Var Group Service Portal
Operational Guide for IT Contacts

Key updates and operational guidance to prepare for the new support model

5 key points about the new support model

1. **The new channel for raising tickets**: the Var Group Service Portal will become the main channel for managing support requests. During the migration, requests will gradually be directed to the new portal, which will be the single point of access for raising tickets.

2. **Controlled access and authorised domains**: access to the service will be managed according to enhanced security and governance criteria. Only previously authorised users and corporate domains will be recognised. Requests from unregistered addresses or domains will receive an automatic message explaining the steps required to regularise access. Third parties may act on behalf of your organisation using a dedicated email address linked to your company's domain.

3. **Role of the IT Contact**: the IT Contact will play a central role in managing access to the platform. They will be involved in validating authorised corporate domains, checking registered users and approving any new registration requests, helping to keep the scope of enabled users accurate and up to date.
   a. Important: the initial configuration will not start from scratch. The user database will be populated using information already recorded in the previous Assyst platform, minimising the activities required during the transition.
   b. New corporate domains may also be added after the service has launched, subject to validation and approval by the client company's IT Contact.

4. **Portal access profiles**: two main access types are available, designed to meet users' different operational needs.
   a. Business User: access through a simplified interface, intended for users who need to raise and monitor their own support requests through an intuitive and straightforward experience.

b. IT User: access with features and views designed for the client company's IT contacts and managers, providing greater visibility of requests and advanced management tools.

User classification and the related permissions can be configured. If the profile assigned to a user needs to be changed or their permissions adjusted, an update may be requested through the dedicated support channels.

Main responsibilities of the Client IT Contact

The initial configurations for the new portal were prepared using the information and settings already held in the Assyst platform, with the aim of ensuring operational continuity and as seamless a transition as possible.
However, during the early stages after migration, some inconsistencies or items requiring refinement may emerge. For this reason, the main verification and alignment activities required of IT Contacts are set out below, together with the steps to take to report any issues to the dedicated migration support team.

Before go-live

Complete the data collection form received with the initial communication, which allows you to:

- Confirm or update all authorised corporate domains
- Confirm the approvers and responsible contacts authorised to approve new or unregistered users
- Specify the primary IT Contact and any secondary IT Contacts
- Identify the users who require an IT profile; all others will be configured as Business users
- Register automated systems that send emails to support
- Register suppliers and third parties authorised to raise tickets on behalf of the Client

During the transition

To support an effective move to the new portal:

- Share access instructions with users through the most appropriate internal channels
- Promote use of the Service Portal from the outset, encouraging adoption ahead of the gradual withdrawal of ticket submission by email
- Promptly report any issues relating to access, domains or user associations so that migrated configurations can be correctly aligned.

Once fully operational

Once the migration is complete:

- Approve self-registration requests through the defined process (using a token)
- Keep authorised contacts, domains and user accounts up to date
- Promptly revoke access for users who change role or leave the organisation, in line with the adopted governance model.

Managing users and access methods

Existing registered users

User accounts already held in the Assyst platform will be migrated automatically to the new Service Portal, retaining their association with authorised corporate domains and the main existing configurations.
Once migration is complete, users will receive an automatic communication containing the information required for their first access to the portal.

Access profiles

By default, users will be configured with a **Business** profile, designed for raising and monitoring support requests through a simplified interface.
IT Contacts, and any users identified by the organisation for specific operational needs, will instead be configured with an **IT** profile, which provides additional features and levels of visibility.

Registering new users

Users not included in the initial register may sign up independently through the **self-registration** process, which requires validation by the client company's IT Contact.
To complete registration, users must use the **company token**, a unique code associated with their organisation that Var Group will send to the primary contact once the data collection form has been completed.

- The IT Contact may decide on the most appropriate way to communicate the token to new authorised users.
- Using the token ensures that the user is correctly linked to their organisation and starts the approval process.
- Without a valid token, registration cannot be completed and it will not be possible to access the portal or raise support requests.

External users and authorised suppliers

To ensure that requests are correctly identified and the platform is managed more effectively, external suppliers and third parties should also use dedicated email addresses linked to the Client's corporate domain, rather than personal or generic addresses.

Adopting a standardised naming convention will:

- improve the identification and classification of support requests;
- make it easier to associate users with the correct organisation;
- help maintain orderly and consistent user management over time;
- simplify governance, verification and periodic platform clean-up activities.

For example, addresses such as the following may be used:

- external_nomecliente@dominio.it

- fornitoreX_nomecliente@dominio.it

For security and traceability reasons, generic or personal domains (for example Gmail, Outlook.com, Libero, Yahoo and similar services) will not be authorised for raising support requests.
Some external domains used historically may have been retained during migration to ensure operational continuity; however, alignment with the new policies is strongly recommended. For new activations and future access requests, preference will be given to dedicated user accounts that can be uniquely linked to the client organisation and to the parties authorised to act on its behalf.

The client company remains responsible for setting up any dedicated email addresses for authorised suppliers and for communicating their use to the third parties involved. This approach supports proper access governance and ensures that requests can be clearly traced back to the relevant organisation.

Further information

For further information and details, please refer to the dedicated FAQ section.

Var Group Support Center