Virtual Apps and Desktops 7 2203 LTSR Premium Edition

Security Target

Version 1.2

April 2022

Document prepared by

www.lightshipsec.com

Document History

Version	Date	Author	Description
1.2	25 Apr 2022	G Nickel	Release for certification

Table of Contents

1 Introduction 5

1.1 Overview 5
1.2 Identification 5
1.3 Conformance Claims 5
1.4 Terminology 5

2 TOE Description 9

2.1 Type 9
2.2 Usage 9
2.3 Security Functions 10
2.4 Physical Scope 11
2.5 Logical Scope 12

3 Security Problem Definition 14

3.1 Threats 14
3.2 Assumptions 14
3.3 Organizational Security Policies 15

4 Security Objectives 16

4.1 Objectives for the Operational Environment 16
4.2 Objectives for the TOE 17

5 Security Requirements 19

5.1 Conventions 19
5.2 Extended Components Definition 19
5.3 Functional Requirements 19
5.4 Assurance Requirements 25

6 TOE Summary Specification 26

6.1 Administrator access control 26
6.2 Administration of virtual desktop and published application authorisation 26
6.3 Desktop user and Application user access control 26
6.4 User Device resource access control 27
6.5 Secure communications 27

7 Rationale 28

7.1 Security Objectives Rationale 28
7.2 Security Requirements Rationale 33
7.3 TOE Summary Specification Rationale 38

List of Tables

Table 1: Evaluation identifiers 5
Table 2: Glossary 5
Table 3: Acronyms 7
Table 4: Threats 14
Table 5: Assumptions 14
Table 6: Organizational Security Policies 15
Table 7: Security Objectives for the Operational Environment 16
Table 8: Security Objectives 17
Table 9: Summary of SFRs 19
Table 10: Assurance Requirements 25
Table 11: Security Objectives Mapping 28

Table 12: Suitability of Security Objectives 29
Table 13: Security Requirements Mapping 33
Table 14: Suitability of SFRs 34
Table 15: SFR Dependencies Analysis 36
Table 16: Map of SFRs to TSS Security Functions 38

1 Introduction

1.1 Overview

1 This Security Target (ST) defines the Citrix Virtual Apps and Desktops 7 2203 LTSR Premium Edition Target of Evaluation (TOE) for the purposes of Common Criteria (CC) evaluation.

2 Citrix Virtual Apps and Desktops are virtualization solutions that give organizations control of virtual machines, applications, licensing, and security, while providing anywhere access for any device.

1.2 Identification

Table 1: Evaluation identifiers

Target of Evaluation	Citrix Virtual Apps and Desktops 7 2203 LTSR Premium Edition Build: 2203.0.0.33220
Security Target	Citrix Virtual Apps and Desktops 7 2203 LTSR Premium Edition Security Target, v1.2

1.3 Conformance Claims

3 This ST supports the following conformance claims:

a) CC version 3.1 Release 5

b) CC Part 2 conformant

c) CC Part 3 conformant

d) Evaluation Assurance Level (EAL) 2 augmented by ALC_FLR.2

1.4 Terminology

Table 2: Glossary

Term	Definition
Access permissions for virtual desktops	Configuration data within the TOE which determines which virtual desktops each user is permitted to access.
Access permissions for (published) applications	Configuration data within the TOE which determines which published applications each user is permitted to access Permitted Published Applications.
Catalog	A collection of machines of the same Machine Type. Catalogs are managed as a single entity. Desktops or servers from more than one catalog can be allocated to a delivery group.
Configdata	Configuration data within the TOE; which includes access permissions for virtual desktops and published applcations,

Term	Definition
	Virtual Desktop configuration data and Endpoint data access control policy. See section 3.1.
Delivery Group	An administrative grouping of machines to supply desktops and/or applications that are allocated to users or groups of users. Machines from one or more catalogs are used to create the delivery group. Users can be given permissions to access one or more delivery groups, but in the evaluated configuration each user is given access to only a single desktop delivery group and a single application delivery group.
Domain pass-through	A means of authentication in which single sign-on is provided using the domain credentials used to log on to a domain-joined client running Citrix Worskpace App.
Endpoint data access control policy	A set of rules, configured within the TOE, which determine whether or not a user can access User Device resources from within a virtual desktop or published application: specifically clipboard, local drives, USB devices; used in conjunction with input evidence values to determine specific settings for any particular virtual desktop.
ICA File	A file used with the Independent Computing Architecture, which contains configuration information enabling a client to connect to a server.
Independent Computing Architecture	A presentation services protocol, used to present input (keystrokes, mouse clicks etc.) To the virtual desktop and published applications for processing and to return output (display, audio etc.) To the citrix receiver running on the client.
License Server	A server that issues licenses for Citrix products.
Machine Type	Defines the machine type (desktop or server OS) as well as a number of other properties relating to how machines in a catalog are provisioned, allocated and managed.
Permitted Published Applications	The set of published applications to which an authorised User has been granted access.
Provisioning	Act of creating new virtual desktops and/or published applications, including the operating system image for the desktops and related configuration.
Published Applications	The applications that administrators can configure to be accessible by authorised Users. The definition also includes data and resources associated with a given application (e.g. Data defining the initial configuration or appearance of an application). Different authorised Users may have access to different sets of applications (see Permitted Published Applications).

Term	Definition
Site	A collection of Catalogs, Delivery Groups, Published Applications, virtual desktops and Configdata that are defined, managed and accessed via the same Delivery Controller, and which are stored within a common, shared database. In the evaluated configuration, there will only be a single application delivery group and a single desktop delivery group defined in the site.
StoreFront	A server that provides a user with an interface to a self-service store which allows them to subscribe to and launch their chosen apps and desktops following authentication.

Table 3: Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
CC	Common Criteria
DDC	Delivery Controller (the leading 'D' is present for historical reasons and to avoid potential confusion with 'Domain Controller')
EAL	Evaluation Assurance Level
ICA	Independent Computing Architecture
LAN	Local Area Network
OSP	Organisational Security Policy
PP	Protection Profile
SAR	Security Assurance Requirement
SFP	Security Function Policy
SFR	Security Functional Requirement
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
VDA	Virtual Delivery Agent

Acronym	Definition
WCF	Windows Communication Foundation

2 TOE Description

2.1 Type

4 The TOE is a desktop and application virtualization software solution.

2.2 Usage

5 The TOE 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. This ensures that performance never degrades, while the high-speed delivery protocol provides unparalleled responsiveness over any network. The TOE delivers a high definition user experience over any connection, including high latency wide area networks.

6 When used in the Desktop configuration, the TOE gives access to both virtual desktops and published applications. When used in the App configuration, the TOE gives access only to published applications.

7 Although the desktops and applications are virtual, running on remote servers, the user experience is equivalent to that of a local Windows desktop. From the user's perspective, logging on to a virtual desktop is the same as logging on to a local desktop. Users enter their credentials once and are connected to their desktops and applications.

8 Citrix Virtual Apps and Desktops core components are shown in Figure 1.

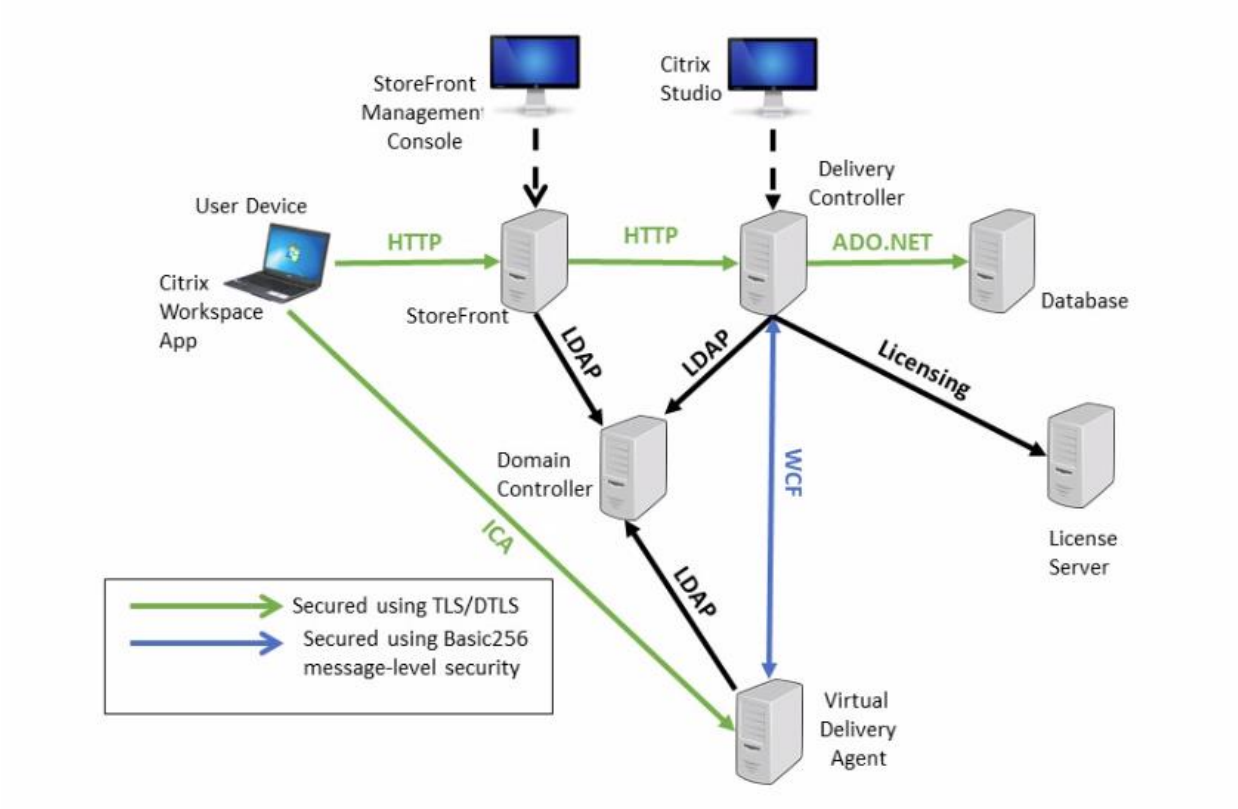

Figure 1: Citrix Virtual Apps and Desktops components

2.2.1 Core components

9 The core components of Citrix Virtual Apps and Desktops (illustrated in Figure 1) are:

a) **StoreFront Management Console**. Provides an administration interface to StoreFront, making use of Windows authentication for administrators. It provides administrators with functions to manage the configuration of StoreFront, including setting the user authentication method. This is installed on the StoreFront server.

b) **Citrix Studio**. Provides an administration interface to the Delivery Controller, making use of Windows authentication for administrators. It provides administrators with a number of functions, to manage the configuration of virtual desktops and applications, manage users' access permissions for virtual desktops and applications and to manage the Endpoint data access control policy. This is installed on the Delivery Controller.

c) **Citrix Workspace App**. Installed on user devices, the Citrix Workspace App enables direct ICA connections from user devices to virtual desktops and published applications.

d) **StoreFront**. Installed on a server in the data centre, StoreFront is used to give authorised users access through the Web or intranet to the virtual desktops and applications that they are authorised to use. Users log on to StoreFront using an Internet browser and are given the ICA file that the Citrix Workspace App needs to connect to the Windows Virtual Delivery Agent for Single-session OS for access to an authorised virtual desktop or application. StoreFront is also accessed from an Internet browser running within the virtual desktop to launch virtual applications the user is authorised to access.

e) **Delivery Controller**. Installed on servers in the data centre, the brokers connections between users and their virtual desktops and applications.

f) **Database**. Stores the Config data managed by the administrators with the Citrix Studio, including the Endpoint data access control policy, configuration of virtual desktops, desktop users' access permissions for virtual desktops, lists of permitted published applications, and access permissions for administrators, as well as data used by the Delivery Controller to manage virtual desktops, users and sessions.

g) **Windows VDA for Single-Session OS and Windows VDA for Multi-Session OS**. Installed on virtual desktops and servers hosting published applications, the agent enables direct ICA (Independent Computing Architecture) connections between the virtual desktop and servers hosting published applications and the end user's User Device.

10 The Domain Controller and License Server are outside of the TOE.

11 The product configuration in this ST is an internal deployment with no external access: the clients and servers are expected to be running within a LAN.

2.3 Security Functions

12 The TOE provides the following security functions:

a) **Authentication of desktop and application users.** The TOE requires users to be authenticated before granting them access to virtual desktops and/or applications. Once authenticated, users are provided with a reliable connection to a virtual desktop that incorporates their personal settings (for Citrix Virtual Desktop only), and access to their permitted published applications, regardless of the User Device or location.

b) **Authenticated administrators.** Only authenticated administrators can use the access management facilities.

c) **Access Management.** Administrators can assign users to virtual desktops and published applications and manage the connections to the virtual desktops and published

applications. Provisioning new users is simply a matter of creating an Active Directory user account and associating the account with a dedicated desktop image and/or set of permitted published applications.

d) **Control over use of User Device resources.** Centralised control policies, set by administrators, determine whether users can access local User Device resources such as the clipboard, local drives, or USB devices, from their virtual desktop and applications.

e) **Secure communications.** High performance, standards-based encrypted transmissions are used for communications between server components, and between User Device and server components.

2.4 Physical Scope

13 The physical boundary of the TOE encompasses the Citrix Virtual Apps and Desktops 7 2203 LTSR Premium Edition server and client software components. Customers download the TOE software from https://www.citrix.com

14 The TOE Server software components:

a) Delivery Controller (includes the Database) 2203.0.0.33220

b) Studio 7.33.0.70

c) StoreFront (includes the StoreFront Management Console) 2203.0.0.36

d) Virtual Delivery Agent 22.03.0.16

15 The TOE Client software component:

a) Citrix Workspace App for Windows 2203.1 (Build: 22.3.1.41)

2.4.1 Guidance Documents

16 The TOE includes the following guidance documents (PDF):

a) Common Criteria Evaluated Configuration Guide for Citrix Virtual Apps and Desktops 7 2203 LTSR Premium Edition [CCECG], April 2022 https://www.citrix.com/about/legal/security-compliance/common-criteria.html

b) Citrix Virtual Apps and Desktops 7 2203 LTSR Premium Edition, Citrix Product Documentation, 14 April 2022 https://docs.citrix.com/en-us/citrix-virtual-apps-desktops/citrix-virtual-apps-and-desktops-7-2203-ltsr.pdf

2.4.2 Non-TOE Components

17 The TOE operates with the following components in the environment:

a) For Citrix StoreFront including the StoreFront Management Console, a server is required with the following software:

i) Microsoft Windows Server 2019, Standard Edition

ii) Microsoft .NET Framework 4.7.2

iii) Microsoft Internet Information Server (IIS) 10.0

iv) Microsoft ASP.NET 4.7.2

b) Citrix License Licensing 11.17.2.0 build 37000

c) For the Delivery Controller including Citrix Studio, a server is required with the following software:

   i) Microsoft Windows Server 2019, Standard Edition

   ii) Microsoft .NET Framework 4.8

d) The Delivery Controller requires a Database with the following software:

   i) Microsoft SQL Server 2017

   ii) Microsoft Windows Server 2019, Standard Edition.

e) A User Device will be a PC with the following software:

   i) Microsoft Windows 10 Enterprise, 64-bit only.

   ii) Microsoft Internet Explorer version 11.

f) Each Desktop VDA for the virtual desktop will require the following software (used in Citrix Virtual Desktop only):

   i) Microsoft Windows 10 Enterprise (x64 only)

   ii) Microsoft Internet Explorer version 11.

g) Each Server VDA for the virtual applications will require the following software:

   i) Microsoft Windows Server 2019, Standard Edition.

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

   i) Microsoft Active Directory Server in Windows Server 2016 native mode.

18 If multi-factor authentication (MFA), such as smart cards, is required, appropriate readers and drivers are required on endpoints, and appropriate middleware is required to integrate the multi-factor authentication with the domain controller. The TOE relies on the operational environment to provide user authentication. This may take the form of passwords or supported multi-factor authentication, including smart cards, depending on the customer's environment and requirements.

19 The TOE also requires the use of a hypervisor on the Delivery Controller, creating and maintaining a virtual machine for each virtual desktop. The only requirement placed on the hypervisor by this Security Target is that the selected hypervisor should meet A.VM_HOST and OE.CONFIG_VM_HOST.

2.5 Logical Scope

20 The logical scope of the TOE comprises the security functions identified at section 2.3.

2.5.1 Features and functions not evaluated

21 The following Citrix components should not be installed and have not been evaluated:

a) **Citrix Gateway.** Offers secure remote access, not used in the evaluated configuration.

b) **Citrix Provisioning Services.** Optimises provisioning of virtual desktops, not used in the evaluated configuration.

c) **Citrix Profile Management.** High-performance user personalisation method, not used in the evaluated configuration.

d) **Citrix SD-WAN**. Accelerator for improved performance on wide area networks, not used in the evaluated configuration.

e) **Citrix Desktop Director.** Provides the help desk with a single console to monitor, troubleshoot and fix virtual desktops, not used in the evaluated configuration.

f) **Citrix Endpoint Management.** 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.

22 The following features of Citrix Virtual Apps and Desktops are disabled in the evaluated configuration and have not been evaluated:

a) Application delivery methods other than Citrix Endpoint Management published apps, also known as server-based hosted applications;

b) Desktop delivery methods other than VDI desktops;

c) Desktop delivery groups of the random type;

d) The capability for users to belong to multiple desktop delivery groups;

e) The capability for desktop users to be assigned multiple desktops in a desktop delivery group;

f) The capability for users to belong to multiple application delivery groups;

g) Delegated administrator roles other than full administrators;

h) Control of local peripheral support using individual and group policy (only global policy is used);

i) The ability for administrators to automatically create virtual desktops and servers using Machine Creation Services;

j) Power management of virtual machines via the Delivery Controller;

k) The use of multiple Delivery Controllers;

l) Connection leasing and use of Zones with Local Host Cache;

m) Disconnected sessions;

n) Non-brokered sessions;

o) Streaming applications using AppV;

p) The ability for administrators to deploy Personal vDisks for users and deliver applications using AppV and AppDisks;

q) The ability for users to access their personal office PC remotely from Citrix Receiver using the Remote PC Access feature;

r) 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,

s) Use of the Federated Authentication Service to support SAML-based logon to StoreFront, and the use of unauthenticated (anonymous) delivery groups and StoreFront stores.

23 Any VM Host used to provide virtual desktops or published applications is outside the scope of the TOE (see OE.CONFIG_VM_HOST in section 4.1).

3 Security Problem Definition

3.1 Threats

Table 4: Threats

Identifier	Description
T.ATTACK_ DESKTOPORAPP	An attacker may gain unauthorised access to a virtual desktop or published application.
T.ATTACK_USERDATA	An attacker may gain unauthorised access to user data.
T.ACCESS_ DESKTOPORAPP	A desktop user or application user may gain unauthorised access to a virtual desktop or published application (i.e. to a virtual desktop that is not their own or to a published application that they have not been given permission to access).
T.ACCESS_USERDATA	A desktop user or application user may gain unauthorised access to another user's data.
T.INTERCEPT	An attacker may intercept communication channels. This may lead to compromise of users' authentication credentials, other user data, or Configdata in transit.
T.SPOOF	An attacker may cause communications between a User Device and a server to be redirected, such that users of the TOE may incorrectly believe they are accessing the TOE when they are not. This may lead to compromise of user data or users' authentication credentials.
T.ATTACK_CONFIGDATA	An attacker, application user or desktop user may modify Configdata.

3.2 Assumptions

Table 5: Assumptions

Identifier	Description
A.PHYSICAL	It is assumed that TOE servers are installed in a physically secure location that can only be accessed by authorised administrators.
A.CONFIG_ENDPOINT	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.

Identifier	Description
A.OPERATIONS_ SECURITY	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.
A.VM_HOST	The VM Host software provides virtual machine isolation and is operating correctly and securely.
A.THIRD_PARTY_SW	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).

3.3 Organizational Security Policies

Table 6: Organizational Security Policies

Identifier	Description
P.RESTRICTIONS	The TOE shall prevent the following actions by users when configured to do so by an administrator in order to meet the TOE customer's security requirements: • Cut and paste between a client clipboard and the clipboard in a published application or virtual desktop; • Client drive mapping in a published application or virtual desktop; and, • Access to User Device USB devices from virtual desktops

4 Security Objectives

4.1 Objectives for the Operational Environment

Table 7: Security Objectives for the Operational Environment

Identifier	Description
OE.CONFIG_SERVER	The operating systems of the server components must be securely configured according to [CCECG], including appropriate file protection. This includes ensuring that the contents of the memory used by the Virtual Delivery Agent to run the virtual desktop during a user's session are not available to other processes when that user's session has ended (this is achieved in the evaluated configuration by maintaining the assignment between each virtual desktop and its user, so that the user is always connected to the same persistent desktop).
OE.CONFIG_VM_HOST	VM Host software must be securely configured. The deployment must provision a VM Host that provides suitable virtual machine isolation since this is relied upon to effect separation of user's virtual desktops in the Citrix Virtual Desktop security architecture. The VM Host should therefore be a hypervisor certified against a security target that includes the separation of virtual machines (including virtual memory, virtual disk and networking).
OE.CONFIG_TP_SW	Trusted third-party software must be securely configured according to [CCECG]. Published applications must be configured by administrators 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.
OE.AUTHENTICATE	Users and administrators must be authenticated by the underlying operating system on the relevant platform. Authentication requirements in the operating system shall be configured according to the risks in the operational environment. This includes authentication using the domain controller in the environment and any two-factor authentication used by the TOE customer such as smart cards.
OE.TLS	All communication between the TOE Servers, between Virtual Delivery Agents and User Device Citrix Workspace Apps, and between StoreFront and the User Device (web browser), uses the configured TLS or DTLS protocol. This is provided by the Windows operating system cryptographic modules.

Identifier	Description
OE.ENCRYPTION	Communications between the DDC and VDA are not protected by TLS, but by WCF message-level security. This is provided by the Windows operating system cryptographic module. It uses XML-based WS-Security mechanisms to provide HMAC and encryption for the message contents together with Kerberos-based authentication.
OE.CONFIG_ENDPOINT	The Endpoint operating system must be securely configured according to [CCECG], including appropriate file protection and other security best practices.
OE.OPERATIONS_ SECURITY	Any keys and other secret data that are generated and stored outside the TOE must be managed in accordance with the level of risk.
OE.SERVER_PHYSICAL	The operational environment shall provide physical protection to the TOE servers to ensure only administrators are able to gain physical access to the servers.
OE.ENDPOINT_TP_SW	Endpoints must have only trusted third-party software installed. This software must be configured securely according to the risks in the operational environment.
OE.DATABASE_PROTECT	The operational environment must protect the Configdata database from unauthorized access.

4.2 Objectives for the TOE

Table 8: Security Objectives

Identifier	Description
O.AUTH_USER	Users and administrators must be successfully identified and authenticated before being granted access to the TOE.
O.AUTH_SERVER	TOE server components must authenticate themselves to User Devices and other servers before communication of user data or Configdata.
O.DESKTOP	Each application user and desktop user must be granted access only to the virtual desktop for which they have been authorised.
O.APPLICATION	Each application user and desktop user must be granted access only to applications for which they have been authorised.
O.SECURE_SETUP_DATA	The confidentiality and integrity of user data being processed on the virtual desktop or in a published application must be maintained.

Identifier	Description
O.CONFIG_ACCESS	The virtual desktops and published applications must only be configurable by trusted administrators.
O.ENDPOINT_RESOURCE	An administrator must be able to control the use of client-side resources by authorised application and desktop users. This includes the ability to cut, copy and paste information between a client operating system clipboard and a published application or virtual desktop; access, from a published application or virtual desktop, to local drives on the client; access, from a virtual desktop, to local USB devices on the User Device.

5 Security Requirements

5.1 Conventions

24 This document uses the following font conventions to identify the operations defined by the CC:

a) **Assignment.** Indicated with italicized text.

b) **Refinement.** Indicated with bold text and strikethroughs.

c) **Selection.** Indicated with underlined text.

d) **Assignment within a Selection:** Indicated with italicized and underlined text.

e) **Iteration.** Indicated by adding a string starting with "/" (e.g. "FCS_COP.1/Hash").

5.2 Extended Components Definition

25 There are no extended components defined by this ST.

5.3 Functional Requirements

Table 9: Summary of SFRs

Requirement	Title
FDP_ACC.1/Application	Subset access control
FDP_ACC.1/Desktop	Subset access control
FDP_ACC.1/Resources	Subset access control
FDP_ACF.1/Application	Security attribute-based access control
FDP_ACF.1/Desktop	Security attribute-based access control
FDP_ACF.1/Resources	Security attribute-based access control
FIA_ATD.1/User	User attribute definition
FIA_UID.2/User	User identification before any action
FMT_MSA.1/Application	Management of Security Attributes
FMT_MSA.3/Application	Static attribute initialisation
FMT_MSA.1/Desktop	Management of security attributes
FMT_MSA.3/Desktop	Static attribute initialisation
FMT_MSA.1/Resources	Management of security attributes
FMT_MSA.3/Resources	Static attribute initialisation

Requirement	Title
FMT_SMF.1/Authorise	Specification of management functions
FMT_SMR.1/Authorise	Security management roles
FPT_ITT.1	Basic Internal TSF Data Transfer Protection

5.3.1 User Data Protection (FDP)

FDP_ACC.1/Application Subset access control

FDP_ACC.1.1/Application The TSF shall enforce the [*Application Access Policy*] on [*application users attempting access to a published application*].

FDP_ACC.1/Desktop Subset access control

FDP_ACC.1.1/Desktop The TSF shall enforce the [*Desktop access policy*] on [*desktop users' access to virtual desktops*].

FDP_ACC.1/Resources Subset access control

FDP_ACC.1.1/Resources The TSF shall enforce the [*Resource access policy*] on [*use by application users and desktop users of the following operations:*

- *transfer of user data between the endpoint clipboard and a published application or virtual desktop clipboard;*
- *access to mapped client drives from a published application or virtual desktop; and,*
- *access to endpoint-attached USB devices from a virtual desktop*].

Application note: A USB storage device may be accessed through client drive mapping or through general USB device access (subject to configuration). General USB device access is available from virtual desktops but not from within published applications. Hence within a published application a USB storage device can only be made available using client drive mapping: there is no general USB device access available from within published applications.

FDP_ACF.1/Application Security attribute-based access control

FDP_ACF.1.1/Application The TSF shall enforce the [*Application Access Policy*] to objects based on the following: [

- *subject (user) security attribute: id, group membership*
- *object (application) security attributes: security permissions*].

FDP_ACF.1.2/Application The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [*An application shall be accessible by a user only if security permissions for the delivery group to*

which the application is assigned explicitly grant the user id or the user group the access required.]

FDP_ACF.1.3/Application The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*None*].

FDP_ACF.1.4/Application The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*None*].

FDP_ACF.1/Desktop Security attribute-based access control

FDP_ACF.1.1/Desktop The TSF shall enforce the [Desktop Access Policy] to objects based on the following: [

- *subject (user) security attribute: id*
- *object (desktop) security attribute: security permissions*].

FDP_ACF.1.2/Desktop The TSF shall enforce the following rules to determine if an operation among controlled subjects and objects is allowed: [*Security permissions explicitly grant the user id the access required.*]

FDP_ACF.1.3/Desktop The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*].

FDP_ACF.1.4/Desktop The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*none*].

FDP_ACF.1/Resources Security attribute-based access control

FDP_ACF.1.1/Resources The TSF shall enforce the [*Resource access policy*] to objects based on the following: [

- *subject (user) security attribute: none*
- *object (application or virtual desktop) security attribute: endpoint data access permissions*].

FDP_ACF.1.2/Resources The TSF shall enforce the following rules to determine if an operation among controlled subjects and objects is allowed: [

- *Users shall be permitted to cut and paste data between a published application or a virtual desktop and an endpoint operating system clipboard if the cut and paste function is enabled in the endpoint data access permissions.*
- *Endpoint drives shall be accessible to a published application or a virtual desktop only if the client drive mapping function is enabled in the endpoint data access permissions.*
- *USB devices on an endpoint shall be accessible to a virtual desktop only if the USB device access function is enabled in the endpoint data access permissions*.]

Application note:	Note that that endpoint data access permissions allowed in the evaluated configuration are global and therefore apply to all users. Individual and group permissions are disallowed in the evaluated configuration.
FDP_ACF.1.3/Resources	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [*none*].
FDP_ACF.1.4/Resources	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [*none*].

5.3.2 Identification and Authentication (FIA)

FIA_ATD.1/User **User attribute definition**

FIA_ATD.1.1/User	The TSF shall maintain the following list of security attributes belonging to individual users: [*id, group membership*].

FIA_UID.2/User **User identification before any action**

FIA_UID.2.1/User	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Application note:	The user identification requirement applies to administrators, as well as to application users and desktop users.

5.3.3 Security Management (SMR)

FMT_MSA.1/Application **Management of Security Attributes**

FMT_MSA.1.1/Application The TSF shall enforce the [*Application Access Policy*] to restrict the ability to [modify] the security attributes: [

- *User id*
- *User group,*
- *Security permissions*]

to [*administrators*].

FMT_MSA.3/Application **Static attribute initialisation**

FMT_MSA.3.1/Application	The TSF shall enforce the [*Application Access Policy*] to provide [restrictive] default values for security attributes that are used to enforce the SFP.
Application note:	Administrators are instructed by [CCECG] to always select the correct options to establish a restrictive configuration.
FMT_MSA.3.2/Application	The TSF shall allow the [*administrator*] to specify alternative initial values to override the default values when an object or information is created.

FMT_MSA.1/Desktop **Management of security attributes**

FMT_MSA.1.1/Desktop The TSF shall enforce the [Desktop access policy] to restrict the ability to [modify] the security attributes: [

- *User id*
- *Security permissions*]

to [*administrators*].

FMT_MSA.3/Desktop Static attribute initialisation

FMT_MSA.3.1/Desktop The TSF shall enforce the [*Desktop access policy*] to provide [restrictive] default values for security attributes that are used to enforce the policy.

Application note: Administrators are instructed by [CCECG] to always select the correct options to establish a restrictive configuration.

FMT_MSA.3.2/Desktop The TSF shall allow the [*administrator*] to specify alternative initial values to override the default values when an object or information is created.

Application note: The administrator is required (see [CCECG]) to set the virtual desktop configuration data to assign each virtual desktop to a single user.

FMT_MSA.1/Resources Management of security attributes

FMT_MSA.1.1/Resources The TSF shall enforce the [*Resource access policy*] to restrict the ability to [modify] the security attributes: [

- *endpoint data access permissions*]

to [*administrators*].

FMT_MSA.3/Resources Static attribute initialisation

FMT_MSA.3.1/Resources The TSF shall enforce the [*Resource access policy*] to provide [restrictive] default values for security attributes that are used to enforce the policy.

Application note: The default values are restrictive in that, although the defaults may be configured differently during installation, the cut and paste, client drive mapping and USB device access functions will default to disabled following installation of the evaluation configuration.

FMT_MSA.3.2/Resources The TSF shall allow the [*administrator*] to specify alternative initial values to override the default values when an object or information is created.

FMT_SMF.1/Authorise Specification of management functions

FMT_SMF.1.1/Authorise The TSF shall be capable of performing the following management functions:[

- *Definition of published applications*
- *Administration of access permissions for published applications*

- *Allocation of administrator role to users*
- *Administration of access permissions for virtual desktops*
- *Administration of virtual desktop configuration data*
- *Administration of Endpoint data access control policy.*]

Application note: Administration of virtual desktop configuration data includes assigning each desktop machine to a single desktop user. Administration of the Endpoint data access control policy consists of enabling or disabling the following functions for published applications and virtual desktops:

- cut and paste between a client clipboard and the clipboard in a published application or virtual desktop;
- client drive mapping in a published application or virtual desktop;
- access to User Device USB devices from virtual desktops.

FMT_SMR.1/Authorise Security management roles

FMT_SMR.1.1/Authorise The TSF shall maintain the roles [*desktop user, application user, administrator*].

FMT_SMR.1.2/Authorise The TSF shall be able to associate users with roles.

5.3.4 Protection of the TSF (FPT)

FPT_ITT.1 Basic Internal TSF Data Transfer Protection

FPT_ITT.1 The TSF shall protect TSF data from [*disclosure and modification*] when it is transmitted between separate parts of the TOE**.**

5.4 Assurance Requirements

26 The TOE security assurance requirements are summarized in Table 10 commensurate with EAL2+ (ALC_FLR.2).

Table 10: Assurance Requirements

Assurance Class	Components	Description
Development	ADV_ARC.1	Security Architecture Description
	ADV_FSP.2	Security-enforcing Functional Specification
	ADV_TDS.1	Basic Design
Guidance Documents	AGD_OPE.1	Operational User Guidance
	AGD_PRE.1	Preparative User Guidance
Life Cycle Support	ALC_CMC.2	Use of a CM System
	ALC_CMS.2	Parts of the TOE CM Coverage
	ALC_DEL.1	Delivery Procedures
	ALC_FLR.2	Flaw Reporting procedures
Tests	ATE_COV.1	Evidence of Coverage
	ATE_FUN.1	Functional testing
	ATE_IND.2	Independent Testing - sample
Vulnerability Assessment	AVA_VAN.2	Vulnerability Analysis

6 TOE Summary Specification

6.1 Administrator access control

27 Administrators are authenticated as part of their Windows login via the operating system and domain controller (see OE.AUTHENTICATION). The authenticated identity is used by the Delivery Controller for authorisation before access is provided for administrators to Configdata.

28 These administrator access control mechanisms satisfy the *FIA_UID.2/User* requirement for administrators.

6.2 Administration of virtual desktop and published application authorisation

29 The management of Configdata is performed by an administrator using Citrix Studio, in conjunction with the Delivery Controller which controls access, and the database wherein the Configdata is stored.

30 Only administrators are able to modify Configdata. Configdata includes:

a) Access permissions for administrators, determining whether administrative users can access configdata;

b) Access permissions for virtual desktops, determining which virtual desktops each user can access; applications (i.e. the list of permitted published applications);

c) Virtual Desktop configuration data, determining the configuration and characteristics of each virtual desktop;

d) Endpoint data access policy, defining a central control policy that determines whether or not the user of a virtual desktop can cut and paste data between virtual desktop and User Device clipboards, whether the user is permitted to access local drives from the virtual desktop, and whether the user is permitted to access User Device USB devices from the virtual desktop.

31 These administration mechanisms satisfy the *FMT_SMR.1/Authorise, FMT_SMF.1/Authorise, FMT_MSA.1/Desktop, FMT_MSA.1/Application, FMT_MSA.3/Desktop, FMT_MSA.3/Application, FMT_MSA.1/Resources, and FMT_MSA.3/Resources* security management requirements as well as the *FIA_ATD.1/User* attribute requirement.

6.3 Desktop user and Application user access control

32 StoreFront provides the means for a user to log in to the TOE using a web browser or Citrix Workspace App, in order to gain access to their virtual desktops and permitted published applications. StoreFront receives the user's credentials, which may be username/password or multifactor authentication using a smart card. It forwards the credentials to the Delivery Controller for authentication by the domain controller. Users must be registered with the domain controller and are identified and authenticated as part of their Windows login.

33 The authenticated identity is used by the Delivery Controller for authorisation to ensure that users are only granted access to virtual desktops and published applications for which they have the appropriate permission. Once a user's access permission has been verified, the Delivery Controller assembles the user's virtual desktop or published application environment using the virtual desktop configuration data or access permissions for published applications. The Delivery Controller starts the virtual desktop and generates a ticket which is passed to the Virtual Delivery Agent and, via StoreFront, to the user's Citrix Workspace App.

34 The Citrix Workspace App in the user's User Device uses the ticket to establish a session with the appropriate Virtual Delivery Agent. The Virtual Delivery Agent provides access to the virtual desktop and permitted published applications for the user. It authenticates the user before establishing the session, by confirming that the same ticket has been presented by the Citrix Workspace App as that supplied by the Delivery Controller.

35 Once a user has logged out of a virtual desktop, the virtual desktop and its virtual machine are preserved and available only for that user.

36 These user access control mechanisms satisfy the *FIA_UID.2/User* requirement for users, as well as the desktop and published application access policy requirements (*FDP_ACC.1/Desktop, FDP_ACF.1/Desktop, FDP_ACC.1/Application and FDP_ACF.1/Application*).

6.4 User Device resource access control

37 Desktop users and application users can use User Device resources if an administrator has enabled the appropriate functions in the Endpoint data access control policy. This is enforced by the Citrix Workspace App and the Virtual Delivery Agent. Only global enabling of the functions (i.e. applicable to the entire Site) is included in the scope of the evaluation.

38 The User Device resource access control mechanisms satisfy the resource access policy requirements (*FDP_ACC.1/Resources* and *FDP_ACF.1/Resources*).

6.5 Secure communications

39 Communication between StoreFront and the User Device web browser is protected by TLS or DTLS (depending on environment configuration).

40 Communication between the Virtual Delivery Agent and the Citrix Workspace App in the user's User Device is protected by Windows secure communications mechanisms, which are configured to use TLS/DTLS for authentication, confidentiality and integrity.

41 Communication between the TOE servers is protected by Windows secure communications mechanisms, which are configured to use either TLS/DTLS or Windows message-level security (as shown in Figure 1) for authentication, confidentiality and integrity.

42 The TOE ensures that communications are protected by leveraging two Windows cryptographic modules in the environment. Server-side components of communication channels leverage the kernel mode cryptographic module. Client applications, including the web browser, use the user-mode DLL module.

43 These secure communications mechanisms satisfy the *FPT_ITT.1* requirements for integrity-protected and encrypted communication channels

7 Rationale

7.1 Security Objectives Rationale

44 Table 11 provides a coverage mapping between security objectives, threats, OSPs and assumptions.

Table 11: Security Objectives Mapping

	T.ATTACK_DESKTOPORAPP	T.ATTACK_USERDATA	T.ACCESS_DESKTOPORAPP	T.ACCESS_USERDATA	T.INTERCEPT	T.SPOOF	T.ATTACK_CONFIGDATA	P.RESTRICTIONS	A.PHYSICAL	A.CONFIG_ENDPOINT	A.OPERATIONS_SECURITY	A.VM_HOST	A.THIRD_PARTY_SW
O.AUTH_USER	X	X					X						
O.AUTH_SERVER					X	X							
O.DESKTOP			X	X									
O.APPLICATION			X	X									
O.SECURE_SETUP_DATA			X		X		X						
O.SECURE_USER_DATA		X		X									
O.CONFIG_ACCESS		X	X	X				X					
O.ENDPOINT_RESOURCE				X				X					
OE.CONFIG_SERVER	X	X	X	X		X	X						
OE.CONFIG_VM_HOST	X	X	X	X		X						X	
OE.CONFIG_TP_SW	X	X	X	X		X	X						X
OE.AUTHENTICATE	X	X		X			X						
OE.TLS		X		X	X	X	X						
OE.CONFIG_ENDPOINT	X	X		X		X		X		X			
OE.ENCRYPTION		X		X	X		X						
OE.OPERATIONS_SECURITY											X		

	T.ATTACK_DESKTOPORAPP	T.ATTACK_USERDATA	T.ACCESS_DESKTOPORAPP	T.ACCESS_USERDATA	T.INTERCEPT	T.SPOOF	T.ATTACK_CONFIGDATA	P.RESTRICTIONS	A.PHYSICAL	A.CONFIG_ENDPOINT	A.OPERATIONS_SECURITY	A.VM_HOST	A.THIRD_PARTY_SW
OE.SERVER_PHYSICAL									X				
OE.ENDPOINT_TP_SW						X							X
OE.DATABASE_PROTECT			X				X						

45 Table 12 provides the justification to show that the security objectives are suitable to address the security problem.

Table 12: Suitability of Security Objectives

Element	Justification
T.ATTACK_DESKTOPORAPP	Attackers are prevented from gaining access to a virtual desktop or published application by a combination of TOE and environment objectives to apply identification and authentication. O.AUTH_USER and OE.AUTHENTICATE ensure that only identified and authenticated desktop users, application users and administrators are granted access to the TOE. OE.CONFIG_SERVER ensures that the servers have been set up properly, while OE.CONFIG_VM_HOST and OE.CONFIG_TP_SW ensure that potentially privileged programs do not undermine security. OE.CONFIG_ENDPOINT ensures that the Endpoints have been set up properly and that authentication credentials are not left in the Endpoint memory to be retrieved by an attacker.
T.ATTACK_USERDATA	Attackers are prevented from gaining access to user data by a combination of TOE and environment objectives to apply authentication, authorisation, confidentiality and integrity. O.AUTH_USER and OE.AUTHENTICATE ensure that only identified and authenticated desktop users, application users and administrators are granted access to the TOE. OE.TLS and OE.ENCRYPTION ensure the confidentiality of User data, including authentication credentials, during login and establishment of a virtual desktop and published application session.

Element	Justification
	O.SECURE_USER_DATA ensures the confidentiality and integrity of User data being processed on a virtual desktop or published application. O.CONFIG_ACCESS ensures that the virtual desktops and published applications have been set up properly, while OE.Config_Server ensures that any content of the virtual desktop memory is reserved for that user after the user has logged out of the virtual desktop. OE.CONFIG_SERVER also ensures that the servers have been set up properly, while OE.CONFIG_VM_HOST and OE.CONFIG_TP_SW ensure that potentially privileged programs do not undermine security. OE.CONFIG_ENDPOINT ensures that the Endpoints have been set up properly and that authentication credentials and other User data are not left in the Endpoint memory to be retrieved by an attacker.
T.ACCESS_DESKTOPORAPP	Users are prevented from gaining unauthorised access to a virtual desktop or published application by a combination of TOE and environment objectives to apply authorisation, confidentiality and integrity. O.DESKTOP ensures that a virtual desktop is only available to an desktop user who has been specifically authorised for access to the relevant desktop. O.APPLICATION similarly ensures that a published application is only available to an application user who has been specifically authorised for access to the relevant application (as recorded in the Configdata). OE.DATABASE_PROTECT ensures that only administrators have access to Configdata and thus the ability to authorise users' access to a virtual desktop or published application. O.SECURE_SETUP_DATA ensures the confidentiality and integrity of the setup and assignment data for virtual desktops and published applications on the servers. O.CONFIG_ACCESS ensures that the virtual desktops and published applications have been set up properly. OE.CONFIG_SERVER also ensures that the servers have been set up properly, while OE.CONFIG_VM_HOST and OE.CONFIG_TP_SW ensure that potentially privileged programs do not undermine security.
T.ACCESS_USERDATA	Desktop users and application users are prevented from gaining unauthorised access to another user's User data by a combination of TOE and environment objectives to apply authentication, authorisation, confidentiality and integrity. O.DESKTOP ensures that a virtual desktop is only available to a desktop user authorised to have access. O.APPLICATION similarly ensures that a published application is only available to an application user who has been specifically authorised for access to the relevant application (as recorded in the Configdata).

Element	Justification
	OE.AUTHENTICATE ensures that the underlying operating system performs the required authenticaiton on which to base access decisions. OE.TLS and OE.ENCRYPTION ensure the confidentiality of User data, including authentication credentials, during login and establishment of a virtual desktop or access to a published application. O.SECURE_USER_DATA, ensures the confidentiality and integrity of User data being processed on a virtual desktop or in a published application. O.CONFIG_ACCESS ensures that the virtual desktops and published applications have been set up properly, while OE.CONFIG_SERVER ensures that any content of the virtual desktop memory is reserved for that user after the user has logged out of the virtual desktop. OE.CONFIG_SERVER also ensures that the servers have been set up properly, while OE.CONFIG_VM_HOST and OE.CONFIG_TP_SW ensure that potentially privileged programs do not undermine security. O.ENDPOINT_RESOURCE ensures that users can only use the clipboard and devices attached to the Endpoint when authorised. OE.CONFIG_ENDPOINT ensures that the Endpoints have been set up properly and that authentication credentials and other User data are not available to be used by an attacker.
T.INTERCEPT	Attackers are prevented from intercepting communications channels by a combination of TOE and environment objectives to apply authentication, confidentiality and integrity. O.AUTH_SERVER ensures that servers authenticate themselves to clients and other servers before communicating User data or Configdata. O.SECURE_SETUP_DATA ensures the confidentiality and integrity of the setup and assignment data for the virtual desktop and published applications during transmission between servers. OE.TLS and OE.ENCRYPTION ensure the confidentiality and integrity of communications between the User Device browser and StoreFront during login and establishment of the virtual desktop or access to a published application, and also ensures the confidentiality and integrity of communications between the User Device and the virtual desktop.
T.SPOOF	Attackers are prevented from redirecting communications between a User Device and a server to a spoof server by a combination of TOE and environment objectives to apply authentication, confidentiality and integrity.

Element	Justification
	O.AUTH_SERVER and OE.TLS ensure that servers authenticate themselves to clients before communicating User data such as authentication credentials. OE.CONFIG_SERVER ensures that the servers have been set up properly, while OE.CONFIG_VM_HOST and OE.CONFIG_TP_SW ensure that potentially privileged programs do not undermine security. OE.CONFIG_ENDPOINT and OE.ENDPOINT_TP_SW ensure that the Endpoints have been set up properly.
T.ATTACK_CONFIGDATA	Attackers, application users and desktop users are prevented from modifying Configdata by a combination of TOE and environment objectives to apply authentication, authorisation, confidentiality and integrity. O.AUTH_USER and OE.AUTHENTICATE ensure that only identified and authenticated desktop users, application users and administrators are granted access to the TOE. OE.DATABASE_PROTECT ensures that only administrators have access to Configdata. O.SECURE_SETUP_DATA, OE.TLS and OE.ENCRYPTION ensure the confidentiality and integrity of the Configdata on the servers and when transmitted between servers. OE.CONFIG_SERVER ensures that the servers have been set up properly, while OE.CONFIG_TP_SW ensures that potentially privileged programs do not undermine security.
P.RESTRICTIONS	Restrictions are in place to control whether TOE facilitates moving data between published applications and virtual desktops and the user's endpoint. O.ENDPOINT_RESOURCE ensures that users can only use the clipboard and devices attached to the Endpoint when authorised. This controls cut and paste and moving files between the published desktop or application and the endpoint. O.CONFIG_ACCESS ensures that the virtual desktops and published applications have been set up properly. OE.CONFIG_ENDPOINT ensures that the security of TOE will not be compromised by the security of the endpoint.
A.PHYSICAL	The assumption that TOE servers are installed in physically secure locations is addressed by the environment objective OE.SERVER_PHYSICAL which ensures that servers are physically protected and only accessible by administrators.
A.CONFIG_ENDPOINT	The assumption that User Device operating systems are securely configured with appropriate access permissions is met by the environment objective OE.CONFIG_ENDPOINT which ensures that the Endpoint is securely configured including the file protection.

Element	Justification
A.OPERATIONS_SECURITY	The assumption that secret data outside the TOE is managed appropriately, is met by environment objective OE.OPERATIONS_SECURITY which ensures that keys and other secret data generated and stored outside the TOE are managed in accordance with the level of risk.
A.VM_HOST	The assumption that VM Host software is operating correctly and securely, and uses a hypervisor to provide VM separation, is met by the environment objective OE.CONFIG_VM_HOST, which ensures that these requirements are met.
A.THIRD_PARTY_SW	The assumption that third-party software is operating correctly and securely is met by the environment objectives OE.CONFIG_TP_SW which ensures that trusted third-party software is securely configured, and OE.ENDPOINT_TP_SW which ensures that only securely configured trusted third-party software is installed on the User Devices.

7.2 Security Requirements Rationale

7.2.1 SAR Rationale

46 EAL2 was chosen to provide a level of assurance that is consistent with good commercial practices with the addition of ALC_FLR.2 to provide assurance that any identified security flaws will be addressed.

7.2.2 SFR Rationale

Table 13: Security Requirements Mapping

	O.AUTH_USER	O.AUTH_SERVER	O.DESKTOP	O.APPLICATION	O.SECURE_SETUP_DATA	O.SECURE_USER_DATA	O.CONFIG_ACCESS	O.ENDPOINT_RESOURCE
FDP_ACC.1/Application				X			X	
FDP_ACC.1/Desktop			X				X	
FDP_ACC.1/Resources								X
FDP_ACF.1/Application				X			X	

	O.AUTH_USER	O.AUTH_SERVER	O.DESKTOP	O.APPLICATION	O.SECURE_SETUP_DATA	O.SECURE_USER_DATA	O.CONFIG_ACCESS	O.ENDPOINT_RESOURCE
FDP_ACF.1/Desktop			X				X	
FDP_ACF.1/Resources								X
FIA_ATD.1/User			X	X				
FIA_UID.2/User	X							
FMT_MSA.1/Application				X	X		X	
FMT_MSA.3/Application				X	X		X	
FMT_MSA.1/Desktop			X		X		X	
FMT_MSA.3/Desktop			X		X		X	
FMT_MSA.1/Resources							X	X
FMT_MSA.3/Resources							X	X
FMT_SMF.1/Authorise			X	X	X		X	X
FMT_SMR.1/Authorise			X	X	X		X	X
FPT_ITT.1		X			X	X		

Table 14: Suitability of SFRs

Objectives	SFRs
O.AUTH_USER	This objective is addressed by FIA_UID.2/User which ensures that desktop users and administrators are successfully identified and authenticated before they can use the TOE functionality. (Authentication is provided in the OE by a domain controller.)
O.AUTH_SERVER	This objective is addressed by FPT_ITT.1. This ensures the confidentiality, integrity and authenticity of TOE components for all communications between TOE servers, and between User Devices and TOE servers.

Objectives	SFRs
O.DESKTOP	This objective is addressed by FIA_ATD.1/User, in conjunction with the security management functions (FMT_SMR.1/Authorise, FMT_SMF.1/Authorise, FMT_MSA.1/Desktop, FMT_MSA.3/Desktop) and the Desktop access policy (FDP_ACC.1/Desktop, FDP_ACF.1/Desktop). FIA_ATD.1/User ensures that individual desktop users can be granted access permissions for virtual desktops, while FMT_SMR.1/Authorise, FMT_SMF.1/Authorise, FMT_MSA.1/Desktop and FMT_MSA.3/Desktop ensure that only administrators can manage the desktop users' access permissions. The Desktop access policy (FDP_ACC.1/Desktop and FDP_ACF.1/Desktop) ensures that only desktop users with the correct access permissions can gain access to a virtual desktop.
O.APPLICATION	This objective is addressed by FIA_ATD.1/User, in conjunction with the security management functions (FMT_SMR.1/Authorise, FMT_SMF.1/Authorise, FMT_MSA.1/Application, FMT_MSA.3/Application) and the application access policy (FDP_ACC.1/Application, FDP_ACF.1/Application). FIA_ATD.1/User ensures that application users can be granted access permissions for published applications, while FMT_SMR.1/Authorise, FMT_SMF.1/Authorise, FMT_MSA.1/Application and FMT_MSA.3/Application ensure that only administrators can manage the application users' access permissions. The application access policy (FDP_ACC.1/Application and FDP_ACF.1/Application) ensures that only application users with the correct access permissions can gain access to a published application.
O.SECURE_SETUP_DATA	This objective is addressed by FPT_ITT.1 in conjunction with the security management functions (FMT_SMR.1/Authorise, FMT_SMF.1/Authorise, FMT_MSA.1/Desktop, FMT_MSA.3/Desktop, FMT_MSA.1/Application, FMT_MSA.3/Application). FPT_ITT.1 ensures the confidentiality and integrity of communications between separate TOE servers to protect Configdata, while FMT_SMR.1/Authorise, FMT_SMF.1/Authorise, FMT_MSA.1/Desktop, FMT_MSA.3/Desktop, FMT_MSA.1/Application, and FMT_MSA.3/Application ensure that only administrators can manage Configdata.
O.SECURE_USER_DATA	This objective is addressed by FPT_ITT.1 which ensures the confidentiality and integrity of communications between Citrix Workspace App and the Virtual Delivery Agent, and the confidentiality and integrity of communications between TOE servers.

Objectives	SFRs
O.CONFIG_ACCESS	This objective is addressed by the security management functions (FMT_SMR.1/Authorise, FMT_SMF.1/Authorise, FMT_MSA.1/Desktop, FMT_MSA.3/Desktop (FMT_MSA.1/Application, FMT_MSA.3/Application), the Desktop access policy (FDP_ACC.1/Desktop, FDP_ACF.1/Desktop), the Application access policy (FDP_ACC.1/Application, FDP_ACF.1/Application), and the Resource access policy (FMT_MSA.1/Resources, FMT_MSA.3/Resources). FMT_SMR.1/Authorise, FMT_SMF.1/Authorise, FMT_MSA.1/Desktop, FMT_MSA.3/Desktop, FMT_MSA.1/Application, FMT_MSA.3/Application, FMT_MSA.1/Resources, and FMT_MSA.3/Resources ensure that only administrators can modify or delete virtual desktop and published application configuration data.
O.ENDPOINT_RESOURCE	This objective is addressed by security management functions (FMT_SMR.1/Authorise, FMT_SMF.1/Authorise, FMT_MSA.1/Resources, FMT_MSA.1/Resources, and FMT_MSA.3/Resources) and the Resource access policy (FDP_ACC.1/Resources, FDP_ACF.1/Resources). FMT_SMR.1/Authorise, FMT_SMF.1/Authorise, and FMT_MSA.3/Resources ensure that only authorised administrators can enable or disable cut and paste, client drive mapping, and USB device access functions. The Resource access policy (FDP_ACC.1/Resources and FDP_ACF.1/Resources) ensures that desktop users can only cut and paste data between a virtual desktop and the User Device operating system clipboard if the cut and paste function has been enabled by an administrator. The Resource access policy (FDP_ACC.1/Resources and FDP_ACF.1/Resources) ensures that desktop users can only access User Device client drives from the virtual desktop if the client drive mapping function has been enabled by an administrator and the user has permitted the access. The Resource access policy (FDP_ACC.1/Resources and FDP_ACF.1/Resources) ensures that desktop users can only access USB devices on a User Device from the virtual desktop if the USB device access function has been enabled by an administrator and the user has permitted the access.

Table 15: SFR Dependencies Analysis

SFR	Dependencies	Rationale
FIA_ATD.1/User	None	
FIA_UID.2/User	None	

SFR	Dependencies	Rationale
FMT_SMR.1/Authorise	FIA_UID.1	Met by FIA_UID.2/User
FMT_SMF.1/Authorise	None	
FDP_ACC.1/Desktop	FDP_ACF.1	Met by FDP_ACF.1/Desktop
FDP_ACF.1/Desktop	FDP_ACC.1	Met by FDP_ACC.1/Desktop
	FMT_MSA.3	Met by FMT_MSA.3/Desktop
FMT_MSA.1/Desktop	FDP_ACC.1 or FDP_IFC.1	Met by FDP_ACC.1/Desktop
	FMT_SMR.1	Met by FMT_SMR.1/Authorise
FMT_MSA.3/Desktop	FMT_MSA.1	Met by FMT_MSA.1/Desktop
	FMT_SMR.1	Met by FMT_SMR.1/Authorise
	FMT_SMF.1	Met by FMT_SMF.1/Authorise
FDP_ACC.1/Application	FDP_ACF.1	Met by FDP_ACF.1/Application
FDP_ACF.1/Application	FDP_ACC.1	Met by FDP_ACC.1/Application
	FMT_MSA.3	Met by FMT_MSA.3/Application
FMT_MSA.1/Application	FDP_ACC.1 or FDP_IFC.1	Met by FDP_ACC.1/Application
	FMT_SMR.1	Met by FMT_SMR.1/Authorise
FMT_MSA.3/Application	FMT_MSA.1	Met by FMT_MSA.1/Application
	FMT_SMR.1	Met by FMT_SMR.1/Authorise
	FMT_SMF.1	Met by FMT_SMF.1/Authorise
FDP_ACC.1/Resources	FDP_ACF.1	Met by FDP_ACF.1/Resources
FDP_ACF.1/Resources	FDP_ACC.1	Met by FDP_ACC.1/Resources
	FMT_MSA.3	Met by FMT_MSA.3/ Resources
FMT_MSA.3/Resources	FMT_MSA.1	Met by FMT_MSA.1/Resources
	FMT_SMR.1	Met by FMT_SMR.1/Authorise
	FMT_SMF.1	Met by FMT_SMF.1/Authorise

SFR	Dependencies	Rationale
FPT_ITT.1	None	

7.3 TOE Summary Specification Rationale

47 Table 16 provides a coverage mapping showing that all SFRs are mapped to the security functions described in the TSS.

Table 16: Map of SFRs to TSS Security Functions

	Administrator access control	Administration of virtual desktop and published application authorisation	Desktop user and Application user access control	User Device resource access control	Secure communications
FDP_ACC.1/Application			X		
FDP_ACC.1/Desktop			X		
FDP_ACC.1/Resources				X	
FDP_ACF.1/Application			X		
FDP_ACF.1/Desktop			X		
FDP_ACF.1/Resources				X	
FIA_ATD.1/User		X			
FIA_UID.2/User	X		X		
FMT_MSA.1/Application		X			
FMT_MSA.3/Application		X			
FMT_MSA.1/Desktop		X			
FMT_MSA.3/Desktop		X			
FMT_MSA.1/Resources		X			
FMT_MSA.3/Resources		X			
FMT_SMF.1/Authorise		X			
FMT_SMR.1/Authorise		X			

	Administrator access control	Administration of virtual desktop and published application authorisation	Desktop user and Application user access control	User Device resource access control	Secure communications
FPT_ITT.1					X