BeyondTrust Password Safe 6.2

(a BeyondInsight component)

Security Target

Version 1.0
June 13, 2018

Prepared for:
BeyondTrust Software, Inc.

5090 N. 40th Street
Phoenix, AZ 85018

Prepared by:

Common Criteria Testing Laboratory
6841 Benjamin Franklin Drive, Columbia, Maryland 21046

LIST OF TABLES

1. Security Target Introduction

This section identifies the Security Target (ST) and Target of Evaluation (TOE) identification, ST conventions, ST conformance claims, and the ST organization. The TOE is the BeyondTrust Password Safe 6.2 (a BeyondInsight component). Hereinafter, the TOE may be referred to as Password Safe, or simply the TOE.

Password Safe provides an automated password and session management solution for any privileged account.

The Security Target contains the following additional sections:

- Product and TOE Description (Section 2)
- Security Problem Definition (Section 3)
- Security Objectives (Section 4)
- IT Security Requirements (Section 5)
- TOE Summary Specification (Section 6)
- Protection Profile Claims (Section 7)
- Rationale (Section 8).

1.1 Security Target, TOE and CC Identification

ST Title – BeyondTrust Password Safe 6.2 (a BeyondInsight component) Security Target

ST Version – Version 1.0

ST Date – June 13, 2018

TOE Identification – BeyondTrust Password Safe 6.2 (a BeyondInsight component)

TOE Developer – BeyondTrust Software, Inc.

Evaluation Sponsor – BeyondTrust Software, Inc.

CC Identification – *Common Criteria for Information Technology Security Evaluation*, Version 3.1, Revision 4, September 2012

1.2 Conformance Claims

This TOE is conformant to the following CC specifications:

- *Standard Protection Profile for Enterprise Security Management Identity and Credential Management*, Version 2.1, October 24, 2013, [ESMICM] and including the following optional SFRs: FIA_AFL.1, FTA_SSL.4, and FTA_TAB.1[1]. The following NIAP Technical Decisions apply to this PP and have been accounted for in the ST development and the conduct of the evaluation:
  - TD0245: Updates to FTP_ITC and FTP_TRP for ESM PPs
  - TD0055: Move FTA_TAB.1 to Selection-Based Requirement

  The remaining NIAP Technical Decisions that apply to the claimed PP (up to and including TD0320) do not apply to this ST based on the SFRs claimed by the TOE.
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 4, September 2012.
  - Part 2 Extended

[1] FTA_TAB.1 should be included in the list of optional SFRs per TD0055 (https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?td_id=58).

- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1 Revision 4, September 2012.
    - Part 3 Conformant

1.3 Conventions

The following conventions have been applied in this document:

- Security Functional Requirements – Part 2 of the CC defines the approved set of operations that may be applied to functional requirements: iteration, assignment, selection, and refinement.
    - Iteration: allows a component to be used more than once with varying operations. In the ST, iteration is indicated by a number in parentheses placed at the end of the component. For example FDP_ACC.1(1) and FDP_ACC.1(2) indicate that the ST includes two iterations of the FDP_ACC.1 requirement, (1) and (2).
    - Assignment: allows the specification of an identified parameter. Assignments are indicated using bold and are surrounded by brackets (e.g., [**assignment**]). Note that an assignment within a selection would be identified in italics and with embedded bold brackets (e.g., [***[selected-assignment]***]).
    - Selection: allows the specification of one or more elements from a list. Selections are indicated using bold italics and are surrounded by brackets (e.g., [***selection***]).
    - Refinement: allows the addition of details. Refinements are indicated using bold, for additions, and strike-through, for deletions (e.g., "… **all** objects …" or "… ~~some~~ **big** things …"). Note that 'cases' that are not applicable in a given SFR have simply been removed without any explicit identification.

1.3.1 Abbreviations and Acronyms

Term	Definition
AD	Active Directory
CC	Common Criteria
DPAPI	Data Protection Application Programming Interface
ESM	Enterprise Security Management
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
NTP	Network Time Protocol
OE	Operational Environment
OS	Operating System
PP	Protection Profile
RBAC	Role-Based Access Control
RDP	Remote Desktop Protocol
RSA	Rivest-Shamir-Adleman
SAR	Security Assurance Requirement
SFR	Security Functional Requirement

Term	Definition
SSH	Secure Shell
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Function

Table 1: Abbreviations and Acronyms

1.3.2 Customer Specific Terminology

Term	Definition
BeyondInsight	BeyondTrust BeyondInsight IT Risk Management Platform provides Centralized Management, Reporting and Threat Analytics for Privilege and Vulnerability Management.
Enrolled User	An enrolled user is one who has been issued credentials, attributes, and uniquely identifying data.
Enterprise User	Enterprise users are users defined in the managed systems and also defined and enrolled on the TOE. The Enterprise users are Managed Accounts.
Functional Account	A functional account on a managed system is required to manage passwords for accounts on that managed system. This account is only used internally by the TOE.
Group	Logical container for user accounts and a mechanism for easing the burden of assigning roles on systems or collections to individual TOE users. Roles that are assigned to a group are inherited by all members of the group. A TOE user who is added to the group is immediately granted all the roles that are assigned to the group. A TOE user can be a member of zero or more groups. All roles that are granted as a member of a group are revoked for a TOE user who is removed from the group.
Interactive User	Administrators and Password Safe (TOE) users that have a User Account and can log in to the TOE. TOE users are defined and authenticated in AD.
Managed Account	Account on a managed system whose password is being stored and maintained through Password Safe. Typically, managed accounts are “privileged accounts” that can perform administrative tasks on the managed system. For example, root is likely to be a managed account on many of Linux managed systems.
Managed System	Computer where one or more account passwords are to be maintained by Password Safe. Managed systems can be Windows machines, Linux machines, and Active Directory domains.
Password Safe User / TOE User	A Password Safe user (or TOE user) is authorized to log in to the TOE for the purposes of requesting access to managed systems using managed accounts and/or to approve/reject access requests. Password Safe users are defined in the environmental Active Directory.
Role	A role is an attribute of a TOE user account that determines whether the user is authorized to request access to managed systems using managed accounts, to approve/deny such requests, or both.
Smart Rule	A Smart Rule is a filter that permits the organization of assets. Assets can be

	organized by Asset Smart Groups.
TOE Administrator / BeyondInsight Administrator	A TOE administrator (or BeyondInsight Administrator) accesses the TOE using the BeyondInsight Management GUI. This interface grants the TOE administrator full access to the management functionality of the TSF. Note that TOE administrator credentials are stored within the TOE; they are not associated with enterprise users.
User Account	A user name assigned to an individual that can log in to the Password Safe appliance and perform tasks, such as requesting or approving password releases. The set of tasks that a user account can perform is determined by the user account type and the roles that are assigned to the user.)
User Enrollment	The process of generating and issuing credentials, defining attributes, assigning unique identifying data for a user, and propagating that data to any repositories that use it.

Table 2: Customer Specific Terminology

2. Product and TOE Description

The TOE is BeyondTrust Password Safe 6.2 (a BeyondInsight component). This section commences with an overview of the BeyondInsight IT Risk Management Platform, and then proceeds to identify the BeyondInsight components that are included in the TOE. The TOE description covers TOE architecture, logical boundaries, and physical boundaries.

2.1 Product Overview

The BeyondInsight IT Risk Management Platform is an integrated suite of software solutions used by IT professionals and security experts to collaboratively:

- Reduce user-based risk and mitigate threats to information assets
- Address security exposures across large, diverse IT environments
- Comply with internal, industry and government mandates

BeyondInsight integrates two foundational security methodologies:

- Password Safe v6.2 is an automated password and session management solution for any privileged account, such as shared administrative accounts and local administrative accounts. Password Safe offers broad and adaptive device support.
- Vulnerability Management enables security to assess risk, measure breach likelihood, and make remediation recommendations. The BeyondInsight Retina CS scanner provides organizations with vulnerability assessment, risk analysis, and reporting. Customers proactively identify exposures, analyze business impact, and conduct remediation across network, web, mobile, cloud and virtual infrastructure.

The BeyondInsight IT Risk Management Platform solution contains functionality that is not covered by the [ESMICM]. As with all evaluations claiming conformance to a Protection Profile, only the functionality specified in the PP is evaluated. This section describes the solution as a whole and Section 2.2 identifies the specific components and functionality included in the TOE.

The BeyondInsight IT Risk Management Platform solution consists of the following components:

- BeyondInsight Management GUI
- Retina CS Scanner
- Retina Protection Agent
- Event Server
- SQL Server database 2014
- BeyondInsight Reporting and Analytics
- Password Safe Service (i.e. Password Safe)
- Session Monitoring
- Proxy Service

The BeyondInsight Management GUI provides the interfaces to configure and manage the TOE. BeyondInsight administrators configure the Retina Network Security Scanners to run vulnerability assessments and to review the results to determine which assets are vulnerable and require remediation. The BeyondInsight Management GUI is used to create the groups that are assigned roles to manage password releases and create the functional accounts and managed accounts in Password Safe.

The Retina CS Scanner is the scan engine responsible for vulnerability scanning of the assets in the network environment. Information gathered by the Retina CS Scanner is sent to the BeyondInsight Event Server which passes the information to the SQL server database 2014.

The Retina Protection Agent performs endpoint host security. It is installed on an asset to provide layers of protection, including: virus and spyware, firewall, intrusion prevention, system protection, and vulnerability assessment. Information gathered by the Retina Protection Agent is sent to the BeyondInsight Event Server which passes the information to the SQL server database 2014.

BeyondInsight Reporting and Analytics permits an administrator to run reports on the scan information that is stored in the BeyondInsight database. Reports are configurable and can include accounts, assets, scan results, patch management, and vulnerability management. The Password Safe administrator can generate reports to display the managed account password age, password and session activity, password update activity, password update schedule, password release activity, and scheduled password change configuration.

The Password Safe service provides automated password and session management solutions for any privileged account, such as shared administrative accounts. Password Safe includes a web based interface for executing password requests and approvals.

Password Safe (the TOE) provides password management and session management.

The HTTPS connection between the TOE and the Password Safe user ensures both integrity and disclosure protection. The connection between the TOE and the external authentication servers are protected using a secure TLS channel. The secure protocols are provided by the Operational Environment.

Password Safe provides four different methods for a Password Safe user to access a managed system such as a Linux or Windows machine or an Active Directory domain using a managed account. Three methods require that the Password Safe user who is requesting this access to log on to the TOE as a TOE user with a requester role, which is mediated by Microsoft Active Directory external authentication. The fourth method consists of BeyondTrust PowerBroker for Windows working with Password Safe to grant and control access to privileged accounts on Windows desktop and server platforms.

The different methods for a Password Safe user to access managed systems are described below.

One-Click Launch Method

This method requires that the access policy to be pre-configured for the Password Safe user to allow auto-approval using the One-Click launch method. This method requires the Password Safe user to have a requester role. The policy includes session recording and monitoring enabled to provide accountability for Password Safe users logging in to managed accounts.

1. The TOE user assigned to a requester role logs into to Password Safe Web Portal GUI via HTTPS. The TOE user is presented a GUI page identifying the managed accounts to which they are authorized access to. The TOE user selects the managed account and connects to it by clicking the One-Click button and then selecting the SSH, RDP, or Application button.
2. Password Safe generates a one-time session key which is sent back to the TOE user's desktop host. At no time is a username, password, or even host name sent back to the desktop host.
3. The desktop host pulls down the session key and automatically launches native desktop tools (PuTTY for SSH sessions or RDP for Windows sessions).
4. RDP or PuTTY ultimately uses the session key to connect to the session proxy.
5. The session proxy looks at the key and knows what host it is, which user name, which password, and it injects those credentials into the data stream.
6. The TOE user seamlessly connects via RDP or SSH to the managed system. Ultimately this permits control of how the users securely log on to the managed system without ever allowing the TOE user to see what those credentials are.

This method provides the ability for a Password Safe user to log in to a managed account without knowledge of its credentials. Since the ability to log in to the managed account is requested by a TOE user, different TOE users who access the managed system using the same managed account will have unique attribution of the activities they perform on that account.

Approval Method

This method requires the Password Safe user to have a requester role and the managed account to have one or more approvers. As with the One-Click Launch Method, the policy includes session recording and monitoring enabled to provide Password Safe user accountability.

1. The TOE user assigned to a requester role logs on to the TOE via HTTPS and requests a session on the managed account by clicking the table entry (not the One-Click button above) and selecting the SSH, RDP, or Application option.
2. An email is generated and sent to a TOE user who has an approver role for the Managed Account Smart Group.
3. The approver clicks on a link in the email, and logs into the TOE via HTTPS to approve or deny the request.
4. If the request is approved, an email is sent to the requester with a link to open the request; if it is denied, an email is sent to the requesting TOE user giving the reason for denial (if given by the approver).
5. The requester can now select the session with the managed account.
6. Password Safe generates a one-time session key which is sent back to the requester's desktop host. At no time is a username, password, or even host name sent back to the desktop host.
7. The desktop host pulls down the session key and automatically launches native desktop tools (PuTTY for SSH sessions or RDP for Windows sessions).
8. RDP or PuTTY ultimately uses the session key to connect to the session proxy.
9. The session proxy looks at the key and knows the managed system that it is for, the managed account to authenticate to, and the credential for that account, and it injects those credentials into the data stream.
10. The TOE user seamlessly connectives via RDP or SSH to the managed system. Ultimately this permits control of how the users securely log on to the managed system without ever allowing the TOE user to see what those credentials are.

As with the One-Click Launch Method, this provides the ability for a Password Safe user to interact with the managed system without knowledge of the managed account's credentials. Since access to the managed system using the managed account is requested by a TOE user, different TOE users who log in to the same managed account will have unique attribution of the activities they perform on that account.

Password Release

The TOE normally does not give out passwords, but rather manages sessions. However, the TOE does provide the ability for a Password Safe user to retrieve a password where the session does not need to be managed. The policy is configured with the Max Concurrent Password Request set to one such that only one Password Safe user at a time can access a managed system using a managed account, thus permitting Password Safe user accountability. The TOE is configured to auto-generate a new password after the password release time period has elapsed.

1. A BeyondInsight Administrator configures the policy to permit "View Password" for the TOE user assigned to a requester role desiring to log in to a managed account. This may be auto-approved, or require one or more approvers.
2. The requesting TOE user logs in via HTTPS, requests a session with the managed account via One-Click (if auto-approval is enabled), and selects "Retrieve Password," which permits the TOE user to retrieve the password. If Approvals are required, the requesting TOE user will go through the same approval process described in the Approval Method steps above.
3. When the TOE user selects the Retrieve Password button, the password displays in a separate window for a maximum of 20 seconds. The TOE user clicks "Highlight Password" followed by a Ctrl-C. The retrieved password is securely delivered to the TOE user via HTTPS.
4. The TOE user has foreknowledge of the username and host of the managed account and may use the password to log on to that managed account within the password release time period.

BeyondTrust PowerBroker for Windows Password Release

The TOE can be integrated with the BeyondTrust PowerBroker for Windows which is installed on a Windows machine for privileged Desktop Application Access, Server Access, or Local Administrative Access. The Active Directory user account to be brought under the TOE as a managed system must already be provisioned in Active Directory.

The Active Directory user can be added to an AD group that has roles authorized to log in to managed accounts in Password Safe, which makes them a TOE user. PowerBroker for Windows would have a rule set to launch an application using a managed account. When prompted by PowerBroker for Windows client, the TOE user's username and password would be entered. The PowerBroker for Windows client would authenticate these credentials against Active Directory.

Active Directory group membership is enumerated by Password Safe, and verification that the role is permitted to log in to the managed account is performed. If authorized, the password for the managed account is sent to PowerBroker for Windows over TLS. Windows authenticates the managed account via Active Directory. The application would be launched using this account as the `run-as` credentials.

Upon termination of the privileged session, PowerBroker for Windows will inform Password Safe that the session has been terminated. TOE user accountability is maintained throughout the privileged session. Microsoft Windows creates an audit trail when a TOE user leverages any managed account and uses the `run-as` command. This provides full accountability by connecting a TOE user to the managed account and the application. The Windows machine is responsible for providing audit records of the enterprise user's activity.

The TOE provides session management and access control thorough administrator defined policies. Password Safe does not push policies to end systems from a central location nor enforce the generation of evidence of receipt for received policies, as a result the product's access control does not meet the requirements of the Standard Protection Profile for Enterprise Security Management Access Control and therefore access control is not included within the scope of the evaluation.

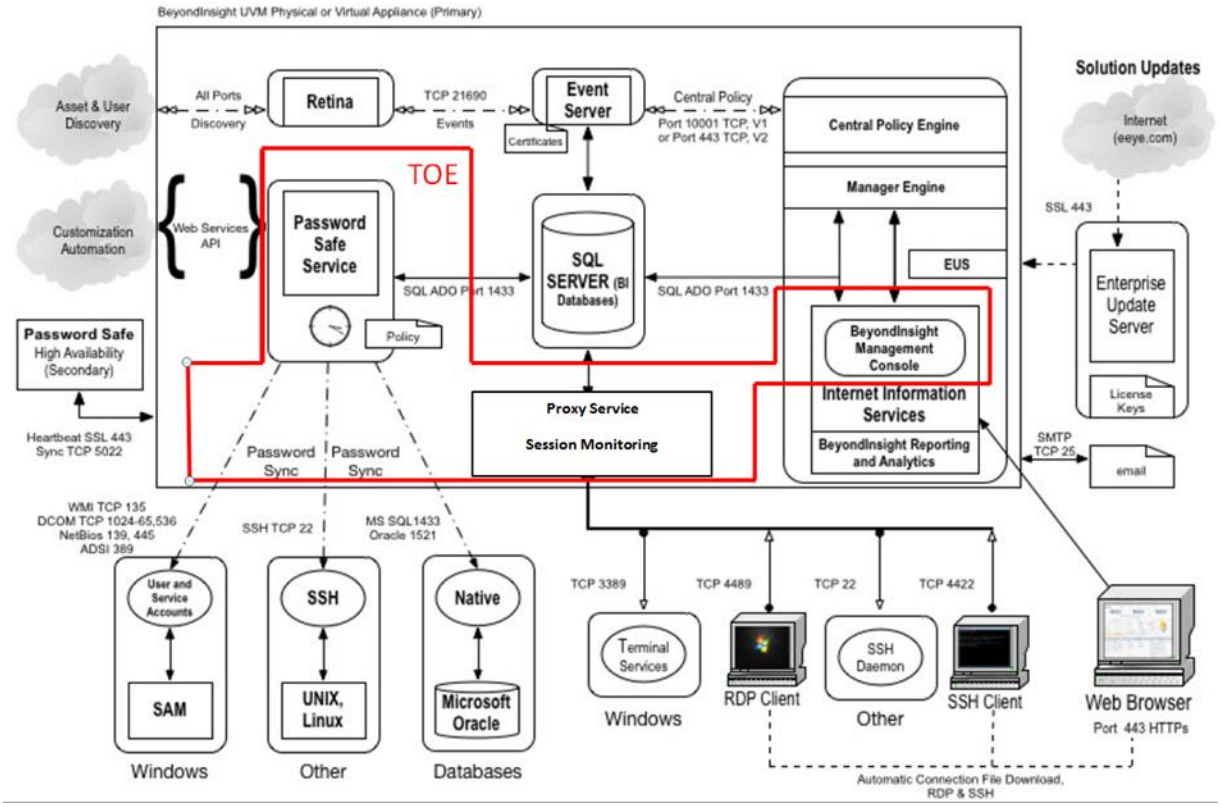

Figure 1: BeyondInsight and Password Safe TOE Functional Components

2.2 ESM Context for the TOE

The TOE is an Enterprise Security Management product. It has the ability to interface with other enterprise-level components and apply security measures that can affect any user that is defined in the enterprise. Specifically, it is an Identity and Credential Management product. The TOE does not replace the organization's existing repository of identity and credential data (e.g. Active Directory); instead, it is responsible for managing administrative credentials

for enterprise users, which are managed accounts on managed systems. Associations between TOE users and these managed accounts are made based on TOE user identity data defined in the environmental Active Directory. The TOE is able to enroll enterprise users into Password Safe and define rules such that any TOE user meeting chosen identity characteristics can be associated with the enrolled users. The TOE can then facilitate the use of managed accounts and the credentials used to access them such that only TOE users with appropriate identity attributes may interact with them.

The TOE is expected to be used with other Enterprise Security Management (ESM) products. In the evaluated configuration, the TOE relies on Active Directory to manage identity and credential attributes for TOE users, and to act as an authentication server for those TOE users attempting to access the TOE itself. Since the TOE communicates directly with Active Directory, an organization may deploy only a single instance of the TOE to cover all managed systems in the enterprise. The TSF extends the identity and credential management aspects of Active Directory by granting specific TOE users access to managed systems based on their identity attributes (e.g., all members of a "system administrator" role in some business unit or geographic region may be granted access to managed systems needed to perform their assigned duties). The TSF then manages the credentials of the managed accounts on these managed systems by granting/revoking access to them on an administrative basis and by enforcing strong password composition rules on them. This is done in a manner that is transparent to the TOE users who log in to managed systems using these managed accounts. The purpose of this is so that individuals in the organization who lack authorization to use these managed accounts cannot bypass the TSF and log on to them directly.

The TOE is also compatible with ESM products that enforce Host-Based Access Control. Any such product is able to enforce access privileges on any accounts that are defined on managed systems, which would include managed accounts by definition. Since the managed accounts configured by the TOE are local accounts on managed systems just like any other, an ESM Access Control product can theoretically be used to limit the extent to which those managed accounts can interact with the managed system they belong to. An example of this is described in "BeyondTrust PowerBroker for Windows Password Release" above. This example has direct linkages between the ESM Access Control product and the TOE in the sense that the TSF can be used to authenticate to PowerBroker as it is running. In other cases there may not be a direct interface between the two; another ESM Access Control product may simply define a policy that applies to a system account that is also defined as a managed account by the TOE. When a TOE user accesses a managed system using that managed account, the ESM Access Control product will enforce its configured policy the same as if the account was accessed directly without the TOE's intervention.

2.3 TOE Overview

The TOE is the BeyondTrust Password Safe 6.2 (a BeyondInsight component) consisting of the following:

- Password Safe
- BeyondInsight Management GUI
- Proxy Service
- Session Monitoring

The TOE components identified above collectively provide functionality defined in the [ESMICM]. The TOE manages identities and password credentials and associates attributes with enterprise users. Specifically, the TOE provides the following Identity and Credential Management functions for an Enterprise System. The functions are described in the more detail in the rest of this section and in Section 6:

- Provision subjects (enroll new subjects to an organizational repository, associate and disassociate subjects with organizationally-defined attributes)
- Issue and maintain credentials associated with user identities
- Enforce password strength rules for enterprise users
- Establish appropriate trusted channels between itself and Authentication Server ESM products
- Generate an audit trail of configuration changes and subject identification and authentication activities
- Write audit trail data to a trusted repository

The TOE is restricted to the functionality identified in the [ESMICM]. The following functionality is not considered part of the evaluation:

- Retina CS Scanner vulnerability scanning
- Retina Protection Agent endpoint host security.
- Event Server passing the scan information to the SQL server database 2014
- The Password Safe password release capabilities (i.e. inserting or making the password available for managed systems) are not addressed by SFRs in the PP, and thus those capabilities are not covered by the evaluation.

The Proxy Service supports the functionality identified in the [ESMICM] by providing a service to establish trusted channels between a requester and the managed system.

The BeyondInsight administrator user group is created by default with full rights to the BeyondInsight Management GUI. The permissions assigned to the group cannot be changed. The default BeyondInsight administrator user group has the permissions to create other BeyondInsight administrator groups. However, these were not tested in the evaluated configuration.

A BeyondInsight administrator defines the external systems to be brought under session management by defining the functional accounts on the managed systems and defining the managed accounts on the systems through configured password management policies. BeyondInsight administrators log onto BeyondInsight Management GUI using a secure HTTPS connection thorough a web browser. BeyondInsight administrator credentials are stored in non-plaintext form in the Microsoft SQL Server database 2014. The Microsoft SQL Server database 2014 is considered to be part of the operational environment.

The BeyondInsight Management GUI provides the interfaces to support all the management functionality defined in the [ESMICM]. A BeyondInsight administrator uses the GUI for all management activities, including the definition and enrollment of enterprise users and the management of TOE users. TOE users using the Password Safe Web Portal GUI perform tasks, such as requesting or approving password releases. A TOE user logs on to the TOE to access the managed accounts they are associated with. Password Safe provides Role-Based Access Control (RBAC). The set of tasks that can be performed by a TOE user is determined by the roles that are assigned to that user. A role also establishes a connection between the TOE user (or groups of TOE users) that belongs to the role and the managed accounts on managed systems that members of the role can log on to (or request the ability to log on to). Managed accounts and managed systems can be added to a group using Smart Rules. If such a group is associated with a role, members of that role are authorized to interact with the contents of that group in a requester and/or approver capacity.

Password Safe roles can only be assigned by a member of the BeyondInsight Administrator group. All changes to user accounts must be managed by a BeyondInsight Administrator account.

Password Safe provides the following predefined roles.

- Requester - Assign this role to TOE users that can request a password.
- Approver - Assign this role to TOE users that will approve password releases.
- Approver/Requester - This cross-functional role enables the TOE user or group to submit or approve requests for password releases. However, this individual cannot approve their own request when dual control is enforced. This role is typically used in a peer approval environment.
- Auditor – The Auditor role enables the TOE user to review Replay Sessions when logged into the Web Portal.
- Information Security Administrator (ISA) – The ISA role permits the bypass the approval workflows for accessing passwords and establishing session.
- No Roles – Assign this role to remove any previously assigned roles from a TOE user or group.

- Recorded Session Reviewer – allows the TOE user to view recorded Password Safe sessions. The TOE user can add comments and mark the session as reviewed. The TOE user can also archive sessions if configured on an appliance.

A BeyondInsight administrator accesses the TOE using the BeyondInsight local password authentication. Password Safe users access Password Safe Web Portal GUI using Microsoft Active Directory external authentication. Communication between the external AD server and the TOE is protected using TLS. This secure protocol is provided by the Operational environment.

Other Enterprise Security Management products are able to make use of the identity and credential data that is centrally managed by Password Safe. Password Safe provides a bridge between TOE users and managed accounts. For example, BeyondTrust PowerBroker for Windows is able to work with Password Safe to grant and control access to privileged accounts on Windows desktop and server platforms. Based upon the TOE policies, TOE users can access privileged accounts and applications on the managed systems without ever knowing the authentication credentials. Sessions on managed accounts can be managed based upon the credential lifetime and the credential status. Password Safe enrolls enterprise users associated with the Microsoft Active Directory domain defined administrative accounts. The TOE defines and manages credential data that it associates with AD users identities and group memberships. TOE user accountability is maintained throughout the privileged session. The Windows machine is responsible for providing audit records of the AD user's activity.

A BeyondInsight administrator defines the external systems that will be brought under Password Safe session management. A managed system computer is where one or more account passwords are to be maintained by Password Safe. Managed systems can be Windows machines, Linux machines, and Active Directory domains. A BeyondInsight administrator is responsible for setting up managed systems and managed accounts. The managed system passwords and credentials are stored in the Microsoft SQL Server database 2014 using AES 256. The Microsoft SQL Server database 2014 and the Microsoft Server 2012 R2 Crypto Primitives are considered to be in the Operational Environment.

A functional account on a managed system is required to manage passwords for accounts on that managed system. A BeyondInsight administrator identifies the platform and operating system, selects the password rule, provides the username, and password, and a description for the account

The TOE enrolls enterprise users and assigns unique identifying data that is associated with the users and their defined security-relevant attributes. Managed accounts are system-level accounts which are local to a managed system, such as a Linux root account. Managed accounts are associated with assets or domains which are managed by Password Safe and whose passwords are stored and maintained through Password Safe. Typically, managed accounts are "privileged accounts" that can perform administrative tasks on the managed system. For example, root is likely to be a managed account on many of Linux managed systems. The passwords are also stored and updated on the managed systems. The TOE provides automatic password changing at configurable intervals. Once accounts become managed accounts on the TOE, the account credentials are always valid/current. Revoking of password credentials is accompanied by assignment of a new password and therefore the managed account's password is always valid. The TOE maintains a history of password changes. Managed accounts can be deleted from TOE control. Deleting a managed account essentially removes all access to the managed account.

The TOE provides the capability to ensure that managed account credentials satisfy specified minimum strength rules and complexity requirements via Password Policies.

The TOE provides access protection functions such as configurable advisory warning message and authentication failure handling. The functions are configurable by a BeyondInsight administrator.

Audit events are generated and logged in the Microsoft SQL Server database 2014 and in Windows Front End Logs internal to the appliance (both in the operational environment). The audit records are accessed by a BeyondInsight administrator through the BeyondInsight GUI. The audit records identify the date and time of the event, type of event, subject identity and the outcome (success or failure) of the event. A checkout (request) of any password, or connection to an RDP/SSH session via the proxy by an enterprise identity is logged under a unique session identifier and correlated with the managed system account/user id. Any action during the life of the request is logged against the session identifier e.g. checkout, check in, password change, etc. Session Monitoring is turned on to provide TOE user accountability. Session monitoring records the actions of a TOE user while they are accessing the password protected assets through the session proxy. The actions are recorded in real-time with the ability to bypass inactivity in the session. This allows only the actions of the TOE user to be viewed. Recorded sessions can be viewed by any

Password Safe user who has been assigned the role of Administrator, Auditor or Recorded Session Reviewer. All recorded RDP or SSH sessions can be replayed.

The following managed system platforms are supported:

- Windows machines
  - Windows 7 SP1 (32-bit and 64-bit)
  - Windows 8 and 8.1 (32-bit and 64-bit)
  - Windows 10 (32-bit and 64-bit)
  - Windows Server 2008 (32-bit and 64-bit)
  - Windows Server 2008 R2 (64-bit)
  - Windows Server 2012 (32-bit and 64-bit)
  - Windows Server 2012 R2 (64-bit)
  - Windows Server 2016 (32-bit and 64-bit)
- Linux machines
  - RHEL/CentOS
  - Ubuntu
  - Fedora
  - Linux Mint
  - Oracle Linux
  - openSUSE
  - SUSE
- Active Directory domains

The TOE relies on the Microsoft Cryptographic Primitives Library (bcryptprimitives.dll and ncryptsslp.dll) in Windows Server 2012 R2, (CMVP Certificate #2357) in the operational environment. The Cryptographic Primitives Library (bcryptprimitives.dll and ncryptsslp.dll) provides cryptographic services to Windows components and applications. It includes cryptographic algorithms in an easy-to-use cryptographic module via the Cryptography Next Generation (CNG) API. The cryptographic libraries provide the secure HTTPS connection for a BeyondInsight administrator to log on to the BeyondInsight Management GUI interface and for a Password Safe user to log on to the Password Safe Web Portal GUI. The TOE uses the OpenSSL in the operational environment to provide the TOE user secure SSH and RDP connections to the Proxy Server and the Proxy Server to the managed systems.

2.4 TOE Architecture

The section describes the TOE architecture including physical and logical boundaries.

The TOE does not operate in a Federation; there is only one instance of Password Safe in the system. **Figure 2** illustrates the TOE in relation to its operational environment.

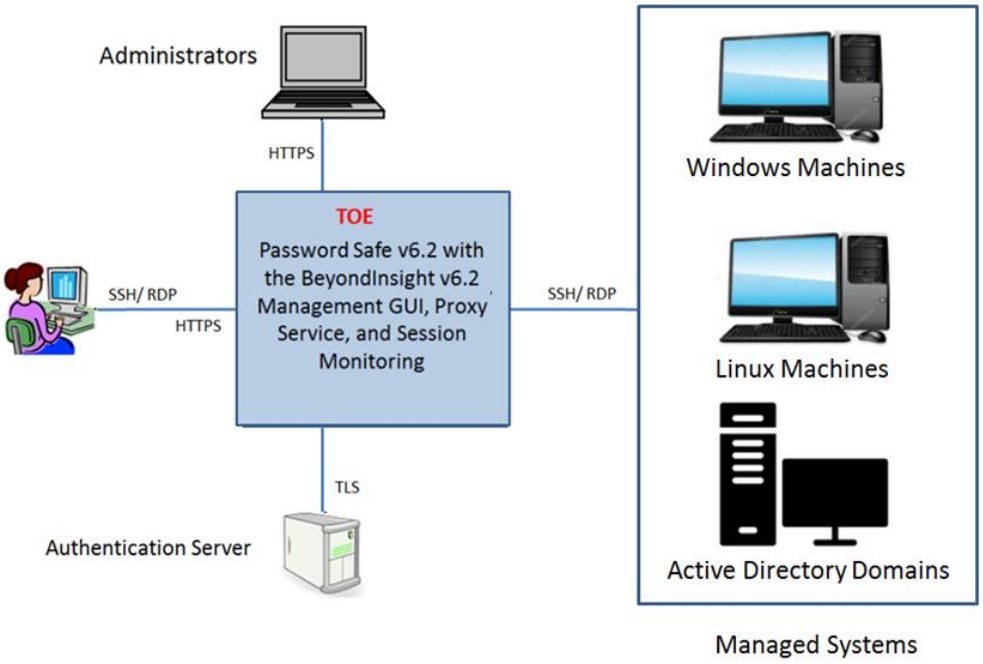

Figure 2 – TOE in Operational Environment

2.4.1 Physical Boundaries

The BeyondTrust Password Safe 6.2 (a BeyondInsight component) is delivered pre-installed on the BeyondTrust UVM20 and UVM50 Security Management Appliances. Each hardware appliance is considered part of the operational environment.

The BeyondTrust UVM20 and UVM50 appliances are delivered with the following installed software. The required software is considered to be part of the operational environment.

- Windows Server 2012 R2 Standard operating system
- MS SQL 2014 Standard database
- Microsoft Enhanced Mitigation Experience Toolkit (EMET) version 4.1
- Dell Systems Management Software
    - OpenManage (oma) version 5.2.0.9999
    - OpenManage Server Administrator 7.2.0
- Microsoft Cryptographic Primitives Library (bcryptprimitives.dll and ncryptsslp.dll) in Windows Server 2012 R2, (CMVP Certificate #2357)
- OpenSSL FIPS Object Module v2.0.10

The Password Safe managed systems and their corresponding clients and services are in the operational environment.

2.4.1.1 Software Requirements

The TOE requires compatible software to be installed on client machines in order to access the BeyondInsight Management GUI and the Password Safe Web Portal GUI:

- Supported browsers:
    - Firefox 48 or later

  - Chrome 54 or later
  - Safari 8 or later
  - Microsoft Internet Explorer 10+, 11 preferred
- Adobe Flash Player version 22.0 or higher
- Any SSH client (i.e. PuTTY)
- Any RDP client (i.e. Microsoft Terminal Server Client)

The TOE relies on the following services and products in the operational environment:

- Active Directory
- Power Broker for Windows Client (installed on Windows managed system platforms only)[2]

2.4.1.2 Hardware Requirements

The TOE software is delivered pre-installed on the BeyondTrust UVM20 and UVM50 Security Management hardware appliances. Each appliance is considered part of the operational environment. The appliances differ only in processing capability and storage capacities.

	UVM20	UVM50
10/100/1000 Mbps Network Ports	4	4
Microprocessor	Single Xeon, 2.4 GHz, 6-core	Dual Xeon, 2.6 GHz, 8-core per CPU
RAM	32 GB	128 GB
Storage	4 x 1TB (RAID 10 - 2TB)	8 x 1 TB (RAID 1 - 4TB)
Operating System	Windows Server 2012 R2 Standard	Windows Server 2012 R2 Standard
Database	MS SQL 2014 Standard	MS SQL 2014 Standard

Table 3: Platform Components

2.4.2 Logical Boundaries

This section summarizes the security functions provided by the TOE:

- Security audit
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels
- Enterprise Security Management

2.4.2.1 Security Audit

The TOE is designed to be able to generate logs for security relevant events including the events specified in [ESMICM]. The audit records identify the date/time, event type, outcome of the event, responsible subject/user, as well as the additional event-specific content indicated in **Table 6**. The TOE stores the audit records locally in the

[2] The TOE establishes a trusted channel (using the Microsoft Server 2012 R2 cryptographic libraries) with the agent on Windows managed systems to update passwords.

Microsoft SQL Server 2014 Database and the Front End Logs on the Microsoft Windows Server 2012 R2. The operational environment protects the stored audit records from unauthorized deletion and modification.

2.4.2.2 Identification and Authentication

The TOE provides authentication failure handling for TOE administrators and associates identity, roles, and groups with both TOE users and TOE Administrators.

2.4.2.3 Security Management

All TSF-relevant administrative actions are performed via the BeyondInsight Management GUI. The TOE uses Role-Based Access Control which defines access to functionality within the TSF only after the TOE user and/or the TOE administrator have provided acceptable user identification and authentication data to the TOE.

2.4.2.4 Protection of the TSF

Credentials/keys used by the TOE are stored in the operational environment. The TOE does not offer any functions that will disclose a stored cryptographic key to any subject; all keys are stored encrypted using AES-256.

The TOE relies upon the operational environment to ensure that reliable time information is available (e.g., for log accountability).

2.4.2.5 TOE Access

The TOE can be configured to display an informative banner that will appear prior to authentication when accessing the BeyondInsight Management GUI and the Password Safe Web Portal GUI. The administrator can terminate their own interactive session.

2.4.2.6 Trusted path/channels

The TOE protects interactive communication with TOE users and TOE Administrators using HTTPS. The TOE protects communication with external IT entities, including authentication servers, using TLS connections, which prevent unintended disclosure or modification of data. The TOE uses cryptographic means to protect communication with remote administrators. When the TOE is configured to use the services of an authentication server in the operational environment, the communication between the TOE and the operational environment component is protected using TLS encryption. The communication between the TOE and managed systems, and PowerBroker for Windows is protected using TLS or SSH.

2.4.2.7 Enterprise Security Management

The TOE authenticates BeyondInsight Administrators and relies on Microsoft Active Directory in the operational environment to authenticate Password Safe users.

The TOE enrolls enterprise users and assigns unique identifying data. The TOE provides the capability to define and securely transmit identity and credential data for automated password and session management solutions. The TOE provides a password restriction policy mechanism to ensure secure passwords are defined for the managed accounts that TOE users can use to access managed systems.

2.5 TOE Documentation

There are numerous documents that provide information and guidance for the deployment of the TOE. In particular, the Common Criteria specific guides that reference the security-related guidance material for all products evaluated are identified below:

- *BeyondInsight Authentication Guide,* Version 6.2 – February 2017 (BeyondTrust proprietary)
- *BeyondInsight Installation Guide,* Version 6.2 – November 2016 (BeyondTrust proprietary)
- *BeyondInsight User Guide User Guide,* Version 6.2 – November 2016 (BeyondTrust proprietary)
- *PowerBroker Password Safe Administration Guide,* Version 6.2 – November 30 2016 (BeyondTrust proprietary)

- *BeyondTrust UVM Appliance Getting Started Guide, Software Version: UVM Appliance 2.1,* Revision Number: 0, January 2017 (BeyondTrust proprietary)
- *PowerBroker Password Safe v6.2.0 Common Criteria – Supplementary Guide,* March 22, 2018

Note: The proprietary guidance documents are provided only to registered customers.

3. Security Problem Definition

This security target includes by reference the Security Problem Definition (composed of organizational policies, threat statements, and assumptions) with the optional assumptions: A.CRYPTO, A.ROBUST, and A.SYSTIME from the [ESMICM].

In general, the [ESMICM] focuses on the aspect of ESM that is responsible for enforcing identity and credential management. Identity and Credential Management products will generate and issue credentials for subjects that reside within the enterprise.

4. Security Objectives

Like the Security Problem Definition, this security target includes by reference the Security Objectives from the [ESMICM]. The [ESMICM] security objectives for the operational environment are reproduced below, since these objectives characterize technical and procedural measures each consumer must implement in their operational environment.

In general, the [ESMICM] has presented a Security Objectives appropriate for Identity and Credential Management products will generate and issue credentials for subjects that reside within the enterprise, and as such are applicable to the TOE.

4.1 Security Objectives for the Environment

Objective	Environmental Security Objective Definition
OE.ADMIN	There will be one or more administrators of the Operational Environment that will be responsible for providing subject identity to attribute mappings within the TOE.
OE.CRYPTO	The Operational Environment will provide cryptographic mechanisms that are used to ensure the confidentiality and integrity of communications.
OE.ENROLLMENT	The Operational Environment will provide a defined enrollment process that confirms user identity before the assignment of credentials.
OE.FEDERATE	Data the TOE exchanges with trusted external entities is trusted.
OE.INSTALL	Those responsible for the TOE shall ensure that the TOE is delivered, installed, managed, and operated in a manner that is consistent with IT security.
OE.MANAGEMENT	The Operational Environment will provide an Authentication Server component that uses identity and credential data maintained by the TOE.
OE.PERSON	Personnel working as TOE administrators shall be carefully selected and trained for proper operation of the TOE.
OE.ROBUST	The Operational Environment will provide mechanisms to reduce the ability for an attacker to impersonate a legitimate user during authentication.
OE.SYSTIME	The Operational Environment will provide reliable time data to the TOE.

Table 4: Security Objectives for the Environment

5. IT Security Requirements

This section defines the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) that serve to represent the security functional claims for the Target of Evaluation (TOE) and to scope the evaluation effort.

The SFRs have all been drawn from the Protection Profile (PP): *Standard Protection Profile for Enterprise Security Management Identity and Credential Management*, Version 2.1, October 24, 2013 [ESMICM].

As a result, refinements and operations already performed in that PP are not identified (e.g., highlighted) here, rather the requirements have been copied from that PP and any residual operations have been completed herein. Of particular note, the [ESMICM] made a number of refinements and completed some of the SFR operations defined in the CC and that PP should be consulted to identify those changes if necessary.

The SARs are the set of SARs specified in [ESMICM].

5.1 Extended Requirements

All of the extended requirements in this ST have been drawn from the [ESMICM]. The [ESMICM] defines the following extended SFRs and since they are not redefined in this ST, the [ESMICM] should be consulted for more information in regard to those CC extensions.

- ESM_EAU.2 Reliance on Enterprise Authentication
- ESM_EID.2 Reliance on Enterprise Identification
- ESM_ICD.1 Identity and Credential Definition
- ESM_ICT.1 Identity and Credential Transmission
- FAU_STG_EXT.1 External Audit Trail Storage
- FPT_APW_EXT.1 Protection of Stored Credentials
- FPT_SKP_EXT.1 Protection of Secret Key Parameters

5.2 TOE Security Functional Requirements

The following table identifies the SFRs that are satisfied by the Password Safe.

Requirement Class	Requirement Component
FAU: Security audit	FAU_GEN.1: Audit Data Generation
	FAU_STG_EXT.1: External Audit Trail Storage
FIA: Identification and authentication	FIA_USB.1: User-Subject Binding
	FIA_AFL.1: Authentication Failure Handling
FMT: Security management	FMT_MOF.1: Management of Functions Behavior
	FMT_SMF.1: Specification of Management Functions
	FMT_SMR.1: Security Management Roles
FPT: Protection of the TSF	FPT_APW_EXT.1: Protection of Stored Credentials
	FPT_SKP_EXT.1: Protection of Secret Key Parameters
FTA: TOE access	FTA_SSL.4: User-initiated Termination
	FTA_TAB.1: Default TOE Access Banners
FTP: Trusted path/channels	FTP_ITC.1: Trusted Channel
	FTP_TRP.1: Trusted Path
ESM: Enterprise Security Management	ESM_EAU.2(1): Reliance on Enterprise Authentication [BeyondInsight Administrator]
	ESM_EAU.2(2): Reliance on Enterprise Authentication [Password Safe Users]
	ESM_EID.2(1): Reliance on Enterprise Identification [BeyondInsight Administrator]
	ESM_EID.2(2): Reliance on Enterprise Identification [Password Safe Users]
	ESM_ICD.1: Identity and Credential Definition
	ESM_ICT.1: Identity and Credential Transmission

Table 5: TOE Security Functional Components

5.2.1 Security Audit (FAU)

5.2.1.1 Audit Data Generation FAU_GEN.1

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions; and
b) All auditable events identified in **Table 6** for the not specified level of audit; and
c) [**no other auditable events**].

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and
b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, [**information specified in column three of Table 6**].

Component	Event	Additional Information
ESM_EAU.2(1)	All use of the authentication	None

Component	Event	Additional Information
	mechanism	
ESM_EAU.2(2)	All use of the authentication mechanism	None
ESM_ICD.1	Creation and modification of identity and credential data.	The attribute(s) modified
ESM_ICD.1	Enrollment or modification of subject	The subject created or modified, the attribute(s) modified (if applicable)
ESM_ICT.1	All attempts to transmit information	The destination to which the transmission was attempted
FAU_STG_EXT.1	Establishment and disestablishment of communications with audit server Audit records are sent to the internal audit log storage only	Identification of audit server
FIA_AFL.1	The reaching of an unsuccessful authentication attempt threshold, the actions taken when the threshold is reached, and any actions taken to restore the normal state	Action taken when threshold is reached
FMT_MOF.1	All modifications of TSF function behavior	None
FMT_SMF.1	Use of the management functions	Management function performed
FTA_SSL.4	All session termination events	None
FTP_ITC.1	All use of trusted channel functions	Identity of the initiator and target of the trusted channel
FTP_TRP.1	All attempted uses of the trusted path functions	Identification of user associated with all trusted path functions, if available

Table 6: Auditable Events

5.2.1.2 External Audit Trail Storage FAU_STG_EXT.1

FAU_STG_EXT.1.1 The TSF shall be able to transmit the generated audit data to [**Microsoft SQL Server 2014 Database and Front End Logs on the Microsoft Windows Server 2012 R2**].

FAU_STG_EXT.1.2 The TSF shall ensure that transmission of generated audit data to any external IT entity uses a trusted channel defined in FTP_ITC.1.

FAU_STG_EXT.1.3 The TSF shall ensure that any TOE-internal storage of generated audit data:

- protects the stored audit records in the TOE-internal audit trail from unauthorized deletion; and
- prevents unauthorized modifications to the stored audit records in the TOE-internal audit trail.

5.2.2 Identification and Authentication (FIA)

5.2.2.1 Authentication Failure Handling FIA_AFL.1

FIA_AFL.1.1 The TSF shall detect when [***an administrator configurable positive integer within [1 to 999]***] unsuccessful authentication attempts occur related to [**unsuccessful TOE Administrator login attempts**].

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been [***surpassed***] the TSF shall [**lock the TOE Administrator account for the duration specified in the "Lockout period" setting**].

5.2.2.2 User-Subject Binding FIA_USB.1

FIA_USB.1.1 The TSF shall associate the following user security attributes with subjects acting on the behalf of that user: **[username, role, group].**

FIA_USB.1.2 The TSF shall enforce the following rules on the initial association of user security attributes with subjects acting on the behalf of users: **[successful user authentication provides for the initial association of attributes].**

FIA_USB.1.3 The TSF shall enforce the following rules governing changes to the user security attributes associated with subjects acting on the behalf of users: **[user is associated with their assigned group or role when authenticated to the TSF].**

5.2.3 Security Management (FMT)

5.2.3.1 Management of Functions Behavior FMT_MOF.1

FMT_MOF.1 The TSF shall restrict the ability to [***determine the behavior of, disable, enable, modify the behavior of***] the functions: **[list of functions in Table 7]** to [**the Role identified in Table 7**].

Requirement	Management Activities	Role	Operation
ESM_EAU.2(1)	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	BeyondInsight Administrator	Determine/modify the behavior of
ESM_EID.2(1)	Management of authentication data for both interactive users and authorized IT entities (if managed by the TSF)	BeyondInsight Administrator	Determine/modify the behavior of
ESM_ICD.1	Definition of identity and credential data that can be associated with users (activate, suspend, revoke credential, etc.)	BeyondInsight Administrator	Full control over establishment, removal etc. of enterprise user's identity and credential data defined within Password Safe. (Determine/modify the behavior of)
ESM_ICD.1	Management of credential status	BeyondInsight Administrator	Determine/modify the behavior of Enable/Disable
ESM_ICD.1	Enrollment of users into repository	BeyondInsight Administrator	(Determine/modify the behavior of)

Requirement	Management Activities	Role	Operation
ESM_ICT.1	Configuration of circumstances in which transmission of identity and credential data (and object attributes, if applicable) is performed	BeyondInsight Administrator	Determine/modify the behavior of
FAU_STG_EXT.1	Configuration of external audit storage location The TOE uses audit storage preconfigured in the operational environment in the Microsoft SQL Server 2014 database and the Front End Logs on the Microsoft Windows Server 2012 R2 installed within the appliance. No configuration is necessary.	BeyondInsight Administrator	N/A
FIA_AFL.1	Management of the threshold for unsuccessful authentication attempts Management of actions to be taken in the event of an authentication failure	BeyondInsight Administrator	Enable/Disable Determine/modify the behavior of
FIA_USB.1	Definition of default subject security attributes, modification of subject security attributes	BeyondInsight Administrator	Determine/modify the behavior of
FMT_MOF.1	Management of sets of users that can interact with security functions	BeyondInsight Administrator	Determine/modify the behavior of
FMT_SMR.1	Management of the users that belong to a particular role	BeyondInsight Administrator	Determine/modify the behavior of
FTA_TAB.1	Maintenance of the banner	BeyondInsight Administrator	Enable/Disable the banner including the message that will be displayed
FTP_ITC.1	Configuration of actions that require trusted channel (if applicable)	BeyondInsight Administrator	Enable/Disable
FTP_TRP.1	Configuration of actions that require trusted path (if applicable)	BeyondInsight Administrator	N/A

Table 7: Management Functions

5.2.3.2 Specification of Management Functions FMT_SMF.1

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions: **[the management functions identified in Table 7]**.

5.2.3.3 Specification of Management Roles FMT_SMR.1

FMT_SMR.1.1 The TSF shall maintain the roles [**BeyondInsight Administrator**].

FMT_SMR.1.2 The TSF shall be able to associate users with roles.

5.2.4 Protection of the TSF (FPT)

5.2.4.1 Protection of Stored Credentials FPT_APW_EXT.1

FPT_APW_EXT.1.1 The TSF shall store credentials in non-plaintext form.

FPT_APW_EXT.1.2 The TSF shall prevent the reading of plaintext credentials.

5.2.4.2 Protection of Secret Key Parameters FPT_SKP_EXT.1

FPT_SKP_EXT.1.1 The TSF shall prevent reading of all pre-shared keys, symmetric key, and private keys.

5.2.5 TOE Access (FTA)

5.2.5.1 User-initiated Termination FTA_SSL.4

FTA_SSL.4.1 The TSF shall allow Administrator-initiated termination of the Administrator's own interactive session.

5.2.5.2 Default TOE Access Banner FTA_TAB.1

FTA_TAB.1.1 Before establishing a user session, the TSF shall display a configurable advisory warning message regarding unauthorized use of the TOE.

5.2.6 Trusted path/channels (FTP)

5.2.6.1 Trusted Channel FTP_ITC.1

FTP_ITC.1.1[3] The TSF shall be capable of using [***SSH, TLS***] to provide a trusted communication channel between itself and authorized IT entities supporting the following capabilities: ***[authentication server, [communication with managed systems, communication with PowerBroker for Windows]***] that is logically distinct from other communication channels and provides assured identification of its end points and protection of the channel data from disclosure and detection of modification of the channel data..

FTP_ITC.1.2 The TSF shall permit the TSF or the authorized IT entities to initiate communication via the trusted channel.

FTP_ITC.1.3 The TSF shall initiate communication via the trusted channel for transfer of policy data, [[***authentication using external authentication servers***]]**.**

5.2.6.2 Trusted Path FTP_TRP.1

FTP_TRP.1.1[4] The TSF shall be capable of using [***HTTPS, TLS***] to provide a communication path between itself and remote users that is logically distinct from other communication channels and provides assured identifications of its end points and protection of the communicated data from modification, disclosure, and [***no other types of integrity or confidentiality violations***].

FTP_TRP.1.2 The TSF shall permit remote users to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for initial user authentication and execution of management functions.

[3] Modified per NIAP TD0245
[4] Modified per NIAP TD0245

5.2.7 Enterprise Security Management (ESM)

5.2.7.1 Reliance on Enterprise Authentication ESM_EAU.2(1) [BeyondInsight Administrator]

ESM_EAU.2.1(1) The TSF shall rely on **[*BeyondInsight internal authentication*]** for ~~subject~~ **BeyondInsight Administrator** authentication.

ESM_EAU.2.2(1) The TSF shall require each ~~subject~~ **BeyondInsight Administrator** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that subject.

5.2.7.2 Reliance on Enterprise Identification ESM_EID.2(1) [BeyondInsight Administrator]

ESM_EID.2.1(1) The TSF shall rely on **[*BeyondInsight internal authentication*]** for ~~subject~~ **BeyondInsight Administrator** identification.

ESM_EID.2.2(1) The TSF shall require each ~~subject~~ **BeyondInsight Administrator** to be successfully identified before allowing any other TSF-mediated actions on behalf of that subject.

5.2.7.3 Reliance on Enterprise Authentication ESM_EAU.2(2) [Password Safe Users]

ESM_EAU.2.1(2) The TSF shall rely on **[*/Microsoft Active Directory/*]** for ~~subject~~ **Password Safe User** authentication.

ESM_EAU.2.2(2) The TSF shall require each ~~subject~~ **Password Safe User** to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that subject.

5.2.7.4 Reliance on Enterprise Identification ESM_EID.2(2) [Password Safe Users]

ESM_EID.2.1(2) The TSF shall rely on **[*/Microsoft Active Directory/*]** for ~~subject~~ **Password Safe User** identification.

ESM_EID.2.2(2) The TSF shall require each ~~subject~~ **Password Safe User** to be successfully identified before allowing any other TSF-mediated actions on behalf of that subject.

5.2.7.5 Identity and Credential Definition ESM_ICD.1

ESM_ICD.1.1 The TSF shall provide the ability to define identity and credential data for use with other Enterprise Security Management products.

ESM_ICD.1.2 The TSF shall define the following security-relevant identity and credential attributes for enterprise users: credential lifetime, credential status, [**username, user group, asset, domain, password**].

ESM_ICD.1.3 The TSF shall provide the ability to enroll enterprise users through assignment of unique identifying data.

ESM_ICD.1.4 The TSF shall provide the ability to associate defined security-relevant attributes with enrolled enterprise users.

ESM_ICD.1.5 The TSF shall provide the ability to query the status of an enterprise user's credentials.

ESM_ICD.1.6 The TSF shall provide the ability to revoke an enterprise user's credentials.

ESM_ICD.1.7 The TSF shall provide the ability for a compatible Authentication Server ESM product to update an enterprise user's credentials.

ESM_ICD.1.8 The TSF shall ensure that the defined enterprise user credentials satisfy the following strength rules:

a) For password-based credentials, the following rules apply:

1. Passwords shall be able to be composed of a subset of the following character sets: [**upper case letters, lower case letters, numbers, and non-alphanumeric characters**] that include the following values [**A-Z, a-z, 0-9, (“!”, “@”, “#”, “$”, “%”, “^”, “&”, “*”, “(“, “)”, “<”, “>”, ”?”, “,”, “.”, “:”)];** and

2. Minimum password length shall settable by an administrator, and support passwords of 15 characters or greater; and

3. Password composition rules specifying the types and numbers of required characters that comprise the password shall be settable by an administrator; and

4. Passwords shall not be reused within the last administrator-settable number of passwords used by that user;

b) For non-password-based credentials, the following rules apply:

1. The probability that a secret can be obtained by an attacker during the lifetime of the secret is less than 2^{-20}.

5.2.7.6 Identity and Credential Transmission ESM_ICT.1

ESM_ICT.1.1 The TSF shall transmit [***identity and credential data***] to compatible and authorized Enterprise Security Management products under the following circumstances: [***immediately following creation or modification of data, at a periodic interval, at the request of the product***].

Application Note: *Specific compatible and authorized Enterprise Security Management products include Active Directory. Also note that since identity and credential data is transmitted to managed systems, any ESM Access Control product that resides on a managed system can also use this data as inputs to enforcement of a host-based access control policy.*

5.3 TOE Security Assurance Requirements

The security assurance requirements for the TOE are included by reference from the NDPP.

Requirement Class	Requirement Component
ADV: Development	ADV_FSP.1 Basic functional specification
AGD: Guidance documents	AGD_OPE.1: Operational user guidance
	AGD_PRE.1: Preparative procedures
ALC: Life-cycle support	ALC_CMC.1 Labelling of the TOE
	ALC_CMS.1 TOE CM coverage
ATE: Tests	ATE_IND.1 Independent testing – conformance
AVA: Vulnerability assessment	AVA_VAN.1 Vulnerability survey

Table 8: Assurance Components

Consequently, the assurance activities specified in [ESMICM] apply to the TOE evaluation.

6. TOE Summary Specification

This chapter describes the security functions:

- Security audit
- Identification and authentication
- Security management
- Protection of the TSF
- TOE access
- Trusted path/channels
- Enterprise Security Management.

6.1 Security Audit

The TOE stores audit records in the operational environment in the Microsoft SQL Server 2014 database and to the Front End Logs on the Microsoft Windows Server 2012 R2 installed within the appliance. Reliable timestamps are provided by the operational environment.

6.1.1 FAU_GEN.1 Audit Data Generation

The TOE generates audit events for startup and shutdown of the audit function. Startup/shutdown of the audit function occurs when the product is started/stopped. Auditing cannot be turned off. The TOE generates audit events for all of the events in **Table 6**.

The generated audit records identify the date and time, the nature or type of the triggering event, an indication of whether the event succeeded, failed or had some other outcome, and the identity of the agent (e.g. user) responsible for the event. The logged audit records also include event-specific content that includes at least all of the content required in **Table 6**.

Session monitoring records the actions of a TOE user while they are accessing the password protected assets through the session proxy. All recorded RDP or SSH sessions can be replayed. Recorded sessions can be viewed by any user who has been assigned the role of BeyondInsight Administrator, Auditor, or Recorded Session Reviewer.

6.1.2 FAU_STG_EXT.1 External Audit Trail Storage

The TOE stores audit records in the operational environment in the Microsoft SQL Server 2014 database and the Windows Front End Logs on the appliance. The database contains the audit records related to user activity while the Windows Front End Logs contain all of the audits including those related to the transmission of information across trusted channels. The audit records are accessed through the BeyondInsight GUI.

Since the audit storage locations are located on the same machine as the TOE, the secure communication connection is provided by a direct, platform-internal channel rather than cryptographic protocols. This architecture prevents the possibility of audit loss due to broken networked channel connections; and ensures all audit records generated are indeed stored in the audit log.

The storage of generated audit data is in the operational environment and therefore the TOE relies on the environment to protect the stored audit records from unauthorized deletion; and to prevent unauthorized modifications to the stored audit records in the audit trail.

6.2 Identification and Authentication

The TOE is designed to require TOE users and TOE Administrators to be identified and authenticated before they can access any of the TOE functions. TOE provides authentication failure handling and user-subject binding functions. The only capability allowed prior to TOE users and TOE Administrators authenticating is the display of the warning banner.

6.2.1 FIA_AFL.1 Authentication Failure Handling

The TOE enforces a maximum failed login attempts value that is configurable by the administrator. The lockout options are applicable to locally defined BeyondInsight Administrators using the BeyondInsight Management GUI interface or the Password Safe Web Portal GUI.

The default value is 3 consecutive unsuccessful attempts after which the BeyondInsight Administrator is denied any further opportunity to log in for the duration specified by the “Lockout period” setting (which is also configurable by the administrator). The maximum number of login attempts value can be set to any integer from 0 to 999. The default lockout period value is disabled but can be configured to any integer from 0 to 999 minutes. When the Account Lockout Duration is set to 0 and the Account Lockout threshold is exceeded, the BeyondInsight Administrator account is locked out until the account gets unlocked manually. Setting the Account Lockout Duration to 0 disables auto-unlock, but not the functionality to lock an account should there be too many incorrect attempts. In the evaluated configuration, the Account Lockout function must be enabled and the Duration set to a value greater than 0.

6.2.2 FIA_USB.1 User-Subject Binding

The TOE associates TOE user and BeyondInsight Administrator security attributes with subjects acting on the behalf of those users. The BeyondInsight Administrator group is created by default and the permissions assigned to the group cannot be changed. TOE Administrators are defined by association of their usernames with the BeyondInsight Administrator group. Members of this group have full access to the TOE. The TOE binds the username and group attributes to the BeyondInsight Administrators upon successful authentication. The group membership is evaluated at login.

After a BeyondInsight Administrator creates a Password Safe user group, Active Directory users are added to the group, making them TOE users. A BeyondInsight Administrator assigns a Password Safe role to the group, thus defining privileges. The group membership is evaluated at login. Permissions and role changes to the Password Safe groups take effect immediately upon next login. The security attributes are associated with the Password Safe users upon successful logging into the TOE. A BeyondInsight Administrator may modify the role assigned to the group, thus modifying the privileges assigned to that group.

6.3 Security Management

A BeyondInsight administrator logs on through the BeyondInsight Management GUI to perform security management functions to set up managed systems and managed accounts. The Password Safe users log on through the Password Safe Web Portal GUI to request/approve password releases. The TOE uses Role-Based Access Control which defines access to functionality within the TSF only after acceptable user identification and authentication data has been provided to the TOE.

6.3.1 FMT_MOF.1 Management of Functions Behavior

A BeyondInsight Administrator has full access to objects and every right within the TOE. This is the only default capability that has this access. Refer to **Table 7: Management Functions** for the role restrictions that the TOE places on the management functions.

6.3.2 FMT_SMF.1 Specification of Management Functions

The TOE provides the management functions identified in **Table 7: Management Functions**.

6.3.3 FMT_SMR.1 Management Roles

A BeyondInsight Administrator has full access to objects and every right within the BeyondInsight IT Risk Management platform and the Password Safe functionality. The BeyondInsight Administrator user group is created by default and the permissions assigned to the group cannot be changed. Password Safe roles can only be assigned by a member of the BeyondInsight Administrator group. All changes to Password Safe user accounts must be managed by a BeyondInsight Administrator account.

Password Safe provides the following predefined roles:

- Requester – The Requester role enables the TOE user or group to submit a request to retrieve a managed password. Typically, system administrators and network engineers are assigned to this role.
- Approver – The Approver role enables the TOE user or group to approve requests from Requesters or Approver/Requesters for the release of managed passwords.
- Approver/Requester – This cross-functional role enables the TOE user or group to submit or approve requests for password releases. However, this individual cannot approve her own request when dual control is enforced. This role is typically used in a peer approval environment.
- Auditor – The Auditor role enables the TOE user to review Replay Sessions when logged into the Web Portal.
- Information Security Administrator (ISA) – The ISA role permits the bypass the approval workflows for accessing passwords and establishing session.
- No Roles – Assign this role to remove any previously assigned roles from a TOE user or group.
- Recorded Session Reviewer – allows the TOE user to view recorded Password Safe sessions. The TOE user can add comments and mark the session as reviewed. The TOE user can also archive sessions if configured on an appliance.

The TOE provides the management functions necessary to manage the TOE; specifically those identified in **Table 7**.

6.4 Protection of the TSF

Credentials and keys used by the TOE are stored in the operational environment. The TOE implements a number of features designed to protect itself to ensure the reliability and integrity of its security features.

6.4.1 FPT_APW_EXT.1 Protection of Stored Credentials

The passwords of BeyondInsight Administrator accounts created for the purpose of logging on and managing the TOE are stored in the SQL Server 2014 database (AppUser table). The TOE does not provide any interfaces for a non-administrator to access the SQL Server 2014 database (AppUser) table or provide any interfaces to read a plaintext credential. The BeyondInsight Administrator passwords are stored as hashed values using the Microsoft Server 2012 R2 SHA512CryptoServicesProvider (.NET Framework).

The TOE uses the Microsoft Server 2012 R2 AESCryptoServiceProvider (.NET Framework) to encrypt the stored passwords for the managed accounts and functional accounts. The passwords are stored encrypted using AES-256 in the SQL Server database in the operational environment and are protected from unauthorized access or disclosure. The TOE does not provide any interfaces for a non-administrator to access the Windows Server 2012 file system or provide any interfaces to read a plaintext credential

The TOE does not store passwords for Password Safe users. The TOE stores the hash value for an empty string and uses pass through authentication to validate an external Active Directory authentication request.

6.4.2 FPT_SKP_EXT.1 Protection of Secret Key Parameters

The TOE stores all pre-shared keys, symmetric keys, and private keys encrypted using ASE-256 in the SQL Server database in the operational environment. The encryption key is stored in the registry, protected by an ACL and by encrypting the secret key using the Microsoft DPAPI and the Machine Key. The encryption key is protected within the hardened appliance and optionally stored in a PKCS#11 compliant Hardware Security Module (HSM).

An administrator is unable to read or view any keys through "normal" interfaces.

6.5 TOE Access

6.5.1 FTA_SSL.4.1 User-initiated Termination

The remote administrator can terminate their own interactive web session. The administrator clicks the "Log Out" button in the BeyondInsight Management GUI and the Password Safe Web Portal GUI to terminate the session.

6.5.2 FTA_TAB.1 TOE Access Banner

The TOE displays a configurable advisory warning message regarding unauthorized use of the TOE before establishing a TOE user or administrator session for the BeyondInsight Management GUI and the Password Safe Web Portal GUI.

6.6 Trusted Path/Channels

Password Safe relies upon the third party Microsoft Cryptographic Primitives Library (CMVP Certificate # 2357) and the OpenSSL library in the operational environment to provide for all communications with trusted external IT entities, and with remote TOE users and TOE Administrators accessing the TOE via the BeyondInsight Management GUI and the Password Safe Web Portal GUI.

6.6.1 FTP_ITC.1 Inter-TSF Trusted Channel

The TSF initiates communication via the trusted channel for transfer of policy data, and for authentication using external authentication. The TSF also permits PowerBroker for Windows and Windows managed systems to initiate communication via the trusted channel.

Password Safe users require the use of an external AD authentication server to perform authentication requests to the TOE. The communication path is protected from modification and disclosure via a TLS protected channel via the Microsoft Server 2012 R2 cryptographic libraries.

The transfer of the TOE identity and credential data with PowerBroker for Windows is protected via TLS using the Microsoft Server 2012 R2 cryptographic libraries.

All policy data is transmitted both to and from managed systems using SSH or RDP (tunneled via TLS) which is provided by OpenSSL in the operational environment.

Components providing the protected communication are identified below:

- Microsoft Server 2012 R2 cryptographic libraries
  - Password Safe Requester connection – with Password Safe (HTTPS)
  - Password Safe communication with Active Directory (TLS)
  - Password Safe with managed system - transfer of policy data (TLS)
  - Password Safe with PowerBroker for Windows
- The TOE is configured to use FIPS Approved algorithms (CAVP certificate numbers AES: #5327; RSA: #2855; DSA: #1377; SHA: #4279; DRBG: #2057; HMAC: #3525; CVL: #1794; CVL: #1795 (KDF135)) for the following communications:
  - Password Safe Requester SSH connection (from user client machine with TOE)
  - Password Safe Requester connection SSH - with managed system

- Password Safe with managed system configuration – transfer of policy data (SSH)
- Password Safe Requester RDP connection –with managed system (TLS)

6.6.2 FTP_TRP.1 Trusted Path

The TOE requires TOE users and TOE Administrators to initiate communication via the trusted path for initial user authentication, and execution of management functions. Password Safe users access the Password Safe Web Portal GUI to perform activities such as executing password requests. The communication channel is protected using HTTPS in the operational environment.

The TOE uses HTTPS/TLS for secure administrative access which is provided by the third party Microsoft Server 2012 R2 cryptographic libraries.

6.7 Enterprise Security Management

The TOE is designed to require TOE users and TOE Administrators to be identified and authenticated before they can access any of the TOE functions.

6.7.1 ESM_EAU.2(1) Reliance on Enterprise Authentication (BeyondInsight Administrator)

BeyondInsight administrators authenticate to the TOE using their username and password which are stored locally in the SQL Server 2014 database. The TOE requires each administrator to be successfully identified and authenticated before allowing any TSF-mediated actions on behalf of that subject.

6.7.2 ESM_EAU.2(2) Reliance on Enterprise Authentication (Password Safer User)

Password Safe users are authenticated using external Active Directory Servers. The TOE requires each user to be successfully identified and authenticated before allowing any TSF-mediated actions on behalf of that subject.

6.7.3 ESM_EID.2(1) Reliance on Enterprise Identification (BeyondInsight Administrator)

See Section 6.7.1 ESM_EAU.2(1) Reliance on Enterprise Authentication (BeyondInsight Administrator).

6.7.4 ESM_EID.2(2) Reliance on Enterprise Identification (Password Safer User)

See Section 6.7.2 ESM_EAU.2(2) Reliance on Enterprise Authentication (Password Safer User).

6.7.5 ESM_ICD.1 Identity and Credential Definition

TOE users are authorized to access the TSF to request permission from the TOE to access managed systems. A managed system is a computer where one or more account passwords are maintained by The TOE. Managed systems can be Windows machines, Linux machines, and Active Directory domains. Managed accounts are local to a Managed System whose password is being stored and maintained through Password Safe.

The TOE enrolls enterprise users and assigns unique identifying data that is associated with the enterprise users and their defined security-relevant attributes.

Once enrolled, all enterprise user credentials are valid and current. A BeyondInsight Administrator can define the following security relevant identity and credential attributes: credential lifetime, credential status, username, user group, asset, domain, and password for the managed accounts. The credential lifetime, credential status, asset, user group, and domain attributes are only defined on Password Safe. The username and password are defined on the TOE and credential consistency is maintained with the managed account.

The TOE provides the ability to automatically update a managed account's password. The frequency of the password changes is configurable in Password Safe. Automatic password changes are controlled by the TOE. Credential

lifetime is defined in the Managed Account Settings using the password change settings. Change Frequency specifies how often the password will be changed in days or by first/last day of the month. Change Password After any Release specifies a maximum password age at which point, the password will be changed. The passwords are changed on the managed accounts, and the modification of the credential data is recorded. Once the password change has been made on the managed account, the TOE also makes the change to the corresponding managed account on the TOE.

The user account for a TOE user corresponds with their username in the environmental Active Directory. The identity attributes associated with these users are used to create and manage policies within Password Safe and map them to specific groups of systems. For managed accounts on Windows and Linux systems, the combination of username and asset uniquely identifies them. For managed accounts in Active Directory, the combination of username and domain uniquely identifies them. The TSF has the ability to change the passwords of managed accounts. Changes to these credentials initiated on the TOE are replicated on the managed accounts. Enrolled user accounts can be removed from TOE control by deleting the account. Deleting an enrolled user account essentially removes all access via the user account deleted.

Other Enterprise Security Management products such as Active Directory and BeyondTrust PowerBroker for Windows are able to make use of the username and password that is centrally managed by Password Safe. Password Safe transmits enterprise user data that it changes back to AD, Windows, and/or Linux managed systems whenever it changes the credential information for a managed account. For managed accounts existing on Windows and Linux OS platforms, the transmission of identity and credential data to these systems can also be used as inputs to any ESM Access Control capability deployed on those platforms. A TOE user who accesses a managed system using a managed account will have their subject identity on that system be the identity of the managed account. Access control policies can subsequently enforced on that subject. One example of this is the BeyondTrust PowerBroker for Windows which is installed on a Windows machine for privileged Desktop Application Access, Server Access, or Local Administrative Access. The Active Directory user account to be brought under the TOE as a managed system must already be provisioned in Active Directory.

The Active Directory user can be added to an AD group that has roles authorized to log in to managed accounts in Password Safe, which makes them a TOE user. PowerBroker for Windows would have a rule set to launch an application using a managed account. When prompted by PowerBroker for Windows client, the TOE user's username and password would be entered. The PowerBroker for Windows client would authenticate these credentials against Active Directory.

Active Directory group membership is enumerated by Password Safe, and verification that the role is permitted to log in to the managed account is performed. If authorized, the password for the managed account is sent to PowerBroker for Windows over TLS. Windows authenticates the managed account via Active Directory. The application would be launched using this account as the `run-as` credentials.

Upon termination of the privileged session, PowerBroker for Windows will inform Password Safe that the session has been terminated. TOE user accountability is maintained throughout the privileged session. Microsoft Windows creates an audit trail when a TOE user leverages any managed account and uses the `run-as` command. This provides full accountability by connecting a TOE user to the managed account and the application. The Windows machine is responsible for providing audit records of the enterprise user's activity.

The TOE provides methods to maintain TOE user accountability by TOE session recording and a combination of TOE audit records and the managed system audit records.

- One-Click Launch Method - The TOE policy is configured to include session recording and monitoring enabled to provide TOE user accountability. Session monitoring records the actions of a TOE user while they are accessing the password protected assets. The session monitoring is linked to the TOE username.
- Approval Method - The TOE policy is configured to include session recording and monitoring enabled to provide TOE user accountability.
- Password Release - The policy is configured with the Max Concurrent Password Request set to permit only one user to log in using the managed account at a time. The TOE is configured to auto-generate a new password after the password release time period has elapsed. TOE user accountability can be linked by the TOE audit records of user password check out and password release times with the date and time stamps on the of the privileged account audit records on the managed system.

- BeyondTrust PowerBroker for Windows Password Release – TOE user accountability is maintained by the audit logs of the domain administrator username on the managed system.

Password Safe provides the capability to configure password length and complexity requirements for the Managed System Accounts. Password Safe ensures enterprise user credentials for the managed accounts satisfy specified minimum strength rules which are set via Password Rules. The following parameters can be set for the Password Rules:

- Minimum and Maximum Characters – The shortest and longest password that can be created. Valid entries are 4 to 128 (thus supporting minimum password lengths of 15 characters or greater as required by the PP).
- Uppercase Requirements – The allowed or required use of uppercase characters.
- Valid Uppercase Requirements – The selection of the uppercase characters permitted. (A – Z)
- Lowercase Requirements – The allowed or required use of lowercase characters.
- Valid Lowercase Requirements – The select the lowercase characters permitted. (a – z)
- Numeric Requirements – The allowed or required use of numeric characters. (0 -9)
- Non-Alphanumeric Requirements – The allowed or required use of non-alphanumeric characters.
- Valid Non-Alphanumeric Characters – The selection of the non-alphanumeric characters permitted. ("!", "@", "#", "$", "%", "^", "&", "*", "(", ")", “<”, “>”, ”?”, “,”, “.”, “:”).
- Maximum Password Age - The maximum number of days before a password must be changed. Range is 0 to 90 days.

Password credentials for managed accounts are defined by the TSF and changed to new TSF-generated values at intervals scheduled on the TOE or following a manually-initiated request to change them. TOE users cannot manually specify passwords for managed accounts, which prevents their reuse. Passwords are randomly generated by the TOE by placing all of the characters allowed in the Password Rule in an array. It then randomizes that array (shuffle the characters) utilizing the .NET framework RandomNumberGenerator provider (Microsoft Cryptographic Primitives Library (bcryptprimitives.dll and ncryptsslp.dll)). After that, it selects a random character from that array using same provider, shuffles array again, and repeats until it meets the password length specified.

6.7.6 ESM_ICT.1 Identity and Credential Transmission

The TOE transmits identity and credential data to the managed systems as part of the privileged session management. Managed account credentials are changed when enterprise users are first enrolled in Password Safe. The TOE immediately transmits newly created or modified identify and credential data to the managed systems. The changes occur immediately both on the TOE and the Managed Systems.

Passwords can be updated and transmitted at a periodic interval. Passwords for the managed systems can be automatically changed when Automatic Password Management is configured and enabled. The changes occur immediately both on the TOE and the Managed Systems. The change frequency is administrator configurable. The updated credentials are securely transmitted using SSH or TLS.

The TOE makes the decision whether or not to transmit the identity and credential data based upon administrator configured policies via the One-Click Launch Method, Approval Method, Password Release Method, and BeyondTrust PowerBroker for Windows Password Release. Username and password are transmitted via SSH or TLS during the session establishment to the managed system for the authorized user to log onto the managed system.

Password Safe provides the ability for a TOE user to retrieve a password where the session does not need to be managed. The password is delivered immediately following approval of the TOE user’s request (or immediately if the policy is defined to grant automated approval for the request). The retrieved password is securely delivered to the TOE user via HTTPS. The TOE is configured to auto-generate a new password after the password release time period has elapsed.

The TOE can be integrated with the BeyondTrust PowerBroker for Windows for password and session management for any privileged Windows account that is used as a managed account. PowerBroker for Windows will query the TOE policy regarding the password release, and if approved, the TOE will immediately transmit the password credential via TLS to the BeyondTrust PowerBroker for Windows product so that the TOE user can access the managed system. Upon termination of the session, PowerBroker for Windows will inform Password Safe that the

session has been terminated. TOE policy can be configured to automatically update the credential immediately after the session termination.

7. Protection Profile Claims

This ST is conformant to the *Standard Protection Profile for Enterprise Security Management Identity and Credential Management, Version 2.1, October 24,* 2013 including the following optional SFRs: FIA_AFL.1, FTA_SSL.4, and FTA_TAB.1.

As explained in Section 3, the Security Problem Definition of the [ESMICM] has been included in this ST by reference and includes the optional assumptions: A.CRYPTO, A.ROBUST, and A.SYSTIME.

As explained in Section 4, the Security Objectives of the [ESMICM] have been included by reference into this ST. The Security Objectives for the Operational Environment of the [ESMICM] have been copied verbatim into this ST and includes the optional Security Objectives for the Operational Environment: OE.CRYPTO, OE.ROBUST, and OE. SYSTIME

The following table identifies all the Security Functional Requirements (SFRs) in this ST. Each SFR is drawn from the [ESMICM]. The only operations performed on the SFRs drawn from the [ESMICM] are assignment and selection operations.

The following table identifies the SFRs that are satisfied by the TOE.

Requirement Class	Requirement Component	Source
FAU: Security audit	FAU_GEN.1: Audit Data Generation	ESMICM
	FAU_STG_EXT.1: External Audit Trail Storage	ESMICM
FIA: Identification and authentication	FIA_USB.1: User-Subject Binding	ESMICM
	FIA_AFL.1: Authentication Failure Handling	ESMICM
FMT: Security management	FMT_SMF.1: Specification of Management Functions	ESMICM
	FMT_SMR.1: Security Management Roles	ESMICM
	FMT_MOF.1: Management of Functions Behavior	ESMICM
FPT: Protection of the TSF	FPT_SKP_EXT.1: Extended: Protection of TSF Data (for reading of all symmetric keys)	ESMICM
	FPT_APW_EXT.1: Extended: Protection of Administrator Passwords	ESMICM
FTA: TOE access	FTA_SSL.4: User-initiated Termination	ESMICM
	FTA_TAB.1: Default TOE Access Banners	ESMICM
FTP: Trusted path/channels	FTP_ITC.1: Trusted Channel	ESMICM
	FTP_TRP.1: Trusted Path	ESMICM
ESM: Enterprise Security Management	ESM_EAU.2(1): Reliance on Enterprise Authentication [BeyondInsight Administrator]	ESMICM
	ESM_EAU.2(2): Reliance on Enterprise Authentication [Password Safe Users]	ESMICM
	ESM_EID.2(1): Reliance on Enterprise Identification [BeyondInsight Administrator]	ESMICM
	ESM_EID.2(2): Reliance on Enterprise Identification [Password Safe Users]	ESMICM
	ESM_ICD.1 Identity and Credential Definition	ESMICM

Requirement Class	Requirement Component	Source
	ESM_ICT.1 Identity and Credential Transmission	ESMICM

Table 9: SFR Protection Profile Sources

8. Rationale

This security target includes by reference the [ESMICM] Security Problem Definition, Security Objectives, and Security Assurance Requirements. The security target makes no additions to the [ESMICM] assumptions. [ESMICM] security functional requirements have been reproduced with the protection profile operations completed. Operations on the security requirements follow [ESMICM] application notes and assurance activities. Consequently, NDPP rationale applies but is incomplete. The TOE Summary Specification rationale below serves to complete the rationale required for the security target.

This security target includes by reference the ESMICM Security Problem Definition, Security Objectives, and Security Assurance Requirements. The security target makes no additions to the ESMICM assumptions. This security target includes the optional assumptions and objectives from the ESMICM as identified below in the mapping: see **Table 10**. ESMICM security functional requirements have been reproduced with the Protection Profile operations completed. Operations on the security requirements follow ESMICM application notes and assurance activities. Consequently, ESMICM rationale applies but is incomplete. The TOE Summary Specification rationale below serves to complete the rationale required for the security target.

According to Tables 6 and 7 in the [ESMICM] PP the optional assumptions and objectives map as follows.

Assumptions	Objectives	Rational
A.CRYPTO	OE.CRYPTO	It is expected that vendors will typically rely on the usage of cryptographic primitives implemented in the Operational Environment to perform cryptographic protocols provided by the TOE. If the TOE provides its own cryptographic primitives, then this becomes an objective for the TOE rather than for the environment. The TOE does not rely on its own cryptographic primitives and therefore this objective is appropriate for the TOE.
A.ROBUST	OE.ROBUST	The ESM deployment as a whole is expected to provide a login frustration mechanism that reduces the risk of a brute force authentication attack being used successfully against the TSF and defines allowable conditions for authentication (e.g. day, time, location). It is expected that if the TSF does not provide this mechanism, then it will receive this capability from elsewhere in the ESM deployment. If the ST claims FIA_AFL.1, FIA_SOS.1, and FTA_TSE.1, the ST author must exclude this mapping because robust TOE authentication will be provided by the TSF. The ST does not claim FIA_SOS.1 or FTA_TSE.1, therefore this objective along with the OE.ROBUST satisfy the deployment requirement.
A.SYSTIME	OE.SYSTIME	The TSF is expected to use reliable time data in the creation of its audit records. If the TOE is a software-based product, then it is expected that the TSF will receive this time data from a source within the Operational Environment such as a system clock or NTP server. If the ST claims FPT_STM.1, the ST author must exclude this mapping because system time functionality will be provided by

		the TSF. The ST does not claim FPT_STM.1. The TOE is software-based product that receives the reliable time data from a source within the Operational Environment.

Table 10: Mapping of optional assumptions and objectives

8.1 TOE Summary Specification Rationale

Each subsection in Section 6, the TOE Summary Specification, describes a security function of the TOE. Each description is followed with rationale that indicates which requirements are satisfied by aspects of the corresponding security function. The set of security functions work together to satisfy all of the security functions and assurance requirements. Furthermore, all of the security functions are necessary in order for the TSF to provide the required security functionality.

This Section in conjunction with Section 6, the TOE Summary Specification, provides evidence that the security functions are suitable to meet the TOE security requirements. The collection of security functions work together to provide all of the security requirements. The security functions described in the TOE summary specification are all necessary for the required security functionality in the TSF. **Table 11** Security Functions vs. Requirements Mapping demonstrates the relationship between security requirements and security functions.

	Security audit	Identification and authentication	Security management	Protection of the TSF	TOE access	Trusted path/channels	Enterprise Security Management
FAU_GEN.1	X						
FAU_STG_EXT.1	X						
FIA_USB.1		X					
FIA_AFL.1		X					
FMT_SMF.1			X				
FMT_SMR.1			X				
FMT_MOF.1			X				
FPT_APW_EXT.1				X			
FPT_SKP_EXT.1				X			
FTA_SSL.4					X		
FTA_TAB.1					X		
FTP_ITC.1						X	
FTP_TRP.1						X	
ESM_EAU.2(1)							X
ESM_EAU.2(2)							X
ESM_EID.2(1)							X
ESM_EID.2(2)							X
ESM_ICD.1							X
ESM_ICT.1							X

Table 11: Security Functions vs. Requirements Mapping