National Information Assurance Partnership

Common Criteria Evaluation and Validation Scheme

Validation Report

for

One Identity Manager v8.1

Report Number: CCEVS-VR-VID11003-2020
Dated: 4 February 2020
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

Acknowledgements

Validation Team

Daniel Faigin
Aerospace Corporation

Michelle Carlson
Jenn Dotson
Clare Olin
Patrick Mallett, PhD
MITRE Corporation

Common Criteria Testing Laboratory

Leidos Inc.
Columbia, MD

Table of Contents

List of Tables

1 Executive Summary

This Validation Report (VR) documents the National Information Assurance Partnership (NIAP) assessment of the evaluation of One Identity Manager v8.1 (the Target of Evaluation, or TOE). It presents the evaluation results, their justifications, and the conformance results. This VR is not an endorsement of the TOE by any agency of the U.S. Government and no warranty of the TOE is either expressed or implied.

This VR 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 Information Technology (IT) product 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. This VR applies only to the specific version and configuration of the product as evaluated and as documented in the ST. Prospective users should carefully read 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.

The evaluation of One Identity Manager v8.1 was performed by Leidos Common Criteria Testing Laboratory (CCTL) in Columbia, Maryland, USA, and was completed in February 2020.

The evaluation was conducted in accordance with the requirements of the Common Criteria and Common Methodology for IT Security Evaluation (CEM), version 3.1, release 4 ([1], [2], [3], [4]) and evaluation activities specified in the following documents:

- *Standard Protection Profile for Enterprise Security Management Identity and Credential Management*, Version 2.1, 24 September 2013 [5]

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).

One Identity Manager v8.1 is an identity and credential management product that provides centralized definition of identity and credential attributes for organizational users. The TOE is configured to connect to environmental systems and applications in the organization so that modifications to user identity and credential data are propagated across the organization to take effect where relevant. The TOE can perform centralized maintenance of credential data, e.g. by suspending or revoking a user's credential, which will then revoke access to systems and services that are synchronized with the TOE. The TOE defines a centralized password policy and can be used to provide a single point of service for user password maintenance so that the TOE's defined password policy is then implicitly enforced across dependent systems.

The Leidos evaluation team determined that the TOE is conformant to the claimed Protection Profile (PP) and, when installed, configured and operated as specified in the evaluated guidance documentation, satisfies all the security functional requirements stated in the ST [6]. The information in this VR is largely derived from the Assurance Activities Report (AAR) ([7]) and the associated test report produced by the Leidos evaluation team ([8]).

The validation team reviewed the evaluation outputs produced by the evaluation team, in particular the AAR and associated test report. The validation team found that the evaluation showed that the TOE satisfies all the security functional and assurance requirements stated in the ST. The evaluation also showed that the TOE is conformant to the claimed PP and that the evaluation activities specified in [5] had been performed appropriately. 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 (ETR) ([9]) are consistent with the evidence produced.

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, commercial testing laboratories called Common Criteria Testing Laboratories (CCTLs) use the Common Criteria and Common Methodology for IT Security Evaluation (CEM) to conduct security evaluations, 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 IT 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 provides information needed to completely identify the product and its evaluation, including:

- The TOE—the fully qualified identifier of the product as evaluated
- The ST—the unique identification of the document describing the security features, claims, and assurances of the product
- The conformance result of the evaluation
- The PP to which the product is conformant

The organizations and individuals participating in the evaluation.

Table 1: Document Information

Document Type	Document Name
Evaluation Scheme	United States NIAP Common Criteria Evaluation and Validation Scheme
TOE	One Identity Manager v8.1
Security Target	One Identity Manager v8.1 Security Target, Version 1.2, 3 February 2020
Sponsor & Developer	One Identity, LLC 4 Polaris Way Aliso Viejo, CA 92656 United States
Completion Date	February 2020
CC Version	Common Criteria for Information Technology Security Evaluation, Version 3.1, Release 4, September 2012
CEM Version	Common Methodology for Information Technology Security Evaluation: Version 3.1, Release 4, September 2012
PP/Extended Package	Standard Protection Profile for Enterprise Security Management Identity and Credential Management, Version 2.1, 24 October 2013
Conformance Result	PP Compliant, CC Part 2 extended, CC Part 3 conformant

CCTL	Leidos Common Criteria Testing Laboratory 6841 Benjamin Franklin Drive Columbia, MD 21046
Evaluation Personnel	Anthony Apted Greg Beaver Justin Fisher Furukh Siddique Kevin Steiner
Validation Personnel	Daniel Faigin Michelle Carlson Jenn Dotson Clare Olin Patrick Mallett

3 Architectural Information

The One Identity Manager v8.1 TOE provides centralized provisioning and management of user accounts based on defined 'identities'. The TOE provides identity and credential management functions by serving as the authoritative source for various user attributes while also designating various external systems to be authoritative sources for other attributes. The end result is that user data can be automatically and accurately propagated to multiple organizational locations so that external systems can subsequently make use of this data. For example, One Identity Manager may interface with an organization's HR system (e.g. Peoplesoft) such that when a new user is created by the HR system, One Identity Manager will automatically generate external system accounts for that new user (e.g. create a new AD entry for them based on the default information and/or information supplied by the HR system). One Identity Manager can also be used to manually create user accounts and as an interface for TOE users to perform self-service management of their own password credentials, which are then pushed out to the organizational repositories (external systems) where that password data resides.

The One Identity Manager v8.1 TOE consists of several components: fat client, web UI, web service, job service (and its connectors) that interface with a centralized Microsoft SQL Server database through a shared object layer interface. The object layer interface is responsible for all database I/O operations and interfacing with external systems. The One Identity Manager Service (Job Service) performs data synchronization and provisioning between the database and any connected target systems and executes actions at the database and file level. The Job Service retrieves process steps from the JobQueue and executes them. The Job Service Application is the only method of interfacing with other organizational systems (e.g. HR system, AD, SAP) and the protected communication is through the use of connectors. The fat client provides the Designer and Synchronization Editor tools that are used for the initial setup of One Identity Manager. The fat client also includes the Manager application, but this interacts with the TOE via the web service. The Web UI and web services component provide interfaces for managing employee data. The Web UI is the graphical front-end that handles administrative management tasks, and where a TOE user can use the Password Reset Portal to change their password. The Web service is a REST API that provides the same functions as the Web UI as well as the interfaces that Manager uses to manage administrative role assignment and password policies.

From an architectural standpoint, the identity data maintained by One Identity Management resides in a central database (in the operational environment). All communications between the TOE and the database use TLS.

The TOE supports a variety of connectors, which are used to communicate with external systems to synchronize identity and credential data with the TOE's operational environment. Depending on the system the TOE is connecting to, TLS, SSH, or HTTPS may be used to secure data in transit. Trusted communications are implemented by the TOE's operational environment and rely on the FIPS-validated algorithm implementations provided by the underlying OS platform.

The tested configuration of the TOE used Windows 10 for the fat client and Windows Server 2016 for all other TOE components. The environmental database used to store TOE data was SQL Server 2017.

4 Security Policy

4.1 Enterprise Security Management

The TOE provides the ability to identify and authenticate administrators using Active Directory. The TOE provides the capability to define and manage enterprise user security attributes and provision modifications in the target systems. The TOE provides the capability to define and securely transmit identity and credential data for use with other ESM products. The TOE provides a password restriction policy mechanism to ensure secure passwords are defined.

4.2 Security Audit

The TOE generates logs for the security relevant events specified in [5]. The TOE writes the logs to the central Microsoft SQL Server database using a TLS channel.

4.3 Identification and Authentication

The TOE associates roles, entitlements, and other user attributes with enterprise users and relies on the operational environment for user authentication. The TOE enforces binding of users to subjects by defining users as ‘employee’ objects inside the TOE. These objects are then mapped to accounts on external systems such that changes to user data on the TOE is propagated to these external systems through synchronization. The TOE also enforces binding between administrators and subjects during initial authentication such that an administrator’s privileges to manage the TSF are assigned when they log in and any changes to their privileges only take effect on subsequent logins.

4.4 Security Management

The TOE provides the following management functions identified in [5]:

- Management of administrator authentication data
- Definition and management of user identity and credential data
- Configuration of password policy for credential data
- Management of user credential status (e.g. suspended)
- Enrollment of users
- Configuration of transmission of identity and credential data to external entities, including enabling of trusted communications where necessary
- Configuration and assignment of administrative roles

The TOE also provides the ability for users to perform self-service management of their own password credential data. The TOE restricts access to the management functions to users with applicable roles and entitlements. By default, the TOE includes a One Identity Manager administrator role with full privileges to manage the TSF, but additional administrative roles can be defined and associated with users to grant a subset of these privileges.

4.5 Protection of the TSF

Credentials/keys used by the TOE are stored in the operational environment. The TOE does not offer any interfaces to view the credentials/keys.

4.6 Trusted Path/Channels

The TOE provides trusted communication channels using TLS for communication with authentication servers, the audit server and for transfer of policy (identity and credential) data. SSH is used for transfer of policy data between the TOE and UNIX systems. HTTPS is used to protect communication channels between distributed TOE components.

The TOE provides trusted communication paths using Web UI/Web Service for remote administrators, which is enforced by IIS.

5 Assumptions and Clarification of Scope

5.1 Assumptions

The ST references the PP to which it claims conformance for assumptions about the use of the TOE. Those assumptions, drawn from the claimed PP, are as follows:

- The product is assumed to rely on cryptographic primitives (algorithms and protocol implementations) provided by its operational environment to provide cryptographic services.
- The product is assumed to be capable of establishing connectivity with other enterprise security management products in its operational environment.
- Third-party entities that exchange attribute data with the product are assumed to be trusted.
- The operational environment is assumed to provide mechanisms that reduce the ability of an attacker to impersonate a legitimate user during authentication, i.e. the TOE relies on a third-party authentication mechanism that includes handling for excessive authentication failure attempts.
- The product is assumed to be able to receive reliable time data from its operational environment.

5.2 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:

- As with any evaluation, this evaluation only shows that the evaluated configuration meets the security claims made, with a certain level of assurance (the evaluation activities specified in [5] as modified by applicable NIAP Technical Decisions cited in [6] and performed by the evaluation team).
- This evaluation covers only the specific software version identified in this document, and not any earlier or later versions released or in process.
- The evaluation of security functionality of the product was limited to the functionality specified in the Security Target [6].
- The TOE is responsible for maintaining centralized identity and credential data for organizational users and transmitting this data as needed to its operational environment based on configured synchronization behavior. Once the data has been transmitted to its operational environment, it is outside the TOE's scope of control, so continued security and correct usage of this data is the responsibility of system administrators.
- The TOE relies on the Windows OS platform's cryptographic libraries to perform cryptographic functions. To ensure that sufficiently strong cryptography is used, the OS platform must be configured into a FIPS-compliant mode of operation.
- The TOE can be configured to use the following components in its operational environment; however, these components have not been evaluated and their use with the TOE is not covered by this evaluation:
  - LDAP Enterprise User Stores – in the evaluated configuration, the TOE used the environmental SQL Server database as its user store.

  - Administrator authentication methods – in the evaluated configuration, the TOE used Active Directory for administrator authentication. Other methods (internal authentication, LDAP server, OpenID Connect, OAUTH2, 2-factor authentication) were not tested.
  - Connectors – in the evaluated configuration, the TOE did not use the following connectors:
    - SCIMv2
    - Database (ADO.NET, OLEDB, ODBC)
    - Structured Files (CSV, tab separated, etc.)
    - IBM Notes
    - SAP R/3 and S/4Hana
    - PowerShell
    - Oracle E-Business Suite
- 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.
- The TOE must be installed, configured and managed as described in the documentation referenced in section 6 of this Validation Report.

6 Documentation

One Identity offers guidance documents describing the installation process for the TOE as well as guidance for subsequent administration and use of the applicable security features. The guidance documentation examined during the evaluation and delivered with the TOE is as follows:

- One Identity Manager 8.1 Common Criteria Supplemental Admin Guidance, February 2020 [10]

One Identity also includes a large number of additional administrative guides. The evaluators reviewed these guides and identified the portions of them that were relevant to the evaluation in in the AAR [7]. The supplemental admin guidance [10] cites these other guides as needed when a security-relevant function summarized in the supplement needs to be described in further detail. The guidance documentation also includes the following preparatory procedures:

- One Identity Manager 8.1 Common Criteria Supplemental Admin Guidance, February 2020 [10]
- Identity Manager 8.1 Installation Guide, April 2019 [11]
- Identity Manager 8.1 Configuration Guide, March 2019 [12]

To use the product in the evaluated configuration, the product must be configured as specified in these guides.

Any additional customer documentation provided with the product, or that which may be available online, was not included in the scope of the evaluation and therefore should not be relied upon to configure or operate the device as evaluated. Consumers are encouraged to download the evaluated administrative guidance documentation from the NIAP website.

7 IT Product Testing

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

- One Identity Manager v8.1 Test Report and Procedures, Version 1.2, February 3, 2020 [8]

A non-proprietary description of the tests performed and their results is provided in the following document:

- One Identity Manager v8.1 Assurance Activities Report, Version 1.2, February 3, 2020 [7]

The purpose of the testing activity was to confirm the TOE behaves in accordance with the TOE security functional requirements as specified in the ST for a product that claims conformance to *Standard Protection Profile for Enterprise Security Management Identity and Credential Management, Version 2.1* [5].

The evaluation team devised a Test Plan based on the Testing Assurance Activities specified in [5]. 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.

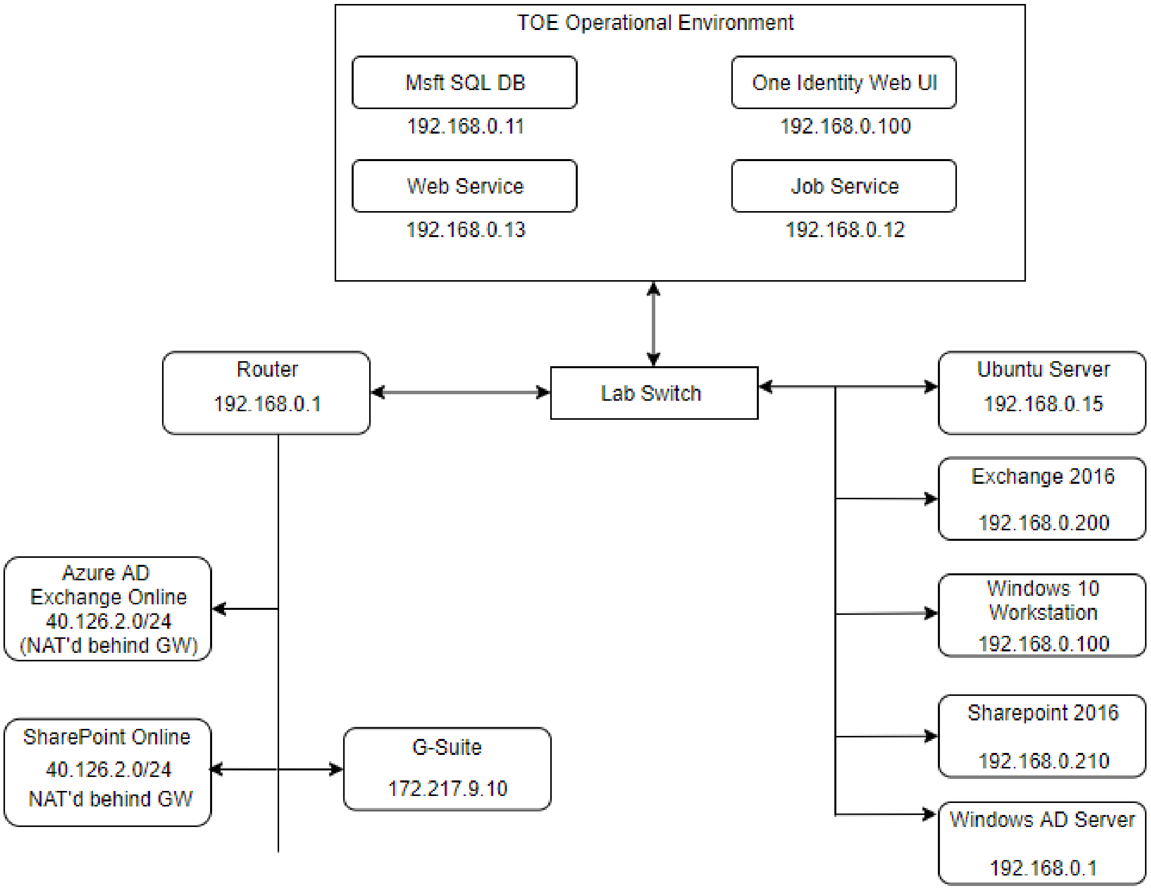
Independent testing took place at Leidos CCTL facilities in Columbia, Maryland.

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.

Given the complete set of test results from the test procedures exercised by the evaluators, the testing requirements for the claimed Protection Profile were satisfied.

7.1 Test Configuration

This section identifies the devices used for testing the TOE and describes the test configuration. The test configuration is shown below:



The following components are installed on the TOE appliance or required to be installed on client machines or in the operational environment and thus were included in the evaluated configuration during testing:

- The TOE application installed on a Microsoft Windows Server 2016 Standard platform with the following additional components:
  - MS SQL Server 2017 (64-bit)
- Non-TOE Components required for the client and operational environment:
  - Active Directory Server
    - Microsoft Internet Information Services Version 10.0.14393.0
    - Microsoft .NET framework 4.7.2
  - Additional computer for Remote Administration through the Web GUI.
    - The following browser versions were used during the course of testing.
      - Microsoft Edge 42.17134.1098.0
      - Internet Explorer 11.1130.17134.0
  - Any SSH client (i.e. PuTTY)
  - Any RDP client (i.e. Microsoft Terminal Server Client)

- Additional computers running Ubuntu, Windows 10 1803 Enterprise and Windows Server 2012 R2 Active Directory for product functionality testing.
- Microsoft Azure Active Directory
- Microsoft Office 365 Exchange Online
- Microsoft Office 365 SharePoint Online
- Ubuntu Server
  - Version: Ubuntu 18.04.3
- Microsoft Exchange 2016 Version 15.1 (Build 1913.5)
- Microsoft SharePoint 2016
- Google G-Suite

8 Evaluated Configuration

The One Identity Manager v8.1 TOE consists of fat client, web UI, web service, job service, and connectors. The TOE provides connectors and any required templates for the following types of external systems:

Connectors and prepared templates:

- Active Directory
- UNIX/Linux
- Exchange 2010, 2013, 2016
- SharePoint 2010, 2013, 2016
- Azure AD
- Exchange Online
- SharePoint Online
- Google G-Suite
- LDAP (including AS/400, RACF, ACF2, Top Secret)

The Operational Environment consists of:

- Database Server
  - SQL Server 2017 (64-bit) with the current cumulative update
- Minimum System Requirements - Administrative Workstations (Fat client)
  - Windows 10 (32-bit or 64-bit) minimum version 1511
  - Microsoft .NET Framework Version 4.7.2 or later
- Minimum system requirements for the Job Service (admin guides refer to as Server Service)
  - Windows Server 2016
  - Microsoft .NET Framework Version 4.7.2 or later
- Minimum system requirements for the Web Service and Web UI
  - Windows Server 2016
  - Microsoft .NET Framework Version 4.7.2 or later
- Microsoft Internet Information Services 10 or 8.5 or 8 or 7.5 or 7 with ASP.NET 4.7.2
- web browser:
  - Internet Explorer 11 or later
  - Firefox (Latest Release)
  - Chrome (Latest Release)
  - Microsoft Edge (Latest Release)
- SSH Client,

- one or more supported external systems (see connectors above),
- Active Directory authentication server.

The TOE relies on the Windows FIPS-compliant cryptographic libraries bcryptprimitives.dll (CMVP2937) and cng.sys (CMVP2936) for trusted channel and trusted path connections. Random seeding for deterministic random bit functions used for key generation is obtained through the Windows bcryptgenrandom function and its underlying OS operations that provide its non-deterministic entropy data. The TOE uses SSHblackbox that in turn uses the same underlying Windows FIPS-compliant cryptographic libraries for SSH functionality. SSHBlackbox is provided with the One Identity Manager TOE but is itself a third-party product.

The evaluation excludes the following Operational Environment software and security functionality that is supported by One Identity Manager but is not included or tested in the evaluated configuration:

- LDAP Enterprise User Stores, and

User authentication methods: Internal One Identity Manager authentication, LDAP Server, OpenID Connect, OAUTH2, and 2-factor authentication.

9 Results of the Evaluation

The results of the evaluation of the TOE against its target assurance requirements are generally described in this section and are presented in detail in the proprietary ETR [9]. The reader of this VR can assume that all assurance activities and work units received passing verdicts.

A verdict for an assurance component is determined by the resulting verdicts assigned to the corresponding evaluator action elements. The evaluation was conducted based upon CC version 3.1, revision 4 ([1], [2], [3]) and CEM version 3.1, revision 4 [4], and the specific evaluation activities defined in the claimed Protection Profile [5].

The evaluation determined the TOE satisfies the conformance claims made in the Security Target [6], which included the PP conformance claim and claims of CC Part 2 extended and Part 3 conformant.

9.1 Evaluation of the Security Target (ST) (ASE)

The evaluation team performed each TSS assurance activity and ASE CEM work unit. The ST evaluation ensured the ST contains an ST introduction, TOE overview, TOE description, security problem definition in terms of threats, policies and assumptions, description of security objectives for the operational environment, a statement of security requirements claimed to be met by the product that are consistent with the claimed Protection Profile, and security function descriptions that satisfy the requirements.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.2 Evaluation of the Development (ADV)

The evaluation team performed each ADV assurance activity and applied each ADV_FSP.1 CEM work unit. The evaluation team assessed the evaluation evidence and found it adequate to meet the requirements specified in the claimed Protection Profile for design evidence. The ADV evidence consists of the TSS descriptions provided in the ST and product guidance documentation providing descriptions of the TOE external interfaces.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.3 Evaluation of the Guidance Documents (AGD)

The evaluation team performed each guidance assurance activity and applied each AGD work unit. The evaluation team determined the adequacy of the operational user guidance in describing how to operate the TOE in accordance with the descriptions in the ST. The evaluation team followed the guidance in the TOE preparative procedures to test the installation and configuration procedures to ensure the procedures result in the evaluated configuration. The guidance documentation was assessed during the design and testing phases of the evaluation to ensure it was complete.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.4 Evaluation of the Life Cycle Support Activities (ALC)

The evaluation team performed each ALC assurance activity and applied each ALC_CMC.1 and ALC_CMS.1 CEM work unit, to the extent possible given the evaluation evidence required by the claimed Protection Profile. The evaluation team ensured the TOE is labeled with a unique identifier consistent with the TOE identification in the evaluation evidence.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.5 Evaluation of the Test Documentation and the Test Activity (ATE)

The evaluation team performed each testing assurance activity and applied each ATE_IND.1 CEM work unit. The evaluation team ran the set of tests specified by the claimed PP and recorded the results in the Test Report, summarized in the AAR.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.6 Vulnerability Assessment Activity (AVA)

The evaluation team performed each AVA assurance activity and applied each AVA_VAN.1 CEM work unit. The evaluation team performed a vulnerability analysis following the processes described in the claimed PPs. This comprised a search of public vulnerability databases.

Searches of public vulnerability repositories were performed during the evaluation and then re-performed a final time on 17 January 2020 to ensure that no additional public vulnerabilities were disclosed prior to the completion of the evaluation.

The evaluation team searched the following public vulnerability repositories:

- http://web.nvd.nist.gov/view/vuln/search
- https://support.oneidentity.com/identity-manager/all/alerts-notifications
- Google

The evaluation team used the following search terms in the searches of these repositories:

- One Identity Manager (TOE name)
- One Identity (alternate branding)
- Quest One Identity Manager (previous name of product)
- Dell One Identity Manager (previous name of product)

- “One Identity Manager” vulnerability (Google search term)
- “One Identity Manager” exploit (Google search term)

The results of these searches did not identify any vulnerabilities that are applicable to the TOE. The conclusion drawn from the vulnerability analysis is that no residual vulnerabilities exist that are exploitable by attackers with Basic Attack Potential as defined by the Certification Body in accordance with the guidance in the CEM.

The validators reviewed the work of the evaluation team and found that sufficient evidence and justification was provided by the evaluation team to confirm that the evaluation was conducted in accordance with the requirements of the CEM, and that the conclusion reached by the evaluation team was justified.

9.7 Summary of Evaluation Results

The evaluation team’s assessment of the evaluation evidence demonstrates that the claims in the ST are met, sufficient to satisfy the assurance activities specified in the claimed Protection Profile. Additionally, the evaluation team’s testing also demonstrated the accuracy of the claims in the ST.

The validation team’s assessment of the evidence provided by the evaluation team is that it demonstrates that the evaluation team followed the procedures defined in the CEM, and correctly verified that the product meets the claims in the ST.

10 Validator Comments/Recommendations

The validators suggest that the consumer pay particular attention to the evaluated configuration of the product. 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 product, to include software that was not part of the evaluated configuration, needs to be assessed separately and no further conclusions can be drawn about their effectiveness.

11 Security Target

The ST for this product's evaluation is *One Identity Manager v8.1 Security Target*, Version 1.2, 3 February 2020 [6].

12 Bibliography

The validation team used the following documents to produce this VR:

[1] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 1: Introduction and general model, Version 3.1, Revision 4, September 2012.

[2] Common Criteria Project Sponsoring Organisations. Common Criteria for Information Technology Security Evaluation: Part 2: Security functional components, Version 3.1, Revision 4, September 2012.

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

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

[5] Standard Protection Profile for Enterprise Security Management Identity and Credential Management, Version 2.1, 24 October 2013

[6] One Identity Manager v8.1 Security Target, Version 1.2, 3 February 2020

[7] One Identity Manager v8.1 Assurance Activities Report, Version 1.2, February 3, 2020

[8] One Identity Manager v8.1 Test Report and Procedures, Version 1.2, February 3, 2020

[9] Evaluation Technical Report for One Identity Manager v8.1, Version 1.2, February 3, 2020

[10] One Identity Manager 8.1 Common Criteria Supplemental Admin Guidance, February 2020

[11] Identity Manager 8.1 Installation Guide, April 2019

[12] Identity Manager 8.1 Configuration Guide, March 2019