Introduction to Doors.WEB™

This reference guide introduces you to Keri Systems new Doors.WEB™ web client. It explains the main features, functions and operation of the web client, plus pre-requisites for installation and the installation procedure itself. It can be very conveniently used on any device that has a web browser (PC, tablet or smart phone) and it can operate over the internet or via a Local Area Network.

Installation takes just a few minutes and you will find it very easy to setup and use. It provides you with the most commonly-used access control functions, such as adding, editing and removing cardholders (and credentials), or locking and unlocking any or all doors in your system and monitoring system events as they occur in real-time.

Doors.WEB User Manual

Keri Systems is a world leader and innovator in facility access and security systems, including proximity access control, telephone entry systems, video surveillance and proximity readers. Doors.WEB™ is designed for use with the Doors.NET access control system. It features an extremely easy to use and simplified user interface, allowing you to carry out a number of common administrative tasks. Doors.WEB™ can be seamlessly combined with the standard Doors.NET software (subject to Doors.WEB™ being enabled on your license key.

Obtaining the Installation File

Doors.WEB™ installation is performed on the Doors.NET Application Server PC using an installation file that is either downloaded from the www.kerisys.com website, or it can be found on the Doors.NET installation DVD. Installation is a very quick and easy process and should take no longer than 10 minutes to complete.

Host PC Requirements

There are certain settings and hardware requirements that must be in place prior to installing Doors.WEB™.

Dependencies
• Doors.NET Version 3.5.22
• Microsoft .NET 4.5 Framework
• Microsoft Internet Information Services 8 (IIS8)

Recommendations
• Windows 10 or Server 2012
• Doors.Net App Server and IIS8 serving the Doors.WEB™ client pages should be on the same machine.

Computer/Server Requirements (for the Doors.NET host PC)

- Microprocessor - Intel Core2 Duo, 2.4 GHz or greater, 8 MB cache or greater.
- Memory - 4 GB or greater.
- Operating System Compatibility:

  - Windows 8
  - Windows 8.1
  - Windows 10
  - Server 2012

- Hard Drive - 500 GB or greater.

The Database
Doors.NET software uses Microsoft SQL Server, SQL Express or higher. Before setting up Doors.WEB™ you should verify that the standard Doors.NET installation is at the latest version (v3.5.1.22) at time of writing.

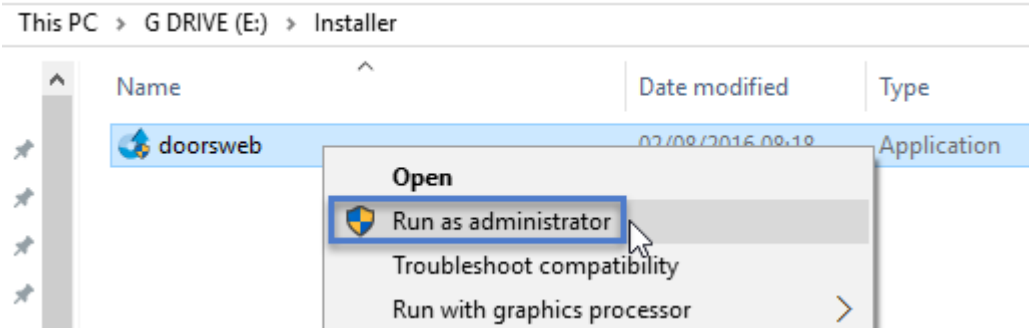
IMPORTANT NOTE
It is important to note that when you log into Doors.WEB™ you are automatically granted full administrative privileges. You will be able to add, edit and delete cardholders and you will be able to lock and unlock all doors on the system.

In standard Doors.NET you can setup system operators who can be prevented from carrying out certain administrative tasks. For example, they may be prevented from accessing cardholders, or hardware. Currently, this is not possible with Doors.WEB.

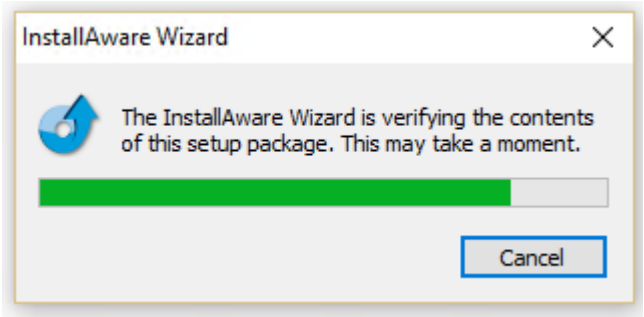
It is therefore important that you change the default administrator password to prevent any unauthorized access to your system.
Click here for a guide to changing the administrator's account details.

Installation Procedure

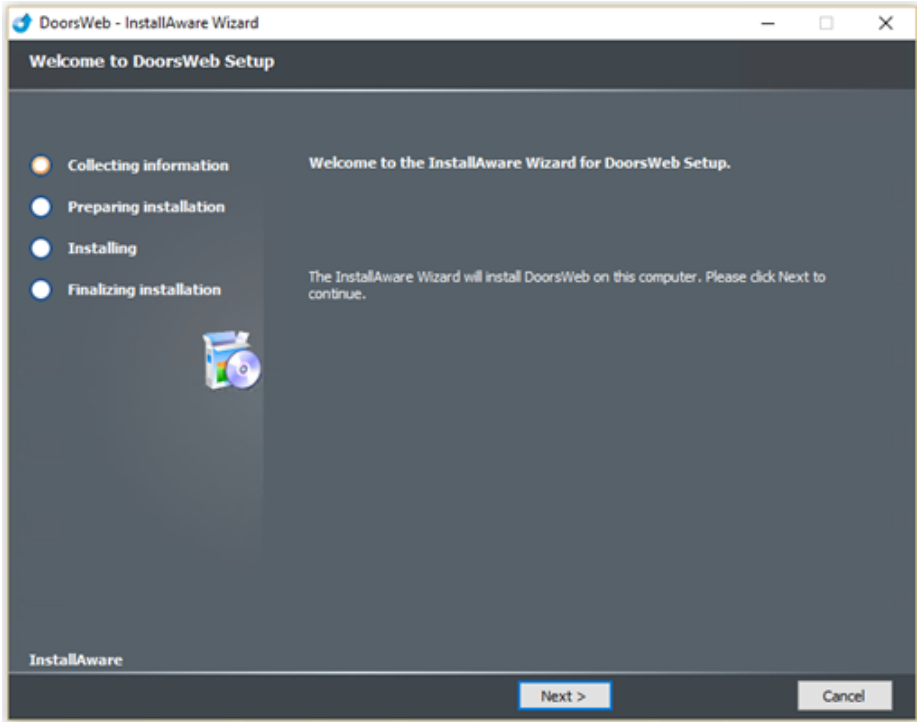
1. Copy across, or download the Doors.WEB™ installation file onto the Doors.NET host PC.
2. Right-click the installation executable and select 'Run as administrator'.



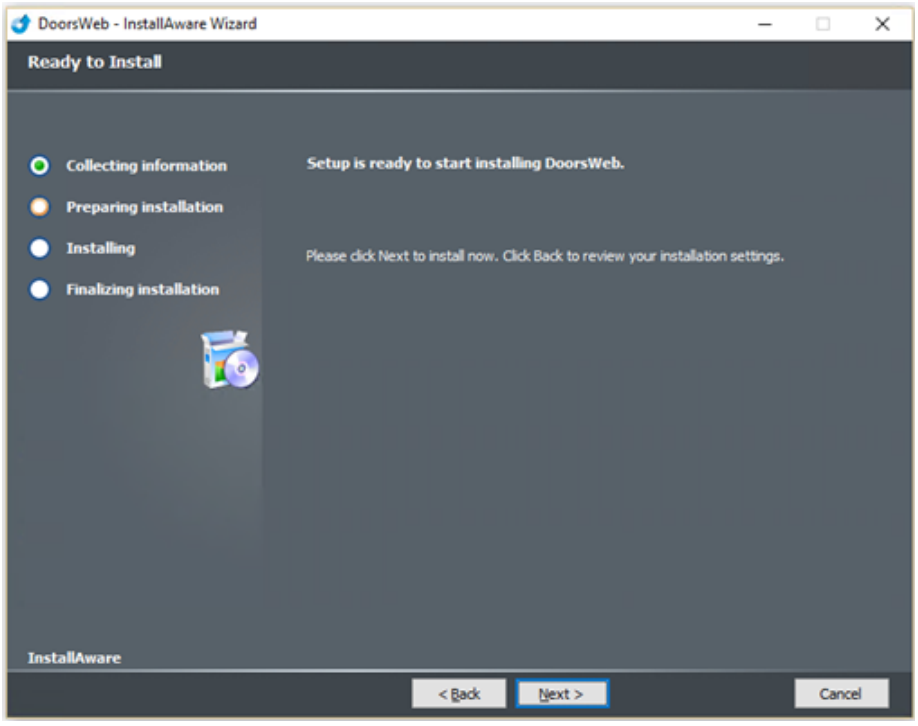
3. The installation wizard will initialize.



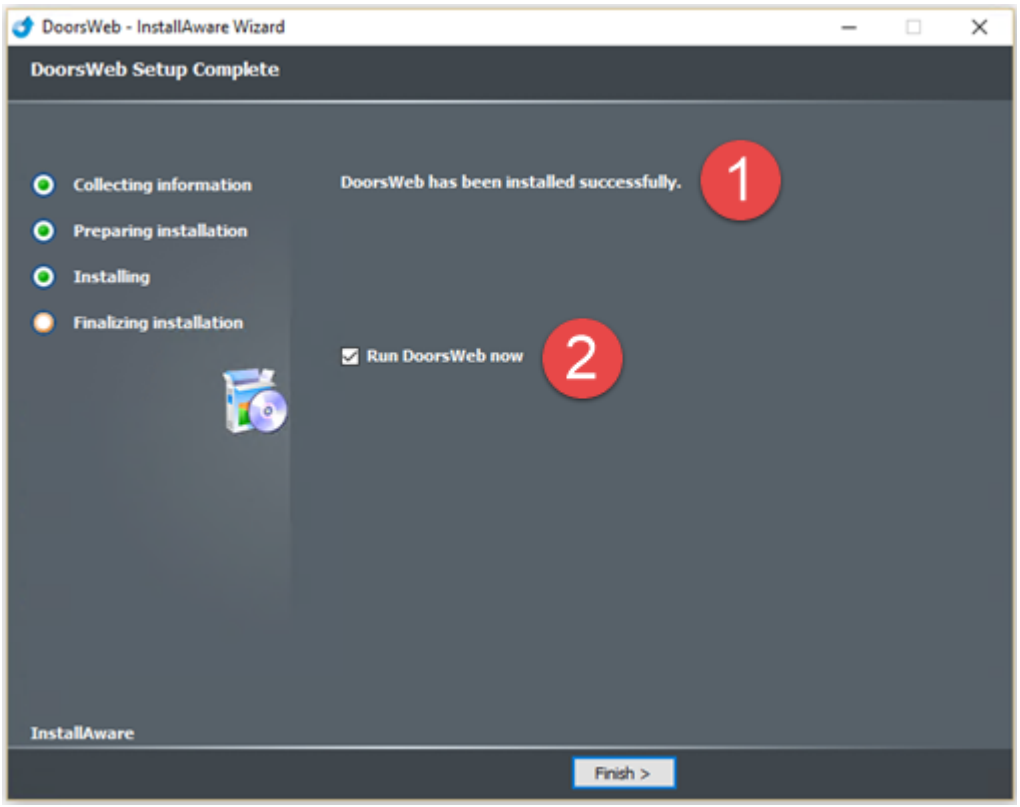
4. Click NEXT on the welcome screen.



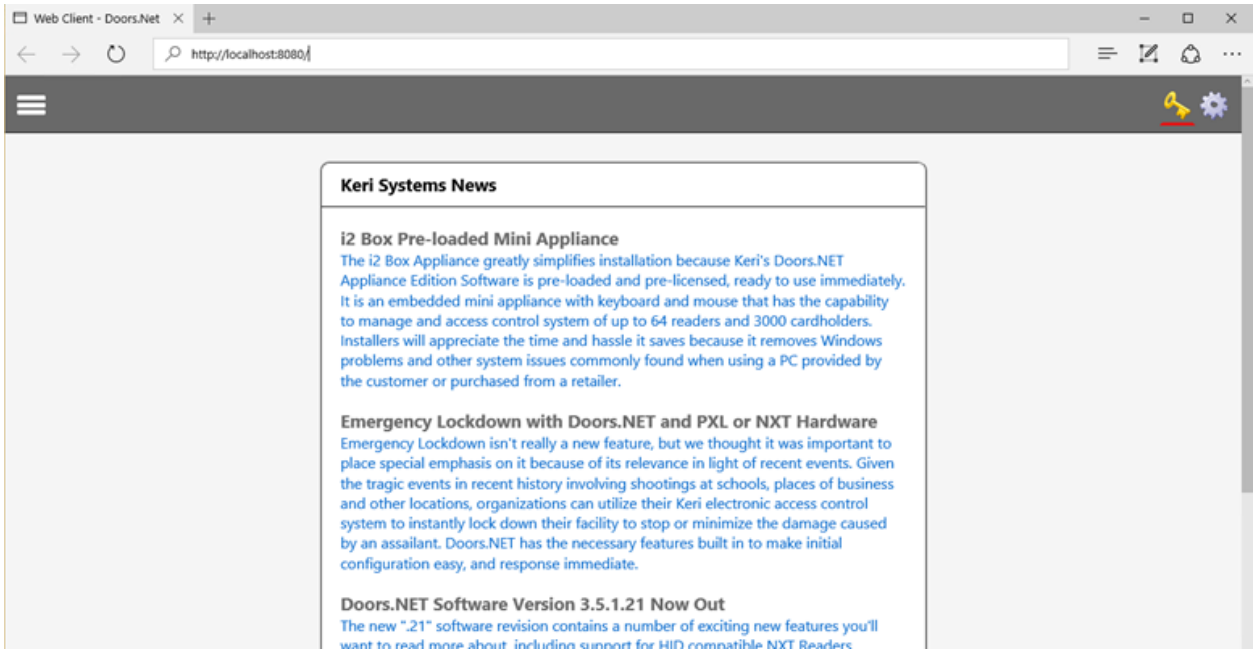
5. Click NEXT on the Ready to Install screen.



6. Installation will begin. Doors.WEB™ uses Internet Information Services and so the installer will automatically enable IIS if it is off. It will then install the various required IIS tools, features, services and settings.
7. Installation should take no longer than a few minutes.
8. Once installation is complete you should see that Doors.WEB™ has been installed successfully (1) and you will be prompted to run the client (2).



9. Leave **Run Doors.WEB™ now** selected and click FINISH.
10. A browser window will open and the URL will be localhost:8080.
11. You should see the Doors.WEB™ home page.



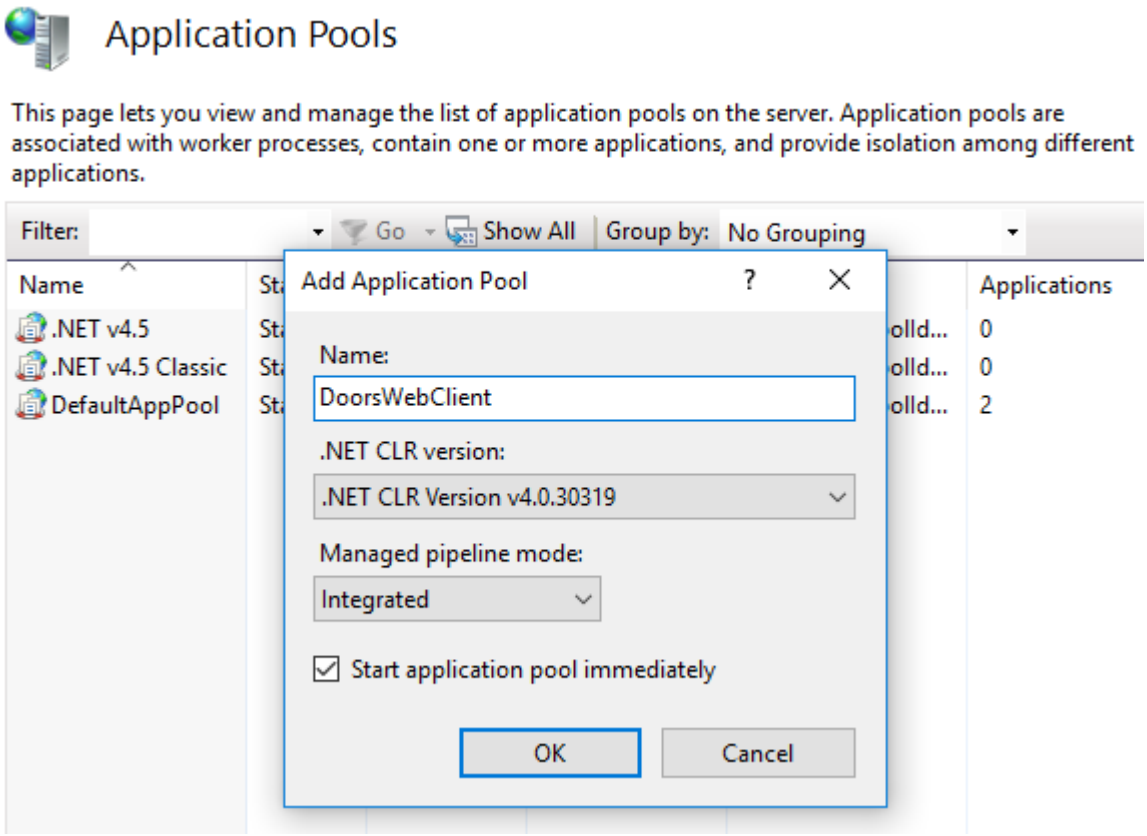
12. Any other workstation which can communicate to the host PC will now also be able to access the web client via a browser (using the host workstation's IP address and port 8080).
13. The Doors.WEB™ client is a licensed feature and therefore is not included with the standard Doors.NET bundle. See the link below for licensing information:

    Doors.WEB™ Licensing

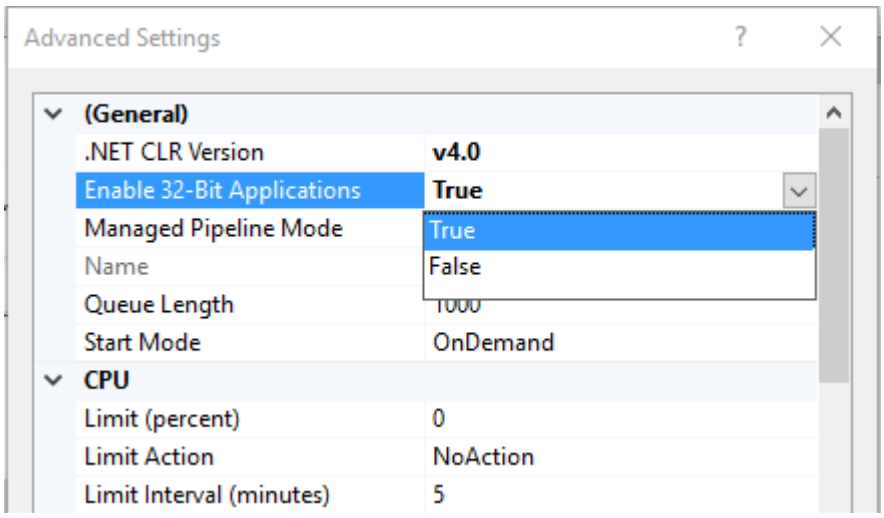
Create Application Pool

The following only needs to be done if the host PC/Server is running another web application and using the **DefaultAppPool** - It is an unlikely scenario but the scenario may arise.

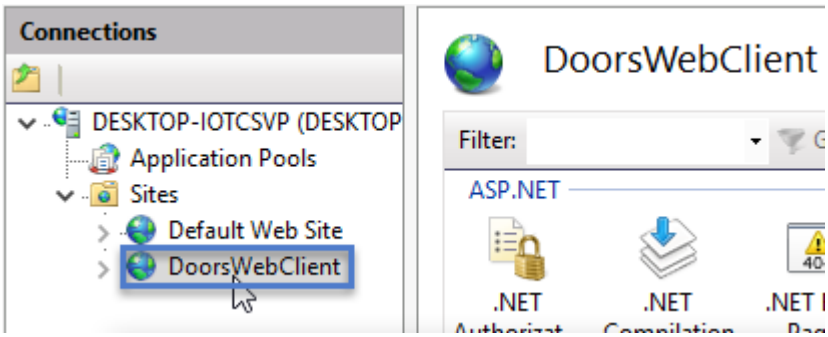
1. Open Internet Information Services/IIS (on a Windows 10 PC type IIS into Cortana)
2. Internet Information Services (IIS) Manager window will open.
3. Right-click on Application Pool >> select Add Application Pool > set the name to DoorsWebClient > press OK.



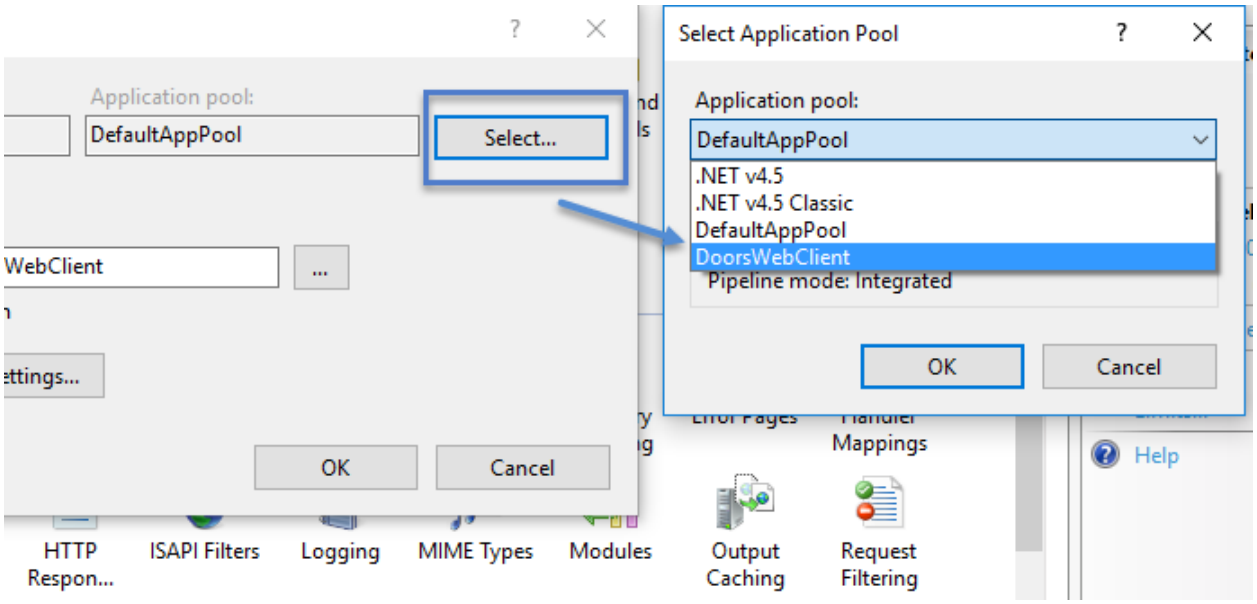
4. Right-click the newly created DoorsWebClient application pool > select Advanced settings > set enable 32-bit Applications: true > press OK.



5. You will see the Connections tree located on the left of the page.
6. From the Sites list, right-click on **DoorsWebClient.**



7. Select Basic Settings.
8. Click the **Select** button, then select the **DoorsWebClient** as the target Application Pool.



9. Close IIS Manager.

Using Secure Sockets Layers

It is very likely that you would want to protect their Doors.WEB™ client connections in the same way that is used when connecting to a bank's website (for online banking). This section of the help will guide you through the process of enabling Self-Signed Certificates and then using the certificate to create a Secure Socket Layer (SSL) connection to the Doors.WEB™ Server).

The process is the same as certificates issued by a Certification Authority, except you do not have to apply for the certificate and it does not have to be bound to a registered domain, such as myowndomain.com or kerisys.com

Important Information about Certified and Self-Signed Certificates

An SSL connection with a self-signed certificate creates an encrypted connection between the server and web browser to assure the information flowing in between can't be intercepted or interpreted by a 3rd party. A self-signed certificate does not guarantee the server is who they claim to be.

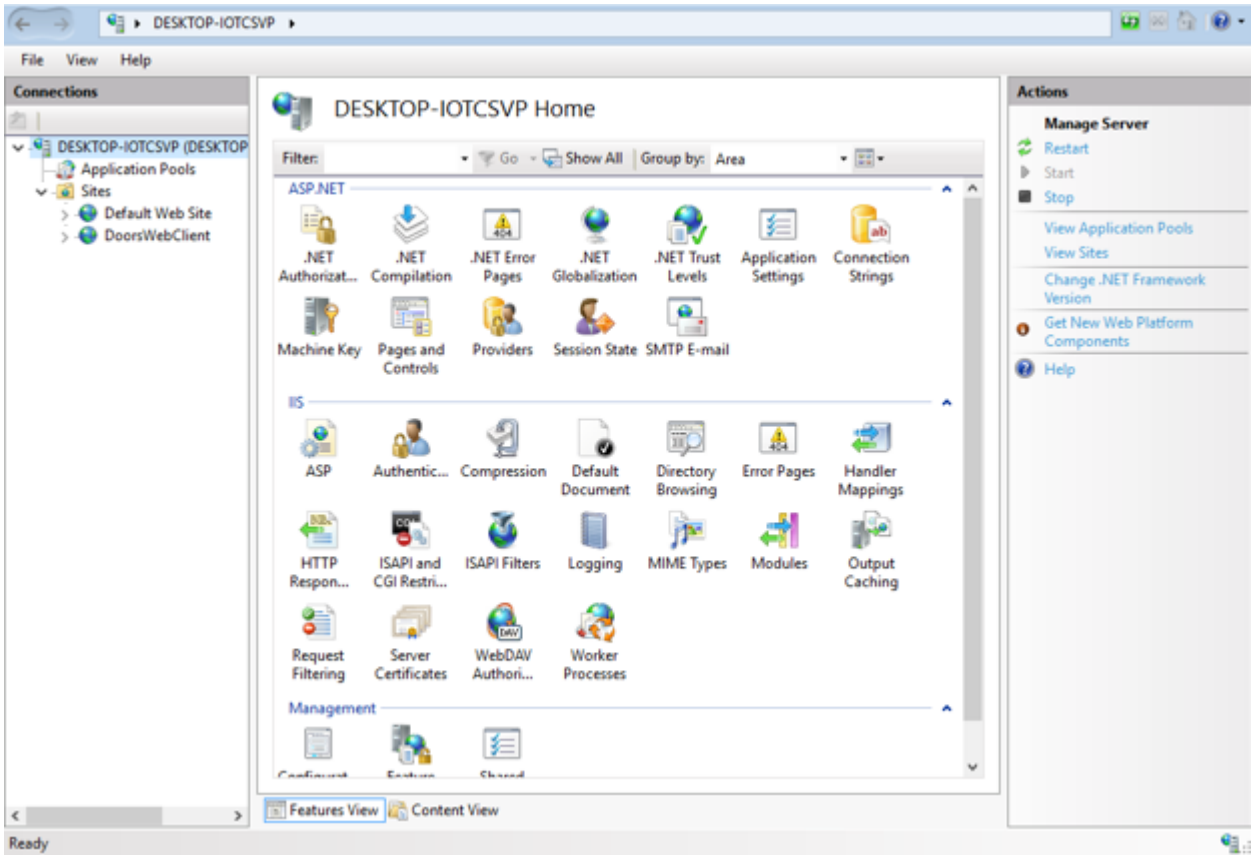
The highest level of security is achieved with a certificate provided from a 3rd party CA (Certification Authority) such as Digicert and GlobalSign. Certificates must be registered to a domain and require the domain owner to submit an application to the CA; however, this process is not covered in this document.

Requirements

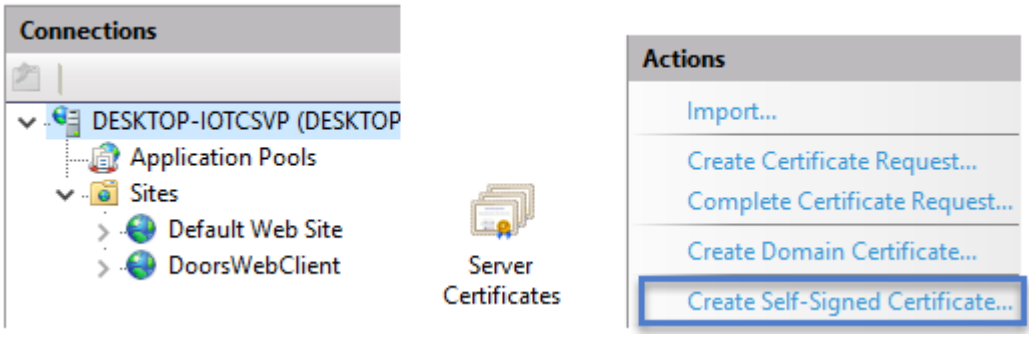
- An existing installation of IIS with Doors.WEB™ (DoorsWebClient) added as a site.
- IIS8 (Internet Information Services).
- Windows 10 operating system.

Setup SSL With Certificate

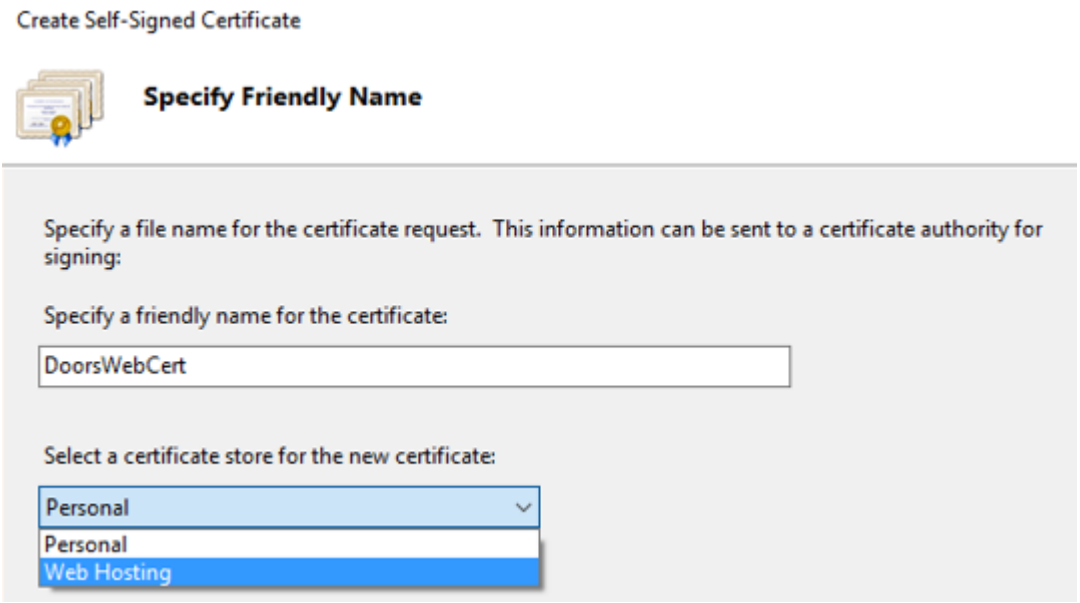
1. Open Internet Information Services (IIS) (Right-click Windows Start Menu >> Control Panel >> Administrative Tools >> Internet Information Services (IIS) Manager.



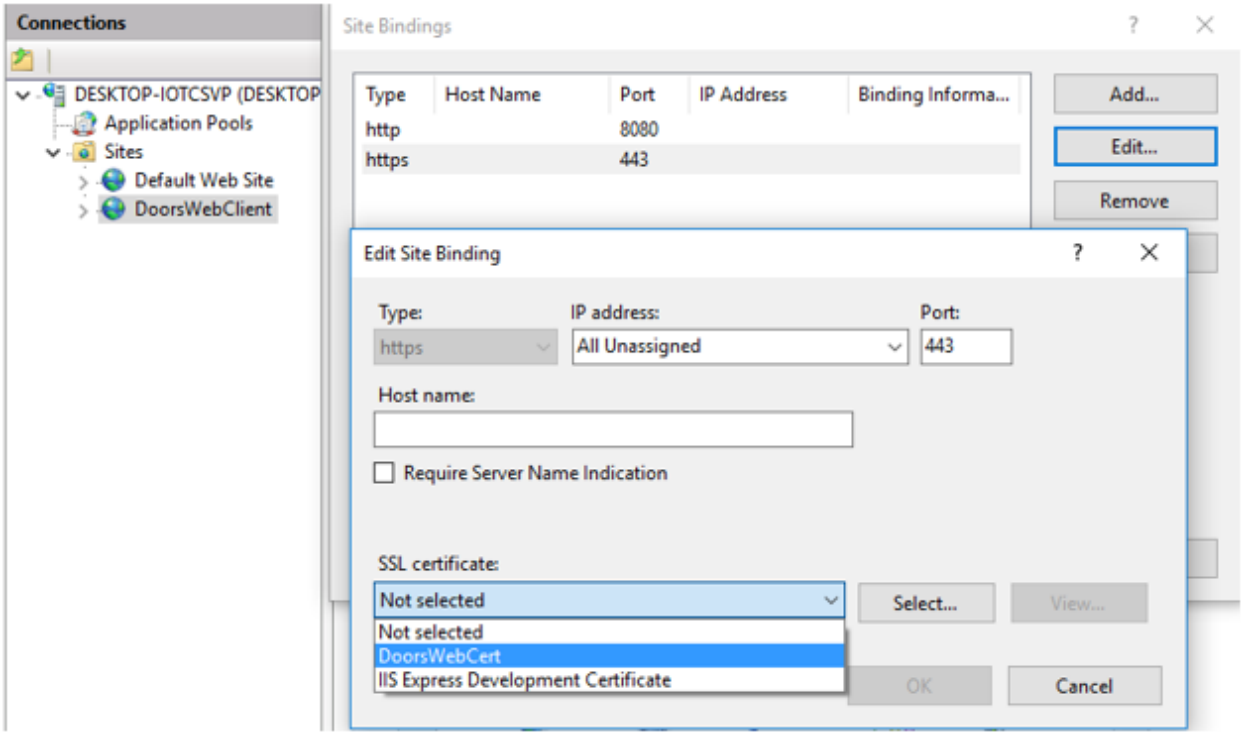
2. From the **Connections** list on the left, select the top connections > run the Server Certificates mode under IIS middle > Under Actions, choose Create Self-Signed Certificate.



3. Name the certificate as **DoorsWebCert** > select Web Hosting as the certificate store > press OK.



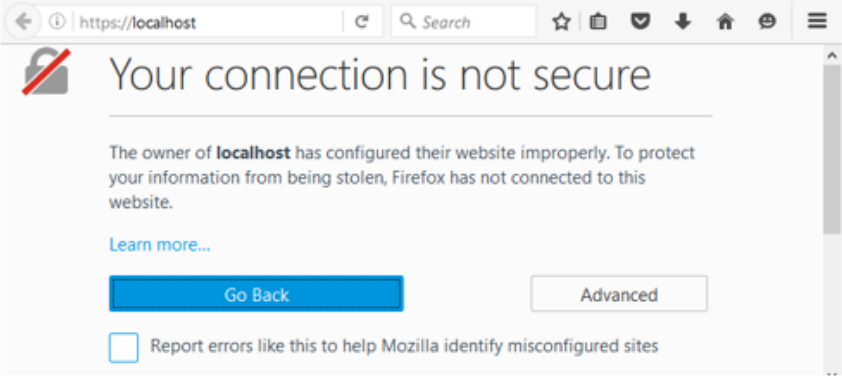
4. Apply the certificate to the site by selecting **DoorsWebClient** under Sites > right click and select **Edit Bindings**
5. From the list, choose https on port 443 > press Edit.
6. From the SSL certificate dropdown, choose DoorsWebCert > press OK.



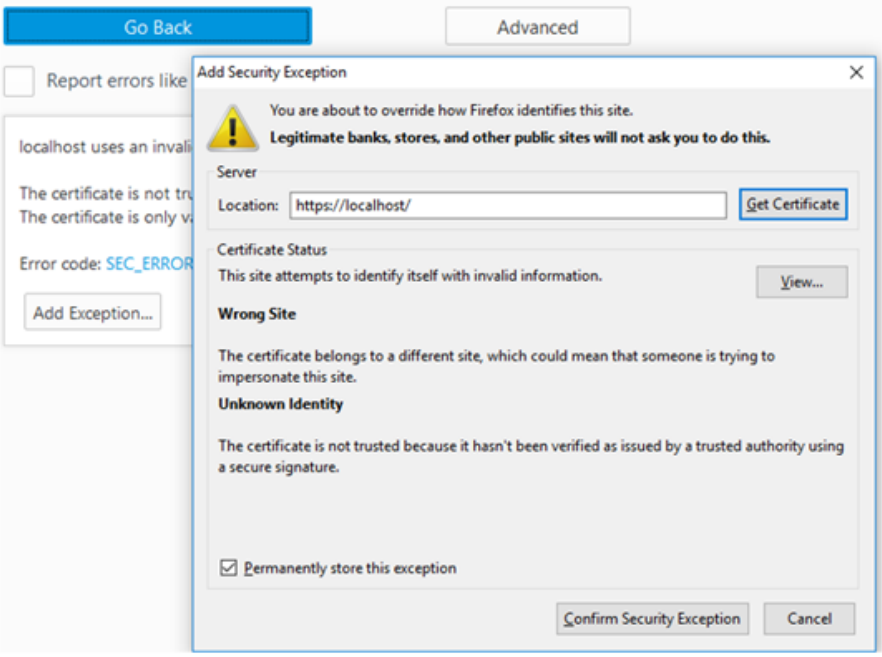
7. Now every time a connection is made to the server, it can be made using a https connection, such as https://localhost (note there is no :8080 at the end).

Accept Self-Signed Certificates on FireFox

The first time the browser connects to the server, the user will need to authorize the self-signed certificate, this is not required for a CA issued certificate. On FireFox the following message is shown:

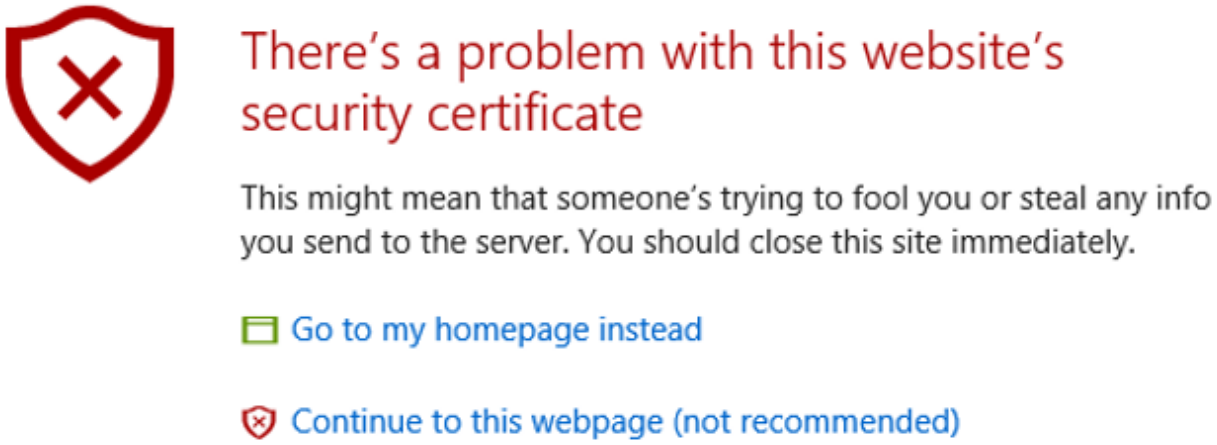


Accept the self-signed certificate by pressing Advanced >> Add Exception >> Confirm Security Exception.



Accept Self-Signed Certificates in Microsoft Edge

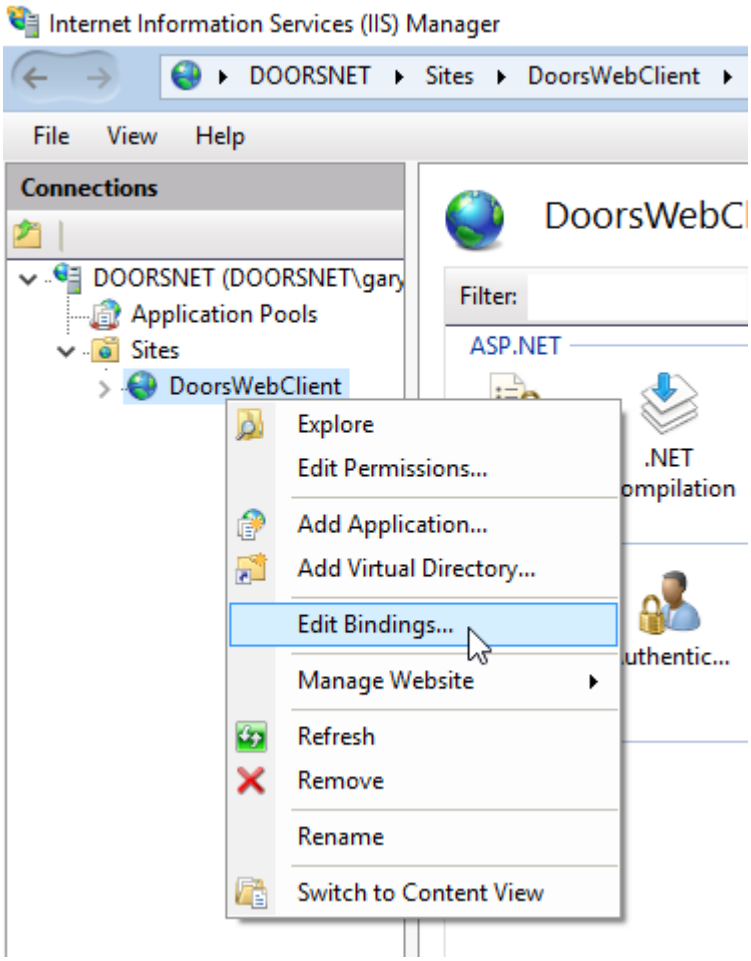
In the Microsoft Edge browser, the following warning is given; select **Continue to this webpage.**



Remove HTTP Connections

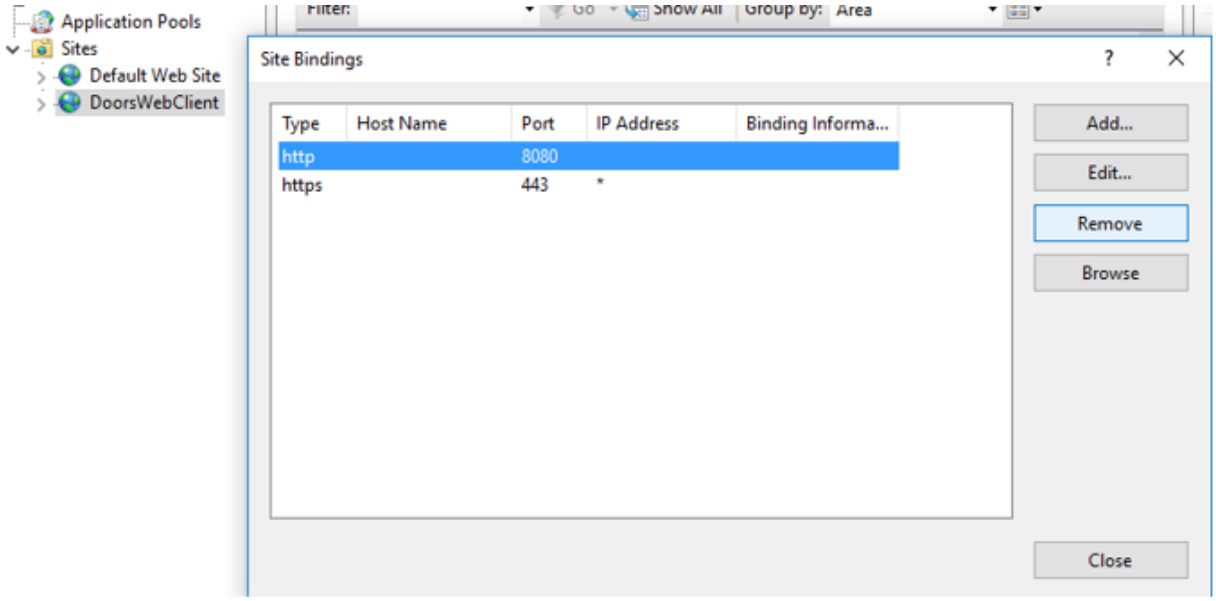
The default method of connecting to Doors.NET using Doors.WEB™ is via HTTP and port 8080. However, these connections are not using SSL. To remove this port binding and discontinue connections on port 8080:

1. Right-click Windows Start menu.
2. Select Control Panel.
3. Click Administrative Tools.
4. Select Internet Information Services (IIS) Manager.
5. Expand the tree-view on the left of the screen.
6. Expand Sites - you should see the Doors.WEB™ site.
7. Right click on DoorsWebClient.
8. Choose Edit Bindings.



9. Select HTTP on port 8080.

10. Click the Remove button.

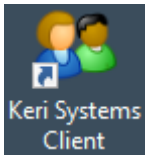


Changing the Default Administrator Password

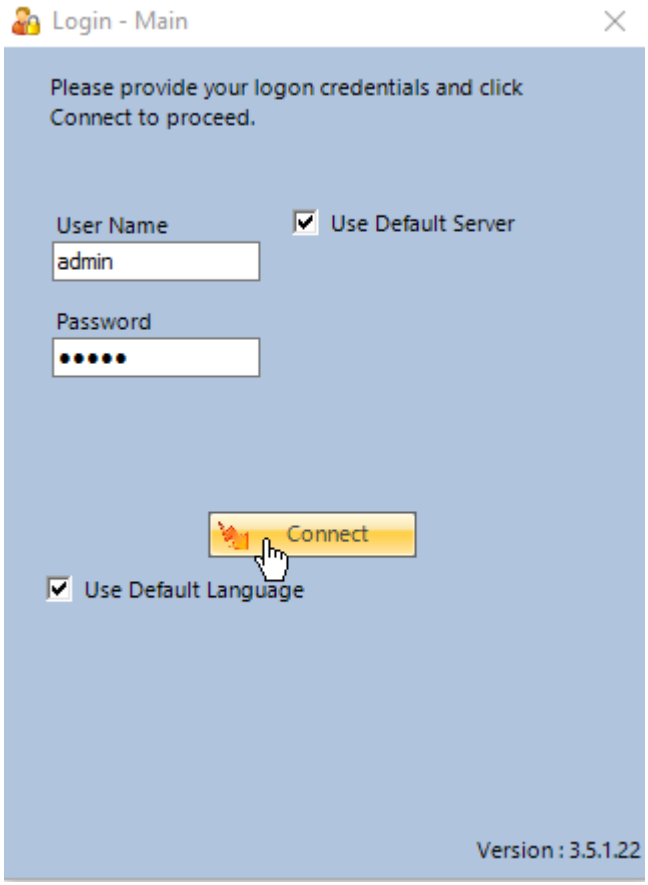
As with most software, there is a default user name and password (both are **admin**). To prevent unauthorized access to your access control system it is vitally important that you change the default administrator password as soon as possible once the software has been installed.

Change the Password

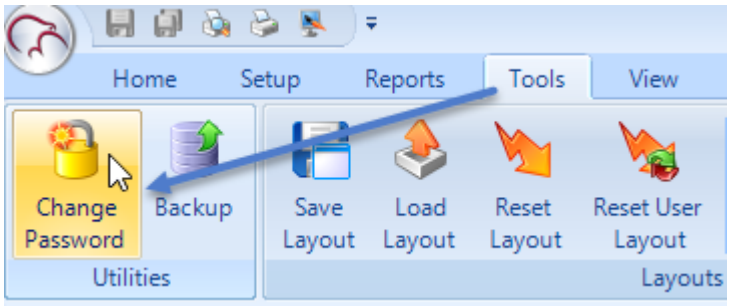
1. Click the Doors.NET icon from the desktop (or via Windows Start menu).



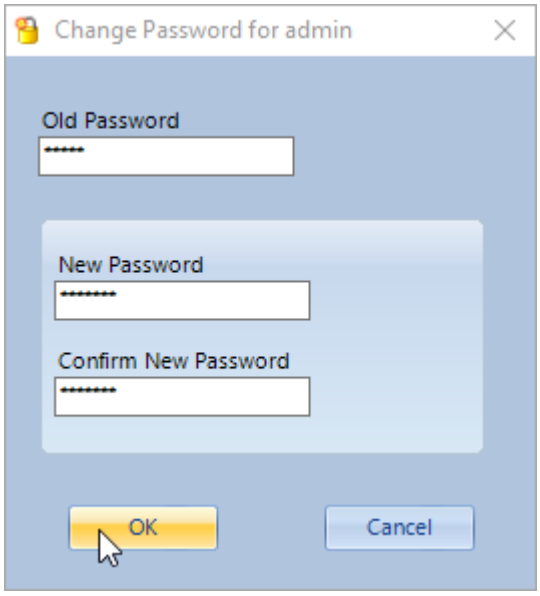
2. Login with the default username and password (both admin).
3. Click the CONNECT button.



4. Once the Doors.NET client is open, click on Tools >> Change Password.



5. A window will open where you should enter **admin** as the old password.
6. Enter a new password.
7. Confirm the new password by entering it again.
8. Click OK.

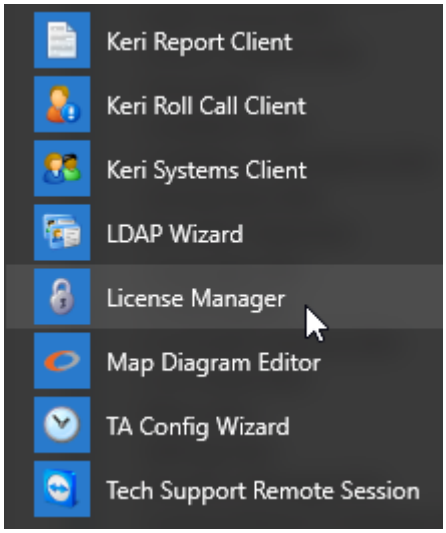


9. The default administrator password will now be changed.

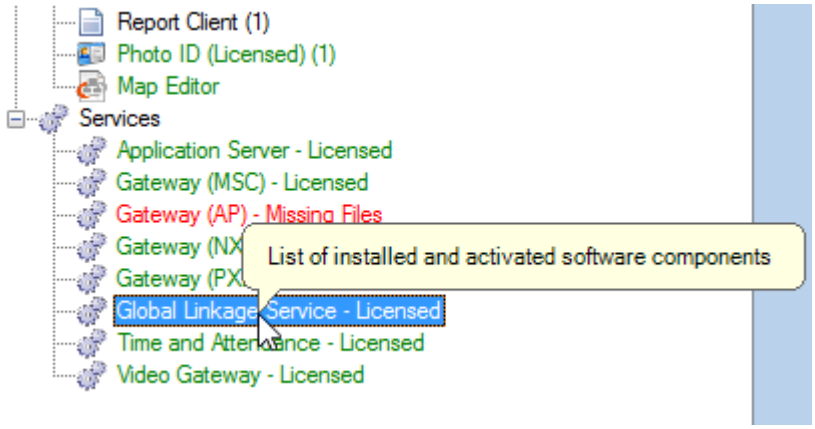
Update the Global Linkage Settings

If the Global Linkage Service (GLS) is installed on your system you will also have to update the Global Linkage settings. GLS allows you to automatically e-mail/SMS message specific system events and allows for a wide range of I/O linkage and automation tasks. GLS uses the default administrator account to carry out its functions.

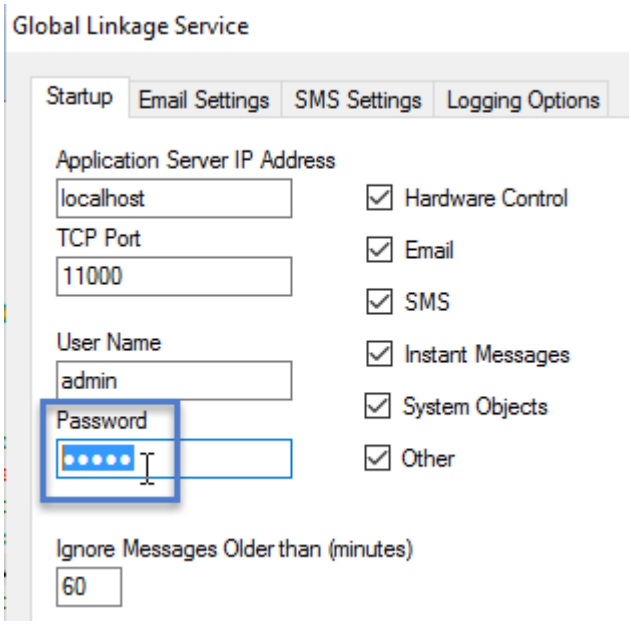
1. From the Windows Start menu, locate the DoorsNET program folder.
2. Click on License Manager.



3. The License Manager window will open.
4. Click on Global Linkage Service from the Services list.



5. Click the SETTINGS button on the right.
6. The GLS settings window will open up on the Startup tab.
7. Enter the new admin password:



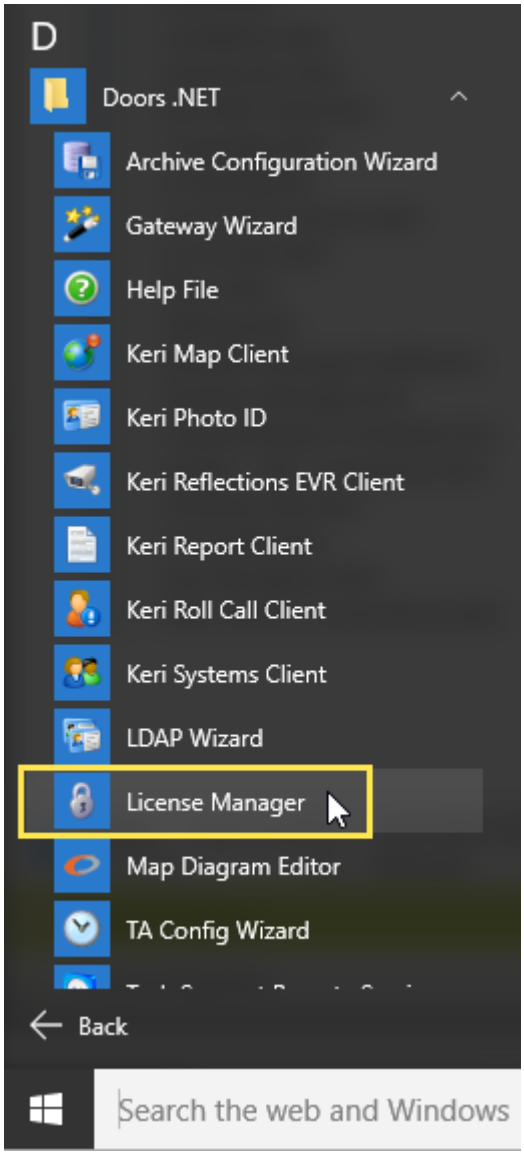
8. Click the SAVE button.
9. Confirm the prompt to restart the GLS service.
10. Close the License Manager window.

Licensing

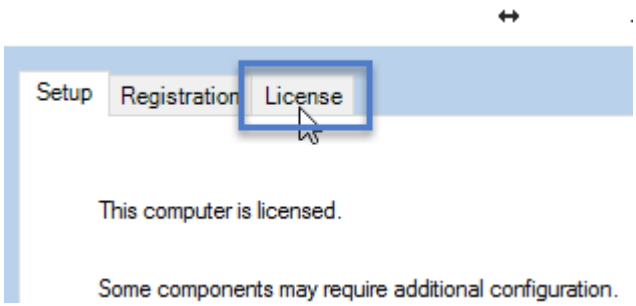
Connecting using the Doors.WEB™ client is not included in the standard Doors.NET software bundle. Therefore the feature must be purchased and enabled on the Doors.NET Application Server PC.

Check the Web Browser Client is Enabled

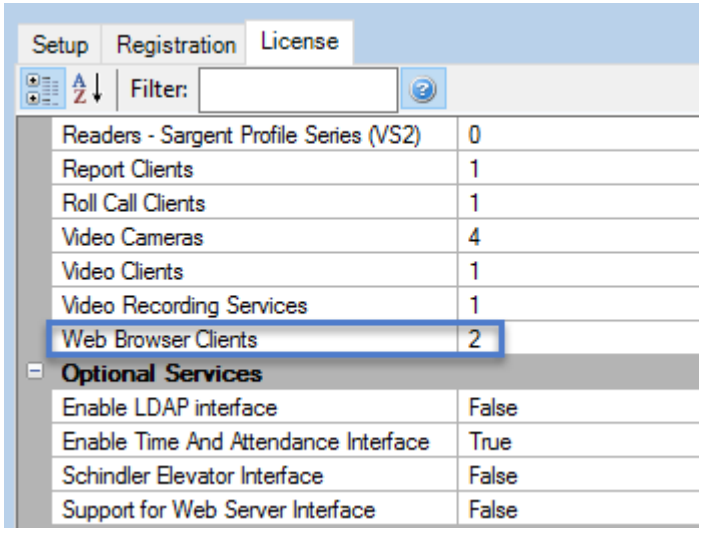
1. On the Doors.NET Application Server PC click on the Windows Start menu.
2. Go to All Apps/All Programs.
3. Locate the Doors.NET file group.
4. Click on License Manager.



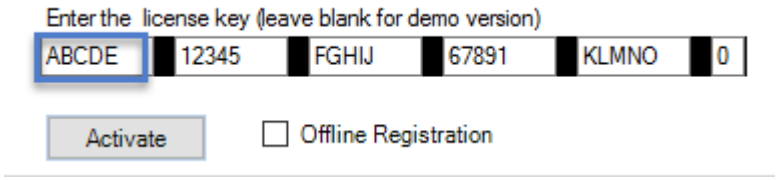
5. The License Manager window will open.
6. Click the License tab on the right of the window.



7. A list of all the licensed features and components will be displayed.
8. Scroll to the bottom of the list of **Capacities** and locate Web Browser Clients.



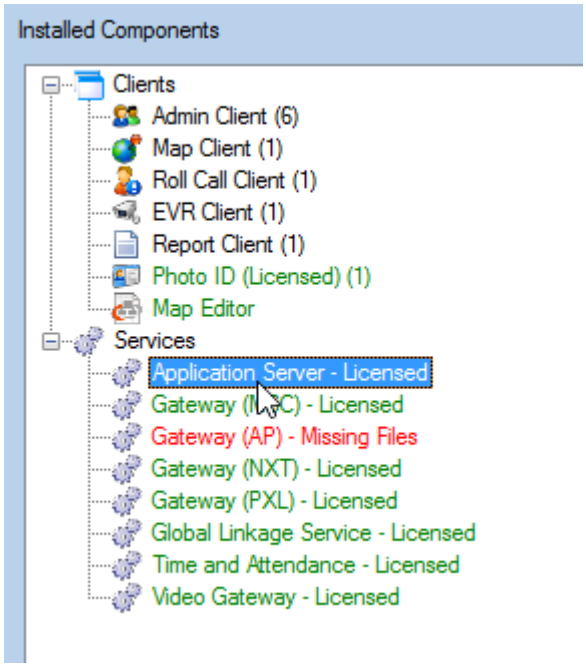
9. Ensure Web Browser Clients is not showing zero.
10. If it is showing zero then you will need to contact Keri Systems inside sales (ensure you have the first 5 characters of your license key to hand) - this is displayed at the bottom of the license window.



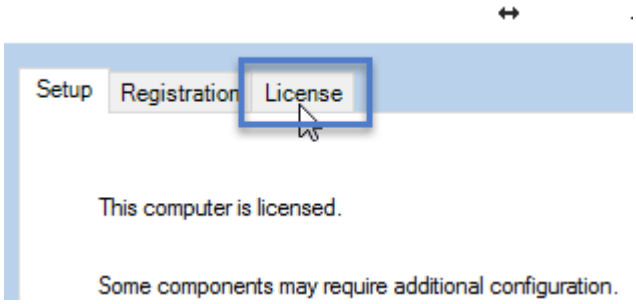
Activating Doors.WEB™ Online

If you have an active, unrestricted internet connection and you have just purchased the Doors.WEB™ feature, then activating the feature on your license key is a very quick and simple process.

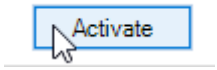
1. Open the License Manager (via Windows Start menu>> All Apps/All Programs >> Doors.NET >> License Manager).
2. Click Application Server on the list of installed services on the left.



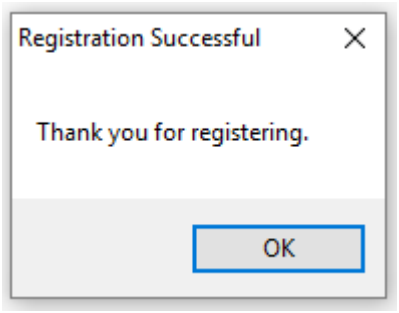
3. Click on the License tab (on the right).



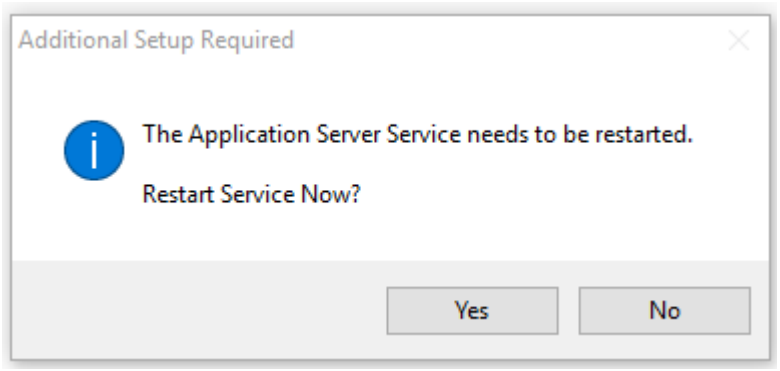
4. At the bottom of the license window click the ACTIVATE button.



5. Within a few seconds you should see the following notification.



6. You will then be prompted to restart the Application Server Windows service.

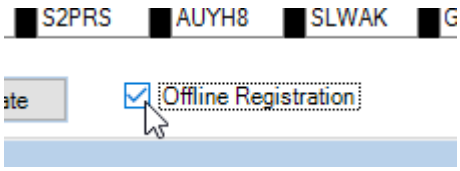


7. The feature will now be enabled.

Activating Doors.WEB™ Client Offline

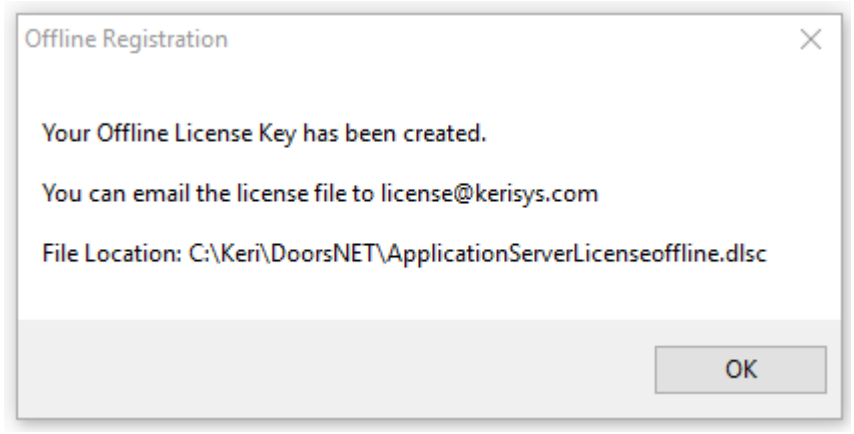
If there is no active internet connection on the host PC, or if the connection is being blocked by a firewall or security setting you can still activate the Doors.WEB™ feature by e-mailing the license file to Keri. This process will typically take 1 business day to complete.

1. Open the License Manager (via Windows Start menu>> All Apps/All Programs >> Doors.NET >> License Manager).
2. Click Application Server on the list of installed services on the left.
3. Click on the License tab on the right.
4. At the bottom of the license manager window place a check mark in **Offline Registration.**

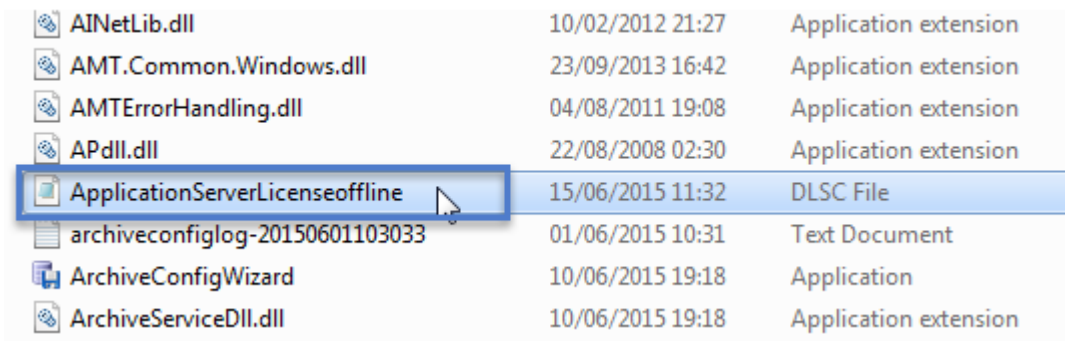


5. Click the ACTIVATE button.

6. You should see a notification stating where on the host PC you can find the offline license file and the email address to send it to.



7. Email a copy of this file to license@kerisys.com for US customers, or to tech-support@kerisystems.co.uk for customer in the UK and outside of the US.

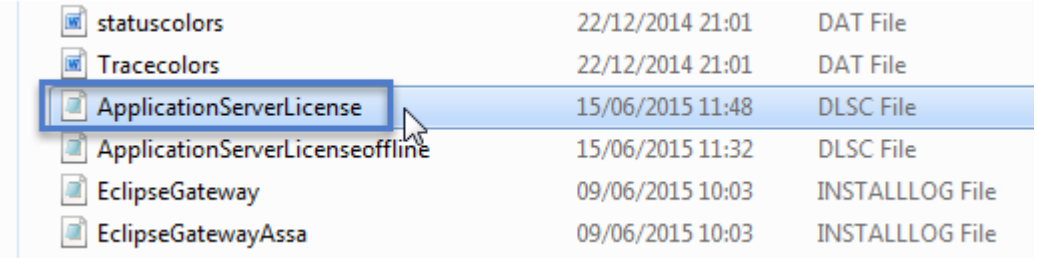


8. In your e-mail you should also include the following information:

   - Your name
   - You company name

- The name of the site
- Your order reference number

9. Close the License Manager Window.
10. Within 1 business day you will receive your activated license file as an e-mail attachment, it will be renamed ApplicationServerLicense.dlsc.
11. Copy the received ApplicationServerLicense.dlsc file into the **C:\Keri\DoorsNET** directory (overwriting any existing file with the same name).



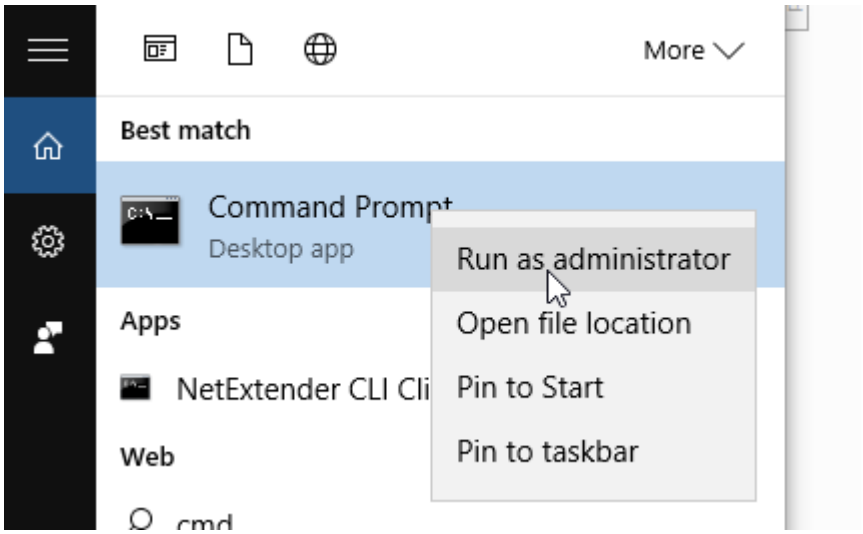
12. Restart the Application Server Windows service.
13. You will now be able to connect to the system using Doors.WEB™.

Using Doors.WEB™ on a Smart Phone

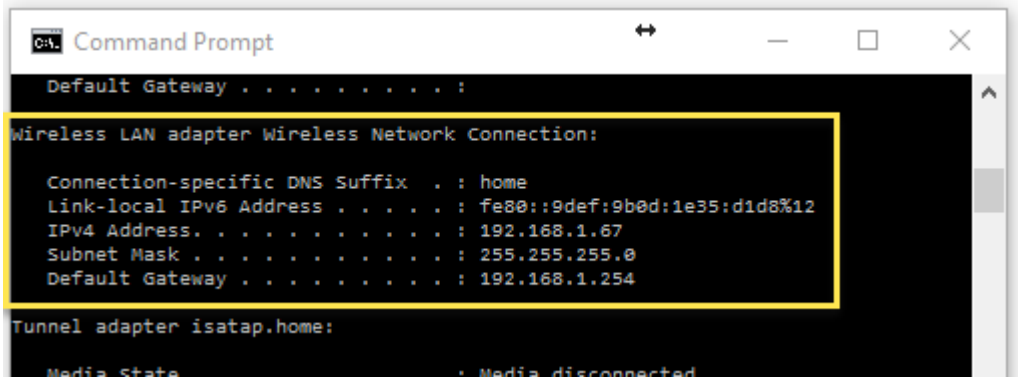
To use the Doors.WEB™ client with a smart phone you have to be connected to the same wireless network as the host PC. The following information explains how to use the web client with a smart phone.

Check the Host Wireless IP Address

1. From the Windows search bar, type CMD, then ENTER.
2. Right-click Command Prompt and select: "Run as Administrator".



3. Type in "IPCONFIG", ENTER.
4. Your host PC network settings will be displayed.
5. Locate the Wireless network IP address.



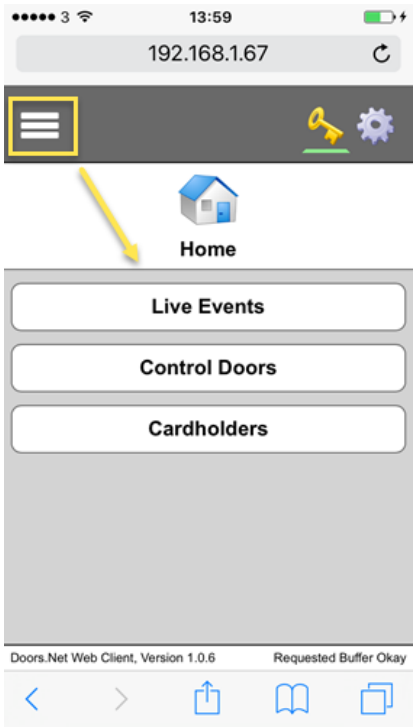
6. Make a note of the IPv4 address. In the above image it is 192.168.1.67.

Connect to the Doors.NET Host Machine From Your Smart Phone

1. Go into the network settings of your phone.
2. Check that you are connected to the correct wireless network.

3. Open a web browser on your phone.
4. Type into the address bar the IP address of the Doors.NET host.
5. You should see the Doors.WEB™ log on window.

6. Enter the Doors.NET user name and password (the default is **admin** for both).
7. Click the LOGIN button.
8. You will see a LOGOUT button in the middle of the screen.
9. Press the menu icon in the upper left to display the three menu items.



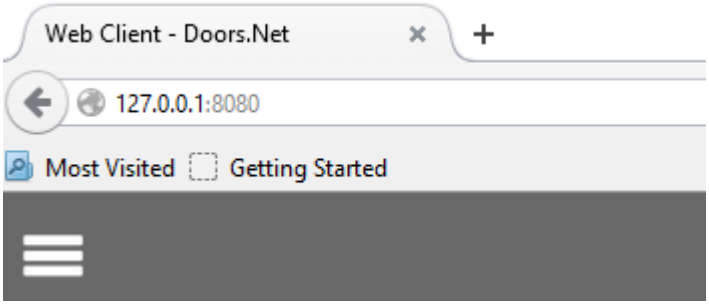
10. You are now ready to use the Doors.WEB™ client.

Related Topics

- Control Doors
- Live Events
- Adding Cardholders
- Editing Cardholders

Navigating the Interface

Connecting to the System



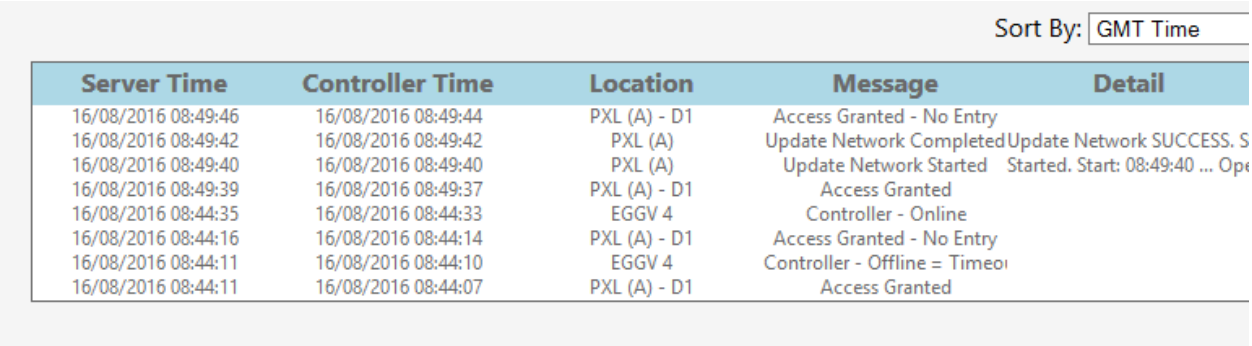
Once Doors.WEB™ is installed the user interface can be accessed from any device which has an internet browser. Following installation, you simply open a browser and then type the Application Server IP address into the address bar. The default URL uses port 8080 but this can be easily changed.

Home

Returns you to the home screen.

Live Events

The Live Events table displays system events as they happen in real-time.



System event examples are: access granted messages, access denied messages, door opened, door closed, door held, door forced, etc. You can sort the information by any column by changing the **Sort By** column and checking or un-checking the Reverse Order check-box.

Control Doors

Loads a list of all readers on the system. Use the control doors screen to lock, unlock or send a command to unlock a door for a short period of time.

- **Lock** - Override any existing schedule the reader is following - the door will be locked.
- **Unlock** - Override any existing schedule the reader is following - the door will be unlocked.
- **Timed Unlock** - Override any existing schedule the reader is following, to unlock a reader for a period of time (strike time) defined in Doors.NET (it is 7 seconds by default).
- **Restore** - Causes a reader to resume following its allocated schedule - The door may be locked or unlocked.

Note: Suspending and restoring auto-unlock time schedules is not supported with the standard NXT controllers. The restore button will not be available for standard NXT doors.

Cardholders

Directs you to sub-menus relating to cardholder and credential administrative tasks. The cardholders section allows you to:

- Add, edit and delete cardholders.
- Add, edit and delete assigned credentials, such as cards, tags and pins.

Tool Bar

Log

The Operator may login or logout through the Key tool, if the operator is not currently logged in, a dialog for username and password is provided to login. If the user is currently logged in, a logout button is provided; user names and passwords are not case sensitive.

The Doors.Net License defines the number of concurrent Doors.WEB™ connections. The license value can be found under Capacities > Web Browser Clients. Each system administrator should possess a unique user name and password to ensure accurate history is maintained in the Doors.Net database.

The Operator's current log status is displayed under the Key icon by a given color:

• No colored line – unknown log status.
• Red line – Operator is logged out.
• Green line – Operator is logged in.

Settings

To affect Doors.WEB™ Client settings, the operator must be signed in. Settings are device specific, so an operator may configure different settings on a range of devices. The operator's settings are stored locally on the device in HTML5 Local Storage, if the operator's browser doesn't support HTML5 Local Storage and they wish to save their set-

tings, a browser update must be performed; using a browser in Private Mode will also prevent the settings from being saved.

Selecting the Settings icon presents the following options.

Cardholders
Cardholder Settings allows the Operator to define the preferences regarding the level of information to display when in the Cardholder related areas of the program. By default, Emergency, Contact and Company information are not displayed, these may be enabled by entering Cardholder Setting and checking the preferred check box.

Live Events Columns
The Operator is directed to Live Events page and a table of columns and display widths are presented. Display or hide any given column by checking the corresponding check box, adjust the column width by changing the number value next to the column name or by using the up and down arrows that appear when the width number is selected; any changes made to the column settings are automatically saved as the changes are made.

Languages
You may choose between the following languages:
• English (United States)
• Spanish (Mexico)

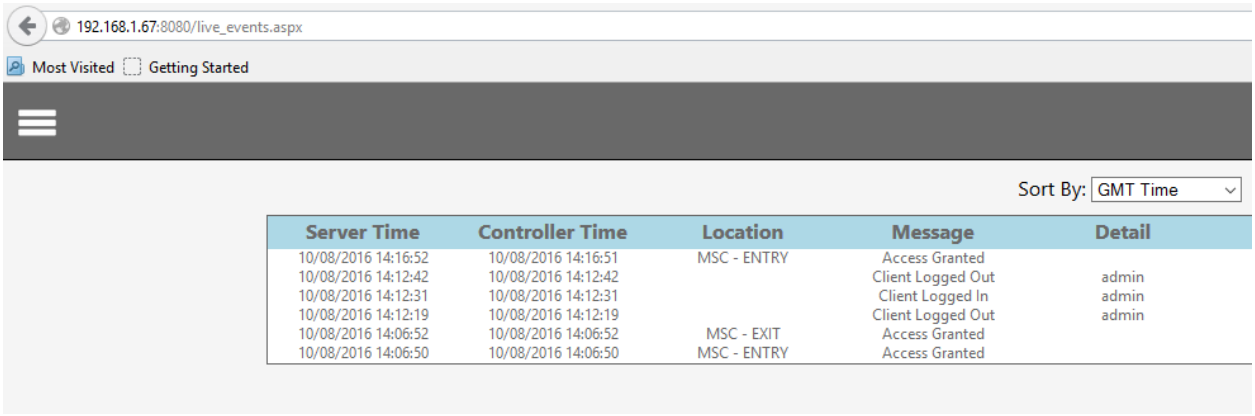
The default language is English (US). If you find that selecting another language fails to translate, then the browser doesn't support HTML5 Local Storage and a browser update is required, or Private Mode is enabled and must be disabled.

Bottom Bar

Version
The left region of the bottom bar will indicate the current version of Doors Web Client.

Connection
The right region of the bottom bar provides connection information between the Doors Web Client and the Web Server.
Card

Live Events



The Live Events grid is accessed via the menu icon.

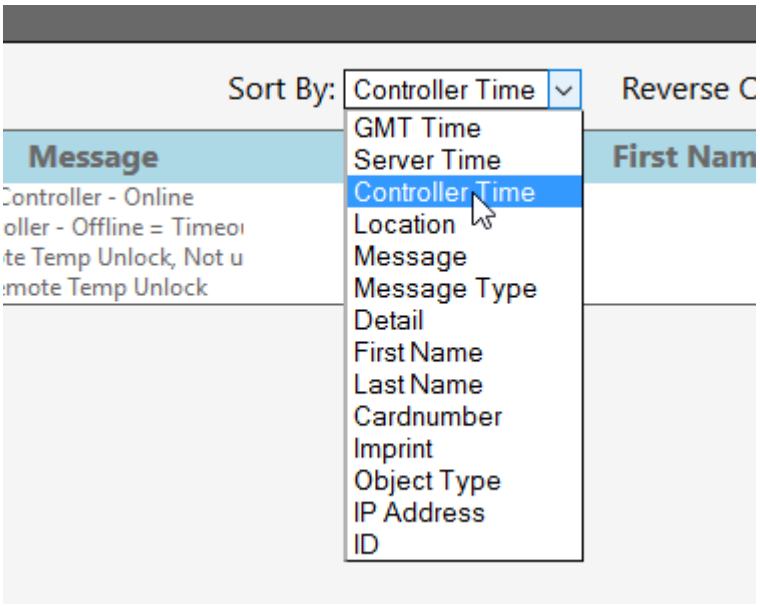
It is a dynamic grid that allows you to view system events as they occur.

Sorting Live Event Information

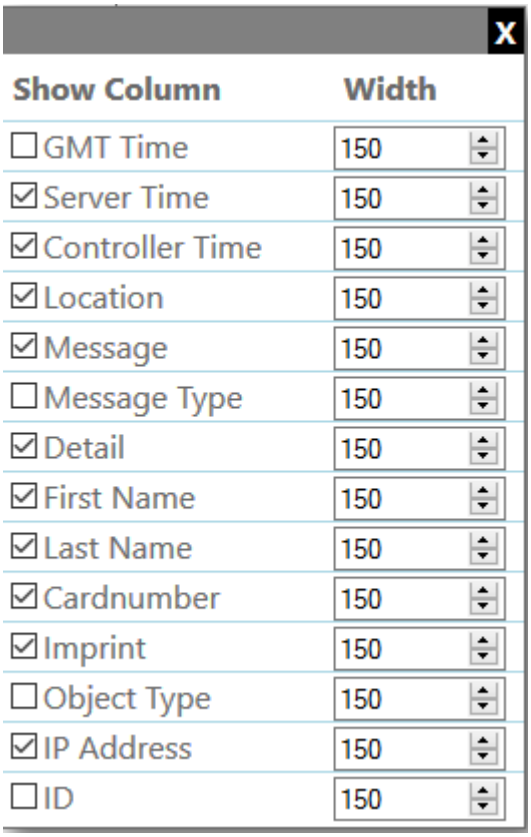
By default, when accessing the live events grid using a smart phone only 3 columns will be displayed. If using a PC you will see the following columns:

- Server Time
- Controller Time
- Location
- Message
- Detail
- First Name
- Last Name
- Cardnumber
- Imprint
- IP address

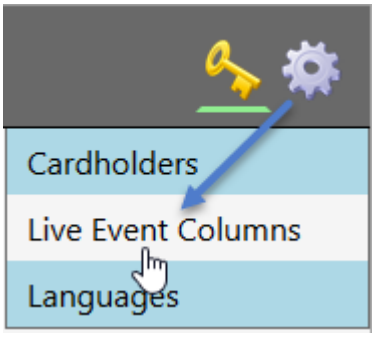
You may sort the event information by selecting one of the options in the Sort By: list.



Live Event Columns



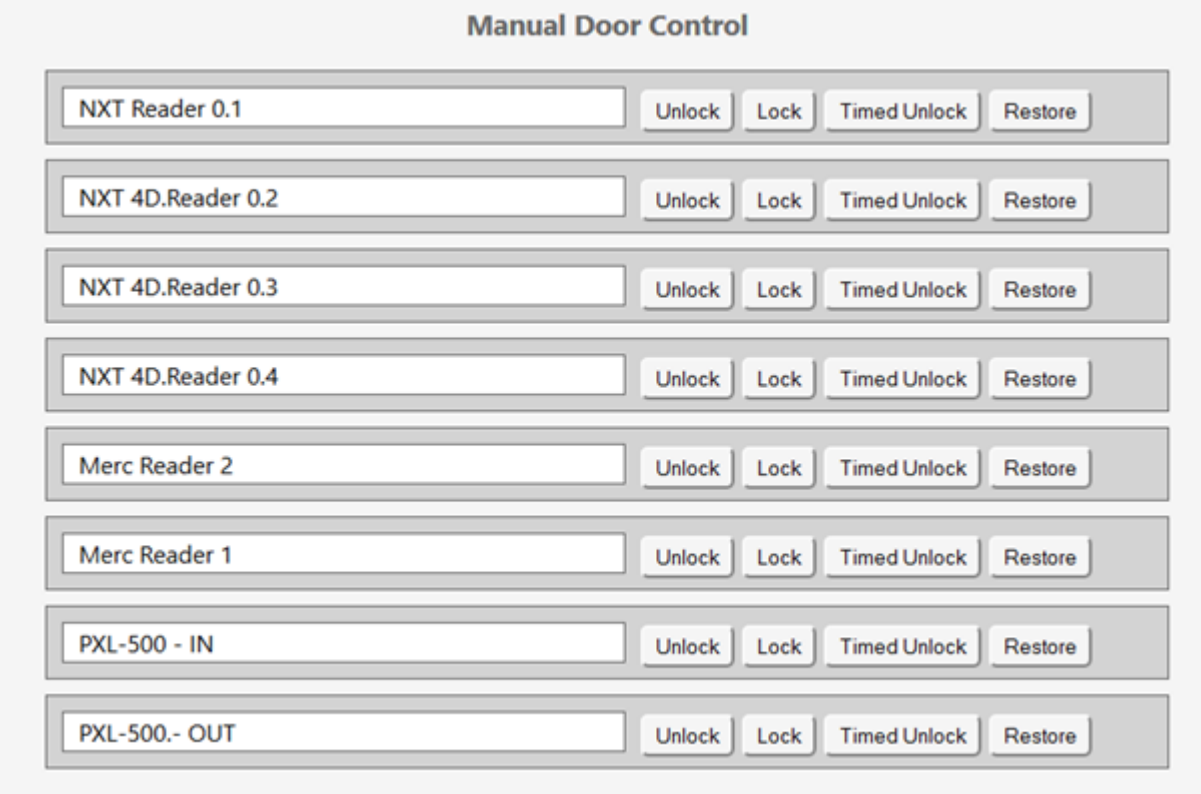
Click the Settings icon >> select Live Event Columns.



You will be directed to Live Events page and a table of columns and display widths are presented. Display or hide any given column by checking the corresponding check box, adjust the column width by changing the number value next to the column name or by using the up and down arrows that appear when the width number is selected; any changes made to the column settings are automatically saved as the changes are made.

Control Doors

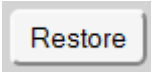
The Control Doors page loads a list of all the doors on the system.



To the right of each door name you can see there are door command buttons allowing you to lock, unlock or unlock the door for a short period of time.

- Unlock - Overrides an existing schedule that the door may be following and will unlock the door.
- Lock - Overrides an existing schedule that the door may be following and will lock the door.
- Timed Unlock - Overrides an existing schedule that the door may be following and will temporarily unlock the door (this is the strike time set in Doors.NET) and the

default time is 7 seconds.

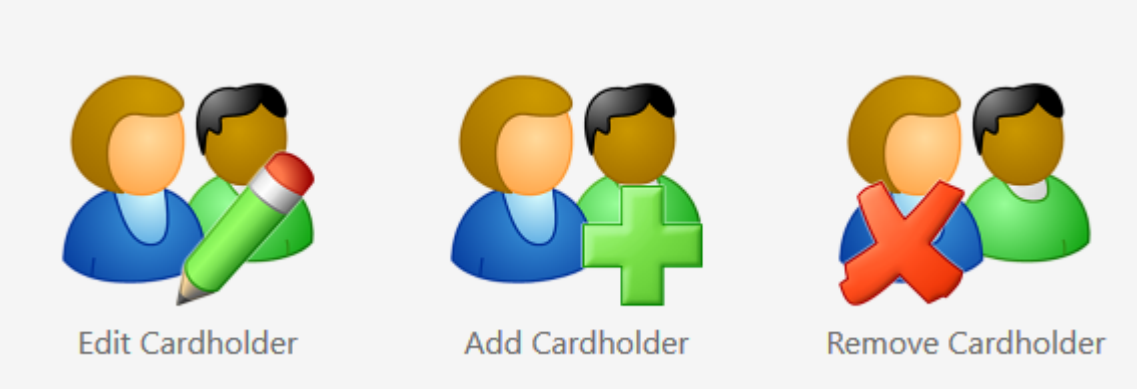
- 

- when one of the above lock or unlock buttons are used any assigned schedule will be suspended. Use the resume button to resume the assigned schedule.

Note: Suspending and restoring auto-unlock time schedules is not supported with the standard NXT controllers.

Cardholders

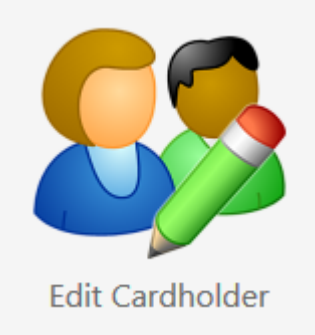
The Cardholders section takes you to the cardholder administrator tasks:



- Add, edit and delete a cardholder.
- Add, edit and delete a cardholder's credential, such as a card or fob/tag

Edit Cardholders

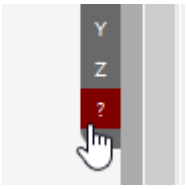
1. Press the Edit Cardholder icon to enter the cardholder edit screen.



2. The last name alphabet menu will appear.
3. To select a specific cardholder:

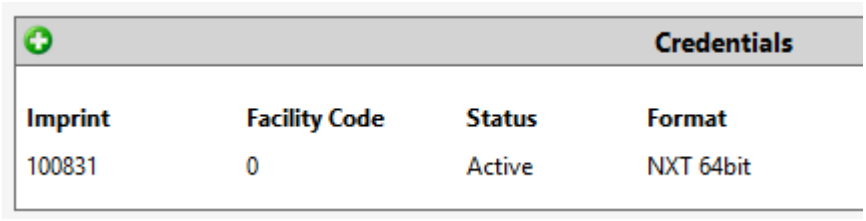
   a. Select the letter corresponding to the cardholder last name via alphabet menu > locate the specific cardholder > press **Edit.**
   b. Press the magnifying glass icon at the top of the alphabet menu > Enter a first name, and/or last name > press the magnifying glass below the last name >> find the cardholder in the list.
   c. To load the entire list of all cardholders on the system, press the small question

mark located at the bottom of the alphabet menu.



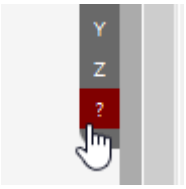
The entire list of cardholders will then appear:

4. Edit the cardholder fields, as required. Only the first name and last name are mandatory fields.
5. Add, Edit or remove cards/tags/PINs in the Credentials section of the cardholders page.



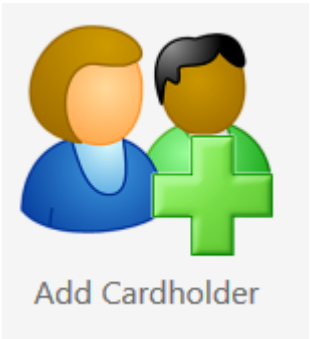
6. After editing cardholder information, remember to press on Save Changes. Changes will not be made until Save Changes has been pressed.

NOTE: To load the entire list of all the cardholders on the system, press the small question mark located at the bottom of the alphabet menu.

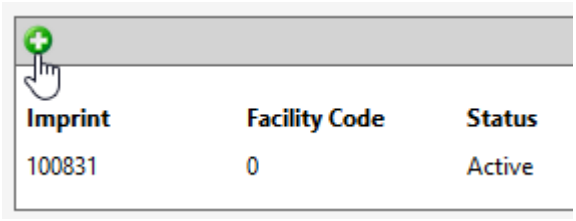


Add Cardholders

1. Press the Add Cardholder icon.



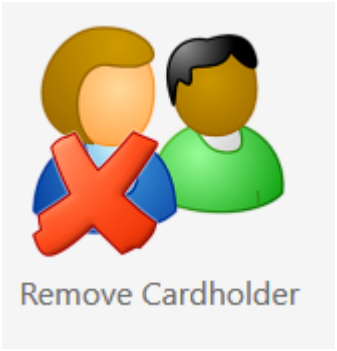
2. Enter the new cardholders full name (first name and last name are required fields).
3. Select the Access Permission for the new cardholder (this determines which doors they can gain access)
4. Add cards/tags/PINs by pressing the green button with a white cross (in the top left of the Credentials section.



5. Remember, to commit changes you must press the **Save Changes** button.

Remove Cardholders

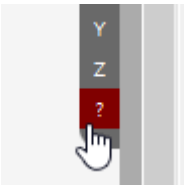
1. Press the Remove Cardholder icon.



a. Select the letter corresponding to the cardholder last name via Alphabet Menu > locate the specific cardholder > press **Delete.**
b. Press the magnifying glass icon at the top of the Alphabet Menu > Enter a first name, and/or last name > press the magnifying glass below the last name >> find the cardholder in the list and press **Delete.**

2. The cardholder will be removed from the software and subsequently will be removed from the system hardware.

NOTE: To load the entire list of all the cardholders on the system, press the small question mark located at the bottom of the alphabet menu.

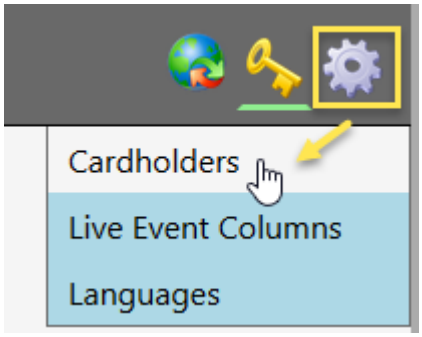


Cardholder Fields

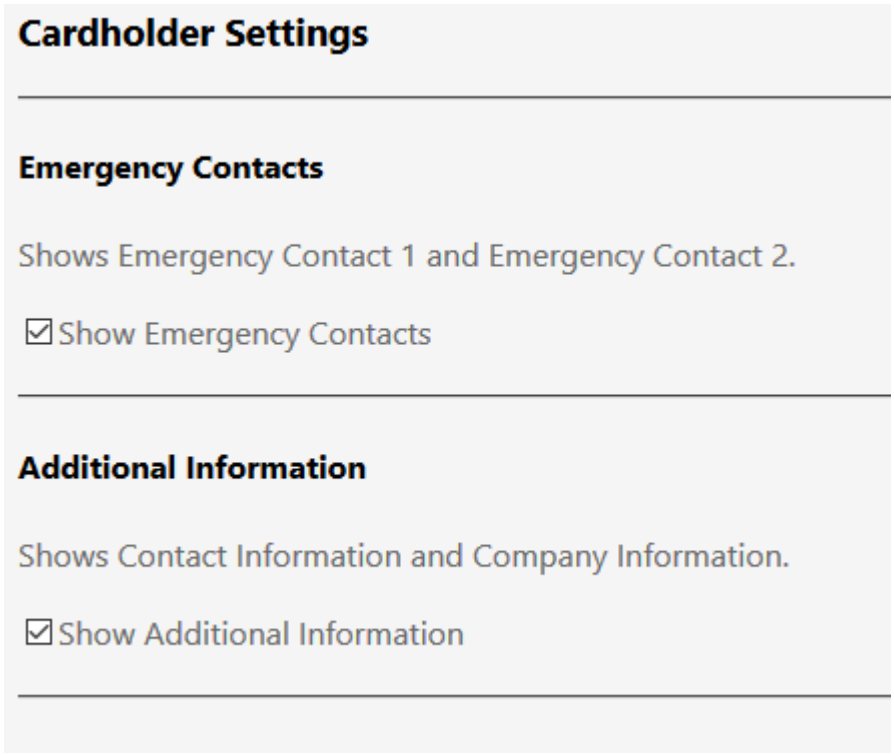
The cardholder fields provide you with information about the selected cardholder. There are additional fields which are not displayed by default.

Enable Additional Cardholder Information

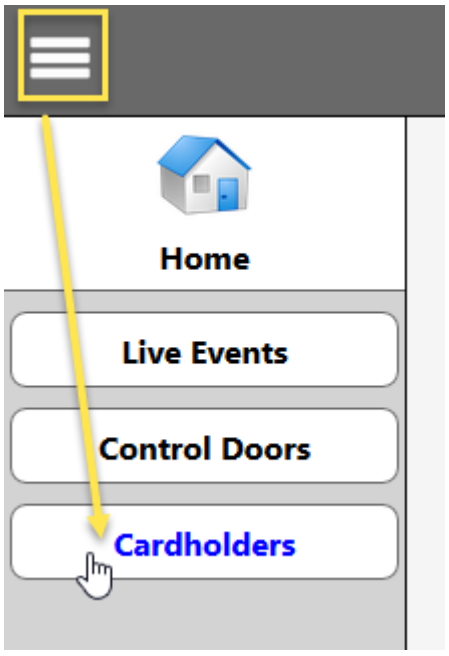
1. To enable additional cardholder information, got to: Settings >> Cardholders >>



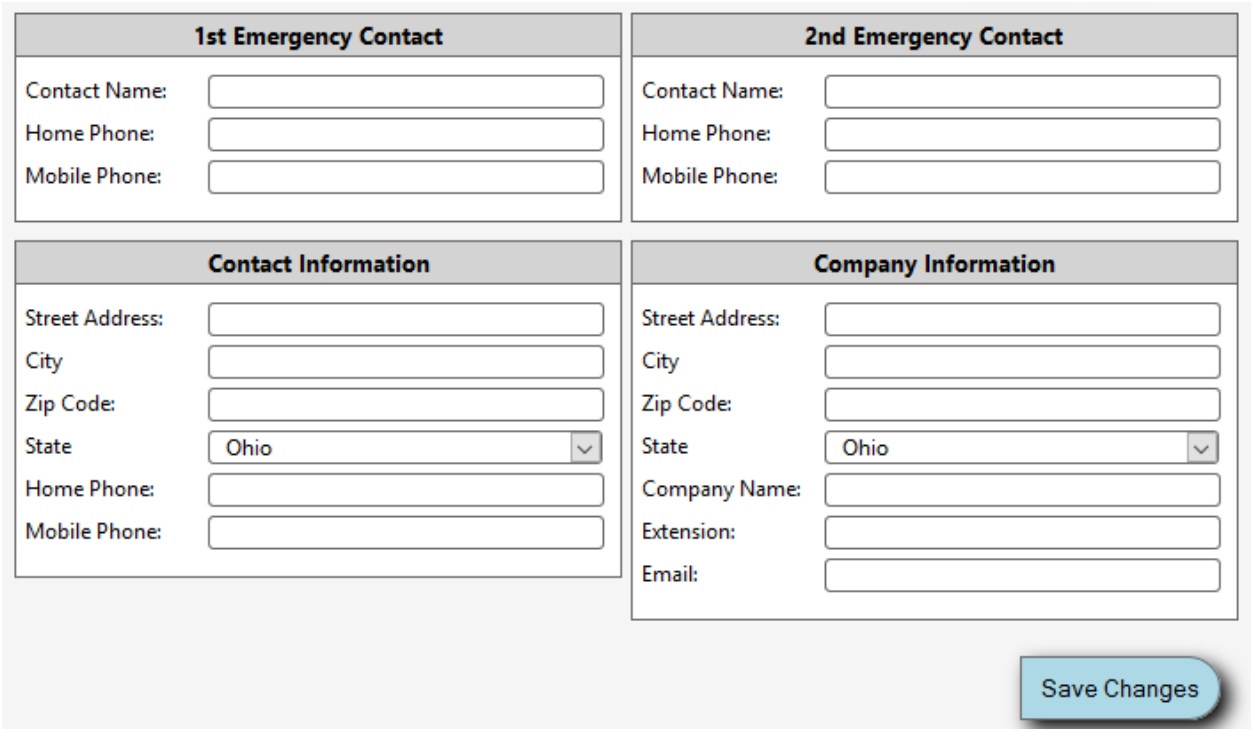
2. The additional selections will appear.
3. Place a checkmark against each option to display.



4. Emergency Contact and Additional Information fields will now display for any cardholder record you open.
5. Go to the main menu and select Cardholders.



6. If you now add or edit a cardholder the additional fields will display.



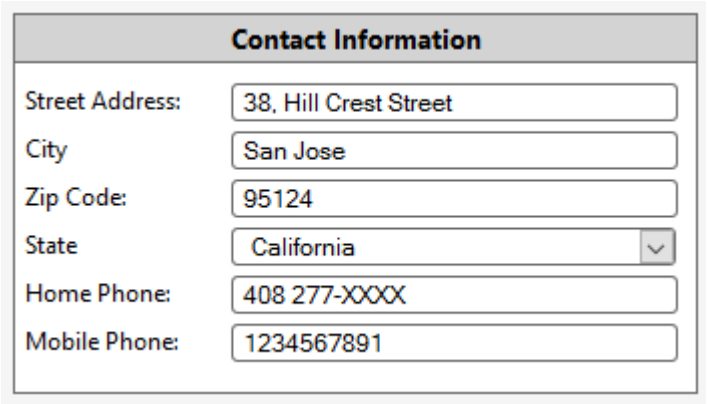
Cardholder Details
Each card record must have a first name and last name (middle name is optional).

Validation
To assign an expiration date for this cardholder, check **Enable Expiration Date for this Cardholder.** This will then display the **Expiration Date** field, allowing you to specify an expiry date. Change the **Valid From** to and enter a future date to pre-register the assigned card/tag. The date formats are determined by the browser's region settings.

1st and 2nd Emergency Contacts
When enabled, the following fields are available but are not mandatory:

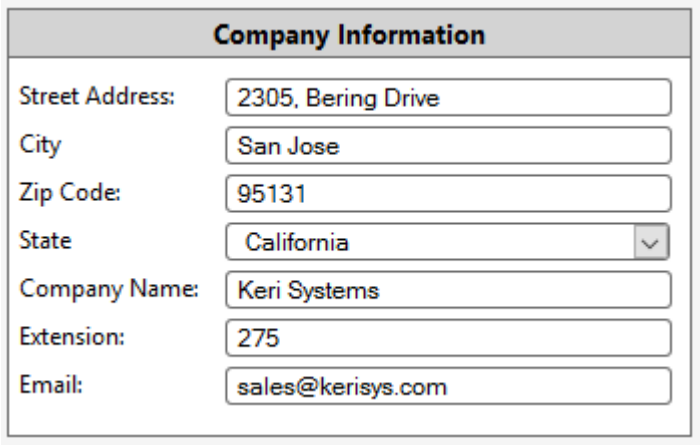
- *Contact Name* - Person to contact in the event of an emergency.
- *Home Phone* - Home number of the emergency contact.
- *Mobile Phone* - Cell/Mobile number of the emergency contact.

Contact Information and Company Information
When enabled, the contact information is intended to record contact details for the card-holders. Complete any of the fields provided, none of the following fields are mandatory.



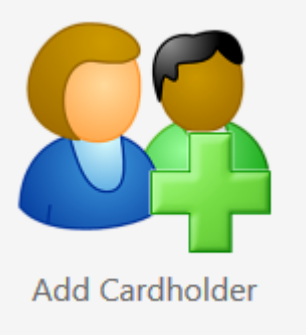
The company information is intended to record details about the company which the card-holder is employed by. Again, none of the following fields are mandatory.

The state drop-down list is populated by the Doors.NET server based on the regional settings.



Credentials

Credentials are the cards or tags that are assigned to cardholders via the **Add Cardholder** button.



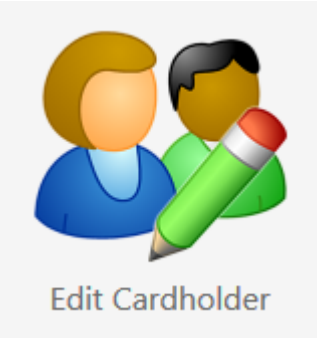
The Doors.NET Web Client allows you to manually enroll the following credential types:

- NXT (64-bit)
- Keri MS Format
- Wiegand 26-bit
- RAW

Manual enrolling a single credential at a time is the only method available with the Web Client. Block Enrollment or Presentation Enrollment must be performed from the standard Doors.NET client.

After adding a new cardholder and a new credential you can then add additional credentials via the **Edit Cardholder** button.

Note: Each cardholder record MUST have at least a first name and a last name, otherwise you will not be able to save the new record.



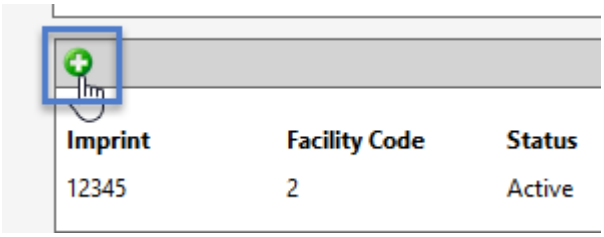
You can also set a cardholder to being temporary but note; all assigned credentials will then be temporary - It is not possible to have a mixture of permanent and temporary cards assigned to the same cardholder.

Edit Credentials

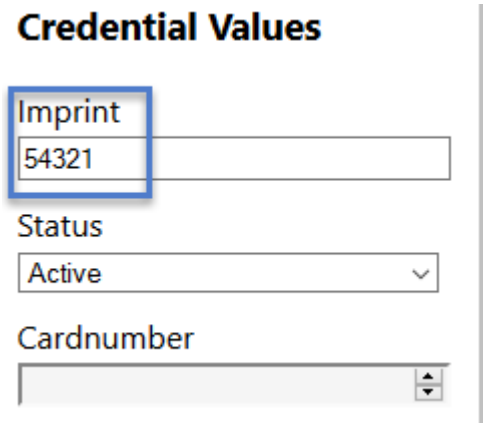
When editing an NXT, MS or 26 Bit Wiegand credential, only the imprint and status may be changed, this doesn't affect the internal number, only the number printed on the credential. If the internal number is not correct, the credential must be deleted and recreated.

Edit a Credential

1. To edit an assigned credential open a cardholder record.
2. Click the green and white icon in the top left of the Credentials section.

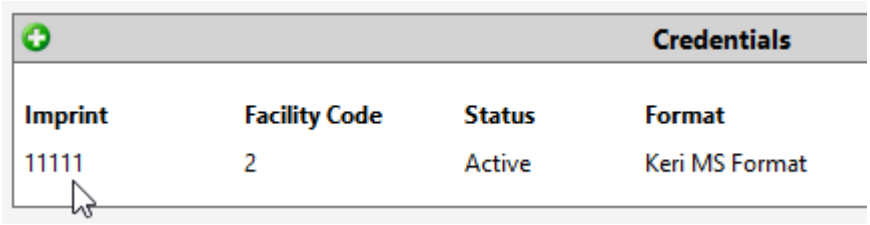


3. Change the required values.



4. Click **Done.**

5. The changed value will be displayed on the cardholder Credential section.



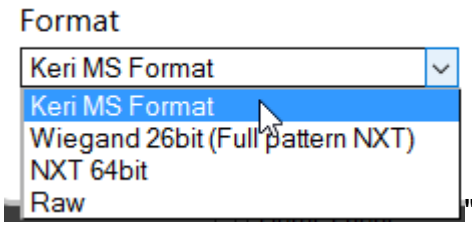
Remove Credentials

Note: To remove a credential, simply press the Delete button

.

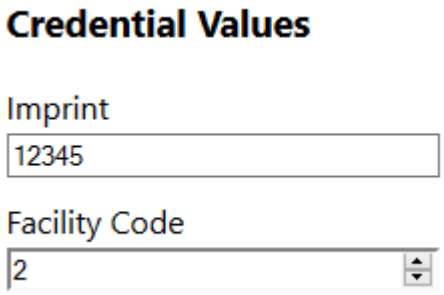
Add Credentials

1. When creating a new Credential, start by selecting the format from the **Format** drop-down list.

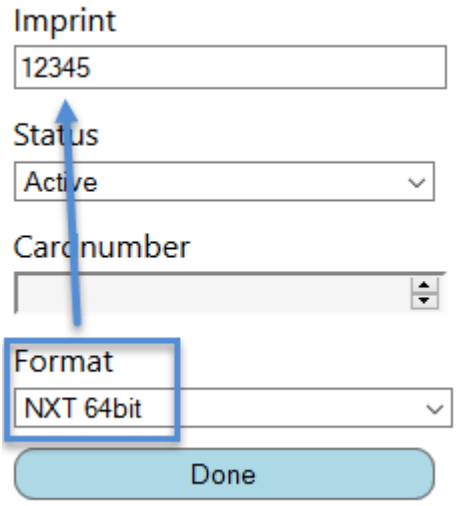


"Add Credentials" above

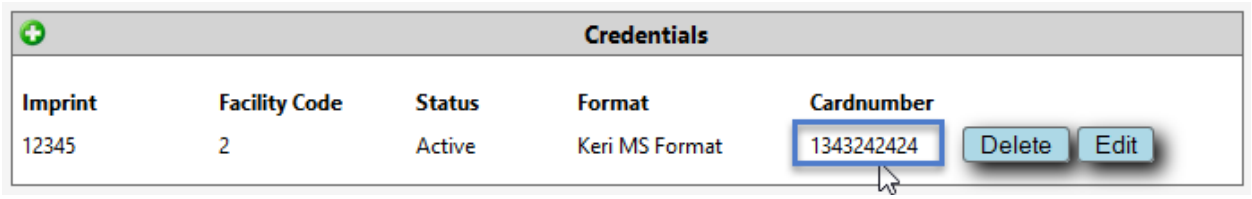
2. The available fields on the credential add window will change according to the selected format.
3. If using MS credentials or 26-bit Wiegand credentials, input the facility code and imprint.



4. If you are using NXT credentials you are not required to enter a facility code. so you only have to enter the imprint.



5. If using and other formats then the card data is formats are enrolled as RAW, enter the imprint and card number > set the issue code to the next sequential value, starting a 0 > set the card status to active > press **Done.**
6. Click Done and the credential will be added to the cardholder record.
7. The Cardnumber field is not editable because the unique cardnumber is automatically calculated when you click **Done.**

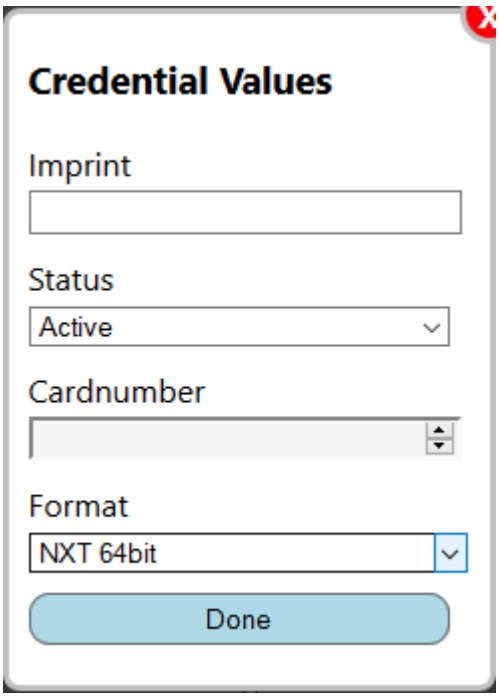


8. If you have already added the cardholders first name and last name click the **Save Changes** button.

NOTE: New, edited and deleted credentials are not saved to the database until the Save Changes button is pressed.

You can add additional credentials to the cardholder record via the Edit Cardholder button.

Summary



Imprint - the number printed on the card or tag, this may also be a PIN. An imprint doesn't contain any letters or special characters.

Status - The status of a credential - Active suggest it's currently is use and is allowed to function. Any other status will prevent the credential from working.

Cardnumber - A calculated number not visible on the credential and only used for enrollment with the RAW format.

Issue Code - A tracking method to determine how many times a credential has been issued, only used with RAW format.

Format - A set of rules about the credential that defines how the system will interpret the credential's information. The format is normally found on the credential packaging or provided by the system installer to the end-user.

- If using NXT credentials, enter the imprint > set the card status to active > press **Done.**
- If using MS credentials, enter the imprint and facility code > set the card status to active > press **Done.**
- If using 26 Bit Wiegand credentials, enter the imprint and facility code > set the card status to active > press **Done.**
- All other formats are enrolled as RAW, enter the imprint and card number > set the issue code to the next sequential value, starting a 0 > set the card status to active > press **Done.**

Remove Credentials

To remove a credential from a Cardholder, find the credential in the list > press Delete > Press Confirm > press **Done.**

Situation Manager

Situation Manager is an advanced Doors.NET feature that implements Global Lock and Global Unlock commands. The icon for Situation Manager is only displayed if Situation Manager is enabled through Doors.Net. Situation Manager can't be enabled via the Doors.WEB™ client. The Situation Manager feature allows you to immediately lock or unlock a designated groups of doors, over multiple controllers.

NOTE: There are certain rules and limitations associated with Situation Manager when using the PXL controllers. These are covered in a separate document which can be accessed at the bottom of this page.

Situation Manager provides three level of global control:

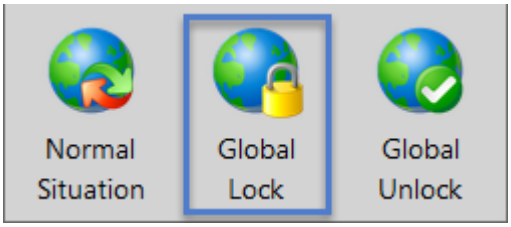
Situation Normal

Returns readers to their normal state – if they are online.

Global Unlock

Unlocks all readers on the system – if they are online.

Global Lock



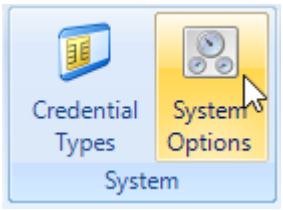
Locks all readers on the system – if they are online.

The following list describes how the Situation Manager implements Global Lock/Unlock:

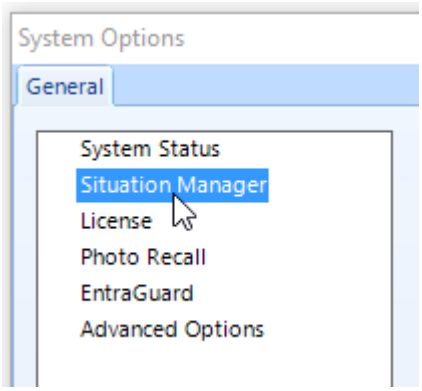
- When enabled, Doors.WEB™ displays a Situation Manager sub-group of icons in the program ribbon bar. These icons display current state and allow an operator to activate Global Lock, Global Unlock, or return to normal operating state.
- When a Global Lock command is initiated, designated doors immediately return to their normal, valid credential required state. All Auto-Unlock/ Lock Timezones are overridden, but all valid credentials will be granted access.
- When a Global Unlock command is initiated, designated doors are immediately unlocked.
- Global Unlock and Global Lock commands can operate over multiple controllers and over multiple gateways, even if they are different gateway types (for example, a site with NXT and PXL doors).

Enable Situation Manager

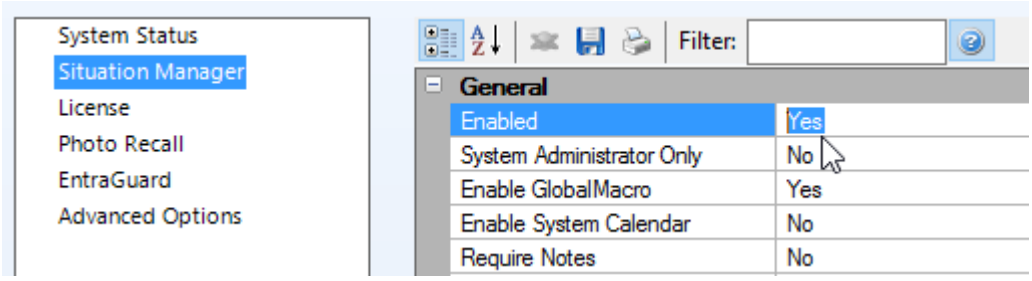
1. Log into the Doors.NET standard client.
2. Got to Setup >> System Options.



3. On the System Options window, click Situation Manager.



4. Within the General settings set Enabled to **Yes.**



5. In the **Global Configuration** section set **Hardware Control** to Software has Precedence.
6. Save the properties.
7. Return to the Doors.WEB™ client home page and you will see the additional Situation Manager icon.

Configuration Options

There are various settings and options for the Situation Manager feature, such as whether Global Lock has precedence or if Global Unlock has precedence, specifying if certain doors should not respond to Global Unlock/Lock commands and there are rules regarding the mandatory use of “Enter Reason for Change” and the minimum length of input are set from within Doors.Net, at a minimum the operator may optionally enter a message of any length. A message will display on all Doors.WEB™ clients as a timed pop-up in the bottom right corner to indicate a change in the Situation Manager has occurred. If a

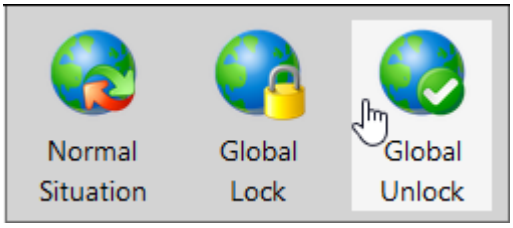
message is entered in “Enter Reason for Change”, the text will be displayed in Live Events.

Note: There are also a few implementation differences between the PXL controllers and other hardware platforms, for further details refer to the appropriate section in the standard Doors.NET online help or download one of the PDF documents listed at the bottom of the page.

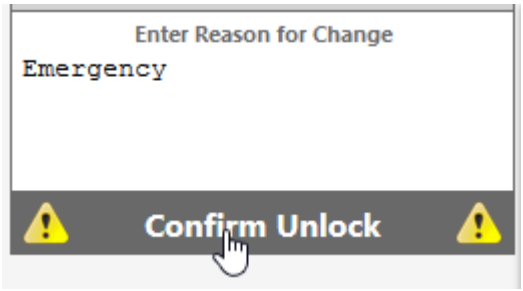
Using Situation Manager

To change the situation manager:

1. Press the required situation manager icon (Normal, Lock or Unlock).



2. Enter a message if required (or desired).
3. Press the confirmation button below the area for “Enter Reason for Change”.



Further Documentation

Doors.NET Global Lock and Global Unlock

Global Lock and Global Unlock Using PXLs