Systems

Downloads Registration/ Support Demos Development

Menu Patriot 6.4 Library

Tutorials
- ⊟ Patriot 6.4 Library
  - ⊞ Alarm Attendance
  - ⊞ Basic Client Maintenance
  - ⊞ Advanced Client Maintenance
  - ⊞ System
  - ⊞ Reports
  - ⊞ Security
  - ⊟ Tasks and Modules
    - ⊞ GSM Module
    - ⊞ SMS Gateway Module
    - ⊞ Email Module
    - ⊞ Escalated Messaging
    - ⊞ Mapping
    - ⊞ Telephony
    - ⊞ Dealers
    - ⊟ ICA
      - ▶ICA Installation.
      - ▶ICA User Setup.
      - ▶ICA Troubleshooting
      - ▶ICA 6.4 Upgrade
    - ⊞ Auto Dialler
    - ⊞ CCTV
    - ⊞ Tracking and Lone Worker
    - ⊞ Receivers
    - ⊞ IP Panels and Converters
    - ⊞ Other Tasks
    - ▶Tasks Overview.
    - ▶Task Settings
    - ▶Assignable Tasks.
    - ▶Instant Messaging Tasks
    - ▶Troubleshooting Tasks
  - ⊞ Installation
  - ⊞ Database Administration

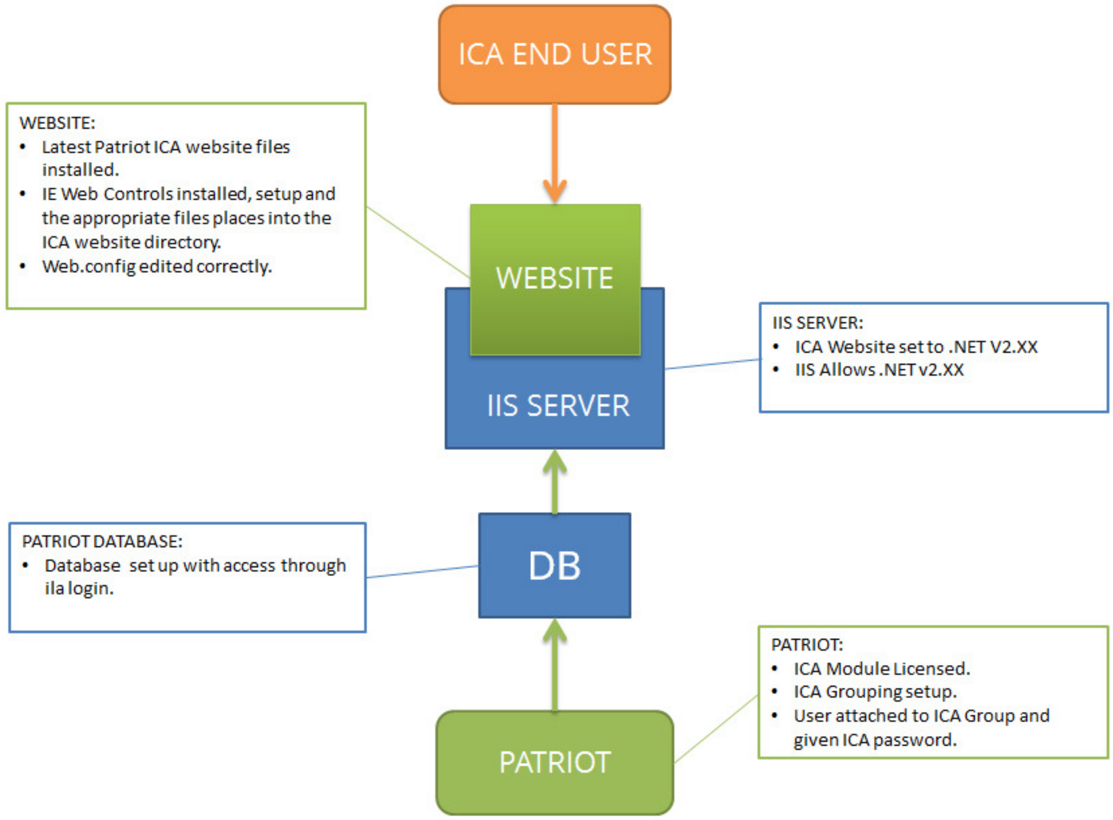
Printer-friendly version

Search Library

Patriot 6.3 Library
Patriot 6.2 Library

Internet Client Access (ICA) Installation

This document covers setting up the ICA module on your own webserver. If you are leasing the ICA module, contact Patriot for installation instructions.


ICA END USER
WEBSITE:
• Latest Patriot ICA website files installed.
• IE Web Controls installed, setup and the appropriate files places into the ICA website directory.
• Web.config edited correctly.
WEBSITE
IIS SERVER
IIS SERVER:
• ICA Website set to .NET V2.XX
• IIS Allows .NET v2.XX
PATRIOT DATABASE:
• Database set up with access through ila login.
DB
PATRIOT:
• ICA Module Licensed.
• ICA Grouping setup.
• User attached to ICA Group and given ICA password.
PATRIOT

Prerequisites

- Make sure that Patriot version is 6 or newer.
- Make sure Patriot 6 has been registered with at least one of the ICA modules. You can test this from the Database Administrator by going to Maintenance -> Users -> User Groupings. Edit a Grouping. Under Special Group Properties, you should be able to select Client Web Access.

Database Setup

Note: These procedures assume that SQL and the Patriot Server are on the same computer. If they aren’t, contact your software distributor.

Run the following script against the patriot database. Make sure you change the password in the script on the 3rd line to a strong password.

This will set up the login and password to the Patriot Database for the ICA Website to access and receive data from.

Make a note of this password.

```
EXEC sp_revokedbaccess 'ila'
EXEC sp_droplogin 'ila'
EXEC sp_addlogin 'ila', 'Str0Ng_Passw0rd','patriot'
EXEC sp_grantdbaccess 'ila', 'ila'
GRANT SELECT ON ActionPlan TO ILA
GRANT SELECT ON Attend TO ILA
GRANT SELECT ON CallChain TO ILA
GRANT SELECT, INSERT, UPDATE, DELETE ON Calllist TO ILA
GRANT SELECT, INSERT, DELETE ON CalllistUserGroupings TO ILA
GRANT SELECT ON Cities TO ILA
GRANT SELECT ON Countries TO ILA

GRANT SELECT, INSERT, UPDATE ON MZone TO ILA

GRANT SELECT, UPDATE ON Memalarm TO ILA

GRANT SELECT ON MemalarmBg TO ILA

GRANT SELECT, INSERT, UPDATE ON MUser TO ILA

GRANT INSERT ON OperatorLog TO ILA

GRANT SELECT ON OpenClosTimes TO ILA

GRANT SELECT ON PanelTypes TO ILA

GRANT SELECT ON Reason TO ILA

GRANT SELECT ON Reminders TO ILA

GRANT SELECT ON Signal TO ILA

GRANT SELECT ON States TO ILA

GRANT SELECT ON Tasks TO ILA

GRANT SELECT ON UserGroupings TO ILA

GRANT SELECT ON UserGroupingAP TO ILA

GRANT SELECT, INSERT, UPDATE ON UserToClient TO ILA

GRANT SELECT ON UserToUserGroupings TO ILA

GRANT SELECT, INSERT ON WebAccess TO ILA
```

You can test the script has run correctly by, still on the Patriot server, bringing up a command line prompt and enter osql –U ILA (or sqlcmd –U ILA) then entering the password.

This will log you into SQL. Type exit to exit out of SQL.

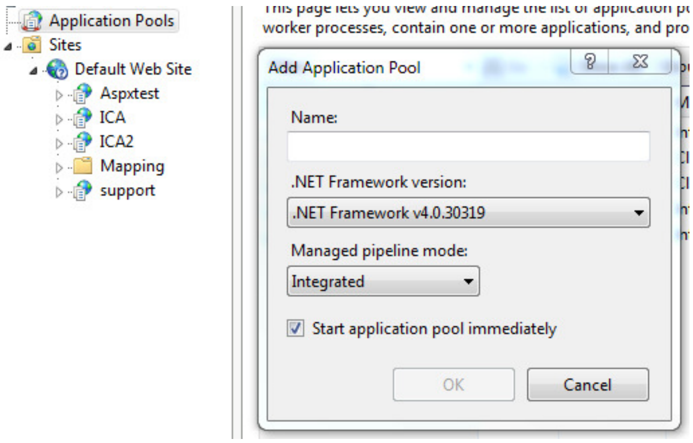
Server .NET Setup

All the following instructions are performed on the webserver, unless specified.

1. Install .NET framework (version 4) if it is not already present.

   You can check what versions of .NET are installed by running the Internet Information Servers Manager, Selecting 'Application Pool' and clicking 'Add Application Pool'.

   This will display a window with a dropdown box of available .NET version, this should included .NET v4.XX as shown below.



This page lets you view and manage the list of application pc
worker processes, contain one or more applications, and pro

Add Application Pool

Name:

.NET Framework version: .NET Framework v4.0.30319

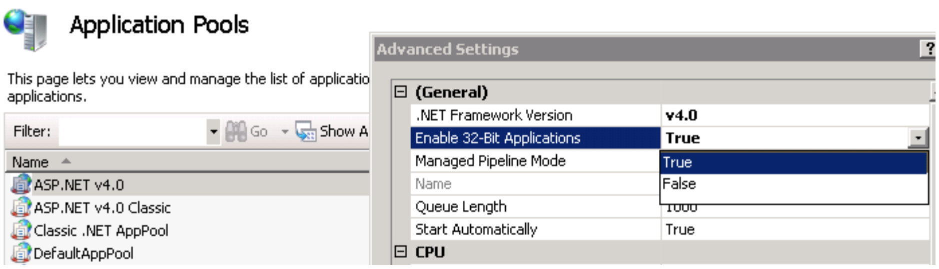
Managed pipeline mode: Integrated

☑ Start application pool immediately

   You can also check using Windows -> Add Remove Programs, .NET V4 should be listed under installed programs as Microsoft .NET Framework version 4.

   If you dont have .NET V4.XX installed download and install from www.asp.net

2. Enable 32 bit applications within your .NET Framework v4 AppPool:



Application Pools

This page lets you view and manage the list of applicatio applications.

Name
ASP.NET v4.0
ASP.NET v4.0 Classic
Classic .NET AppPool
DefaultAppPool

Advanced Settings

(General)	
.NET Framework Version	v4.0
Enable 32-Bit Applications	True
Managed Pipeline Mode	True False
Name	
Queue Length	1000
Start Automatically	True
CPU	

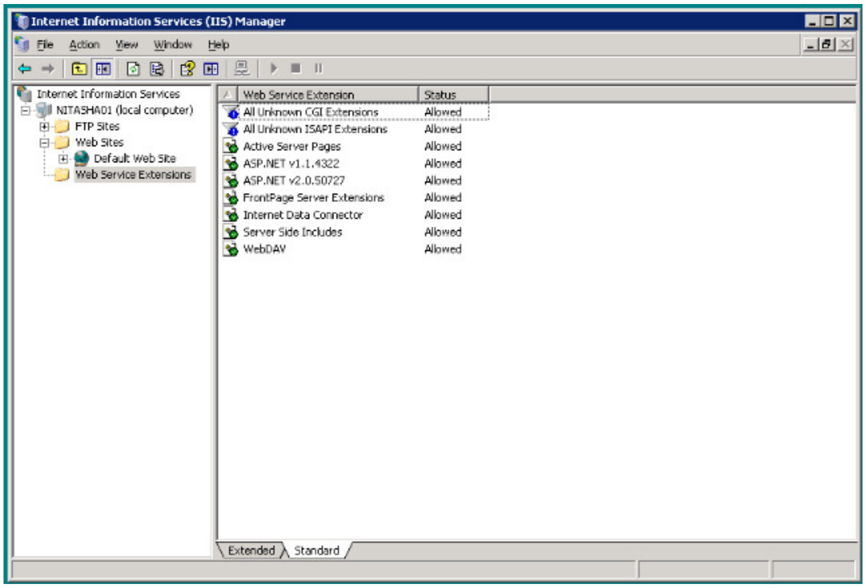
32-Bit Applications must be enabled within your ICA Application Pool for the latest ICA versions to run correctly.

3. Install the ASP.NET windows component. This will be listed and can be installed under add/remove programs --> add/remove windows components ("turn windows features on or off" in windows 7).

4. Reboot and check to make sure everything is installed by one of the methods listed above.

5. If you are using IIS v6 or v6.1 you need to make sure that ASP.NET v4 has status Allowed.

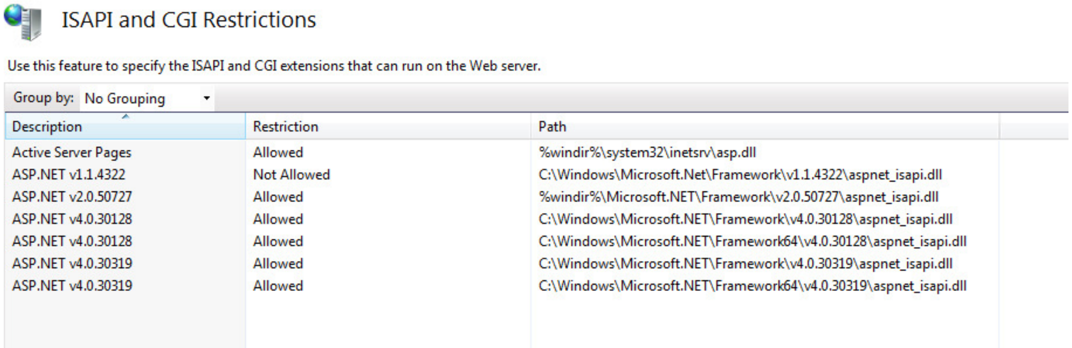
   In IIS v6 this setting is under Web Service Extensions:



Internet Information Services (IIS) Manager

Web Service Extension	Status
All Unknown CGI Extensions	Allowed
All Unknown ISAPI Extensions	Allowed
Active Server Pages	Allowed
ASP.NET v1.1.4322	Allowed
ASP.NET v2.0.50727	Allowed
FrontPage Server Extensions	Allowed
Internet Data Connector	Allowed
Server Side Includes	Allowed
WebDAV	Allowed

   In IIS v6.1, the setting is under ISAPI and CGI Restrictions:



ISAPI and CGI Restrictions

Use this feature to specify the ISAPI and CGI extensions that can run on the Web server.

Description	Restriction	Path
Active Server Pages	Allowed	%windir%\system32\inetsrv\asp.dll
ASP.NET v1.1.4322	Not Allowed	C:\Windows\Microsoft.Net\Framework\v1.1.4322\aspnet_isapi.dll
ASP.NET v2.0.50727	Allowed	%windir%\Microsoft.NET\Framework\v2.0.50727\aspnet_isapi.dll
ASP.NET v4.0.30128	Allowed	C:\Windows\Microsoft.NET\Framework\v4.0.30128\aspnet_isapi.dll
ASP.NET v4.0.30128	Allowed	C:\Windows\Microsoft.NET\Framework64\v4.0.30128\aspnet_isapi.dll
ASP.NET v4.0.30319	Allowed	C:\Windows\Microsoft.NET\Framework\v4.0.30319\aspnet_isapi.dll
ASP.NET v4.0.30319	Allowed	C:\Windows\Microsoft.NET\Framework64\v4.0.30319\aspnet_isapi.dll

Patriot ICA Website Install

1. Download the Patriot ICA Website install file (ICAInstall.exe) from the ICA downloads page on the Patriot website.

2. Create a folder under default website folder (usually c:\Inetpub\wwwroot by default) called 'ICA'. Run ICAInstall.exe and extract all contents into the ICA folder(C:\Inetpub\wwwroot\ICA).

3. 1. Run IIS

   2. Change settings on the ICA folder to application.

3. Click create, then set Execute permissions to Scripts and Executables, and Application Protection to Low.
4. If SSL certificate is installed, on Directory Security tab, under secure communications, click Edit, then tick on Require secure channel.

Setup ICA Website web.config

1. Go into the ICA folder, and find the file web.config (you may have to show system hidden files). Edit this file with Notepad.
2. **Set Site ID:** Replace xxxx (or the 4 digit number after key=") in the keys with a chosen 4 digit code. This will be your Site ID for your monitoring station and will be used when a user logs in to the ICA website as part of their username

   e.g.

   key="xxxxDBConn" *change to* key="1000DBConn"

   key="xxxxHomePage" *change to* key="1000HomePage"

   key="xxxxStationName" *change to* key="1000StationName"

   And so on. When a user in our example logs onto the ICA Website their username will be 1000 and then their Patriot User ID e.g. 10002049
3. **Connection Strings:** <add key="xxxxDBConn" value=" server=[Webserver IP Address];database=patriot;uid=ila;pwd=[ICA User Password]" />

   Replace [Webserver IP Address]with the ipaddress of the patriot server. Change [ICA User Password] to the password you gave the ila user.

   Use the same key value for the key "HostDBConn"
4. **Station ID:** <add key="xxxxStationID" value="[Your Company Name]" />

   Replace [Your Company Name] with your Monitoring station name. This name appears in web access log. Keep this under 30 characters in length.
5. **Home Page:** <add key="xxxxHomePage" value="[Your Home Page URL]" />

   Replace [Your Home Page URL] with station home page address. The page you wish your clients to go to on exit.
6. **Station Name:** <add key="xxxxStationName" value="[Company Name]" />

   Enter in your company name. This name appears in header of each page.
7. **Station Moto:** <add key="xxxxStationMoto" value="[Your Moto]" />

   This appears underneath Station name.
8. **Station Logo:** <add key="xxxxStationLogo" value="Images/[Image Name]" />

   Appears above station name in page headers. Include extension, eg Logo.gif
9. **Station Email:** <add key="xxxxStationEmail" value="[Station Email Address]" />

   Email address that feedback/change requests are sent to.
10. **Station Email Server:** <add key="xxxxStationEmailServer" value="[smpt server name]" />

    Replace with Stations smtp server.

    eg smtp.xtra.co.nz

    You must also add 3 additional key entries to configure email server authentication, as follows

    add key="XXXXStationEmailLogin" value=""

    add key="XXXXStationEmailPassword" value=""

    add key="XXXXStationEmailSSL" value="NO"

    If your email server does not require authentication, enter the keys as above, otherwise fill in the authentication details. SSL can be enabled by changing the SSL value to "YES"
11. **Show Header:** <add key="xxxxShowHeader" value="YES" />

    Make sure the following key exists. For now set the value to “YES”. If you wish to use your own header and footer files, you will need to change this to “NO”.
12. **Encryption**<add key="UseEncrypt" value="NO" />

    Make sure the following key exists. Leave the value as “NO” for now.
13. **Save changes to web.config**

Configuring ICA for Data Service Access

Some ICA functionality requires the web server to access the Patriot Data service. If the web server is located on the same machine as your Patriot Data service, or the connection between the web server and the Patriot server is on a secure internal connection, this communication doesn't need to be encrypted, so follow the Setup - Unencrypted. If the connection to the Patriot Data service is not via a secure internal connection then it is highly recommended to encrypt the connection, see Setup - Encrypted.

Setup - Unencrypted

The following keys must be added to the ICA config (web.config),

```
    ....

    <add key="1000ServerName" value="PATRIOTSERVER1" />

    <add key="1000ServerPortNumber" value="8001" />

    <add key="1000ServerUseEncryption" value="NO" />

    <add key="1000ServerDomain" value="" />

    <add key="1000ServerPassword" value="" />

    <add key="1000ServerUserName" value="" />

</appSettings>
```

Where 1000 should be replaced with your appropriate Station ID.

ServerName needs to be set to the address of the machine hosting the Patriot Data service. ServerPortNumber needs to the same port number the Patriot clients use to connect.

No further configuration is required.

Setup - Encrypted

The Patriot Data Service must first be configured so an encrypted connection can be made to it. A windows user also needs to be created to authenticate against. See Encrypting Communication.

The following keys must be added to the ICA config (web.config),

```
    ....

    <add key="1000ServerName" value="PATRIOTSERVER1" />

    <add key="1000ServerPortNumber" value="9001" />

    <add key="1000ServerUseEncryption" value="YES" />

    <add key="1000ServerDomain" value="EncryptedDomainName" />

    <add key="1000ServerPassword" value="EncryptedUserName" />

    <add key="1000ServerUserName" value="EncryptedUserPassword" />

</appSettings>
```

Where 1000 should be replaced with your appropriate Station ID.

ServerName needs to be set to the external address of the machine hosting the Patriot Data service. ServerPortNumber needs to be set to the encrypted service port used on the Patriot Data service.

Set UseEncryption to YES.

A windows user must be setup on the domain hosting the Patriot Data service. This user can have limited access as its only required to authenticate the password. This users credentials will be used to access authenticate access to the data service. Details of setting up this user, and configuring the data service are contained in the above link on Encrypting Communication.

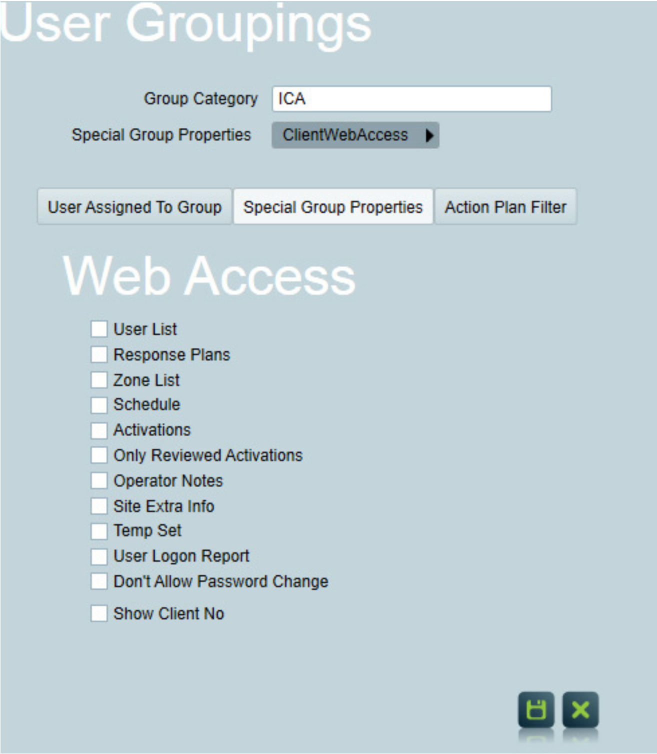
The values for ServerDomain, ServerUserName, and ServerPassword must be encrypted. The easiest way to do this is to use the Patriot Client. From the login window, edit the settings, set encryption on, and set Use Alternate Authentication. This will display the 3 entry boxes for domain, user, and password. Enter in your values here, then save. From the Patriot Client installation folder, open the config file, and copy the values for these 3 fields, as they will now be encrypted.

Patriot User Setup

Full documentation on ICA User groupings and access rights can be found in ICA User Setup. A quick summary is also provided in this section.

ICA User Access Group Configuration

1. In Patriot go to Maintenance -> Users -> User Groupings.
2. Add a new Grouping.
3. Name it appropriatly and give it Special Group Properties of 'ClientWebAccess' from the drop down menu.
4. You can also change Special Group Properties to allow or deny access to specific data.


User Groupings

Group Category: ICA

Special Group Properties: ClientWebAccess

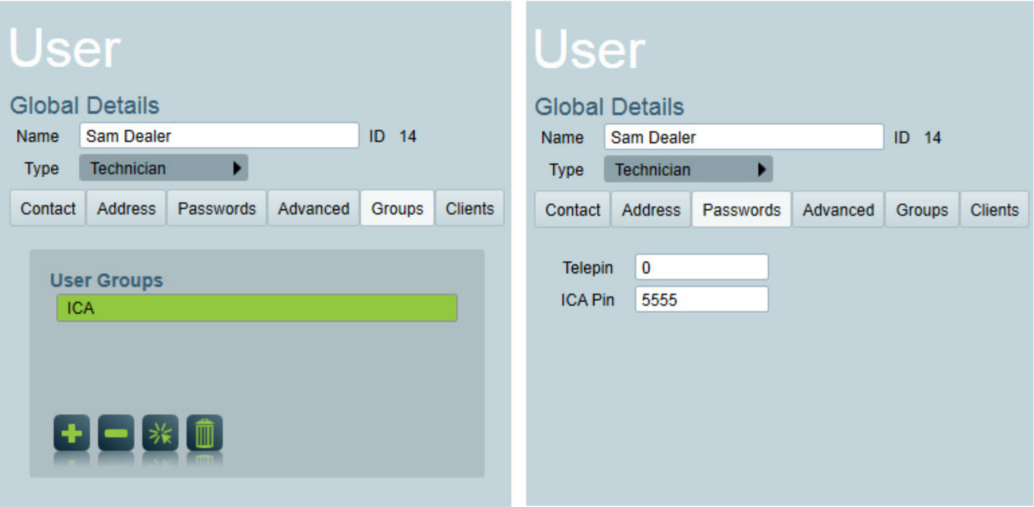
Web Access

□ User List
□ Response Plans
□ Zone List
□ Schedule
□ Activations
□ Only Reviewed Activations
□ Operator Notes
□ Site Extra Info
□ Temp Set
□ User Logon Report
□ Don't Allow Password Change
□ Show Client No

Creating a user group with ICA rights.

ICA User Configuration

1. Select a site User from the Users tab of a client file or directly with the User Maintenance tool
2. In the Global Details section, on the 'Groups' tab assign the new ICA Group you created.
3. On the 'Passwords' Tab enter a password in the ICA Pin input feild.
4. Take note of the USER ID.


User

Global Details

Name: Sam Dealer ID 14

Type: Technician

User Groups

ICA

User

Global Details

Name: Sam Dealer ID 14

Type: Technician

Telepin: 0

ICA Pin: 5555

Assigning a site user to an ICA grouping.

Testing the ICA Website

1. Open a web browser.
2. Go to http://[Your ICA webserver address]/ICA/memalarm3.aspx
3. In the User ID field enter the 4 digit code (you used in the web.config) followed by the user's User ID, then use the ICA Pin you entered for this user.

In our set up example the USER ID is 14 and the SITE ID we used was 1000. This would make the User: '100014' and the Paswword: '5555'.

Once logged in you will have access to the Site/Clients details that this user has been assigned to.

ICA Advanced

If you have the Advanced ICA module registered your users will have access to a number of advanced features including site user, alarm response and schedule maintenance. Each advanced ICA function has a corresponding security right which can be assigned to individual ICA access user groupings via Maintenance -> Users -> User Groupings within Patriot.

Additional Setup - Security, Language and Timezones

Encryption:

For additional security, the database connection string should be encrypted.

1. Go into the ICA folder, and find the file web.config (you may have to show system hidden files). Edit this file with Notepad.
2. Copy the value of the "HostDBConn" key
3. Startup a browser and login to ICA. Then enter the following URL into the address field of your browser,

   http://[ICA address]/ICA/TestEncryption.aspx

   This should display the Test Encryption Page. Paste the value of the "HostDBConn" key into the Data To Encrypt field. Don't include the " " around the conncetion string. Press the Encrypt button, this should display an encrypted string in the Encrypted Data field. Copy this string, then go back into the web.config file, and paste it into the value of the "HostDBConn" key and the "xxxxDBConn" key.
4. Alter the "UseEncrypt" key in the web.config file and change the value to "YES"
5. Save the changes to the web.config file. And test logging in to ICA.
6. Remove the file testencryption.aspx from the ICA folder, but keep a copy of this incase you need to change the value of the connection strings.

Regional Settings:

It is possible to change the regional settings to control how dates and numbers are displayed in ICA. To do this, edit the web.config file. Directly underneath the <system.web> line, add in a new line as follows:

<globalization culture="en-NZ" uiCulture="en-NZ"/>

Change en-NZ to whichever regional settings you require. Click here for a list of valid culture codes.

The regional settings can also be adjusted from inside Internet Information Services Manager. Select the ICA site in the IIS settings manager, and select .NET Globalisation. In this section you can select the required regional setting from a drop-down list.

It is also possible to attempt auto-detection of the users regional settings. This is useful if your users are from different regions and require different settings. To do this, set the culture to "auto" (Auto-Detect when using IIS Manager). When auto detection is being used, the users browser selects the regional settings used (if their browser supports this feature and is configured with the correct regional settings). To specify a fallback setting if the user browser doesn't support auto-detection, you can add a : and then the fallback culture name, e.g. culture="auto:en-NZ"

Timezone Support:

You must also add 2 new key entries to the web.config file, as follows

```
add key="XXXXDLSStart" value="0000"

add key="XXXXDLSEnd" value="0000"
```

where XXXX is replaced by your monitoring station ID. If you don't require time zone support, enter the keys as above. If you do require time zone support, 0000 can be replaced with the start and end dates of daylight saving for the monitoring station, in the format of DDMM

Modifying the Look

Due to the nature of ASP.NET, the logic and the display of ICA are kept quite separate. This allows the look of the website to be changed without altering the functionality.

Note: Experience with html, and possibly some experience of asp.net will be required to change to look of your website.

If you are going to make your own changes, please backup all files beforehand.

Below is the recommended way of changing the look of ICA:

- Go into the ICA folder on the web server. If a Patriot technician installed ICA for you, this folder can usually called ICA and can be found in the c:\inetpub\wwwroot\ICA.
- ICA uses master pages to apply a general layout to all pages.

There are 2 seperate master pages that define a standard template for all pages in the website. **ICA.master** (in the root folder) and**/Views/Shared/_Layout.cshtml**. The ICA website is being migrated from an older style to a new style, hence the use of two master pages. Here you can edit page headers, footers, and menus.

- You can stop ICA from automatically generating a header on each page by altering the web.config file, and changing the value of the key "xxxxShowHeader" to "NO". This will hide the default station logo, name, and motto displayed at the top of the page.
- **Stylesheets**

  The master pages references style sheets which can be used to customise the look and layout of ICA. These are found in the Scriptfiles subfolder.

  styles.css is the main stylesheet for ICA. This is divided into sections for headers, content, footers, tables, and responsive styling. The responsive section is used for changing the look of ICA for smaller screen sizes, such as for mobile phones.

  side-menu.css is a stylesheet for an optional side menu you can add your own links to.

  pure-min.css contains styling used for some of the page controls, such as buttons and forms. Visit purecss.io for documentation and examples of styles.

  font-awesome.css is used for the icons.

  pickadate: The files in this folder are used for the calendar control.
- **Choosing which fields to display on small screens**

  An example of this is found in Memalarm3.aspx: The external reference number field will be hidden on small screens.

  To achieve this, the following attributes are added to a field of the GridView control (attributes marked in green):

  ```
  <asp:HyperLinkField ItemStyle-CssClass="grid-detail-column"
                         HeaderStyle-CssClass="grid-detail-column"
                 DataNavigateUrlFields="ExternalRefNo"
                 DataNavigateUrlFormatString="signals.aspx?ExternalRefNum={0}"
                 DataTextField="ExternalRefNo"
                 HeaderText="External Reference No"></asp:HyperLinkField>
  ```

  You can add these 2 attributes to any GridView field, if you want it to be hidden on small screens. This way only essential information is displayed when screen space is limited. At higher resolutions all columns will show as normal.
- **Changing other aspx pages.**

  It is not recommended to edit any other pages within ICA. All other pages are likely to be updated by future patches. If you do change any other pages, it will be your responsibility to merge your changes in manually after each patch.