DOCUMENTATION

Password Safe Cache

User Guide

Version 6.8 – December 2018

Revision/Update Information: December 2018
Software Version: Password Safe API 6.8
Revision Number: 0

CORPORATE HEADQUARTERS
5090 N. 40th Street
Phoenix, AZ 85018
Phone: 1 818-575-4000

Contents

BeyondTrust Product Name Conventions

This User Guide uses the following naming conventions for BeyondTrust products:

PowerBroker Password Safe	Password Safe

Overview

Password Cache is a lightweight proxy for the Password Safe API providing high performance throughput for password requests.

Running as a specified Password Safe user, Password Cache makes “View Password”-type requests to Password Safe for all Managed Accounts (for which the user has Requestor or Requestor/Approver roles defined) via the Password Safe API, caching the returned system/account details, request details, and credentials in an encrypted state.

API calls to the Password Cache serve the locally cached data.

Requests are refreshed every five minutes or sooner if a request is due to expire before that time.

If communication with the server is lost, the last known good credentials are served from the local cache even if the associated request has expired.

Note:

BeyondInsight and Password Safe v6.4.4 and below paired with Password Cache v1.7.4-732 and below
Because the Password Cache is performing regular password requests on behalf of the configured Password Safe user, notifications will be sent when requests are made and credentials are retrieved.

BeyondInsight and Password Safe v6.4.6 and above paired with Password Cache v1.7.5-757 and above
Request and credential retrieval notifications are now suppressed when the API calls are performed by the Password Cache.

Requirements

Roles & Settings

Roles

Requestor & Requestor/Approver Roles

The Password Safe user running the Password Cache must have at least one Managed Account Smart Rule configured with the Requestor or Requestor/Approver role.

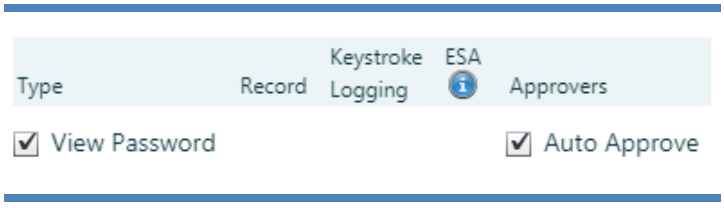
ISA Role

The Password Cache does not currently support ISA-based password requests, therefore it’s important to ensure the user running the cache does not have the ISA role defined for any Managed Account Smart Rules.

Access Policy

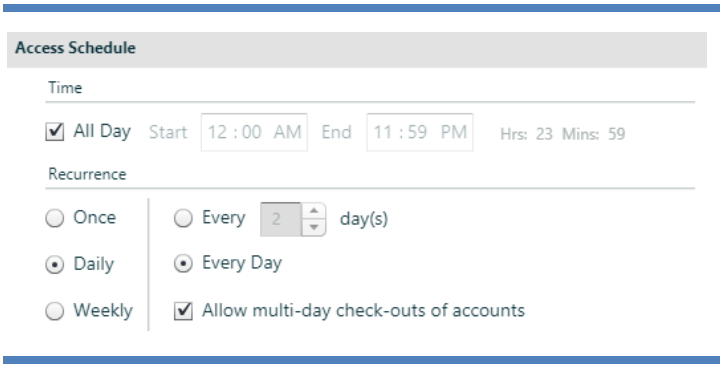
Auto Approval

The Managed Account Smart Rule configured with the Requestor or Requestor/Approver roles must have an Access Policy assigned that has with “View Password” access set to "Auto Approved".



Daily Recurrence - Multi-day Checkouts

If the Access Policy is configured for 'Daily' recurrence, ensure the 'Allow multi-day-check-outs of accounts' is enabled.



Managed Account Settings

Enable for API Access

Ensure this property is enabled for Managed Accounts that will be cached.

Default Release Duration

The Default Release Duration is used to determine how long the account credentials are cached before being renewed.

Concurrent Requests

If the Managed Accounts configured to be cached will also be used by other Password Safe users at the same time, concurrent requests should be set to zero (0 - unlimited) or a value greater than one. Requests performed by the Password Cache count as a request.

Disk Space & Memory

Approximately 10 KB of disk space and RAM is required per Managed Account.

For example, if you are caching 100 accounts, approximately 1MB disk space and RAM is required.

Network Bandwidth

Approximately 13 KB per Managed account is required for network bandwidth over HTTPS.

Supported Operating Systems

- Windows Server 2012 R2 and upper releases
- RHEL/Centos 64 bit 6.8 and upper releases

Supported APIs

- POST Auth/SignAppIn
- POST Auth/Signout
- GET Requests
- POST Requests
- POST Aliases/{aliasId}/Requests
- GET Credentials/{requestId}
- GET Aliases/{aliasId}/Credentials/{requestId}
- GET ManagedAccounts
- GET ManagedAccounts?systemName={systemName}&accountName={accountName}
- GET Aliases

See the *BeyondInsight and Password Safe API Guide* for details on each method.

Installation

Windows

msiexec.exe /i PSPCA-<version>.msi

Linux

rpm -i PSPCA-<version>.x86_64.rpm

Location

Windows

C:\Program Files (x86)\BeyondTrust\Password Cache\pspca

Linux

/opt/pbps/pspc

Service Control

Windows

sc stop pspca

sc start pspca

Linux

systemctl stop pspca

systemctl start pspca

Configuration

To configure the cache call Password Cache with the “cfg” options “pspca cfg <args>”

pspca cfg -?

Usage: cfg [options]

-I --insecure_ssl	Insecure SSL (no validation)
-T --trusted_ certificate=<arg>	Trusted Password Safe CA Certificate file(s)
-C --server_ certificate=<arg>	Password Cache Certificate file
-p --pem=<arg>	Password Cache PEM encoded private key
-P --pem_passwd=<arg>	Password Cache private key passphrase
-u --username=<arg>	<username> Requestor username
-k --key=<arg>	<key> API Key
-h --host=<arg>	Password Safe host[:port]
-? –help	Display this usage message

Example

```
pspca cfg -u psreq -k 638AA550-37C4-7126-A9C1-22186D5A40A0 -h
 192.168.1.128
```


Advanced Settings

The following advanced settings can be configured outside the configuration tool:

LogFile – location of log file. Default /var/opt/pbps/log/pspca.log

runuser – which user will own the cache service. Default “nobody”

http_rest – This can be used to define custom settings for the http REST interface

listen_port – The port the cache will use to listen for incoming API calls. Default 443

listen_host – The interface the cache will use to listen for incoming API calls. Default 0.0.0.0

Windows

Advanced settings are stored in the registry:

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BeyondTrust\PBPS\pspca_cfg]

Configuration

"LogFile"="C:\Program Files (x86)\BeyondTrust\Password Cache\logs\pspca.log"

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\BeyondTrust\PBPS\pspca_cfg\http_rest]

"listen_port"=dword:000001bb

"listen_host"="0.0.0.0"

Linux

The advanced options are stored in a json format in /etc/opt/pbps/pspca.conf .

```
{
"LogFile": "/var/opt/pbps/log/pspca.log",
"runuser": "nobody",
"http_rest": {
"listen_port": 443,
"listen_host": "0.0.0.0"
}
```

