Communications Security Establishment
Centre de la sécurité des télécommunications

COMMON CRITERIA CERTIFICATION REPORT

Citrix XenDesktop 7.15 LTSR Platinum Edition and Citrix XenApp 7.15 LTSR Platinum Edition

30 January 2018

383-4-433

v1.0

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 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5. 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.

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

Citrix XenDesktop 7.15 LTSR Platinum Edition and Citrix XenApp 7.15 LTSR Platinum Edition (hereafter referred to as the Target of Evaluation, or TOE), from Citrix Systems, Inc., was the subject of this Common Criteria evaluation. A description of the TOE can be found in Section 1.2. The results of this evaluation demonstrate that TOE meets the requirements of the conformance claim listed in Table 1 for the evaluated security functionality.

DXC Security Testing/Certification Laboratories is the CCEF that conducted the evaluation. This evaluation was completed 30 January 2018 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 Canadian 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	Citrix XenDesktop 7.15 LTSR Platinum Edition and Citrix XenApp 7.15 LTSR Platinum Edition
Developer	Citrix Systems, 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 5, for conformance to the Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5.

1.2 TOE DESCRIPTION

The TOE is a virtualisation product that centralises and delivers Microsoft Windows virtual desktops and/or applications as a service to users anywhere. Applications hosted on Microsoft Windows Server 2016 and personalised virtual desktops hosted on Microsoft Windows 10 can be run on demand each time they log on.

When used in the full XenDesktop configuration, the TOE gives access to both virtual desktops and published applications. When used in the XenApp configuration, the TOE gives access only to published applications.

1.3 TOE ARCHITECTURE

A diagram of the TOE architecture is as follows:

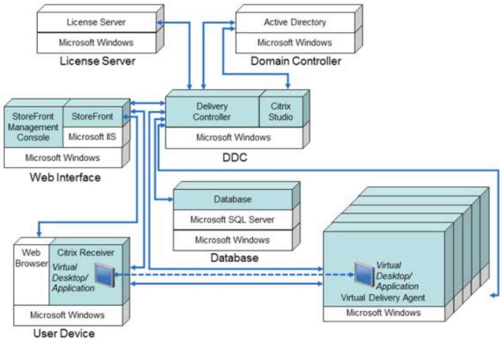


Figure 1 TOE Architecture

2 SECURITY POLICY

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

- User Data Protection
- Identification and Authentication
- Security Management
- Trusted Path/Channels

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

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 TOE servers are installed in a physically secure location that can only be accessed by authorised administrators.
- The Endpoint operating system is securely configured, including appropriate file protection. In particular, a non-administrative user should not have access to facilities to edit the User Device registry.
- Data (including keys) generated, processed, and stored outside the TOE is managed in accordance with the level of risk. This includes the application of appropriate controls to prevent the use of cameras and smart phones to photograph screens, and disabling screen capture and print screen functions on endpoints if required by the TOE customer.
- The VM Host software provides virtual machine isolation and is operating correctly and securely.
- Trusted third-party software is operating correctly and securely. This shall include administrators ensuring that applications are published and configured such that it is not possible for users to gain access to the underlying operating system or hardware on which the Virtual Delivery Agent is running, other than in the context of an unprivileged user account, or other applications. The security state of the published applications should also be maintained according to the user’s risk environment (e.g. by applying relevant patches).

3.2 CLARIFICATION OF SCOPE

The Citrix XenServer hypervisor was used in the environment for testing, but is not part of the TOE and is therefore not included in this evaluation. The following Citrix components should not be installed and are therefore not evaluated:

- Citrix NetScaler Gateway – offers secure remote access, not used in the evaluated configuration;
- Citrix Provisioning Services – optimises provisioning of virtual desktops, not used in the evaluated configuration;
- Citrix Profile Management – high performance user personalisation method, not used in the evaluated configuration;
- Citrix NetScaler SD-WAN – accelerator for improved performance on wide area networks, not used in the evaluated configuration;
- Citrix Desktop Director – provides the help desk with a single console to monitor, troubleshoot and fix virtual desktops, not used in the evaluated configuration;

- Citrix XenMobile – a comprehensive solution to manage mobile devices, apps and data, and allowing users to access all of their mobile, SaaS and Windows apps from a unified corporate app store, not used in the evaluated configuration;
- Citrix AppDNA - reduces the time, cost and risk for OS migration and virtualization technology adoptions by automating application compatibility and overall application migration, not used in the evaluated configuration.

The following features of XenDesktop and XenApp are disallowed in the evaluated configuration and are therefore not evaluated:

- Application delivery methods other than XenApp published apps, also known as server-based hosted applications;
- Desktop delivery methods other than VDI (Virtual Desktop Infrastructure) desktops;
- Desktop delivery groups of the random type;
- The capability for users to belong to multiple desktop delivery groups;
- The capability for desktop users to be assigned multiple desktops in a desktop delivery group;
- The capability for users to belong to multiple application delivery groups;
- Delegated administrator roles other than full administrators;
- Control of local peripheral support using individual and group policy (only global policy is used);
- The ability for administrators to automatically create virtual desktops and servers using Machine Creation Services;
- Power management of virtual machines via the Delivery Controller;
- The use of multiple Delivery Controllers;
- Connection leasing and use of Zones with Local Host Cache;
- Disconnected sessions;
- Non-brokered sessions;
- Streaming applications using AppV;
- The ability for administrators to deploy Personal vDisks for users and deliver applications using AppV and AppDisks;
- The ability for users to access their personal office PC remotely from Citrix Receiver using the Remote PC Access feature;
- The recording, archiving and playback of the on-screen activity of a user session hosted on a Server or Desktop VDA using the Session Recording feature; and,
- Use of the Federated Authentication Service to support SAML-based logon to StoreFront, and the use of unauthenticated (anonymous) delivery groups and StoreFront stores.
- Any VM Host used to provide virtual desktops or published applications is outside the scope of the TOE

4 EVALUATED CONFIGURATION

The evaluated configuration for the TOE comprises:

StoreFront (including StoreFront Management Console) 3.12.0.17, on a server with the following software:

- Microsoft Windows Server 2016, Standard Edition
- Microsoft .NET Framework 4.6
- Microsoft Internet Information Server (IIS) 10.0
- Microsoft ASP.NET 4.6
- Citrix License Server 11.14.

Delivery Controller 7.15.0.15097 & Citrix Studio 7.15.0.93, a server is required with the following software:

- Microsoft Windows Server 2016, Standard Edition
- Microsoft .NET Framework 4.6
- Citrix XenServer 7.1 LTSR (Long Term Service Release)

The Delivery Controller requires a Database with the following software:

- Microsoft SQL Server 2016
- Microsoft Windows Server 2016, Standard Edition.

Each Desktop Virtual Delivery Agent (Virtual Delivery Agent 7.15.0.15097) will require the following software (used in XenDesktop only):

- Citrix Receiver 4.9.0.2539 with Online Plug-in 14.9.0.2539
- Microsoft Windows 10 Enterprise, 64-bit.
- Microsoft Internet Explorer version 11.

Each Server Virtual Delivery Agent (Virtual Delivery Agent 7.15.0.15097) for the virtual applications will require the following software:

- Microsoft Windows Server 2016, Standard Edition.

Access to the domain controller is required, which will be a Microsoft server in the environment running:

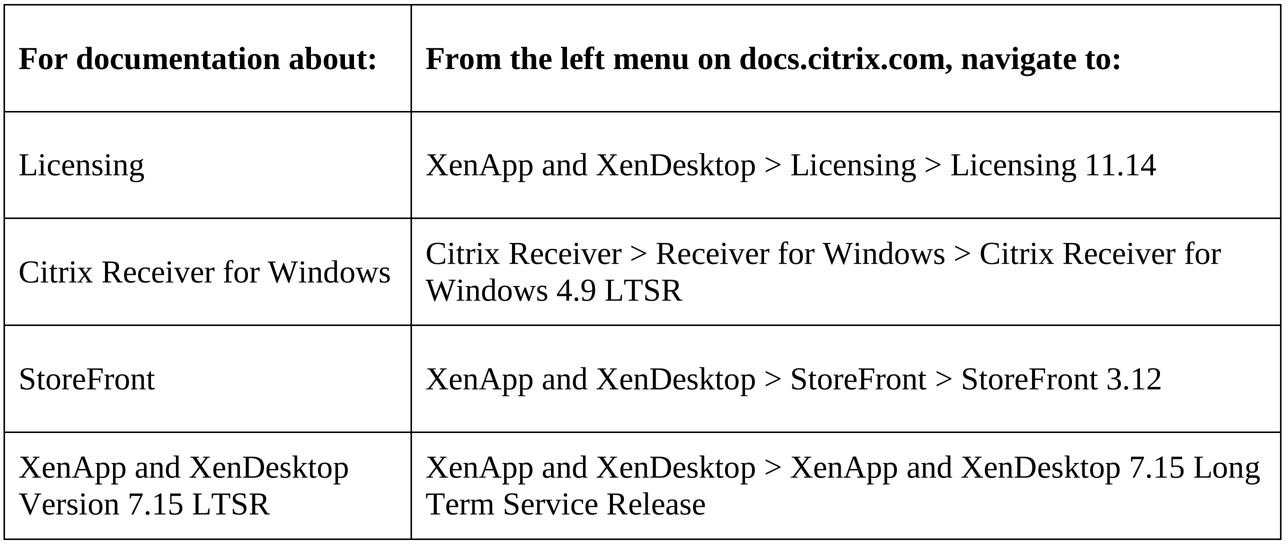
- Microsoft Active Directory Server in Windows Server 2016 native mode.

4.1 DOCUMENTATION

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

a. Common Criteria Evaluated Configuration Guide for Citrix XenDesktop 7.15 LTSR Platinum Edition and Citrix XenApp 7.15 LTSR Platinum Edition, 11 January 2018

b. Citrix product documentation is provided at https://docs.citrix.com/



For documentation about:	From the left menu on docs.citrix.com, navigate to:
Licensing	XenApp and XenDesktop > Licensing > Licensing 11.14
Citrix Receiver for Windows	Citrix Receiver > Receiver for Windows > Citrix Receiver for Windows 4.9 LTSR
StoreFront	XenApp and XenDesktop > StoreFront > StoreFront 3.12
XenApp and XenDesktop Version 7.15 LTSR	XenApp and XenDesktop > XenApp and XenDesktop 7.15 Long Term Service Release

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 documentation provided by the vendor; they determined that the design completely and accurately describes the TOE security functionality (TSF) interfaces and how the TSF implements the security functional requirements (SFRs). The evaluators determined that the initialization process is secure, that the security functions are protected against tamper and bypass, and that security domains are maintained.

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.

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 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. Restrictions on access and User Identification: The evaluator tested the ability of identify users and restrict access to functionality;

c. Clipboard redirection and double hop: The evaluator confirmed the ability of the TOE to redirect Cut/Paste between virtual desktops/applications; and

d. Secure communications: The evaluator verified that communications between different parts of the TOE are secure.

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; and

b. Predictability of the Xen Authentication: Verify that the authentication token is random and unpredictable; and

c. XenApp jail breaking: Verify if insecure implementation could allow a user to gain privilege beyond what was assigned.

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 this 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 5, for conformance to the Common Criteria for IT Security Evaluation, Version 3.1 Revision 5. 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.

7.1 RECOMMENDATIONS/COMMENTS

It is recommended that all guidance outlined in Section 4.1 be followed to configure the TOE in the evaluated configuration.

Click here to enter text.

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
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GC	Government of Canada
IT	Information Technology
ITS	Information Technology Security
LTSR	Long Term Service Release
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Function
VDI	Virtual Desktop Infrastructure

8.2 REFERENCES

Reference
Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 5, April 2017.
Common Methodology for Information Technology Security Evaluation, CEM, Version 3.1 Revision 5, April 2017.
Citrix XenDesktop 7.15 LTSR Platinum Edition and Citrix XenApp 7.15 LTSR Platinum Edition Security Target, v1.0, 15 January 2018
Citrix XenDesktop 7.15 LTSR Platinum Edition and Citrix XenApp 7.15 LTSR Platinum Edition Evaluation Technical Report v1.1, 30 January 2018