1

Prompt Fuel Level Line 2

Send Fuel Level Other Event ☐

Prompt Reason for Trip ☒

Prompt Reason for Trip Line

Additional Questions Add Question Refresh

	ID	Order	Direction	Question Line 1	Question Line 2	Save 'Yes'	'Yes' Action	Save 'No'	'No' Action
▶	1	1	PICKUP	Do you have a	Class A license?	True	NEXT	True	EXIT
	2	1	RETURN	Did you remove all	trash from vehicle?	True	NEXT	True	EXIT

Prompt Fuel Level Line 1 and 2: Enter the text to display on the screen to prompt the user to enter the fuel level.

Send Fuel Level Other Event: Enables KeyValet to send a Fuel Other Event transaction from the controller to the server.

Prompt Reason for Trip: Check this box to prompt the user to enter a reason for the trip.

Prompt Reason for Trip Line: If this option is enabled, enter the text here to display to user to ask them for their trip reason.

Additional Questions: Use this section to add additional questions if needed.

Add Question: Click this button to add additional questions for the KeyBox.

- **Order:** The order in which the additional questions will be asked.
- **Direction:** The workflow directions in which the question will be asked (PICKUP, RETURN).
- **Line 1 and Line 2:** First and second lines of the question.

- **Save 'Yes':** Save the **Yes** button response on reservation notes. Options are TRUE or FALSE.
- **'Yes' Action:** When **Yes** is clicked as a response, use this option to set what the system does next. Options are BACK, EXIT, and NEXT.
- **Save 'No':** Save the **No** button response on reservation notes. Options are TRUE or FALSE.
- **'No' Action:** When **No** is clicked as a response, use this option to set what the system does next. Options are BACK, EXIT, and NEXT.

Refresh: Click **Refresh** to refresh the list.

VDC & Telematics Tab

The settings on this tab enable VDC and telematics data transmission.

The screenshot shows a software configuration window titled "Emergency Keys" with "Save" and "Close" buttons. Below the title bar is a checkbox for "Force Writing XML Nodes". A tabbed interface at the bottom includes "Controller", "Display 1", "Display 2", "Display 3", "VDC & Telematics" (which is selected), "Connections", "Parking Stalls", and "Watcher". The "VDC & Telematics" tab contains a list of settings: "VDC Enabled" (checked), "VDC Path" (text box with "C:\...\.VDC"), "WAF Debug Logging" (checked), "Telematics Enable" (checked), "Telematics Measures" (unchecked), and "Telematic Alerts" (checked).

VDC Enabled: Enables or disables the VDC software, and allows the system to perform vehicle VIB data collection. Enable if using VIBs to collect meter readings, alerts, and measures.

VDC Path: Path to VDC directory on the KeyValet controller. This should never need changing.

VDC Logging: Enable or disable the logging of VIB raw data and transmission converted to xml format. Log filename: WAFEvent.log.

Telematics Enabled: Enable or disable telematic data collection.

Telematics Measures: Enable or disable telematic measure data collection for FA host systems only when processing telematic data.

Telematics Alerts: Enable or disable telematic fault data collection for FA host systems only when processing telematic data.

Connections Tab

The Connections tab allows you to configure connection settings for SmartApps. The second half of this configuration area will vary by system setup. See the below sections for more information on this setup.

The screenshot shows a configuration window with the 'Connections' tab selected. At the top, there are buttons for 'Emergency Keys', 'Save', and 'Cancel'. Below these is a checkbox for 'Force Writing XML Nodes'. The 'Connections' tab contains a section titled 'MAXQueue Interface Services' which includes a text input field for the 'MAXQueue Interface Services URL' containing the text 'http://.../MAXQueue_MS/MAXQueue/InterfaceServices.asmx' and a 'Test' button.

MAXQueue Interface Services: This is the endpoint address to the MAXQueue web services.

M5 SmartApps Configuration

M5 SmartApps (Root) URL: If the host system (General Settings dialogue) is configured to be M5, this field will display the URL settings.

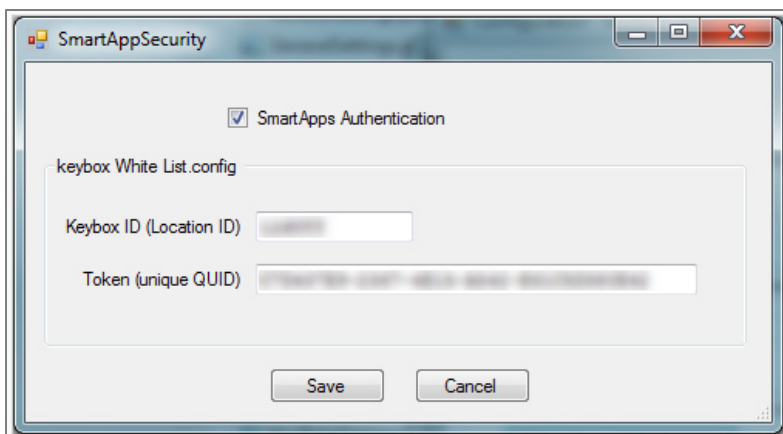


Note: The URL is only the root part of the URL. By clicking on the **M5 SmartApps Connections** group field, it will display the remainder of the URL for each specific web service. For example the full URL used to call the Service Request web service will be: (URL Root) + (Appended Create Service Request). So if the Root URL is `http://m5.assetworks.com/smartapps` and the Appended *Create Service Request* is `rotf/reservations`, the full URL is <http://m5.assetworks.com/smartapps/rotf/reservations>.

SmartApps Authentication Button

1. Click SmartApps Authentication.

The SmartAppSecurity dialogue displays.



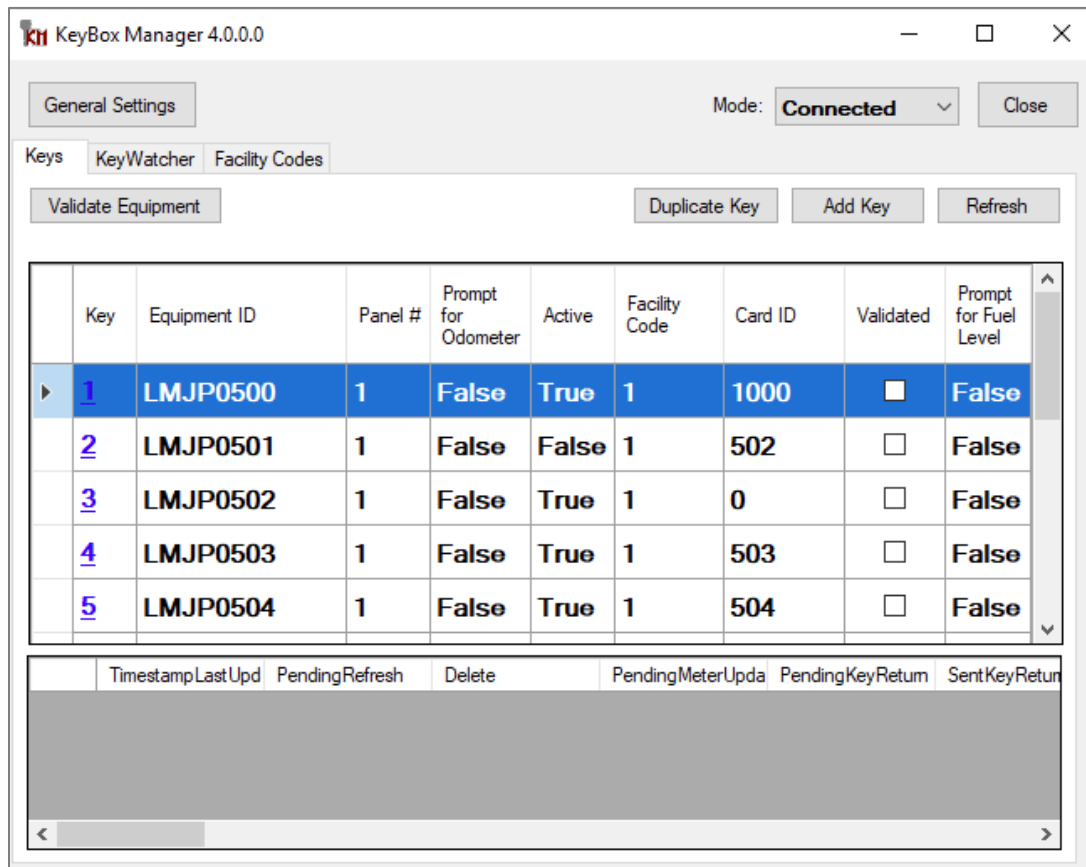
2. Fill out the necessary fields:
 - **Keybox ID (Location ID):** This should be the same value as found in the Location1.xml.
 - **Token (unique GUID):** This is a uniquely generated GUID.
3. Provide both of these fields' contents to the server administrator to be configured in the web.config file.

Asset Management System Configuration

FA Suite Connections: If the host system is configured to be FA, the FA Suite Connections field displays.

- **FASuite Application host name or IP Address:** Host name or IP address to access the FA server.
- **Port number:** Port number for the application server.
- **FA User:** MAXQueue FA user authorized to access the database.
- **FA Password:** MAXQueue FA user's password authorized to access the database.

Main KeyBox Manager Window



Keys Tab

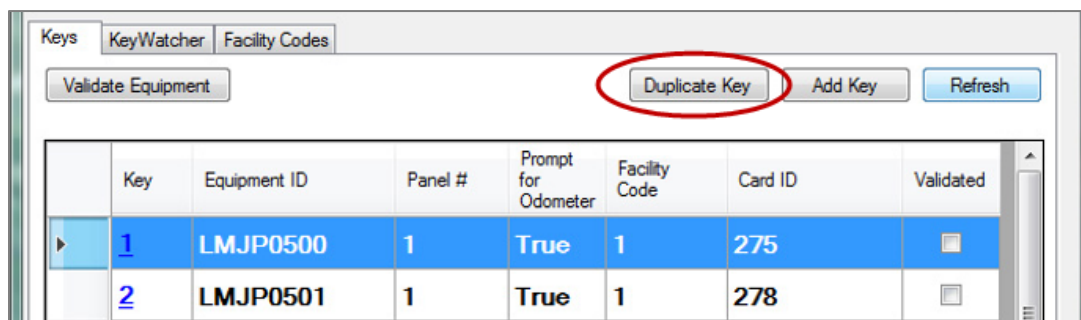
Use this tab to assign equipment IDs to a physical key. The data grid lists physical key numbers and their assigned Equipment IDs. The columns in this table show the following data:

- **Key:** The physical key number.
 - For Key Systems this is the slot number and key assigned to the lock.
 - For KeyWatcher it is the physical key # assigned by the keybox, not the slot number
- **Equipment ID:** Equipment ID of the asset as defined in the host system (FA, M5) to be associated to the key. This value is also used to request data from the keybox to the MAXQueue web server (KeyValet.GetPoolEquipment). If no equipment ID is assigned at this position leave the value empty (this must be done by manually editing Location1.xml file, for example: <EquipmentID></EquipmentID>).
- **Panel #:** Door panel number. This will always be 1. Even when a KeyWatcher site has multiple cabinets daisy chained together.

- **Prompt for Odometer:** Prompt for odometer when returning a key for the assigned equipment ID.
- **Facility Code:** The facility code assigned to the HID security card or key fob.
- **Card ID:** Card ID assigned to the HID security card or key fob. A keybox cannot have mixed HID card ID types or settings.
- **Validated:** If checked, this indicates the validate equipment operation has been done, and the equipment ID was found to be valid on the application server.

Duplicate Key

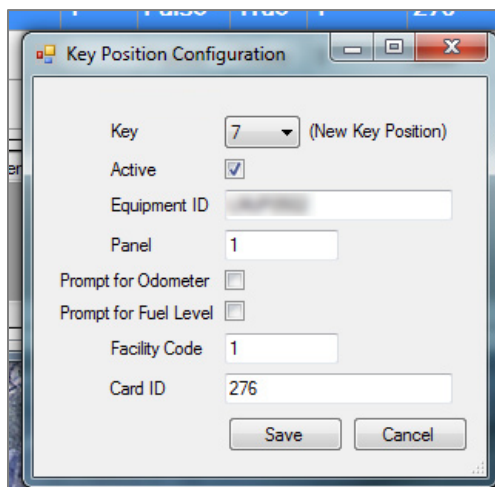
You can easily duplicate rows using the **Duplicate Key** button.



To duplicate a key:

1. Highlight a row in the table.
2. Click **Duplicate Key**.

This displays the Key Position Configuration window.



3. Enter the information on the Key Position Configuration window.

- **Key:** The Key drop-down menu (as shown in the screenshot above) populates by querying the keybox for its keys or slots and selects the next highest key value not already defined.
- **Equipment ID** and **Card ID:** These two fields must be changed. An error will occur if you try to duplicate without changing these fields.

4. Click **Save**.

Add Key

➡ Click the **Add Key** button to open the Key Position Configuration window with all fields empty except for the Key drop-down (which has the next highest key number selected).

Refresh

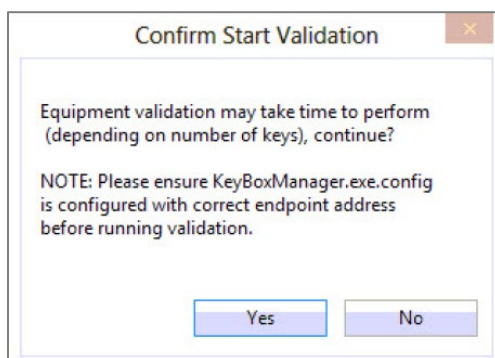
➡ Click **Refresh** to reload the Location1.xml file and update the Keys data grid.

Validate Equipment

Use this button to perform validations on each of the equipment IDs listed in the Keys data grid. To successfully perform validations, the KeyBoxManager.exe config file must have the endpoint address configured to the correct MAXQueue InterfaceServices.asmx.

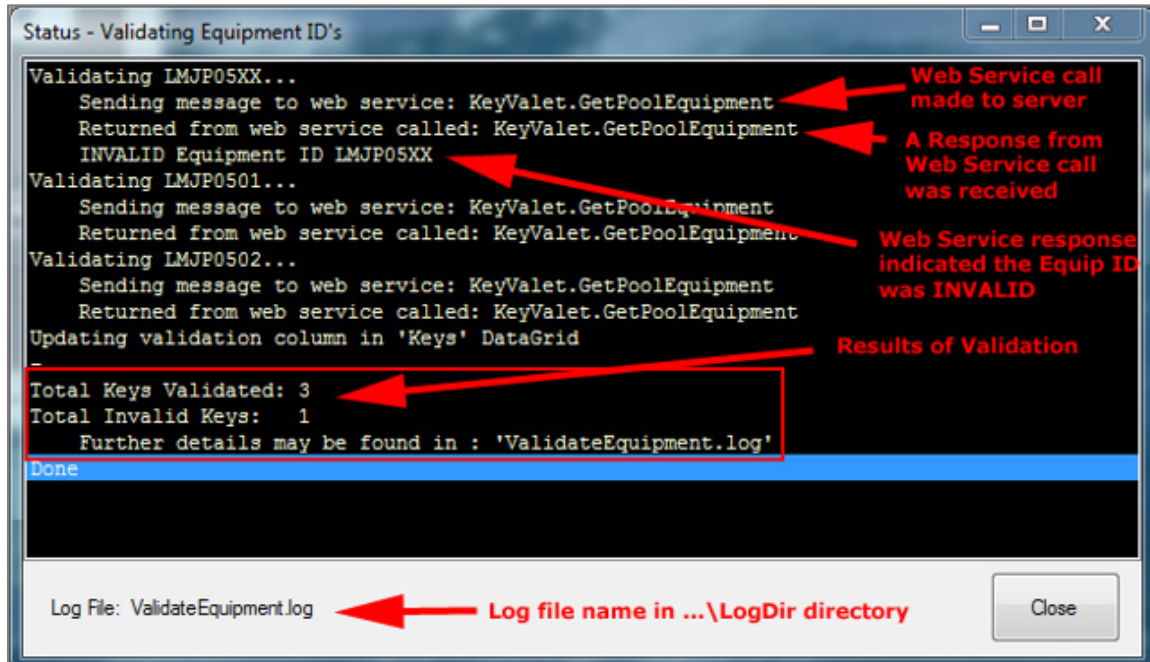
1. Click **Validate Equipment**.

A confirmation pop-in displays indicating that the procedure can take a significant amount of time if there is a large number of keys configured.



2. Click **OK**.

A command window displays similar to the following.



As seen above, each equipment ID configured in the Keys data grid will call the *GetPoolEquipment* web service. If the *KeyBoxManager.exe.config* is configured correctly, a response is indicated. If the response from the server is valid, no further message is displayed and the next key in the list will be validated. If the response indicates it is an invalid equipment ID (not found on the server for the configured Motor Pool Location ID) then an **INVALID** message is displayed.

At the end of the processing, a message displays with the total number of equipment IDs validated, and total number of invalid equipment IDs. The bottom of the window displays the name of the log file containing the results.

List of Reservations

At the bottom of the Keys tab, you can see a data grid the lists all reservations found in the keybox reservation directory. The data grid is for viewing purposes only.

	TimestampLastUpd	PendingRefresh	Delete	PendingMeterUpda	PendingKeyReturn	SentKeyReturn
▶	8/17/2015 2:11 ...	☐	☐	☐	☐	☐
	8/17/2015 2:11 ...	☐	☐	☐	☐	☐
	8/17/2015 2:11 ...	☐	☐	☐	☐	☐

KeyWatcher Tab

This tab has settings specific to the Morse Watchmen's KeyWatcher Keybox. There are three sections to this tab, and a button to configure parking stalls.

Settings

- **Door Latch Time Out:**
 - **Key Systems:** Number of seconds the door latch is activated to permit operator to open door.
 - **KeyWatcher:** Number of seconds the Dispatch screen is displayed before returning to the Options screen. A numeric value is required.
- **Administrator Password:** This displays the password to gain access to the administrator dialog. This is a view-only field.
- **Screen Saver Text:** Defines the character string to be displayed on screen saver. The maximum number of characters allowed is 25.
- **HID Reader Port:** KeyWatcher: Virtual COM port for Linkstream USB converter for Wiegand card reader. The string value prefix with **COM** (example: COM5).

HID Settings

- **HID Bit Size:** The size (in bits) of HID security card data in Wiegand format. A numeric value is required.
- **Facility ID Offset:** Offset position for the beginning of facility ID on HID security card in Wiegand format. A numeric value is required.
- **Facility ID Length:** Length of the Facility ID on HID security card in the Wiegand format. A numeric value is required.
- **Card ID Offset:** Offset position for the beginning of Card ID field in HID security card in Wiegand format. Numeric value required.
- **Card ID Length:** Length of the Card ID on HID security card in Wiegand format. A numeric value is required.

Slot Records¶



Note: This section is for informational purposes. These **Generate Slow Records XML** records are automatically generated. If the KeyBox Address has been correctly configured for the correct COM port, this section is automatically populated. The software should identify if Box 1 or Box 2 are connected, and the number of slots found in each box cabinet.

Parking Stalls¶

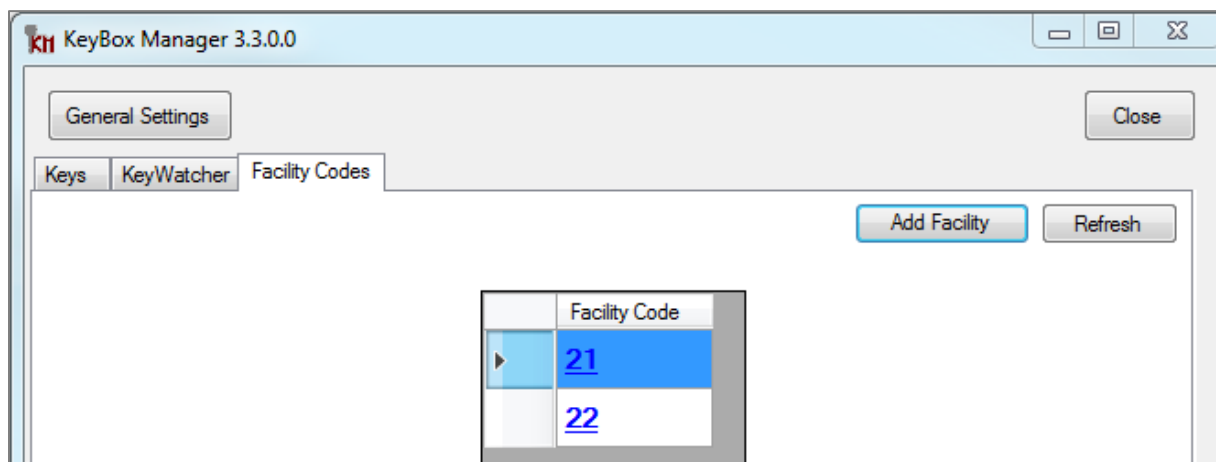
The parking stall configuration XML file is found in the ...**Data\Parking directory**. For KeyWatcher, the parking stall screen can be configured to be displayed. This screen prompts for the parking stall the operator has placed the returned vehicle in. This is a drop-down select control, which is populated by the configured parking stalls in this dialog.

Force Writing XML Nodes¶

This option forces writing all XML nodes to the Location1.xml file.

Facility Codes Tab

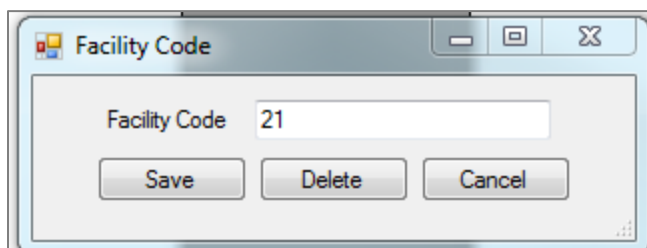
A KeyValet site using VDC may have issues with other companies in the area using VDC. This can result in vehicles being detected that do not belong to the desired site. To filter vehicles, enter the facility codes into the Facility Codes tab. Only VIBs who are in the list of facility codes will have their vehicle data processed.



To edit or delete a code:

1. Click the hyperlinked number to open the facility code.

The Facility Code window displays.



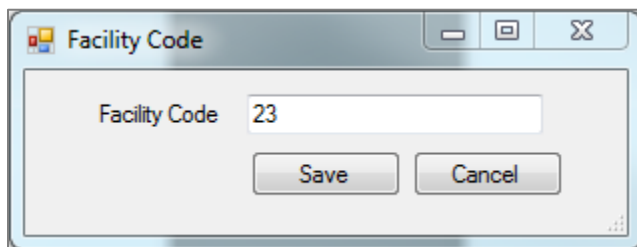
2. Change the facility code.
3. Click **Save** to save the code, **Delete** to delete the code, or **Cancel** to close the window with no changes.

Add Facility

To add a facility code:

1. Click **Add Facility**.

The Facility Code window displays.



2. Enter the new code.
3. Click **Save** to save the new code, or **Cancel** to close the window with no changes.

Refresh

 Click **Refresh** to reload the Location1.xml file and update the information.

3. KeyValet MAXQueue Setup

4. Understanding KeyValet

How It Works

- A motor pool customer logs on to your secure intranet and clicks the Reservations tab to make their reservation.
- Once the reservation has been completed, the customer receives an automated email containing a confirmation code which allows them to access the vehicle's key at the motor pool lot.
- Using this confirmation code and their employee ID, the customer is able to release the correct key from the secure keybox. Only the key for their pool type vehicle can be accessed. If a Committed reservation was set up, then only the key for the exact equipment ID is released.
- When the key lock box door is closed, the reservation automatically dispatches the vehicle in FleetFocus.
- The customer starts the vehicle and continues their trip.
- Once the customer returns with the vehicle, the odometer reading is taken wirelessly as the car enters the parking lot.
- The customer returns to the keybox and enters the confirmation code or vehicle number to open the keybox. Once the keys are inserted back into the required position and the door is closed, FleetFocus automatically updates the reservation as returned using the most recent wireless meter update. A completed reservation with cost summary is sent to the customer via email using FleetFocus Notifications. The vehicle's mileage is updated accurately in real-time in the maintenance system.

Using KeyValet and Reservations

This section provides a high level overview of how to use the Reservations Module and Key Valet.

1. **Make a Reservation:** Login to the Reservations Module and create a new reservation.

The **Reservations Home** page has two sections. The **My Info** section shows the driver's basic information, including contact info and license expiration. The **My Reservations** section displays driver's current vehicle reservations.

Reservations 

My Info

Operator ID

Name

Department ID

Account ID

License Expiration Date

Email Address

Mobile Phone

Address Line 1

Address Line 2

Address Line 3

Address Line 4

Work phone

What Do You Want To Do?

Update My Info

New Reservation

My Reservations

Expand All Collapse All

	Reservation ID	Status*	Pickup Date & Time	Return Date & Time	Vehicle Type	Pickup Location
	1-2019-00004 Confirmation Code: 032758	CONFIRMED	06/17/2019 10:30	06/21/2019 10:30		1 - OPS

* APPR REQD: Dispatch has not yet approved reservation;

COMMITTED: Reservation confirmed for a specific vehicle

CONFIRMED: Reservation confirmed

DISPATCHED: Vehicle is out for use and due by the return date and time

LATE: Vehicle is overdue - late fee(s) may be assessed

STANDBY: Vehicle not yet available;

Please refer to the Reservations Module Administrator Guide for details about this module and instructions for creating reservations.

2. **Receive email confirmation:** After you successfully create a reservation, you will receive an email containing a confirmation code and reservation ID. You need this code to access the vehicle's key at the motor pool lot.

Vehicle Reservation Details

Reservation ID 189 is CONFIRMED.
 Confirmation Code Required
 Use code 845903 at key station next to building stairs

Call 800-555-0987 if you need help

Customer: ALAN SIMPSON
 Department: 075
 Account: 4525
 Work Phone: 555-1423

Pickup Location:
 CAPITL
 123 MAIN STREET
 MESA, AZ

Phone: 800-555-1212
 Fax: 801-345-0987

Pickup Time: 02/01/2010 09:00 AM
 Return Time: 02/01/2010 04:00 PM

Vehicle Type: BAM

3. **Get the key from the keybox:** On the day of the reservation, go to the motor pool parking lot and enter the confirmation code into the keybox (or swipe a key fob in front of the HID reader). If prompted, validate your driver's license number using the keypad.

4. Open the door, and locate the key with the green light.

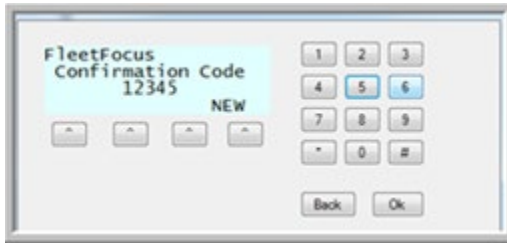
5. To release the key from the secure keybox, turn the key clockwise.

When the key is removed and the door is closed, the reservation is dispatched.

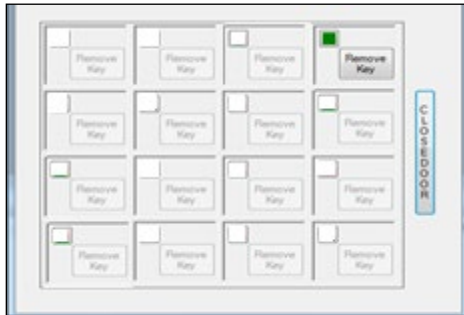
6. **Make the trip:** As the driver leaves, the meter reading is sent from the VIB through the Vehicle Data Controller (VDC). Upon return, another meter reading is sent from the VIB through the VDC.

 **Note:** The fuel level will also be retrieved by the VDC, or entered by the user.

7. **Return key to the keybox:** When the trip is finished, return to the parking lot and open the keybox door by entering the confirmation code (or swiping a key fob in front of the HID reader). Enter the parking stall using the keypad and press **Ok**.



8. Insert the key into the required position (as indicated by the green light) and turn the key counter clockwise.



9. After closing the door, the reservation is completed using the last updated meter reading from the VDC.
10. **Receive email receipt/cost summary:** You will receive a completed reservation with cost summary via email.

5. SSL Setup

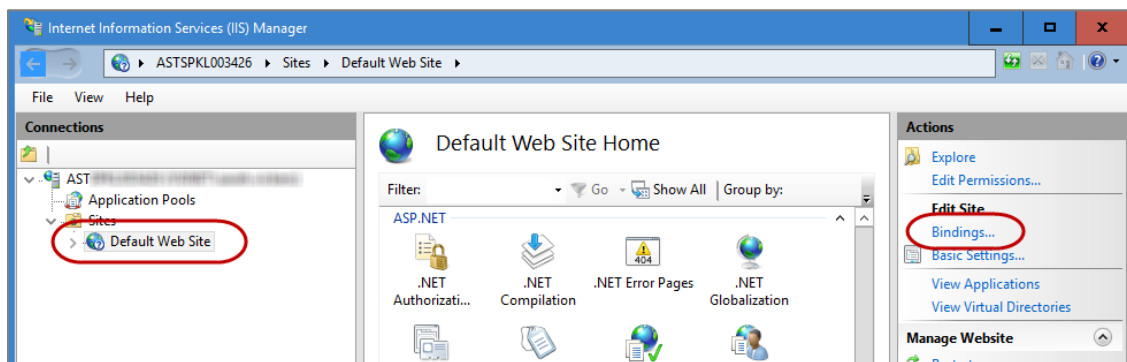
Changing Bindings to Support HTTPS in IIS

Requirements:

The SSL CA Certificate must be configured on the App Server before proceeding.

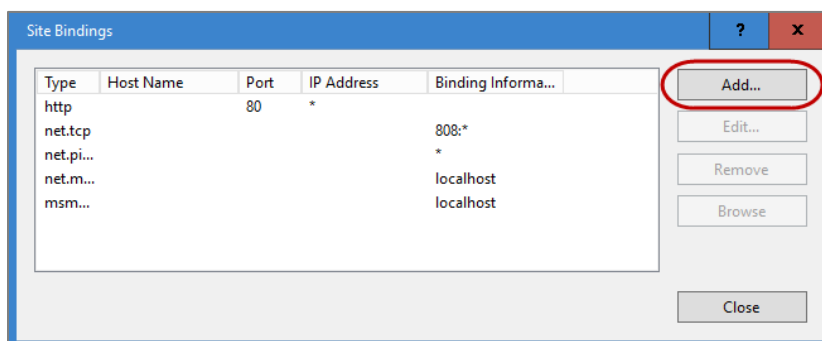
To configure the certificate:

1. Open the IIS Manager for the server.
2. Click **Default Web Site** on the left, then click **Bindings** on the right.

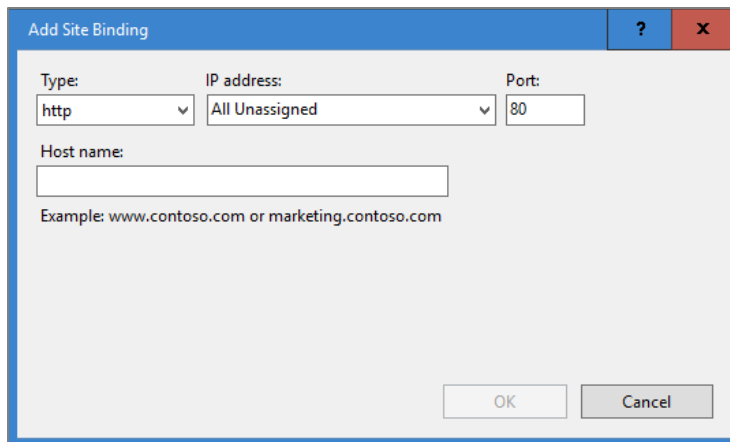


The Site Bindings window displays.

3. Click **Add**.



The Add Site Binding window displays.



4. Update the settings as follows:

- **Type: https**
- **IP Address:** Leave as **All Unassigned**
- **SSL Certificate:** Select the SSL Certificate installed on the server from the drop-down. This option only displays once the https type option is selected.

5. Click **OK**.

After this is set, the URLs will start with HTTPS instead of HTTP.

6. For example: This MAXQ Interface Services URL changed from

http://fuelfaserver.vgnet.volgrp.com/MAXQueueInterface/MAXQueue/InterfaceServices.aspx

to

https://fuelfaserver.vgnet.volgrp.com/MAXQueueInterface/MAXQueue/InterfaceServices.aspx

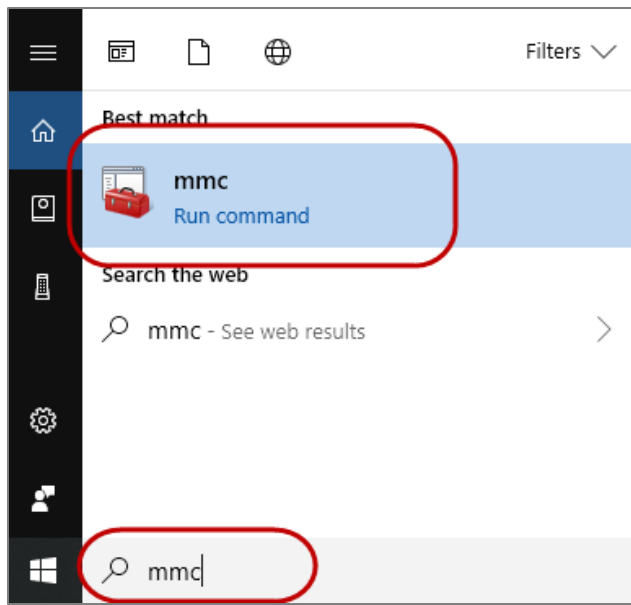
Export SSL Certificate

Requirements:

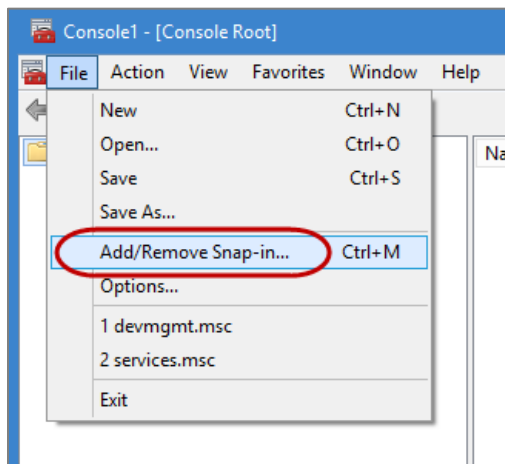
- The SSL CA certificate must be configured on the application server before proceeding.
- The Default Website bindings must be set to HTTPS (as done in the previous section).

To export the certificate:

1. Remotely connect to the application server.
2. On your computer, in the search menu, type in MMC, and click that mmc command to run.

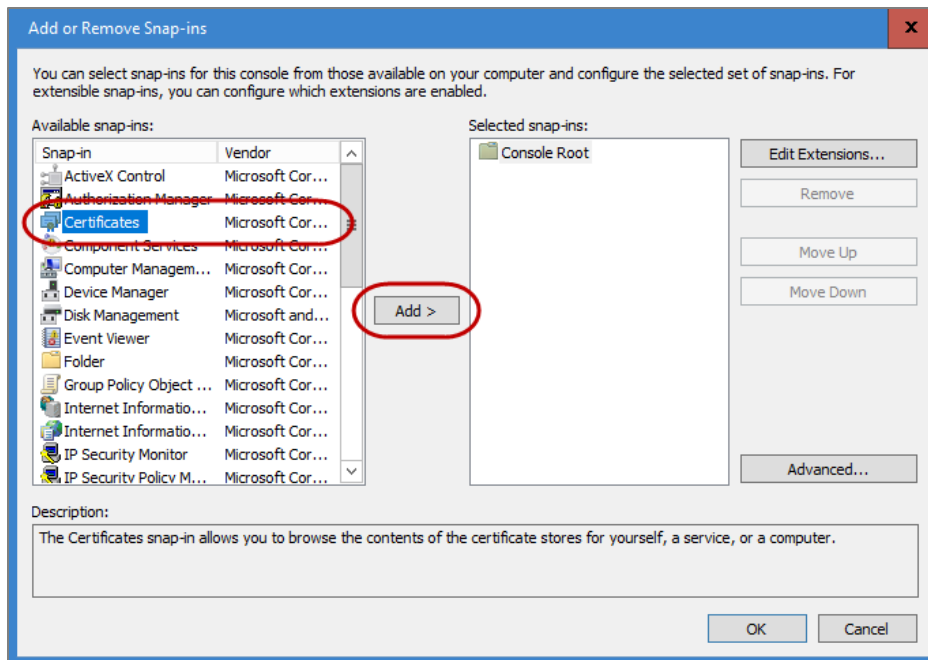


3. When the User Account Control window displays asking for permission to run the application, click **Yes**.
4. Click **File**, then click **Add/Remove Snap In**.

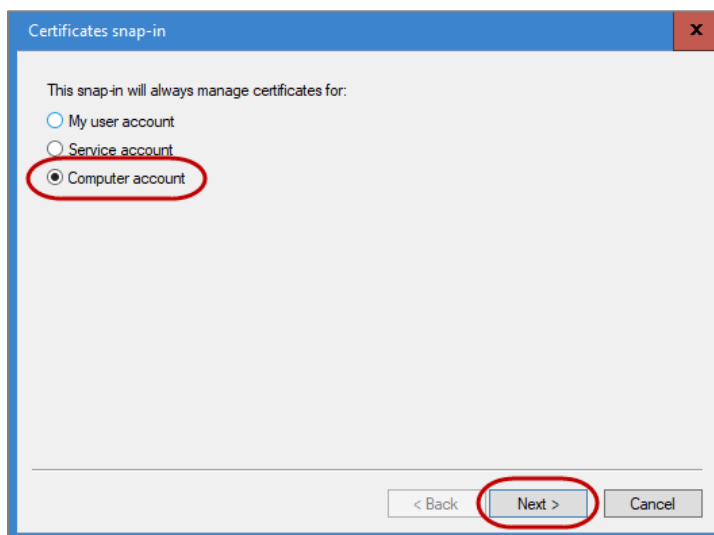


The Add of Remove Snap-ins window displays.

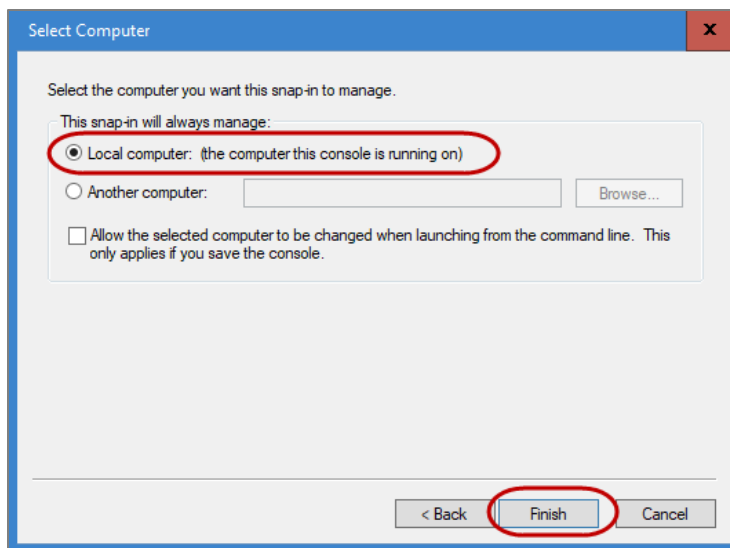
5. Click **Certificates** then **Add**.



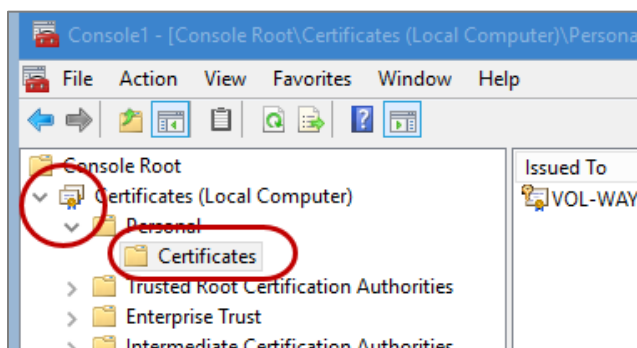
6. Select **Computer Account** then **Next**.



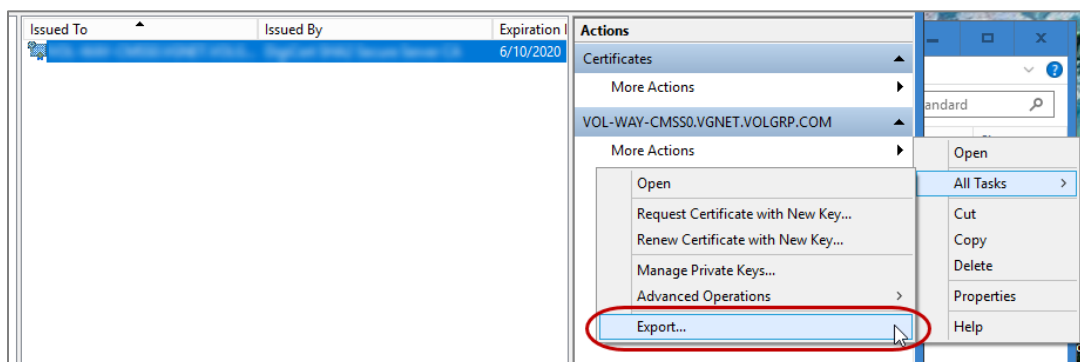
7. Click **Local Computer** then **Finish**.



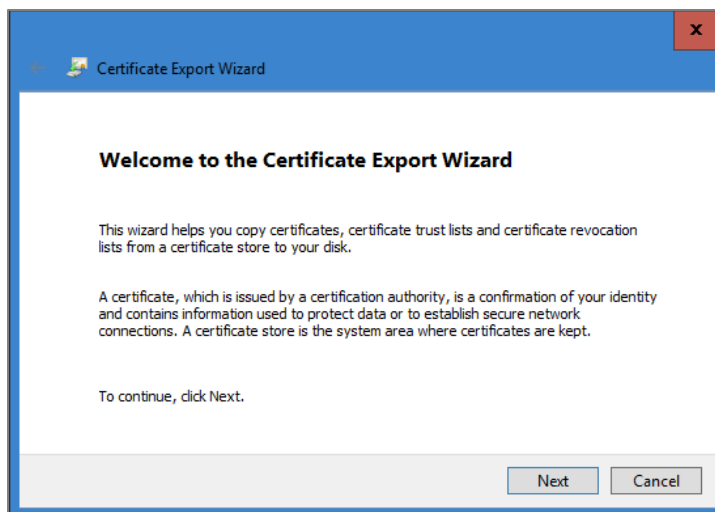
8. Click **OK** to exit the Add/Remove Snap-ins window.
9. Click the arrows to expand Certificates (Local Computer) and Personal, then click **Certificates**.



10. Click the certificate that will be exported to KeyValet.
11. In the Actions panel to the right, click **More Actions > All Tasks > Export**.

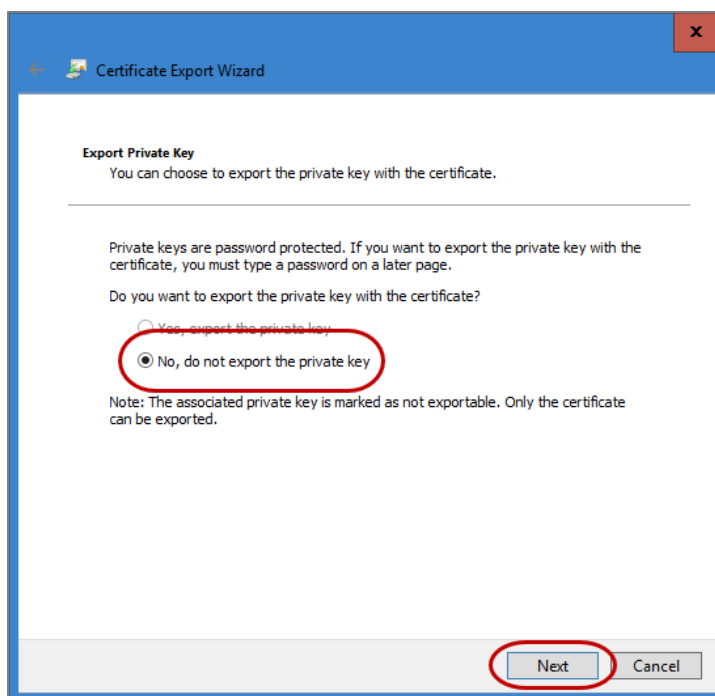


The Certificate Export Wizard will open.

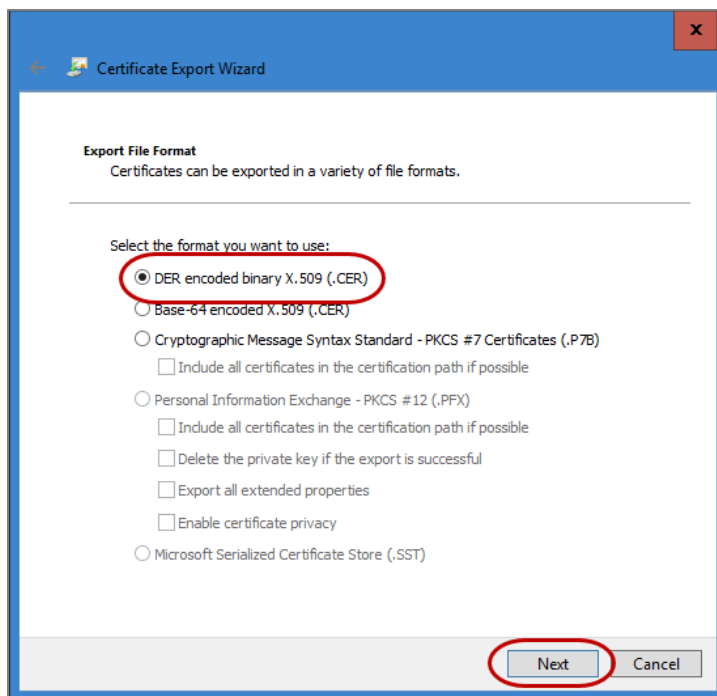


12. Click **Next**.

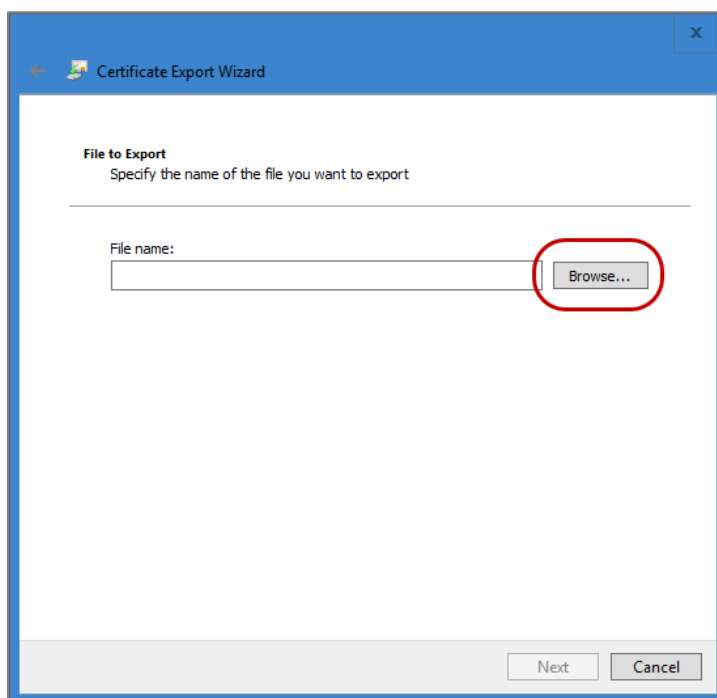
13. Select **No, do not export the private key**, then click **Next**.



14. Select **DER encoded binary X.509 (.CER)**, then click **Next**.



15. Click **Browse** to open the file path to where you need to export the certificate.

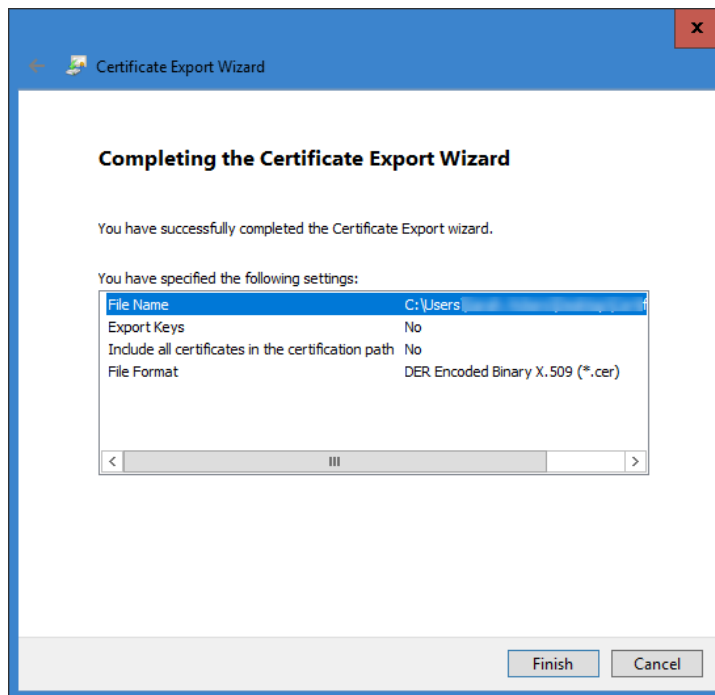


16. Enter a name for the certificate in the Save As dialogue and click **Save**.

The Save as dialogue closes.

17. Click **Next** in the Certificate Export Wizard.

18. Click **Finish**.

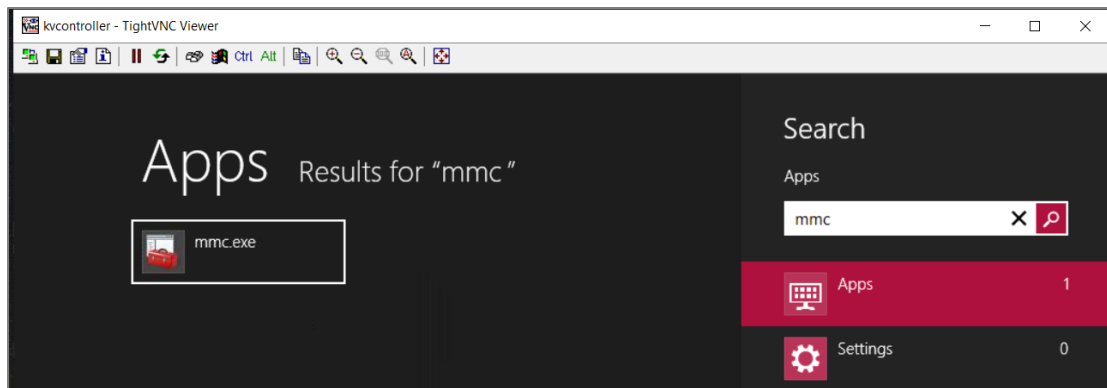


19. The system saves the certificate to a local computer that has remote access to the KeyValet.

Import the SSL Certificate to the KeyValet

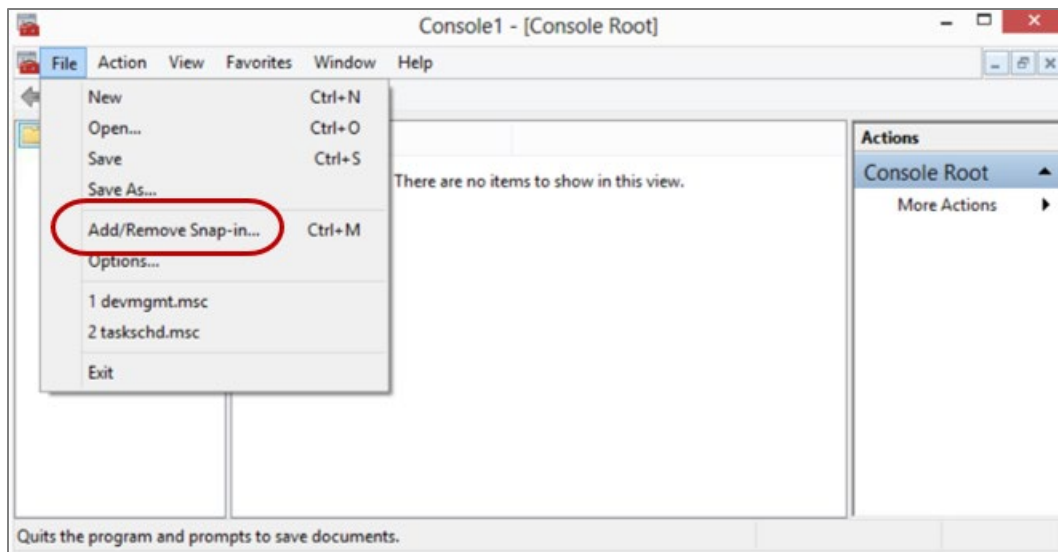
To open MMC:

1. Connect to the KeyValet with TightVNC.
2. Copy the certificate from the local computer folder to the KeyValet folder on the main computer drive (usually the C drive).
3. Click the Windows icon from the TightVNC toolbar.
4. In the Search field, type MMC, then click **MMC.exe**.

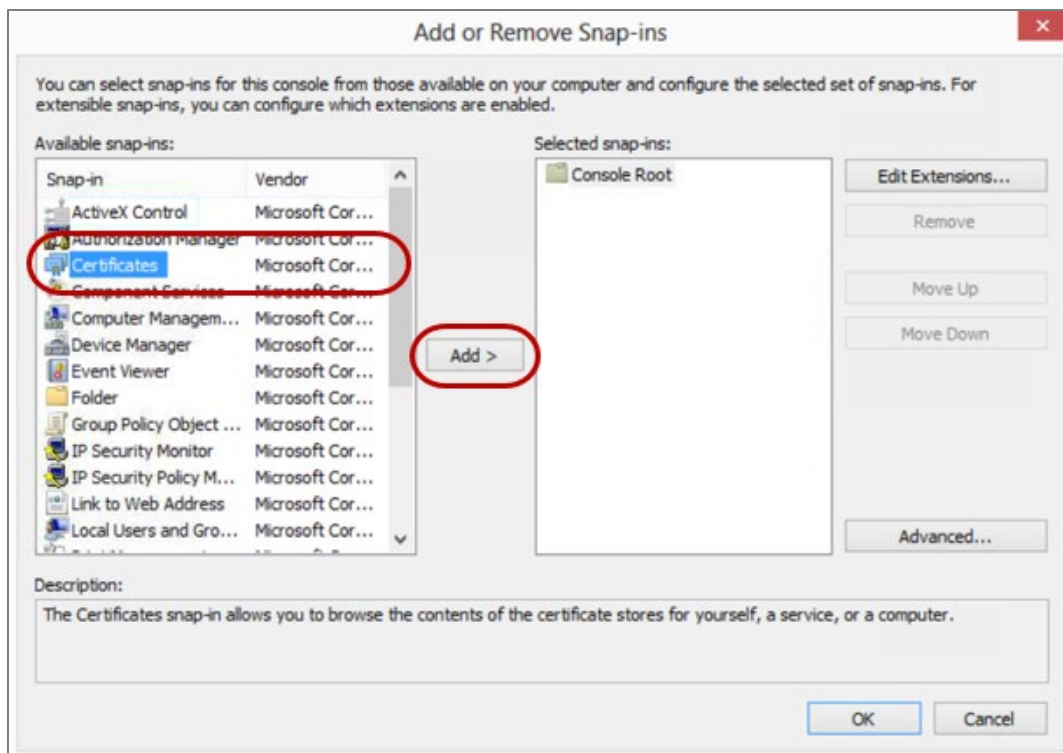


To add the certificate to the console:

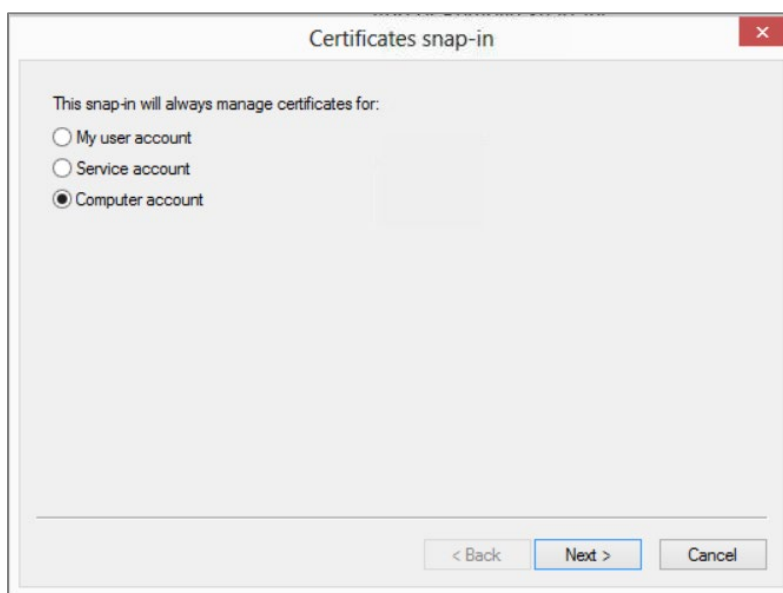
1. In the Console window, click **File**, then click **Add/Remove Snap-in**.



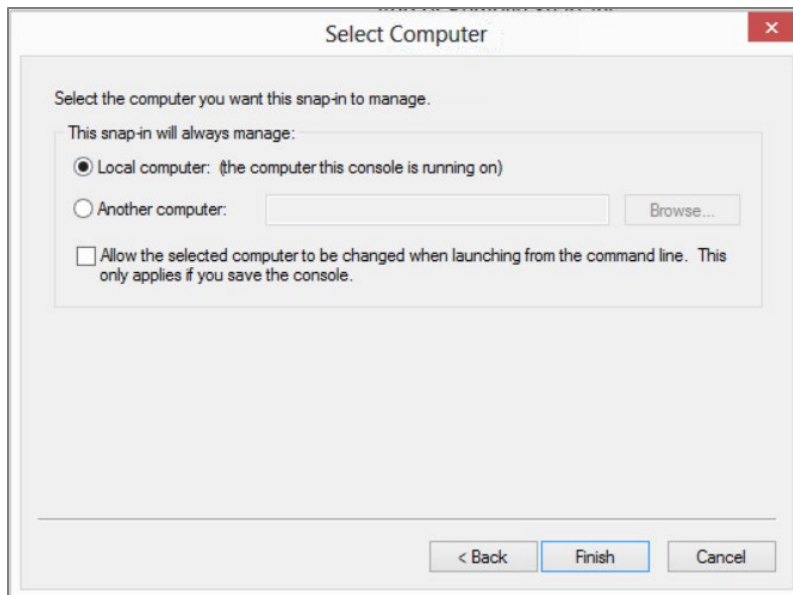
2. Click **Certificates** then click **Add**.



3. Select **Computer Account**, then click **Next**.



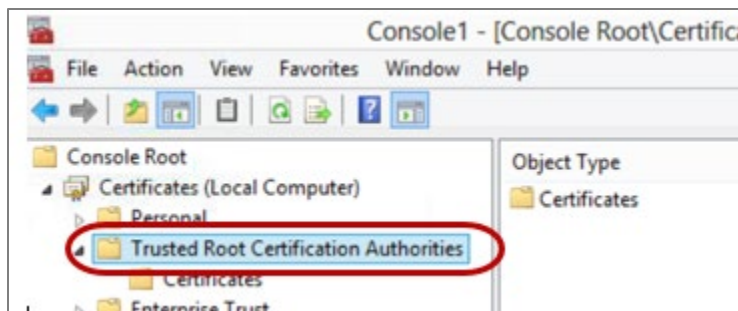
4. Select **Local computer**, then click **Finish**.



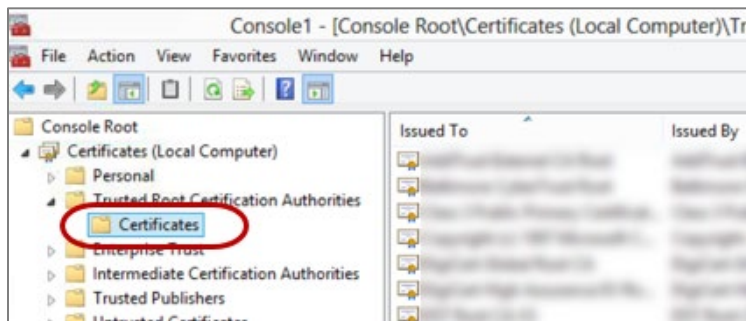
5. Click **OK** to exit the Add or Remove Snap-Ins screen.

To import the certificate:

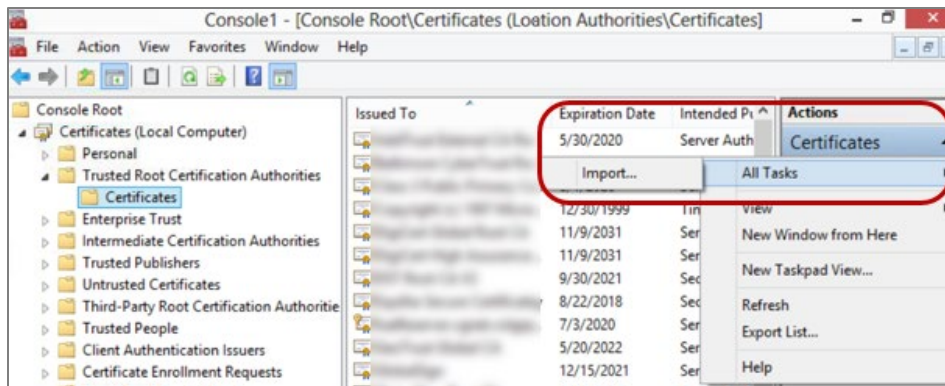
1. Click the arrow to expand **Certificates (Local Computer)**, and **Trusted Root Certification Authorities**.



2. Double-click **Certificates** under Trusted Root Certification Authorities.

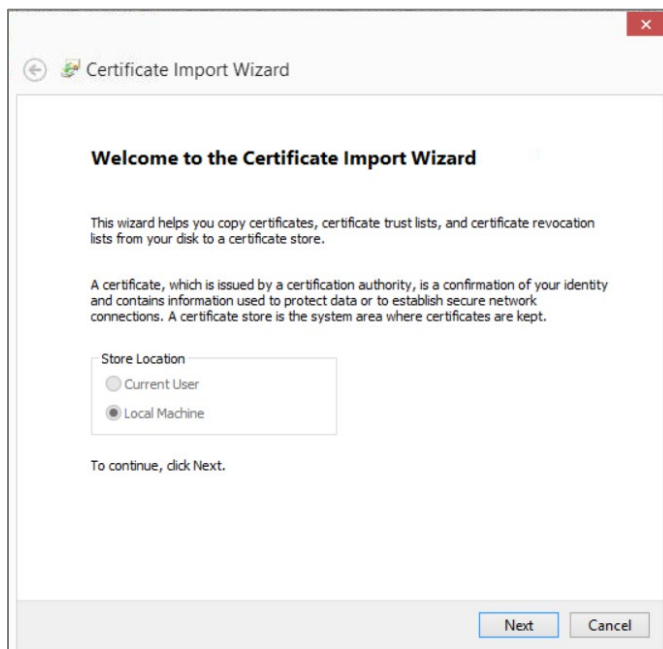


3. On the right of the Console window, under Actions, click **More Actions > All Tasks > Import**.

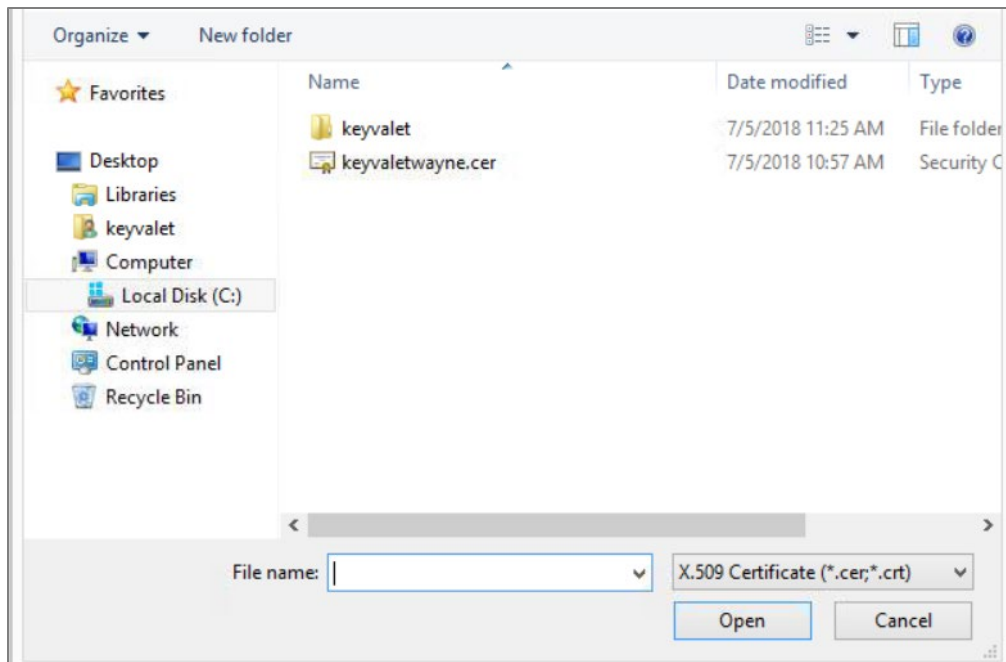


The Certificate Import Wizard displays.

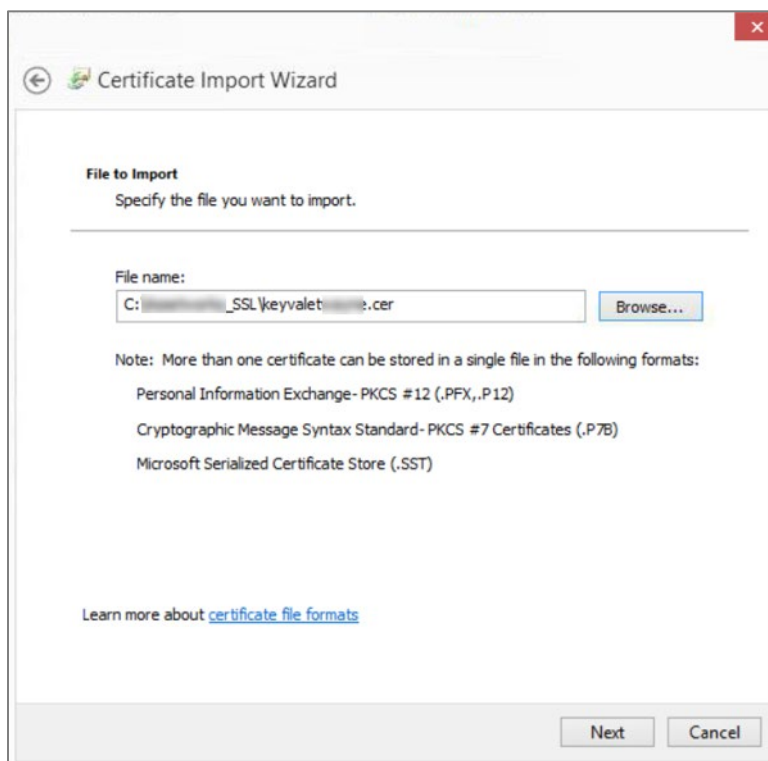
4. Click **Next**.



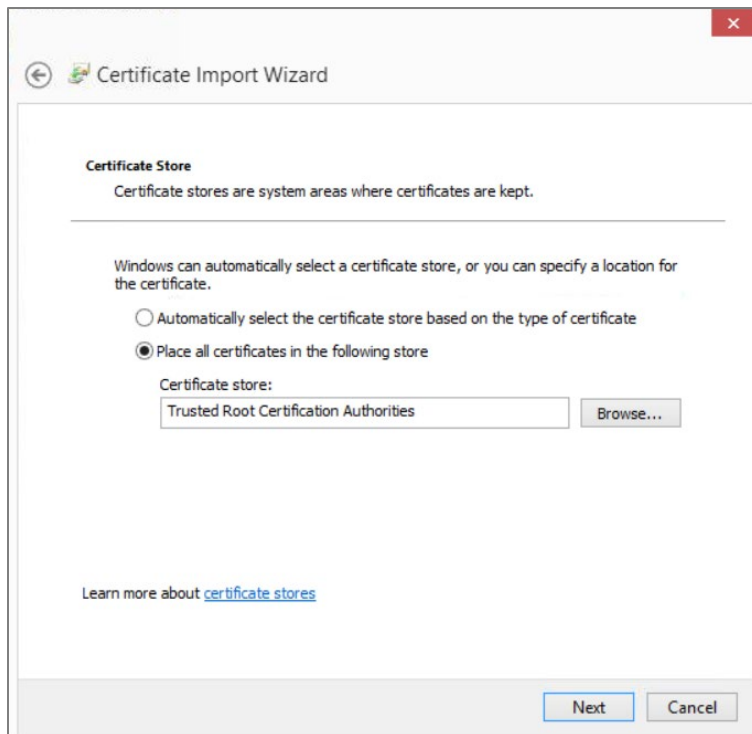
5. Click **Browse** and select the Certificate that was copied over in the beginning of this process.



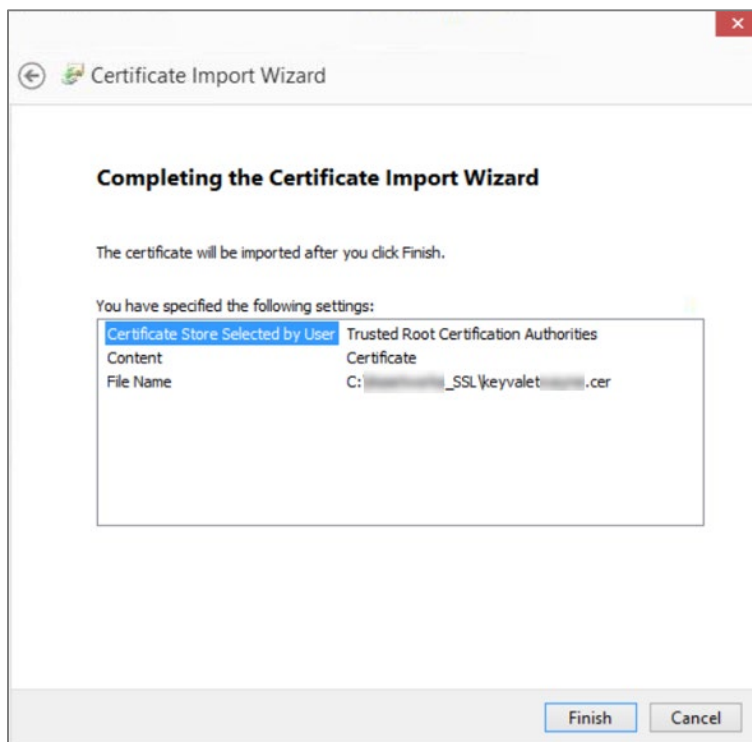
6. Click **Next**.



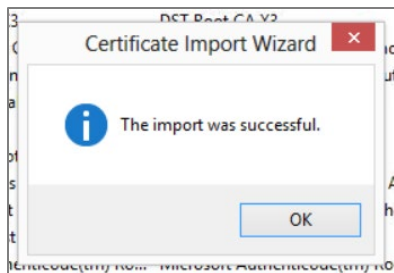
7. Set **Certificate Store:** to Trusted Root Certification Authorities (if it is not already) then click **Next**.



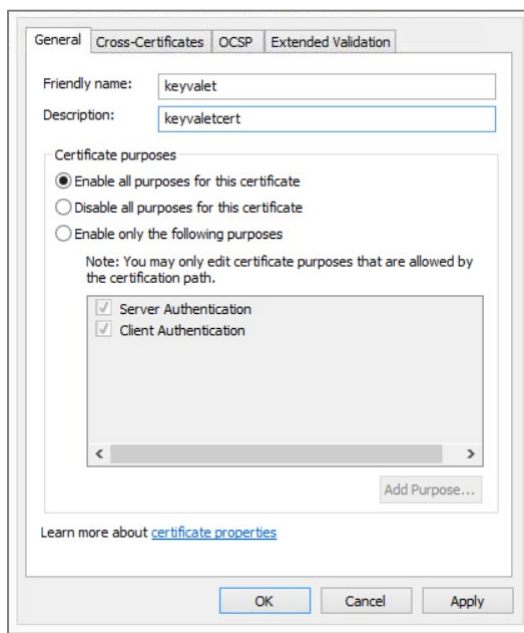
8. Click **Finish**.



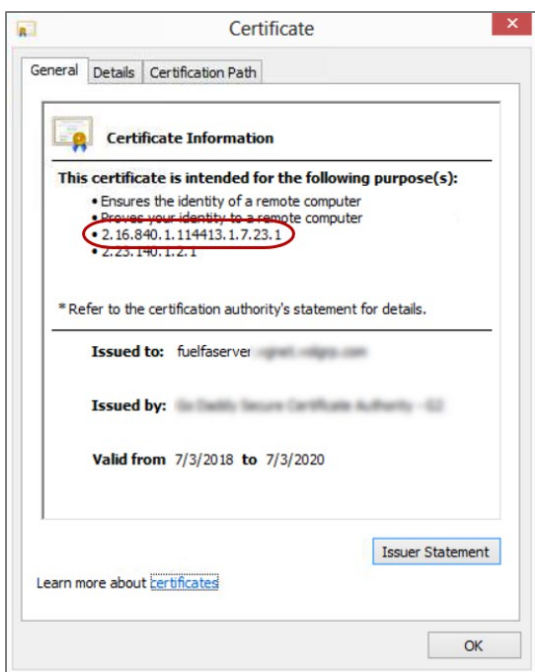
9. Click **OK** when the Certification Import Wizard complete message displays.

**To finish setting up the certificate:**

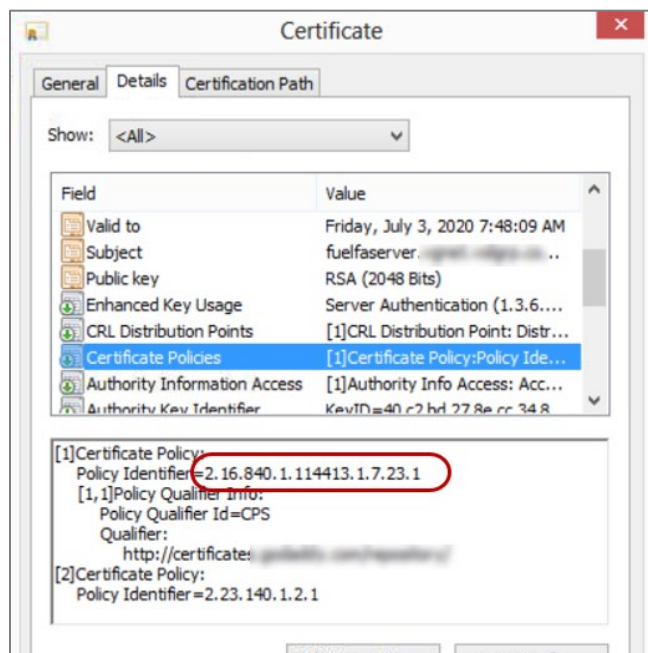
1. In the MMC application, in the Trusted Root Certification Authorities > Certificates area, right-click the certificate.
2. Click **Properties**.
3. Specify a friendly name and description for the certificate, then click **Apply**.



4. Click **OK**.
5. While still in MMC.exe, double-click the certificate.
6. Copy the first string of numbers.



- i. If there is no information or string of numbers on the General tab, click the Details tab.
- ii. Scroll down and click on Certificate Policies and copy the numbers after **[1]**
Certificate Policy: Policy Identifier =



7. Open a new notepad document and paste the numbers to notepad. These are needed for a later step.

Configure KeyBoxManager.exe.config for SSL

1. Download the [KeyBoxManagerSSL.exe.config](#) file.
2. Change the file extension from *KeyBoxManagerSSL.exe.config.txt* to *KeyBoxManagerSSL.exe.config*.
3. On the customer KeyValet, go to C:\Assetworks\keyvalet, change the existing *KeyBoxManager.exe.config* file name to *DefaultKeyBoxManager.exe.config*.
4. File transfer *KeyBoxManagerSSL.exe.config* to C:\Assetworks\keyvalet.
5. Change the *KeyBoxManagerkSSL.exe.config* file name to *KeyBoxManager.exe.config*.
6. Open the *KeyBoxManager.exe.config* file.
7. Fill in the Endpoint Address. This is the MAXQ Interface Services URL.

KeyBoxManager.exe.config

```
<?xml version="1.0"?>
<configuration>
  <system.serviceModel>
    <behaviors>
      <serviceBehaviors>
        <behavior>
          <serviceMetadata httpsGetEnabled="true" />
          <serviceDebug includeExceptionDetailInFaults="true" />
          <dataContractSerializer maxItemsInObjectGraph="2147483647" />
        </behavior>
      </serviceBehaviors>
    </behaviors>
    <bindings>
      <basicHttpsBinding>
        <binding name="InterfaceServicesSoap" maxBufferSize="65536"
          maxBufferPoolSize="524288" maxReceivedMessageSize="65536"
          messageEncoding="Text" textEncoding="utf-8"
          transferMode="Streamed">
          <readerQuotas maxDepth="32" maxStringContentLength="65536"
            maxArrayLength="16384" maxBytesPerRead="4096"
            maxNameTableCharCount="16384" />
        </binding>
      </basicHttpsBinding>
    </bindings>
    <client>
      <endpoint
        address="https://fuelserver.vgnet.volgrp.com/MAXQueueInterface/MAXQ
          ueue/InterfaceServices.asmx" binding="basicHttpsBinding"
        bindingConfiguration="InterfaceServicesSoap"
        contract="MAXQInterfaceServices.InterfaceServicesSoap"
        name="InterfaceServicesSoap" />
    </client>
  </system.serviceModel>
  <startup>
  </startup>
</configuration>
```

8. Save the file.

Configure KeyBoxKiosk.exe.config for SSL

1. Download the KeyBoxKioskSSL.exe.config file.
2. Change the file name extension from **KeyBoxKioskSSL.exe.config.txt** to **KeyBoxKioskSSL.exe.config**.
3. On the customer KeyValet, go to C:\Assetworks\keyvalet, change the existing **KeyBoxKiosk.exe.config** file name to **DefaultKeyBoxKiosk.exe.config**.
4. Move the **KeyBoxKioskSSL.exe.config** file to C:\Assetworks\keyvalet.
5. Change the **KeyBoxKioskSSL.exe.config** file name to **KeyBoxKiosk.exe.config**.
6. Open the **KeyBoxKiosk.exe.config** file.
7. If the KeyValet was set up prior to implementing SSL, the following values can be taken from the DefaultKeyBoxKiosk.exe.config file. If they have not, these will need to be obtained from the App Server from the Configurator
[hostname]\%Servername%\WebModules\Web\bin\Configurator.exe on the Database tab.
 - i. FASuite.App.ConnectionString
 - ii. FASuite.App.FAUser
 - iii. FASuite.App.FAPass
8. Fill in the MAXQueue Interface Services URL that includes HTTPS.
9. Fill in ClientCertificate findValue which is the string of numbers pasted to Notepad from the previous section.
10. Save the file.



Note: An example config file can be seen below.

KeyBoxKiosk.exe.config

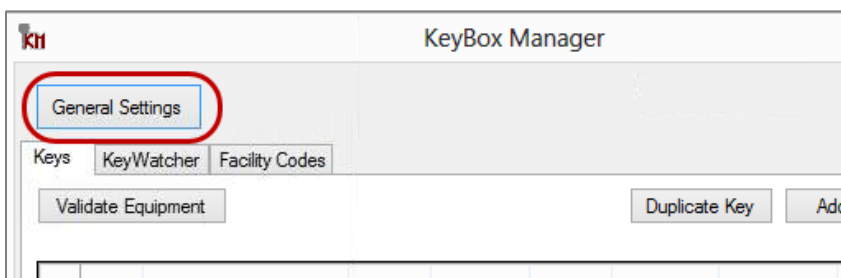
```

<?xml version="1.0"?>
<configuration>
  <configSections>
    <section name="KeyBoxSettings"
      type="KeyBoxCommander.Library.Common.KeyBoxSettings, KeyBoxCommander.Library" />
  </configSections>
  <appSettings>
    <add key="FASuite.App.ConnectionString" value="AppServerIP:Port" />
    <add key="FASuite.App.FAUser" value="MAXQUEUE" />
    <add key="FASuite.App.FAPass" value="maxqueue" />
    <add key="FASuite.FuelFocus.URL" value="" />
    <add key="SmartApps.M5User" value="smartapps" />
    <add key="SmartApps.URL" value="" />
    <add key="CreateServiceRequestURL" value="sr/vehicles/{0}/serviceRequests" />
    <add key="GetSymptomsURL" value="sr/vehicles/{0}/Source/{1}/symptoms" />
    <add key="GetRentalClassURL" value="rotf/rentalclasses" />
    <add key="ValidateCardURL" value="rotf/card/{0}/validate" />
    <add key="CreateReservationURL" value="rotf/reservations" />
    <add key="ClientSettingsProvider.ServiceUri" value="" />
    <add key="WPFTabletSupport" value="false" />
  </appSettings>
  <system.serviceModel>
    <behaviors>
      <endpointBehaviors>
        <behavior name="endpointCredentialBehavior">
          <clientCredentials>
            <clientCertificate findValue="CertificatePolicyNumbers"
              storeLocation="LocalMachine"
              storeName="Root" x509FindType="FindByCertificatePolicy" />
          </clientCredentials>
        </behavior>
      </endpointBehaviors>
    </behaviors>
    <bindings>
      <basicHttpsBinding>
        <binding name="Binding1">
          <security mode="Transport">
            <transport clientCredentialType="Certificate" />
          </security>
        </binding>
      </basicHttpsBinding>
    </bindings>
    <client>
      <endpoint address="MAXQUEUE INTERFACE SERVICES ASMX URL"
        behaviorConfiguration="endpointCredentialBehavior" binding="basicHttpsBinding"
        bindingConfiguration="Binding1"
        contract="MAXQInterfaceServices.InterfaceServicesSoap"
        name="InterfaceServicesSoap" />
    </client>
  </system.serviceModel>

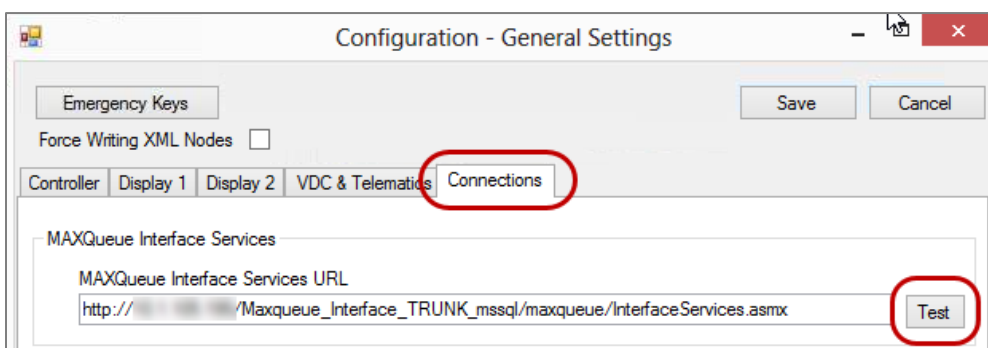
```

Verify Connectivity

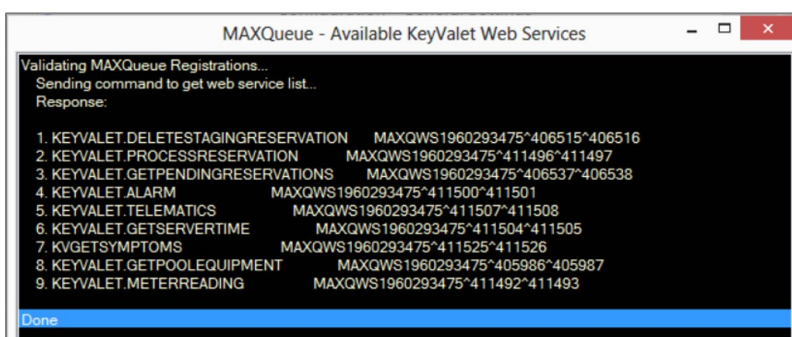
1. Launch the KeyBoxManager and click **General Settings**.



2. Click the Connections tab.
3. Click **Test**.



4. The system lists the running MAXQ Services.



5. Close KeyBoxManager.
6. Open KeyBoxKiosk.
7. Click the gear icon and enter the admin password.
8. Ensure the Online indicator is green (as shown below).

MinimizeRemove KeyReturn KeyRelease SlotShutdown

AlarmsClear Staging

Keys Found: 18

	Box	Key	Slot	Equip ID	Detected
1	1	1	1	17803	☒
2	1	2	2	17804	☒
3	1	3	3	17805	☒
4	1	4	4	17806	☒
5	1	5	5	21441	☒
6	1	6	6	21442	☒
7	1	7	7	21443	☒
8	1	8	8	21444	☒
9	1	9	9	35671	☒
10	1	10	10	35672	☒
11	1	11	11	35673	☒
12	1	12	12	35674	☒
13	1	13	13	44201	☒
14	1	14	14	44202	☒

OnlineRefreshClose

Appendix A. Additional Information

This appendix outlines additional notes, assumptions, and information to assist with installing and wiring the KeyValet unit.

A.1 Notes and Assumptions

1. All quotes are based on site being *KeyValet ready*. KeyValet ready means that all KeyValet system devices are mounted to the appropriate location. All conduits are connected between the VDC radio unit, KeyValet keybox, and controller unit. All wires are pulled and left disconnected at each end unless otherwise specified. See KeyValet Ready checklist below.
2. Permits, permit fees, and site as-built drawings are not included.
3. Subject to any applicable state or local sales tax.
4. Warranty is one year parts with telephone Help Desk support. Extended warranty plans are available for subsequent years. Warranty expires at 12 months from date of install or 15 months from date of shipment, whichever comes first.
5. Client must have a tested network connection at the Controller unit. This connection needs to be able to ping the FleetFocus server successfully. Delay of this connectivity could result in additional time being added to contract.

A.2 KeyValet Ready Checklist

The following represents a checklist of the items to complete in order to be KeyValet ready.

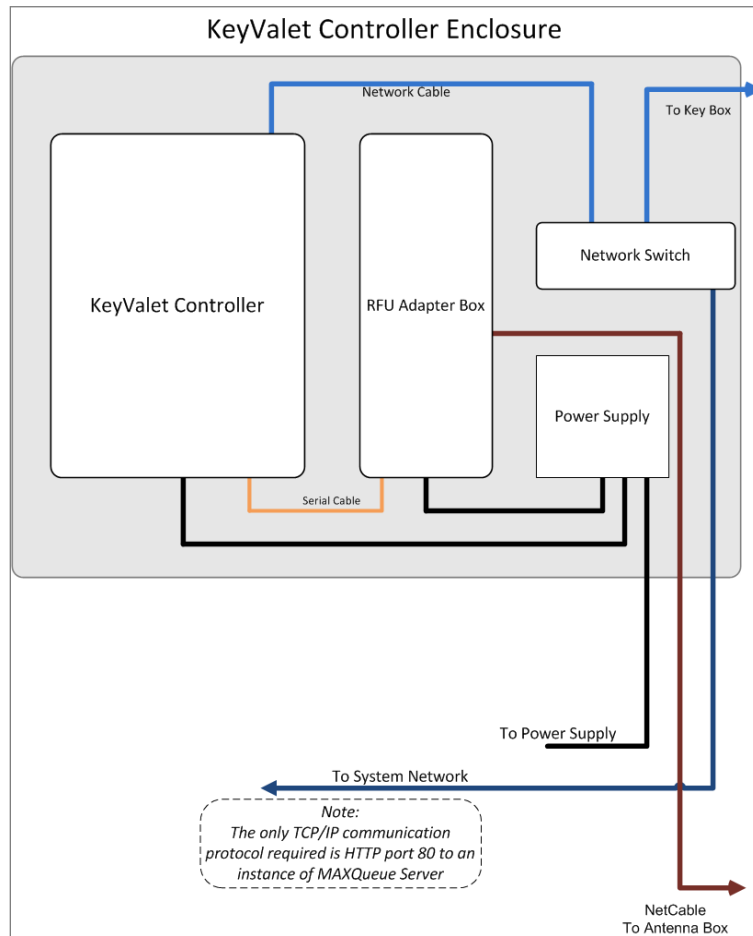
1. **Device installation:** The customer is responsible for mounting KeyValet devices to their property. Devices may include external National Electrical Manufacturers Association (NEMA) weatherproof box, key control box, and VDC antenna box, and connecting wires and conduit. The VDC antenna must be mounted centrally to reach all vehicles within a 333 foot radius. Conduit must be from nearest Controller enclosure to this point with wires installed.
2. **Conduit Requirements:** An electrician should run a conduit from the VDC System to Controller units as needed. Electrical requirements to each KeyValet Controller are as follows:
 - A network cable must be run from the VDC unit to the Controller unit's Radio Frequency Unit (RFU) adapter. Network cable to be terminated with RJ45 adapters 8 pin per wire chart diagram. A single 14AWG THHN green wire for grounding purposes at the nearest grounding connection. Wire run is limited to 3,000 feet.
 - Provide a grounded 110v outlet for the location that the KeyValet unit will be mounted. The KeyValet unit can be hard wired and this wiring is the client responsibility.
 - Provide a grounded 110v outlet for the controller unit. If the controller unit is connected to the KeyValet enclosure, then both will share the same outlet or circuit.
 - We will need either of the following:
 - A second conduit from the KeyValet to the controller unit
 - The KeyValet controller unit mounted in an enclosure next to the KeyValet enclosure.
 - Call to schedule a date for final terminations when all of the items are complete.



All wiring and conduits described above are required for KeyValet system control only. This document assumes the VIB installation any vehicle is covered under a separate installation manual.

A.3 Site Layout Diagram

Following is a diagram depicting the software and hardware package with a connection to the customers' network and the VDC antenna.

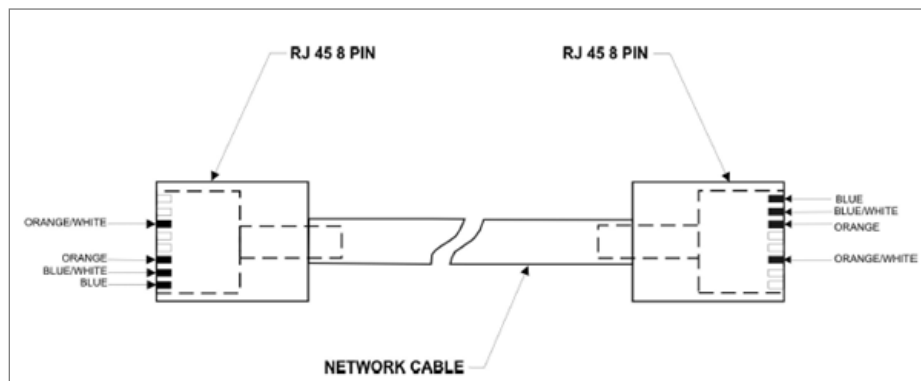


Patent Pending©

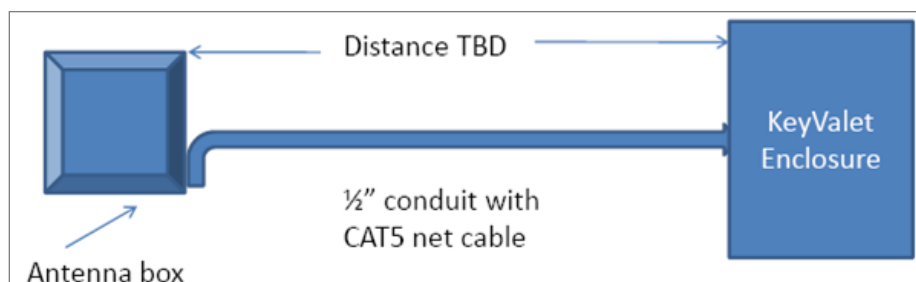
A.4 Antenna Diagrams for Wiring to KeyValet Controller

This section provides diagrams to assist with wiring to the KeyValet Controller.

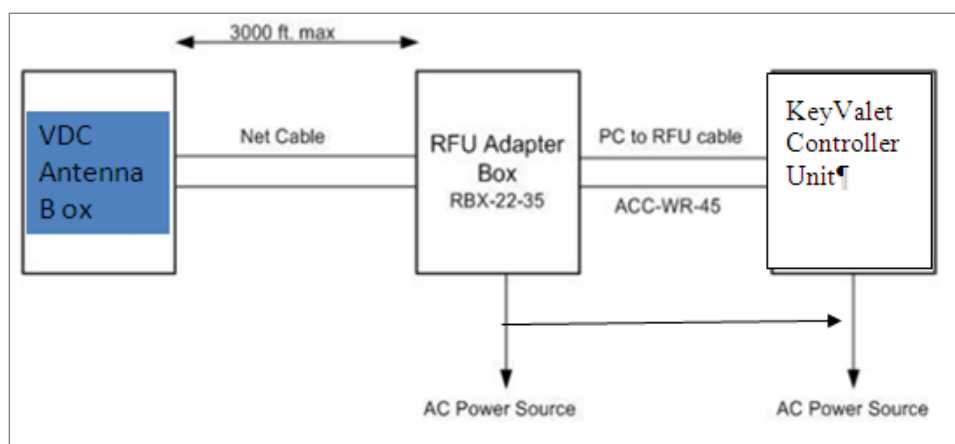
Prepare the Net Cable for the required distance (3,000 feet max.) for connecting the RFU adapter to the PC as described in the following diagram.



Net Cable Preparation



Mounting Antenna Diagram



VDC System Connection Diagram

Location Criteria

Location criteria include the following:

- The VDC Antenna Set Box can be located at any place at distance of 3000 ft. max from Controller and RFU adapter.
- The Controller and the RFU adapter can be located at any office or under a roofed place nearby the parking area or Office entrance and connected to the VDC Antenna Box by using a Net Cable.

System Components

VDC System connection diagram: VDC antenna is connected by serial cable to RFU adapter. VDC antenna operates at 900-915 MHZ radio to read the VIB devices installed on the vehicles. VIB device installation for the vehicles is covered in a separate document.

Vehicle List

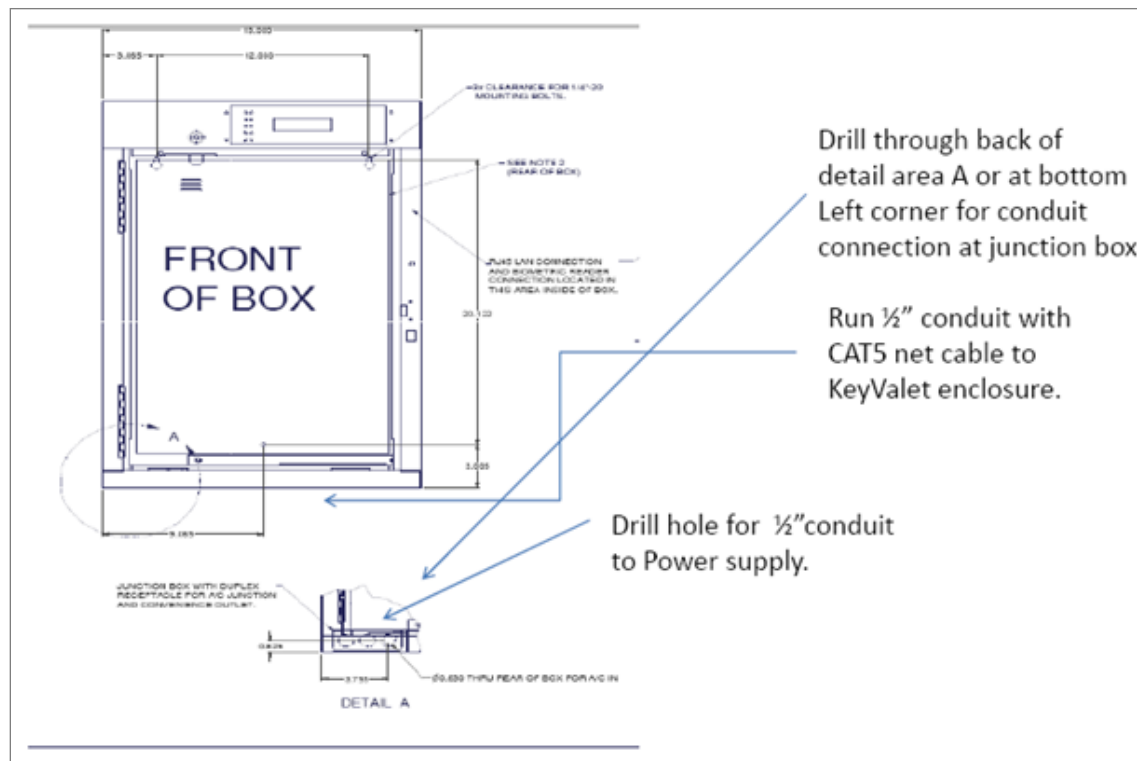
Please provide a list of vehicles to determine VIB hardware ordering. The vehicle list must include the Year, Make, Model, and VIN in an Excel spreadsheet. Include any vehicles on order as well if required.

A.5 Keybox Diagrams

This section provides several keybox diagrams.

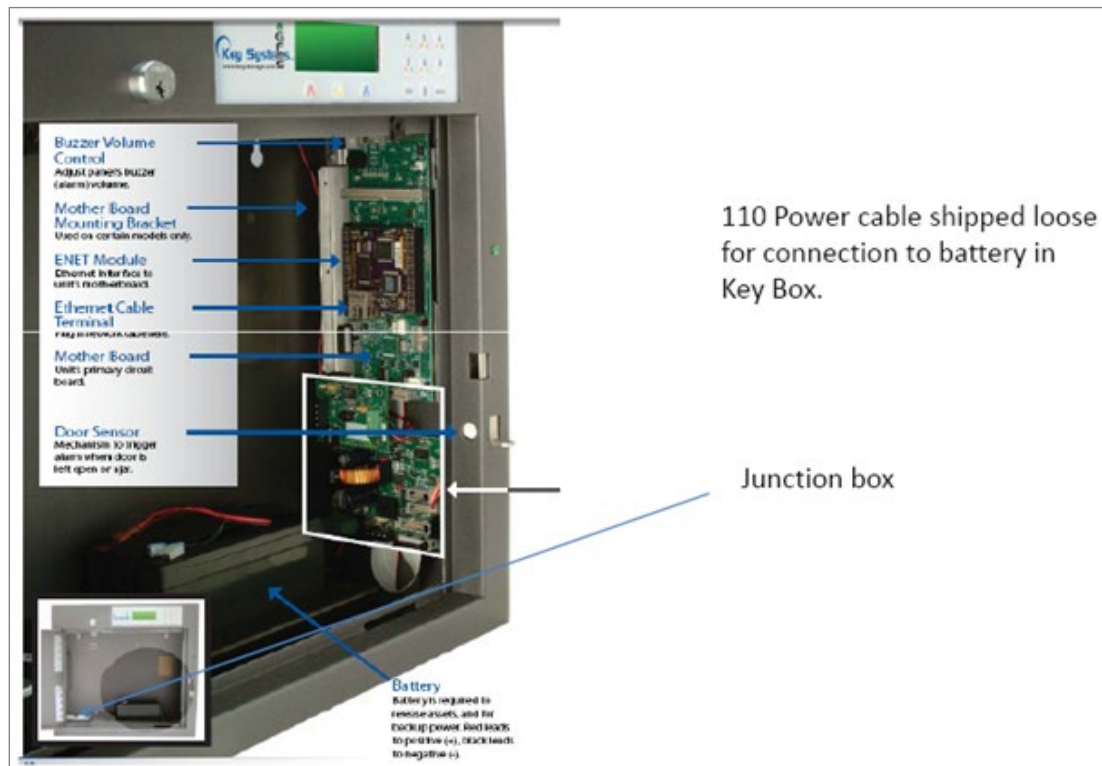
Keybox Mounting Diagram

The following is a diagram to help with mounting the Keybox:



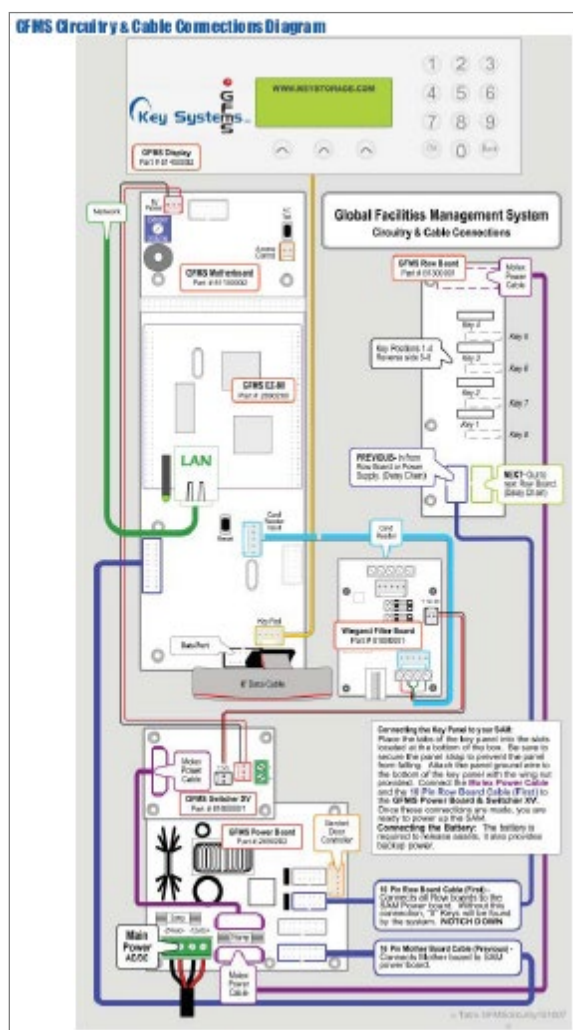
KeyBox Power Box

The following diagram provides an overview of the Keybox power box.



Circuitry and Cable Connections

The following diagram represents circuitry and cable connections.

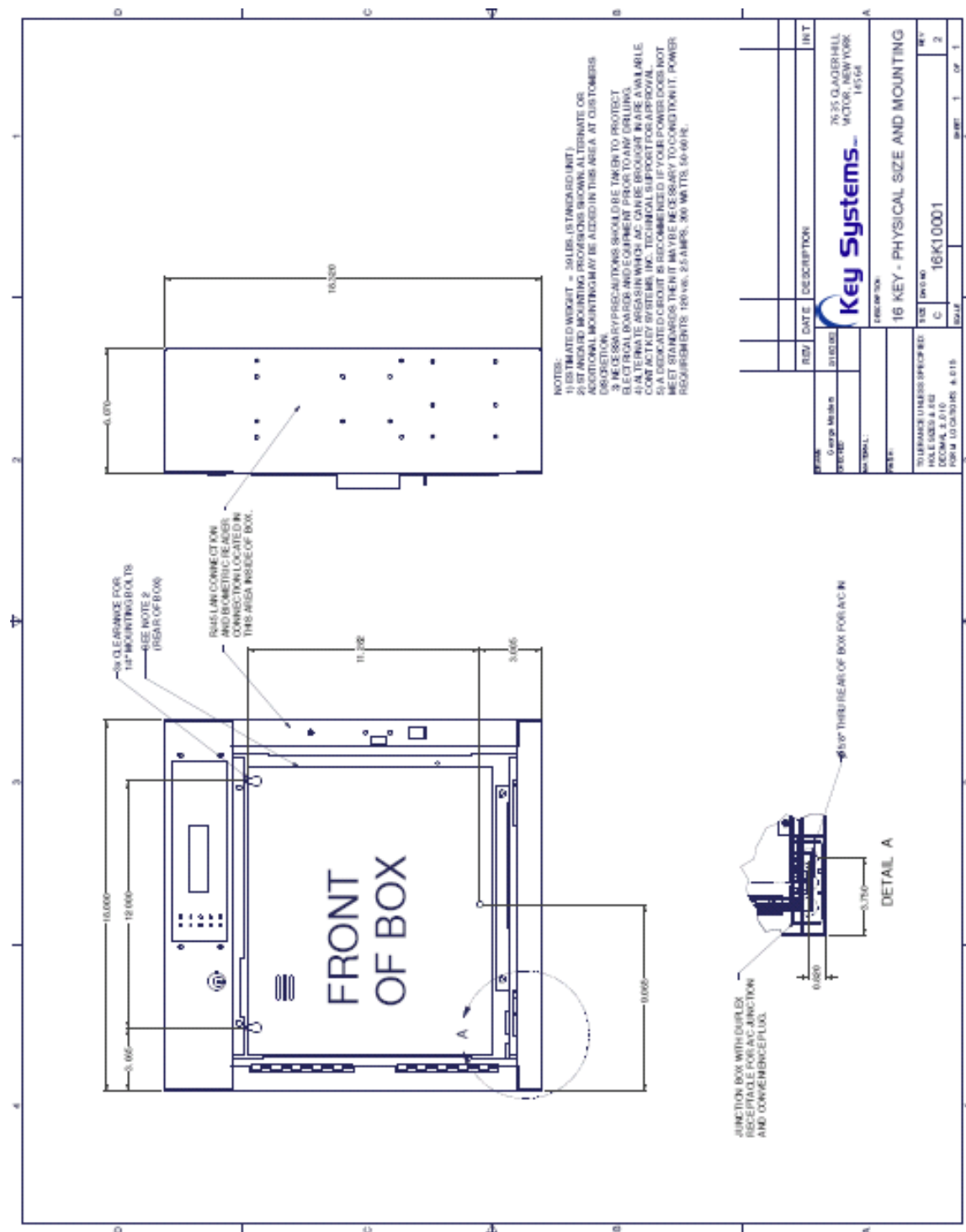


Mount the Keybox facing away from direct sunlight to avoid glare on the stainless steel internal key panel.

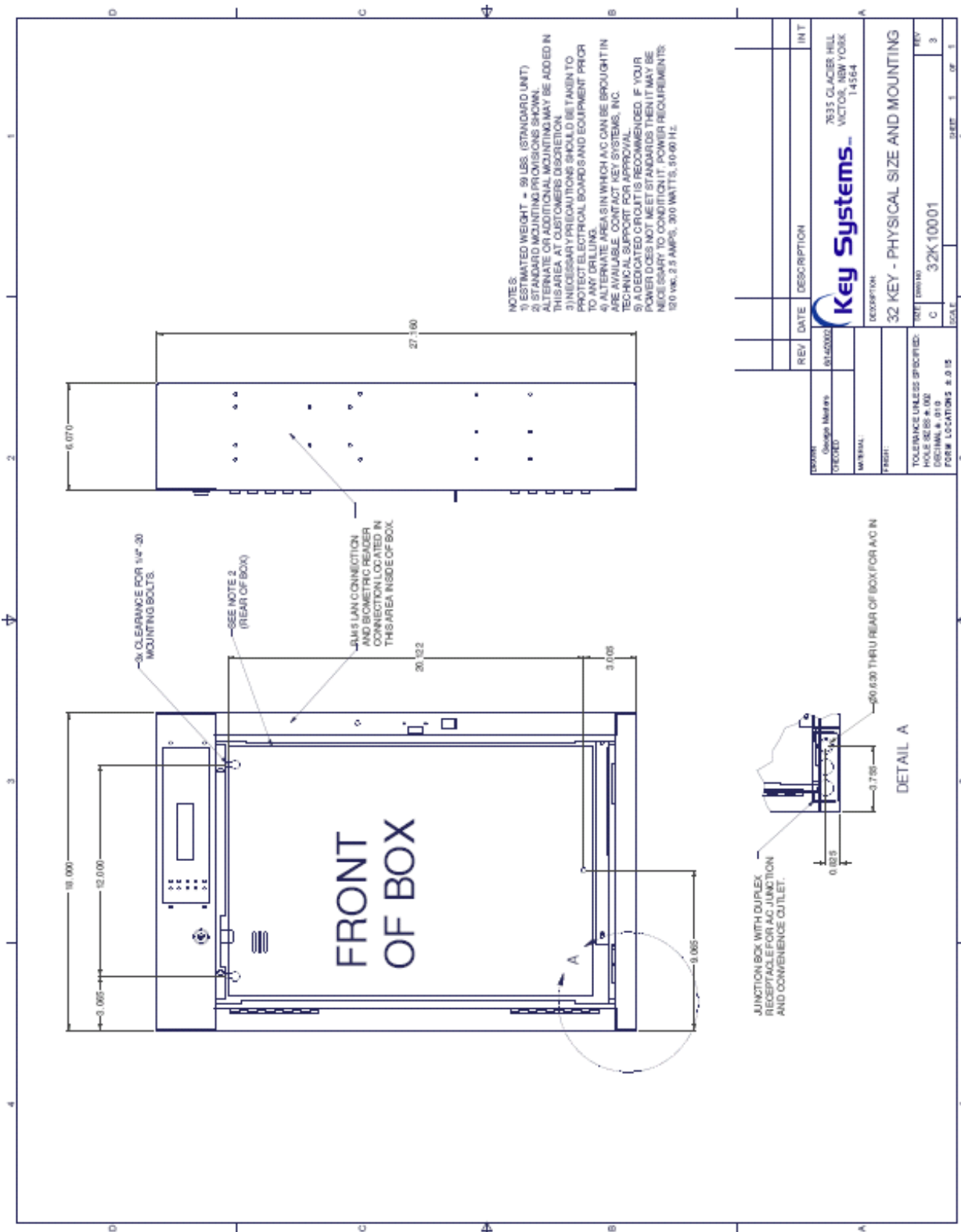
Keybox Schematics for Various Keybox Sizes

Following are diagrams representing keybox schematics for keyboxes varying from 16-96 keys.

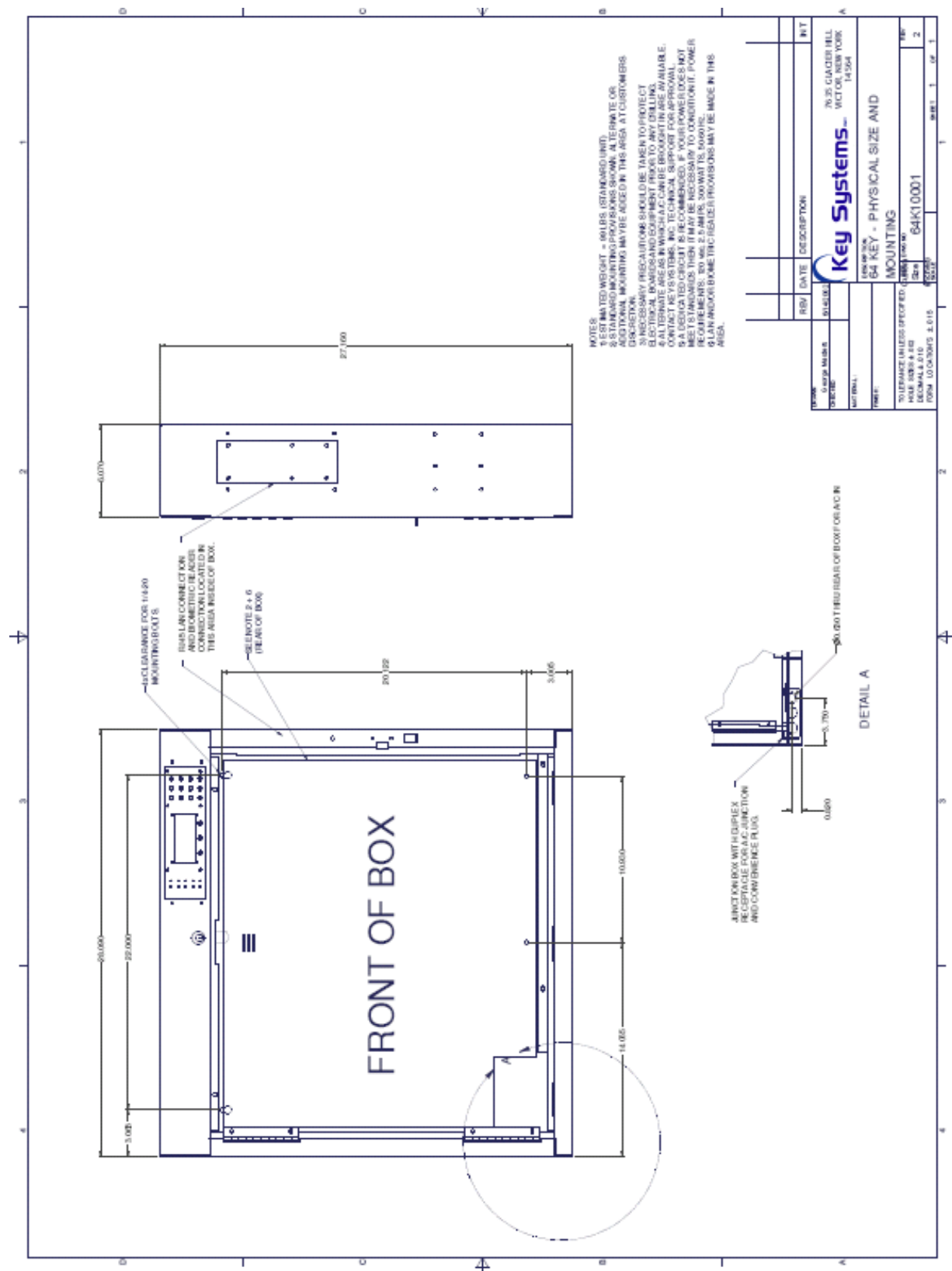
16 Keys



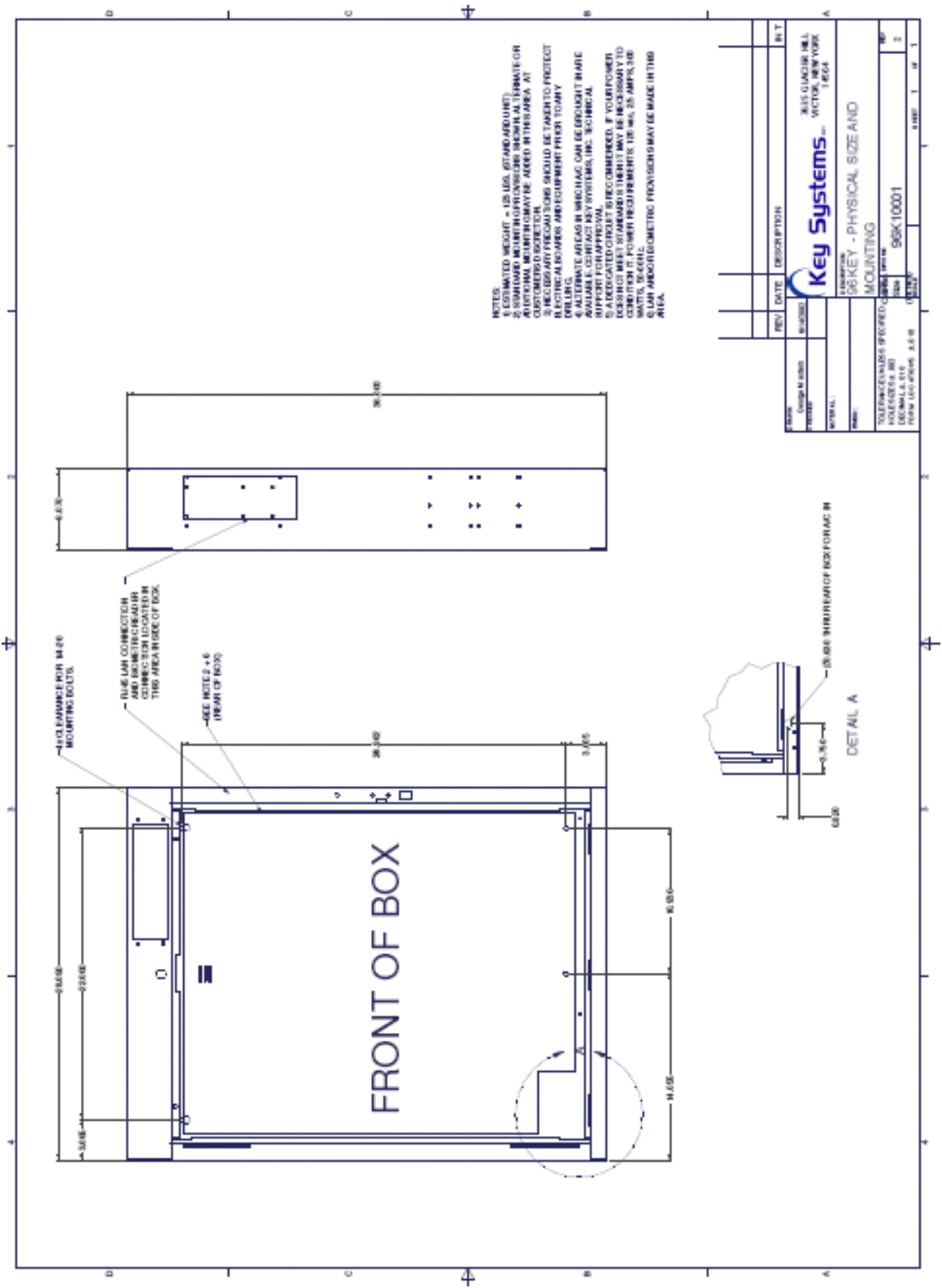
32 Keys



64 Keys



96 Keys



A.6 Module Config

MAXQueueDesigner Settings Tab

These are shared settings and may already be configured

Variable	Value
vars.MPUserId	[Enter FA UserId]
vars.MPUserPass	[Enter FA User Password]
vars.KeyValetServerURL	http://localhost/[Enter Web Instance Name]
vars.KeyValetAlarmUserId	[Enter FA UserId to receive alerts]
vars.KeyValetNetworkFleet	[Enter true or false] -if true MAXQueue Interface: Network Fleet must be installed
vars.ODBCName	[Enter Valid FA ODBC System Data Source Name(DSN)]
vars.ODBCUser	[Enter Valid FA ODBC System Data User ID]
vars.ODBCPassword	[Enter Valid FA ODBC System Data Password]

Services to enable

- KeyValet - Alarm
- KeyValet - GetPoolEquipment
- KeyValet - GetReservations
- KeyValet - GetServerTime
- KeyValet - MeterReading
- KeyValet - ProcessReservations
- KeyValet - Telematics (only required if Telematics are enabled)
- KeyValet - DeleteStaged (FA only)
- KeyValet - CreateServiceRequest (FA only - only required if Service Request screen is enabled)
- KeyValet - GetSymptoms (FA only - only required if Service Request screen is enabled)
- KeyValet - SaveStaging (FA only)
- KeyValet - AddReservationNote (FA only)
- Notification - Rules

Data Events enabled

- AWResrvRequestUpdate
- AWResrvRequestInsert



Note: KeyValet - SaveStaging service has a Data Event Custom trigger action for Delete. This is applicable for MAXQueue v15.0 and forward. Previous versions of MAXQueue will need to define the AWResrvRequestDelete data event.

Module Dependencies

- MAXQueue.KeyValet.dll (GetReservations,Telematics services)
- FuelFocusSecurity.dll (Authentication between controller and server)

Services to configure

MAXQueueDesigner - Services: KeyValet - GetPoolEquipment

Adapter: GetFilter

Create/Edit XML - Options to prompt for odometer reading on the key box when motor pool equipment are returned. Configures a list of meter 1 types which are to be included in prompt for odometer. If the equipment unit's meter 1 type is not found in the colon ';' delimited list the key box will not prompt for odometer reading even if the vars.PromptOdometer value has been set to "true".

Node	Value
vars.ValidMeter1Types	"[colon delimited list of meter 1 types to be included in prompt for odometer option]"
vars.PoolLocationID	DO NOT CHANGE
vars.EquipmentID	DO NOT CHANGE
vars.KeyValetNetworkFleet	[true or false]
vars.NWFUserId	[only needed if NWF enabled]
vars.NWFUserPass	[only needed if NWF enabled]

MAXQueueDesigner - Services: KeyValet - GetSymptoms

Node	Value
vars.ReportingSource	[FA reporting Source]

A.7 KeyValet Upgrade

Packaged folders

Folder	Description
Controller	New KeyValet assembly files for controller
Doc	KeyValet configuration variables and services to enable
Server/Packages	MAXQueue KeyValet service package

Steps to perform KeyValet upgrade

Remote desktop in the Keyvalet Controller.

1. To shut down the KeyValet Controller console application, press and hold **ALT** and press **Q**.
2. Copy all assembly files from installer package \Controller folder into *C:\AssetWorks\FASuite\KeyValet*.
3. Validate the configuration file exists in *C:\Assetworks\FASuite\KeyValet\KeyBoxKiosk.exe.config*. If it does not, copy the configuration file from the \KeyValet\ConfigFiles\KeyBoxKiosk.exe.config into the *KeyValet* folder. Change <endpoint address="[your internet address for KeyValet Service in MAXQueue]" xml node.

Access KeyValetServices in MAXQueue Designer

1. Use the **Remove** service action to remove all existing KeyValetServices in the MAXQueue Designer.
 - i. Remove KeyValet - GetPoolEquipment service
 - ii. Remove KeyValet - GetReservations service
 - iii. Remove KeyValet - MeterReading service
 - iv. Remove KeyValet - ProcessReservation service
 - v. Remove KeyValet - Update Reserv service
 - vi. Remove KeyValet - DeleteStaged service (if exists and FA installation)
 - vii. Remove KeyValet - GetSymptoms service (if exists and FA installation)

- viii. Remove KeyValet - SaveStaging service (if exists and FA installation)
2. Perform the Config Action - Force Publish in MAXQueue Designer.
 3. After the KeyValetService MAXQueue service has finished restarting and has a new instance, copy the new KeyValet server package from `\Server\Packages\KeyValetServices.xml` into the `MAXQueue\Server\Packages` directory on the MAXQueue server.
 4. Stop the MAXQueue service and IIS.
 5. Start IIS and the MAXQueue service.
 6. After the KeyValetService MAXQueue service has finished consuming the new service (reading and receiving all data), refresh the browser.
 7. Ensure all the following KeyValetServices are found in MAXQueue Designer:
 - KeyValet - Alarm
 - KeyValet - KeyValet - GetPoolEquipment
 - KeyValet - GetReservations
 - KeyValet - GetServerTime
 - KeyValet - MeterReading
 - KeyValet - ProcessReservation
 - KeyValet - DeleteStaged service (FA only)
 - KeyValet - GetSymptoms service (FA only)
 - KeyValet - SaveStaging service (FA only)
 - Notification - Rules
 8. Add the following variables to the Settings tab in MAXQueue designer:

Variable	Value
vars.MPUserId	[Enter FA UserId]
vars.MPUserPass	[Enter FA User Password]
vars.KeyValetServerURL	[Enter Web Instance Name] (example: http://localhost/MAXQueue)
vars.KeyValetAlarmUserId	[Enter FA UserId to receive alerts]

9. Ensure all services in step 7 are enabled except the KeyValet - Alarm service (this should only be enabled for FA installations).
10. Perform the Config Action - Force Publish in MAXQueue Designer.

To complete the system start:

1. In remote desktop for Keyvalet Controller, start the KeyValet Controller console application

The update is completed.