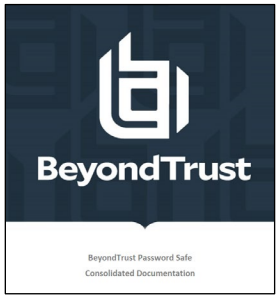


BeyondTrust Password Safe Consolidated Documentation

Thank you for downloading this BeyondTrust Resource. Carahsoft is the Distributor for BeyondTrust solutions available via GSA 2GIT, NASA SEWP V, ITES-SW2, and other contract vehicles.

To learn how to take the next step toward acquiring BeyondTrust's solutions, please check out the following resources and information:

For additional resources:
carah.io/beyondtrustresources

For upcoming events:
carah.io/beyondtrustevents

For additional BeyondTrust solutions:
carah.io/beyondtrustsolutions

For additional Cyber solutions:
carah.io/cybersolutions

To set up a meeting:
beyondtrust@carahsoft.com
(866)-421-4683

To purchase, check out the contract vehicles available for procurement:
carah.io/beyondtrustcontracts

BeyondTrust Password Safe

Consolidated Documentation

BeyondTrust PasswordSafe: Cisco ISE

Cisco Identity Services Engine (ISE) Use Cases Demo:
https://www.youtube.com/watch?v=pdvoEd57I90

Cisco Functional Account Creation Guide:

You'll need this for the Cisco as well: Cisco Functional Account:

To create the functional account on the Cisco device, do the following:

1. Log on to the Cisco device using the Enable password.

2. Type the following command:

   configure terminal

3. Type the following command:

   username sypkfunc privilege 15 secret password

where sypkfunc is the username of the functional account and password is the password.

4. Type the following command:

   line vty 0 4

5. Type the following command:

   privilege level 15

6. Save the new functional account by pressing Ctrl-Z.

These steps establish the functional account with the specified user name and password. The password has a type of Secret, or encrypted. It is recommended to use Secret passwords because they are more difficult to compromise. The privilege level of both the user and the virtual terminal are set to 15 so that the functional account can manage the Enable password without knowing the password.

Custom Platform or Application Platform

Custom Platforms allows you to add SSH and Telnet platforms, as well as SSH application platforms, tailored to your environment. Password Safe contains several built-in SSH and Telnet platforms designed for the most common configurations, such as Linux, Solaris, and Cisco.

Custom Platforms: https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/custom-platforms/index.htm

SSH and RDP Connections

In the Password Safe web portal, requesters can request access to use SSH or RDP remote connections. Access Policies are configured to allow remote connections.

Configure SSH and RDP Connections: https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/ssh-rdp-connections.htm

Applications

Applications can be managed by Password Safe. Requestions can request access to an application and launch a session through the Password Safe web portal. Applications sessions can be recorded for audit as well.

Add Applications to Password Safe: https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/admin/add-applications.htm

Password Safe Cloud Frequently Asked Questions

Frequently asked questions: https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/cloud/faq/index.htm

Password Safe Cloud Resource Broker

This document explains how Password Safe Cloud uses resource brokers within resource zones to manage resources across segmented networks and how to configure resource zones. By configuring resource zones effectively, you have centralized control over resource allocation,

enhanced security, and the ability to meet compliance standards, providing you with peace of mind and a smoother resource management experience.

Password Safe Cloud Resource Broker Installation and Configuration Guide:
https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/cloud/resource-broker/index.htm

Security in BeyondTrust Password Safe Cloud

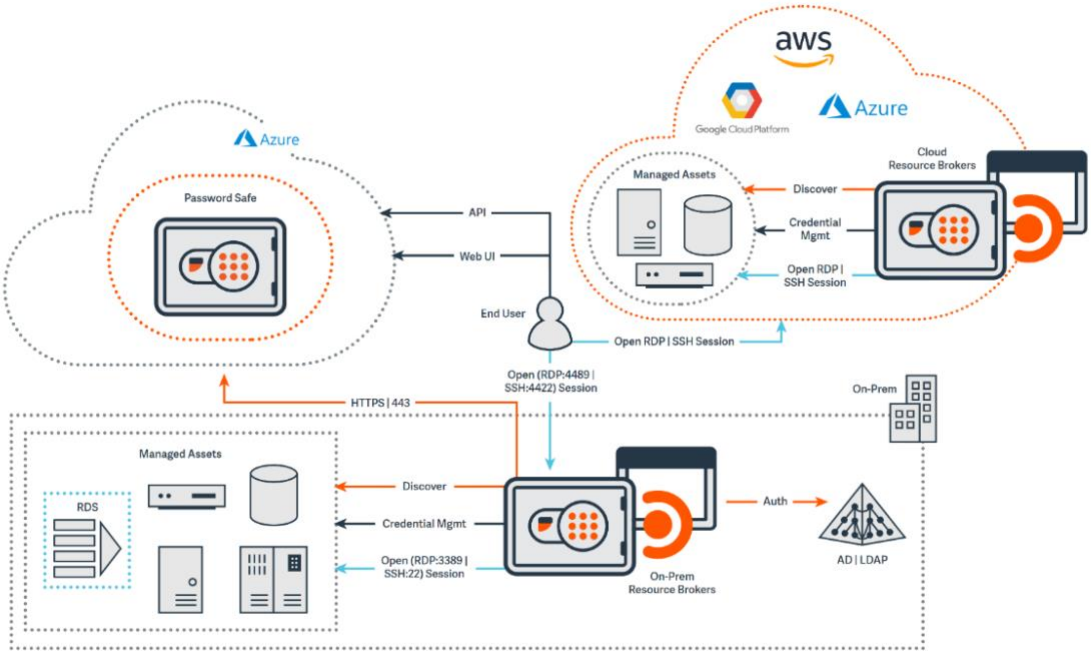
The purpose of this document is to help technically-oriented professionals understand the security-related value BeyondTrust can bring to their organization. BeyondTrust can help your support organization stay secure and compliant, while improving the efficiency and success of your organization with a better end-user support experience.

BeyondTrust Virtual Appliance:

https://www.beyondtrust.com/docs/beyondinsight-password-safe/appliance/install/configure-virtual-images.htm

Cloud Security: https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/cloud/security/index.htm

Architecture of BeyondTrust Password Safe Cloud:
https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/cloud/security/architecture.htm



Azure Infrastructure Security: https://learn.microsoft.com/en-us/azure/security/fundamentals/infrastructure

Data Protection in BeyondTrust Password Safe Cloud:
https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/cloud/security/data-protection.htm

Access Management and Monitoring in BeyondTrust Password Safe Cloud:
https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/cloud/security/access-management-monitoring.htm

Site24x7 Monitoring

Site24x7 is utilized for monitoring functionality of Password Safe Cloud instances. Each hosted instance is associated with Site24x7 automatically during the build process. Health checks are performed periodically to ensure each instance is operating correctly. Instances that fail two consecutive health checks are then marked as down and an alert is triggered. Alerts are in the form of both email and notifications on the Site24x7 portal. Multiple geographic locations are utilized to ensure global availability.

Security and Vulnerability

BeyondTrust uses a vulnerability management solution in our cloud environment(s). The solution scans at least every 24 hours and submits its findings back to the main console as well as to our SIEM. This includes IAM misconfigurations, authentication, lateral movement, data at risk, neglected assets, network misconfigurations, and vulnerabilities. All of the items listed above are alerted to the BeyondTrust InfoSec team, analyzed, and acted on based on validity and criticality.

Password Safe Deployment and Failover Guide:
https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/deployment/index.htm

Default Ports: https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/deployment/default-ports.htm

System Discovery

Functionality	Service	Ports	Requirements/Notes
User Enumeration	nb-ssn | ms-ds	TCP 139 / 445[1]	
Hardware Enumeration	nb-ssn | ms-ds	TCP 139 / 445[2]	WMI Service running on target
Software Enumeration	nb-ssn | ms-ds	TCP 139 / 445[3]	Remote Registry service running on target
Local Services	ms-ds	TCP 445	

Desktop Connectivity

Functionality	Service	Ports
User Interface	https	TCP 443
Remote Desktop	rdp	TCP 4489
SSH	ssh	TCP 4422

Session Management

Functionality	Service	Ports
Remote Desktop	rdp	TCP 3389
SSH	ssh	TCP 22

System Discovery

Functionality	Service	Ports	Requirements/Notes
User Enumeration	nb-ssn | ms-ds	TCP 139 / 445[1]	
Hardware Enumeration	nb-ssn | ms-ds	TCP 139 / 445[2]	WMI Service running on target
Software Enumeration	nb-ssn | ms-ds	TCP 139 / 445[3]	Remote Registry service running on target
Local Services	ms-ds	TCP 445	

Desktop Connectivity

Functionality	Service	Ports
User Interface	https	TCP 443
Remote Desktop	rdp	TCP 4489
SSH	ssh	TCP 4422

Session Management

Functionality	Service	Ports
Remote Desktop	rdp	TCP 3389
SSH	ssh	TCP 22

Network Devices

Functionality	Service	Ports
Checkpoint	ssh	TCP 22
Cisco	ssh	TCP 22
Dell iDRAC	ssh	TCP 22
F5 BIG IP	ssh	TCP 22
HP Comware	ssh	TCP 22
HP iLO	ssh	TCP 22
Juniper	ssh	TCP 22
Palo Alto	ssh	TCP 22
Fortinet	ssh	TCP 22
SonicWall	ssh	TCP 22

Operating Systems

Functionality	Service	Ports	Requirements/Notes
AIX	ssh	TCP 22	
HP-UX	ssh	TCP 22	
IBMi (AS400)	telnet	TCP 22	
Linux	ssh	TCP 22	
MAC OSX	ssh	TCP 22	
Solaris	ssh	TCP 22	
Windows Desktop	adsi-ldap adsi-ldaps	TCP / UDP 389 TCP 636 / UDP 389	ms-ds (TCP 445) is used as a fallback
Windows Server	adsi-ldap adsi-ldaps	TCP / UDP 389 TCP 636 / UDP 389	ms-ds (TCP 445) is used as a fallback
Windows Update/Restart Service	wmi	TCP 135	WMI Service running on target

Applications

Functionality	Ports
VMware vSphere API	API
VMware vSphere SSH	TCP 22
SAP	API

U-Series Appliance

Functionality	Service	Ports
Mail Server Integration	smtp	TCP 25
AD Integration	ldap ldaps	TCP / UDP 389 TCP 636 / UDP 389
Backup	smb	TCP 445
Time Protocol	ntp	UDP 123
HA Replication (pair)	sql-mirroring | https	TCP 5022 / 443

Directories

Functionality	Service	Ports	Requirements/Notes
Active Directory	adsi-ldap adsi-ldaps	TCP / UDP 389 TCP 636 / UDP 389	ms-ds (TCP 445) is used as a fallback
RACF	ssh	TCP 22	
LDAP/S	ldap ldaps	TCP / UDP 389 TCP 636 / UDP 389 TCP 88 (Kerberos) TCP 80 (CRL Validation) TCP 135 (RPC) TCP 389 (LDAP) TCP 445 (CIFS) TCP 464 (Directories) TCP 636 (LDAPS) TCP 3268 (Global Catalog) TCP 3269 (Global Catalog LDAPS)	

Databases

Functionality	Service	Ports
Oracle	oracle-listener	TCP 1521
MS SQL Server	netlib	TCP 1433
Sybase ASE		TCP 5000
MySQL		TCP 3306
Teradata		TCP 1025

BeyondInsight and Password Safe Supported Platforms:
https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/supported-platforms/index.htm

BeyondInsight, Password Safe, and U-Series Appliance FIPS 140-2 Compliance Statement:
https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/fips/index.htm

The link above regarding FIPS 140-2 compliance also goes over Third-Party cryptographic modules used in BeyondInsight, Password Safe, and U-Series Appliances.

Password Safe User Guide: https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/user/index.htm

Active / Active

https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/deployment/active-active-architecture.htm

Active/ Passive

https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/deployment/active-passive-architecture.htm

BI and PS Architecture

https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/deployment/ps-architecture.htm

Active /Active DR

https://www.beyondtrust.com/docs/beyondinsight-password-safe/ps/deployment/dr-active-active-deployment/index.htm