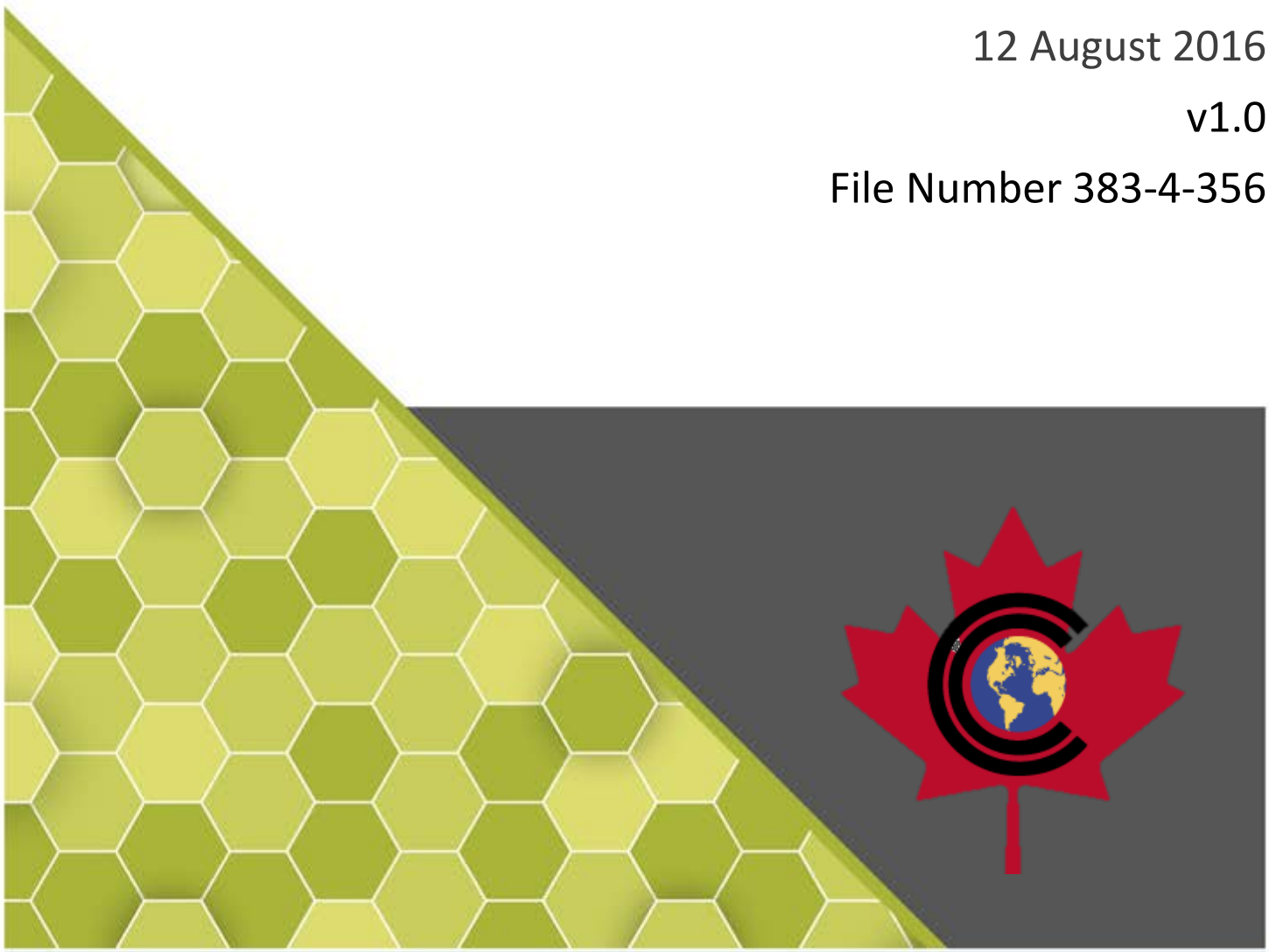
COMMON CRITERIA CERTIFICATION REPORT

VMware Horizon 6 version 6.2.2 and Horizon Client 3.5.2

12 August 2016

v1.0

File Number 383-4-356



Canada

FOREWORD

This certification report is an UNCLASSIFIED publication, issued under the authority of the Chief, Communications Security Establishment (CSE). Suggestions for amendments should be forwarded through departmental communications security channels to your Client Services Representative at CSE.

The Information Technology (IT) product identified in this certification report, and its associated certificate, has been evaluated at an approved evaluation facility – established under the Canadian Common Criteria Scheme – using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4. This certification report, and its associated certificate, applies only to the identified version and release of the product in its evaluated configuration. The evaluation has been conducted in accordance with the provisions of the Canadian CC Scheme, and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This report, and its associated certificate, are not an endorsement of the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, and no warranty for the IT product by the Communications Security Establishment, or any other organization that recognizes or gives effect to this report, and its associated certificate, is either expressed or implied.

If your department has identified a requirement for this certification report based on business needs and would like more detailed information, please contact:

ITS Client Services
Telephone: (613) 991-7654
E-mail: itsclientservices@cse-cst.gc.ca

OVERVIEW

The Canadian Common Criteria Scheme provides a third-party evaluation service for determining the trustworthiness of Information Technology (IT) security products. Evaluations are performed by a commercial Common Criteria Evaluation Facility (CCEF) under the oversight of the Certification Body, which is managed by the Communications Security Establishment.

A CCEF is a commercial facility that has been approved by the Certification Body to perform Common Criteria evaluations; a significant requirement for such approval is accreditation to the requirements of ISO/IEC 17025:2005, the General Requirements for the Competence of Testing and Calibration Laboratories. Accreditation is performed under the Program for the Accreditation of Laboratories - Canada (PALCAN), administered by the Standards Council of Canada.

The CCEF that carried out this evaluation is CGI IT Security Evaluation & Test Facility.

By awarding a Common Criteria certificate, the Certification Body asserts that the product complies with the security requirements specified in the associated security target. A security target is a requirements specification document that defines the scope of the evaluation activities. The consumer of certified IT products should review the security target, in addition to this certification report, in order to gain an understanding of any assumptions made during the evaluation, the IT product's intended environment, the evaluated security functionality, and the testing and analysis conducted by the CCEF.

The certification report, certificate of product evaluation and security target are posted to the Certified Products list (CPL) for the Canadian CC Scheme, and to the Common Criteria portal (the official website of the International Common Criteria Project).

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

EXECUTIVE SUMMARY

VMware Horizon 6 version 6.2.2 and Horizon Client 3.5.2 (hereafter referred to as the Target of Evaluation, or TOE), from VMware, Inc., was the subject of this Common Criteria evaluation. The results of this evaluation demonstrate that TOE meets the requirements of the conformance claim listed in Table 1 for the evaluated security functionality.

The TOE is a virtualization environment that delivers virtual desktops and applications that run in the datacenter to remote users, allowing them to securely access their desktops and applications from any number of devices either within the enterprise or elsewhere. The TOE does not perform the virtualization but rather manages large numbers of virtualized desktops and applications. A single administration console provides granular levels of access control to support corporate policy, along with providing centralized control, efficiency, and security by having desktop data in the data center.

CGI IT Security Evaluation & Test Facility is the CCEF that conducted the evaluation. This evaluation was completed on 12 August 2016 and was carried out in accordance with the rules of the Canadian Common Criteria Scheme.

The scope of the evaluation is defined by the security target, which identifies assumptions made during the evaluation, the intended environment for TOE, and the security functional/assurance requirements. Consumers are advised to verify that their operating environment is consistent with that specified in the security target, and to give due consideration to the comments, observations and recommendations in this certification report.

Communications Security Establishment, as the Certification Body, declares that the TOE evaluation meets all the conditions of the Arrangement on the Recognition of Common Criteria Certificates and that the product will be listed on the Certified Products list (CPL) and the Common Criteria portal (the official website of the International Common Criteria Project).

1 IDENTIFICATION OF TARGET OF EVALUATION

The Target of Evaluation (TOE) is identified as follows:

Table 1 TOE Identification

TOE Name and Version	VMware Horizon 6 version 6.2.2 and Horizon Client 3.5.2
Developer	VMware, Inc.
Conformance Claim	EAL 2+ (ALC_FLR.2)

1.1 COMMON CRITERIA CONFORMANCE

The evaluation was conducted using the Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4.

1.2 TOE DESCRIPTION

The TOE is a virtualization environment that delivers virtual desktops and applications that run in the datacenter to remote users, allowing them to securely access their desktops and applications from any number of devices either within the enterprise or elsewhere. The TOE does not perform the virtualization but rather manages large numbers of virtualized desktops and applications. A single administration console provides granular levels of access control to support corporate policy, along with providing centralized control, efficiency, and security by having desktop data in the data center.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

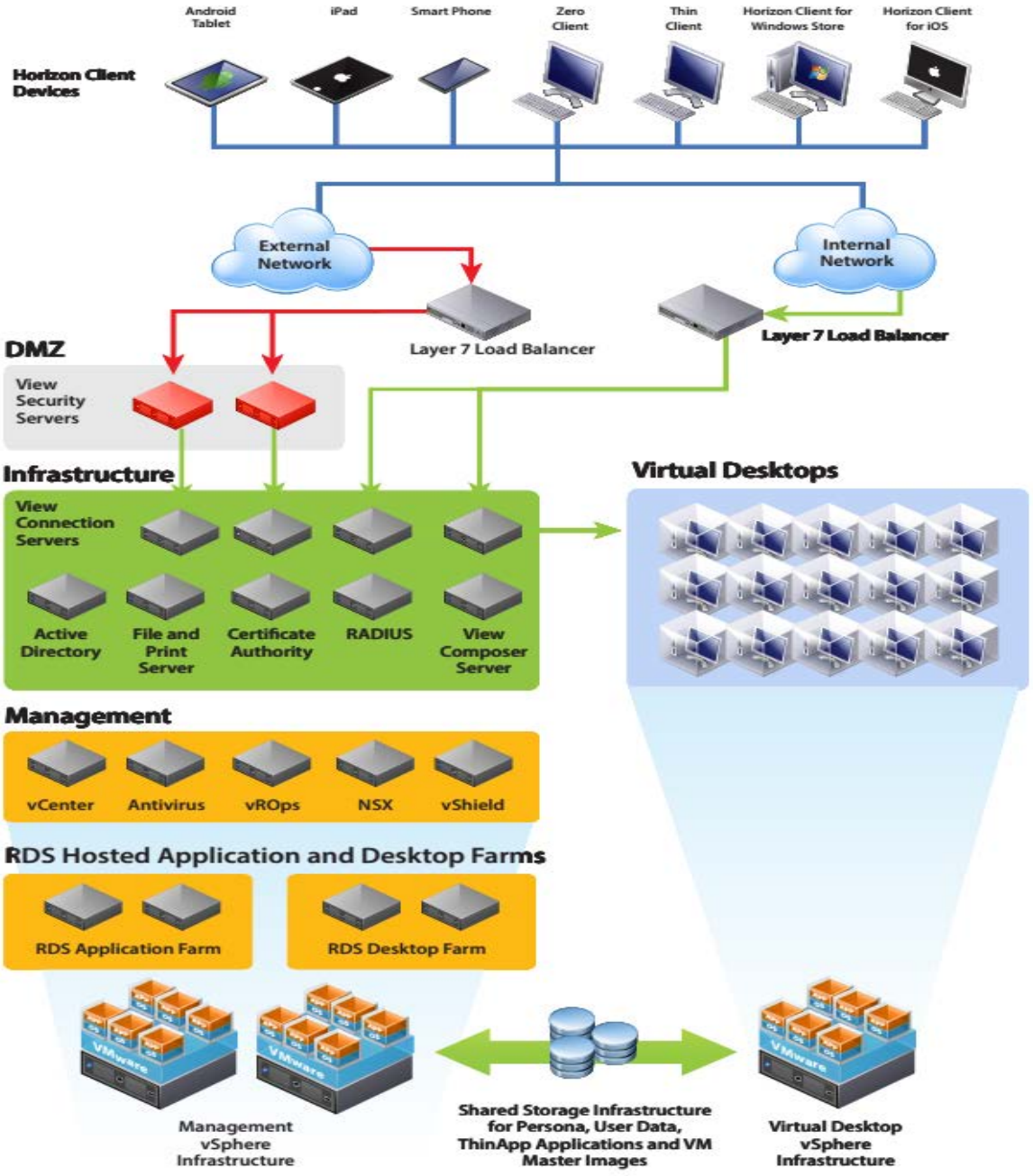


Figure 1 TOE Architecture

2 SECURITY POLICY

The TOE implements policies pertaining to the following security functional classes:

- User Data Protection
- Identification and Authentication
- Security Management
- Cryptographic Operations
- Protection of the TSF
- Session Locking and Termination

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) referenced in section 8.2.

2.1 CRYPTOGRAPHIC FUNCTIONALITY

The following cryptographic modules were evaluated by the CMVP to the FIPS 140-2 Standard and implemented in the TOE:

Table 2 Cryptographic Module(s)

Cryptographic Module	Certificate Number
VMware Horizon JCE	2559
OpenSSL with FIPS Canister 2.0	1747

3 ASSUMPTIONS AND CLARIFICATIONS OF SCOPE

Consumers of the TOE should consider assumptions about usage and environmental settings as requirements for the product's installation and its operating environment. This will ensure the proper and secure operation of the TOE.

3.1 USAGE AND ENVIRONMENTAL ASSUMPTIONS

The following assumptions are made regarding the use and deployment of the TOE:

- It is assumed that the appropriate physical security is provided within the domain for the value of the IT assets protected by the TSF and the value of the stored and processed information.
- It is assumed that the VM host software provides virtual machine isolation and is operating correctly and securely.
- It is assumed that administrators have configured IPsec associations between security servers and connection servers such that forwarded requests from client components to connection servers, and responses to such requests are protected.

3.2 CLARIFICATION OF SCOPE

The OpenSSL with FIPS Canister 2.0 cryptographic module is being claimed as vendor affirmed in accordance with CMVP Implementation Guidance IG.5.

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises the following components:

- Horizon View Client for Windows version 3.5.2 running on Windows 10, Windows 8, Windows 8.1, and Windows 7.
- View Connection Server v6.2.2 and View Security Server v6.2.2 running on Windows Server 2008 R2 and Windows Server 2012 R2.
- View Composer v6.2.2 running on Windows Server 2008 R2 and Windows Server 2012 R2 with the following DBMSs: Microsoft SQL Server 2008 SP4 (express, standard, enterprise) Microsoft SQL Server 2008 R2 (express, standard, enterprise, datacenter) Microsoft SQL Server 2012 (express, standard, datacenter) Microsoft SQL Server 2014 (standard, enterprise) Oracle Database 11g Release 2, Oracle Database 12c Release 1.
- View Agent v6.2.2 running on Windows 10 (64-bit and 32-bit) Enterprise and Professional, Windows 8.1 (64-bit and 32-bit) Enterprise and Professional, Windows 8 (64-bit and 32-bit) Enterprise and Professional, Windows 7 (64-bit and 32-bit) Enterprise and Professional SP1, Windows Server 2012 R2 (64-bit) Datacenter, Windows Server 2008 R2 (64-bit) Datacenter SP1.

The following hardware, firmware, and software, which are supplied by the operational environment, are required for the network configuration. These components are not part of the TOE.

- VMware ESXi 6.0.0b
- VMware vCenter Server 6.0.0b
- VMware vSphere 6.0.0b
- Microsoft Active Directory
- Smartcard readers

4.1 DOCUMENTATION

The following documents are provided to the consumer to assist in the configuration and installation of the TOE:

a. VMware Horizon 6 Version 6.2.2 Administration Guide, 2016;
b. VMware Horizon 6 Version 6.2.2 Security Guide, 2015;
c. VMware Horizon 6 Version 6.2.2 Horizon Client and View Agent Security Guide, 2015;
d. VMware Horizon 6 Version 6.2.2 Installation Guide, 2016;
e. VMware Horizon 6 Version 6.2.2 Architecture and Planning Guide, 2015;
f. Using VMware Horizon Client for Windows 3.5.2, March 2016;
g. Release Notes for VMware Horizon 6 version 6.2.2, September 2015;
h. Reviewer's Guide for View in Horizon 6; and

i. Operational User Guidance and Preparative Procedures for VMware Horizon 6 v0.2.

5 EVALUATION ANALYSIS ACTIVITIES

The evaluation analysis activities involved a structured evaluation of the TOE. Documentation and process dealing with Development, Guidance Documents, and Life-Cycle Support were evaluated.

5.1 DEVELOPMENT

The evaluators analyzed the TOE functional specification and design documentation; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces, the TSF subsystems and how the TSF implements the security functional requirements (SFRs). The evaluators analyzed the TOE security architectural description and determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained. The evaluators also independently verified that the correspondence mappings between the design documents are correct.

5.2 GUIDANCE DOCUMENTS

The evaluators examined the TOE preparative user guidance and operational user guidance and determined that it sufficiently and unambiguously describes how to securely transform the TOE into its evaluated configuration and how to use and administer the product. The evaluators examined and tested the preparative and operational guidance, and determined that they are complete and sufficiently detailed to result in a secure configuration.

Section 4.1 provides details on the guidance documents.

5.3 LIFE-CYCLE SUPPORT

An analysis of the TOE configuration management system and associated documentation was performed. The evaluators found that the TOE configuration items were clearly marked.

The evaluators examined the delivery documentation and determined that it described all of the procedures required to maintain the integrity of the TOE during distribution to the consumer.

The evaluators reviewed the flaw remediation procedures used by developer for the TOE. During a site visit, the evaluators also examined the evidence generated by adherence to the procedures. The evaluators concluded that the procedures are adequate to track and correct security flaws, and distribute flaw information and corrections to consumers of the TOE.

6 TESTING ACTIVITIES

Testing consists of the following three steps: assessing developer tests, performing independent functional tests, and performing penetration tests.

6.1 ASSESSMENT OF DEVELOPER TESTS

The evaluators verified that the developer has met their testing responsibilities by examining their test evidence, and reviewing their test results, as documented in the ETR.

The evaluators analyzed the developer's test coverage analysis and found it to be complete and accurate. The correspondence between the tests identified in the developer's test documentation and the functional specification was complete.

6.2 CONDUCT OF TESTING

The TOE was subjected to a comprehensive suite of formally documented, independent functional and penetration tests. The detailed testing activities, including configurations, procedures, test cases, expected results and observed results are documented in a separate Test Results document.

6.3 INDEPENDENT FUNCTIONAL TESTING

During this evaluation, the evaluator developed independent functional tests by examining design and guidance documentation.

All testing was planned and documented to a sufficient level of detail to allow repeatability of the testing procedures and results. The following testing activities were performed:

a. Repeat of Developer's Tests: The evaluator repeated a subset of the developers tests;

b. Smart Card: The objective of this test is to demonstrate that by requiring smartcard only authentication, password authentication will not be successful;

c. Session Timeout: The objective of this test is to demonstrate varying timeout periods on the TOE; and

d. Cryptographic Module Verification: The objective of this test is to identify the cryptographic modules and their software versions implemented in the TOE.

6.3.1 FUNCTIONAL TEST RESULTS

The developer's tests and the independent functional tests yielded the expected results, providing assurance that the TOE behaves as specified in its ST and functional specification.

6.4 INDEPENDENT PENETRATION TESTING

Subsequent to the independent review of public domain vulnerability databases and all evaluation deliverables, limited independent evaluator penetration testing was conducted. The penetration tests focused on:

a. Use of automated vulnerability scanning tools to discover potential network, platform and application layer vulnerabilities such as Heartbleed, Shellshock, FREAK, POODLE, and GHOST.

6.4.1 PENETRATION TEST RESULTS

The independent penetration testing did not uncover any exploitable vulnerabilities in the intended operating environment.

7 RESULTS OF THE EVALUATION

This evaluation has provided the basis for the conformance claim documented in Table 1. The overall verdict for the evaluation is **PASS**. These results are supported by evidence in the ETR.

The IT product identified in this report has been evaluated at an approved evaluation facility established under the Canadian Common Criteria Scheme using the Common Methodology for IT Security Evaluation, Version 3.1 Revision 4, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 4. These evaluation results apply only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete certification report.

The evaluation has been conducted in accordance with the provisions of the Canadian Common Criteria Scheme and the conclusions of the evaluation facility in the evaluation report are consistent with the evidence adduced. This is not an endorsement of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by CSE or by any other organization that recognizes or gives effect to this certificate, is expressed or implied.

8 SUPPORTING CONTENT

8.1 LIST OF ABBREVIATIONS

Term	Definition
CAVP	Cryptographic Algorithm Validation Program
CCEF	Common Criteria Evaluation Facility
CM	Configuration Management
CMVP	Cryptographic Module Validation Program
CSE	Communications Security Establishment
DBMS	Database Management System
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GC	Government of Canada
IPsec	Internet Protocol Security
IT	Information Technology
ITS	Information Technology Security
ITSET	Information Technology Security Evaluation and Testing
PALCAN	Program for the Accreditation of Laboratories – Canada
PP	Protection Profile
SFR	Security Functional Requirement
SP	Service Pack
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
VM	Virtual Machine

8.2 REFERENCES

Reference
CCS Publication #4, Technical Oversight, Version 1.8, October 2010.
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, September 2012.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 4, September 2012.
VMware Horizon 6 Security Target, Version 0.8, August 11, 2016.
Evaluation Technical Report for VMware Horizon 6 Version 6.2.2 and Horizon Client Version 3.5.2, Version 0.8, 12 August 2016.