
Acronis DeviceLock Data Loss Prevention Support Guidelines for Customers

Contents

INTRODUCTION	3
SERVICE OVERVIEW	3
SCOPES OF SUPPORT.....	3
<i>Items Out Of Scope of Acronis Support.....</i>	<i>4</i>
SUPPORT LEVELS.....	4
<i>Basic Support Level.....</i>	<i>4</i>
CASE SEVERITY DEFINITIONS	4
BASIC SUPPORT LEVEL OBJECTIVES. RESPONSE TIME.....	5
CASE RESOLUTION.....	6
<i>Customer Cooperation.....</i>	<i>6</i>
<i>Actions before contacting Support</i>	<i>6</i>
<i>Contact Acronis Support</i>	<i>6</i>
<i>Case Resolution Policies.....</i>	<i>7</i>
<i>Escalation</i>	<i>8</i>
ACRONIS SUPPORT	8
FREE SUPPORT RESOURCES	8
<i>Acronis DeviceLock DLP Support web page https://www.acronis.com/en-us/support/protect/dlp/</i>	<i>8</i>
<i>Knowledge Base</i>	<i>8</i>
<i>User Guides.....</i>	<i>9</i>
<i>Acronis Community.....</i>	<i>9</i>
<i>Acronis DeviceLock DLP upgrades</i>	<i>9</i>
PRODUCT LIFECYCLE AND TECHNICAL SUPPORT	9

Introduction

Acronis is committed to provide world-class customer service and support.

This guide provides information about Acronis DeviceLock DLP customer support services, policies, and procedures. We recommend that our customers review this Guide in its entirety to ensure the effective utilization of all aspects of their relevant support plans and features. It can help in locating appropriate resources, tools and information that will aid in resolving any issues with our products before they become problems.

This guide is also the Support Level Agreement and contains a description of the terms of technical support, valid for Acronis DeviceLock DLP Customers worldwide.

Service Overview

Scopes of Support

To ensure that our customers are successfully achieving their business objectives with Acronis DeviceLock DLP, Support Team is intended to assist, troubleshoot, and resolve specific issues resulting from the use of DeviceLock DLP on supported platforms with all prerequisites met.

Acronis Support Team provides the expert level guidance and troubleshooting related to any questions and issues:

- Installation;
- Configuration;
- Usage;
- Providing workarounds and bug fixes for technical issues;
- Providing access to actual releases of Acronis DeviceLock DLP as Acronis Software.

Acronis reserves the right to request that a Customer upgrade to the most current software version to proceed with resolving a problem or technical issue, if there is no known solution to the problem for the Customer's current version and the problem has been recognized and resolved in newer versions of DeviceLock DLP software. The provision of technical support does not imply that Acronis will fix software defects or make changes to the software.

Data of a technical nature required by Support Team to problem diagnosis and solving means log data (logs) generated by the OS or utilities provided by Acronis or other software vendors, memory dumps of problem computers, software configuration reports, etc. Acronis will use this data exceptionally to provide the solution for the declared problem. Acronis guarantees confidentiality and the impossibility of transferring such data to third parties.

The following items are not generally supported:

- Continued support for issues, which Acronis has provided corrections not implemented by the customer or technical data requested from the customer but not provided;
- Enhancement requests;
- Beta versions of DeviceLock DLP software.

Acronis provides support service in English only.

Items Out Of Scope of Acronis Support

The following activities are excluded from Acronis Support Team obligations:

- Product administration activities: remote assistance with initial software setup or upgrade, defining / setting up DLP policies, other activities described under deployment/user guides.
- Infrastructure setup/administration activities with Operating systems, Databases and any other 3rd party software and appliances, virtual environments.
- Writing additional requests/scripts – any kind of customization or integration outside standard Acronis Software functionality;
- Product Training or Consulting: Acronis Support Team does not provide training or consultancy services as part of the Acronis Support program, but Acronis does offer you as optional services at additional fees as part of the Professional Services program. Please contact our Professional Services Team for additional training and other consultancy requirements.
- Gathering and analyzing Customer’s requirements, understanding how they can be addressed.

Support Levels

Acronis offers different Support Levels designed to fit the needs of different customer categories from Small/Medium businesses to Enterprise.

Basic Support Level

Basic Support includes assistance with DeviceLock DLP as declared in the **Scopes of Support** section of this Guidelines.

Basic Support includes Online Helpdesk services, web access to Product Upgrades, Online User Forum, Product Documentation, FAQs, and Knowledge Base as described in the **Acronis Support** section of this Guidelines.

Case Severity definitions

Support case severity levels are specified by Support specialist during case review based on the business impact description of the problem or issue. The table below outlines the available severity levels of support requests with their definitions and examples.

Acronis Support Severity Definitions		
Severity	Definition	Examples
Sev. A (Critical)	The DeviceLock DLP product or its component is non-operational, several or all major features are affected. Customer’s critical business operations are affected. No workaround available.	<ol style="list-style-type: none"> 1. Protected workstation performance critically affected (BSOD, OS unable to start). 2. DeviceLock fails to correctly operate on certain hardware devices
Sev. B (High)	Major DeviceLock DLP product function or feature affected. Customer performance regarding their job functions is severely limited. Workaround exists but it does not resolve the problem to a reasonable extent in most cases.	<ol style="list-style-type: none"> 1. DeviceLock affects on from proper functioning of other software. 2. Lost credentials for a DeviceLock Administrator account with „DeviceLock Administrators“ functionality activated.

<p>Sev. C (Medium)</p>	<p>Problem impact is medium: customer performance or business processes are mostly unaffected. Irregular Problematic behavior happens only under specific conditions and/or environment. Workaround exists that resolves the issue to a considerable extent. There is no urgency in addressing the issue.</p>	<ol style="list-style-type: none"> 1. Lacking or invalid system settings/services required by DeviceLock DLP. 2. Undocumented DeviceLock product behavior or inaccurately documented feature. 3. Intermittent product issues that happens irregularly at specific conditions.
<p>Sev. D (Minor)</p>	<p>Minimal or no business impact. No workaround required. Customer service, pre-sales, website-related queries; minor usability and GUI issues; how-to questions, product information (functionality, requirements, setup, etc.) requests.</p>	<ol style="list-style-type: none"> 1. Product enhancements requests. 2. Usage questions. 3. Cosmetic issues with Product GUI or features.

The severity of a support case may be changed downwards by the Support Team during the case resolution process because of the following developments:

- If a temporary or workaround solution is provided to mitigate the material impact of the problem.
- If it is found that the customer has not studied DeviceLock DLP documentation enough when the case relates to the improper use of the product.
- If the customer does not properly engage in the case resolution process.

Basic Support Level Objectives. Response Time.

Acronis understands the importance of responsiveness and fast resolution times in case of a technical error. The following table describes response metrics (Basic Service Level Objectives) applicable to the Acronis DeviceLock DLP software at Basic Support Level. Incidents caused by third-party software are not subject to these response metrics.

Acronis Support Team will apply all reasonable efforts to meet the level objectives regarding remedial software support, and it will make a continuous effort to resolve Severity 1 support cases. Please be aware that the following targeted response times are intended for setting mutual expectations and not indicative of issue resolution times.

Customers may be required to provide additional technical information regarding their support cases to facilitate the resolution process. When requested by Acronis, it is expected that Customer will do prompt and full cooperation in providing any necessary information and performing necessary tests. Any access delay may impact Support Team's efforts to provide relief within the SLO targets specified.

Case Severity	Initial Response ¹	Status Update Frequency ²
Critical (Severity A)	12 hours	Once per business day
High (Severity B)	24 hours	Once every 2-3 business days
Medium (Severity C)	36 hours	Once a week
Minor (Severity D)	48 hours	Once a month

¹ Initial Response in particular indicates the time spent/taken for the Support Team to contact (reply to) the client via Online Helpdesk service, email or by any other means aimed to prove the beginning of the issue resolution process, collecting the necessary information about the issue and the steps to reproduce it, as well as providing the consultation on the request, etc.

² Status Update Frequency is the frequency with which Acronis Support Team will update Customer on their open support cases. This frequency may be extended by mutual agreement between the customer and Acronis Support Team.

Case Resolution

Customer Cooperation

Resolving technical issues requires a cooperative partnership between the customer and the Acronis Support Team. Customers are expected to actively cooperate with the Support Team during their case resolution process by timely responding to relevant questions and performing other required actions (e.g. gathering additional diagnostic information).

Acronis Support Team reserves the right to downward the severity of a support case may during the case resolution process because of a temporary or workaround solution is provided to mitigate the material impact of the problem, or the customer does not properly cooperate in the case resolution process.

Actions before contacting Support

Before contacting Support Team customers are required to complete the following steps:

- Clearly define the problem or question
- Try to identify possible sources of the problem
- Gather environment, product and diagnostic information
- Study product documentation and self-support resources available at the Acronis website.

Contact Acronis Support

Best practices for contacting Acronis Support are:

- Each case must follow the formula "1 technical issue = 1 ticket". If the case is resolved, it should be closed even if you have new questions or issues – you should create new cases instead of continue to post messages into the existing case.
- To initiate a new support request, please follow the instructions given [in the Knowledge Base article](#).
- Please provide a detailed issue description and diagnostic information, if possible.
- Each incident has a unique identification number, named "Case Number". You may be asked to reference this "Case number" for all future correspondence with Support until resolution.
- You can track and browse all your cases submitted to Acronis Customer Central under your Acronis Account.

Please have the following information available before contacting Acronis Technical Support:

1. Define the issue:
 - Explain the symptoms of the issue;
 - Provide error messages or error output associated with the issue, if any;
 - Describe steps to reproduce the issue;
 - Attach screen shots of the issue you are facing, if possible.
2. Determine the business impact:
 - Describe how the issue affects your system and your ability to meet your business needs;

- Define how many users/machines are affected / whether strategic end-users are affected.
3. Provide relevant information:
 - Installed DeviceLock DLP components and build number;
 - Explain if the issue occurred before or if this is an isolated incident;
 - Explain what occurred before the issue was detected;
 - List the hardware, software or other environmental changes recently made to the system, if any.
 4. Additional Information:
 - Provide environment details (OS, network configuration, etc.);
 - Share troubleshooting steps already performed / KB articles used.

A Support Case will be opened once the product is identified, the Customer's support contract or software license is verified, and the Case Severity level is defined.

Case Resolution Policies

For all customer support cases, Support Team implements a FIFO-based procedure, which also considers the customers Support Level and the Case Severity to prioritize its processing.

Any cases from non-registered customers, cases without valid Software licenses or Trial license are registered and processed with a lowest Case Severity.

Any cases from customers having expired Software licenses, are registered, and processed with a lowest Case Severity. Acronis reserves the right to request that the Customer renews the license and maintenance. Otherwise the case can be closed, or support level can be limited to consultations on general issues only.

Case Relief

Based on the information collected during problem identification and replication, Support Team tries to provide "relief" for the problem. Relief is defined as the answer to customers question or, in the case of a product issue, a temporary fix, a workaround (configuration changes, temporarily turning off non-critical product functionality) or an action plan to get the product in question up and running. In the event relief cannot be determined during initial response, research will continue off-line and will include additional research and testing. Once relief is provided and confirmed by the customer, Support Team will downgrade the Case Severity level.

Case Resolution

Case Resolution is defined as a permanent solution to a customer problem. The relief provided to the customer problem may also be the solution that resolves the problem completely. Given the customer confirmation has been received, the case will be closed.

If relief is delivered and it has not resolved the problem, Support Team will continue research until case resolution is found and delivered so the customer confirms that it resolves the problem, at which time the case will be closed.

For some product defects, a permanent solution may be available in the next minor product build. Also, custom workarounds may be developed to circumvent a product defect that will not be included in future builds or releases; in such cases, these workarounds will be considered a permanent resolution.

Criteria for Closing Cases

Support cases will be closed when one of the following events occurs:

- Support Team has provided a solution that the customer has confirmed resolved the problem.
- Customer initiates case closing.
- A workaround is provided.
- A product defect is identified, and the activity on this case is postponed until a build or release containing the fix for the problem is delivered. Customers shall confirm that the problem is resolved before the case will be closed.
- A documentation defect is identified and delivered to Product Engineering.
- The case has been caused by an inconsistency in a 3rd party product.
- No response from the Customer on three or more messages over a one-week period.
- The issue is out of the Support Scope.
- The issue is identified as a desired product feature that is not currently supported by the product. This case is then converted to a request for enhancement and submitted to Product Engineering for possible implementation in a future release. A relevant notice is sent to the customer and the case is closed.
- The Customer refuses to renew maintenance (license) when it is expired.

Escalation

The Technical Support Specialist, which is assigned for a case, should be the first individual to receive all customer concerns and issues. The Specialist will review the customer problem and situation and will either provide information about the customer's concern or transfer the problem to the correct internal department. If after interaction with the Technical Support Engineer about a problem or concern, a customer does not feel that they have been given the urgency or priority deserved, the escalation process goes into effect.

Whether or not, the problem is to be escalated, it is important that all information regarding the problem, requested by the assigned Technical Support Specialist, must be provided for their examination and that all (reasonable) actions they have requested be undertaken.

To formally escalate the problem, the customer should request to contact with a Technical Support manager on the escalation case.

Acronis Support

Free support resources

Acronis Customer Central provides 24x7 access to Self-Service options.

Acronis DeviceLock DLP Support web page

Answers to frequently asked questions, known solutions, hot topics, and other useful information can be found at <https://www.acronis.com/en-us/support/protect/dlp/>

Knowledge Base

[Acronis Knowledge Base](#) is a repository of articles about existing issues, frequently asked questions and step-by-step instructions on how to use our products. You can search by product, key words or choose articles by

category. You can also leave comments or feedback on any knowledge base article as well as vote on whether the content was helpful. This will allow Acronis to continuously improve the content for you.

User Guides

[Acronis Product user guides](#) help you find information on our products like, how the product works, what the system requirements are, how to install the product, features and functions of the product, and more.

Acronis Community

Share and discuss best practices with [live community](#) of Acronis employees, partners and customers.

Acronis DeviceLock DLP upgrades

[Product upgrades](#) are released in the form of builds or new product versions. A Customer is eligible for upgrading DeviceLock DLP software to any new build or a version released until the expiration of his/her support subscription.

Product Lifecycle and Technical Support

All DeviceLock Data Loss Prevention products go through the following phases during their lifecycle:

1. Beta version: technical support with lowest Case Severity, limited to consultations on general issues.
2. General Availability (Current Release): technical support services accordingly to the terms of available Support Level.
3. Continued Support: Once a new DeviceLock version becomes available, DeviceLock Product Engineering will no longer develop new upgrades and fixes (maintenance builds) for the previous product release. Acronis reserves the right to request that the customer upgrade to the current version. Technical support can be limited to consultations on general issues only.
4. Decommissioning (End-of-Life): Acronis will only support Product installations that are no older than two (2) prior released versions. Customer self-service tools will remain available for a reasonable period beyond this withdrawal date.