**Helix Containerized Products Support Policy**

This Support policy applies to the 21.x and later versions of the BMC products listed here: https://documents.bmc.com/products/documents/54/12/545412/545412.pdf, which BMC may update from time to time. This policy was last updated on January 1, 2025.

**Support Service Levels**

Each of BMC's support offerings includes the following, if and when available:

- In accordance with the policies set forth below, BMC provides bug fixes, patches or workarounds in order to cause the Product to operate in substantial conformity with its then-current operating Documentation, and

- BMC provides new releases or versions, to the extent they are furnished to all other enrolled Support customers without additional charge.

BMC provides Support via Web, Email and Phone.

Initial Response goals are relative to the impact of the reported problem on the customer environment.

Note: All of BMC's Support Offerings are subject to change without notice, and that not all support offerings are available for all BMC products.

| Offering | Hours of Operation | Initial Response Goals |
|---|---|---|
| BMC Continuous Support | 24 hours x 7 days *(for S1)* *(Includes published holidays)* Local Business Hours *(for S2 - S4)* *(Excludes published holidays)* | S1 = 1 Clock Hour S2 = 2 Business Hours S3 = 4 Business Hours S4 = 12 Business Hours |

Support business hours reflect normal country business hours in your time zone. For all specific hours of operation, see the country specific Support Contact pages.

**Customer Impact Definitions**

| Impact Level | Customer Impact Criteria |
|---|---|
| 1 | **Critical impact to production environment, primary business service, large number of users experience critical loss of function or data integrity at risk.** Customer resources should be available to work on a 24x7 basis with BMC to resolve the issue. |

| Impact Level | Customer Impact Criteria |
|---|---|
| 2 | **Significant Impact** to business service or system performance affecting production systems or normal operations for multiple groups of users. |
| 3 | **Limited Impact** to the business service, localized to specific service, application or group of users. Workaround may be available to circumvent. |
| 4 | **No service impact,** Non-critical issues, or general questions. |

**Support Policy**

Product technical support is provided to customers currently enrolled in support for BMC's on premises software products, based on the terms and conditions of the customer's license agreement and order with BMC and BMC's current support terms and policies.

If you are currently enrolled in support, you can contact BMC via phone and web during all product technical support stages. Extended support options may be available for some products for an additional annual support cost. Contact your BMC account representative for assistance.

For current support status and product information, sign up for Proactive Alerts and visit the Supported Product A-Z pages. (Proactive Alert email messages and the associated documentation are provided in English only).

For a product to be eligible for Support, all its Licensed Capacity needs to be enrolled.

BMC reserves the right, for the benefit of all its customers, to use or incorporate into any BMC products or services any suggestions, enhancement requests, recommendations or other feedback provided by its customers.

**Release numbering**

BMC uses a three-place numbering scheme to designate released versions of its Helix Containerized products in the following format:

- VV.RR.PP.HFX
  VV=major version, RR=minor release, PP= patch, and HFX=additional hotfixes that might be applied.

**Support Policy for DSOM Products Containerized Releases**

1. BMC has the following version levels for its containerized products:

- A containerized **major and minor software version** (VV.RR) is a significant release that encompasses a fully functional solution and can be installed on the intended Kubernetes

platform using the BMC installation program or implemented as an overlay/upgrade installation to existing containerized software. Such versions might include substantial architectural or structural transformation and introduce new product functionality.

- A **patch release** (PP) refers to a minor deliverable that serves as a revision release, ensuring compatibility with its corresponding major version. This release might include functional enhancements and introduce new capabilities, while being implemented as an overlay/upgrade installation to the existing software.

- **Hotfixes** (HFX) are a deliverable for cumulative critical fixes that cannot wait for a major and minor (VV.RR) release or a patch. Hotfixes apply to products designated as Full or Limited support only. All hotfixes are included in future releases of the product.

2. Support Period

- Each release of a containerized **major and minor** (VV.RR) software version receives full technical support for a period of 1 year starting from the general availability (GA) date.

- Following the full support period, BMC provides an additional 6 months of limited technical support for the respective containerized release.

3. Full Support

- During the 1-year full support period, BMC provides comprehensive technical support for the containerized product, including:

- Full documentation of the product installation, configuration, and usage.

- Patches, hotfixes, or workarounds to enable the product to operate in substantial conformity with its then-current operating documentation, and to address functional issues and security vulnerabilities.

- Access to BMC Software's technical support team for assistance and guidance.

- Compatibility updates for supported third-party software and platforms.

4. Limited Support

- During the 6-month limited support period, BMC will address only critical security vulnerabilities and major defects that significantly impact the functionality of the product or have high technical impact or business exposure to our customers. With customer input, BMC will determine the degree of impact and exposure to inform consequent activities.

- Limited support includes providing workarounds or hotfixes for identified critical security vulnerabilities, as deemed necessary by BMC.

- New enhancements will not be made to the version or release.

- Customer Support will direct customers to upgrade to the current major and minor (VV.RR) version release or patch of the product.

- Research and Development will be engaged on critical cases only and on a limited basis for problem identification.

5. End of Support (EOS)

- After the 1-year full support period and the 6-month limited support period, the containerized major and minor (VV.RR) software version will reach end of support (EOS).

- Access to most technical documentation through BMC Support Central portal, Knowledge Base search, known resolutions and workarounds, existing patches and hotfixes, and BMC Support communities will remain available, where applicable.

- No new sustaining releases, enhancements, patches, or hotfixes will be made to a version or release in "End of Support" status.

- For troubleshooting or Support Cases created, Customer Support will direct customers to upgrade to the current major and minor (VV.RR) version release or patch of the product.

- If a customer would like advice on upgrading their product or has questions about the status of a product's support status, they can contact Customer Support during business hours Monday through Friday.

6. Security Vulnerability Remediation

BMC Software is committed to promptly addressing security vulnerabilities and providing necessary fixes to maintain the security of its products. BMC's holistic approach to product security can be found here: [A Holistic Approach to BMC Product Security](#).

- BMC follows robust processes in development and testing to ensure that every product release adheres to stringent security standards. BMC prioritizes addressing both the most critical (P1) and high-priority (P2) items, as well as other important security issues that require attention.

- BMC currently follows a security fix cycle based on a vulnerabilities CVSS score, providing timely updates by its containerized major releases or patches, as applicable. This approach is in line with our defined policy as detailed in BMC's [secure product development policy](#), which outlines our commitment to maintaining the security and integrity of our products.

- When determining timelines for addressing security vulnerabilities, BMC considers the distinction between findings that are actively exploitable and those that pose hypothetical or theoretical risks as exposed by publicly known CVEs, including vulnerabilities in container images. BMC adheres to common industry standards. If the vulnerability is proven to be actively exploitable, BMC will begin corrective action immediately, develop a fix or workaround, and provide it to customers in the shortest, commercially reasonable time possible.

- BMC expects the customer's security team to establish an exception process that enables BMC to conduct a risk analysis and accurately assess the vulnerability's severity. This process should move beyond relying solely on a projected CVSS score, which tends to emphasize the worst-case scenario without confirming the vulnerability's exploitability in BMC products. These exceptions become necessary when addressing the vulnerability entails significant technological changes that cannot be backported or necessitate architectural modifications.

- BMC uses all reasonable efforts to maintain a quick fix time as commonly accepted in the market, but there are cases that a vulnerability fix might be unavailable from an upstream

vendor of any software utilized by the product. In addition, there are cases where the applied security standards window for addressing the issue begins from the moment the fix is released by the upstream vendor, rather than when the vulnerability is initially identified. BMC anticipates that in such cases the customer's security team may also need to make certain exceptions. BMC acknowledges that its ability to provide a fix might be hindered by external factors beyond its control. Therefore, BMC will work closely with the customer's security team to evaluate alternative solutions and determine the best course of action.

- Because there is typically a delay between when the customer performs scans or deploys BMC products in their production environment, it is important that customers use the latest version of BMC software products to benefit from the most up-to-date security updates. BMC also recommends that customers utilize the latest version of the customer's security scanner. BMC reserves the right to not backport fixes to previously released versions. While certain products undergo the practice of backporting fixes to previous releases, this might not be the case for all products. In such instances, fixes will only be included in the subsequent upcoming release.

BMC encourages customers to actively engage in maintaining the security of BMC's products by promptly reporting any discovered vulnerabilities. Customer contributions play a vital role in helping BMC maintain a robust and secure software ecosystem. To submit a discovered vulnerability, please refer to https://www.bmc.com/corporate/trust-center/vulnerability-disclosure.html.

7. Third-Party Products

- To receive full support for a BMC product, customers must have such products installed in a supported Kubernetes environment or use a supported associated commercial management tool, as specified in the BMC product documentation.

- If a third-party vendor cancels support for one of its products (such as a Kubernetes version, operating system, or subsystem), and that third-party product is underlying, integrates, or interacts with the BMC product, the customer must upgrade to a supported version of that third-party product before BMC Customer Support can provide support for the affected BMC product.

8. Relationship to Kubernetes Versions

- BMC recognizes the limited lifespan of Kubernetes versions and places great importance on BMC products remaining current with the latest supported versions of Kubernetes and its associated commercial management systems.

- BMC strives to provide support for the latest version of Kubernetes and its associated commercial management tools at the time of each containerized product major and minor (VV.RR) version release.

- BMC Helix containerized products' major and minor (VV.RR) version releases will support at least three Kubernetes minor releases.

- For each fully supported major and minor (VV.RR) version release or patch, BMC will support at least one supported version of Kubernetes.

- Customers must ensure that their underlying Kubernetes platform or associated commercial management product remains within a supported version to maintain compatibility and receive essential updates.

- BMC reserves the right to update the list of supported Kubernetes versions and associated commercial management tools for its already generally available (GA) versions. This update may occur even after the GA date, particularly if a specific Kubernetes version is no longer supported by any third-party vendors.

- Internally, BMC tests its platform against a range of Kubernetes platforms that are regularly reviewed and updated. BMC does not test with every single Kubernetes configuration, platform vendor, or associated commercial management tool, but aims to cover a representative sample of popular Kubernetes implementations. For the full list of supported Kubernetes versions and tested commercial management tools, please refer to [BMC Helix On-Premises Deployment System Requirements documentation](#).

- BMC Helix containerized products' version may still be deployed on and operate with Kubernetes configurations or associated commercial management tools not listed and thus customers might choose to deploy and run BMC Helix containerized products' version on-premises in a configuration that is not listed as supported. Such configurations would be considered as "unconfirmed." BMC will accept issues reported in unconfirmed configurations, but BMC reserves the right to request customer assistance in problem determination, including re-creating the problem on a supported configuration. Reported defects either found to be unique to an unconfirmed configuration or found to be not reproducible within a supported environment will be addressed at the discretion of BMC. Defects requiring time and resources beyond commercially reasonable effort might not be addressed. If a configuration is found to be incompatible with BMC Helix containerized products' version, support for that configuration will be specifically documented as not supported (or unsupported).

- BMC provides its customers with a deployment automation tool to assist in installing BMC Helix containerized products' version on-premises. The BMC deployment automation tool can be wrapped into any pipeline a customer may want to create, but it is a required component to launching the orchestration of BMC helm charts, and there is no option to use BMC helm charts directly to create a customer's own installation steps. Customers using their own deployment tool are expected to have the necessary skills and knowledge needed to use it effectively and to wrap BMC deployment tool into their pipelines without BMC assistance.

9. Upgrade path (N-2 support)

- BMC Software offers its customers a streamlined upgrade path, allowing them to upgrade to the current major and minor (VV.RR) version release (N) directly from the latest two major and minor (VV.RR) version releases (N-1, and N-2).

- BMC may decide at its sole discretion to make exceptions during the introduction of a new major and minor (VV.RR) release, wherein the upgrade support may extend beyond N-2 versions.

- During the upgrade process, BMC will maintain at least one version overlap between the two major and minor (VV.RR) releases for the underlying Kubernetes version. This overlap means customers can first upgrade their Kubernetes stack before they proceed to upgrade their BMC Software containerized product, ensuring a smooth and manageable transition. In some cases, BMC might recommend an upgrade of the BMC Helix containerized products' version before upgrading the underlying Kubernetes version.

- A customer using a version older than the N-2 supported upgrade path will have to first upgrade to the N-2 or N-1 version before they can upgrade to the latest version.

10. Examples:

- Supported upgrade:

| | Kubernetes version support | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Release Increment | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Current release | 23.1.02 | 1.20 | 1.21 | 1.22 | 1.23 | 1.24 | | | |
| Target Release | 23.3.02 | | | | 1.24 | 1.25 | 1.26 | 1.27 | |

- Unsupported upgrade:

| | Kubernetes version support | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| Release Increment | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| Current release | 22.1.01 | 1.20 | 1.21 | 1.22 | 1.23 | | | | |
| Target Release | 23.3.02 | | | | 1.24 | 1.25 | 1.26 | 1.27 | |

11. Additional Information

- For additional information regarding the availability and support periods of certain products, please refer to BMC Helix Product A-Z page or contact your local BMC representative.

- This support policy is subject to change, and customers are encouraged to consult the BMC Software Support website or contact BMC Support directly for the most up-to-date information regarding specific product releases and their support status.

**Extension of Support Periods**

In some cases, BMC may extend its support of certain product lines beyond the dates specified in this document. Announcements to this effect are made through the BMC Support Central web site and the Proactive Alert service via the Release Notes of the affected products.

**Product End of Life**

- At any time BMC may "end of life" a product by terminating support for such product.

- At least 12 months prior to the termination of support, BMC will post a notification to the BMC Support Central web site and send physical or electronic notice to each customer who is enrolled in such support to the customer address on file.

- During the timeframe between when "end of life" notification is posted to the BMC Support Central web site and the actual termination of support, the product will be supported as follows:

  - New enhancements will not be made to the product.

  - No enhancements will be made to the product to support new or updated versions of the platforms on which the product runs or to which it connects. BMC Customer Support will direct customers to existing fixes, patches, or workarounds applicable to the reported case.

  - BMC Software will develop new hot fixes for problems of high technical impact or business exposure for customers. With customer input, BMC will determine the degree of impact and exposure and the consequent activities.

  - Research and Development will be engaged on critical cases only and on a limited basis for problem identification.

**Third-Party Products**

To receive full support for a BMC product, you must have such product installed in a generally available supported environment. If a third-party vendor cancels support for one of its products (such as an operating system or subsystem), and that third-party product integrates or interacts with the BMC product you have licensed, you must upgrade to a generally available supported version of that third-party product before BMC Customer Support can provide you with support for the affected BMC product.

Where a third-party vendor cancels general support, but offers a paid extended support option, BMC will have no obligation to continue to Support the canceled version, irrespective of whether you have chosen to pay for extended support or not.

**Upgrading**

When you are ready to upgrade, you can download the latest version from BMC's Electronic Product Distribution (EPD) site. To access this site, you must be currently enrolled in support for that product.

**Customization Policy**

**Definition**

A customization is any added functionality to a product that is not included in the base (out of the box) installation of that product.

**Prioritizing Product Cases**

While we will make every effort to address all customer cases in a timely manner, it should be understood that customization cases may be assigned a lower priority than production or installation cases involving base code.

**Getting Customization Assistance**

The Customer Support Center is available to give general suggestions and assist in troubleshooting on a case by case basis at BMC's discretion. Customer Support can also direct customers to white papers focused on architecture and other resources available on our Web site. The design and development of customizations are the responsibility of the customer/consultant and BMC Consulting Services and BMC partners are available for this purpose. Customer Support will NOT provide code customizations to customers.

**Training Requirements**

Customers must attend the appropriate product training before attempting any customizations. This training will empower the customer with the necessary knowledge and ability to design and implement simple changes to the base product. Customizations that are more complex should be implemented by BMC Consulting Services or a BMC partner.

**Identifying Custom Code**

Customers should maintain records and be able to identify all customizations that they have made to their application(s). Customers should keep a centralized file detailing changes that have been made, when they were made and what code was changed. This will help the customer and BMC support identify whether a problem is with the base product or with a customization. This will also aid in the migration or upgrade process to future product versions.

**Maintaining Custom Code**

Customizations are the responsibility of the customer and must be maintained by the customer. Customer Support does not take ownership of any customized code whether the customer, BMC Consulting Services or a BMC Partner generated it. Serious consideration should be given to all customizations since it will require additional work during future migration or upgrade processes for new product versions.

**Multi-Language Support**

English is the only language BMC contractually commits to providing. However, to enhance our follow-the-sun support model and better serve our customers, BMC Software has contact centers worldwide that have multiple language capabilities. Local offices can provide support in the prevailing local languages, but BMC's priority is to get the most knowledgeable person to handle your case. In addition to English, BMC can offer a "first point of contact" local language service for the following languages:

Americas:

- English

- Spanish (LATAM)

- Portuguese (LATAM)

EMEA:

- French

- German

- Spanish

- Portuguese

AP

- Chinese

- Japanese

The first point of contact service is hosted by BMC's contact centers and the language offerings are only available during local business hours. Following the initial communication between the customer and our customer support center, BMC will endeavor to distribute the support issue to a local specialist. However, BMC cannot guarantee local language support from our product specialists. Translation services are available on an exception basis.

**Additional Information**

For additional information regarding the availability and support periods of certain product lines, contact your local BMC representative.

**BMC Support Resources**

- [Support Central](#)

- [Knowledge Base](#)

- [Documentation](#)

- [BMC Communities](#)

- [Training Locations](#)

- [BMC Consulting Services](#)

- [Support Contacts](#)

**Additional Support Centers**

- [BladeLogic](#)

- BMC Service Desk Express

**Upgrade Assistance**

- The BMC Assisted Migration Offering (AMIGO) program is designed to assist customers with the planning of product upgrades to a newer version – "Success through proper planning".

Explore AMIGO Program ›