

Basic Support Services



BESECURE provides a wide range of tools and resources to help you get the most from your products and ensure that any problems are resolved as quickly as possible.

Support Help Desk

Customers registered to BESECURE Support Services are provided an account to access BESECURE Support Help Desk Portal <https://support.besecuregroup.com> to submit online support tickets, track tickets status, review tickets history and access Frequent Access Questions Database. Each organization can register up to three technical support contacts that are allowed to submit support tickets.

BESECURE Support Help Desk Portal offers several options for viewing the status of your Service Requests.

- View your own Open Service Requests
- View History Service Requests
- View all Company Service Requests

Telephone Support

Specific telephone support numbers are provided from BESECURE. If calling outside business working days and hours an Automatic Call Distribution System will prompt you to authenticate based on your ADVANCED SUPPORT ID Number and direct you to a technical representative. Technical representative will require your contact details and email address. Within predefined time a case assignment will be generated and a Service Request will be provided to you either through phone or email

Remote Support

To the extent possible, and as requested by BESECURE, you may be requested to provide BESECURE or its authorized Technical Representative access to the affected network environment in order to remotely diagnose and resolve an issue. If access is not provided as requested by BESECURE, problem determination might be slower.

Escalation and response times

Depending on the severity level, BESECURE Support Program sets out clear guidelines as to how frequently you'll be contacted by our technicians about the status of a service request. Our Support Program also provides the maximum duration a Service Request can be open before it is automatically escalated to the next tier. BESECURE defines the "severity" of an issue based on how it impacts your ability to conduct business. A severity code is associated with all service requests, failures, and enhancement requests to indicate the impact and the urgency of the request.

Severity 1—Business has stopped

- Your organization cannot conduct business or business is severely impacted
- Reported Error with a direct security impact on the product
- Reported defect in the supported product in a production environment, which cannot be reasonably circumvented, in which there is an emergency condition that significantly restricts the use of the supported product to perform necessary business functions
- Inability to use the supported product or a critical impact on operation requiring an immediate solution.
- An issue in which the product causes your network or system to fail catastrophically or that compromised overall system integrity or data integrity when the product is installed or when it is in operation (i.e. causing a system crash, loss or corruption of data, or loss of system security) and significantly impacts your ongoing operations in a production environment and there is no immediately available workaround.

Severity 2—Business is severely impeded

- Your organization's business is impeded but can continue to operate
- An Error isolated to a specific functionality of the product, eg Administration, Policy Enforcement that substantially degrades the performance of the product or materially restricts business; e.g., major system impact, temporary system hanging;
- There are widespread symptoms across your organization's infrastructure
- Reported defect in the supported product, which restricts the use of one or more features of the licensed product to perform necessary business functions but does not completely restrict use of the licensed product
- Ability to use the supported product, but an important function is not available, and operations are severely impacted.
- Operations can continue in a restricted fashion, although long term productivity might be adversely affected.

Severity 3—Business is impacted, but your organization can function normally

- Your organization's ability to conduct business is not affected
- An Error isolated to a specific functionality of the product that causes only a moderate impact on its use; e.g., moderate system impact, performance/operational impact; Specific functionality is not working
- Reported defect in the supported product that restricts the use of one or more features of the licensed product to perform necessary business functions, while the defect can be easily circumvented
- Error that can cause some functional restrictions but it does not have a critical or severe impact on operations

Severity 4—Business is not affected, but there are noticeable problems

- Your organization's ability to conduct business is not affected
- Symptoms affect only a few systems
- Reported anomaly in the supported product that does not substantially restrict the use of one or more features of the product to perform necessary business functions; this is a minor problem and is not significant to operation
- Anomaly that may be easily circumvented or may need to be submitted to Vendor as a request for enhancement.

Severity 5—Requests for information or feature modifications

- Requests for product documentation or other information that does not require troubleshooting and issue resolution

Support request are escalated from Tier I up to Tier III support level within specific timeframes based on support request severity.

Tier 1 Support

“Tier 1 Support” means the ability to provide general pre and post-sales product information; hardware and software configuration; questions on upgrade Support; collect relevant technical problem identification information; perform base problem determination; provide basic Support on the standard products, protocols and features; replace Field Replaceable Units (FRUs) or whole Hardware units.

Tier 2 Support

“Level 2 Support” means the ability to provide Level 1 Support plus the ability to resolve the majority of misconfigurations, troubleshoot and simulate complex configuration, hardware, and software problems; perform Hardware diagnostics to determine Hardware malfunction; support problem isolation and determination of product specification defects; provide lab simulation and interoperability and compatibility testing for new software and hardware releases prior to being deployed into a Customer production network; define an action plan; provide advanced Support on all products, protocols and features; have the ability to analyze traces, diagnose problems remotely, and provide Customer with complete steps to reproduce a problem.

Tier 3 Support

“Level 3 Support” means the ability to provide Level 1 and Level 2 Support plus the ability to provide product enhancements such as patches and Hotfixes, fixing or generating workarounds that address software bugs; troubleshoot bugs that were not diagnosed during Level 2 Support; work with Customers to resolve critical situations, and building action plans with Customers to address complex issues.

Response Times based on Tier Level and Severity

Severity Level	Acknowledgement and case assignment	Tier 1 Response	Tier I Escalation to Tier II	Tier II Escalation to Tier III	Customer Status Updates
Severity 1	Within 15 Minutes	Average under 30 minutes	30 minutes	4 hours	Continues communication
Severity 2	Within 15 Minutes	Average under 2 hours	2 hours	8 hours	Hourly
Severity 3	Within 15 Minutes	Average under 8 hours	3 days	5 days	Daily
Severity 4	Within 15 Minutes	Average under 1 business day	10 days	15 days	Weekly
Severity 5	Within 15 Minutes	Average under 2 business days	15 Days	20 Days	Every two Weeks

About BESECURE

BESECURE provides compliance services based on legal and regulatory requirements, designs and implements advanced IT security solutions, delivers information security training seminars, provides Managed Security Services, performs Penetration Tests and Vulnerability Assessments covering all phases of the life cycle of information security. BESECURE adapts HISP Institute methodology for the implementation of a Holistic Information Security framework and employs the most HISP Certified Professionals among Greece and Balkans.

