

ENA G98/G99 Type Test Verification Register

Concise User Guide

1. Introduction

The core purpose of the system is to allow registered manufacturer users to submit details and supporting documents relating to micro generator and associated devices (up to 16A per phase) in terms of their compliance to ENA standards G98, G99 and G100. Restricted access to these device records is then available to all (anonymous) visitors to the site and unrestricted access is available to registered Distribution Network Operator (DNO) users and Independent Distribution Network Operator (IDNO) users. The system doesn't distinguish between DNOs and IDNOs in terms of permissions and they are generally all grouped under the term DNO within this document.

If you have any query or feedback regarding the system, please use the 'Contact Us' facility, which is available from the menu at the top of the screen. We undertake to answer all such queries/feedback within 24 hours.

The first version of the system went live on 10th December 2018. Development is ongoing and a second version was released during Q1 2019 to include improvements to registration, full system admin functionality and device alert functionality.

Due to a significant number of compliance issues in devices submitted to the system, ENA engaged WSP to assess device compliance starting in 2019. Compliance assessment is continuous, and the system was subject to modifications during the second half of 2020 to assist in the process. The most significant of these was the addition of a compliance status and compliance status comments to each device registration. This functionality is covered in some detail in section 4 of this document.

In September 2022, further modifications were implemented to introduce a new compliance status 'non-compliant for new installations' to capture device registrations that were previously compliant but became non-compliant on implementation of changes to the relevant standards. More information can be found in section 4 of this document. The system was concurrently modified to allow manufacturers to register their devices compliant to G100 in Great Britain.

2. User Access, Login and Registration

Device records can be browsed by anonymous users with two restrictions: manufacturers are able, at their own discretion, to flag any documents they upload against device records as 'Restricted' and these documents are only visible to DNO users, system administrators and users from the same manufacturer. The 'Full Compliance Status' (covered in detail later) is also unavailable to anonymous users and users from other manufacturers.

For this reason, registered users from manufacturers or DNOs should always log in to ensure they are viewing full device detail.

Manufacturer users can browse devices but will not have access to restricted data regarding other manufacturers' devices. All manufacturer users are also able to submit device records on behalf of their company.

DNO users can browse all device records and have access to all documents uploaded by manufacturers including those flagged as 'Restricted' as well as the full compliance status and compliance status comments. DNO users cannot submit device records nor amend or comment on them.

DNO (& IDNO) users can also be assigned 'Company Administrator' status by System Administrators. Company Administrators can maintain the list of users at their own DNO and can raise device alerts on devices with compliance issues. The alert functionality is described in section 6 of this document. Users should use the 'Contact Us' facility to request Company Administrator status or contact ENA directly.

DNO and manufacturer users should log in by selecting the 'Login' option under the 'Guest' drop down menu at the top of the screen.

DNO and manufacturer users who don't yet have an account should register by selecting the Register option from the Guest menu. All registrations are subject to approval by a system administrator before the account is validated.

System administrators have full access to the system and can publish/amend/version device records if necessary. They will generally only do so if the manufacturer is not able to for some reason.

3. Device data principles and system references

Once a device is published on the system, it can be subject to two forms of modification but under both, the original data is always preserved for audit purposes.

If there are errors or omissions in a registration, manufacturers can publish an amendment. If the device hardware, firmware or software has been modified or upgraded, manufacturers can create a new version. Whether the device has been 'versioned' or amended is clearly indicated by the system reference for the device.

Amendments should always be used when updating a device record to address the compliance issues of a device that has been assessed and assigned one of the non-compliant statuses. If a new device record is submitted for a device that has already been assessed and found not to be compliant, then it is likely that there will be delays in re-assessing the device.

System administrators can also 'Delete' device records. This makes them inaccessible to users browsing the system, but all data is retained for audit purposes.

The system reference for the first or original version of each device is always structured as follows:
MANUF/nnnnn/V1

Where 'MANUF' represents a five character abbreviation of the manufacturer name, which is set when the manufacturer is registered. 'nnnnn' is a system allocated unique number. 'V1' simply represents version 1.

If this is amended the system reference will take the form:

MANUF/nnnnn/V1/A1

Where the 'A1' represents the first amendment.

If a new version is submitted, the version number increments. Likewise the amendment number can increment so:

MANUF/01234/V3/A2

represents the second amendment of the third version of a device whose original system reference would have been MANUF/01234/V1.

If a new version is created from an amended device record, the version number increments but the amendment index is reset so, taking the example above, if a new version is created from MANUF/01234/V3/A2, the system reference of the new version would be MANUF/01234/V4.

The system reference therefore clearly represents a useful quick indication of the history of the device registration on the system.

4. Compliance Status

When a new device or an amendment or new version of an existing device is submitted to the system, it is always assigned the 'Awaiting Assessment' compliance status.

As the volume of devices being submitted to the site for assessment is very large, the current assessment lead time is 4-6 weeks. Devices are assessed strictly in order of submission and there is no fast-track option. The latest assessments are updated on the site twice per month.

Once assessed, one of the following **full compliance statuses** will be assigned:

- **Compliant:** This device and its respective documentation have been reviewed against G98/G99 and can be deemed as 'compliant'. This is to the ENA's **best engineering judgement** and is indicative only. DNOs retain the right to review the suitability of the device for connection to their network.
- **Compliant — on-site confirmation by DNO Required:** This device and its respective documentation have been reviewed against G98/G99 and the device can be deemed 'compliant' if confirmed on-site by the DNO. No further action is required by the manufacturer. In situ compliance may depend on other site-specific technical factors such as LoM protection. DNOs retain the right to review the suitability of the device for connection to their network.
- **Minor Non-compliance or Document Error:** Due to further assessment required, or documentation errors, the device cannot be declared 'fully compliant'. Please see the 'Compliance Status Comments' on the device record for more information. Once the comments have been actioned and documentation updated by the manufacturer, it will be reviewed again - in due course.
- **Non-compliant:** This device and documentation cannot be deemed compliant at this stage. Please see the 'Compliance Status Comments' on the device record for more information. Once the comments have been actioned and documentation updated by the manufacturer, it will be reviewed again - in due course.
- **Non-compliant for new installations:** This compliance status introduced in September 2022 captures device registrations that were previously assessed compliant but where the device

doesn't conform to requirements introduced in later issues of the standards. It was introduced for the Limited Frequency Sensitivity Mode – Over-frequency (LFSM-O) requirements that were implemented on 1 Sep 2022 but will also be used where future changes to the standards have the same impact on existing device registrations.

The list above shows the full compliance status, which is available to in-company manufacturer users, DNO/IDNO and System Administrator users. For anonymous users or manufacturer users browsing device records submitted by other manufacturers only the restricted compliance status is displayed: the two compliant statuses are displayed as 'Compliant'. 'Non-compliant' and 'Minor Non-compliance or Document Error' statuses are displayed as 'Further Information Required'. Status 'Non-compliant for new installations' is displayed in full for all users.

As well as assigning a compliance status, the assessor will provide Compliance Status Comments that are visible on the device record to users with access to the full compliance status. For non-compliant devices these comments will indicate what action is required to achieve compliance.

The compliance status and the compliance status comments (most relevantly, the reasons for a non-compliant assessment) are visible to manufacturer users for their own devices by finding the device on the main search screen once logged in and then, in the listed search results, clicking on the device reference to view the device detail. This will display the full compliance status and comments for devices submitted by the manufacturer the user is registered to. This information is suppressed for anonymous users and users registered to other manufacturers.

When updating a device record to address the compliance issues of a non-compliant device, manufacturer users should always issue an amendment. Creating a new device record so that the device is duplicated in the system will cause confusion and will likely result in delays re-assessing the device.

To issue an amendment, log in and, from the drop-down menu beneath your registered name, select Device Administration -> Live Device Registrations and then select the 'Amend' button against the device that needs updating. If the system states 'No Actions Available' in the Actions column, it is because a new version or amendment is already underway on the device. Go to Device Administration -> Pending Device Registrations to manage these. It may be necessary to delete a pending registration to re-enable the 'Amend' button on the device that needs updating.

See also more general guide on publishing device records in section 6 below.

Please use the 'Contact Us' facility to raise any query you may have regarding the compliance status.

5. Browsing devices

The Latest Devices tab shows the 20 most recently published device registrations, but it will generally be more effective to find or browse devices using the 'Find/Browse Devices' panel on the left of the home page.

As a general rule, we recommend that you start by entering a single search criterium and then refine your search by adding one or more criteria if too many devices are returned by the initial search. It is normally best to start with the manufacturer if this is known. Searches on the full model name can be unsuccessful. If you search on a long/complex device model, please try a sensible fragment of it

rather than entering the whole thing as it is likely to be differently formatted in the system as compared to promotional materials etc.

In the lists returned by this function, click on the System Reference link to display the full device detail. You can also search results ascending or descending by any column using the icon in the column header.

Browsing should be intuitive but anybody having difficulty with it should feel free to use the 'Contact Us' facility to request assistance.

6. Publishing device records

Only manufacturers and system administrators can publish device records. In practice, the vast majority (if not all) will be submitted by manufacturers.

To submit device records, you will need to be registered on the system. There is a link to the registration screen in the site introduction on the home page. If your manufacturer company is not already available on the system, follow the instructions to register the company at the same time as your user registration. Once a company is registered in the system, it can have an unlimited number of users. As a general rule, the first person to register becomes the company administrator and is then responsible for approving further user registrations.

Login as described in Section 2. Once logged in with manufacturer credentials, the device publishing options will be available from the drop-down menu beneath your name.

Use the 'Publish New Device Registration' to create an original (first) version of any device.

To amend or create a new version from an existing device, select 'Live Device Registrations' from the menu. Likewise, if you need to delete a device record from the system but, please note, deleted device records are no longer available on the site but are retained for audit purposes.

When submitting an amendment or a new version, please be absolutely sure that the distinction between these is correctly applied. Amendments only apply if there was an error or omission in the previous submission including updating the original if it was assessed as non-compliant. If the device has been updated in terms of hardware, firmware or software, please issue a new version.

It is possible to save registrations without publishing them. This enables them to be built and refined over a period of time. Pending registrations also available to all users registered at the same manufacturer so it is possible to construct registrations collaboratively with colleagues. Such pending or saved registrations are accessed via 'Pending Device Registrations' beneath your user name on the menu. Pending registrations are deleted after 90 days.

When uploading documents to the system, these can be flagged as 'Restricted' at the manufacturer's discretion. Restricted documents are only available to DNO users, system administrators and all manufacturer users registered to the device manufacturer. Restricted **PDF** documents that are not AES 256 (or later) encrypted or are less than 10 pages long are watermarked to further discourage unauthorised sharing. In addition, there is a strongly worded popup when downloading any document that the manufacturer has flagged as 'Restricted'. However, the ENA cannot be held responsible if DNO users ignore these warnings and share restricted documents.

If a new device record (either an amendment or a new version) is created from an existing device record with a live alert, the alert is inherited by the new device (see section 7 of this document for more on device alerts). Alerts are now deprecated in the system – they've been superseded by the compliance status functionality – see section 4.

Please refer to the user guide on the device publication screen and field tooltips when submitting device records whether new, amended or new versions of existing devices.

7. Device Alerts

The device alert functionality has been replaced by the compliance assessment functionality outlined in Section 4.

Device alerts can be raised by system administrators at the ENA and by nominated company administrators at each DNO/IDNO in order to share information about compliance issues.

The device alert functionality has been largely supplanted by the compliance status functionality but is still available in the system.

Device alerts are distributed by email to all DNO users, manufacturer users registered to the manufacturer of the device concerned and system administrators. Recipients will number 200+. The person raising the alert is named on the notification and when viewing the alert online.

Device alerts are not live until distributed. The device alert facility allows alerts to be refined and test emails to be sent to the person creating the alert prior to distribution.

System administrators and DNO/IDNO company administrators can also clear alerts but DNO/IDNO company administrators can only clear alerts that were raised by their DNO/IDNO.

DNO/IDNO company administrators must assign a contact to any alert or alert clearance that they raise. The contact can be a user from their DNO/IDNO including themselves or any other person entered on the alert screen following selection of '—Not In List —' from the Contact drop down box. System administrators are not obliged to assign a contact.

Attachments can be added to both the original alert and the clearance if required. Attachments added to the original alert will be distributed with the alert but not re-distributed with the clearance notification. Attachments added when clearing an alert will be distributed with the alert clearance notification.

Alerts are visible on online device records to all DNO/IDNO users, system administrators and users from the manufacturer of the device concerned.

It isn't possible to raise a new alert on a device with an existing alert but once an alert has been cleared, a new one can be raised.

If a new device record (either an amendment or a new version) is created from an existing device record with a live alert, the alert is inherited by the new device.

For company administrators, the device alert functionality is accessed via 'Create or Manage Device Alerts' under the user's name. For system administrators it is accessed from the list of live devices from the System Administration menu. Filter the list of devices as appropriate to include the device you wish to raise or manage an alert on and then click the appropriate button in the right-hand column of the list. Note that it is possible to begin both an alert and the clearance, save without distributing and return to them at a later date (via the 'Manage Alert; button) to complete and distribute them.

Please use the 'Contact Us' facility to raise any query you may have regarding device alerts.

8. Privacy and Cookies

All registered user data is held securely on the site and is never passed to third parties. No data regarding usage of the site is passed to third parties but it may be analysed internally at the ENA – generally in order to evaluate the popularity and efficacy of the system and to inform cost benefit analysis of potential improvements. No third-party data analytics is implemented on the site.

Session cookies are used in the site to retain data as the user navigates. This includes a user identifier and other non-personal information core to the user experience such as the last page or tab visited or viewed. These cookies expire when the user logs out. The only persistent cookie is the one that is used at login to prefill the user's email address. This facilitates login but serves no other purpose.

An additional cookie is used to validate the session to protect against session hijacking and fixation (forms of hacking). This cookie only holds an encrypted code, expires after one day and is automatically expired when you log out. It holds no personal/sensitive data.

9. Queries and Feedback

Please post a message via the 'Contact Us' facility from the main menu if you have any query or comment regarding the system including shortcomings. We will reply within 24 hours if the enquiry is legitimate and will address any serious issues as quickly as possible. Users are expected to have read this guide and shouldn't post queries on basic functionality described here such as how to register or search for devices.

10. Log Out

To log out, close your browser or select 'Log Out' from the drop-down menu beneath your name.