

Password Safe Cloud Frequently Asked Questions

What Hosting Regions Are Available for the Solution?

Password Safe Cloud can be deployed to several regions across the globe. The specific region is determined by the proximity to the customer. A list of available regions can be found in our supported platforms documentation.



For more information, please see *BeyondInsight and Password Safe Supported Platforms* at <https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/supported-platforms/index.htm>.

What Cloud Provider is Leveraged to Deliver the Password Safe Cloud Solution?

The solution is hosted in a single tenant instance in Microsoft Azure. This environment is audited under the requirements for SOC 2 Type 2 and ISO 27001.

Vulnerability and Penetration Testing

Does the Solution Undergo Frequent Vulnerability and Penetration Testing?

Yes, BeyondTrust performs regular, internal vulnerability scanning and penetration testing on all product solutions. Also, BeyondTrust contracts with third-party vendors to perform periodic penetration tests on the platform to identify risks and remediation that help secure the solution.

Can I Perform My Own Penetration Testing Against the Solution?

Yes, you must notify BeyondTrust in advance of any test by submitting a request using the BeyondTrust Online Support Portal and completing a penetration testing agreement. This activity can be performed only once per calendar year.

Data and Access

How long is audit data retained with PS Cloud?

Audit data is retained for a minimum of 1 year. Information may be kept longer but is subject to deletion after 1 year to accommodate new audit data.

Can I export the audit data if I need to keep it for longer than 1 year?

Audit data can be exported through Reporting and Analytics or the REST API. Session detail information is included in the audit data, but it is not possible to export session video recordings.

Does the Solution Support Role-Based Access for End Users and System Administrators?

Yes, this is a core component of the solution that can be configured and managed.

Who Can Access My Data?

Access to cloud services by BeyondTrust employees is protected by authentication and authorization mechanisms, and BeyondTrust has implemented an access control authentication approach based on need to know and separation of duties.