



“Powered by Nerv8 Future”

National Grid Gas Shipper User Guide

nationalgrid

**Issue: 15
Date: 30th April 2014**

Website URL's to use:

Primary Site access:- <https://www.s2.emergencycallsecure.com/newlogin>

In the event of system down-time or if a users faces issues please use:

Secondary:- <https://www.emergencycallsecure.com/newlogin>

Tertiary:- <https://www.s4.emergencycallsecure.com/newlogin>

CONTENTS

CONTENTS	2
DOCUMENT CHANGE RECORD.....	3
LOGGING INTO THE EMERGENCYCALL System.....	4
Unsuccessful Login Attempt.....	5
PASSWORD SECURITY SETTINGS.....	7
Expired Password.	7
Successful Login Attempt.....	7
RECIPIENT SECURITY GROUPS	9
Shipper Contact Devices.....	10
Applying (saving) Changes.....	11
GROUP MEMBERSHIP.....	12
PERMISSIONS.....	14
Unsecure passwords.....	14
Password memory	15
Opt In / Out functionality	15
HELP / SUPPORT.....	16

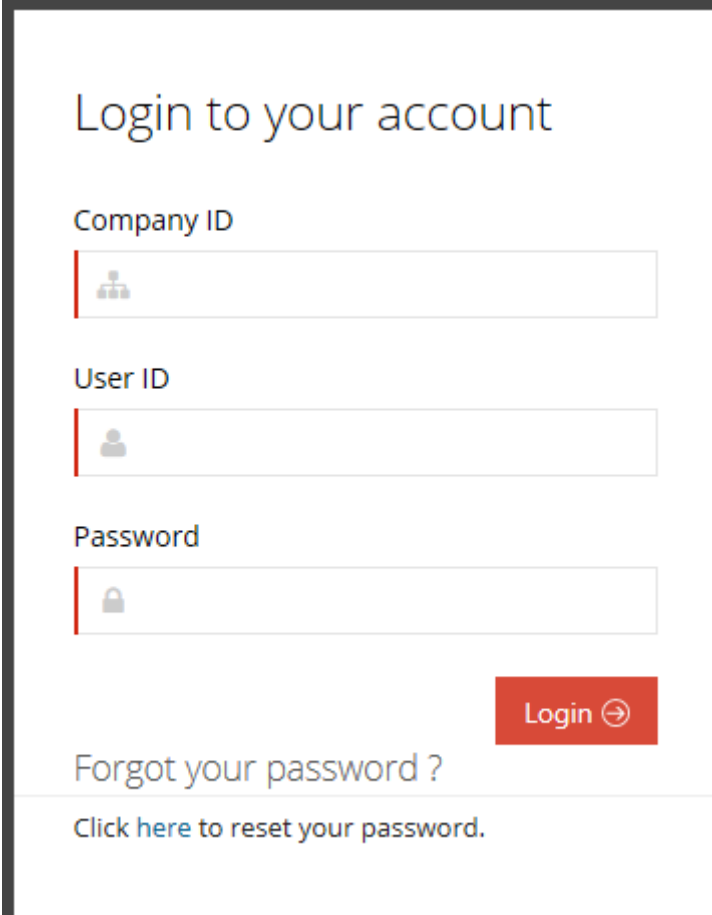
DOCUMENT CHANGE RECORD

Date	New Version Number	Changed By	Reason For Change
12/08/14	V 14.1	Christopher Beaumont	New NGGAS specific Administration Guide
09/09/14	V 14.2	G.Kilburn	National Grid update

EMERGENCY CALL ADMINISTRATION

LOGGING INTO THE EMERGENCYCALL SYSTEM

The EmergencyCall System is accessed via a web browser using the appropriate URL. If using the correct URL you will initially be presented with the following login screen:



The screenshot shows a login interface with the following elements:

- Title: "Login to your account"
- Company ID field: A text input box with a group of people icon.
- User ID field: A text input box with a single person icon.
- Password field: A text input box with a lock icon.
- Login button: A red button with the text "Login" and a right-pointing arrow.
- Forgot password link: A link that says "Forgot your password?" with "Click here to reset your password." below it.

In order to gain access to the system, enter the correct Company ID, User ID and Password.

Unsuccessful Login Attempt

If you input incorrect Login details, this will result in access to the system being rejected and the following warning will be displayed:

Invalid Login Login →

Forgot your password ?

[Click here](#) to reset your password.

If this happens then you should re-check your login details and attempt to login again. If you continue to experience a problem when logging in you should first attempt to use the password reset functionality (Click here to reset your password) which will open a “security captcha” enabling you to send a password reset email to your registered ‘primary’ email address, the primary email address is the 1st email address in the users contact list (see page 10).

Forgot Password ?

Company ID

User ID

sloter

(Refresh Image)

(Enter the characters shown in above image)

← Back Submit →

If you do not know the company ID or User ID then the password reset request will not work. If this is the case; or if any other problems persist then the issue should be escalated to the National Grid Service Help Desk see (0800-9177111) quoting ANS System or 'Active Notification System'.

If 3 unsuccessful login attempts are made in a 5-minute period, then you will be locked out of the system and will not be allowed access (even with a correct set of login details) for a period of 10 minutes.

Note: Number of permitted login attempts by default is set to 3 but this is configurable to match each individual client's specific requirements.

PASSWORD SECURITY SETTINGS

Expired Password.

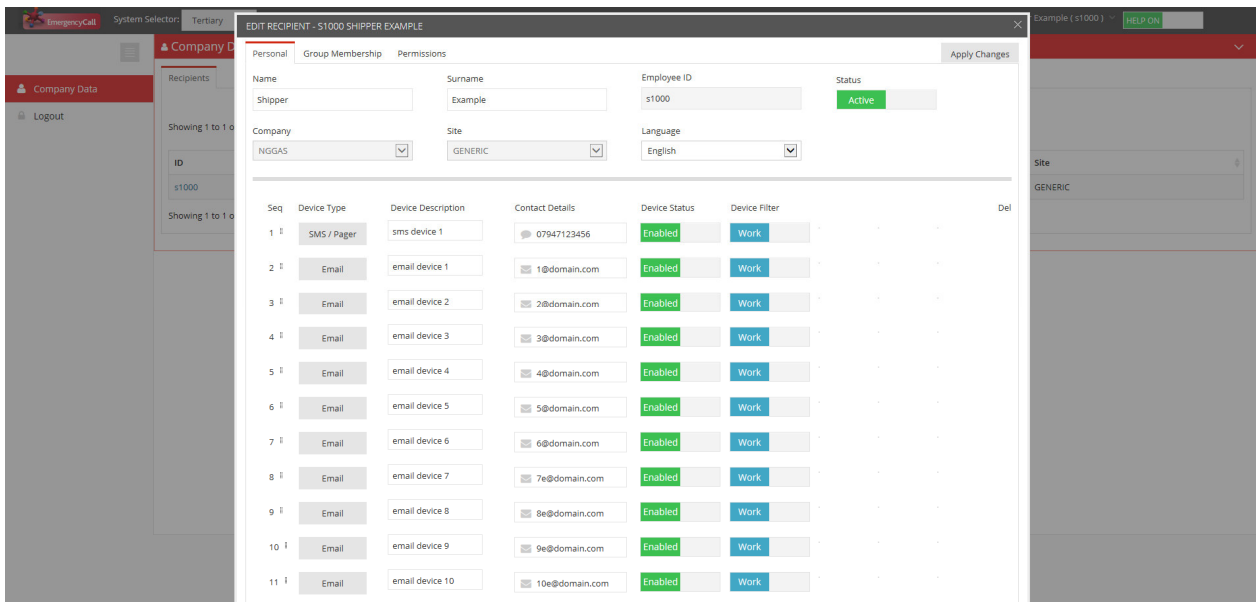
If it has been more than “90” days since your password was last changed then you will not be able to gain access to the system until a new secure password has been configured. When setting a new password you will not be permitted to re-use any of the last “5” passwords that are stored on the system against your user id by default.

Note: The values relating to the number of days and number of stored passwords is also configurable to match each individual client’s specific requirements (the values of 90 days and 5 attempts are default settings and are being used to describe the feature but your individual settings may be different to these).

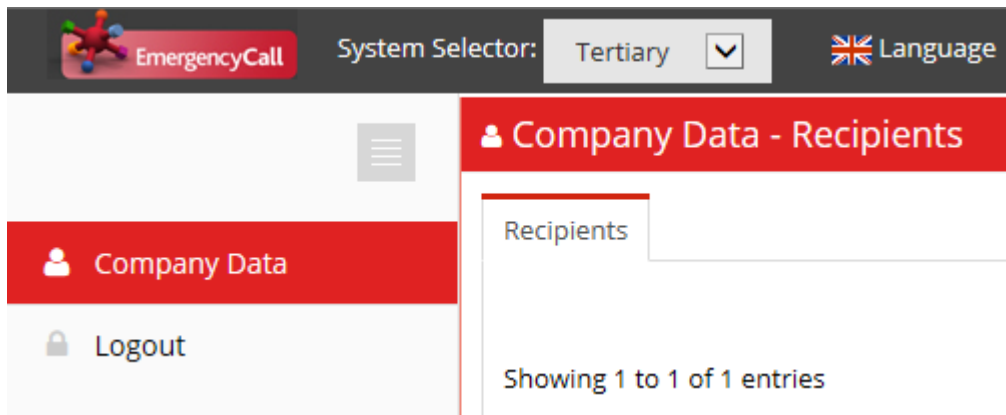
Successful Login Attempt

A successful login will provide access to the EmergencyCall System. After a few moments the system will be ready for use and the Home Screen will be displayed.

When logged in as a Shipper, by default the Shippers profile page will be launched ready for the user to edit their Device settings but if you have a higher security level then a different home screen may be displayed.

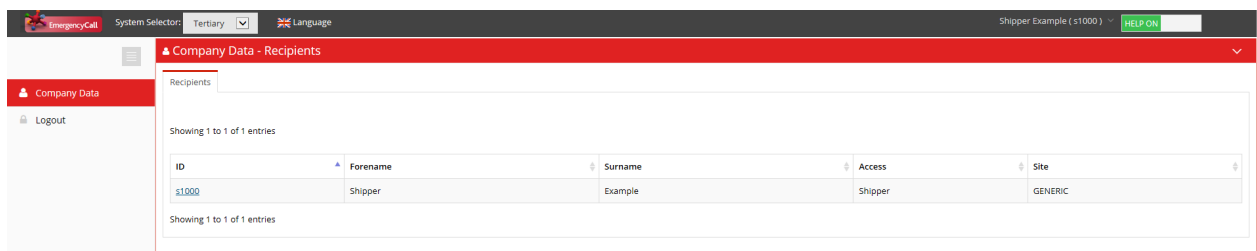


As a Shipper, if you close the device profile using the “x” in the top right hand corner of the open windows then you will only be able to select between 2 system functions:



1. Company Data (Shipper Administration)
2. Logout (Log Out of the System)

When Company Data is selected the user will see their details in the main administration window and can re-open their profile by clicking on their “User ID” entry (in the image below this is “s1000”)



When Logout is selected the user will be securely logged out of the system and returned to the main login page.

RECIPIENT SECURITY GROUPS

Recipients held within the EmergencyCall database are categorised within different security group levels. The security group associated with the Recipient will determine the functionality that can be accessed by them when they log on to the system via a web browser.

The “Shipper” security category is set up for you by the relevant National Grid System Administrator.

The Shipper security level enables a user to access the EmergencyCall system via a web browser and view / edit their own details (including contact devices) only. They will not be able to Initiate a Callout (Send an ANS message), add any new devices to the system, perform any further administration functions, or view the Reporting Suite.

The Shipper can ONLY administer their own details and check to find out which groups they are a member of.

The Shipper security level can:

- Update their Name and Surname entries.
- Switch their Status between Enabled and Disabled.
- Modify their active Device details
- Change their system web access password.

But they cannot:

- ADD any EXTRA devices to the system or perform any other kind of system administration.

SHIPPER CONTACT DEVICES

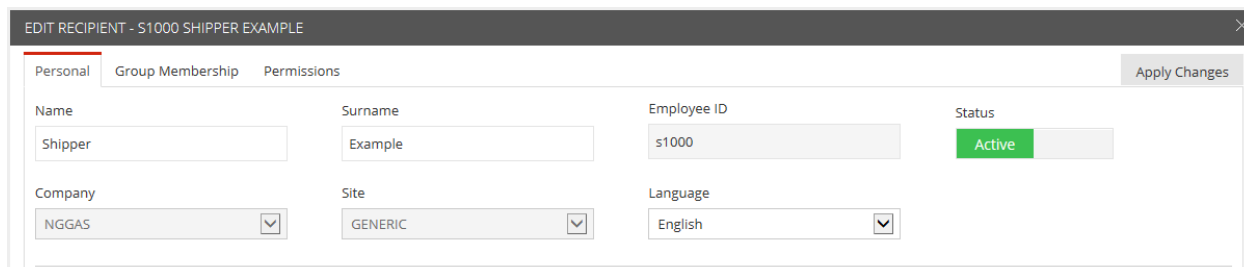
When a Shipper is added to the EmergencyCall system, their available device profile will have been pre-populated by a System Administrator at the National Grid with 1 sms device and 10 email devices.

Seq	Device Type	Device Description	Contact Details	Device Status	Device Filter
1	SMS / Pager	sms device 1	07947123456	Enabled	Work
2	Email	email device 1	1@domain.com	Enabled	Work
3	Email	email device 2	2@domain.com	Enabled	Work
4	Email	email device 3	3@domain.com	Enabled	Work
5	Email	email device 4	4@domain.com	Enabled	Work
6	Email	email device 5	5@domain.com	Enabled	Work
7	Email	email device 6	6@domain.com	Enabled	Work
8	Email	email device 7	7@domain.com	Enabled	Work
9	Email	email device 8	8@domain.com	Enabled	Work
10	Email	email device 9	9@domain.com	Enabled	Work
11	Email	email device 10	10@domain.com	Enabled	Work

- “Seq” controls which order the devices are contacted in.
- “Device Type” specifies the type of device to be contacted.
- “Device Description” is for your own internal use to describe the device.
- “Contact Details” is the most important field. This is where you specify the phone number you want the sms message sent to (for “SMS / Pager” devices) or the email address you want the email sent to (for “Email” devices.)
- “Device Status” controls if the device is Enabled or Disabled. If “Enabled” the device will be contacted during a callout, if “Disabled” the device will NOT be contacted during a callout.
- “Device Filter” is used for advanced filtering in some systems, but it is not used in callouts to shippers, for consistency this should be set to “Work”.

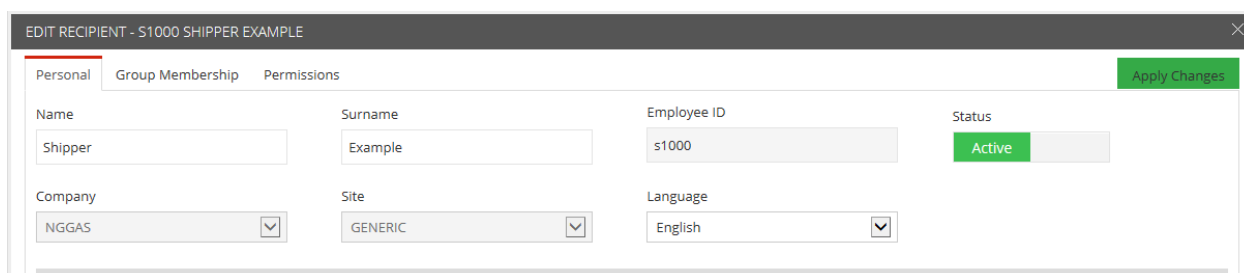
Applying (saving) Changes

If no changes have been made to the open profile then the “Apply Changes” button in the top right hand corner will be Grey.



The screenshot shows a web form titled "EDIT RECIPIENT - S1000 SHIPPER EXAMPLE". It has three tabs: "Personal", "Group Membership", and "Permissions". The "Personal" tab is active. The form contains several input fields: "Name" (Shipper), "Surname" (Example), "Employee ID" (s1000), "Status" (Active), "Company" (NGGAS), "Site" (GENERIC), and "Language" (English). The "Apply Changes" button in the top right corner is grey.

When a change of any kind is made to the open profile the “Apply Changes” button will turn green and you can save the changes made by clicking on the “Apply Changes” button.



This screenshot is identical to the previous one, but the "Apply Changes" button in the top right corner is now green, indicating that changes have been made to the profile.

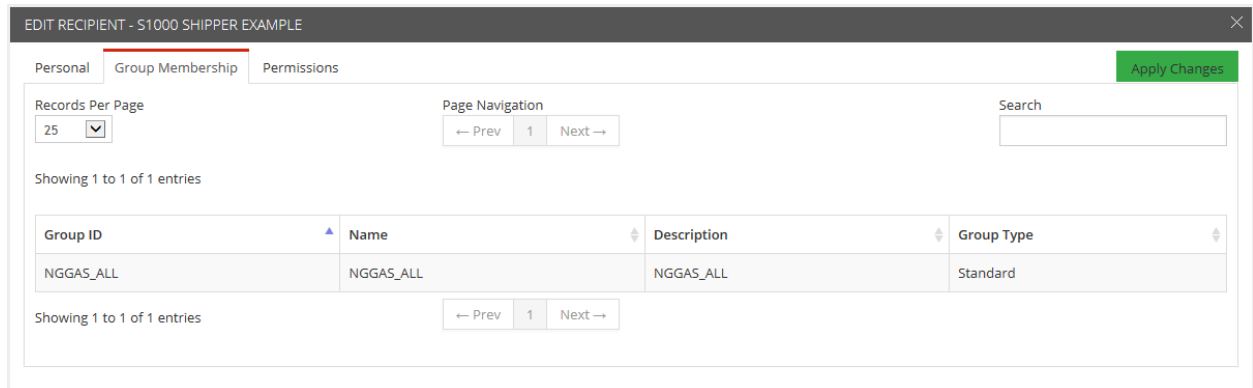
When the “Apply Changes” button is pressed the system will perform some basic validation to ensure that the data entered is in the correct format. Any obvious problems like a letter in a phone number or a missing @ symbol in an email address will generate a warning message to screen and the problems will need to be rectified before the changes made can be saved.

Seq	Device Type	Device Description	Contact Details	Device Status	Device Filter
1	SMS / Pager	sms device 1	07947abcdef	Enabled	Work
			Please enter a valid numeric entry		
2	Email	email device 1	1domain.com	Enabled	Work
			Please enter a valid entry		

When the changes have been correctly saved the button will turn Grey again to signify that the changes have been saved. If you want to exit without saving the changes that you made then you should NOT click on the green “Apply Changes” button and instead click directly on the “x” located just above the “Apply Changes” button to close the screen instead.

GROUP MEMBERSHIP

When logged in as a shipper it is possible to view the groups that you are a member of on the system. This data can be seen on the “Group Membership” tab within the active profile screen.

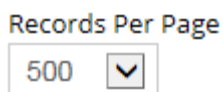


If the shipper is a member of multiple groups and all of the groups are not visible on screen at the same time then it is possible for the user to search for a specific group in the system database in two different ways:

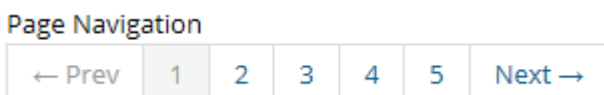


1. Navigation

Using the “Page Navigation” selector, you can scroll through the entire list of groups that you are a member of. Up to 500 Groups can be displayed on each page at any one time and the number of results is controlled using the “Records Per Page” dropdown option on screen.



To view the next page of groups you click on the “Next” button in the page navigator and to view the previous page of groups, click the “Prev” button in the page navigation list.



2. Searching

By entering a value in the “Search” field you can search specifically for groups that you are interested in locating with matching data in their profile.

A search for a group using a search entry of “port” will return Groups with an id of “Port123”, a name of “Cramport”, a description of “Portugal” etc ...:

PERMISSIONS

By default ALL of the permissions for Shippers are disabled apart from “Administration” which is enabled so that the shipper can log in and edit their own details on the system.

The only item on the Permissions screen which can be modified by the shipper is the “Web Access Password” which is used when logging into the User Interface.

EDIT RECIPIENT - S1000 SHIPPER EXAMPLE

Personal Group Membership **Permissions** Apply Changes

Security Level : Shipper User Group manager Client manager Inter - Site Manager Superuser

Web Access: Enabled Disabled Web Access Password

Administration callout Initiation

Inbound Voice: Disabled Disabled Disabled

Voicebank Listening Voicebank Recording callout Initiation

Unsecure passwords

Weak passwords are not permitted on the system. If you try to configure an unsecure password you will get the following “Weak” web access password warning and you will not be able to apply your changes to the system.



Web Access Password **Weak**

Clicking on the “eye icon” whilst entering a password will enable you to double check the value that has been entered before applying your changes.

The web access password, which is configured on the system, must be at least 8 characters in length and must contain at least 1 ‘alpha’, 1 ‘numeric’ and 1 ‘special’ character. An example of a secure password is **123?\$ab%c**.

As soon as an acceptable password has been entered the “Strong” web access password message will be displayed.



Web Access Password **Strong**

Password memory

When setting a new password, you will not be permitted to re-use one of the last "5" passwords that are stored on the system against your User ID.

If you attempt to reuse a password which has been used too recently then you will be prompted to change it to a different password instead.

Opt In / Out Function for daily, routine messages

When user is logged in they will see the following recipient screen:

Seq	Device Type	Device Description	Contact Details	Device Status	Device Filter
1	SMS / Pager	SMS	0700000000	Enable	Work
2	Email	email 1	test1@email.com	Enable	Work
3	Email	email 2	test2@email.com	Enable	Work

Navigate to tab: Opting In and Out

Device Type	Contact Details	DEM01	DEM02	UIOLI
SMS / Pager	0700000000	Enabled	Enabled	Enabled
Email	test1@email.com	Enabled	Enabled	Enabled
Email	test2@email.com	Enabled	Enabled	Enabled

User will see a list of their devices on the left and a list of message types across the top, the user has the flexibility to 'disable any messages types they do not wish to receive by device. They also have the flexibility to 'enable again if required later.

Once a change has been made the 'apply changes' in the top right will be green, please click to save, this will then turn back grey.



Daily routine messages that can currently be selected for opt in/out are:

DEM01: Demand Attribution has run for Gas Day DD/MM/YYYY

DEM02: Demand Attribution has run for Gas Day DD/MM/YYYY. Demand for D-1 is (*).

UIOLI: Indicative figures for release for Gas Day DD/MM/YY

CRITICAL SUPPORT

Raise a call via the 'helpdesk' on:

Telephone:

0800-9177111

Quoting ANS System or 'Active Notification System', a ticket will then be logged and passed for resolution to the support team. The support team will resolve in business hours; however users may request a password via the 'forgotten password' link (see pages 5 and 6).