Assurance Activities Report
for
Veeam ONE v12

Version 1.0
14 August 2023

Evaluated By:

Leidos Inc.
https://www.leidos.com/civil/commercial-cyber/product-compliance
Common Criteria Testing Laboratory
6841 Benjamin Franklin Drive
Columbia, MD 21046

Prepared for:
National Information Assurance Partnership
Common Criteria Evaluation and Validation Scheme

The Developer of the TOE:
Veeam Software
8800 Lyra Drive, Suite 350
Columbus, OH 43240

The TOE Evaluation was Sponsored by:
Veeam Software
8800 Lyra Drive, Suite 350
Columbus, OH 43240

Evaluation Personnel:
Anthony J. Apted
Kofi Owusu
Pascal Patin

Common Criteria Version:

- Common Criteria for Information Technology Security Evaluation Part 1: Introduction and general model, Version 3.1, Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation Part 2: Security functional components, Version 3.1, Revision 5, April 2017.
- Common Criteria for Information Technology Security Evaluation Part 3: Security assurance components, Version 3.1, Revision 5, April 2017.

Common Evaluation Methodology Version:

- Common Methodology for Information Technology Security Evaluation, Evaluation Methodology, Version 3.1, Revision 5, April 2017.

Protection Profiles:

- Protection Profile for Application Software, Version 1.4, 7 October 2021.

Revision History

Version	Date	Description
0.1	12 May 2023	Initial draft
1.0	14 August 2023	Final version for check-out.

Contents

1. INTRODUCTION 1

1.1 TECHNICAL DECISIONS 1
1.2 REFERENCES 2
1.3 SAR EVALUATION 2

2. SECURITY FUNCTIONAL REQUIREMENT EVALUATION ACTIVITIES 3

2.1 CRYPTOGRAPHIC SUPPORT (FCS) 3
2.1.1 Certificate Table 3
2.1.2 Cryptographic Key Generation Services (FCS_CKM_EXT.1) 4
2.1.3 Random Bit Generation Services (FCS_RBG_EXT.1) 4
2.1.4 Storage of Credentials (FCS_STO_EXT.1) 5
2.2 USER DATA PROTECTION (FDP) 6
2.2.1 Encryption of Sensitive Application Data (FDP_DAR_EXT.1) 6
2.2.2 Access to Platform Resources (FDP_DEC_EXT.1) 7
2.2.3 Network Communications (FDP_NET_EXT.1) 9
2.3 SECURITY MANAGEMENT (FMT) 9
2.3.1 Secure by Default Configuration (FMT_CFG_EXT.1) 9
2.3.2 Supported Configuration Mechanism (FMT_MEC_EXT.1) 11
2.3.3 Specification of Management Functions (FMT_SMF.1) 12
2.4 PRIVACY (FPR) 12
2.4.1 User Consent for Transmission of Personally Identifiable Information (FPR_ANO_EXT.1) 12
2.5 PROTECTION OF THE TSF (FPT) 13
2.5.1 Anti-Exploitation Capabilities (FPT_AEX_EXT.1) 13
2.5.2 Use of Supported Services and APIs (FPT_API_EXT.1) 15
2.5.3 Use of Third Party Libraries (FPT_LIB_EXT.1) 16
2.5.4 Software Identification and Versions (FPT_IDV_EXT.1) 16
2.5.5 Integrity for Installation and Update (FPT_TUD_EXT.1) 17
2.5.6 Integrity for Installation and Update (FPT_TUD_EXT.2) 19
2.6 TRUSTED PATH/CHANNELS (FTP) 21
2.6.1 Protection of Data in Transit (FTP_DIT_EXT.1) 21

3. SECURITY ASSURANCE REQUIREMENT EVALUATION ACTIVITIES 22

3.1 CLASS ASE: SECURITY TARGET 22
3.2 CLASS ADV: DEVELOPMENT 22
3.2.1 Basic Functional Specification (ADV_FSP.1) 22
3.3 CLASS AGD: GUIDANCE DOCUMENTS 22
3.3.1 Operational User Guidance (AGD_OPE.1) 22
3.3.2 Preparative Procedures (AGD_PRE.1) 23
3.4 CLASS ALC: LIFE-CYCLE SUPPORT 23
3.4.1 Labeling of the TOE (ALC_CMC.1) 24
3.4.2 TOE Coverage (ALC_CMS.1) 24
3.4.3 Timely Security Update (ALC_TSU_EXT.1) 25
3.5 CLASS ATE: TESTS 25
3.5.1 Independent Testing – Conformance (ATE_IND.1) 25
3.6 CLASS AVA: VULNERABILITY ASSESSMENT 27
3.6.1 Vulnerability Survey (AVA_VAN.1) 27

LIST OF TABLES

NO TABLE OF FIGURES ENTRIES FOUND.

1. Introduction

This document presents the results of performing evaluation activities associated with the Veeam ONE v12 evaluation. This report contains sections documenting the performance of evaluation activities associated with each of the Security Functional Requirements (SFRs) and Security Assurance Requirements (SARs) as specified in the following document:

- *Protection Profile for Application Software*, Version 1.4, 7 October 2021 [PP_APP_v1.4].

Note that, in accordance with NIAP Policy Letter #5, all cryptography in the TOE for which NIST provides validation testing of FIPS-approved and NIST-recommended cryptographic algorithms and their individual components must be NIST validated. The CCTL will verify that the claimed NIST validation complies with the NIAP-approved PP requirements the TOE claims to satisfy. The CCTL verification of the NIST validation will constitute performance of the associated assurance activity. As such, Test assurance activities associated with functional requirements within the scope of Policy Letter #5 are performed by verification of the relevant CAVP certification and not through performance of any testing as specified in the claimed PP documents.

1.1 Technical Decisions

This subsection lists the Technical Decisions that have been issued by NIAP against [PP_APP_v1.4], along with rationale as to their applicability or otherwise to this evaluation.

TD0624 – Addition of DataStore for Storing and Setting Configuration Options

This TD has been applied to this evaluation.

TD0628 – Addition of Container Image to Package Format

This TD has been applied to this evaluation.

TD0650 – Conformance claim sections updated to allow for MOD_VPNC_V2.3 and 2.4

N/A – the ST does not claim conformance to MOD_VPNC_V2.4.

TD0664 – Testing activity for FPT_TUD_EXT.2.2

This TD has been applied to this evaluation.

TD0669 – FIA_X509_EXT.1 Test 4 Interpretation

N/A – the ST does not include FIA_X509_EXT.1.

TD0717 – Format changes for PP_APP_V1.4

This TD has been applied to this evaluation.

TD0719 – ECD for PP APP V1.3 and 1.4

This TD has been applied to this evaluation.

TD0736 – Number of elements for iterations of FCS_HTTPS_EXT.1

N/A – the ST does not include FCS_HTTPS_EXT.1.

TD0743 – FTP_DIT_EXT.1.1 Selection exclusivity

This TD has been applied to this evaluation.

TD0756 – Update for platform-provided full disk encryption

This TD has been applied to this evaluation.

1.2 References

[ST]	Veeam ONE v12 Security Target, Version 1.6, 9 July 2023
[CCECG]	Veeam ONE v12 Common Criteria Evaluated Configuration Guide (CCECG), Version 1.0, 9 July 2023
[MG]	Veeam ONE Version 12 Monitoring Guide, July 2023
[Report]	Veeam ONE Version 12 Reporting Guide, July 2023
[QSG]	Veeam ONE Version 12 Quick Start Guide, May 2023
[DG]	Veeam ONE Version 12 Deployment Guide, July 2023
[Harden]	CC Hardening Guide for 12a.

1.3 SAR Evaluation

The following Security Assurance Requirements (SARs) were evaluated during the evaluation of the TOE:

SAR	Verdict
ASE_CCL.1	Pass
ASE_ECD.1	Pass
ASE_INT.1	Pass
ASE_OBJ.1	Pass
ASE_REQ.1	Pass
ASE_TSS.1	Pass
ADV_FSP.1	Pass
AGD_OPE.1	Pass
AGD_PRE.1	Pass
ALC_CMC.1	Pass
ALC_CMS.1	Pass
ALC_TSU_EXT.1	Pass
ATE_IND.1	Pass
AVA_VAN.1	Pass

The evaluation work units are listed in the proprietary ETR. The evaluators note per the PP evaluation activities that many of the SARs were successfully evaluated through completion of the associated evaluation activities presented in the claimed PP.

2. Security Functional Requirement Evaluation Activities

This section describes the evaluation activities associated with the SFRs defined in the ST and the results of those activities as performed by the evaluation team. The evaluation activities are derived from [PP_APP_v1.4]. NIAP Technical Decisions have been applied and are identified as appropriate.

2.1 Cryptographic Support (FCS)

2.1.1 Certificate Table

The TOE does not implement any cryptographic functionality. It relies on platform-provided cryptographic functionality in order to meet FTP_DIT_EXT.1. The evaluated configuration, as documented in [CCECG] and [Harden], restricts the Windows platform to the following ciphersuites, which in turn rely on the listed cryptographic algorithms:

- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
  - FFC Key Establishment (DSA KeyGen, KAS-FFC Sp800-56Ar3)
  - RSA Signature Generation and Verification (RSA SigGen, RSA SigVer)
  - 256-bit AES in GCM Mode (AES-GCM)
  - HMAC-SHA-384 (SHA2-384, HMAC-SHA2-384)
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  - ECC Key Establishment (ECDSA KeyGen, KAS-ECC Sp800-56Ar3)
  - RSA Signature Generation and Verification (RSA SigGen, RSA SigVer)
  - 256-bit AES in GCM Mode (AES-GCM)
  - HMAC-SHA-384 (SHA2-384, HMAC-SHA2-384)
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384.
  - ECC Key Establishment (ECDSA KeyGen, KAS-ECC Sp800-56Ar3)
  - ECDSA Signature Generation and Verification (ECDSA SigGen, ECDSA SigVer)
  - 256-bit AES in GCM Mode (AES-GCM)
  - HMAC-SHA-384 (SHA2-384, HMAC-SHA2-384)

In accordance with NIAP Policy Letter 5 and Policy 5 Addendum 3 Item 5 (Certificate Report Template), the table below provides the following information for the SFR claimed for the TOE that relies on platform-provided cryptography:

- the platform-provided cryptographic functionality the TOE relies on to satisfy FTP_DIT_EXT.1
- the applicable CAVP algorithm list names for the platform-provided cryptographic algorithms that implement the platform-provided cryptographic functionality
- the applicable NIST standards defining the algorithm implementation
- the applicable CAVP certificate number.

Platform-provided Function	CAVP Algorithms	NIST Standard	CAVP Certs
Asymmetric key generation	ECDSA KeyGen (FIPS186-4)	FIPS186-4	#A2014
	DSA KeyGen (FIPS186-4)	FIPS186-4	#A2014
Key Establishment	KAS-ECC Sp800-56Ar3	Sp800-56Ar3	#A2014
	KAS-FFC Sp800-56Ar3	Sp800-56Ar3	#A2014

Platform-provided Function	CAVP Algorithms	NIST Standard	CAVP Certs
Digital signature generation	ECDSA SigGen (FIPS186-4)	FIPS186-4	#A2014
	RSA SigGen (FIPS186-4)	FIPS186-4	#A2014
Digital signature verification	ECDSA SigVer (FIPS186-4)	FIPS186-4	#A2014
	RSA SigVer (FIPS186-4)	FIPS186-4	#A2014
Symmetric encryption	AES-GCM	NIST SP 800-38	#A2014
Keyed-hash message authentication	HMAC-SHA2-384	FIPS PUB 180-4 FIPS PUB 198-1	#A2014
Cryptographic hash	SHA2-384	FIPS PUB 180-4	#A2014

2.1.2 Cryptographic Key Generation Services (FCS_CKM_EXT.1)

2.1.2.1 TSS Activities

> The evaluator shall inspect the application and its developer documentation to determine if the application needs asymmetric key generation services. If not, the evaluator shall verify the ***generate no asymmetric cryptographic keys*** selection is present in the ST. Otherwise, the evaluation activities shall be performed as stated in the selection-based requirements.

The evaluator inspected the application and its documentation, specifically [CCECG], and determined the TOE does not need asymmetric key generation services. The TOE invokes the third-party Windows Schannel library to call platform-provided functionality to provide asymmetric key generation. As such, the evaluator verified the ST selects “generate no asymmetric cryptographic keys” in FCS_CKM_EXT.1.

2.1.2.2 Guidance Activities

> None.

2.1.2.3 Test Activities

> None.

2.1.3 Random Bit Generation Services (FCS_RBG_EXT.1)

2.1.3.1 TSS Activities

> If *“use no DRBG functionality”* is selected, the evaluator shall inspect the application and its developer documentation and verify that the application needs no random bit generation services.
>
> If *“implement DRBG functionality”* is selected, the evaluator shall ensure that additional FCS_RBG_EXT.2 elements are included in the ST.
>
> If *“invoke platform-provided DRBG functionality”* is selected, the evaluator performs the following activities. The evaluator shall examine the TSS to confirm that it identifies all functions (as described by the SFRs included in the ST) that obtain random numbers from the platform RBG. The evaluator shall determine that for each of these functions, the TSS states which platform interface (API) is used to obtain the random numbers. The evaluator shall confirm that each of these interfaces corresponds to the acceptable interfaces listed for each platform below.

It should be noted that there is no expectation that the evaluators attempt to confirm that the APIs are being used correctly for the functions identified in the TSS; the activity is to list the used APIs and then do an existence check via decompilation.

In FCS_RBG_EXT.1, the ST author has selected ***use no DRBG functionality***. The evaluator examined the TOE and its documentation and determined it does not require random bit generation services.

2.1.3.2 Guidance Activities

None defined.

2.1.3.3 Test Activities

If "*invoke platform-provided DRBG functionality"* is selected, the following tests shall be performed:

The evaluator shall decompile the application binary using a decompiler suitable for the application (TOE). The evaluator shall search the output of the decompiler to determine that, for each API listed in the TSS, that API appears in the output. If the representation of the API does not correspond directly to the strings in the following list, the evaluator shall provide a mapping from the decompiled text to its corresponding API, with a description of why the API text does not directly correspond to the decompiled text and justification that the decompiled text corresponds to the associated API.

The following are the per-platform list of acceptable APIs:

Platforms: Microsoft Windows…

The evaluator shall verify that rand_s, RtlGenRandom, BCryptGenRandom, or CryptGenRandom API is used for classic desktop applications. The evaluator shall verify the application uses the RNGCryptoServiceProvider class or derives a class from System.Security.Cryptography.RandomNumberGenerator API for Windows Universal Applications. It is only required that the API is called/invoked, there is no requirement that the API be used directly. In future versions of this document, CryptGenRandom may be removed as an option as it is no longer the preferred API per vendor documentation.

In FCS_RBG_EXT.1, the ST author has selected ***use no DRBG functionality***. As such, there are no Test activities to perform.

2.1.4 Storage of Credentials (FCS_STO_EXT.1)

2.1.4.1 TSS Activities

The evaluator shall check the TSS to ensure that it lists all persistent credentials (secret keys, PKI private keys, or passwords) needed to meet the requirements in the ST. For each of these items, the evaluator shall confirm that the TSS lists for what purpose it is used, and how it is stored.

Section 6.2.3 of [ST] (“Storage of Credentials (FCS_STO_EXT.1)”) states the TOE uses the following credentials:

- TLS certificate used with the platform-provided Web server (HTTPS)—stored in the Windows Certificate Store.
- VBR server credentials.

Section 6.3.1 of [ST] (“Encryption of Sensitive Application Data (FDP_DAR_EXT.1)”) states the TOE uses the platform-provided Data Protection API (DPAPI) to encrypt VBR server credentials it then stores in MS SQL database.

2.1.4.2 Guidance Activities

None defined.

2.1.4.3 Test Activities

For all credentials for which the application implements functionality, the evaluator shall verify credentials are encrypted according to FCS_COP.1/SKC or conditioned according to FCS_CKM.1.1/AK and FCS_CKM.1/PBKDF. For all credentials for which the application invokes platform-provided functionality, the evaluator shall perform the following actions which vary per platform.

Platforms: Microsoft Windows…

The evaluator shall verify that all certificates are stored in the Windows Certificate Store. The evaluator shall verify that other credentials, like passwords, are stored in the Windows Credential Manager or stored using the Data Protection API (DPAPI). For Windows Universal Applications, the evaluator shall verify that the application is using the ProtectData class and storing credentials in IsolatedStorage.

The evaluator verified that the TOE used credential manager to protect the sensitive data. This was accomplished by using the credential manager setting to view the application stored credentials.

The evaluator also verified that the TOE used DPAPI to protect the sensitive data. This was accomplished by using the PsExec64 sysinternals tool to view the credentials stored and protected by DPAPI. Additionally, the evaluator verified that the TOE’s TLS certificate is stored in the Windows Certificate Store.

2.2 User Data Protection (FDP)

2.2.1 Encryption of Sensitive Application Data (FDP_DAR_EXT.1)

2.2.1.1 TSS Activities

The evaluator shall examine the TSS to ensure that it describes the sensitive data processed by the application. The evaluator shall then ensure that the following activities cover all of the sensitive data identified in the TSS.

Section 6.3.1 of [ST] (“Encryption of Sensitive Application Data (FDP_DAR_EXT.1)”) states the only sensitive data the TOE processes are VBR credentials. The TOE protects VBR credentials in accordance with FCS_STO_EXT.1.

If ***not store any sensitive data*** is selected, the evaluator shall inspect the TSS to ensure that it describes how sensitive data cannot be written to non-volatile memory. The evaluator shall also ensure that this is consistent with the filesystem test below.

The ST does not select “not store any sensitive data”, so this activity is not applicable.

2.2.1.2 Guidance Activities

None defined.

2.2.1.3 Test Activities

Modified in accordance with TD0756.

Evaluation activities (after the identification of the sensitive data) are to be performed on all sensitive data listed that are not covered by FCS_STO_EXT.1.

If "implement functionality to encrypt sensitive data as defined in the PP-Module for File Encryption" or "protect sensitive data in accordance with FCS_STO_EXT.1" is selected, the evaluator shall inventory the filesystem locations where the application may write data. The evaluator shall run the application and attempt to store sensitive data. The evaluator shall then inspect those areas of the filesystem to note where data was stored (if any), and determine whether it has been encrypted.

Veeam ONE stores no sensitive data not already covered by FCS_STO.

If “leverage platform-provided functionality” is selected, the evaluation activities will be performed as stated in the following requirements, which vary on a per-platform basis:

Platforms: Microsoft Windows…

The Windows platform currently does not provide data-at-rest encryption services which depend upon invocation by application developers. The evaluator shall verify that the Operational User Guidance makes the need to activate platform encryption, such as BitLocker or Encrypting File System (EFS), clear to the end user.

The ST does not select “leverage platform-provided functionality”. Therefore, this activity is not applicable.

2.2.2 Access to Platform Resources (FDP_DEC_EXT.1)

2.2.2.1 FDP_DEC_EXT.1.1

2.2.2.1.1 TSS Activities

None defined.

2.2.2.1.2 Guidance Activities

The evaluator shall perform the platform-specific actions below and inspect user documentation to determine the application's access to hardware resources. The evaluator shall ensure that this is consistent with the selections indicated. The evaluator shall review documentation provided by the application developer and for each resource which it accesses, identify the justification as to why access is required.

The statement of FDP_DEC_EXT.1.1 in Section 5.2.2.2 of [ST] (“FDP_DEC_EXT.1 Access to Platform Resources”) selects “network connectivity” as the only platform hardware resource the TOE requires to access.

Section “TOE Overview”, subsection “Logical Boundaries” of [CCECG] states the TOE accesses the minimum amount of platform hardware resources in order to perform its function. Section “TOE Overview”, subsection “Physical Boundaries” of [CCECG] includes a diagram of the TOE deployment, showing the only network connection to be from the Windows Server host to an administrator workstation that provides access via a web browser to the TOE’s user interface. This is consistent with the selection of “network connectivity” made in FDP_DEC_EXT.1.1.

2.2.2.1.3 Test Activities

Platforms: Microsoft Windows…

For Windows Universal Applications the evaluator shall check the WMAppManifest.xml file for a list of required hardware capabilities. The evaluator shall verify that the user is made aware of the required hardware capabilities when the application is first installed. This includes permissions such as ID_CAP_ISV_CAMERA, ID_CAP_LOCATION, ID_CAP_NETWORKING, ID_CAP_MICROPHONE, ID_CAP_PROXIMITY and so on. A complete list of Windows App permissions can be found at:

- http://msdn.microsoft.com/en-US/library/windows/apps/jj206936.aspx

For Windows Desktop Applications the evaluator shall identify in either the application software or its documentation the list of the required hardware resources.

The evaluator confirmed the information on page 22 of the [CCECG] makes clear the TOE’s need to access platform-provided network connectivity.

2.2.2.2 FDP_DEC_EXT.1.2

2.2.2.2.1 TSS Activities

None defined.

2.2.2.2.2 Guidance Activities

The evaluator shall perform the platform-specific actions below and inspect user documentation to determine the application's access to sensitive information repositories. The evaluator shall ensure that this is consistent with the selections indicated. The evaluator shall review documentation provided by the application developer and for each sensitive information repository which it accesses, identify the justification as to why access is required.

The statement of FDP_DEC_EXT.1.2 in Section 5.2.2.2 of [ST] (“FDP_DEC_EXT.1 Access to Platform Resources”) specifies “VBR event logs and infrastructure information”.

Section “Software Download, Installation and Configuration”, subsection “Management” of [CCECG] states the TOE provides authorized administrators with the ability to configure retrieval and analysis of VBR event logs and infrastructure information from VBR systems. This description is consistent with the specification of FDP_DEC_EXT.1.2.

2.2.2.2.3 Test Activities

Platforms: Microsoft Windows…

For Windows Universal Applications the evaluator shall check the WMAppManifest.xml file for a list of required capabilities. The evaluator shall identify the required information repositories when the application is first installed. This includes permissions such as ID_CAP_CONTACTS, ID_CAP_APPOINTMENTS, ID_CAP_MEDIALIB and so on. A complete list of Windows App permissions can be found at:

- http://msdn.microsoft.com/en-US/library/windows/apps/jj206936.aspx

For Windows Desktop Applications the evaluator shall identify in either the application software or its documentation the list of sensitive information repositories it accesses.

The evaluator confirmed the information on page 22 of the [CCECG] makes clear the TOE's need to access VBR event logs and infrastructure information from VBR systems.

2.2.3 Network Communications (FDP_NET_EXT.1)

2.2.3.1 TSS Activities

None defined.

2.2.3.2 Guidance Activities

None defined.

2.2.3.3 Test Activities

The evaluator shall perform the following tests:

Test 1: The evaluator shall run the application. While the application is running, the evaluator shall sniff network traffic ignoring all non-application associated traffic and verify that any network communications witnessed are documented in the TSS or are user-initiated.

The evaluator observed the network traffic between the TOE and the agent devices and observed that no traffic was sent outside of the TCP channel. It was observed that the TOE was receiving Web Server (HTTPS) connections on port 1239 for administration.

Test 2: The evaluator shall run the application. After the application initializes, the evaluator shall run network port scans to verify that any ports opened by the application have been captured in the ST for the third selection and its assignment. This includes connection-based protocols (e.g. TCP, DCCP) as well as connectionless protocols (e.g. UDP).

The evaluator used NMAP to scam the TOE for open ports. All ports were either documented in the [ST] or were opened by the underlying platform OS rather than the TOE.

2.3 Security Management (FMT)

2.3.1 Secure by Default Configuration (FMT_CFG_EXT.1)

2.3.1.1 FMT_CFG_EXT.1.1

2.3.1.1.1 TSS Activities

The evaluator shall check the TSS to determine if the application requires any type of credentials and if the application installs with default credentials.

Section 6.4.1 of [ST] ("Secure by Default Configuration (FMT_CFG_EXT.1)") states there are no administrator credentials for the TOE. Users access the Veeam ONE Client component of the TOE by first logging in to the Windows server hosting the TOE. Users access the Veeam ONE Web Client component using a web browser on a remote workstation. In order to access the Veeam ONE Web Client console remotely, the user must be a member of the Veeam ONE Administrators, Veeam ONE Read-Only Users or Veeam ONE Power Users group on the server where the TOE is installed.

2.3.1.1.2 Guidance Activities

None.

2.3.1.1.3 Test Activities

If the application uses any default credentials the evaluator shall run the following tests.

Test 1: The evaluator shall install and run the application without generating or loading new credentials and verify that only the minimal application functionality required to set new credentials is available.

Test 2: The evaluator shall attempt to clear all credentials and verify that only the minimal application functionality required to set new credentials is available.

Test 3: The evaluator shall run the application, establish new credentials and verify that the original default credentials no longer provide access to the application.

The TOE does not use any default credentials. As such, these tests are not applicable.

2.3.1.2 FMT_CFG_EXT.1.2

2.3.1.2.1 TSS Activities

None.

2.3.1.2.2 Guidance Activities

None.

2.3.1.2.3 Test Activities

The evaluator shall install and run the application. The evaluator shall inspect the filesystem of the platform (to the extent possible) for any files created by the application and ensure that their permissions are adequate to protect them. The method of doing so varies per platform.

Platforms: Microsoft Windows…

The evaluator shall run the SysInternals tools, Process Monitor and Access Check (or tools of equivalent capability, like icacls.exe) for Classic Desktop applications to verify that files written to disk during an application's installation have the correct file permissions, such that a standard user cannot modify the application or its data files. For Windows Universal Applications the evaluator shall consider the requirement met because of the AppContainer sandbox.

The evaluator examined the TOE's data files and verified that standard user accounts only have read access to them.

2.3.2 Supported Configuration Mechanism (FMT_MEC_EXT.1)

2.3.2.1 TSS Activities

The evaluator shall review the TSS to identify the application's configuration options (e.g. settings) and determine whether these are stored and set using the mechanisms supported by the platform or implemented by the application in accordance with the PP-Module for File Encryption. At a minimum the TSS shall list settings related to any SFRs and any settings that are mandated in the operational guidance in response to an SFR.

Section 6.4.2 of [ST] ("Supported Configuration Mechanism (FMT_MEC_EXT.1)") states the TOE stores its configuration settings, comprising information about the MS SQL database (location, basic listening ports, license information, and logging options) in the Windows Registry.

The TOE saves VBR event logs and infrastructure information under the Windows Program Data folder.

Conditional: If "implement functionality to encrypt and store configuration options as defined by FDP_PRT_EXT.1 in the PP-Module for File Encryption" is selected, the evaluator shall ensure that the TSS identifies those options, as well as indicates where the encrypted representation of these options is stored.

The ST does not make this selection.

2.3.2.2 Guidance Activities

None.

2.3.2.3 Test Activities

If "invoke the mechanisms recommended by the platform vendor for storing and setting configuration options" is chosen, the method of testing varies per platform as follows:

Platforms: Microsoft Windows...

The evaluator shall determine and verify that Windows Universal Applications use either the Windows.Storage namespace, Windows.UI.ApplicationSettings namespace, or the IsolatedStorageSettings namespace for storing application specific settings. For .NET applications, the evaluator shall determine and verify that the application uses one of the locations listed in https://docs.microsoft.com/en-us/dotnet/framework/configure-apps/ for storing application specific settings. For Classic Desktop applications, the evaluator shall run the application while monitoring it with the SysInternals tool ProcMon and make changes to its configuration. The evaluator shall verify that ProcMon logs show corresponding changes to the the Windows Registry or C:\ProgramData\ directory.

The evaluator used ProcMon to verify that TOE configuration changes are written to the Windows Registry.

If "implement functionality to encrypt and store configuration options as defined by FDP_PRT_EXT.1 in the PP-Module for File Encryption" is selected, for all configuration options listed in the TSS as being stored and protected using encryption, the evaluator shall examine the contents of the configuration option storage (identified in the TSS) to determine that the options have been encrypted.

The ST does not make this selection.

2.3.3 Specification of Management Functions (FMT_SMF.1)

2.3.3.1 TSS Activities

None.

2.3.3.2 Guidance Activities

The evaluator shall verify that every management function mandated by the PP is described in the operational guidance and that the description contains the information required to perform the management duties associated with the management function.

As described in Section 6.4.3 of [ST] (“Specification of Management Functions (FMT_SMF.1)”), the TOE supports the following security-relevant management functions:

- Configuration of retrieval and analysis of VBR event logs and infrastructure information from VBR systems
- Reviewing of TOE-generated reports concerning analyzed VBR event logs and infrastructure information.

Section “Software Download, Installation and Configuration”, subsection “Management” of [CCECG] describes these management functions. The descriptions contain the information required to perform the management duties associated with these management functions.

2.3.3.3 Test Activities

The evaluator shall test the application's ability to provide the management functions by configuring the application and testing each option selected from above. The evaluator is expected to test these functions in all the ways in which the ST and guidance documentation state the configuration can be managed.

The evaluator followed the application guidance and tested the application’s ability to provide the management functions of retrieval and analysis of VBR event logs and infrastructure information from VBR systems, and reviewing reports that the TOE generates concerning the analyzed event logs and infrastructure.

2.4 Privacy (FPR)

2.4.1 User Consent for Transmission of Personally Identifiable Information (FPR_ANO_EXT.1)

2.4.1.1 TSS Activities

The evaluator shall inspect the TSS documentation to identify functionality in the application where PII can be transmitted.

Section 6.5 of [ST] (“Privacy”) states the TOE does not transmit PII over the network.

2.4.1.2 Guidance Activities

None.

2.4.1.3 Test Activities

If ***require user approval before executing*** is selected, the evaluator shall run the application and exercise the functionality responsible for transmitting PII and verify that user approval is required before transmission of the PII.

The ST does not make this selection.

2.5 Protection of the TSF (FPT)

2.5.1 Anti-Exploitation Capabilities (FPT_AEX_EXT.1)

2.5.1.1 FPT_AEX_EXT.1.1

2.5.1.1.1 TSS Activities

The evaluator shall ensure that the TSS describes the compiler flags used to enable ASLR when the application is compiled.

Section 6.6.2 of [ST] ("Anti-Exploitation Capabilities (FPT_AEX_EXT.1)") states the vendor enables address space layout randomization (ASLR) by setting the /DYNAMICBASE linker option.

2.5.1.1.2 Guidance Activities

None.

2.5.1.1.3 Test Activities

The evaluator shall perform either a static or dynamic analysis to determine that no memory mappings are placed at an explicit and consistent address. The method of doing so varies per platform. For those platforms requiring the same application running on two different systems, the evaluator may alternatively use the same device. After collecting the first instance of mappings, the evaluator must uninstall the application, reboot the device, and reinstall the application to collect the second instance of mappings.

Platforms: Microsoft Windows…

The evaluator shall run the same application on two different Windows systems and run a tool that will list all memory mapped addresses for the application. The evaluator shall then verify the two different instances share no mapping locations. The Microsoft SysInternals tool, VMMap, could be used to view memory addresses of a running application. The evaluator shall use a tool such as Microsoft's BinScope Binary Analyzer to confirm that the application has ASLR enabled.

The evaluator used VMMap to verify that two instances of the TOE do not map memory to the same locations.

2.5.1.2 FPT_AEX_EXT.1.2

2.5.1.2.1 TSS Activities

None.

2.5.1.2.2 Guidance Activities

None.

2.5.1.2.3 Test Activities

The evaluator shall verify that no memory mapping requests are made with write and execute permissions. The method of doing so varies per platform.

Platforms: Microsoft Windows…

The evaluator shall use a tool such as Microsoft's BinScope Binary Analyzer to confirm that the application passes the NXCheck. The evaluator may also ensure that the /NXCOMPAT flag was used during compilation to verify that DEP protections are enabled for the application.

The evaluator used BinScope to verify that the TOE passes NXCheck.

2.5.1.3 FPT_AEX_EXT.1.3

2.5.1.3.1 TSS Activities

None.

2.5.1.3.2 Guidance Activities

None.

2.5.1.3.3 Test Activities

The evaluator shall configure the platform in the ascribed manner and carry out one of the prescribed tests:

Platforms: Microsoft Windows…

If the OS platform supports Windows Defender Exploit Guard (Windows 10 version 1709 or later), then the evaluator shall ensure that the application can run successfully with Windows Defender Exploit Guard Exploit Protection configured with the following minimum mitigations enabled; Control Flow Guard (CFG), Randomize memory allocations (Bottom-Up ASLR), Export address filtering (EAF), Import address filtering (IAF), and Data Execution Prevention (DEP). The following link describes how to enable Exploit Protection, https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/customize-exploit-protection.

If the OS platform supports the Enhanced Mitigation Experience Toolkit (EMET) which can be installed on Windows 10 version 1703 and earlier, then the evaluator shall ensure that the application can run successfully with EMET configured with the following minimum mitigations enabled; Memory Protection Check, Randomize memory allocations (Bottom-Up ASLR), Export address filtering (EAF), and Data Execution Prevention (DEP).

The evaluator verified that the TOE could be run without disabling any platform security features.

2.5.1.4 FPT_AEX_EXT.1.4

2.5.1.4.1 TSS Activities

None.

2.5.1.4.2 Guidance Activities

None.

2.5.1.4.3 Test Activities

The evaluator shall run the application and determine where it writes its files. For files where the user does not choose the destination, the evaluator shall check whether the destination directory contains executable files. This varies per platform:

Platforms: Microsoft Windows…

For Windows Universal Applications the evaluator shall consider the requirement met because the platform forces applications to write all data within the application working directory (sandbox). For Windows Desktop Applications the evaluator shall run the program, mimicking normal usage, and note where all user-modifiable files are written. The evaluator shall ensure that there are no executable files stored in the same directories to which the application wrote user-modifiable files.

The evaluator verified that the TOE does not write user-modifiable files to directories which contain executable files.

2.5.1.5 FPT_AEX_EXT.1.5

2.5.1.5.1 TSS Activities

None.

2.5.1.5.2 Guidance Activities

None.

2.5.1.5.3 Test Activities

The evaluator will inspect every native executable included in the TOE to ensure that stack-based buffer overflow protection is present.

Platforms: Microsoft Windows…

Applications that run as Managed Code in the .NET Framework do not require these stack protections. Applications developed in Object Pascal using the Delphi IDE compiled with RangeChecking enabled comply with this element. For other code, the evaluator shall review the TSS and verify that the /GS flag was used during compilation. The evaluator shall run a tool like, BinScope, that can verify the correct usage of /GS.

As described in section 6.6.2 of the [ST] the TOE is a .NET application. Because of this the TOE does not require stack protection.

2.5.2 Use of Supported Services and APIs (FPT_API_EXT.1)

2.5.2.1 TSS Activities

The evaluator shall verify that the TSS lists the platform APIs used in the application.

Section 6.6.1 of [ST] ("Use of Supported Services and APIs (FPT_API_EXT.1)") states the TOE invokes the Microsoft products identified in Appendix A of [ST]. Table 8 of [ST] ("Supported Services and APIs") lists the following platform services and APIs used in the TOE:

- Microsoft SQL Server 2016 (Microsoft SQL Server 2016 SP2 Express Edition is included in the TOE setup)
- Microsoft .NET Framework 4.7.2

- Windows Installer 4.5
- Microsoft Windows PowerShell 5.1
- Microsoft SQL Server Management Objects
- Microsoft SQL Server System CLR Types
- Microsoft Report Viewer Redistributable 2015
- Microsoft Universal C Runtime
- Windows DPAPI
- Windows Schannel
- Windows Registry.

2.5.2.2 Guidance Activities

None.

2.5.2.3 Test Activities

The evaluator shall then compare the list with the supported APIs (available through e.g. developer accounts, platform developer groups) and ensure that all APIs listed in the TSS are supported.

The evaluator verified that all of the TOE's listed APIs are properly documented.

2.5.3 Use of Third Party Libraries (FPT_LIB_EXT.1)

2.5.3.1 TSS Activities

None.

2.5.3.2 Guidance Activities

None.

2.5.3.3 Test Activities

The evaluator shall install the application and survey its installation directory for dynamic libraries. The evaluator shall verify that libraries found to be packaged with or employed by the application are limited to those in the assignment.

The evaluator verified that the TOE does not have any undocumented libraries.

2.5.4 Software Identification and Versions (FPT_IDV_EXT.1)

2.5.4.1 TSS Activities

If "other version information" is selected the evaluator shall verify that the TSS contains an explanation of the versioning methodology.

Section 5.2.5.3 of [ST] ("FPT_IDV_EXT.1 Software Identification and Versions") selects "other version information" in FPT_IDV_EXT.1.1 and completes the assignment with "a Major, Minor and Build Number". Section 6.6.3 of [ST] ("Software Identification and Versions (FPT_IDV_EXT.1)") explains the TOE versioning methodology. The TOE uses the version format Major.0.Minor.Build PYYYYMMDD, where 'Major' is the major release with a number of significant features, '0' is not used, 'Minor' is the minor release, usually centered around support for new platforms and bug fixes, and 'Build' is the build number, which starts at

1 and has no upper bound within the given Major version. The string 'PYYYYMMDD' denotes cumulative hotfix rollups, labelled with the date on which the package was built.

2.5.4.2 Guidance Activities

None.

2.5.4.3 Test Activities

The evaluator shall install the application, then check for the existence of version information. If SWID tags is selected the evaluator shall check for a .swidtag file. The evaluator shall open the file and verify that is contains at least a SoftwareIdentity element and an Entity element.

The TOE does not use SWID tags. The evaluator verified that it uses a major.0.minor.build versioning system.

2.5.5 Integrity for Installation and Update (FPT_TUD_EXT.1)

2.5.5.1 FPT_TUD_EXT.1.1

2.5.5.1.1 TSS Activities

None.

2.5.5.1.2 Guidance Activities

The evaluator shall check to ensure the guidance includes a description of how updates are performed.

Section "Software Download, Installation and Configuration", subsection "Trusted Update" of [CCECG] describe how the administrator performs updates of the TOE.

2.5.5.1.3 Test Activities

The evaluator shall check for an update using procedures described in either the application documentation or the platform documentation and verify that the application does not issue an error. If it is updated or if it reports that no update is available this requirement is considered to be met.

The evaluator was able to check the TOE's version number and compare it to the most recent version on the vendor's website.

2.5.5.2 FPT_TUD_EXT.1.2

2.5.5.2.1 TSS Activities

None.

2.5.5.2.2 Guidance Activities

The evaluator shall verify guidance includes a description of how to query the current version of the application.

Section "Software Download, Installation and Configuration", subsection "Trusted Update" of [CCECG] provides a description of how to query the current version of the TOE by selecting **Help -> About** on the user interface, which displays the current version of the TOE.

2.5.5.2.3 Test Activities

The evaluator shall query the application for the current version of the software according to the operational user guidance. The evaluator shall then verify that the current version matches that of the documented and installed version.

The evaluator was able to query the TOE version and verified that it matched what it should be.

2.5.5.3 FPT_TUD_EXT.1.3

2.5.5.3.1 TSS Activities

None.

2.5.5.3.2 Guidance Activities

None.

2.5.5.3.3 Test Activities

The evaluator shall verify that the application's executable files are not changed by the application.

Platforms: Apple iOS…

The evaluator shall consider the requirement met because the platform forces applications to write all data within the application working directory (sandbox).

For all other platforms, the evaluator shall perform the following test:

Test 1: The evaluator shall install the application and then locate all of its executable files. The evaluator shall then, for each file, save off either a hash of the file or a copy of the file itself. The evaluator shall then run the application and exercise all features of the application as described in the ST. The evaluator shall then compare each executable file with the either the saved hash or the saved copy of the files. The evaluator shall verify that these are identical.

The evaluator verified that the TOE's executable files are not modified by the TOE.

2.5.5.4 FPT_TUD_EXT.1.4

2.5.5.4.1 TSS Activities

The evaluator shall verify that the TSS identifies how updates to the application are signed by an authorized source. The definition of an authorized source must be contained in the TSS. The evaluator shall also ensure that the TSS (or the operational guidance) describes how candidate updates are obtained.

Section 6.6.5 of [ST] ("Trusted Update (FPT_TUD_EXT.1)") states the vendor signs TOE update packages with the Veeam Software Group GmbH certificate. DigiCert is the Certificate Authority in this case.

Section "Software Download, Installation and Configuration", subsection "Trusted Update" of [CCECG] states the administrator manually checks for product updates at https://www.veeam.com/download-version.html?tab=current. Section 6.6.5 of [ST] states the administrator must manually download and install updates.

2.5.5.4.2 Guidance Activities

None.

2.5.5.4.3 Test Activities

None.

2.5.5.5 FPT_TUD_EXT.1.5

2.5.5.5.1 TSS Activities

The evaluator shall verify that the TSS identifies how the application is distributed. If "with the platform" is selected the evaluated shall perform a clean installation or factory reset to confirm that TOE software is included as part of the platform OS. If "as an additional package" is selected the evaluator shall perform the tests in FPT_TUD_EXT.2.

Section 6.6.5 of [ST] ("Trusted Update (FPT_TUD_EXT.1)") states the TOE is distributed and installed separately from Windows. Section 6.6.6 of [ST] ("Integrity for Installation and Update (FPT_TUD_EXT.2)") states the .exe file is distributed within a .iso file.

2.5.5.5.2 Guidance Activities

None.

2.5.5.5.3 Test Activities

None.

2.5.6 Integrity for Installation and Update (FPT_TUD_EXT.2)

2.5.6.1 FPT_TUD_EXT.2.1

2.5.6.1.1 TSS Activities

None.

2.5.6.1.2 Guidance Activities

None.

2.5.6.1.3 Test Activities

The evaluator shall verify that application updates are distributed in the format supported by the platform. This varies per platform:

Platforms: Microsoft Windows…

The evaluator shall ensure that the application is packaged in the standard Windows Installer (.MSI) format, the Windows Application Software (.EXE) format signed using the Microsoft Authenticode process, or the Windows Universal Application package (.APPX) format. See https://msdn.microsoft.com/en-us/library/ms537364(v=vs.85).aspx for details regarding Authenticode signing.

The TOE's installer was verified to be a .MSI file.

2.5.6.2 FPT_TUD_EXT.2.2

2.5.6.2.1 TSS Activities

None.

2.5.6.2.2 Guidance Activities

None.

2.5.6.2.3 Test Activities

Modified in accordance with TD0664.

Platforms: Android...

The evaluator shall consider the requirement met because the platform forces applications to write all data within the application working directory (sandbox).

~~**Platforms:** Microsoft Windows...~~

~~The evaluator shall install the application and then locate all of its executable files. The evaluator shall then, for each file, save off either a hash of the file or a copy of the file itself. The evaluator shall then run the application and exercise all features of the application as described in the ST. The evaluator shall then compare each executable file with the either the saved hash or the saved copy of the files. The evaluator shall verify that these are identical.~~

Platforms: Apple iOS...

The evaluator shall consider the requirement met because the platform forces applications to write all data within the application working directory (sandbox).

All Other Platforms:

The evaluator shall record the path of every file on the entire filesystem prior to installation of the application, and then install and run the application. Afterwards, the evaluator shall then uninstall the application, and compare the resulting filesystem to the initial record to verify that no files, other than configuration, output, and audit/log files, have been added to the filesystem.

The evaluator examined the file system of the TOE platform prior to TOE installation and after installing, running and then uninstalling the TOE. The evaluator verified that the TOE uninstalls itself correctly and does not leave residual files beyond those permitted by the test activity.

2.5.6.3 FPT_TUD_EXT.2.3

2.5.6.3.1 TSS Activities

The evaluator shall verify that the TSS identifies how the application installation package is signed by an authorized source. The definition of an authorized source must be contained in the TSS.

Section 6.6.6 of [ST] ("Integrity for Installation and Update (FPT_TUD_EXT.2)") states the vendor signs the TOE installation package with the Veeam Software Group GmbH certificate. DigiCert is the Certificate Authority in this case.

2.5.6.3.2 Guidance Activities

None.

2.5.6.3.3 Test Activities

None.

2.6 Trusted Path/Channels (FTP)

2.6.1 Protection of Data in Transit (FTP_DIT_EXT.1)

2.6.1.1 TSS Activities

For platform-provided functionality, the evaluator shall verify the TSS contains the calls to the platform that TOE is leveraging to invoke the functionality.

Section 6.7.1 of [ST] ("Protection of Data in Transit (FTP_DIT_EXT.1)") states the TOE invokes platform-provided Schannel to receive Web server connections on port 1239 for remote administration.

2.6.1.2 Guidance Activities

None.

2.6.1.3 Test Activities

The evaluator shall perform the following tests:

Test 1: The evaluator shall exercise the application (attempting to transmit data; for example by connecting to remote systems or websites) while capturing packets from the application. The evaluator shall verify from the packet capture that the traffic is encrypted with HTTPS, TLS, DTLS, SSH, or IPsec in accordance with the selection in the ST.

The TOE's management data was shown to be protected by TLS.

Test 2: The evaluator shall exercise the application (attempting to transmit data; for example by connecting to remote systems or websites) while capturing packets from the application. The evaluator shall review the packet capture and verify that no sensitive data is transmitted in the clear.

The TOE's management data was shown to be protected by TLS.

Test 3: The evaluator shall inspect the TSS to determine if user credentials are transmitted. If credentials are transmitted the evaluator shall set the credential to a known value. The evaluator shall capture packets from the application while causing credentials to be transmitted as described in the TSS. The evaluator shall perform a string search of the captured network packets and verify that the plaintext credential previously set by the evaluator is not found.

The evaluator examined the TSS in [ST] and determined the TOE does not transmit user credentials.

3. Security Assurance Requirement Evaluation Activities

3.1 Class ASE: Security Target

As per ASE activities defined in [CEM].

The evaluation team performed the ASE work units as defined in [CEM] and assigned a Pass verdict to each work unit.

3.2 Class ADV: Development

The information about the TOE is contained in the guidance documentation available to the end user as well as the TSS portion of the ST. The TOE developer must concur with the description of the product that is contained in the TSS as it relates to the functional requirements. The evaluation activities contained in Section 5.1 Security Functional Requirements should provide the ST authors with sufficient information to determine the appropriate content for the TSS section.

3.2.1 Basic Functional Specification (ADV_FSP.1)

3.2.1.1 Evaluation Activities

There are no specific assurance activities associated with these SARs, except ensuring the information is provided. The functional specification documentation is provided to support the evaluation activities described in Section 5.1, and other activities described for AGD, ATE, and AVA SARs. The requirements on the content of the functional specification information is implicitly assessed by virtue of the other assurance activities being performed; if the evaluator is unable to perform an activity because there is insufficient interface information, then an adequate functional specification has not been provided.

The Assurance Activities identified above provided sufficient information to determine the appropriate content for the TSS section and to perform the assurance activities. Since these are directly associated with the SFRs, and are implicitly already done, no additional documentation or analysis is necessary.

3.3 Class AGD: Guidance Documents

The guidance documents will be provided with the ST. Guidance must include a description of how the IT personnel verifies that the Operational Environment can fulfill its role for the security functionality. The documentation should be in an informal style and readable by the IT personnel. Guidance must be provided for every operational environment that the product supports as claimed in the ST. This guidance includes instructions to successfully install the TSF in that environment; and Instructions to manage the security of the TSF as a product and as a component of the larger operational environment. Guidance pertaining to particular security functionality is also provided; requirements on such guidance are contained in the evaluation activities specified with each requirement.

3.3.1 Operational User Guidance (AGD_OPE.1)

3.3.1.1 Evaluation Activities

Some of the contents of the operational guidance will be verified by the assurance activities in Section 5.1 and evaluation of the TOE according to the [CEM]. The following additional information is also required.

If cryptographic functions are provided by the TOE, the operational guidance shall contain instructions for configuring the cryptographic engine associated with the evaluated configuration of the TOE. It shall provide a warning to the administrator that use of other cryptographic engines was not evaluated nor tested during the CC evaluation of the TOE.

The documentation must describe the process for verifying updates to the TOE by verifying a digital signature – this may be done by the TOE or the underlying platform.

The evaluator shall verify that this process includes the following steps:

- Instructions for obtaining the update itself. This should include instructions for making the update accessible to the TOE (e.g., placement in a specific directory).
- Instructions for initiating the update process, as well as discerning whether the process was successful or unsuccessful. This includes generation of the digital signature. The TOE will likely contain security functionality that does not fall in the scope of evaluation under this PP. The operational guidance shall make it clear to an administrator which security functionality is covered by the evaluation activities.

The TOE does not implement cryptographic functions. Instead, it leverages platform-provided cryptography to protect sensitive data at rest (DPAPI) and in transit (Schannel).

The guidance provided by [CCECG] includes a description of how the administrator performs updates of the TOE. The description covers how to obtain the update and make it accessible to the TOE and how to initiate the update process. Refer to section “Software Download, Installation and Configuration”, subsection “Trusted Update” of [CCECG]. The administrator can discern the success or otherwise of an upgrade attempt by viewing the running TOE version using the “Help > About” function in the administrator UI.

Section “Logical Boundaries” of [CCECG] describes the security functionality of the TOE that falls within the scope of evaluation, while section “Functionality Excluded From the Evaluation Configuration” lists specific TOE functionality not covered by the evaluation.

3.3.2 Preparative Procedures (AGD_PRE.1)

3.3.2.1 Evaluation Activities

As indicated in the introduction above, there are significant expectations with respect to the documentation—especially when configuring the operational environment to support TOE functional requirements. The evaluator shall check to ensure that the guidance provided for the TOE adequately addresses all platforms claimed for the TOE in the ST.

The TOE in its evaluated configuration is supported on a single platform that is adequately addressed in the guidance documentation. Section “TOE Overview”, subsection “Physical Boundaries” of [CCECG] states the TOE is installed on a single instance of Microsoft Windows Server 2019.

3.4 Class ALC: Life-Cycle Support

At the assurance level provided for TOEs conformant to this PP, life-cycle support is limited to end-uservisible aspects of the life-cycle, rather than an examination of the TOE vendor’s development and configuration management process. This is not meant to diminish the critical role that a developer’s practices play in contributing to the overall trustworthiness of a product; rather, it is a reflection on the information to be made available for evaluation at this assurance level.

3.4.1 Labeling of the TOE (ALC_CMC.1)

3.4.1.1 Evaluation Activities

The evaluator shall check the ST to ensure that it contains an identifier (such as a product name/version number) that specifically identifies the version that meets the requirements of the ST. Further, the evaluator shall check the AGD guidance and TOE samples received for testing to ensure that the version number is consistent with that in the ST. If the vendor maintains a web site advertising the TOE, the evaluator shall examine the information on the web site to ensure that the information in the ST is sufficient to distinguish the product.

Section 1.1 of [ST] ("Security Target, Target of Evaluation, and Common Criteria Identification") includes the TOE identification. The TOE is identified in terms of the software included in the evaluated configuration. This consists of Veeam ONE v12. This is consistent with the version number of the TOE identified in [CCECG] and the version identified by the TOE sample received for testing.

3.4.2 TOE Coverage (ALC_CMS.1)

3.4.2.1 Evaluation Activities

The "evaluation evidence required by the SARs" in this PP is limited to the information in the ST coupled with the guidance provided to administrators and users under the AGD requirements. By ensuring that the TOE is specifically identified and that this identification is consistent in the ST and in the AGD guidance (as done in the assurance activity for ALC_CMC.1), the evaluator implicitly confirms the information required by this component. Life-cycle support is targeted aspects of the developer's life-cycle and instructions to providers of applications for the developer's devices, rather than an in-depth examination of the TSF manufacturer's development and configuration management process. This is not meant to diminish the critical role that a developer's practices play in contributing to the overall trustworthiness of a product; rather, it's a reflection on the information to be made available for evaluation.

The evaluator shall ensure that the developer has identified (in guidance documentation for application developers concerning the targeted platform) one or more development environments appropriate for use in developing applications for the developer's platform. For each of these development environments, the developer shall provide information on how to configure the environment to ensure that buffer overflow protection mechanisms in the environment(s) are invoked (e.g., compiler flags). The evaluator shall ensure that this documentation also includes an indication of whether such protections are on by default, or have to be specifically enabled. The evaluator shall ensure that the TSF is uniquely identified (with respect to other products from the TSF vendor), and that documentation provided by the developer in association with the requirements in the ST is associated with the TSF using this unique identification.

As described in Section 3.4.1 above, the evaluator confirmed the TOE is labelled with unique software version identifiers. Section 6.6 of [ST] ("Protection of the TSF") describes how the TOE uses security features and APIs provided by the Windows platform. This includes data execution protection, Windows Defender Exploit Guard, and stack-based buffer overflow protection.

3.4.3 Timely Security Update (ALC_TSU_EXT.1)

This component requires the TOE developer, in conjunction with any other necessary parties, to provide information as to how the end-user devices are updated to address security issues in a timely manner. The documentation describes the process of providing updates to the public from the time a security flaw is reported/discovered, to the time an update is released. This description includes the parties involved (e.g., the developer, carriers(s)) and the steps that are performed (e.g., developer testing, carrier testing), including worst case time periods, before an update is made available to the public.

3.4.3.1 Evaluation Activities

The evaluator shall verify that the TSS contains a description of the timely security update process used by the developer to create and deploy security updates. The evaluator shall verify that this description addresses the entire application. The evaluator shall also verify that, in addition to the TOE developer's process, any third-party processes are also addressed in the description. The evaluator shall also verify that each mechanism for deployment of security updates is described.

The evaluator shall verify that, for each deployment mechanism described for the update process, the TSS lists a time between public disclosure of a vulnerability and public availability of the security update to the TOE patching this vulnerability, to include any third-party or carrier delays in deployment. The evaluator shall verify that this time is expressed in a number or range of days.

The evaluator shall verify that this description includes the publicly available mechanisms (including either an email address or website) for reporting security issues related to the TOE. The evaluator shall verify that the description of this mechanism includes a method for protecting the report either using a public key for encrypting email or a trusted channel for a website.

Section 6.1 of [ST] ("Timely Security Updates") describes the timely security update process used by the developer. The description encompasses the entirety of the TOE.

Users may submit security issues to Veeam via https://www.veeam.com/vulnerability-disclosure.html?ad=in-text-link. Availability of updates is announced via email sent to customers as well as via the Veeam website. Updates are provided within 60 days of public disclosure of vulnerabilities, including those for third-party components.

3.5 Class ATE: Tests

Testing is specified for functional aspects of the system as well as aspects that take advantage of design or implementation weaknesses. The former is done through the ATE_IND family, while the latter is through the AVA_VAN family. At the assurance level specified in this PP, testing is based on advertised functionality and interfaces with dependency on the availability of design information. One of the primary outputs of the evaluation process is the test report as specified in the following requirements.

3.5.1 Independent Testing – Conformance (ATE_IND.1)

3.5.1.1 Evaluation Activities

The evaluator shall prepare a test plan and report documenting the testing aspects of the system, including any application crashes during testing. The evaluator shall determine the root cause of any application crashes and include that information in the report. The test plan covers all of the testing actions contained in the [CEM] and the body of this PP's evaluation activities.

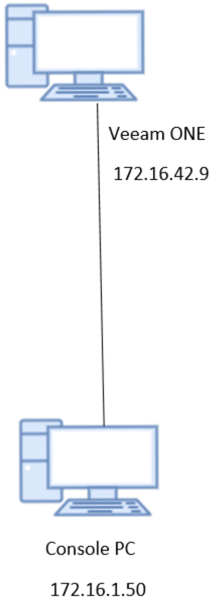
While it is not necessary to have one test case per test listed in an evaluation activity, the evaluator must document in the test plan that each applicable testing requirement in the ST is covered. The test plan identifies the platforms to be tested, and for those platforms not included in the test plan but included in the ST, the test plan provides a justification for not testing the platforms. This justification must address the differences between the tested platforms and the untested platforms, and make an argument that the differences do not affect the testing to be performed. It is not sufficient to merely assert that the differences have no affect; rationale must be provided. If all platforms claimed in the ST are tested, then no rationale is necessary. The test plan describes the composition of each platform to be tested, and any setup that is necessary beyond what is contained in the AGD documentation. It should be noted that the evaluator is expected to follow the AGD documentation for installation and setup of each platform either as part of a test or as a standard pre-test condition. This may include special test drivers or tools. For each driver or tool, an argument (not just an assertion) should be provided that the driver or tool will not adversely affect the performance of the functionality by the TOE and its platform.

This also includes the configuration of the cryptographic engine to be used. The cryptographic algorithms implemented by this engine are those specified by this PP and used by the cryptographic protocols being evaluated (e.g., SSH). The test plan identifies high-level test objectives as well as the test procedures to be followed to achieve those objectives. These procedures include expected results.

The test report (which could just be an annotated version of the test plan) details the activities that took place when the test procedures were executed, and includes the actual results of the tests. This shall be a cumulative account, so if there was a test run that resulted in a failure; a fix installed; and then a successful re-run of the test, the report would show a “fail” and “pass” result (and the supporting details), and not just the “pass” result.

The TOE was tested at Leidos’s Columbia, MD location from May 2023 to July 2023. The procedures and results of this testing are available in the DTR document.

The following figure identifies the devices used for testing the TOE and describes the test configuration.



The following components were used to create the test configurations:

TOE Hardware (Physical)

- CPU: Intel Xeon Gold 6126
- Operating System: Microsoft Windows Server 2019 Standard
- Storage: 2.0 TB HDD
- Software: Veeam ONE 12.0.0.2365

Lab Equipment

- Virtual machines
  - tlss.leidos.ate
    - Operating System: Ubuntu 18.04
    - Purpose: NMAP Scans, Packet Captures
- Physical machines
  - cctl-jump.leidos.ate
    - Operating System: Windows Server 2016
    - Purpose: Terminal Server to access test network from corporate network, Access to the TOE web interface
    - Software utilized: Chrome v112.0.5615.49.

3.6 Class AVA: Vulnerability Assessment

For the current generation of this protection profile, the evaluation lab is expected to survey open sources to discover what vulnerabilities have been discovered in these types of products. In most cases, these vulnerabilities will require sophistication beyond that of a basic attacker. Until penetration tools are created and uniformly distributed to the evaluation labs, the evaluator will not be expected to test for these vulnerabilities in the TOE. The labs will be expected to comment on the likelihood of these vulnerabilities given the documentation provided by the vendor. This information will be used in the development of penetration testing tools and for the development of future protection profiles.

3.6.1 Vulnerability Survey (AVA_VAN.1)

3.6.1.1 Evaluation Activities

The evaluator shall generate a report to document their findings with respect to this requirement. This report could physically be part of the overall test report mentioned in ATE_IND, or a separate document. The evaluator performs a search of public information to find vulnerabilities that have been found in similar applications with a particular focus on network protocols the application uses and document formats it parses.

The evaluator documents the sources consulted and the vulnerabilities found in the report.

For each vulnerability found, the evaluator either provides a rationale with respect to its non-applicability, or the evaluator formulates a test (using the guidelines provided in ATE_IND) to confirm the vulnerability, if suitable. Suitability is determined by assessing the attack vector needed to take advantage of the vulnerability. If exploiting the vulnerability requires expert skills and an electron microscope, for instance, then a test would not be suitable and an appropriate justification would be formulated.

For Windows, Linux, macOS and Solaris: The evaluator shall also run a virus scanner with the most current virus definitions against the application files and verify that no files are flagged as malicious.

The evaluation team performed a search of the CVE (Common Vulnerabilities and Exposures) database (https://cve.mitre.org/).

The evaluation team performed searches on 21 July 2023, using the following search terms:

- “veeam”
- “Veeam ONE”
- The identity of each of the third-party libraries listed in Appendix A, Table 9, of [ST].

No vulnerabilities were identified for the TOE.

The evaluator scanned the installer script using a corporate provided virus scan software (Microsoft Windows Defender) and verified that no virus signatures were detected.

The evaluation team determined that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential.