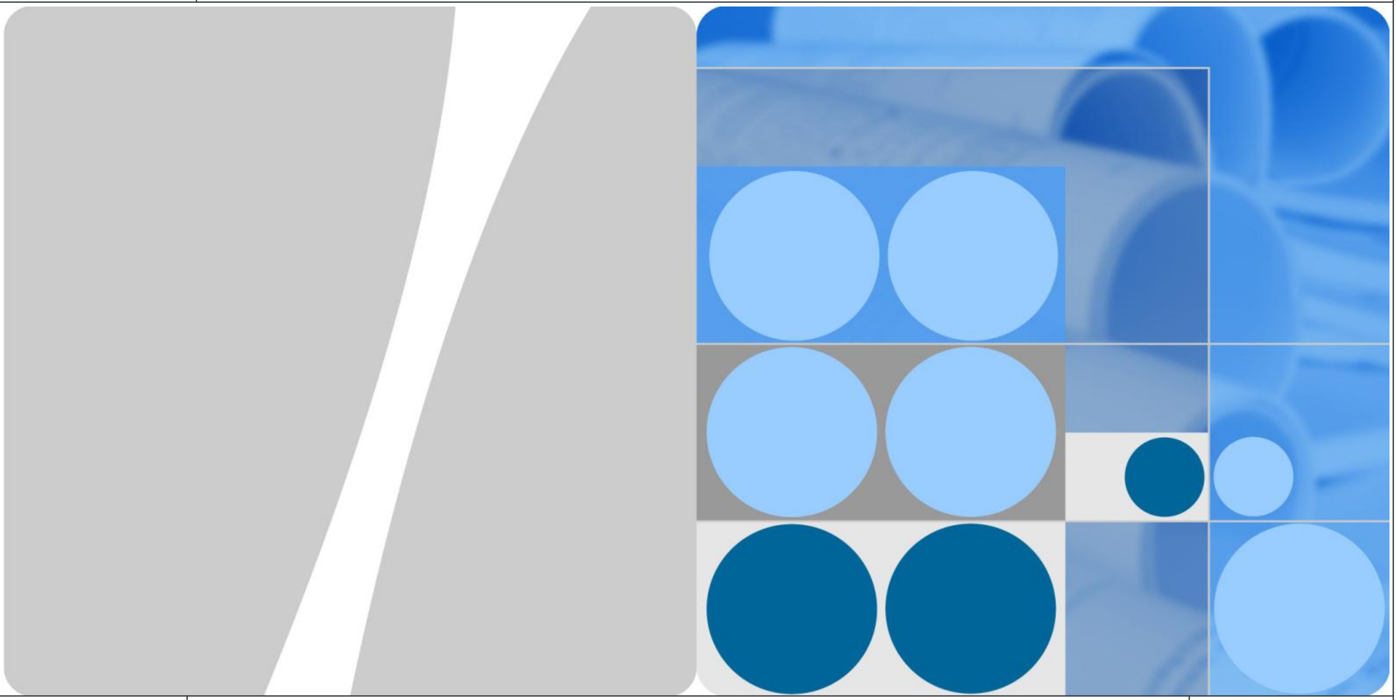

Huawei FusionAccess V100R006C20

Security Target

Issue	1.4
Date	2018-09-27

HUAWEI TECHNOLOGIES CO., LTD.

Huawei Technologies Co., Ltd.

Address:	Huawei Industrial Base Bantian, Longgang Shenzhen 518129 People's Republic of China
Website:	http://e.huawei.com

About This Document

Purpose

This document provides description about ST (Security Target).

Change History

Changes between document issues are cumulative. The latest document issue contains all the changes made in earlier issues.

Date	Revision Version	Section	Change Description	Author
2016-08-15	0.1	All	Initial Draft	Chen Zhen
2016-08-15	0.2	All	update	Yang Ze
2016-08-20	0.3	All	update	Chen Zhen
2016-09-09	0.4	All	update	Zhang Jing
2016-12-23	0.5	All	update	Guochunguang and Cheng Xiaoping
2017-01-06	0.6	All	Updated the format	Cheng Xiaoping
2018-01-31	0.7	All	Updated with lab feedback.	Guochunguang
2018-02-26	0.8	All	Updated with lab feedback.	Guochunguang
2018-06-08	1.2	All	Updated with lab feedback.	Guochunguang

2018-08-28	1.3	All	Updated with lab feedback.	Guochunguang
2018-09-27	1.4	All	Updated with lab feedback	Guochunguang

Contents

List of Tables

List of Figures

1 Introduction

This [CC] Security Target is for the evaluation of the Huawei FusionAccess V100R006C20.

1.1 Security Target Reference

Name:	Huawei FusionAccess V100R006C20 Security Target
Issue:	1.4
Publication Date:	2018-09-27
Author:	Huawei Technologies Co., Ltd.

1.2 TOE Reference

Name:	FusionAccess Software
Version:	V100R006C20

TOE Client:

AccessClient	version V100R006C20

TOE Server:

HDC	version V100R006C20
WI	version V100R006C20
ITA	version V100R006C20
vLB	version V100R006C20
vAG	version V100R006C20

DB	version V100R006C20
License	version V100R006C20
AccessAgent	version V100R006C20

Sponsor: Huawei

Developer: Huawei Technology Co., Ltd

1.3 TOE overview

1.3.1 TOE usage and major security features

The Target of Evaluation (TOE) is a virtualization product that centralise and deliver virtual desktops and applications to end users. End users can access their virtual desktops and applications wherever connection is available.The TOE provides a web portal graphical user interface (GUI) for administrators to quickly provision, maintain, and reclaim virtual desktops and applications. This helps to elastically manage virtual resources, improve resource utilization, and reduce operational expenditure (OPEX).

FusionAccess provides the following key security features:

- Identification and Authentication: Only authenticated local administrators can access management portal to provision, maintain, and reclaim virtual desktops and applications. If authentication is failed, local administrator cannot access the TOE. Only authenticated end users can access AccessClient application and WI web portal to gain access to virtual desktops and published applications assigned by a local administrator. In case of multiple authentication failure in a row the affected account is locked to avoid unauthorized access.

- Security Audit: An operation log records the operations that a local administrator has performed on the system and the result of the operation and is used for tracing and auditing. Only local administrator can review and query the records. Operation logs are stored in such a way that unauthorized modification are prevented.

- User access policy: local administrator can assign virtual desktops and applications to end users. End users only can access to their permitted virtual desktops and applications. Local administrator can set end user access policy to determine whether the end users can access to local device resources such as USB device, the clipboard or local drivers.

- Secure communications: TOE server can be accessed by TLS creating a trusted path between the TOE and the end user.

- Security management: local administrator is able to configure the password policy, the user attributes, set lock timeouts, lock/unlock accounts, end user access control policy, and local resource policy. The TOE is able to manage different user roles.
- TOE Access: The TOE is able to manage the concurrent multiple sessions by limiting the number of active sessions per user. The TOE is also able to terminate an interactive session after an inactivity period of time.

1.3.2 TOE type

Desktop and Application Virtualization Software.

1.3.3 Non-TOE Hardware/Software/Firmware

The list of non-TOE elements is detailed below. They are not part of the TOE, but they are required to the proper TOE operation.

1.3.3.1 OS and Software requirements for TOE components

WI, ITA, HDC, License and vLB/vAG TOE server components run on a:

- SUSE Linux Enterprise Server11 SP3 (64 bits architecture)

ITA and HDC requires access to a Database with the following software:

- Huawei GaussDBV100R003C10

End User device is a PC running on a:

- Microsoft Windows 7 Ultimate (32 bits architecture)

Access Agent for the virtual desktop and virtual Application run on:

- Microsoft Windows Server 2012 R2 Standard (64 bits architecture)
- Microsoft .NET Framework 4.0

Access to the Active Directory Domain Service (AD) is required, it is running on a:

- Microsoft Windows Server 2012 R2 Standard (64 bits architecture)
- Microsoft .NET Framework 4.0

A firewall should be configured in order to create two different and isolated networks: the external one and the internal one.

The external network contains the AccessClient application, meanwhile the internal network contains the rest of the TOE components: ITA, WI, HDC, License, vlB/vAG and AccessAgent. The isolation is guaranteed due to the firewall configuration, which shall be as follows:

- Incoming traffic from the external network to the IPs and ports where the WI web portal and ITA web portal are allocated shall be allowed.
- Communication between the AccessClient application and the vAG/vLB and the VMs shall be allowed.
- Rest of the incoming traffic coming from the external network shall be denied.

1.3.3.2 Software requirements for TOE environment

The TOE also requires the use of Huawei FusionSphere that virtualizes hardware resources so that one physical server can function as multiple virtual machine(VMs). Ensure that the PC, servers, storage devices, and networks meet FusionSphere installation requirements.

Item	Version or specifications
FusionSphere	FusionSphere V100R006C00U1_FusionSphereInstaller.zip
VRM VM template	FusionCompute V100R006C00U1_VRM.zip
FusionCompute host OS	FusionCompute V100R006C00U1_CNA.iso

Table 1: Non-TOE software elements

1.3.3.3 Hardware requirements

Huawei H22H-03 Rack Server with Xenon E5-2690 v3 CPU for TOE server

General Purpose Computer for TOE client

1.4 TOE description

FusionAccess is a virtual desktop and application management system supported by the Huawei FusionSphere. FusionAccess provides a portal graphical user interface for administrators to quickly provision, maintain, and reclaim virtual desktops and applications. End users can access virtual desktops and applications wherever connection is available.

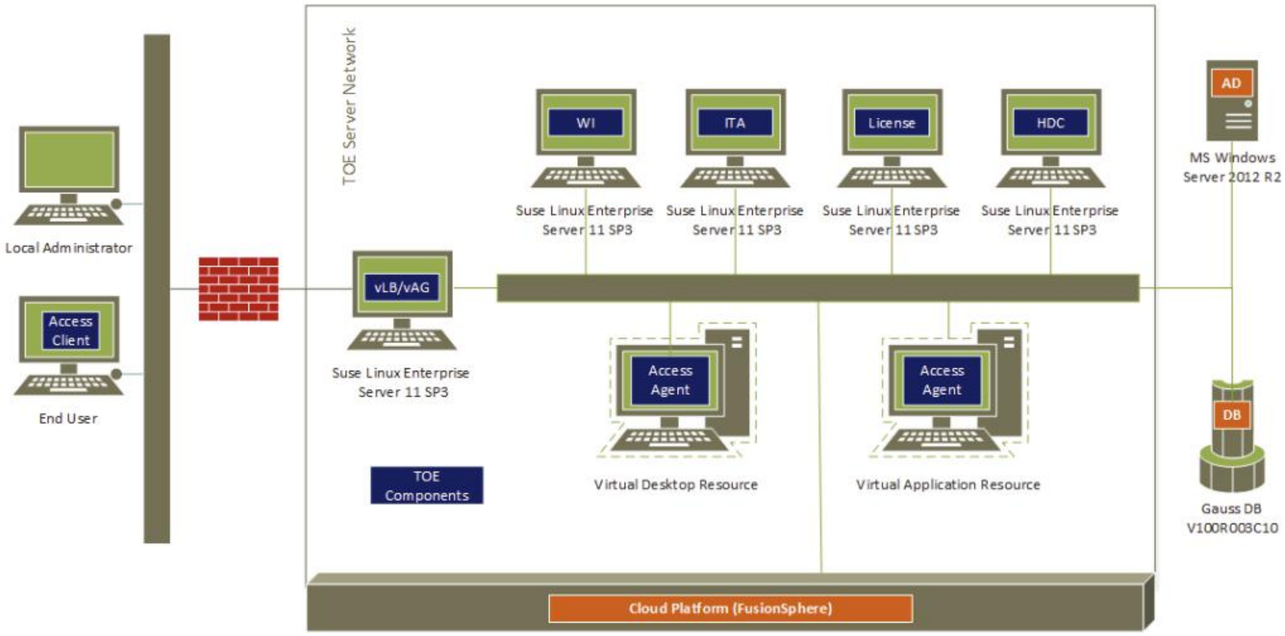
TOE Server Network
Local Administrator
Access Client
End User
vLB/vAG
Suse Linux Enterprise Server 11 SP3
WI
ITA
License
HDC
Suse Linux Enterprise Server 11 SP3
Suse Linux Enterprise Server 11 SP3
Suse Linux Enterprise Server 11 SP3
Suse Linux Enterprise Server 11 SP3
AD
MS Windows Server 2012 R2
Access Agent
Virtual Desktop Resource
Access Agent
Virtual Application Resource
DB
Gauss DB V100R003C10
TOE Components
Cloud Platform (FusionSphere)

Figure 1: FusionAccess Components

The above figure provides an architectural overview of the FusionAccess, the elements displayed with a blue background are components of the TOE.

The TOE is composed by following components:

Component	Function Description
ITA	The ITA provides interfaces for administrator to manage desktops and application. It interacts with the HDC and FusionSphere to create and assign VMs, manage VM status and images, and operate and maintain VMs.
HDC	As the core of the virtual desktop management software, the HDC manages desktop groups, assigns VMs to users, unassigns VMs from users, and enables users to log in to VMs after receiving requests from the ITA.
License	The license component manages and distributes licenses for the HDC and restricts the amount of users who login virtual desktop.

WI	The WI provides a web login page for end users. After an end user initiates a login request, the WI forwards the user login information (the encrypted username and password) to the AD for authentication. If the authentication succeeds, the WI displays a desktop and application list provided by the HDC to the user. The user can choose a desktop or application from the list to log in.
vLB/vAG	The vLB implements load balancing of WIs to prevent a large number of users from accessing the same WI (in case of there are more than one instance for each TOE component). The vAG serves as the access gateway to connect to the elements located at the internal network.
AccessClient	AccessClient installed on user devices and enabled HDP connections from user devices to virtual desktops and published applications.
AccessAgent	AccessAgent software installed on VMs and enables VMs to interact with desktop management components

Table 2: FusionAccess components and their functions

Local administrator can assign virtual desktop and application to the end user and configure end user’s access permissions for virtual desktop and applications by the ITA Portal. The end user can access own virtual desktops and applications by AccessClient (the application exists on an application virtual machine and is available to the terminal user to choose from, the huawei desktop that was assigned by local administrator lies on fusionsphere). The interactions between the components for the end user accessing its virtual desktop and applications (illustrated bellow in Figure 3) are as follows:

1. Local administrator login on ITA Portal and will be authenticated by ITA TOE component.

2. The ITA provides interfaces for local administrator to manage desktop and application resource, and distributes user/virtual resource information which local administrator configured.

3. The end users enter their username/password, which will be sent to WI as a HTTPs request protected by TLS 1.2.

4. WI requests the AD to authenticate the end user’s username/password and get authenticated result.

5. WI will send username/password to HDC as a HTTPs request protected by TLS 1.2.

6. HDC queries the end user’s virtual desktops and applications information from the database

7. HDC sends the list of the end user available virtual desktops and applications to WI.

8. The available virtual desktops and applications are displayed by AccessClient to the end user.

9. AccessClient sends a pre-login (User information and user action) request to obtain logon information for the selected virtual desktop or application.

10. WI forwards pre-login request to HDC.

11. HDC generates login ticket and sends the policy information, prepares login to the selected virtual machine.

12. The HDC sends the license number to the license server to confirm that the license is fulfilled.

13 HDC returns login information (includes login ticket, vAG IP, vAG port,VM name, domain name,etc) to WI.

14. WI sends login information to AccessClient.

15. AccessClient establishes the connection with vAG and sends a Login request to vAG according to login information.

16. vAG forwards connection request to virtual machine.

17. AccessAgent sends login ticket to HDC that verifies the login ticket, and get the associated end user username/password to logon.

18. AccessAgent returns connection success response to vAG.

19. vAG forwards response to AccessClient.

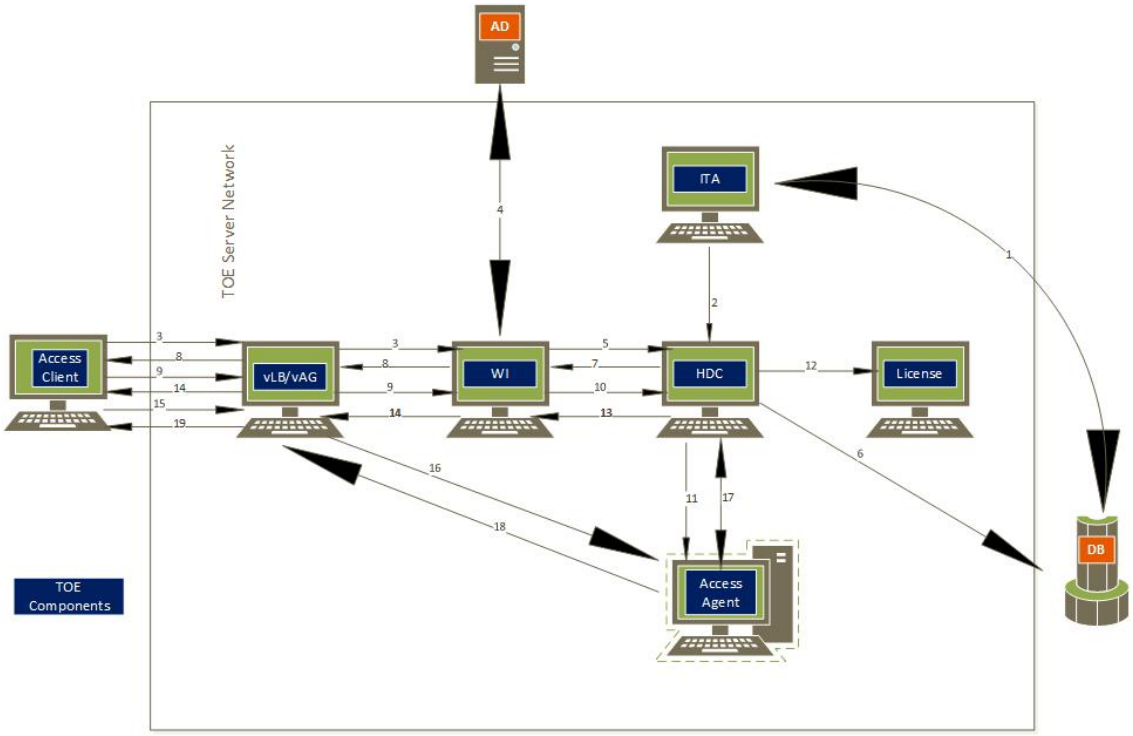

Figure 2: Interaction between components

1.4.1 Evaluated Configuration

The TOE Server was evaluated using the following physical platform:

- Huawei H22H-03 Rack Server with Xenon E5-2690 v3 CPU.

The TOE Client (AccessClient) was evaluated using the following platform:

- Windows 7 Ultimate Desktop PC (32 bits architecture) with Intel i7-7700 CPU.

1.4.2 Logical Scope

FusionAccess provides the following main security features:

- **Security Audit**: Management operations carried out by the local administrator user role are recorded. Only local administrator can review and query the records.

- **User Data Protection:** Only the authorized users are permitted access to the published application or desktop or terminal resource.

- **Identification and Authentication:** The TOE handles authentication failures, it requires the user to be identified and authenticated before doing any action.

- **Security Management:** The TOE maintain separation of functions based on user roles.

- **TOE Access:** The TOE restricts the access to the resources (application or desktop virtual machine). User sessions are automatically finished after an inactivity time interval.

- **Trusted Path/Channel:** The TOE implements a secure trusted path in the communications with the end user.

1.4.3 Physical Scope

The physical boundary of the TOE is integrated by the TOE Server and TOE Client components.

The TOE Server components consists of ITA, WI, HDC, License, vLB/vAG and AccessAgent (which is installed in the managed VMs). The TOE Client component is the AccessClient running on a user device.

FusionAccess software packages are binary compressed files. The following software packages and documents are required:

Type	Name	Version	Delivery Format
Software	FusionAccess	V100R006C20	.iso file
Software	FusionAccess Client	V100R006C20	.msi file
Software	FusionAccess Tools	V100R006C20	.iso file
Document	[AGD_PRE] CC Huawei FusionAccess V100R006C20 Preparative procedures	0.7	.docx format
Document	[AGD_OPE] CC Huawei FusionAccess V100R006C20 Operational user guidance	0.8	.docx format

Table 3: TOE software elements and guidance list

Software elements are not delivered to the final users since the installation is remotely performed by Huawei, and therefore the final users does not need to receive the software packages. On the other hand, guidance and documents associated are delivered to the final users by e-mail and in .docx format.

1.4.4 Summary of items out of scope of the TOE

The items out of scope of the TOE include the components with which FusionAccess is integrated, as detailed in section 1.3.3.

In addition, certain features of FusionAccess are not included in the scope of the evaluation:

- Only single user desktop assignment type is included in the evaluation. Each VM only supports one user to access it. All other desktop assignment methods are excluded from the evaluation.

- Only **Full Copy VM** (a type of desktop assignment) is included in the evaluation. It is virtual application running a Windows desktop operating system, rather than running in a shared, server-based environment. All other VM deliver types are excluded from the evaluation.

- GaussDB is the only database considered for the evaluation. And Windows Server 2012 is the only Active Directory considered. All other environment alternatives are excluded for evaluation.

- The login mode is the username/password, the evaluation does not include the dynamic password/USBkey/fingerprint which need third-party-software support.

2 CC Conformance Claim

This ST claims conformance with CC Part 2 and CC Part 3, no extended components. The CC version of [CC] is Version 3.1, Revision 4.

This ST is EAL3 conformance as defined in [CC] Part 3, with the assurance level of EAL3 Augmented with ALC_FLR.2.

No conformance to a Protection Profile is claimed.

3 TOE Security Problem Definition

3.1 Assets

Asset	Description
A1.Desktop	A virtual desktop. Protection requirements are for confidentiality, accessibility and integrity.
A2.Application	The published applications made available by the TOE. Protection requirements are for confidentiality, accessibility and integrity.
A3.User Credentials	Credentials used by the end user to be authenticated in the AccessClient and local administrator credentials to be authenticated in the ITA portal. Protection requirements are for confidentiality and integrity.
A4.System Data	Data generated by an administrator during configuration and management of the TOE. This includes desktop users' access permissions for virtual desktops, virtual desktop configuration data, etc. Moreover, the list of virtual machines and applications belonging to an user, relative data about the use of virtual desktops or applications, local administrator credentials, audit data generated by the TOE, data exchanged between server components and with the client component during the establishment of a virtual desktop for provision to a desktop user, are also considered system data. Protection requirements are for confidentiality and

	integrity.

Table 4: TOE Assets

3.2 Threats Agent

Agent	Description
Network attacker	An attacker who is connected to the terminal network through which end user accesses TOE but does not have credentials to use the TOE. This attacker may have the AccessClient application installed (since it is a public application) in his machine, having also access to the WI and ITA portals.

Table 5: Threats Agent

3.3 Threats

Threat: T1.Attack_UserCredentials	
Attack	An attacker may gain unauthorized access through the AccessClient or the web WI portal, to a virtual desktop or application belonging to another user. An attacker may gain unauthorized access through the web ITA portal to the local administrator managements functions. It could be done through a brute force attack trying to get the credentials of an authorized user. Once the attacker has the credentials, depending on the credential obtained, the access to the end user VMs or local administrator managements functions would be achieved.
Asset	A1.Desktop A2.Application A3.User Credentials A4.System Data

Agent	network attacker
Threat: T2.Attack_Intercept	
Attack	An attacker may intercept communication data between the: - AccessClient application and TOE server. - End user and web WI portal. - Local Administrator and web ITA portal These interceptions may lead to compromise of users credentials, and System data in transit and the communication between a Virtual Desktop or Application with the end user. It could be done spoofing these TOE server components and sniffing traffic packets interchanged.
Asset	A1.Desktop A2.Application A3.User Credentials A4.System Data
Agent	network attacker

Table 6: Threats

3.4 Assumptions

Assumption	Description
A.Physical Protection	It is assumed that the TOE is physically protected against unauthorized physical access.
A.Trustworthy Authorized Users	The authorized users (local administrators and end users) are not careless or hostile and trusted. They will follow and abide the instructions provided by the TOE documentation.
A.Third Party Components	Third Party components are secure and trusted. List of third party software components:

	• SUSE Linux Enterprise Server11 SP3 • Huawei GaussDBV100R003C10 • Microsoft Windows 7 Ultimate • Microsoft .net framework 4.0 • Microsoft Windows Server 2012 R2 Standard • Microsoft Active Directory Server in windows server 2012 • Huawei FusionSphere 6.0 List of third party hardware components: • Huawei H22H-03 Rack Server with Xenon E5-2690 v3 CPU. • Desktop PC with Intel i7-7700 CPU. 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 AccessAgent 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).
A.Timestamps	The reliable time stamps are based on the information of the real time clock (RTC) of the hardware. This RTC is trusted.

Table 7: TOE Assumptions

3.5 Organizational Security Policies

Policy	**Description**
OSP.Audit	The TOE shall audit all the security-relevant events performed by the local administrators.
OSP. Inspection	There must be periodic revisions of the audit logs generated by the TOE during its operation in order to detect any attempt to comprise the security of the TOE.

Table 8: TOE Organizational Security Policies

4 Security Objectives

4.1 Security Objectives for the TOE

O.Authentication

Local administrators must be successfully identified and authenticated before being granted access to the TOE. To be able to maintain identified the users, the TOE contains special user attributes.The TOE also verify the complexity of the user password and the number of authentication attempts.

O.Authorization

The TOE difference between two kind of users, end user and local administrator. Local administrator performs all management functions, such as assigning resources (e.g. desktop and application VMs) to end user or limiting their usage.

End user has only access to the resources authorized and under the usage conditions defined by the local administrator.

O. Communication

The TOE provides a secure communication channel for end users accessing to the desktop and application VMs. It includes the accessing to the WI ITA Portal or AccessClient application and the following access to the Virtual Desktops or applications.

The TOE provides a secure communication channel for local administrator accessing to management portal (ITA web Portal).

O.Audit

The TOE generates and stores audit records for security-relevant events. The TOE provides access to the local administrator to review the audit records. Every 24 hours, if the audit trail exceeds 500.000 entries, the oldest records are deleted.

4.2 Security Objectives for the Operational Environment

OE. Physical Protection

The operational environment provides physical protection to the TOE, ensuring that only local administrators are able to gain physical access to it.

OE. Trustworthy Authorized Users

Those responsible for the operation of the TOE and its operational environment must be trustworthy, and trained such that they are capable of securely managing the TOE and following the provided guidance.

OE. Third Party Components

The operational environment ensures the third-party components for the TOE are trusted and will not be used to attack the TOE.

Desktop and application VMs are configured by local administrators such that it is not possible for any user to gain access to the underlying operating system or hardware on which the AccessAgent is running, other than in the context of an unprivileged user account, or other applications.

OE. Timestamps

The operational environment ensures the timestamps for TOE is trusted and will not be used to attack the TOE.

4.3 Security Objectives rationale

4.3.1 Coverage

Threats/Assumption Security Objectives	T1.Attack_UserCredentials	T2.Attack_Intercept	OSP.Audit	OSP.Inspection	A.Physical Protection	A. Trustworthy Authorized Users	A.Third Party Components	A.Timestamp
O.Authentication	X							
O.Authorization	X							
O.Communication		X						
O.Audit			X	X				
OE.Physical Protection					X			
OE.Trustworthy Authorized Users						X		
OE.Third Party Components							X	
OE.Timestamps								X

Table 9: Security Objectives rationale

4.3.2 Sufficiency

Rationale for security objectives and threats:

Threat	Rationale for security objectives
T1.Attack_UserCredentials	O.Authentication and O. Authorization ensures that only authenticated and authorized user have access to the TOE resources such as desktop and application VMs.
T2.Attack_Intercept	O. Communication ensures a secure communication channel to access the ITA web portal and the WI web portal. It also ensure a secure communication channel for

	end users accessing to the desktop and application VMs.

Table 10: Rationale for security objectives and threats

Rationale for security objectives and OSPs:

Threat	**Rationale for security objectives**
OSP.Audit	O.Audit ensures that the TOE generates and stores records for security-relevant events.
OSP.Inspection	O.Audit ensures that the TOE provides to the local administrators the capability to review the audit records in order to detect any attempt to compromise the security of the TOE

Table 11: Rationale for security objectives and OSPs

Rationale for security objectives and assumptions:

Assumption	**Rationale for security objectives**
A.Physical Protection	This assumption is directly implemented by the security objective for the environment OE.Physical Protection.
A. Trustworthy Authorized Users	This assumption is directly implemented by the security objective for the environment OE. Trustworthy Authorized Users.
A.Third Party Components	This assumption is directly implemented by the security objective for the environment OE. Third Party Components.
A.Timestamps	This assumption is directly implemented by the security objective for the environment OE. Timestamps.

Table 12: Rationale for security objectives for the operational environment and assumptions

5 Extended Components Definition

No extended components have been defined for this ST.

6 Security Requirements

6.1 Conventions

The following conventions are used for the completion of operations:

~~Strikethrough~~ indicates text removed as a refinement

(underlined text in parentheses) indicates additional text provided as a refinement.

[Bold text] (between brackets) indicates the completion of an assignment.

Italicised and bold text indicates the completion of a selection.

Iteration/N indicates an element of the iteration, where N is the iteration element name.

6.2 Security Functional Requirements

6.2.1 Security Audit (FAU)

6.2.1.1 FAU_GEN.1 Audit data generation

FAU_GEN.1.1 The TSF shall be able to generate an audit record of the following auditable events:

a) Start-up and shutdown of the audit functions;
b) All auditable events for the ***not specified*** level of audit; and

c) **[The following auditable events:**

1. **Local administrator login or log out the TOE.**
2. **The operations performed on users and user rights, which include adding, deleting, and modifying user information, unlocking user's account, changing passwords, and modifying user rights.**
3. **All operations performed on authentication types and password policies.**
4. **All operations performed on virtual resources, including allocating, starting, and stopping a virtual desktop or application.**
5. **All operations performed on resource access. Including usb, camera, and other peripheral.]**

FAU_GEN.1.2 The TSF shall record within each audit record at least the following information:

a) Date and time of the event, type of event, subject identity (if applicable), and the outcome (success or failure) of the event; and

b) For each audit event type, based on the auditable event definitions of the functional components included in the PP/ST, **[none]**.

6.2.1.2 FAU_GEN.2 User identity association

FAU_GEN.2.1 For audit events resulting from actions of identified users, the TSF shall be able to associate each auditable event with the identity of the end user that caused the event.

6.2.1.3 FAU_SAR.1 Audit review

FAU_SAR.1.1 The TSF shall provide **[local administrator]** with the capability to read **[all information]** from the audit records.

FAU_SAR.1.2 The TSF shall provide the audit records in a manner suitable for the user to interpret the information.

6.2.1.4 FAU_SAR.2 Restricted audit review

FAU_SAR.2.1 The TSF shall prohibit all users read access to the audit records, except those users that have been granted explicit read-access.

6.2.1.5 FAU_SAR.3 Selectable audit review

FAU_SAR.3.1 The TSF shall provide the ability to apply **[querying]** of audit data based on **[User/ administrator, Login type, Operation name, User/administrator IP address, Start time, End Time, Result].**

6.2.1.6 FAU_STG.1 Protected audit trail storage

FAU_STG.1.1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion.

FAU_STG.1.2 The TSF shall be able to ***prevent*** unauthorized modifications to the stored audit records in the audit trail.

6.2.1.7 FAU_STG.3 Action in case of possible audit data loss

FAU_STG.3.1 The TSF shall **[delete oldest audit records every 24 hours]** if the audit trail exceeds **[500,000 entries]**.

6.2.2 User Data Protection (FDP)

6.2.2.1 FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the **[UsersAccess Policy]** on **[Authorized user as subjects, resources as objects and assignment and access of the authorized user to the resources].**

6.2.2.2 FDP_ACF.1 Security attribute based access control

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

a) **Subjects: end user & local administrator**

b) **Objects: published application, desktop or terminal resources**

c) **Attributes:**

   a. **end user (relation with Object/Access policy of resources),**

   b. **Administrator (user type/password/ session timeout/lock time)**

].

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

a) **Only the end users authorized by the administrator are permitted access to the published application, desktop or terminal resources.**

b) **Only the authenticated local administrators are able to assign the published application or desktop or terminal resource to the end users.**

]

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

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

6.2.3 Identification and Authentication (FIA)

6.2.3.1 FIA_AFL.1 Authentication failure handling

FIA_AFL.1.1 The TSF shall detect when **[5]** unsuccessful authentication attempts occur related to **[local administrator log in].**

FIA_AFL.1.2 When the defined number of unsuccessful authentication attempts has been ***met***, the TSF shall **[lock local administrator until automatic unlock after 10 minutes].**

6.2.3.2 FIA_SOS.1 Verification of secrets

FIA_SOS.1.1 The TSF shall provide a mechanism to verify that secrets meet **[**

a) **The combination of two of the following requirements for the local administrator:**

i. at least one lower-case alphanumerical character

ii. at least one upper-case alphanumerical character

iii. at least one numerical character

b) **an administrator configurable combination of the**

following:

i. contain special character

ii. reject contain username or reversed username

c) **an administrator configurable minimum and maximum password length (default minimum length is 8 and maximum is 32 characters)].**

6.2.3.3 FIA_UAU.2/local administrator User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.3.4 FIA_UAU.2/end user User authentication before any action

FIA_UAU.2.1 The TSF shall require each user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

6.2.3.5 FIA_UID.2/local administrator User identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.3.6 FIA_UID.2/end user User identification before any action

FIA_UID.2.1 The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

6.2.4 Security Management (FMT)

6.2.4.1 FMT_MOF.1 Management of security functions behaviour

FMT_MOF.1.1 The TSF shall restrict the ability to ***disable, enable*** the functions **[defined in FMT_SMF.1]** to **[the local administrator]**.

6.2.4.2 FMT_MSA.1 Management of security attributes

FMT_MSA.1.1 The TSF shall enforce the **[UsersAccess Policy]** to restrict the ability to ***query, modify*** the security attributes **[identified in FDP_ACF.1]** to **[the local administrator]**.

6.2.4.3 FMT_MSA.3 Static attribute initialization

FMT_MSA.3.1 The TSF shall enforce the **[UserAccess Policy]** to provide ***restrictive*** default values for security attributes that are used to enforce the SFP.

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

6.2.4.4 FMT_SMF.1 Specification of Management Functions

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

[

a) **configuration of password policy**
b) **local administrator management (creation, deletion, modification of lockout status or password)**
c) **configuration of idle local administrator session timeout duration**
d) **configuration of access permissions for published application**
e) **configuration of access permissions for virtual desktop**
f) **configuration of access permissions for local resources**

]

6.2.4.5 FMT_SMR.1 Security roles

FMT_SMR.1.1 The TSF shall maintain the roles [**end user and local administrator**].

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

6.2.5 TOE access (FTA)

6.2.5.1 FTA_MCS.1 Limitation on multiple concurrent sessions

FTA_MCS.1.1 The TSF shall restrict the maximum number of concurrent sessions that belong to the same user.

FTA_MCS.1.2 The TSF shall enforce, by default, a limit of **[1]** sessions per user.

Application Note: a session is defined as the status in which either the end user has successfully logged on the desktop VM, or the local administrator has successfully logged on the ITA portal.

6.2.5.2 FTA_SSL.3 TSF-initiated termination

FTA_SSL.3.1 The TSF shall terminate an interactive session after a **[10 minutes].**

Application Note: this SFR only applies to the session created when a local administrator has successfully logged on the ITA portal, so the session created when an end user is successfully logged on the desktop VM does not terminate after any period of time.

6.2.6 Trusted Path/Channels (FTP)

6.2.6.1 FTP_TRP.1 Trusted path

FTP_TRP.1.1 The TSF shall provide a communication path between itself and ***remote*** users that is logically distinct from other communication paths and provides assured identification of its end points and protection of the communicated data from ***modification, disclosure.***

FTP_TRP.1.2 The TSF shall permit ***remote users*** to initiate communication via the trusted path.

FTP_TRP.1.3 The TSF shall require the use of the trusted path for ***initial user authentication***.

Application notes: This trusted path is used by end user accessing WI. It has to be used for initial end user authentication and it is created between the end user accessing WI.

6.3 Rationale for the Security Requirements

6.3.1 Security Requirements Dependency Rationale

The security functional requirements in this Security Target do not introduce dependencies on any security assurance requirements. The security assurance requirements in this Security Target also do not introduce dependencies on any security functional requirement.

The following table demonstrates the dependencies of SFRs modeled in CC Part 2 and how the SFRs for the TOE resolve those dependencies:

Security Functional Requirement	**Dependency**	**Resolution**
FAU_GEN.1	FPT_STM.1	OE.Timestamps: The operational environment ensures the timestamps for TOE is trusted and will not be used to attack the TOE.
FAU_GEN.2	FAU_GEN.1 FIA_UID.1	FAU_GEN.1 FIA_UID.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1	FAU_STG.1
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 FMT_MSA.3	FDP_ACC.1 FMT_MSA.3
FIA_AFL.1	FIA_UAU.1	FIA_UAU.2
FIA_SOS.1	No Dependencies	None

FIA_UAU.2/local administrator	FIA_UID.1	FIA_UID.2
FIA_UAU.2/end user	FIA_UID.1	FIA_UID.2
FIA_UID.2/local administrator	No Dependencies	None
FIA_UID.2/end user	No Dependencies	None
FMT_MOF.1	FMT_SMF.1 FMT_SMR.1	FMT_SMF.1 FMT_SMR.1
FMT_MSA.1	[FDP_ACC.1 or FDP_IFC.1] FMT_SMR.1 FMT_SMF.1	FDP_ACC.1 FMT_SMR.1 FMT_SMF.1
FMT_MSA.3	FMT_MSA.1 FMT_SMR.1	FMT_MSA.1 FMT_SMR.1
FMT_SMF.1	No Dependencies	None
FMT_SMR.1	FIA_UID.1	FIA_UID.2
FTA_MCS.1	FIA_UID.1	FIA_UID.2
FTA_SSL.3	No Dependencies	None
FTP_TRP.1	No Dependencies	None

Table 13: Dependencies resolution

6.3.2 Coverage

The following table provides a mapping of SFR to the security objectives, showing that each security functional requirement addresses at least one security objective.

Threats/ Assumption Security Objectives	O.Authentication	O.Authorization	O.Communication	O.Audit
FAU_GEN.1				X
FAU_GEN.2				X
FAU_SAR.1				X
FAU_SAR.2				X
FAU_SAR.3				X
FAU_STG.1				X
FAU_STG.3				X
FDP_ACC.1		X		
FDP_ACF.1		X		
FIA_AFL.1	X			
FIA_SOS.1	X			
FIA_UID.2/end user	X			
FIA_UID.2/local administrator	X			
FIA_UAU.2/end user	X			
FIA_UAU.2/local administrator	X			
FMT_MOF.1		X		
FMT_MSA.1		X		
FMT_MSA.3		X		
FMT_SMF.1		X		
FMT_SMR.1		X		
FTA_MCS.1		X		
FTA_SSL.3		X		
FTP_TRP.1			X	

Table 14: Mapping SFRs to objectives

6.3.3 Sufficiency

The following rationale provides justification for each security objective for the TOE, showing that the security functional requirements are suitable to meet and achieve the security objectives:

Security Objective	SFRs	Rationale
O. Authentication	FIA_UID.2/Local administrator FIA_UID.2/End user FIA_UAU.2/Local administrator FIA_UAU.2/End user	Local administrator needs to be identified and authenticated before doing any action. End user needs to be identified and authenticated before doing any action
	FIA_AFL.1 FIA_SOS.1	Not allowing unlimited login attempts Ensuring password quality.
O. Authorization	FDP_ACC.1 FDP_ACF.1	These SFRs ensure that only properly authorized users can access terminal resource.
	FMT_MOF.1 FMT_MSA.1 FMT_MSA.3 FMT_SMR.1 FMT_SMF.1	These SFRs define the actions that the administrator is able to do.
	FTA_MCS.1	This SFR restricts the number of the user sessions and assures there is only one user session established.
	FTA_SSL.3	Logging out users after an inactivity period.
O.Audit	FAU_GEN.1 FAU_GEN.2	These SFRs ensure that audit records can be generated from significant events and that these audit records contain useful information, including the correct time of the events.
	FAU_SAR.1 FAU_SAR.2 FAU_SAR.3	These SFRs ensure that the correct users can read the correct information from the audit records.

	FAU_STG.1 FAU_STG.3	These SFRs ensure the audit data is protected against unauthorized modification and deletion, and what happens when audit storage fills up.
O.Communication	FTP_TRP.1	This SFR provides the secure communication between end user and the TOE.

Table 15: SFR sufficiency analysis

6.4 Security Assurance Requirements

The security assurance requirements for the TOE are the Evaluation Assurance Level 3 components augmented with ALC_FLR.2, as specified in [CC] Part 3. No operations are applied to the assurance components.

Assurance Class	Assurance Components
ADV: Development	ADV_ARC.1 Security architecture description ADV_FSP.3 Functional specification with complete summary ADV_TDS.2 Architectural design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance AGD_PRE.1 Preparative procedures
ALC: Life-cycle support	ALC_CMC.3 Authorisation controls ALC_CMS.3 Implementation representation CM coverage ALC_DEL.1 Delivery procedures ALC_DVS.1 Identification of security measures ALC_LCD.1 Developer defined life-cycle model ALC_FLR.2 Flaw reporting procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims ASE_ECD.1 Extended components definition

	ASE_INT.1 ST Introduction ASE_OBJ.2 Security objectives ASE_REQ.2 Derived security requirements ASE_SPD.1 Security problem definition ASE_TSS.1 TOE Summary Specification
ATE: Test	ATE_COV.2 Analysis of coverage ATE_DPT.1 Testing: basic design ATE_FUN.1 Functional Testing ATE_IND.2 Independent Testing - sample
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

Table 16: Security Assurance Requirements

6.5 Rationale for Security Assurance Requirements

The evaluation assurance level 3 augmented with ALC_FLR.2 has been chosen commensurate with the threat environment that is experienced by typical consumers of the TOE.

7 TOE Summary Specification

7.1 TOE Security Functional Specification

This chapter identifies and describes how the Security Functional Requirements identified above are met by the TOE.

7.1.1 Security Audit

An operation log records operations performed by the local administrator user on the system and the result of the operation and is used for tracing and auditing.

Fields contained in an operation log include:

User(user name)
Login Type
Operation Name
Level
User IP address
Start Time
End Time
Result
Details
Failure cause

Only local administrators can query and export operation logs. Logs cannot be modified or deleted on the management portals.

The TOE allows local administrator to query operation logs by specifying search criteria. The search criteria can be any field contained in an operation log, except Level, Details and

Failure Cause. The operation logs of the TOE can be exported to a local directory for auditing.

The FusionAccess checks the number of operation logs every 24 hours. If the number of logs exceeds 500.000, the TOE automatically deletes the earliest logs.

The Security Audit function is designed to satisfy the following security functional requirements:FAU_GEN.1, FAU_GEN.2, FAU_SAR.1, FAU_SAR.2, FAU_SAR.3, FAU_STG.1 and FAU_STG.3 .

7.1.2 Identification and Authentication

When a local administrator logs into the Fusion Access management portal (ITA portal), a username and password are requested to verify his identity before the access is given.

The local administrator can log into the Fusion Access system and obtain related rights only after the authentication is checked successful. After a local administrator successfully logs into the system, the local administrator could perform the security management functions on the system.

End users can log into the Fusion Access system using the AccessClient application and WI web portal providing its username and password. Once the end user is successfully authenticated, the virtual desktops, applications and terminal resources assigned by the administrator are available.

On the other hand, if a local administrator fails to be authenticated for several consecutive times (5 by default and configurable) within a specified time period (5 minutes by default and configurable), the TOE automatically locks the local administrator within a specified time period (10 minutes by default and configurable).

Both failed and successful login events for local administrator are recorded in the login logs.

Identification and authentication function are designed to satisfy the following security functional requirements: FIA_AFL.1, FIA_UAU.2/local administrator, FIA_UAU.2/end user, FIA_UID.2/local administrator, FIA_UID.2/end user and FMT_SMR.1.

7.1.3 User access policy

TOE restricts the ability to disable or enable the management functions to the local administrator. As well as, it enforces the the UsersAccess Policy to restrict the ability to query and modify the security attributes to the local administrator and to provide restrictive default values for security attributes that are used to enforce the SFP.

Local administrator can assign virtual desktop, applications and local resources to an end user. This end user will be only able to access the virtual desktop, applications and local resources which have been assigned to him.

After administrator configured the access policy of local device resource, this policy will be distributed to AccessClient by AccessAgent. The AccessClient will redirect the local device to AccessAgent.

The desktop, application user and local device resource access control function is designed to satisfy the following security functional requirements: FMT_MSA.1, FMT_MSA.3, FDP_ACC.1 and FDP_ACF.1.

7.1.4 Secure communications

Data transmitted between End User and WI is encrypted using Transport Layer Security (TLSv1.2). End user can connect to WI through AccessClient application and WI web portal. Both ways used TLSv1.2 to transmit the data. When the communication channel between them is going to be established, a certificate to the client is requested. Bidirectional authentication is configured, so without providing a valid client certificate the connection is not established. Client and server exchange their certificates during the handshake and if both certificates are valid, the trusted channel is created.

Data transmitted between Local administrator and ITA Portal is encrypted using Transport Layer Security (TLSv1.2) but bidirectional authentication is not configured among Client and ITA. In spite of this, the communication is not risky.

The* Secure communications *function is designed to satisfy the following security functional requirements: FTP_TRP.1

7.1.5 Security management

After being authenticated, local administrator is able to configure the user attributes, create, delete and modify local administrator users, configure idle local administrator session timeout duration, set lock timeouts, lock/unlock accounts, end user access control policy and local resource policy.

Moreover, local administrators can configure password policy. Password must meet the following base requirements:

The password is a string of 8 to 32 characters.
The password must contain at least two of the following combinations:

1. Lowercase letters
2. Uppercase letters
3. Digits

The password must comply with the pre-configured password policies:

Minimum length
Maximum length
Contain special characters
Allow username or reversed username
Rules on using the same password
Password validity (days)
Forcibly change password upon initial login
Minimum change interval (minutes)
Advance warning of password expiration (days)
Maximum number of incorrect passwords allowed
Statistics period (minute)
User locking duration (minutes)

The* Security management *function is designed to satisfy the following security functional requirements: FIA_SOS.1, FMT_MOF.1. and FMT_SMF.1

7.1.6 TOE Access

After a local administrator user login the TOE (ITA web Portal), TOE will check whether the user is in an active state. If the user has been in inactivity beyond 10 minutes which can be configured, the session will be ended.

A virtual desktop cannot be accessed by two different end user as the same time.

A local administrator account only can have one concurrent session in the ITA web portal. The same account cannot access to the ITA web portal as the same time from different browsers.

The* TOE Access *function is designed to satisfy the following security functional requirements: FTA_SSL.3, FTA_MCS.1

8 Abbreviations, Terminology and References

8.1 Abbreviations

AD	Active Directory
CC	Common Criteria
CNA	Compute Node Agent
FTP	File Transfer Protocol
GUI	Graphical User Interface
HTTPS	Hypertext Transfer Protocol Secure
NTP	Network Time Protocol
O&M	Operation and Management
PP	Protection Profile
SFR	Security Functional Requirement
ST	Security Target
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functions

VM	Virtual Machine
HDP	Huawei Desktop protocol

Table 17: Abbreviations

8.2 Terminology

This section contains definitions of technical terms that are used with a meaning specific to this document. Terms defined in the [CC] are not reiterated here, unless stated otherwise.

Local Administrator	A local administrator is a user of the TOE who may have been assigned specific administrative privileges within the TOE. This ST may use the term administrator occasionally in an informal context, and not in order to refer to a specific role definition – from the TOE’s point of view, a local administrator is simply a user who is authorized to perform certain administrative actions on the TOE and the objects managed by the TOE.
End User:	The user is a human who has the rights to use the desktop or application, and the local device resources of the machine where the virtual desktop is opened.
Management VM	Virtual machine used to deploy management components, such as ITA, WI, etc.
virtual desktop:	Virtual desktop implementations operate in a client/server computing environment. Virtual desktop execution takes place on a remote operating system which communicates with the local client device over a network using a remote display protocol through which the user interacts with virtual desktops. All applications and data used remain on the remote system with only display, keyboard,

	and mouse information communicated with the local client device, which may be a conventional PC/laptop, a thin client device, a tablet, or even a smartphone.
virtual application:	Virtual application improves delivery and compatibility of applications by encapsulating them from the underlying operating system on which they are executed. A fully virtualized application is not installed on hardware, in the traditional sense. Instead, a hypervisor layer intercepts the application which at runtime acts as if it is interfacing with the original operating system and all the resources managed by it, when in reality it is not.
Hypervisor	An abstraction layer implementing a set of software calls that can be made by domains, and providing an asynchronous event-based interface for communication from the hypervisor to domains. The hypervisor controls the scheduling of the CPU and the partitioning of memory between virtual machines.
FusionSphere	Huawei's FusionSphere OS integrates the FusionCompute virtualization platform and FusionManager cloud management software
GaussDB	GaussDB is a relational database system based on open source database PostgreSQL developed by HUAWEI Technology Co., ltd..

Table 18: Terminology

8.3 References

[CC] Common Criteria for Information Technology Security Evaluation. Part 1-3. September 2012. Version 3.1 Revision 4.

[CEM] Common Methodology for Information Technology Security Evaluation.

September 2012. Version 3.1 Revision 4.