National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

TM

Validation Report

for

BeyondTrust Password Safe 6.2 (a BeyondInsight component)

Report Number: CCEVS-VR-VID10913-2018
Dated: June 26, 2018
Version: 1.0

National Institute of Standards and Technology
Information Technology Laboratory
100 Bureau Drive
Gaithersburg, MD 20899

National Security Agency
Information Assurance Directorate
9800 Savage Road STE 6940
Fort George G. Meade, MD 20755-6940

Table of Contents

List of Tables

List of Figures

1 Executive Summary

This report is intended to assist the end-user of this product and any security certification agent for that end-user in determining the suitability of this Application Software in their environment. End-users should review the Security Target (ST), which is where specific security claims are made, in conjunction with this Validation Report (VR), which describes how those security claims were evaluated and tested and any restrictions on the evaluated configuration. Prospective users should read carefully the Assumptions and Clarification of Scope in Section 4 and the Validator Comments in Section 10, where any restrictions on the evaluated configuration are highlighted.

This report documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of the BeyondTrust Password Safe 6.2 (a BeyondInsight component). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the Target of Evaluation (TOE) by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST.

The evaluation of the BeyondTrust Password Safe 6.2 (a BeyondInsight component) was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, in the United States and was completed in June 2018. The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, revision 4 and assurance activities specified in *Standard Protection Profile for Enterprise Security Management Identity and Credential Management*, Version 2.1, 24 October 2013, and including the following optional SFRs: FTA_SSL_EXT.1, FTA_SSL.4, and FTA_TAB.1.

The evaluation was consistent with NIAP Common Criteria Evaluation and Validation Scheme (CCEVS) policies and practices as described on their web site (www.niap-ccevs.org).

The Leidos evaluation team determined that the BeyondTrust Password Safe 6.2 (a BeyondInsight component) is conformant to the claimed Protection Profile (PP) and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all of the security functional requirements stated in the ST. The information in this VR is largely derived from the Assurance Activities Report (AAR) [7] and associated test report [6] produced by the Leidos evaluation team.

Password Safe v6.2 (a BeyondInsight component) is an automated password and session management solution for any privileged account, such as shared administrative accounts and local administrative accounts. TOE users 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, Unix/Linux machines, and Active Directory domains.

BeyondTrust Password Safe 6.2 (a BeyondInsight component) contains functionality that is not covered by *Standard Protection Profile for Enterprise Security Management Identity and Credential Management*. As with all evaluations claiming conformance to a NIAP-approved protection profile, only the functionality specified in the profile is evaluated.

The validation team monitored the activities of the evaluation team, examined evaluation evidence, provided guidance on technical issues and evaluation processes, and reviewed the evaluation results produced by the evaluation team. The validation team found that the evaluation results showed that all assurance activities specified in the claimed PPs had been completed successfully and that the product satisfies all of the security functional and assurance requirements stated in the ST. Therefore, the validation team concludes that the testing laboratory's findings are accurate, the conclusions justified, and the conformance results are correct. The conclusions of the testing laboratory in the evaluation technical report are consistent with the evidence produced.

Table 1: Evaluation Details

Item	Identifier
Evaluated Product	BeyondTrust Password Safe 6.2 (a BeyondInsight component)
Sponsor & Developer	BeyondTrust Software, Inc. 5090 N. 40th Street Phoenix, AZ 85018
CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Completion Date	June 2018
CC	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 4, September 2012
Interpretations	There were no applicable interpretations used for this evaluation.
CEM	Common Methodology for Information Technology Security Evaluation: Version 3.1, Revision 4, September 2012
PP	Standard Protection Profile for Enterprise Security Management Identity and Credential Management, Version 2.1, 24 October 2013, and including the following optional SFRs: FIA_AFL.1, FTA_SSL.4, and FTA_TAB.1.
Disclaimer	The information contained in this Validation Report is not an endorsement either expressed or implied of the BeyondTrust Password Safe 6.2 (a BeyondInsight component).
Evaluation Personnel	Dawn Campbell Cody Cummins Pascal Patin Bobby Russ
Validation Personnel	Daniel Faigin, Senior Validator Marybeth Panock, Lead Validator Meredith Hennan, ECR Team

2 Identification

The CCEVS is a joint National Security Agency (NSA) and National Institute of Standards and Technology (NIST) effort to establish commercial facilities to perform trusted product evaluations. Under this program, security evaluations are conducted by commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) in accordance with National Voluntary Laboratory Assessment Program (NVLAP) accreditation.

The NIAP Validation Body assigns Validators to monitor the CCTLs to ensure quality and consistency across evaluations. Developers of information technology products desiring a security evaluation contract with a CCTL and pay a fee for their product's evaluation. Upon successful completion of the evaluation, the product is added to NIAP's Product Compliant List (PCL).

The following table identifies the evaluated Security Target and TOE.

Table 2: ST and TOE Identification

Name	Description
ST Title	BeyondTrust Password Safe 6.2 (a BeyondInsight component) Security Target
ST Version	1.0
Publication Date	June 13, 2018
Vendor	BeyondTrust Software, Inc.
ST Author	Leidos
TOE Reference	BeyondTrust Password Safe 6.2 (a BeyondInsight component)
TOE Software Version	6.2
Keywords	Identity and Credential Management

2.1 Threats

The ST references the *Standard Protection Profile for Enterprise Security Management Identity and Credential Management*, Version 2.1, 24 October 2013, including the following optional SFRs: FIA_AFL.1, FTA_SSL.4, and FTA_TAB.1, The protection profile identifies the following threats, which the TOE and its operational environment are intended to counter:

- An administrator may incorrectly install or configure the TOE resulting in ineffective security mechanisms.
- A malicious user could eavesdrop on network traffic to gain unauthorized access to TOE data.
- A malicious user may falsify the TOE's identity and transmit false data that purports to originate from the TOE to provide invalid data to the ESM deployment.
- A malicious user may falsify the identity of an external entity in order to illicitly request to receive security attribute data or to provide invalid data to the TOE.
- An Assignment Manager may be incapable of using the TOE to define identities, credentials, and attributes in sufficient detail to facilitate authorization and access control, causing other ESM products to behave in a manner that allows illegitimate activity or prohibits legitimate activity.
- A malicious user may attempt to mask their actions, causing audit data to be incorrectly recorded or never recorded.

- A malicious user may attempt to access stored credential data directly, in order to obtain credentials that may be replayed to impersonate another user.
- A malicious user could bypass the TOE's identification, authentication, or authorization mechanisms in order to illicitly use the TOE's management functions.
- A malicious user could be illicitly authenticated by the TSF through brute-force guessing of authentication credentials.

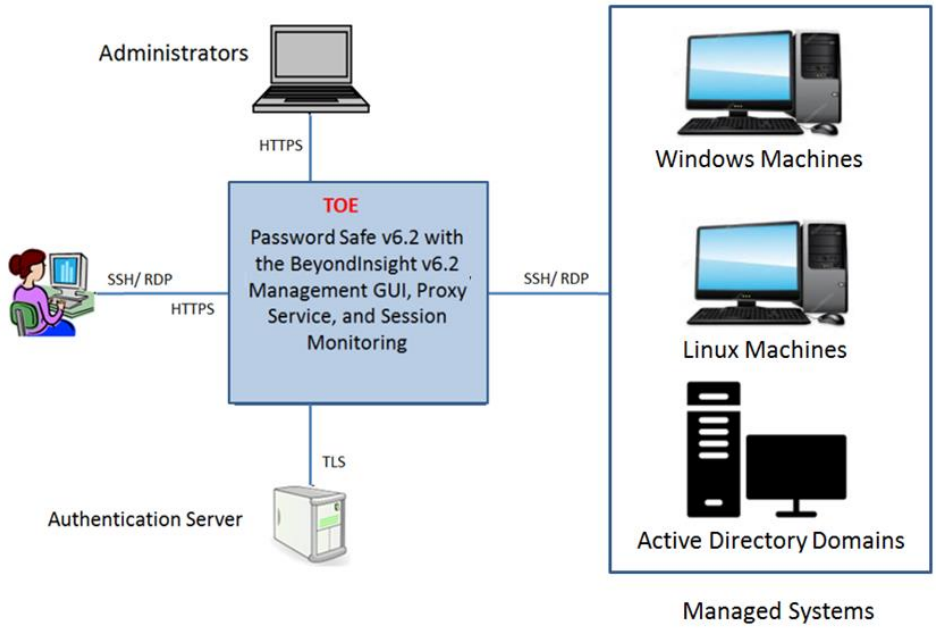
2.2 Organizational Security Policies

The TOE shall display an initial banner describing restrictions of use, legal agreements, or any other appropriate information to which users consent by accessing the system.

3 Architectural Information

The section describes the TOE architecture including physical and logical boundaries. Figure 1 shows the TOE in relation to its operational environment.

Figure 1 TOE Boundary



The TOE consists of the BeyondTrust Password Safe 6.2 (a BeyondInsight component) and includes the following components:

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

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

4 Assumptions

The ST references the *Standard Protection Profile for Enterprise Security Management Identity and Credential Management*, Version 2.1, 24 October 2013, to identify following assumptions about the use of the product:

- The TOE will use cryptographic primitives provided by the Operational Environment to perform cryptographic services.
- There will be a defined enrollment process that confirms user identity before the assignment of credentials.
- The TOE will be able to establish connectivity to other ESM products in order to share security data.
- Third-party entities that exchange attribute data with the TOE are assumed to be trusted.
- There will be one or more competent individuals assigned to install, configure, and operate the TOE.
- The Operational Environment will provide mechanisms to the TOE that reduce the ability for an attacker to impersonate a legitimate user during authentication.
- The TOE will receive reliable time data from the Operational Environment.

4.1 Clarification of Scope

All evaluations (and all products) have limitations, as well as potential misconceptions that need clarifying. This text covers some of the more important limitations and clarifications of this evaluation. Note that:

1. As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the assurance activities specified in the claimed PPs and performed by the evaluation team).
2. This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
3. The evaluation of security functionality of the product was limited to the functionality specified in the claimed PPs and scoped to those Security Functional Requirements (SFRs) declared in the ST. Any additional security related functional capabilities of the product were not covered by this evaluation.
4. The TOE relies on the FIPS 140-2 validated Microsoft Cryptographic Primitives Library (bcryptprimitives.dll and ncryptsslp.dll) in Windows Server 2012 R2, (CMVP Certificate #2357) and the FIPS approved algorithms (CAVP certificate numbers AES: #5327; RSA: #2855; DSA: #1377; SHA: #4279; DRBG: #2057; HMAC: #3525; CVL: #1794; CVL: #1795 (KDF135)) in the OpenSSL FIPS Object Module v2.0.10 in the operational environment for cryptographic functions. The TOE itself does not implement any cryptographic functions and, as such, the FCS requirements in the Architectural Variations section of the ESM ICM PP were not included in the ST, and were, therefore, not evaluated.
5. This evaluation did not specifically search for, nor attempt to exploit, vulnerabilities that were not “obvious” or vulnerabilities to objectives not claimed in the ST. The CEM defines an “obvious” vulnerability as one that is easily exploited with a minimum of understanding of the TOE, technical sophistication and resources.

5 Security Policy

The TOE enforces the following security policies as described in the ST.

5.1 Enterprise Security Management

The TOE enrolls enterprise users and assigns uniquely 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 enterprise users

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

5.2 Security Audit

The TOE generates logs for security relevant events including the events specified in Standard Protection Profile for Enterprise Security Management Identity and Credential Management. The audit records identify the date/time, event type, outcome of the event, and the responsible subject/user. The TOE stores the audit records locally in the 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. Reliable timestamps are provided by the operational environment.

5.3 Identification and Authentication

The BeyondInsight administrator accesses the TOE using the BeyondInsight local password authentication. TOE users assigned a Password Safe role access the TOE using Microsoft Active Directory external authentication. The TOE provides authentication failure handling and associates identity, roles, and groups with users.

5.4 Security Management

The TOE provides the management functions identified in the Standard Protection Profile for Enterprise Security Management Identity and Credential Management. The TOE restricts all management functions to users that belong to the BeyondInsight administrator role.

5.5 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 to any users a stored cryptographic key; and all keys are stored encrypted using AES-256.

5.6 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.

5.7 Trusted Path/Channels

The TOE protects interactive communication with users and 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.

The TOE itself does not implement any cryptographic functions. Consequently, the Cryptographic Support (class FCS) requirements from the Architectural Variations section of the ESM ICM PP do not apply to the TOE. The security target does not claim any requirements from the FCS class and so the FCS requirements were outside the scope of evaluation and were not evaluated.

6 Documentation

There are numerous documents that provide information and guidance for the deployment of the TOE. In particular, the following Common Criteria specific information is available:

- *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.

7 Independent Testing

This section describes the testing efforts of the evaluation team. It is derived from information contained in the following:

- *BeyondTrust PowerBroker Password Safe 6.2 Common Criteria Test Report and Procedures*, version 1.0, 13 June 2018

The purpose of this activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product claiming conformance to the *Standard Protection Profile for Enterprise Security Management Identity and Credential Management*, Version 2.1, 24 October 2013.

To this end, the evaluation team devised a Test Plan based on the Testing Assurance Activities specified in the above-referenced Protection Profile.

The Test Plan described how each test activity was to be instantiated within the TOE test environment. The evaluation team executed the tests specified in the Test Plan and documented the results in the team test report listed above.

Independent testing took place at the Leidos facility in Columbia, Maryland from February 15, 2017 to March 15, 2018 and April 2nd through April 12th.

The evaluators received the TOE in the form that normal customers would receive it, installed and configured the TOE in accordance with the provided guidance, and exercised the Team Test Plan on equipment configured in the testing laboratory. As can be seen below, the configuration used during testing of the TOE matches that which was defined in the Security Target.

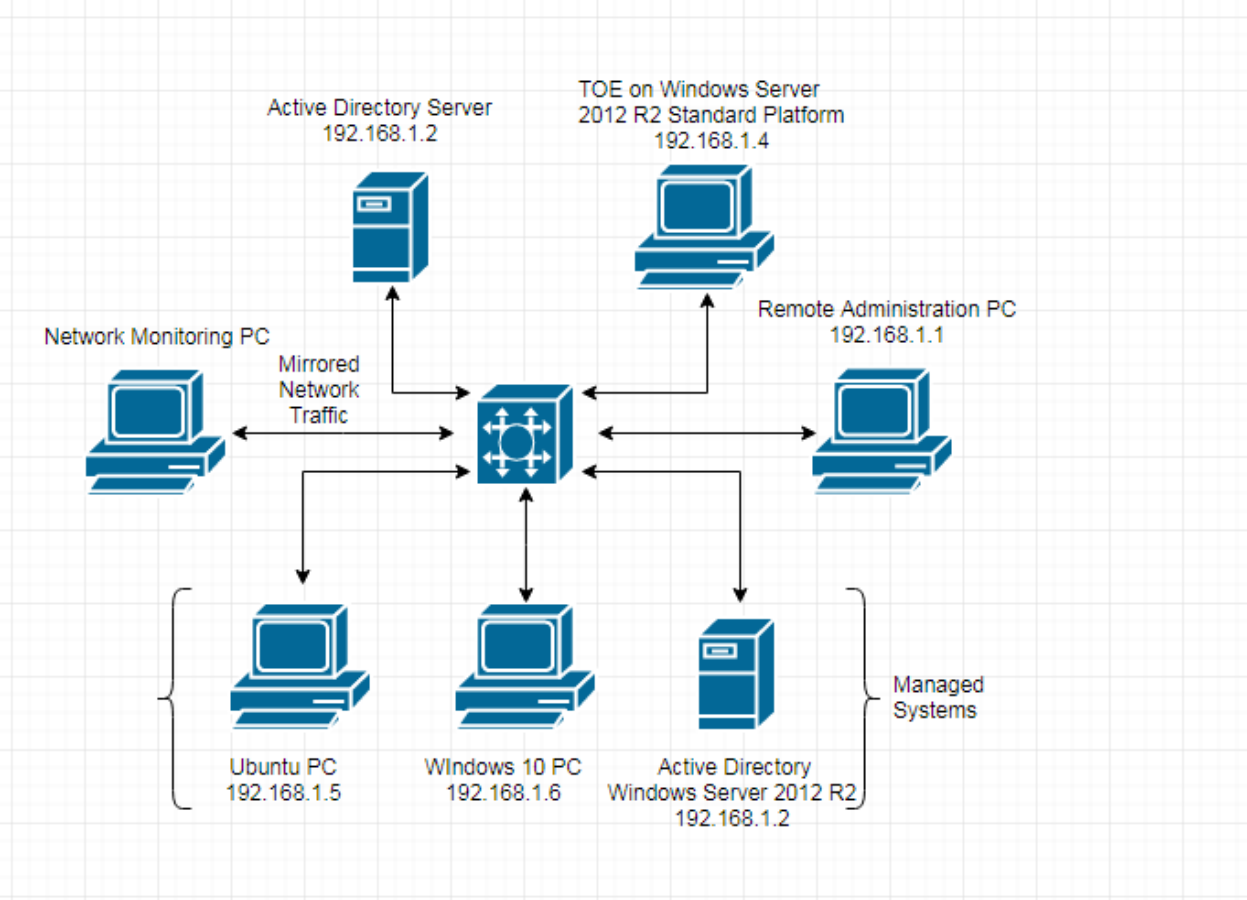


Figure 2 Test Configuration

The following hardware and software components were included in the evaluated configuration during testing:

- The TOE application installed on a Microsoft Windows Server 2012 R2 Standard platform with the following additional components:
  - 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
- Additional Non-TOE Components
  - Active Directory Server (for user authentication and used as a managed domain)
  - Additional computer for Network Monitoring.
    - Connected to test network via monitor port on mirrored switch.
    - Running Wireshark to capture all traffic on the test network.
  - Additional computer for Remote Administration through the Web GUI.

        - The following browser versions were used during the course of testing:
        - Firefox 59
        - Chrome 65
        - Microsoft Internet Explorer 11 was used for administration
    - Adobe Flash Player version 22.0 or higher
    - Any SSH client (i.e. PuTTY)
    - Any RDP client (i.e. Microsoft Terminal Server Client)
    - Additional computers running Ubuntu, Windows 10 and Windows 12 Server 2012 R2 Active Directory for product functionality testing.
        - Power Broker for Windows Client was installed on the Windows platforms.
    - All devices in the Tested Configuration were connected via a switch with supports port mirroring

The configuration used during testing of the TOE matches that which was defined in the Security Target. The evaluated version of the TOE was installed and configured according to the *PowerBroker Password Safe v6.2.0 Common Criteria – Supplementary Guide*, as well as the supporting guidance documentation identified in Section 6.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for the *Standard Protection Profile for Enterprise Security Management Identity and Credential Management,* Version 2.1, 24 October 2013 are fulfilled.

7.1 Penetration Testing

The evaluation team conducted an open-source search for vulnerabilities in the product. The open-source search did not identify any vulnerability applicable to the TOE in its evaluated configuration. No additional testing was required to verify the vulnerabilities were mitigated.

8 Evaluated Configuration

The evaluated version of the TOE is BeyondTrust Password Safe 6.2 (a BeyondInsight component). The TOE must be deployed as described in section 4 Assumptions of this document and must be configured in accordance with *PowerBroker Password Safe v6.2.0 Common Criteria – Supplementary Guide* identified in section 6.

Per NIAP Policy Letter #22 (https://www.niap-ccevs.org/Documents_and_Guidance/policy.cfm), user installation of vendor-delivered bug fixes and security patches is encouraged between completion of the evaluation and the Assurance Maintenance Date. The product is still considered by NIAP to be in its evaluated configuration with such updates properly installed.

9 Results of the Evaluation

The evaluation was conducted based upon the assurance activities specified in the *Standard Protection Profile for Enterprise Security Management Identity and Credential Management*, Version 2.1, 24 October 2013.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements.

The validation team's assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team performed the assurance activities in the claimed PPs, and correctly verified that the product meets the claims in the ST.

The details of the evaluation are recorded in the Evaluation Technical Report (ETR), which is controlled by the Leidos CCTL. The security assurance requirements are listed in the following table.

Table 3 TOE Security Assurance Requirements

Assurance Component ID	Assurance Component Name
ASE_CCL.1	Conformance Claims
ASE_ECD.1	Extended Components Definition
ASE_INT.1	ST Introduction
ASE_OBJ.1	Security Objectives
ASE_REQ.1	Security Requirements
ASE_TSS.1	TOE Summary Specification
ADV_FSP.1	Basic Functional Specification
AGD_OPE.1	Operational User Guidance
AGD_PRE.1	Preparative Procedures
ALC_CMC.1	Labeling of the TOE
ALC_CMS.1	TOE CM Coverage
ATE_IND.1	Independent Testing - Conformance
AVA_VAN.1	Vulnerability Survey

10 Validator Comments/Recommendations

The functionality evaluated is scoped exclusively to the security functional requirements specified in the Security Target, and only the functionality implemented by the SFR's within the Security Target was evaluated. All other functionality provided by the Password Safe that are outside the scope of ESM ICM v2.1 PP, are not covered by this evaluation, need to be assessed separately, and no further conclusions can be drawn about their effectiveness.

The Validators note that this product does not manage the "Enterprise Users" defined in Active Directory. Rather, the Enterprise Users managed by this product are the accounts used through Password Safe by those Active Directory users.

11 Annexes

Not applicable

12 Security Target

Name	Description
ST Title	BeyondTrust Password Safe 6.2 (a BeyondInsight component) Security Target
ST Version	Version 1.0
Publication Date	June 13, 2018

13 Abbreviations and Acronyms

Abbreviation	Description
AAR	Assurance Activity Report
AFX	Access Fulfillment Express
API	Application Programming Interface
CC	Common Criteria
CEM	Common Evaluation Methodology
CCEVS	Common Criteria Evaluation and Validation Scheme
CCTL	Common Criteria Testing Laboratory
ESM	Enterprise Security Management
ICM	Identity and Credential Management
NIAP	National Information Assurance Partnership
NIST	National Institute of Standards and Technology
NSA	National Security Agency
NVLAP	National Voluntary Laboratory Assessment Program
OS	Operating System
PCL	Product Compliant List
PP	Protection Profile
SAR	Security assurance requirement
SFR	Security functional requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSS	TOE Summary Specification
VR	Validation Report

14 Bibliography

The Validation Team used the following documents to produce this Validation Report:

[1] Common Criteria for Information Technology Security Evaluation Part 1: Introduction, Version 3.1, Revision 4, September 2012.

[2] Common Criteria for Information Technology Security Evaluation Part 2: Security Functional Requirements, Version 3.1 Revision 4, September 2012.

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

[4] Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 4, September 2012.

[5] *BeyondTrust Password Safe 6.2 (a BeyondInsight component) Security Target*, Version 1.0, June 13, 2018

[6] *BeyondTrust PowerBroker Password Safe 6.2 Common Criteria Test Report and Procedures*, Version 1.0, June 13, 2018

[7] *BeyondTrust PowerBroker Password Safe Common Criteria Assurance Activities Report*, Version 1.0, June 13, 2018

[8] *PowerBroker Password Safe v6.2.0 Common Criteria – Supplementary Guide*, March 22, 2018

[9] *Evaluation Technical Report For PowerBroker Password Safe v6.2*, Version 1.0 June 13, 2018