StillSecure Safe Access™ V5.0
Security Target V1.1

September 17, 2007

Prepared by

CYGNACOM
SOLUTIONS

Suite 5200 West ♦ 7925 Jones Branch Drive ♦ McLean, VA 22102-3321 ♦ 703 848-0883 ♦ Fax 703 848-0960

TABLE OF CONTENTS

SECTION **PAGE**

Table of Tables

Table of Figures

1 Security Target Introduction

1.1 *Security Target Identification*

TOE Identification:	StillSecure Safe Access V5.0, build number 3146
ST Title:	StillSecure Safe Access V5.0 Security Target
ST Version:	Version 1.1
ST Authors:	CygnaCom Solutions Inc.
ST Date:	9/17/2007
Assurance Level:	EAL2
Strength of Function:	SOF-basic
Registration:	<To be filled in upon registration>
Keywords:	Network Access Control, Safe Access, NAC, Endpoint Security Solution.

1.2 *Security Target Overview*

This Security Target (ST) defines the Information Technology (IT) security requirements for StillSecure Safe Access V5.0. StillSecure Safe Access is a flexible Network Access Control (NAC) solution that provides three methods of endpoint compliance testing and three methods of NAC policy enforcement. Safe Access enforces compliance with the NAC security policy by matching endpoint attributes against an administrator configured NAC security policy. If an endpoint fails to meet the NAC security policy requirements the endpoint is quarantined it to a specific portion of the network. This ensures that potentially damaging applications such as peer-to-peer or spyware software and the latest worms and viruses cannot take root inside a protected network,

1.3 *Common Criteria Conformance*

The TOE is Part 2 extended, Part 3 conformant, and meets the requirements of Evaluation Assurance Level (EAL) 2 from the Common Criteria Version 2.3.

1.4 *Document Organization*

The main sections of an ST are:

- Section 1, Security Target Introduction, which provides a brief overview of the TOE and the ST.
- Section 2, TOE Description, describes the product type and the scope and boundaries of the TOE.
- Section 3, TOE Security Environment, identifies assumptions about the TOE's intended usage and environment and threats relevant to secure TOE operation.
- Section 4, Security Objectives, defines the security objectives for the TOE and its environment.
- Section 5, IT Security Requirements, specifies the TOE Security Functional Requirements (SFR), Security Requirements for the IT Environment, and the Security Assurance Requirements.
- Section 6, TOE Summary Specification, describes the IT Security Functions and Assurance Measures.
- Section 7, Protection Profile (PP) Claims, is not applicable, as this product does not claim conformance to any PP.
- Section 8, Rationale, presents evidence that the ST is a complete and cohesive set of requirements and that a conformant TOE would provide an effective set of IT security countermeasures within the security environment. The Rationale has three main parts: Security Objectives Rationale, Security Requirements Rationale, and TOE Summary Specification Rationale.

1.5 *Acronyms*

Table 1-1: Acronyms

Acronym	Definition
ACM	Configuration Management
ADO	Delivery and Operation
ADV	Development
AGD	Guidance Documents
ALC	Life cycle support
ATE	Tests
AVA	Vulnerability assessment
CC	Common Criteria [for IT Security Evaluation]
EAL	Evaluation Assurance Level
FAU	Security Audit
FDP	User Data Protection
FIA	Identification and Authentication
FMT	Security Management
FPT	Protection of the TSF
FTA	TOE Access
ID	Identifier
IT	Information Technology
NAC	Network Access Control
SF	Security Function
SFP	Security Function Policy
ST	Security Target
TOE	Target of Evaluation
TSC	TSF Scope of Control
TSF	TOE Security Functions
TSFI	TOE Security Functions Interface
TSP	TOE Security Policy

1.6 *References*

Table 1-2: References

ID	Document Name
[CC p1]	Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model, CCMB-2005-08-001, Version 2.3, August 2005
[CC p2]	Common Criteria for Information Technology Security Evaluation, Part 2: Security functional requirements, CCMB-2005-08-002, Version 2.3, August 2005
[CC p3]	Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance requirements, CCMB-2005-08-003, Version 2.3, August 2005
[CEM]	Common Criteria for Information Technology Security Evaluation,

	Part 2: Evaluation Methodology, CCMB-2005-08-004, Version 2.3, August 2005
[SA IG]	Safe Access v5.0 Installation Guide July 13, 2007, (rev-j)
[SA QS]	Safe Access Quick-start Card, v5.0 (rev-c)
[SA UG]	Safe Access v5.0 User's Guide July 13, 2007 (rev-m)
[SA RN]	Safe Access v5.0 Release Notes, July 20, 2007 (rev-s)
[SA CC Sup]	StillSecure Safe Access V5.0 Common Criteria Supplement to the Guidance Documentation
[SA ADV]	StillSecure Safe Access V5.0 Development Specification (FSP/HLD/RCR) Common Criteria Evaluation
[SA SOF]	StillSecure Safe Access V5.0 Strength of Function Analysis
[SA VLA]	StillSecure Safe Access V5.0 Vulnerability Analysis
[SA COV]	StillSecure Safe Access V5.0 Evaluation Test Coverage Analysis
[SA FUN]	Safe Access v5.0 Common Criteria test cases
[SA DEL]	Safe Access v5.0 Delivery
[SA CM]	Safe Access v5.0 Configuration Management
[CCTL TR]	Safe Access v5.0 Test Report – CygnaCom CCTL

1.7 *Terminology*

Table 1-3: Customer Specific Terminology

Term	Definition
Management Server (MS)	Used by administrators to centrally configure and manage enforcement servers.
Enforcement Server (ES)	Detects and tests endpoints for compliance with administrator defined security standards and controls the access granted to the endpoints.
Cluster	A cluster is a group of one or more enforcement servers (ES)
Endpoint	The physical computer that an end-user is using to connect to the network.

Table 1-4: CC Specific Terminology

Term	Definition
Authorized user	A user who may, in accordance with the TSP, perform an operation.
External IT entity	Any IT product or system, untrusted or trusted, outside of the TOE that interacts with the TOE.
Role	A predefined set of rules establishing the allowed interactions between a user and the TOE.
TOE Security Functions (TSF)	A set consisting of all hardware, software, and firmware of the TOE that must be relied upon for the correct enforcement of the TSP.
User	Any entity (human user or external IT entity) outside the TOE that interacts with the TOE.

2 TOE DESCRIPTION

2.1 *Product Type*

StillSecure Safe Access is a flexible Network Access Control (NAC) Solution that provides three enforcement mechanisms to support fitting into existing network architecture and provides three endpoint testing methods to cover a range of endpoints and users. Safe Access protects the network by ensuring that endpoints are in compliance with the organization's NAC policy before they are granted access to the protected network.

Safe Access administrators create NAC policies that define the Security Functional Policy (SFP) enforced on the endpoint before it is granted access to the protected network and also specifies the access control actions to be taken when the endpoints do not comply. NAC policies can specify how often the endpoint is re-tested while connected, the length of time an endpoint can be inactive before being quarantined, tests that assess operating systems settings and services, ensure anti-virus and other security applications are present and up-to-date[1], detect the presence of worms, trojans, and viruses, and check for potentially dangerous applications such as file sharing, peer-to-peer (P2P), or spyware.

With support from the IT environment, Safe Access automatically applies the NAC policies to endpoints as they attempt to connect to the protected network. Depending on the endpoint testing method chosen, Safe Access can periodically re-test endpoints that have been granted access to ensure that real-time system changes do not violate the NAC security policy.

Based on the test results, endpoints are either permitted access to the protected network or quarantined to a specific part of the network, thus enforcing the NAC security policy. Safe Access audits all testing and connection activity and produces a range of reports for auditors.

The Safe Access product consists of the following components:

1. The Safe Access Management Server (MS) and
2. The Safe Access Enforcement Server (ES).
3. The StillSecure Safe Access Agent
4. The StillSecure ActiveX Control

Safe Access can be deployed in a Single-Server configuration or Multi-Server configuration. The Single-Server configuration utilizes one MS and one ES on a single server. In the Multi-Server configuration, the MS and the ES are installed on their own hardware platforms, and the ES communicates with the MS utilizing a channel secured by the SSL protocol. In the Multi-Server configuration there may be multiple instances of the ES. If multiple ES are configured, the MS allows administrators to centrally configure and manage multiple ES(s) using a single Web-based console. The ES(s) are located at points in the network that allow them to control the access of endpoints. The ES(s) test endpoints for compliance and, with the support of the IT environment, enforce access control of the endpoints based on the test results. The tested configuration will have two hardware platforms hosting the TOE, one with an ES installed on it and the other with a MS installed on it (see Figure 2-1).

The NAC functionality implemented by Safe Access can be described in terms of two independent implementation choices made by the end-user: the endpoint **testing method** used to test an endpoint for compliance to the NAC Security Functional Policy (SFP) which gives a result of ‘quarantine’ or ‘connect’, and the **enforcement method** used to enforce the NAC SFP compliance test result (quarantine or connect) on the endpoint. Some enforcement methods also support a TOE action of ‘disconnect’ which after a configurable interval of time causes the endpoint to be disconnected from the network and re-tested when the endpoint attempts to reconnect.

[1] The terms “up-to-date and “latest” are subject to when StillSecure managed service database actually receives vendor information regarding third party updates/patches and when the administrator receives updates to test policy rules.

Safe Access offers three endpoint **testing methods** for testing the endpoint for admission to the protected network. Testing methods can be ordered from most preferred to least preferred. These are:

1 **Agentless testing method:** Agentless testing uses an existing Windows service (RPC) on the endpoint. The Agentless test method requires that file and printer sharing be enabled on the endpoint.

2 **ActiveX-based testing method:** ActiveX testing uses a signed ActiveX control that is downloaded by the end-user via a browser. The ActiveX plug-in requires the end-user to download and run the signed ActiveX control. Hence, browser security settings must allow the execution of signed ActiveX controls. ActiveX testing only runs once, when the endpoint connects to the network and the endpoint is not monitored again until it re-connects to the network.

3 **Agent-based testing method:** StillSecure agent-based testing installs the StillSecure Safe Access Agent onto the endpoint where it then runs as a privileged new Windows service. Once installed, the StillSecure Agent is available for re-testing of the endpoint when invoked by an authorized TOE user through the TOE interfaces.

Safe Access provides three NAC SFP **enforcement methods** for quarantining non-compliant endpoints. Physical deployment of the Safe Access V5.0 is dependent on the enforcement method used. The three enforcement methods are:

1 **Inline for VPN and RAS connections enforcement method –** This enforcement method is for use with VPN and RAS connections, and is depicted in Figure 2-2. It requires that the TOE be physically inserted into the network connection between the endpoint and the protected network.

2 **DHCP enforcement method** – This enforcement method is depicted in Figure 2-3. It requires that the all DHCP requests pass through the Safe Access server. For a quarantined endpoint, Safe Access distributes the quarantined IP address for the endpoint. If Safe Access allows the endpoint to have access, Safe Access allows the corporate network DHCP server to distribute a non-quarantined IP address. Safe Access assigns a DHCP IP address based on the quarantine area parameters defined by the administrator during configuration.

3 **802.1X enforcement method** – This enforcement method is depicted in Figure 2-4. It requires that the network architecture include a RADIUS server and an 802.1X capable Layer 2 device. The Safe Access server is installed where it can communicate with the Remote Authentication Dial-In User Service (RADIUS) server. The RADIUS server communicates with the 802.1X capable Layer 2 device, which performs the quarantining by moving ports or MAC addresses in and out of virtual local area networks (VLANs).

Enforcement methods can be blended within a Safe Access implementation and managed from a single Web-based console. Any endpoint testing method may be used with any NAC security policy enforcement method.

The combination of flexible endpoint testing methods and NAC security policy enforcement methods allows endpoints, including those belonging to LAN-connected users, remote users, contractors, visitors, and wireless users, to be thoroughly tested before being granted access to the protected network.

2.2 *Safe Access Components*

The Safe Access V5.0 is comprised of an MS and at least one ES. In the evaluated configuration, Safe Access is deployed in multi-server configuration, with two servers, one hosting the MS, and the other hosting the ES.

2.2.1 Management Server (MS)

The functions of the MS are:

- o **Configuration:** The System configuration window allows the system administrator to set the operating parameters for Safe Access. Operating parameters are:
  - Configure Enforcement Clusters and Servers.
  - Manage TOE user accounts.
  - Manage TOE user roles.

    - Set date and time.
    - Configure NAC security policy enforcement method (quarantine options).
    - Configure the backup features used to back up the management server's database, properties files, keystore files, and subscription files (related to licensing).
- **Configure NAC policies**: An administrator uses the MS to establish the NAC policies used by the ES to evaluate the security status of endpoints attempting to access the network.
- **Quarantining:** The NAC security policy enforcement method is defined per cluster. All of the enforcement servers in a given cluster use the same NAC security policy enforcement method (Inline, DHCP, or 802.1X).
- **Endpoint activity:** Monitors endpoint connection activity, Access Control state of the endpoints, and endpoint Test Status state.
- **License:** Download license control data, enter and submit new license keys, view license information such as start date, end date, days remaining, renewal date, endpoints under license.
- **Test updates:** Set date and time for automatic download of test updates. Manually execute or disable test updates. Test updates consist of downloading "Red Hat Package Management" (rpm) packages which contain updates to existing test scripts and/or new test scripts for new testing functionality. The rpm packages are downloaded by the MS to update the existing policies and then forwarded to the ES(s). No new functionality is enabled by default.
- **TOE user authentication**
- **Audit reporting**
- **Protected network security status reporting**

The security functions supported by the MS are:

- Security audit
- Identification and authentication.
- Security management
- Protection of TOE security functions
- Security status reporting
- Use of Trusted paths and channels

2.2.2 Enforcement Server (ES)

The functions of the ES are:

- **Test method selection and installation for the endpoint**
- **Testing:** The ES automatically tests all endpoints attempting to access the protected network. Tests are fast and the administrator is kept informed of test progress and results. After the initial compliance tests, for endpoints where either the Agentless testing method or the Agent-based testing method have been configured, Safe Access periodically re-tests the endpoints to ensure the endpoint's configuration conforms with the NAC security policy. Periodic re-testing is not available if the ActiveX testing method was selected for the endpoint.
- **Access control:** Based on endpoint test results, Safe Access takes the configured action. Endpoints that are compliant with the NAC security policy are permitted access to the protected network. Non-compliant endpoints are either quarantined, or are given access for a temporary period in order to implement the necessary fixes during this period.

The security functions supported by the ES are:

- User data protection

- Protection of TOE security functions
- Collection of data for StillSecure security status reporting
- Use of Trusted paths and channels

2.2.3 StillSecure Safe Access Agent

The function of the StillSecure Safe Access Agent is:

- Support an interface through which the ES can test and re-tests endpoints attempting to access the protected network

2.2.4 StillSecure ActiveX Control

The function of the StillSecure ActiveX Control is:

- Support an interface through which the ES can test endpoints attempting to access the protected network.

2.3 *TSF Physical Boundary and Scope of the Evaluation*

2.3.1 The TOE includes the following software only components

The TOE includes the following components of the Safe Access V5.0:

- Management Server
- Enforcement Server
- StillSecure Safe Access Agent
- StillSecure ActiveX Control

Figure 2-1 shows the Safe Access components in a generalized multi-server configuration.

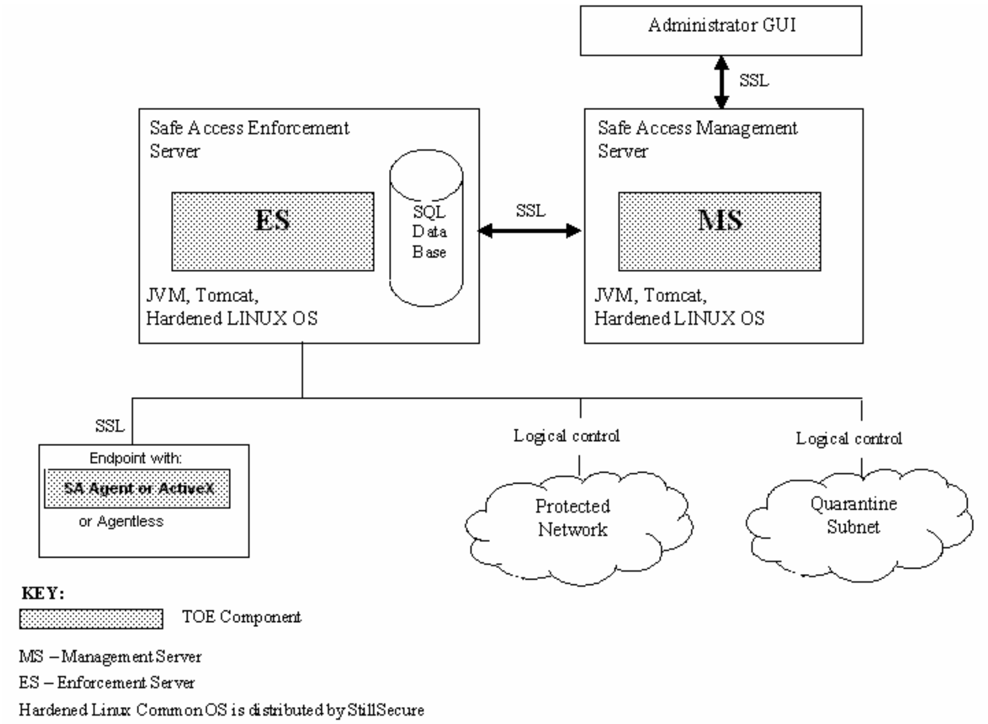

Figure 2-1 Safe Access Server Components and Logical Relationship to the Network Components

Figure 2-1 shows the TOE components installed on two servers, where the server hosting the ES has control over the endpoint's access to the protected network. The MS component of the TOE supports an interface to the Administrative user secured in the IT environment via HTTPS/SSL and supported in the IT environment by Tomcat and the JVM. Through an encrypted channel supported by the IT environment, the MS TOE component access data stored in the Postgre SQL database and also configures the ES TOE component. The MS also access the stillsecure.com web site under the control of the TOE administrator to download rules, reports, upgrades, and license data. The ES component of the TOE communicates with the endpoint via HTTPS/SSL and supported in the IT environment by Tomcat and the JVM if the Agent or ActiveX control based test methods are selected. An unencrypted connection to the endpoint is used if the RPC based test method is selected. When the inline or DHCP enforcement method has been selected, the Safe Access acts a Layer 2 bridge and captures packets and then conditionally drops or transmits the packet to the destination endpoint. The OS for the endpoint and the Administrator GUI is Windows XP.

The MS component includes a programmable API that through the JMS message bus can be utilized to publish and receive events to/from the StillSecure® VAM™, which is available separately and is not delivered with the Safe Access product. This product feature is "off" by default in that the product is configured out-of-the-box to disallow the publication of events to the JMS bus and the iptables firewall is configured to block external servers attempting to send requests to or receive requests from the JMS message bus. This interface is not included in the evaluated configuration.

The choice of testing method of the endpoint for compliance with the NAC SFP is not depicted in Figure 2-1. The endpoint can be tested using an ActiveX control, RPC calls, or the Safe Access Agent. All three testing present a simple command line like interface to the ES, thru which the endpoint is tested.

2.3.2 Enforcement Configurations

The TOE provides three enforcement methods: Inline, DHCP, and 802.1X, as explained in Section 2.3.2. Each enforcement method requires a separate deployed network configuration and each configuration will be tested individually. The TOE, installed on two servers, as shown in Figure 2-1, will be evaluated in the specific network configuration required for the three enforcement methods for each endpoint testing method as shown in the following three diagrams:

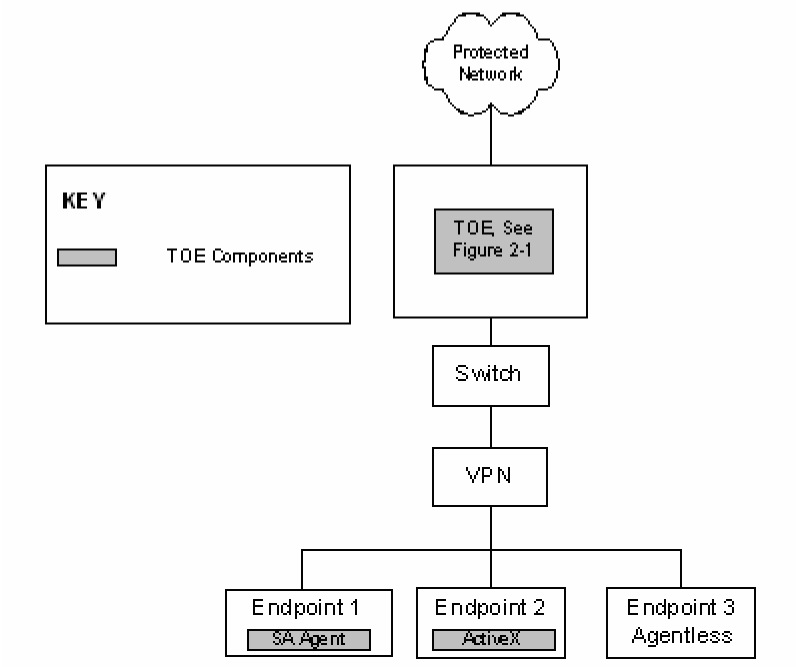

Figure 2-2 Evaluated Configuration for Inline Enforcement Method

As shown in Figure 2-2, when configured in the Inline enforcement method, Safe Access must be placed on the network where all traffic to be quarantined passes through Safe Access. It also must be inline with an endpoint like a VPN. This configuration requires that the Server 1 platform support two physically isolated network interfaces. This configuration does not support re-direction of the endpoint connection to a quarantine LAN. When configured for Inline mode, the process Safe Access follows for allowing end-users to connect is: an IP address is assigned to the endpoint outside of Safe Access. When the endpoint attempts to connect to the network, Safe Access either blocks access or allows access by not adding or adding the endpoint IP address to the internal list of network traffic to pass.

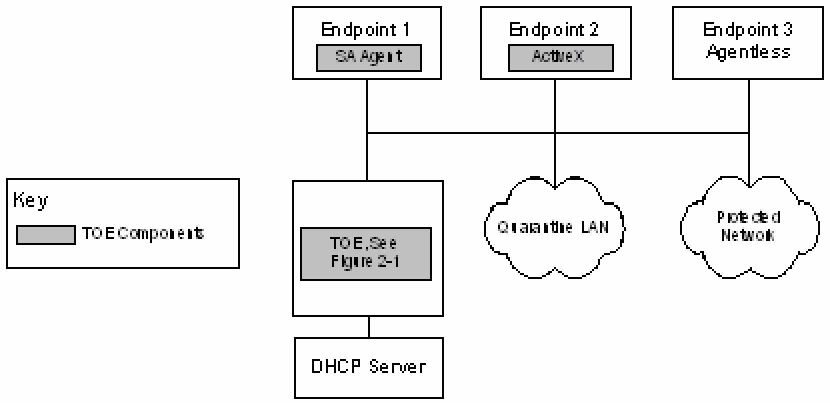

Figure 2-3 Evaluated Configuration for DHCP Enforcement Method

As shown in Figure 2-3, when configured with a DHCP enforcement method, Safe Access must sit inline with the DHCP server. All endpoints requesting a DHCP IP address are issued a temporary address on a quarantine subnet by the TOE. Once the endpoint is allowed access, the IP address is renewed, and the main DHCP server assigns an address to the main LAN. With a multiple subnet or VLAN network, a distinct quarantine area must be configured for each sub-network. This configuration requires that the Server 1 platform support two physically isolated network interfaces. When configured for DHCP mode, a new end-user first boots their endpoint (computer). As part of initializing the network connections, the OS boot process looks for an IP address. This request is intercepted by Safe Access. Because the user is new no information is known about the endpoints, and a temporary quarantined IP address is assigned. After the user has authenticated with the endpoint, Safe Access attempts to test the endpoint, and based on the test result the endpoint either retains the quarantined IP address or are assigned the protected network IP address by the DHCP server.

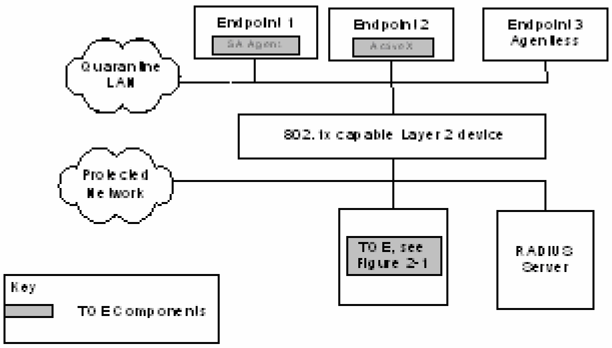

Figure 2-4 Evaluated Configuration for 802.1X Enforcement Method

As shown in Figure 2-4, when using the 802.1X enforcement method, Safe Access must sit in a place on the network where it can communicate with the RADIUS server, which communicates with the Layer 2

802.1X device (i.e.: a switch or router), which performs the quarantining. When Safe Access and the host network are configured for 802.1X mode, an endpoint attempting to connect to the network is directed to the authentication server by the 802.1X capable Layer 2 device and end user's identity is verified by an authentication (RADIUS) server. If the end user's identity is not authenticated, the endpoint is quarantined (allowed access to a limited VLAN) by the 802.1X compatible Layer 2 device. If the endpoint is authenticated by the authentication server, the endpoint is next tested by Safe Access. If the endpoint fails the Safe Access testing, the 802.1X capable Layer 2 device is configured to quarantine the endpoint (allowed access to a limited VLAN). Otherwise (if the endpoint passes the Safe Access testing) it is allowed access to the protected network (VLAN).

2.3.3 The TOE does not include the following IT Environment Components:

- Hardware platform(s) for all product components
- Cryptographic module(s): SSL implementation on all platforms
- Internet Browser (e.g.: Internet Explorer, Mozilla Firefox)

These IT Environment components are not included in the TOE, but have an interface to the TOE that is included in the evaluation:

- Operating System platform(s) for all product components
- Transport standards HTTP, HTTPS, and FTP implementations
- Network or other connectivity: (Trusted Ethernet network)
- Third party relational database (PostgreSQL) and its interface
- Firewall installed on the ES platform
- Tomcat Server
- JVM
- Safe Access API, which supports an interface to an external server for the purpose of communicating events.

The high availability and load balancing functions of Safe Access are not claimed or tested as part of the evaluation.

2.4 *Logical Boundary*

The logical boundary of the TOE will be broken down into the following security class features which are further described in sections 5 and 6. StillSecure Safe Access provides the following security features:

- **Security audit** – StillSecure Safe Access provides its own internal auditing capabilities separate from those of the Operating System. StillSecure Safe Access provides the ability to search and view its own audit records.
- **Network Access Control** – StillSecure Safe Access provides user data protection by enforcing, default or administrator defined NAC policy on endpoints accessing the protected network. StillSecure Safe Access tests all endpoints for compliance and grants or denies access to the protected network based on test results.
- **Identification and authentication** – StillSecure Safe Access provides TOE user identification and authentication through the use of user accounts and passwords.
- **Security management** – StillSecure Safe Access provides security management through the Management Server's Web-based console and by reporting the endpoint compliance and access activity. Also, the TOE provides two administrative roles (FMT_SMR.1).
- **Protection of TSF** – StillSecure Safe Access partially protects its programs and data from unauthorized access through its own interfaces.
- **StillSecure Safe Access Reporting -** Safe Access provides a provision for Safe Access users with the necessary privileges to generate and view reports providing security status information on endpoint compliance and access activity. System administrators can operate on the reports

pertaining to all clusters. Cluster administrator, Help desk technician, and User defined role with explicitly assigned privilege can operate on the reports pertaining to their own clusters..

- **Trusted Path/Channel usage** – The TOE makes use of trusted paths and channel supported in the IT environment.

2.5 *TOE Security Environment*

It is assumed that there will be no untrusted users or software on the StillSecure Safe Access hosts. StillSecure Safe Access relies upon the underlying operating system[2] and platform to provide reliable time stamps and to protect the StillSecure Safe Access Server host from other interference or tampering. StillSecure Safe Access relies on a Web Server to provide web services. The TOE environment is one where the potential attacker is unsophisticated, with access to only standard equipment and public information about the product.

The TOE security environment can be categorized as follows:

- **Security Audit –** StillSecure Safe Access relies on the IT environment to protect the audit records from unauthorized modifications and deletions.
- **Protection of TSF –** StillSecure Safe Access relies on the underlying OS to provide security capabilities for the TOE's protection. For the TOE's own protection the OS includes requirements that relate to the integrity of the TSF. These include SFP domain separation, reliable time-stamp, and Non-bypassability of the TSP.
- **Network Devices and Services –** These include DHCP servers, RADIUS servers, 802.1X capable Layer 2 device and Windows RPC service.
- **iptables Firewall installed on ES platform–** If configured for the DHCP and Inline enforcement method, the firewall installed with the product on the ES platform quarantines packets based on MAC address.
- **Reliable Time Stamps –** The OS and Hardware are being relied on for reliable time stamps.

[2] Safe Access is provided with the CommonOS operating system (a hardened Linux OS) created and maintained by StillSecure. The CommonOS is hardened by employing the following controls:

- Packages – The number and contents of packages present on the system are thoroughly inspected and tightly controlled.
- Firewall – An on-board firewall restricts outside connections to only secure services (encrypted traffic) on specific ports.
- Network parameters – Certain types of dangerous or unnecessary network services are disabled. Other undesirable traffic is reduced or eliminated.

3 TOE Security Environment

This section identifies secure usage assumptions and threats to security. There are no organizational security policies.

3.1 *Assumptions*

This section contains assumptions regarding the security environment and the intended usage of the TOE.

Table 3-1: Assumptions for the IT Environment

Item	Assumption Name	Description
1	A.AdmTra	Administrators and operators are non-hostile, appropriately trained and follow all administrative guidance, including guidance on setting passwords.
2	A.Env	Administrators will ensure that the environment has adequate facility to provide disk storage and other capabilities for the TOE's protection.
3	A.Low	The attack potential on the TOE is assumed to be low.
4	A.NoUntrusted	It is assumed that there will be no untrusted users and no untrusted software on the StillSecure Safe Access Server host which hosts the Management Server and the Enforcement Servers
5	A.Physical	Physical protection is assumed to be provided by the environment. The TOE hardware and software is assumed to be protected from unauthorized physical access.
6	A.ProtectComm	Those responsible for the TOE will ensure the communications between the Administrator PC and StillSecure Safe Access Server host are secure.
7	A.Users	It is assumed that authorized users will protect their authentication data.

3.2 *Threats*

The TOE itself has threats and the TOE is also responsible for addressing threats to the environment in which it resides. The assumed level of expertise of the attacker is unsophisticated, with access to only standard equipment and public information about the product.

The TOE must counter the following threats to security:

Table 3-2: Threats

Item	Threat	Threat Description
1	T.Bypass	An attacker may attempt to bypass TSF security functions to gain unauthorized access to TSF.
2	T.Vul	The TOE may fail to identify non-compliant endpoints.
3	T.Mismanage	Authorized administrators may make errors in the management of security functions and TSF data. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE.
4	T.Privil	An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data.
5	T.Tamper	An attacker may attempt to modify TSF programs and data.
6	T.Undetect	Attempts by an attacker to violate the security policy may go undetected. If the attacker is successful, TSF data may be lost or altered.

4 Security Objectives

4.1 *Security Objectives for the TOE*

The security objectives for the TOE are as follows:

Table 4-1: TOE Objectives

Item	Objective	Objective Description
1.	O.Access	The TOE will provide its authorized users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of user roles.
2.	O.Admin	The TOE will include a set of functions that allow effective management of its functions and data.
3.	O.Audit	The TOE will record audit records for data accesses and use of the TOE functions and will ensure protection of the audit storage.
4.	O.IDAuth	The TOE will be able to identify and authenticate users prior to allowing access to TOE functions and data.
5.	O.IDScan	The TOE will collect and store system data from the endpoints on the target network and will enforce the NAC security policy on them.
6.	O.PartialNonBypass	The TOE will ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed.
7.	O.PartialSelfProtection	The TSF when invoked by the underlying host OS, will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorised disclosure, through its own interfaces.
8.	O.ProtectAuth	The TOE will provide protected authentication.
9.	O.Revoke	The TOE will allow administrators to revoke privileges of users.
10.	O.Roles	The TOE will support multiple roles.

4.2 *Security Objectives for the Environment*

4.2.1 Security Objectives for the IT Environment

The security objectives for the IT environment are as follows:

Table 4-2: IT Environment Objectives

Item	Environment Objective	Environment Objective Description
11.	OE.AuditProtect	The IT environment will ensure the protection of the audit storage.
12.	OE.NonBypass	The IT environment will ensure that its protection mechanisms cannot be bypassed.
13.	OE.PartialSelfProtection	The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces.
14.	OE.Time	The underlying operating system will provide reliable time stamps.
15.	OE.IDScan	The IT environment will support the scanning of endpoints and enforcement of the NAC security policy.

4.2.2 Security Objectives for Non-IT Security Environment

The Non-IT security objectives are as follows:

Table 4-3: Non-IT Environment Objectives

Item	Non-IT Environment Objective	Non-IT Environment Objective Description
16.	ON.Install	Those responsible for the TOE will ensure that the TOE is delivered and installed in a manner that maintains IT security.
17.	ON.Low	Those responsible for the TOE will ensure that the TOE is in an environment where there is only a low attack potential.
18.	ON.NoUntrusted	The administrator will ensure that there are no untrusted users and no untrusted software on the StillSecure Safe Access Server host.
19.	ON.Operations	The TOE will be managed and operated in a secure manner as outlined in the supplied guidance.
20.	ON.ProtectAuth	Users will ensure that their authentication data is held securely and not disclosed to unauthorized persons.
21.	ON.ProtectComm	Those responsible for the TOE will ensure that communications between the Administrator PC and StillSecure Safe Access Server host are secure.
22.	ON.Person	Authorized administrators shall be carefully selected and trained for proper operation of the system.
23.	ON.Physical	Those responsible for the TOE will ensure that those parts of the TOE critical to the security policy are protected from any physical attack.

5 IT Security Requirements

This section provides the TOE security functional and assurance requirements. In addition, the IT environment security functional requirements on which the TOE relies are described. These requirements consist of functional components from Part 2 of the CC, explicit functional components derived from the CC Part 2, and assurance components from Part 3 of the CC.

5.1 Formatting Conventions

The notation, formatting, and conventions used in this security target (ST) are consistent with version 2.3 of the Common Criteria for Information Technology Security Evaluation. Font style and clarifying information conventions were developed to aid the reader.

The CC permits four functional component operations: assignment, iteration, refinement, and selection to be performed on functional requirements. These operations are defined in Common Criteria, Part 1, section 4.4.1.3.2 as:

- assignment: allows the specification of an identified parameter;
- refinement: allows the addition of details or the narrowing of requirements;
- selection: allows the specification of one or more elements from a list; and
- iteration: allows a component to be used more than once with varying operations.

This ST indicates which text is affected by each of these operations in the following manner:

- *Assignments* and *Selections* specified by the ST author are in **[*italicized bold text*]**.
- *Refinements* are identified with "**Refinement:**" right after the short name. Additions to the CC text are specified in ***<u>italicized bold and underlined text</u>***.
- *Iterations* are identified with a dash number "-#". These follow the short family name and allow components to be used more than once with varying operations. "-*" refers to all iterations of a component.
- *Explicitly Stated Requirements* will be noted with a "_EXP" added to the component name.
- *Application notes* provide additional information for the reader, but do not specify requirements. Application notes are denoted by *italicized text.*

5.2 TOE Security Functional Requirements

The functional security requirements for the TOE consist of the following components derived from Part 2 of the CC and explicit components derived from Part 2 of the CC, summarized in the Table 5-1: below.

Table 5-1: Functional Components

Item	Component	Component name
1.	FAU_GEN.1	Audit data generation
2.	FAU_GEN.2	User identity association
3.	FAU_SAR.1	Audit review
4.	FAU_SAR.3	Selectable audit review
5.	FAU_STG_EXP.1-1	Protected audit trail storage
6.	FDP_ACC.1	Subset access control
7.	FDP_ACF.1	Security attribute based access control
8.	FDP_ACC_8021X_EXP.1-1	Partial subset access control
9.	FDP_ACF_8021X_EXP.1-1	Partial security attribute based access control
10.	FDP_ACC_BRIDGE_EXP.1-1	Partial subset access control
11.	FDP_ACF_BRIDGE_EXP.1-1	Partial security attribute based access control

Item	Component	Component name
12.	FIA_ATD.1	User attribute definition
13.	FIA_UAU.2	User authentication before any action
14.	FIA_UAU.7	Protected authentication feedback
15.	FIA_UID.2	User identification before any action
16.	FMT_MSA.3	Static attribute initialization
17.	FMT_MTD.1	Management of TSF data
18.	FMT_SMR.1	Security roles
19.	FMT_SMF.1	Specification of management functions
20.	FPT_RVM_EXP.1-1	Non-bypassability of the TSP
21.	FPT_SEP_EXP.1-1	TSF domain separation
22.	FSR_SRG_EXP.1	StillSecure report generation
23.	FSR_SRR_EXP.1	StillSecure report review
24.	FTP_TRP_EXP.1-1	Partial trusted channel

5.2.1 Class FAU: Security Audit

FAU_GEN.1 Audit data generation

Hierarchical to: No other components.

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:***

- ***change in access control states of endpoints for the following endpoint states:***
  - Quarantined
  - Quarantined by exception
  - Temporarily quarantined until XX/XX/XX at HH:MM pm
  - Granted access
  - Granted access by exception
  - Has temporary access until XX/XX/XX at HH:MM pm (by admin)
  - Has temporary access until XX/XX/XX at HH:MM pm (by NAC policy)
  - Disconnected or Error

- ***change in test status of endpoints for the following endpoint status states:***
  - Unknown error
  - Connecting
  - Awaiting credentials
  - Bad credentials
  - Testing (agentless test)
  - Pass
  - Fail
  - Could not be tested
  - License limit exceeded
  - License expired
  - Test canceled
  - Access always allowed
  - Access always quarantined
  - Awaiting test initiation

- Installing test service
- Install canceled
- Testing (installed test)
- Testing (one-time test)
- Installing one-time plug-in
- One-time plug-in installation failed
- Validating install
- Install failed
- Agent not active
- Awaiting IP transition
- Connection failed - endpoint busy or file and print sharing disabled
- Connection failed - unsigned SMB
- Connection failed - endpoint/domain trust failure
- Connection failed - timed out
- Connection failed - session setup
- Test failed - insufficient test privileges
- Connection failed - no route to host, and
- Endpoint disconnected before could be tested

]

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, 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*]**

Dependencies: FPT_STM.1 Reliable time stamps

FAU_GEN.2 User identity association

Hierarchical to: No other components.

FAU_GEN.2.1 The TSF shall be able to associate each auditable event with the identity of the user that caused the event.

Dependencies: FAU_GEN.1 Audit data generation
FIA_UID.1 Timing of identification

FAU_SAR.1 Audit review

Hierarchical to: No other components.

FAU_SAR.1.1 The TSF shall provide **[*cluster administrator, View-Only user, System Administrator, Help Desk Technician and a user with explicitly assigned privilege*]** with the capability to read **[*all audit 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.

Dependencies: FAU_GEN.1 Audit data generation

FAU_SAR.3 Selectable audit review

Hierarchical to: No other components

FAU_SAR.3.1 The TSF shall provide the ability to perform ***[searches]*** of audit data based on ***[access control, test status, time, cluster, NetBIOS Name, IP address, user ID, windows domain, NAC policy, MAC address and operating system]***

Dependencies: FAU_SAR.1 Audit review

FAU_STG_EXP.1-1 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG_EXP.1.1-1 The TSF shall protect the stored audit records in the audit trail from unauthorized deletion initiated through its own TSFI.

FAU_STG_EXP.1.2-1 The TSF shall be able to prevent unauthorized modifications to the audit records in the audit trail initiated through its own TSFI.

Dependencies: FAU_GEN.1 Audit data generation

5.2.2 Class FDP: User Data Protection

FDP_ACC.1 Subset access control

FDP_ACC.1.1 The TSF shall enforce the **[*NAC SFP*]** on **[*subjects: endpoints, objects: network domain, and operations: connect, quarantine, disconnect*]**

Dependencies: FDP_ACF.1 Security attribute based access control

FDP_ACF.1 Security attribute based access control

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

Subjects: endpoints

Subject security attributes:

- ***Test Status State***
- ***Access Control State***

Objects: network domains

Object security attributes:

- ***Associated enforcement cluster***
- ***Access Mode (Normal Operation, Quarantine All, Allow All)***
- ***Test method (Agentless testing, ActiveX, StillSecure Agent)***
- ***Temporarily quarantine/temporarily grant access settings***
- ***Exceptions by endpoint***
    - ***i. Endpoints to always grant access and never test***
    - ***ii. Endpoints to always quarantine and never test***
- ***Associated access control policy]***

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

1. ***An access control policy has the following configuration options:***
    - ***Name of policy***
    - ***NAC policy group***
    - ***Enabled or disabled***
    - ***Unsupported operating systems that will be allowed access without testing***

- ***Retest Frequency***
- ***Inactivity period (time allowed before an inactive endpoint is disconnected)***
- ***Tests to be run on an endpoint before it is allowed to connect to the network.***
  - ***Tests are divided into the following categories: security settings, software, operating system, and browser security policy***
  - ***The following administrator configuration actions may be taken if a test fails: grant temporary access, temporarily quarantine, send email notification***

2. ***Checks to determine whether to grant access or quarantine are made in the following order:***

- ***Access mode (normal operation, quarantine all, or allow all). Set for a cluster.***
- ***Temporarily quarantine/temporarily grant access settings. Set to temporarily override endpoint test exceptions or test results by temporarily granting access to or quarantining a endpoint for a specified time period.***
- ***Endpoint testing exceptions (always grant access, always quarantine)***
- ***NAC policies.***

3. ***If an endpoint is quarantined, it may still access the specified accessible services.***

4. ***If the endpoint testing method is Agentless testing or Agent-based testing and the Retest Frequency interval has elapsed checks to determine whether to permit the endpoint to stay connected, or be disconnected are run in the following order:***

- ***Access mode (normal operation, quarantine all, or allow all). Set for a cluster.***
- ***Temporarily quarantine/temporarily grant access settings. Set to temporarily override endpoint test exceptions or test results by temporarily granting access to or quarantining a endpoint for a specified time period.***
- ***Endpoint testing exceptions (always grant access, always quarantine)***
- ***NAC policies.*** **]**

FDP_ACF.1.3 The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: **[**

1. ***If Access Control Policy is Low, Medium, or High Security setting then***

- ***test category (Anti-Virus, etc.)***
- ***With test property (Tools used to determine the compliance state for the test category)***

2. ***if the tests for the specified default access control policy pass, the TSF shall allow the endpoint to connect.***

3. ***If the Low Security Policy is associated with the network enforcement cluster fails then***

- ***The TSF shall enforce quarantining of the endpoint***

- ***The TSF shall grant the endpoint temporary access of the network for 7 days when all critical service packs and hot fixes are not installed.***

4. If the Medium Security Policy is associated with the network enforcement cluster fails then

- ***The TSF shall enforce quarantining of the end-user***
- ***The TSF shall grants the endpoint temporary access to the network for 3 days when all critical service packs and hot fixes are not installed or anti-virus software is not installed.***
- ***If the High Security Policy is associated with the network enforcement cluster fails, the TSF shall enforce quarantining of the endpoint until compliant to the security policy.***

Application Note: For the default policies, the determination of compliancy to the Low, Medium, High access control policy is based on StillSecure's paid subscription updates.

***5. The TSF shall also provide the capability for the authorized administrator to define custom NAC policies*].**

FDP_ACF.1.4 The TSF shall explicitly deny access of subjects to objects based on the following rules: **[*no additional rules*]**.

Dependencies: FMT_MSA.3 Static attribute initialisation,
FDP_ACC.1 Subset access control,
FPT_IDSCAN_EXP.1 Endpoint scan

FDP_ACC_8021X_EXP.1-1 Partial subset access control

FDP_ACC_8021X_EXP.1.1-1 The TSF in conjunction with the IT Environment shall enforce the NAC SFP in accordance to SFR FDP_ACC.1.

Dependencies: FDP_ACF_8021X_EXP.1-1 Partial security attribute based access control
FDP_ACC_8021X_EXP.1-2 Partial security attribute based access control

Application Note: This SFR applies when the TOE is configured to use an 802.1X capable network device in the IT environment.

FDP_ACF_8021X_EXP.1-1 Partial Security attribute based access control

FDP_ACF_8021X_EXP.1.1-1 The TSF in conjunction with the IT Environment shall enforce the NAC SFP in accordance to SFR FDP_ACF.1.

Dependencies: FDP_ACC_8021X_EXP.1-1 Partial subset access control,
FDP_ACF_8021X_EXP.1-1 Partial subset access control

Application Note: This SFR applies when the TOE is configured to use an 802.1X capable network device in the IT environment.

FDP_ACC_BRIDGE_EXP.1-1 Partial subset access control

FDP_ACC_BRIDGE_EXP.1.1-1 The TSF in conjunction with the IT Environment shall enforce the NAC SFP in accordance to SFR FDP_ACC.1.

Dependencies: FDP_ACF_BRIDGE_EXP.1-1 Partial security attribute based access control
FDP_ACC_BRIDGE_EXP.1-2 Partial security attribute based access control

Application Note: This SFR applies when the TOE is configured to use an inline or DHCP enforcement control.

FDP_ACF_BRIDGE_EXP.1-1 Partial Security attribute based access control

FDP_ACF_BRIDGE_EXP.1.1-1 The TSF in conjunction with the IT Environment shall enforce the NAC SFP in accordance to SFR FDP_ACF.1.

Dependencies: FDP_ACC_BRIDGE_EXP.1-1 Partial subset access control
FDP_ACF_BRIDGE_EXP.1-2 Partial subset access control

Application Note: This SFR applies when the TOE is configured to use an inline or DHCP enforcement control.

5.2.3 Class FIA: Identification and Authentication

FIA_ATD.1 User attribute definition

Hierarchical to: No other components.

FIA_ATD.1.1 The TSF shall maintain the following list of security attributes belonging to individual users:

- **[*User ID;***
- ***Password;***
- ***Full name;***
- ***Email address;***
- ***Account status;***
- ***User role;***
- ***Enabled/disabled;***
- ***Accessible cluster(s)*]**

Dependencies: No dependencies.

FIA_UAU.2 User authentication before any action

Hierarchical to: FIA_UAU.1

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.

Dependencies: FIA_UID.1 Timing of identification

FIA_UAU.7 Protected authentication feedback

Hierarchical to: No other components.

FIA_UAU.7.1 The TSF shall provide only **[*a display of the typed in user name and asterisks for the password for password-based authentication*]** to the user while the authentication is in progress.

Dependencies: FIA_UAU.1 Timing of authentication

FIA_UID.2 User identification before any action

Hierarchical to: FIA_UID.1

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

Dependencies: No dependencies.

5.2.4 Class FMT: Security Management

FMT_MSA.3 Static attribute initialization

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

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

Dependencies: FMT_MSA.1 Management of security attributes
FMT_SMR.1 Security roles

FMT_MTD.1 Management of TSF data

Hierarchical to: No other components.

FMT_MTD.1.1 The TSF shall restrict the ability to **[*change_default, query, modify, delete,* [*and other operations as specified in Table 5-2*]]** the **[*TSF Data as specified in Table 5-2*]** to **[*the role as specified as Authorized Role in Table 5-2*].**

Dependencies: FMT_SMR.1 Security roles
FMT_SMF.1 Specification of Management Functions

Table 5-2: Management of TSF Data

Security Function	Operation	TSF data	Authorized Role	Notes
Security Audit	Query	all audit data	System Administrator.	
Identification and Authentication	Query, add, modify, disable and delete	user account name	System Administrator.	System Administrators manage user accounts
Security Management	Add, Delete	Agentless Credentials	System Administrator or a User-defined role with explicitly granted privilege.	Can provide agentless end-user login information
Security Management	Create and modify	permissions	System Administrators or a User-defined role with Configure cluster settings **, Configure servers, and Configure the system privileges.	Create custom policies that are based on existing policies, or new policies from scratch. The assigned permission are cluster administrator, view-only user, system administrator, help desk technician and a user with explicitly assigned privilege
Security Management	Query, create, modify, and delete	NAC policies	System Administrator.	System Administrators can operate on the TSF data pertaining to all clusters

Security Function	Operation	TSF data	Authorized Role	Notes
Security Management	Query, create, modify, and delete	NAC policies within the cluster	Cluster Administrator or a User-defined role with Configure cluster settings **, Configure servers, Configure the system, and Manage NAC policies privileges.	Cluster Administrators and user with explicitly assigned privilege can operate on the TSF data pertaining to their own cluster.
Security Management	Query	Endpoint activity	System administrator	System Administrators can operate on the TSF data pertaining to all clusters.
Security Management	Query	Endpoint activity with the cluster	Cluster administrator, help desk technician, and user-defined role with the Retest endpoints privilege.	Cluster Administrators, help desk technicians, and user with explicitly assigned privilege can operate on the TSF data pertaining to their own clusters.
Security Management	Enable, disable	Email notifications	System Administrator or a User-defined role with explicitly granted privilege.	
NAC	Query, modify	Endpoint access control information	System Administrator	System Administrators can operate on the TSF data pertaining to all clusters
NAC	Query, modify	Endpoint access control information within the cluster	Cluster administrator, help desk technician and a user defined role with the Control Access privilege.	Cluster Administrators, view-only users, and help desk technicians can operate on the TSF data pertaining to their own cluster
NAC	Enable, disable,	Automatic test updates	System Administrator.	System Administrators can operate on the TSF data pertaining to all clusters
NAC	Run	Manual test updates	System Administrator.	System Administrators can operate on the TSF data pertaining to all clusters
StillSecure Security Status Reporting	Run, View	Reports about the security status on endpoint compliance and access activity	System administrator, Cluster administrator, View only, Help desk technician, and User defined role with the Generate reports, View endpoint activity, and Monitor system status privileges.	System Administrators can operate on the reports pertaining to all clusters. Cluster administrator, Help desk technician, and User defined role with explicitly assigned privilege can operate on the reports pertaining to their own clusters.

*Application Note: ** Please see Chapter 3 of the StillSecure SA User Guide for more information on Cluster settings.*

FMT_SMR.1 Security roles

Hierarchical to: No other components.

FMT_SMR.1.1 The TSF shall maintain the roles ***[Cluster Administrator, View-Only user, System Administrator, Help Desk Technician, User Defined Role].***

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

Dependencies: FIA_UID.1 Timing of identification

FMT_SMF.1 Specification of Management Functions

Hierarchical to: No other components.

FMT_SMF.1.1 The TSF shall be capable of performing the following security management functions: **[*change_default, query, modify, delete, and other operations as specified on the "Operation" column in Table 5-2 on the "TSF Data" as specified in Tables 5-2 (see FMT_MTD.1)*].**

Dependencies: No dependencies.

5.2.5 Class FPT: Protection of the TOE Security Functions

FPT_RVM_EXP.1-1 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM_EXP.1.1-1 The TSF, when invoked by the underlying host OS, shall ensure that TSP enforcement functions are invoked and succeed before each function within the TSC is allowed to proceed.

Dependencies: No dependencies.

FPT_SEP_ EXP.1-1 TSF domain separation

Hierarchical to: No other components.

FPT_SEP_ EXP.1.1-1 The TSF, when invoked by the underlying host OS, shall maintain a security domain that protects it from interference and tampering by untrusted subjects in the TSC.

FPT_SEP_ EXP.1.2-1 The TSF, when invoked by the underlying host OS, shall enforce separation between the security domains of subjects in the TSC.

Dependencies: No dependencies.

5.2.6 Class FSR: StillSecure Security Status Reporting

FSR_SRG_EXP.1 StillSecure report generation

Hierarchical to: No other components

FSR_SRG_EXP.1.1 The TSF shall be able to generate reports about the security status on endpoint compliance and access activity.

FSR_SRG_EXP.1.2 The TSF shall be able of generating the following reports:

- NAC Policy Results
- Endpoint List
- Test Details
- Test Results
- Test Results by IP address
- Test Results by NetBIOS name
- Test Results by user.

Dependencies: No dependencies.

FSR_SRR_EXP.1 StillSecure report review

Hierarchical to: No other components

FSR_SRR_EXP.1.1 The TSF shall provide system administrator, cluster administrator, help desk technician and user defined role with the View endpoint activity and Monitor system status privileges with the capability to view reports about the security status on endpoint compliance and access activity.

FSR_SRR_EXP.1.2 The TSF shall provide the reports in a manner suitable for the user to interpret the information.

Dependencies: FSR_SRG_EXP.1

5.2.7 Class FTP: Trusted Path/channels

FTP_TRP_EXP.1-1 Partial trusted channel

Hierarchical to: No other components.

FTP_TRP_EXP.1.1-1 The TSF shall provide a communication path between itself and remote and local users that is logically distinct from other communication paths and relies on the IT environment to provide protection of the trusted channel from modification or disclosure using HTTPS/SSL.

FTP_TRP_EXP.1.2-1 The TSF shall permit the local users and remote users to initiate communication with the TSF via the trusted channel.

FTP_TRP_EXP.1.3-1 The TSF shall require the use of the trusted channel for initial user authentication and all communication between TOE and its users.

FTP_TRP_EXP.1.4-1 The TSF shall provide a communication path between the TSF components that is logically distinct from other communication paths and relies on the IT environment to provide protection of the trusted channel from modification or disclosure using HTTPS/SSL.

FTP_TRP_EXP.1.5-1 The TSF shall provide a communication path between the TSF and the remote StillSecure update and upgrade web site that is logically distinct from other communication paths and relies on the IT environment to provide protection of the trusted channel from modification or disclosure using HTTPS/SSL.

Dependencies: FTP_TRP_EXP.1-2

5.2.8 Strength of Function

The overall strength of function requirement is SOF-basic. IA-2 User Authentication before any action, is realized by probabilistic or permutational mechanisms. The methods used to provide difficult-to-guess passwords are probabilistic. The specific password policy is specified as the following:

- Minimum length of 8,
- At least one special character,
- At least one numeric character,
- At least one uppercase and one lowercase character
- Must not be a common word, a word in any existing password dictionaries, or a word easily guessed (such as "password").

The SOF claim for IA-2 is SOF-basic.

5.3 Security requirements for the IT Environment

StillSecure Safe Access requires that the operating system platform provide reliable time stamps. StillSecure Safe Access requires that the operating system provides TSF domain separation and Non-Bypassability.

Table 5-3: Functional Components for the IT environment

No.	Component	Component Name
1.	FAU_STG_EXP.1-2	Protected audit trail storage
2.	FDP_ACC_8021X_EXP.1-2	Partial Subset access control
3.	FDP_ACF_8021X_EXP.1-2	Partial security attribute based access control
4.	FDP_ACC_BRIDGE_EXP.1-2	Partial Subset access control
5.	FDP_ACF_BRIDGE_EXP.1-2	Partial Security attribute based access control
6.	FIA_UAU_8021X_EXP.1	Timing of authentication
7.	FIA_UID_8021X_EXP.1	Timing of identification
8.	FPT_IDSCAN_EXP.1	Endpoint scan
9.	FPT_RVM_EXP.1-2	Non-bypassability of the TSP
10.	FPT_SEP_EXP.1-2	TSF domain separation
11.	FPT_STM.1	Reliable time stamps
12.	FTP_TRP_EXP.1-2	Partial trusted channel

5.3.1 Class FAU: Security Audit

FAU_STG_EXP.1-2 Protected audit trail storage

Hierarchical to: No other components.

FAU_STG_EXP.1.1-2 The IT Environment shall protect the stored audit records in the TSF audit trail from unauthorised deletion initiated through the IT Environment's Interfaces.

FAU_STG_EXP.1.2-2 The IT Environment shall be able to prevent unauthorised modifications to the audit records in the TSF audit trail initiated through the IT Environment's Interfaces.

Dependencies: FAU_GEN.1 Audit data generation

5.3.2 Class FDP: User Data Protection

FDP_ACC_8021X_EXP.1-2 Partial Subset access control

FDP_ACC_8021X_EXP.1.1-2 The IT Environment shall provide support for the 802.1X portion of the NAC SFP on subjects: endpoints, objects: network domains, and operations: receive packet and transmit packet in accordance to FDP_ACC.1 with 802.1X authentication and VLAN functionality as the enforcement method in conjunction with the TSF.

Dependencies: FDP_ACF_8021X_EXP.1-2 Partial security attribute based access control

Application Note: See StillSecure User Guide Chapter 11 for 802.1X details.

FDP_ACF_8021X_EXP.1-2 Partial Security attribute based access control

FDP_ACF_8021X_EXP.1.1-2 The IT Environment, in conjunction with the TSF, shall enforce the 802.1X portion of the NAC SFP on

subjects: endpoints,

subject security attributes:

- Radius Authentication credentials
- MAC address of Endpoint

objects: network,

object security attributes:

- network port

and operations:

- receive packet,
- transmit packet

operations security attributes:

- Endpoint Radius Authentication credentials
- Source/destination MAC address of packet

FDP_ACF_8021X_EXP.1.2-2 The IT Environment shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a) the subject is an endpoint, the operation is transmit packet, and the operation is allowed or disallowed based upon the source MAC address and the authentication credentials specified in the RADIUS server;

b) the subject is an network domain, the operation is receive packet, and the operation is allowed or disallowed based upon destination MAC address and the authentication credentials specified in the RADIUS server;

Dependencies: FDP_ACC_8021X_EXP.1-2 Partial subset access control

FDP_ACC_BRIDGE_EXP.1-2 Partial Subset access control

FDP_ACC_BRIDGE_EXP.1.1-2 The IT Environment shall provide support for the Inline and DHCP portion of the NAC SFP on subjects: endpoints, objects: network domains, and operations: receive packet and transmit packet in accordance to FDP_ACC.1 with Inline or DHCP as the enforcement method in conjunction with the TSF.

Dependencies: FDP_ACF_BRIDGE_EXP.1-2 Partial security attribute based access control

Application Note: See StillSecure User Guide Chapter 8 for Inline enforcement method details and Chapter 9 for DHCP enforcement method details.

FDP_ACF_BRIDGE_EXP.1-2 Partial Security attribute based access control

FDP_ACF_BRIDGE_EXP.1.1-2 The IT Environment, in conjunction with the TSF, shall enforce the 802.1X portion of the NAC SFP on

subjects: endpoints,

subject security attributes:

- Access Control State
- Test Status State

- MAC address of Endpoint

objects: network,

object security attributes:

- network port

and operations:

- receive packet,
- transmit packet

operations security attributes:

- Source/destination MAC address of packet

FDP_ACF_BRIDGE_EXP.1.2-2 The IT Environment shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed:

a) the subject is an endpoint, the operation is transmit packet, and the operation is allowed based upon the source MAC address and the access control and test status state in the Enforcement server;

b) the subject is an network domain, the operation is receive packet, and the operation is allowed based upon the destination MAC address and the access control and test status state in the Enforcement server;

Dependencies: FDP_ACC_BRIDGE_EXP.1-2 Partial subset access control

5.3.3 Class FIA: Identification and Authentication

FIA_UAU_8021X_EXP.1 Timing of authentication

Hierarchical to: No other components.

FIA_UAU_8021X_EXP.1.1 The IT Environment shall allow the passing of authentication data through the 802.1X device to and from the RADIUS server on behalf of the endpoint user to be performed before the user is authenticated.

FIA_UAU_8021X_EXP.1.2 The IT Environment shall require each endpoint user to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.

FIA_UID_8021X_EXP.1 Timing of identification

Hierarchical to: No other components.

FIA_UID_8021X_EXP.1.1 The IT Environment shall allow the passing of network traffic through the 802.1X device and the passing of authentication data to and from the RADIUS server on behalf of the endpoint user to be performed before the user is identified.

FIA_UID_8021X_EXP.1.2 The IT Environment shall require each endpoint user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.

5.3.4 Class FPT: Protection of the TOE Security Functions

FPT_IDSCAN_EXP.1 Endpoint scan

Hierarchical to: No other components.

FPT_IDSCAN_EXP.1.1 The IT environment shall support an interface through which endpoints may be scanned by one of the following testing methods:

a) Agentless testing method: Agentless testing using Windows RPC service on the endpoint, and with file and printer sharing enabled on the endpoint OS.

b) ActiveX-based testing method: ActiveX control based testing initiated by the end-user via a browser when the endpoint connects to the network.

c) Agent-based testing method: Safe Access Agent installed onto the endpoint.

FPT_RVM_EXP.1-2 Non-bypassability of the TSP

Hierarchical to: No other components.

FPT_RVM_EXP.1.1-2 The IT environment shall ensure that the Operating System's Security Policy enforcement functions are invoked and succeed before each function within the Operating System's Scope of Control is allowed to proceed.

FPT_SEP_EXP.1-2 TSF domain separation

Hierarchical to: No other components.

FPT_SEP_EXP.1.1-2 The IT environment shall maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects.

FPT_SEP_EXP.1.2-2 The IT environment shall enforce separation between the security domains of subjects in the Operating System's Scope of Control.

FPT_STM.1 Reliable time stamps

Hierarchical to: No other components.

FPT_STM.1.1 The ***IT environment*** shall be able to provide reliable time stamps for its own use.

Dependencies: No dependencies

5.3.5 Class FTP: Trusted Path/channels

FTP_TRP_EXP.1-2 Partial trusted channel

Hierarchical to: No other components.

FTP_TRP_EXP1.1-2 The IT Environment shall provide a communication path between the TSF and remote and local users that is logically distinct from other communication paths and relies on the IT environment to provide protection of the trusted channel from modification or disclosure using SSL.

FTP_TRP_EXP.1.2-2 The IT Environment shall permit the local users and remote users to initiate communication with the TSF via the trusted channel.

FTP_TRP_EXP.1.3-2 The IT Environment shall require the use of the trusted channel for initial user authentication and all communication between the TSF and its users.

FTP_TRP_EXP.1.4-2 The IT Environment shall provide a communication path between the TSF components that is logically distinct from other communication paths and relies on the IT environment to provide protection of the trusted channel from modification or disclosure using SSL.

FTP_TRP_EXP.1.5-2 The IT Environment shall provide a communication path between the TSF and the remote StillSecure update and upgrade web site that is logically distinct from other communication paths and relies on the IT environment to provide protection of the trusted channel from modification or disclosure using SSL.

Dependencies: None

5.4 TOE Security Assurance Requirements

The Security Assurance Requirements for the TOE are the assurance components of Evaluation Assurance Level 2 (EAL2) taken from Part 3 of the Common Criteria. None of the assurance components are refined. The assurance components are listed in Table 5-4.

Table 5-4: EAL2 Assurance Components

Component	Component Title
ACM_CAP.2	Configuration items
ADO_DEL.1	Delivery procedures
ADO_IGS.1	Installation, generation, and start-up procedures
ADV_FSP.1	Informal functional specification
ADV_HLD.1	Descriptive high-level design
ADV_RCR.1	Informal correspondence demonstration
AGD_ADM.1	Administrator guidance
AGD_USR.1	User guidance
ATE_COV.1	Evidence of coverage
ATE_FUN.1	Functional testing
ATE_IND.2	Independent testing – sample
AVA_SOF.1	Strength of TOE security function evaluation
AVA_VLA.1	Developer vulnerability analysis

Further information on these assurance components can be found in the Common Criteria for Information Technology Security Evaluation (CCITSE) Part 3.

6 TOE Summary Specification

6.1 IT Security Functions

6.1.1 Overview

Section 6 describes the specific security functions that meet the criteria of the security class features that are described in section 2.4. The following sections describe the IT Security Functions of the TOE. These security functions satisfy the TOE security functional requirements. Table 6-1: includes a bi-directional mapping between functions and requirements that clearly shows which functions satisfy which requirements and that all requirements are met. In sections 6, 7, and 8, the TOE and all its software modules and components will be mutually referred to as StillSecure Safe Access.

Table 6-1: Security Functional Requirements mapped to Security Functions

Item	SFRs	Security Class	Security Functions	Sub-functions
1	FAU_GEN.1	Audit data generation	Security Audit	AU-1
2	FAU_GEN.2	User identity association	Security Audit	AU-2
3	FAU_SAR.1	Audit review	Security Audit	AU-3
4	FAU_SAR.3	Selectable audit review	Security Audit	AU-4
5	FAU_STG_EXP.1-1	Protected audit trail storage	Security Audit	AU-5
6	FDP_ACC.1	Subset access control	NAC	NAC-1
7	FDP_ACF.1	Security attribute based access control	NAC	NAC-1
8	FDP_ACC_8021X_EXP.1-1	Partial Subset access control	NAC	NAC-1
9	FDP_ACF_8021X_EXP.1-1	Partial Security attribute based access control	NAC	NAC-1
10	FDP_ACC_BRIDGE_EXP.1-1	Partial Subset access control	NAC	NAC-1
11	FDP_ACF_BRIDGE_EXP.1-1	Partial Security attribute based access control	NAC	NAC-1
12	FIA_ATD.1	User attribute definition	Identification and Authentication	IA-1
13	FIA_UAU.2	User authentication before any action	Identification and Authentication	IA-2
14	FIA_UAU.7	Protected authentication feedback	Identification and Authentication	IA-3
15	FIA_UID.2	User identification before any action	Identification and Authentication	IA-4
16	FMT_MSA.3	Static attribute initialization	Security Management	SM-1
17	FMT_MTD.1	Management of TSF data	Security Management	SM-2
18	FMT_SMR.1	Security roles	Security Management	SM-3
19	FMT_SMF.1	Specification of Management Functions	Security Management	SM-4
20	FPT_RVM_EXP.1-1	Non-bypassability of the TSP	Protection of the TSF	PT-1
21	FPT_SEP_EXP.1-1	TSF Domain Separation	Protection of the TSF	PT-2
22	FSR_SRG_EXP.1	StillSecure Report Generation	StillSecure Security Status Reporting	SR-1
23	FSR_SRR_EXP.1	StillSecure Report Review	StillSecure Security Status Reporting	SR-2
24	FTP_TRP_EXP.1-1	Partial trusted channel	Trusted Channel	TC-1

6.1.2 Security Audit

AU-1 Audit data generation (FAU_GEN.1)

StillSecure Safe Access provides an audit trail function. Audit trails are logs maintained by StillSecure that track the changes in the access control states of the endpoints and the changes in the test status states.

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

- Start-up and shutdown of the audit functions
- Change in the access control states of endpoints
- Change in the test status of endpoints

Safe Access provides on-going feedback on the test status and the access control states of endpoints. Safe Access provides feedback on the access control states of endpoints as follows: Quarantined, Quarantined by exception, Temporarily quarantined until XX/XX/XX at HH:MM pm, Granted access, Granted access by exception, Has temporary access until XX/XX/XX at HH:MM pm (by admin), Has temporary access until XX/XX/XX at HH:MM pm (by NAC policy), Disconnected or Error. Safe Access provides feedback on the test status of endpoints as follows: Unknown error, Connecting, Awaiting credentials, Bad credentials, Testing (agentless test), Pass, Fail, Could not be tested, License limit exceeded, License expired, Test canceled, Access always allowed, Access always quarantined, Awaiting test initiation, Installing test service, Install canceled, Testing (installed test), Testing (one-time test), Installing one-time plug-in, One-time plug-in installation failed, Validating install, Install failed, Agent not active, Awaiting IP transition, Connection failed - endpoint busy or file and print sharing disabled, Connection failed - unsigned SMB, Connection failed - endpoint/domain trust failure, Connection failed - timed out, Connection failed - session setup, Test failed - insufficient test privileges, Connection failed - no route to host, and Endpoint disconnected before could be tested.

Further details regarding the access control states and test status states can be found in Chapter 4 of Still Secure SA Users Guide.

AU-2 User Identity Association (FAU_GEN.2)

StillSecure Safe Access is able to associate each auditable event with the identity of the TOE user that caused the event. Users activating auditable events can be identified via their user ID.

AU-3 Audit review (FAU_SAR.1)

StillSecure Safe Access provides the System Administrator, Cluster Administrator, view-only user, help desk technician and a user with a user-defined role of generate report with the capability to read all audit information from the audit records.

The Endpoint activity window is used to monitor end-user connection activity. This window enables users to review audit records.

AU-4 Selectable audit review (FAU_SAR.3)

StillSecure Safe Access provides the ability to perform searches of audit data based on the access control status, endpoint test status, the configurable time frame, cluster, NetBIOS Name, IP address, MAC address, user ID, Windows Domain, and NAC policy operating system.

The administrator may also configure the number of endpoints to display.

AU-5 Protected audit trail storage (FAU_STG_EXP.1-1)

The TSF is able to protect stored audit records from unauthorized deletion as well as prevent unauthorized modifications to the audit records

The audit logs are stored in the on board PostgreSQL database, which is password protected (remote users are disallowed) and firewalled (the PostgreSQL connection port is protected from outside requests by the on board iptables firewall). The machine hosting the PostgreSQL database will be physically located in a secure location. All system and application passwords are encrypted. The database login password given during the installation initially is stored in clear text in a flat file on the file system, and it gets encrypted upon first boot. The method of encryption of the database login password is outside the scope of the TOE.

Normal authorization controls that apply within the Safe Access web-based console, as well as the database password protection and on board firewall prevent unauthorized users from modifying or deleting the audit data.

6.1.3 NAC

NAC-1:
Subset Access control (FDP_ACC.1),
Partial Subset access control (FDP_ACC_8021X_EXP.1),
Partial Subset access control (FDP_ACC_BRIDGE_EXP.1),
Security attribute based access control (FDP_ACF.1),
Partial Security attribute based access control (FDP_ACF_8021X_EXP.1), and
Partial Security attribute based access control (FDP_ACF_BRIDGE_EXP.1)

The NAC SFP controls the access of the endpoints to the objects within the TOE's scope of control.

Endpoint Quarantine Precedence - Endpoints are quarantined in the following hierarchical order:

1. Access mode (normal operation, quarantine all, or allow all)
2. Temporarily quarantine for/Temporarily grant access for radio buttons
3. Endpoint testing exceptions (always grant access, always quarantine)
4. NAC policies

- **Access mode** (item 1 above) overrides the items listed below it (items 2, 3, and 4). The Access mode radio buttons are used to act globally on all endpoints in an enforcement cluster.
- The **Temporarily quarantine for**/**Temporarily grant access for radio buttons** (2) override Endpoint testing exceptions and NAC policies (items 3 and 4 in the above list). The **Temporarily quarantine for** radio button is used to temporarily quarantine endpoints that:

  – Have been designated **Always grant access and never test**
  – Are defined in NAC policies and have passed tests

  The **Temporarily grant access for** radio button is used to allow temporary access to endpoints that:

  – Have been designated **Always quarantine and never test**
  – Are defined in NAC policies and have failed tests

  The **Clear temporary states** radio button is used to remove the temporary access or temporary quarantine state enabled by the **Temporarily quarantine for**/**Temporarily grant access for** radio buttons.
- **Endpoint testing exceptions** overrides NAC policies. The **Endpoint testing exceptions** radio button is used to always allow or always quarantine endpoints that are defined in NAC policies. For example, an NAC policy might have a range of IP addresses defined for testing, but to exclude specific IP addresses within that range from the tests, the **Always grant access and never test** or **Always quarantine and never test** radio buttons are used.

NAC policies - An access control policy has the following configuration options:

- Name of policy
- NAC policy group
- Enabled or disabled

- Unsupported operating systems that will be allowed access without testing
- Retest Frequency
- Inactivity policy (time allowed before endpoint is disconnected)
- Tests to be run on an endpoint before it is allowed to connect to the network. Tests are divided into the following categories:
  1. Browser Security Policy – Windows,
  2. Operating System – Windows,
  3. Security Settings – OS X,
  4. Security Settings – Windows, and
  5. Software - Windows.
- The following administrator configuration actions may be taken if a test fails:
  1. grant temporary access,
  2. temporarily quarantine,
  3. send email notification,

Endpoints attempting to connect to the network that is protected by StillSecure Safe Access are evaluated by the NAC SFP. Safe Access is shipped with three standard NAC policies –

- high security,
- low security and
- medium security.

The three standard NAC policies are described in Table 6-2. Apart from the standard NAC policies, users with the requisite privileges can create custom NAC policies as well. Each of the NAC policies is associated with the Safe Access tests that are used to test the endpoints that are attempting to connect. The Safe Access tests have either standard properties (non-selectable), selectable properties or text entry fields and are updated regularly.

Table 6-2:Standard NAC policies

NAC Policy	Description and Actions Taken
High Security	A endpoint assigned to this policy must meet four requirements to gain access to the network. It must have, 1)all critical service packs and hot fixes installed, 2) all critical software installed, 3) all software security best practices, and 4) no worms, viruses, trojans or unauthorized person-to-person software present. When the tests in all the categories mentioned above pass, the endpoint is granted complete access to the network and when any of the tests fail, the endpoint is quarantined. Specific information on these requirements follows: o Security settings verified: • MS Excel macros setting level • MS Outlook macros setting level • MS Word macros setting level • Check for Services that are not allowed • Windows security policy (Windows local security policy best practices) o Software verified: • Anti-Virus software installed • P2P software installed is approved

NAC Policy	Description and Actions Taken
	• Personal firewalls software installed and running • Anti-Virus software software installed and up-to-date. • Verify that the endpoint attempting to connect does not host the configured list of worms, viruses, and trojans. o Operating system attributes verified: • Service packs are up-to-date as configured by the administrator • Hotfixes are up-to-date as configured by the administrator • Windows automatic updates are enabled o Browser security policy settings verified: • IE internet security zone configured as specified in the NAC FSP • IE local intranet security zone configured in the NAC SFP • IE restricted site security zone configured in the NAC SFP • IE trusted sites security zone configured in the NAC SFP • IE version configured in the NAC SFP
Medium Security	An endpoint assigned to this policy must meet three requirements to gain access to the network. It must have, 1) the latest service packs and all critical hot fixes installed, 2) anti-virus software installed, and 3) no worms, viruses or trojans present. When the tests for service packs, critical hotfixes or anti-virus software fail, temporary network access for three days is allowed but if the tests for worms, virus or trojan fail, the endpoint is immediately quarantined. Specific information on these requirements follows: Software verified: o Anti-Virus software installed and up-to-date o Verify that the endpoint attempting to connect does not host the configured list of worms, viruses, and trojans Operating system attributes verified: o Service packs are up-to-date as configured by the administrator o Hotfixes are up-to-date as configured by the administrator
Low Security	A endpoint assigned to this policy must meet three requirements to gain access to the network. It must have, 1) the latest service packs installed, 2) all critical hot fixes installed, and 3) no worms, viruses or trojans present When the tests for service packs or critical hotfixes fail, temporary network access for seven days is allowed but if the tests for worms, virus or trojan fail, the endpoint is immediately quarantined. Specific information on these requirements follows: Software verified: o Anti-Virus software installed and up-to-date Operating system attributes verified: o Service packs are up-to-date as configured by the administrator o Hotfixes are up-to-date as configured by the administrator

The administrator assigns each endpoint attempting to connect to one of the NAC policies. The tests that are associated with that particular NAC policy are conducted on the endpoint and depending on the outcome of those tests; Safe Access takes appropriate action depending on the NAC policy properties. When a particular endpoint is added to multiple NAC policies, that endpoint is assigned to the first enabled NAC policy in the list.

Safe Access offers multiple testing options of the endpoints. The endpoints supported by Safe Access are – Windows 98, Windows 2000, Windows Server (2000, 2003), Windows XP Professional, Windows XP Home, Windows NT, and Mac OS X.

The testing methods include –

1 **Agentless testing method:** Agentless testing uses an existing Windows service (RPC) on the endpoint. The Agentless test method requires that file and printer sharing be enabled on the endpoint.

2 **ActiveX-based testing method:** ActiveX testing uses a signed ActiveX control that is downloaded by the end-user via a browser. Hence, browser security settings must allow the execution of signed ActiveX controls. ActiveX testing only runs once, when the endpoint connects to the network and the endpoint is not monitored again until it re-connects to the network.

3 **Agent-based testing method:** StillSecure agent-based testing installs an agent (Safe Access Agent) onto the endpoint which then runs as a new Windows service. This testing method supports all Microsoft-supported Windows OSs. Once installed, the StillSecure Agent is available for re-testing of the endpoint.

The process Safe Access follows for allowing end-users to connect is - inline, DHCP or 802.1X method. These three methods are described in detail in Section 2.

6.1.4 Identification and Authentication

IA-1 User attribute definition (FIA_ATD.1)

The TSF shall maintain the following list of security attributes belonging to individual users:

- User ID – The user ID used to log in to Safe Access;
- Password – The password used to log in to Safe Access;
- Full name – The name associated with the user account;
- Email address – The email address used for email notifications;
- Account status – enabled or disabled
- User role – description of the permissions associated with the role
- Enabled/disabled – disable all permissions or enabled selected permissions/roles
- Accessible Cluster(s) – allow access to one or more clusters

IA-2 User Authentication before any action (FIA_UAU.2)

StillSecure Safe Access provides a password mechanism to authenticate TOE users before they are able to access the TOE.

IA-3 Protected authentication feedback (FIA_UAU.7)

StillSecure Safe Access provides only a display of the typed in user name and asterisks for the password for authentication to the user while the authentication is in progress.

IA-4 User identification before any action (FIA_UID.2)

StillSecure Safe Access identifies users before they are able to access the TOE. Users are identified by their user name.

6.1.5 Security Management

SM-1 Static Attribute initialization (FMT_MSA.3)

The TSF allows for default values to be assigned to the selectable test properties (security attributes) of an endpoint for the enforcement of the NAC SFP. The default values assigned can be overridden by the System administrator and the cluster administrator and replaced with values depending on the security attributes of the endpoint attempting to connect to the network.

Further details regarding the selectable test properties can be found in Chapter 6 and Appendix A of Still Secure SA Users Guide.

SM-2 Management of TSF Data (FMT_MTD.1)

- Users with Cluster Administrator roles can configure the settings of their assigned clusters and view endpoint activity, change endpoint access control, retest endpoints and generate reports for the cluster they are administering.
- Users with View-Only roles can view endpoint activity and generate reports about their cluster.
- Users with Help desk technician roles view endpoint activity, change endpoint access control, retest endpoints and run reports for the cluster they are responsible for.
- Users with User-defined roles are created with their own user roles and definitions.
- Users with System Administrator roles are given all of the above permissions for all the clusters and can control the download of test updates.

Please see Table 6, User Role Permissions in Chapter 3 of the StillSecure SA User Guide for more information on User Role Permissions. Please see Chapter 3 of the StillSecure SA User Guide for more information on Cluster settings.

SM-3 Security Roles (FMT_SMR.1)

The TOE maintains the following trusted roles each with their own permissions and privileges:

- System Administrator
- Cluster Administrator
- View-only user
- Help Desk Technician
- User-defined role

Users with **Cluster Administrator** roles can configure the endpoints in the clusters that the user account can access and view endpoint activity, change endpoint access control, retest endpoints and generate reports for the cluster they are administering.

Users with **View only user** roles can view endpoint activity and generate reports about their cluster.

Users with **Help desk technician** roles view endpoint activity, change endpoint access control, retest endpoints and run reports for the cluster they are responsible for.

Users with **User-defined** roles are created with their custom role name, custom description and permissions. Users with User-define role may have any combination of the following permissions:

- Configure clusters
- Configure servers
- Configure the system
- View system alerts
- Generate reports
- Manage NAC policies

- View endpoint activity
- Monitor system status
- Control Access
- Retest endpoints.

Users with **System Administrator** roles are given all of the above permissions for all the clusters and can control the download of test updates.

SM-4 Specification of Management Functions (FMT_SMF.1)

The TOE provides the users in assigned in a specific role (defined in the FMT_SMR.1) to perform specific operations (specified on the "Operation" column in Table 5-2) on data specified on "TSF Data" column in the Table 5-2 (see FMT_MTD.1).

6.1.6 Protection of the TSF

PT-1 Non-bypassability (FPT_RVM_EXP.1-1)

The TSF ensures that TOE security functions are non-bypassable. Since this is a software-only TOE, it also relies on the underlying OS to provide non-bypassability. The TOE ensures that security protection enforcement functions are invoked and succeed before each function within the TOE's scope of control is allowed to proceed. StillSecure Safe Access identifies users before they are able to access the TOE. The TOE provides a password mechanism to authenticate users before they are able to access the TOE.

PT-2 TSF domain separation (FPT_SEP_EXP.1-1)

The TSF maintains a security domain for its own execution that protects it from interference and tampering by untrusted subjects. Since this is a software-only TOE, it also relies on the underlying OS to provide TSF domain separation.

StillSecure Safe Access' protected domain includes the StillSecure Safe Access software and all of its software components as specified in section 2.4 as being in the TOE Boundary. The TSF enforces separation between the security domains of subjects in the TSC. StillSecure Safe Access relies on the Operating System to provide security capabilities for the TOE's protection. The underlying assumption regarding the operation of the TOE is that it is maintained in a physically secure environment.

6.1.7 StillSecure Security Status Reporting

SR-1 StillSecure Report Generation (FSR_SRG_EXP.1)

Safe Access provides a provision for Safe Access users with the necessary privileges to generate reports providing security status information on endpoint compliance and access activity. System administrator can generate reports on the security status of all the clusters whereas the rest of the users can only run reports on their clusters. The different types of reports that can be generated are described below:

- **NAC policy Results** – the report lists each NAC policy and the last pass/fail policy results.
- **Endpoint List** – the report lists each endpoint and the last pass/fail policy results.
- **Test Details** – the report comprehensive list of all test results, including remediation messages.
- **Test Results** – the report lists each test and the test's pass/fail status.
- **Test Results by IP address** – the report lists the number of tests that passed or failed for each IP address.
- **Test Results by NetBIOS name** – the report lists the number of tests that passed or failed for each NetBIOS name
- **Test Results by user** – the report lists the number of tests that passed or failed for each user.

SR-2 StillSecure Report Review (FSR_SRR_EXP.1)

Safe Access provides System administrator, Cluster administrator, View only, Help desk technician, and User defined role with the Generate reports, View endpoint activity, and Monitor system status privileges with the capability to view reports about the security status on endpoint compliance and access activity. System administrators can operate on the reports pertaining to all clusters. Cluster administrator, Help desk technician, and User defined role with explicitly assigned privilege can operate on the reports pertaining to their own clusters.

The reports are provided in a manner suitable for the user to interpret the information and contain information listed in the following table:

Table 6-3: Report information

Report	Description	Report information
NAC security policy results	Lists each NAC security policy condition and the last pass/fail policy results	• policy name • test status • # of times • % of total • details
Endpoint list	Lists each endpoint and the last pass/fail policy results	• MAC address • IP address • cluster • NetBIOS • user • test status
Test details	Comprehensive list of all test results, including remediation messages.	• date/time • IP address • NetBIOS • user • policy • test name • actions • test status • message
Test results	Lists each test and the test's pass/ fail status.	• test name • test status • # of times • % of total • details
Test results by IP address	Lists the number of tests that passed or failed for each IP address.	• IP address • cluster • NetBIOS • user • test status • # of times • % of total • details
Test results by NetBIOS name	Lists the number of tests that passed or failed for each NetBIOS name.	• NetBIOS • cluster • IP address • user • test status • # of times • % of total • details

Test results by user	Lists the number of tests that passed or failed for each user.	• user • cluster • IP address • NetBIOS • test status • # of times • % of total • details

6.1.8 Trusted Path/channels

TC-1 Partial trusted channel (FTP_TRP_EXP.1-1)

The TOE with the support of the IT environment provides protection of the trusted channel from modification or disclosure between the TSF and the remote StillSecure update and upgrade web site by using HTTPS/SSL. It allows the local users and remote users to initiate communication with the TSF via the trusted channel and requires the use of the trusted channel to be authenticated. The IT environment provides protection of the trusted channel from modification or disclosure.

6.1.9 SOF Claims

The threat level for the TOE authentication function is assumed to be SOF-basic. This defines a level of authentication strength of function where analysis shows that the function provides basic protection against straightforward or intentional breach of TOE security by attackers possessing a minimum attack potential.

IA-2 User Authentication before any action, is realized by probabilistic or permutational mechanisms. The methods used to provide difficult-to-guess passwords are probabilistic. The specific password policy is specified as the following:

- Minimum length of 8,
- At least one special character,
- At least one numeric character,
- At least one uppercase and one lowercase character
- 30 day expiration date
- Must not be a common word, a word in any existing password dictionaries, or a word easily guessed (such as “password”).

The SOF claim for IA-2 is SOF-basic.

6.2 Assurance Measures

The TOE satisfies the assurance requirements for Evaluation Assurance Level EAL2. The following items are provided as evaluation evidence to satisfy the EAL2 assurance requirements:

Table 6-4: Assurance Measures and How Satisfied

Component	Evidence Requirements	How Satisfied	Document ID
ACM_CAP.2	CM Documentation - CM Proof - Configuration Item List	The vendor provided configuration management documents and a Configuration Item list.	[SA CM]
ADO_DEL.1	Delivery Procedures	The vendor provided delivery procedures.	[SA DEL]

Component	Evidence Requirements	How Satisfied	Document ID
ADO_IGS.1	Installation, generation, and start-up procedures	The vendor provided secure installation, generation and start up procedures.	[SA IG] [SA QS] [SA CC Sup]
ADV_FSP.1	Functional Specification	The vendor provided informal function specification.	[SA ADV]
ADV_HLD.1	High-Level Design	The vendor provided descriptive high-level design document	
ADV_RCR.1	Representation Correspondence	The informal correspondence demonstration provided in the design documentation. ST to FSP in the FSP, FSP to HLD.	
AGD_ADM.1	Administrator Guidance	The vendor submitted system administration manual.	[SA UG] [SA CC Sup]
AGD_USR.1	User Guidance	The vendor submitted user guide.	[SA UG]
ATE_COV.1	Test Coverage Analysis	StillSecure Safe Access V5.0 Evaluation Test Coverage Analysis	[SA COV]
ATE_FUN.1	Test Documentation	The test evidence submitted to the CCTL.	[SA FUN]
ATE_IND.2	TOE for Testing	TOE for Testing The laboratory used development evidence submitted by the vendor along with functional testing evidence as a baseline for an independent test plan.	[CCTL TR]
AVA_SOF.1	SOF Analysis	The vendor submitted analysis of the SOF for the password.	[SA SOF]
AVA_VLA.1	Vulnerability Analysis	The vendor submitted vulnerability analysis. The laboratory conducted an independent vulnerability assessment by building on the vendor's. The laboratory conducted penetration testing.	[SA VLA]

7 PP Claims

The StillSecure Safe Access Security Target was not written to address any existing Protection Profile.

8 Rationale

8.1 *Security Objectives Rationale*

8.1.1 Threats to Security Objectives

Table 8-1 shows that all the identified threats to security are countered by Security Objectives for the TOE and the IT Environment. Rationale is provided for each threat below the table.

Table 8-1: All Threats to Security Countered

Item	Threat Name	Security Objective
1	T.Bypass	O.PartialNonBypass OE.NonBypass
2	T.Vul	O.IDScan OE.IDScan
3	T.Mismanage	O.Admin O.Revoke O.Roles
4	T.Privil	O.Access O.PartialSelfProtection OE.PartialSelfProtection O.IDAuth O.ProtectAuth ON.Operations ON.Physical
5	T.Tamper	O.Access O.IDAuth O.PartialNonBypass O.PartialSelfProtection OE.PartialSelfProtection OE.NonBypass O.Revoke
6	T.Undetect	O.Audit OE.AuditProtect OE.Time

T.Bypass: An attacker may attempt to bypass TSF security functions to gain unauthorized access to TSF. T.Bypass is countered by:

- O.PartialNonBypass: The TOE will ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed. This objective counters this threat by ensuring the TOE's protection mechanisms cannot be bypassed, which requires that TSF security functions not be bypassable.
- OE.NonBypass: The IT environment must ensure that its protection mechanisms cannot be bypassed. As a result, an attacker would not be able to bypass the TSF security functions.

T.Vul: The TOE may fail to identify non-compliant endpoints. T.Vul is countered by:

- O.IDScan: The TOE will collect and store system data from the endpoints on the target network and will enforce the NAC policy on those endpoints. This objective counters this threat by the TOE collecting system data from endpoints on the target network and quarantining endpoints found to be non-compliant.
- OE.IDScan: The IT environment will support the scanning of endpoints and enforcement of the NAC security policy.

T.Mismanage: Authorized administrators may make errors in the management of security functions and TSF data. Administrative errors may allow attackers to gain unauthorized access to resources protected by the TOE. T.Mismanage is countered by:

- O.Admin: The TOE will include a set of functions that allow effective management of its functions and data. Administrative tools make it easier for administrators to correctly manage the TOE.
- O.Roles: The TOE will support multiple roles. The TSF is able to associate a human user with one or more roles and these roles isolate administrative functions in that the functions of these roles do not overlap. If an administrator were to perform a malicious action, the auditing requirements afford some measure of detectability of the rogue administrator's actions.
- O.Revoke: The TOE will allow administrators to revoke privileges of users. This will limit the access of users.

T.Privil: An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and data. T.Privil is countered by:

- O.Access: The TOE will provide its authorized users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of user roles. This objective addresses this threat by providing for levels of user permissions, so that some users have more access to functions than others. This objective builds upon the O.IDAuth objective by only permitting authorized user accounts to access TOE functions. In addition, this objective builds upon the O.Roles objective by providing multiple roles and levels of user access.
- O.PartialSelfProtection: The TSF when invoked by the underlying host OS, will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces. This objective addresses this threat by providing partial TOE self-protection and separation between users. In addition, the TOE will maintain separation between code executing on behalf of different user accounts.
- OE.PartialSelfProtection: The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces. This objective addresses this threat by the underlying Operating System providing partial protection to the TOE and its data.
- O.IDAuth: The TOE will be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of user accounts prior to any TOE function access.
- O.ProtectAuth: The TOE will provide protected authentication feedback. This objective provides for the password to not be displayed when an authorized user is typing in their password. This will limit the ability to see what an authorized user account holder's password is.
- ON.Operations: The TOE will be managed and operated in a secure manner as outlined in the supplied guidance. This objective addresses this threat by making certain the TOE is managed and operated in a secure manner according to the TOE Guidance documentation.
- ON.Physical: Those responsible for the TOE will ensure that those parts of the TOE critical to the security policy are protected from any physical attack. This objective addresses this threat by making sure the parts of the TOE critical to enforcing the StillSecure Safe Access security are located in a physically secure area.

T.Tamper: An attacker may attempt to modify TSF programs and data. T.Tamper is countered by:

- O.Access: The TOE will provide its authorized users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of user roles. This objective addresses this threat by providing for levels of user permissions, so that some users have more access to functions than others. This objective builds upon the O.IDAuth objective by only permitting authorized user accounts to access TOE functions. In addition, this objective builds upon the O.Roles objective by providing multiple roles and levels of user access.

- O.IDAuth: The TOE will be able to identify and authenticate users prior to allowing access to TOE functions and data. This objective provides for authentication of user accounts prior to any TOE function access.
- O.PartialNonBypass: The TOE will ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed. This objective counters this threat by ensuring the TOE's protection mechanisms cannot be bypassed, which requires that TSF security functions not be bypassable.
- O.PartialSelfProtection: The TSF when invoked by the underlying host OS, will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces. This objective addresses this threat by providing partial TOE self-protection and separation between users. In addition, the TOE will maintain separation between code executing on behalf of different user accounts.
- OE.PartialSelfProtection: The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces. This objective addresses this threat by the underlying Operating System providing partial protection to the TOE and its data.
- OE.NonBypass: The IT environment must ensure that its protection mechanisms cannot be bypassed. As a result, an attacker would not be able to bypass the TOE security functions.
- O.Revoke: The TOE will allow administrators to revoke the privileges of the users. This will limit the access of users.

T.Undetect: Attempts by an attacker to violate the security policy may go undetected. If the attacker is successful, TSF data may be lost or altered. T.Undetect is countered by:

- O.Audit: The TOE will record audit records for data accesses and use of the TOE functions and will ensure protection of the audit storage. This objective provides for the TOE to generate audit records in an audit trail. Since the TOE records data accesses and use of the TOE functions, violations to the security policy will be recorded. In addition, this objective provides for the protection of the audit trail storage.
- OE.AuditProtect: The IT environment will ensure partial protection of the stored audit records. This objective counters the threat by requiring the IT Environment to provide protection of the audit storage.
- OE.Time: The underlying operating system will provide reliable time stamps. This objective provides for a reliable way to correlate audit records to reconstruct a potential compromise.

Table 8-2: Reverse mapping of TOE Security Objectives to Threats

Item	Objective	Threat
1.	O.Access	T.Privil T.Tamper
2.	O.Admin	T.Mismanage
3.	O.Audit	T.Undetect
4.	O.IDAuth	T.Privil T.Tamper
5.	O.IDScan	T.Vul
6.	O.PartialNonBypass	T.Bypass T.Tamper
7.	O.PartialSelfProtection	T.Privil T.Tamper
8.	O.ProtectAuth	T.Privil
9.	O.Revoke	T.Mismanage T.Tamper
10.	O.Roles	T.Mismanage

8.1.2 Assumptions

Table 8-3 shows that all of the secure usage assumptions are addressed by either security objectives for the IT environment or Non-IT security objectives. Rationale for each assumption is provided below the table.

Table 8-3: All Assumptions Addressed

Item	Assumption	Objective
1	A.AdmTra	ON.Install ON.Operations ON.Person
2	A.Env	ON.Install
3	A.Low	ON.Low
4	A.NoUntrusted	ON.NoUntrusted
5	A.Physical	ON.Physical
6	A.ProtectComm	ON.ProtectComm
7	A.Users	ON.ProtectAuth

A.AdmTra: Administrators and operators are non-hostile, appropriately trained and follow all administrative guidance, including guidance on setting passwords. A.AdmTra is supported by:

- ON.Install: Those responsible for the TOE will ensure that the TOE is delivered and installed in a manner that maintains IT security. Installing the TOE in a manner that maintains IT security includes correctly configuring the TOE. This objective provides for secure installation and configuration of the TOE.
- ON.Operations: The TOE will be managed and operated in a secure manner as outlined in the supplied guidance. The procedures will provide guidance to the administrators and users on setting passwords and how to securely operate the TOE. This objective provides for operation procedures to be in place.
- ON.Person: Authorized administrators shall be carefully selected and trained for proper operation of the system. This objective provides for competent personnel to administer the TOE.

A.Env: Administrators will ensure that the environment has adequate facility to provide disk storage and other capabilities for the TOE’s protection. A.Env is supported by:

- ON.Install: Those responsible for the TOE will ensure that the TOE is delivered and installed in a manner that maintains IT security. Installing the TOE in a manner that maintains IT security includes installing the TOE on the recommended Operating Systems and hardware according to the product’s installation requirements and Guidance documentation. This objective provides for secure installation of the TOE.

A.Low: The attack potential on the TOE is assumed to be low. A.Low is supported by:

- ON.Low: Those responsible for the TOE will ensure that the TOE is in an environment where there is only a low attack potential. This objective provides protection by placing the TOE in a low attack potential environment.

A.NoUntrusted: It is assumed that there will be no untrusted users and no untrusted software on the StillSecure Safe Access Server host which hosts the Management Server and the Enforcement Servers. A.NoUntrusted is supported by:

- ON.NoUntrusted: The administrator will ensure that there are no untrusted users and no untrusted software on the StillSecure Safe Access Server host. This objective provides for the protection of the TOE from untrusted software and users.

A.Physical: Physical protection is assumed to be provided by the environment. The TOE hardware and software is assumed to be protected from unauthorized physical access. A.Physical is supported by:

- ON.Physical: Those responsible for the TOE will ensure that those parts of the TOE critical to the security policy are protected from any physical attack. This objective provides for the physical protection of the TOE hardware and software.

A.ProtectComm: Those responsible for the TOE will ensure the communications between the Administrator PC and StillSecure Safe Access Server host are secure.

- ON.ProtectComm: Those responsible for the TOE will ensure that communications between the Administrator PC and StillSecure Safe Access Server host are secure.

A.Users: It is assumed that users will protect their authentication data. A.Users is supported by:

- ON.ProtectAuth: The users will ensure that their authentication data is held securely and not disclosed to unauthorized persons. This objective provides for user account holders to protect their authentication data.

8.2 *Security Requirements Rationale*

8.2.1 Functional Requirements

Table 8-4 shows that all of the security objectives of the TOE are satisfied. Rationale for each objective is included below the table.

Table 8-4: All Objectives Met by Functional Components

Item	Objective	Security Functional Requirement
1.	O.Access	FAU_STG_EXP.1-1 Protected audit trail storage FIA_UAU.2 User authentication before any action FIA_UID.2 User identification before any action FMT_MTD.1 Management of TSF data
2.	O.Admin	FAU_SAR.1 Audit review FAU_SAR.3 Selectable audit review FIA_ATD.1 User attribute definition FMT_MSA.3 Static attribute initialization FMT_MTD.1 Management of TSF data FMT_SMF.1 Specification of management functions FSR_SRR_EXP.1 StillSecure report review
3.	O.Audit	FAU_GEN.1 Audit data generation FAU_GEN.2 User identity association FAU_STG_EXP.1-1 Protected audit trail storage
4.	O.IDAuth	FIA_UAU.2 User authentication before any action FIA_UID.2 User identification before any action
5.	O.IDScan	FDP_ACC.1 User data protection FDP_ACF.1 Subset access control FDP_ACC_8021X_EXP.1-1 Partial subset access control FDP_ACF_8021X_EXP.1-1 Partial security attribute based access control FDP_ACC_BRIDGE_EXP.1-1 Partial subset access control FDP_ACF_BRIDGE_EXP.1-1 Partial security attribute based access control FSR_SRG_EXP.1 StillSecure report generation

Item	Objective	Security Functional Requirement
6.	O.PartialNonBypass	FPT_RVM_EXP.1-1 Non-bypassability of the TSP
7.	O.PartialSelfProtection	FPT_SEP_EXP.1-1 TSF domain separation FTP_TRP_EXP.1-1 Partial trusted channel
8.	O.ProtectAuth	FIA_UAU.7 Protected authentication feedback FTP_TRP_EXP.1-1 Partial trusted channel
9.	O.Revoke	FMT_MTD.1 Management of TSF data FMT_SMF.1 Specification of management functions
10.	O.Roles	FMT_SMR.1 Security roles

O.Access: The TOE will provide its authorized users with the means of controlling and limiting access to the objects and resources they own or are responsible for, on the basis of user roles. O.Access is addressed by:

- FAU_STG_EXP.1-1 Protected audit trail storage, which requires the audit log be protected from unauthorized deletion and modifications.
- FIA_UAU.2 User authentication before any action, which requires each user with a user account be successfully authenticated before allowing access to the TOE.
- FIA_UID.2 User identification before any action, which requires that each user with a user account to be successfully identified before allowing access to the TOE.
- FMT_MTD.1 Management of TSF data, which specifies the management of TSF Data according to assigned roles.

O.Admin: The TOE will include a set of functions that allow effective management of its functions and data. O.Admin is addressed by:

- FAU_SAR.1 Audit review, which requires that users with audit permission be able to read all audit information from the audit records.
- FAU_SAR.3 Selectable audit review, which requires that the TSF will provide the ability to search audit data based on the specified criteria.
- FIA_ATD.1 User attribute definition, which requires the TSF to maintain a list of security attributes belonging to individual users. The list of security attributes are user ID, Password, Full Name, Email Address, Account Status, User Role.
- FMT_MSA.3 Static attribute initialization, which requires the TOE to provide default and alternative values for security attributes used to enforce the SFP.
- FMT_MTD.1 Management of TSF data, which specifies the management of TSF Data according to assigned roles.
- FMT_SMF.1 Specification of Management Functions, which requires the TOE to provide the specification of the management functions provided by the TOE. Management functions provide TSFI that allow users in different roles to define the parameters that control the operation of security-related aspects of the TOE.
- FSR_SRR_EXP.1 StillSecure Report Review, which require the TOE to provide users in different roles with the capability to view specific reports about the security status on endpoint compliance and access activity.

O.Audit: The TOE will record audit records for data accesses and use of the TOE functions and will ensure protection of the audit storage. O.Audit is addressed by:

- FAU_GEN.1 Audit data generation, which requires the ability to audit specified events.
- FAU_GEN.2 User identity association, which requires each auditable event be associated with a user.

- FAU_STG_EXP.1-1 Protected audit trail storage, which requires the audit log be protected from unauthorized deletion and modifications.

O.IDAuth: The TOE will be able to identify and authenticate users prior to allowing access to TOE functions and data. O.IDAuth is addressed by:

- FIA_UAU.2 User authentication before any action, which requires each user account to be successfully authenticated before allowing access to the TOE.
- FIA_UID.2 User identification before any action, which requires that each user with a user account to be successfully identified before allowing access to the TOE.

O.IDScan: The TOE will collect and store system data from the endpoints on the target network and will enforce the NAC on those endpoints.

- FDP_ACC.1 User Data Protection, which requires the TOE to enforce NAC on endpoints.
- FDP_ACF.1 Subset access control, which requires the TOE to enforce NAC on endpoints based on security attributes of the endpoints.
- FDP_ACC_8021X_EXP.1-1, Partial subset access control, which requires the TOE, with the support from the IT Environment, to enforce the 802.1X enforcement method of the NAC SFP in accordance to FDP_ACC.1.
- FDP_ACF_8021X_EXP.1-1, Partial Security attribute based access control, which requires the TOE, with the support from the IT Environment, to enforce the 802.1X enforcement method of the NAC SFP in accordance to FDP_ACF.1.
- FDP_ACC_BRIDGE_EXP.1-1, Partial subset access control, which requires the TOE, with the support from the IT Environment, to enforce the Inline and DHCP enforcement methods of the NAC SFP in accordance to FDP_ACC.1.
- FDP_ACF_BRIDGE_EXP.1-1, Partial Security attribute based access control, which requires the TOE, with the support from the IT Environment, to enforce the Inline and DHCP enforcement method of the NAC SFP in accordance to FDP_ACF.1.
- FSR_SRG_EXP.1 StillSecure Report Generation, which requires the TOE to generate different reports about the security status on endpoint compliance and access activity.

O.PartialNonBypass: The TOE will ensure the security enforcing functions are invoked and succeed before allowing a TOE function to proceed.

- FPT_RVM_EXP.1-1 Non-bypassability of the TSP which requires that TSP enforcement functions are invoked and succeed before a security relevant function is allowed to proceed.

O.PartialSelfProtection: The TSF when invoked by the underlying host OS, will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces.

- FPT_SEP_EXP.1-1 TSF domain separation, which requires the TSF to provide a domain, that partially protects itself from interference and tampering by untrusted users. This requires that the TOE provide partial protection to maintain separation between code executing on behalf of different users.
- FTP_TRP_EXP.1-1, Partial trusted path, requires the TOE to establish and maintain trusted communication to or from users and the TSF. The TOE, with the support of the IT environment, provides protection of the trusted channel from modification or disclosure between the TSF and the remote StillSecure update and upgrade web site by using HTTPS/SSL.

O.ProtectAuth: The TOE will provide protected authentication. O.ProtectAuth is addressed by:

- FIA_UAU.7 Protected authentication feedback, the TSF shall provide only a display of the typed in user account name and asterisks for the password for password authentication.
- FTP_TRP_EXP.1-1, Partial trusted path, requires the TOE to establish and maintain trusted communication to or from users and the TSF. The TOE with the support of the IT environment

provides protection of the trusted channel from modification or disclosure between the TSF and the remote StillSecure update and upgrade web site by using HTTPS/SSL.

O.Revoke: The TOE will allow administrators to revoke privileges of users.

- FMT_MTD.1 Management of TSF data, which specifies the management of TSF Data according to assigned roles.

O.Roles: The TOE will support multiple roles. O.Roles is addressed by:

- FMT_SMR.1 Security roles, which requires that the TSF maintain multiple roles.

Table 8-5: Reverse mapping of TOE SFRs to TOE Security Objectives

Item	Security Functional Requirement	Objective
1.	FAU_GEN.1	O.Audit
2.	FAU_GEN.2	O.Audit
3.	FAU_SAR.1	O.Admin
4.	FAU_SAR.3	O.Admin
5.	FAU_STG_EXP.2-1	O.Access O.Audit
6.	FDP_ACC.1	O.IDScan
7.	FDP_ACF.1	O.IDScan
8.	FDP_ACC_8021X_EXP.1-1	O.IDScan
9.	FDP_ACF_8021X_EXP.1-1	O.IDScan
10.	FDP_ACC_BRIDGE_EXP.1-1	O.IDScan
11.	FDP_ACF_BRIDGE_EXP.1-1	O.IDScan
12.	FIA_ATD.1	O.Admin
13.	FIA_UAU.2	O.Access O.IDAuth
14.	FIA_UAU.7	O.ProtectAuth
15.	FIA_UID.2	O.Access O.IDAuth
16.	FMT_MSA.3	O.Admin
17.	FMT_MTD.1	O.Access O.Admin O.Revoke
18.	FMT_SMR.1	O.Roles
19.	FMT_SMF.1	O.Admin
20.	FPT_RVM_EXP.1-1	O.PartialNonBypass
21.	FPT_SEP_EXP.1-1	O.PartialSelfProtection
22.	FSR_SRG_EXP.1	O.IDScan
23.	FSR_SRR_EXP.1	O.Admin
24.	FTP_TRP_EXP.1-1	O.PartialSelfProtection O.ProtectAuth

Note: Table 8-5 has been included as a consistency check to show that each TOE SFR maps back to at least one TOE security objective

8.2.2 Dependencies

Table 8-6 shows the dependencies between the functional requirements. All dependencies are satisfied. Dependencies that are satisfied by a hierarchical component are denoted by an (H) following the dependency reference. If the TOE dependency is met by an SFR in the IT environment an "E" will be next to the reference number.

Table 8-6: TOE Dependencies Satisfied

No.	Component	Component Name	Dependencies	Reference
1	FAU_GEN.1	Audit data generation	FPT_STM.1	1 (E)
2	FAU_GEN.2	User Identity Association	FAU_GEN.1	1
			FIA_UID.1	15 (H)
3	FAU_SAR.1	Audit review	FAU_GEN.1	1
4	FAU_SAR.3	Selectable audit review	FAU_SAR.1	3
5	FAU_STG_EXP.1-1	Protected audit trail storage	FAU_GEN.1	1
6	FDP_ACC.1	Subset access control	FDP_ACF.1	7
7	FDP_ACF.1	Security attribute based access control	FMT_MSA.3	16
			FDP_ACC.1	6
			FPT_IDSCAN_EXP.1	8(E)
8	FDP_ACC_8021X_EXP.1-1	Partial Subset access control	FDP_ACF_8021X_EXP.1-1	9, 2(E), 6(E), 7(E)
9	FDP_ACF_8021X_EXP.1-1	Partial Security attribute based access control	FDP_ACC_8021X_EXP.1-1	8, 3(E)
10	FDP_ACC_BRIDGE_EXP.1-1	Partial Subset access control	FDP_ACF_BRIDGE_EXP.1-1	11, 4(E)
11	FDP_ACF_BRIDGE_EXP.1-1	Partial Security attribute based access control	FDP_ACC_BRIDGE_EXP.1-1	10, 5(E)
12	FIA_ATD.1	User attribute definition	None	None
13	FIA_UAU.2	User authentication before any action	FIA_UID.1	15 (H)
14	FIA_UAU.7	Protected authentication feedback	FIA_UAU.1	13 (H)
13	FIA_UID.2	User identification before any action	None	None
15	FMT_MSA.3	Static attribute initialization	FMT_MSA.1	See section 8.2.3
			FMT_SMR.1	18
16 17	FMT_MTD.1	Management of TSF data	FMT_SMR.1	18
			FMT_SMF.1	19
18	FMT_SMR.1	Security roles	FIA_UID.1	15 (H)
19	FMT_SMF.1	Specification of management functions	None	None
20	FPT_RVM_EXP.1-1	Non-bypassability of the TSP	None	None
21	FPT_SEP_EXP.1-1	TSF domain separation	None	None
22	FSR_SRG_EXP.1	StillSecure report generation	None	None
23	FSR_SRR_EXP.1	StillSecure report review	FSR_SRG_EXP.1	22

No.	Component	Component Name	Dependencies	Reference
24	FTP_TRP_EXP.1-1	Partial trusted channel	FTP_TRP_EXP.1-2	12(E)

Table 8-7: IT Environment Dependencies are Satisfied

No.	Component	Component Name	Dependencies	Reference
1 (E)	FAU_STG_EXP.1-2	Protected audit trail storage	FAU_GEN.1	1
2 (E)	FDP_ACC_8021X_EXP.1-2	Partial Subset access control	3 (E)	None
3 (E)	FDP_ACF_8021X_EXP.1-2	Partial Security attribute based access control	2 (E)	None
4 (E)	FDP_ACC_BRIDGE_EXP.1-2	Partial Subset access control	5 (E)	None
5 (E)	FDP_ACF_BRIDGE_EXP.1-2	Partial Security attribute based access control	4 (E)	None
6 (E)	FIA_UAU_8021X_EXP.1	Timing of authentication	None	None
7 (E)	FIA_UID_8021X_EXP.1	Timing of identification	None	None
8 (E)	FPT_IDSCAN_EXP.1	Endpoint scan	None	None
9 (E)	FPT_RVM_EXP.1-2	Non-bypassability of the TSP	None	None
10(E)	FPT_SEP_EXP.1-2	TSF domain separation	None	None
11(E)	FPT_STM.1	Reliable time stamps	None	None
12(E)	FTP_TRP_EXP.1-2	Partial trusted channel	None	None

8.2.3 Rationale why dependencies are not met

For FMT_MSA.3, Static attribute initialization, the dependency on FMT_MSA.1, Management of Security attributes is satisfied by FMT_MTD.1, Management of TSF data.

8.2.4 Strength of Function Rationale

A strength of function level of SOF-Basic counters an attack level of low. The environment is one where the potential attacker is unsophisticated, with access to only standard equipment and public information about the product. A user password is required to be used when accessing the Safe Access web-based console.

8.2.5 Assurance Requirements Rationale

Evaluation Assurance Level EAL2 was chosen to provide a basic level of assurance due to the low level threat of malicious attacks.

8.2.6 Rationale that IT Security Requirements are Internally Consistent

The IT Security Requirements are internally consistent. There are no requirements that conflict with one another. When different IT security requirements apply to the same event, operation, or data there is no conflict between the security requirements. The requirements mutually support each other to apply to the event, operation, or data.

For auditing, each of the SFRs builds on the others. For example, FAU_GEN.1 details the auditable events generated by the TSF. FAU_GEN.2 provides for the TSF to associate each auditable event with the identity of the user that caused the event. FAU_SAR.1 states that the TSF shall provide the System Administrator, Cluster Administrator, view-only user, help desk technician and a user with a user-defined role of generate report with the capability to read all audit information from the audit records. FAU_SAR.3 gives the TOE the ability to perform searches of the audit event data. FAU_STG_EXP.1-1 provides protection of the stored audit records from unauthorized deletion and modifications. Audit records are generated for many events where other requirements are coming to bear, such as login and management functions.

Login processing brings in elements of many requirements, but all in a complementary way. FIA_ATD.1 defines the security attributes belonging to System administrators, cluster administrators, view only user, help desk technician and user-defined role. FIA_UID.2 requires the user identified before allowing any other operations and FIA_UAU.2 requires the user authenticated before allowing any other operations. FIA_UAU.7 requires that feedback from authentication input be obscured.

Together FDP_ACC.1 and FDP_ACF.1 provide User data protection. FDP_ACC.1 defines the NAC SFP. FDP_ACF.1 specifies that the TSF enforce access based upon security attributes and named groups of attributes. The subjects with roles are defined in FMT_SMR.1. FDP_ACC.1 and FDP_ACF.1 are supported by FDP_ACC_8021X_EXP.1-1, FDP_ACF_8021X_EXP.1-1, FDP_ACC_BRIDGE_EXP.1-1, and FDP_ACF_BRIDGE_EXP.1-1, which insure that the TOE enforcement configurations will be supported by network components in the IT environment.

The management requirements (FMT_) are related to many of the mechanisms involved with other requirements. FMT_MSA.3 enforces the NAC SFP to provide restrictive default values for security attributes. FMT_MTD.1 specifies the management of TSF Data according to assigned roles which are defined in FMT_SMR.1. In many cases, the other mechanisms will enforce the settings made through management functions. Installation mechanisms (see ADO_IGS.1) rely on management functions. The administrator guidance (see AGD_ADM.1) documents the management functions.

FPT_RVM_EXP.1-1 makes certain the TSP enforcement functions are invoked and succeed before any other functions within the TSC are allowed to proceed. FPT_SEP_EXP.1-1 makes certain that the TSF maintains a security domain for its own execution that protects it from interference and tampering by untrusted subjects

8.2.7 Explicitly Stated Requirements Rationale

A refinement that adds additional detail and narrows the scope has to be iterated to meet the original scope of the SFR. FAU_STG_EXP.1, FPT_RVM_EXP.1 and FPT_SEP_EXP.1 had to be explicitly stated because it provides partial TOE self-protection while relying on the OS and Hardware platforms to provide the full protection. According to CCIMB RI#19, which states the following: “Where necessary to cover different aspects of the same requirement (e.g. identification of more than one type of user), repetitive use (i.e. applying the operation of iteration) of the same Part 2 components to cover each aspect is possible. The statement of TOE security requirements shall define the functional and assurance security requirements that the TOE and the supporting evidence for its evaluation need to satisfy in order to meet the security objectives for the TOE. Since the iteration of FAU_STG_EXP.1, FPT_RVM_EXP.1 and FPT_SEP_EXP.1 span both the TOE requirements and IT Environment, it must be explicitly stated. FSR_SRG_EXP.1 and FSR_SRR_EXP.1 are explicitly stated because the CC Part 2 does not have any security status reporting related SFRs that can describe the functions of the TOE.

FDP_ACC_8021X_EXP.1-1, FDP_ACF_8021X_EXP.1-1, FDP_ACC_BRIDGE_EXP.1-1, FDP_ACF_BRIDGE_EXP.1-1, FDP_ACC_8021X_EXP.1-2, FDP_ACF_8021X_EXP.1-2, FIA_UAU_8021X_EXP.1, FIA_UID_8021X_EXP.1, FDP_ACC_BRIDGE_EXP.1-2, and FDP_ACF_BRIDGE_EXP.1-2 are explicitly stated SFr which define the TOE’s interaction with the IT environment to support the conditional blocking or transmission of packets originating from or transmitted to a particular endpoint.

8.2.8 Requirements for the IT Environment

Table 8-8 shows that all of the security objectives for the IT environment are satisfied. Rationale for each objective is included below the table.

Table 8-8: All Objectives for the IT Environment map to Requirements in the IT environment

Item	Objective	Requirement for the IT Environment
1	OE.AuditProtect	FAU_STG_EXP.1-2
2	OE.NonBypass	FPT_RVM_EXP.1-2
3	OE.PartialSelfProtection	FPT_SEP_EXP.1-2 FTP_TRP_EXP.1-2

Item	Objective	Requirement for the IT Environment
4	OE.Time	FPT_STM.1
5	OE.IDScan	FDP_ACC_8021X_EXP.1-1, FDP_ACF_8021X_EXP.1-1, FDP_ACC_BRIDGE_EXP.1-1, FDP_ACF_BRIDGE_EXP.1-1, FDP_ACC_8021X_EXP.1-2, FDP_ACF_8021X_EXP.1-2, FIA_UAU_8021X_EXP.1, FIA_UID_8021X_EXP.1, FDP_ACC_BRIDGE_EXP.1-2, and FDP_ACF_BRIDGE_EXP.1-2

OE.AuditProtect: The IT environment will ensure the protection of the audit storage. OE.AuditProtect is addressed by:

- FAU_STG_EXP.1-2 Protected audit trail storage, which requires the IT environment to protect the stored records in the audit trail from unauthorized deletion and can prevent unauthorized modifications to the audit records in the audit trail. The TOE relies on the underlying OS to protect the audit trail storage.

OE.NonBypass: The IT environment will ensure that its protection mechanisms cannot be bypassed. OE.NonBypass is addressed by:

- FPT_RVM_EXP.1-2 Non-bypassability of the TSP, which requires that the IT Environment ensures the OS enforcement functions are invoked and succeed before a security-relevant function is allowed to proceed.

OE.PartialSelfProtection: The IT environment will maintain a domain for its own execution that protects itself and its resources from external interference, tampering, or unauthorized disclosure, through its own interfaces. OE.PartialSelfProtection is addressed by:

- FPT_SEP_EXP.1-2 TSF domain separation, which requires the Operating System to maintain a security domain for its own execution that protects it from interference and tampering by untrusted subjects initiating actions through the Operating System's Interface. The IT environment will enforce separation between security domains of subjects in the Operating System's Scope of Control.
- FTP_TRP_EXP.1-2, Partial trusted channel, which requires the IT Environment to provide a communication path between the TSF and remote and local users that is logically distinct from other communication paths, and to provide protection of the trusted channel from modification or disclosure using SSL.

OE.Time: The underlying operating system will provide reliable time stamps. OE.Time is addressed by:

- FPT_STM.1 Reliable time stamps, which requires that time stamps be provided by the IT environment.

OE.IDScan: The IT environment will support the scanning of endpoints and enforcement of the NAC security policy. OE.IDScan is addressed by:

- FDP_ACC_8021X_EXP.1-2 Partial Subset access control, which requires an access control mechanism to support the 802.1X TOE configuration.
- FDP_ACF_8021X_EXP.1-2 Partial Security attribute based access control, which requires an access control mechanism to support the 802.1X TOE configuration.
- FDP_ACC_BRIDGE_EXP.1-2 Partial Subset access control, which requires an access control mechanism to support filtering based on MAC addresses in the inline and DHCP TOE configurations.
- FDP_ACF_BRIDGE_EXP.1-2 Partial Security attribute based access control, which requires an access control mechanism to support filtering based on MAC addresses in the inline and DHCP TOE configurations.

- FIA_UAU_8021X_EXP.1 Timing of authentication, which requires an 802.1X compliant access control mechanism to authenticate endpoints in the TOE 802.1X configuration..
- FIA_UID_8021X_EXP.1 Timing of identification, which requires an 802.1X compliant access control mechanism to identify endpoints in the TOE 802.1X configuration..

8.3 *TOE Summary Specification Rationale*

8.3.1 IT Security Functions

Table 8-9: shows that the IT Security Functions in the TOE Summary Specification (TSS) address all of the TOE Security Functional Requirements.

Table 8-9: Mapping of Functional Requirements to TOE Summary Specification

Item	Functional Component	Functional Requirement	Requirement is met by:	
			Security Function Ref. No	Rationale
1.	FAU_GEN.1	Audit data generation	AU-1	Specifies the types of events to be audited and the information to be recorded in an audit record.
2.	FAU_GEN.2	User Identity Association	AU-2	Specifies how each audit event can be associated with the TOE user who caused the event and how they can be identified.
3.	FAU_SAR.1	Audit review	AU-3	Specifies who has the capability to read information from the audit records.
4.	FAU_SAR.3	Selectable audit review	AU-4	Specifies that the TOE provides the ability to perform searches of the audit data, based on various criteria.
5.	FAU_STG_EXP.1	Protected audit trail storage	AU-5	Specifies that the TOE is able to protect the stored audit records from unauthorized deletion and prevent modifications to the audit records.
6.	FDP_ACC.1	Subset access control	NAC-1	Specifies the subjects, objects, and operations for the NAC SFP
7.	FDP_ACF.1	Security attribute based access control	NAC-1	Specifies the subject attributes, object attributes, and rules for the NAC SFP.
8.	FDP_ACC_8021X_EXP.1-1	Partial Subset access control	NAC-1	Specifies the TOE interaction with the IT environment to enforce the 802.1X enforcement method.
9.	FDP_ACF_8021X_EXP.1-1	Partial Security attribute based access control	NAC-1	Specifies the TOE interaction with the IT environment to enforce the 802.1X enforcement method.
10.	FDP_ACC_BRIDGE_EXP.1-1	Partial Subset access control	NAC-1	Specifies the TOE interaction with the IT environment to enforce the inline and DHCP enforcement method.
11.	FDP_ACF_BRIDGE_EXP.1-1	Partial Security attribute based access control	NAC-1	Specifies the TOE interaction with the IT environment to enforce the inline and DHCP enforcement method.

Item	Functional Component	Functional Requirement	Requirement is met by:	
			Security Function Ref. No	Rationale
12.	FIA_ATD.1	User attribute definition	IA-1	Specifies the security attributes maintained for each user account.
13.	FIA_UAU.2	User authentication before any action	IA-2	Specifies that the TOE requires each user account to successfully authenticate with a password before being allowed any other actions. (consistent with SOF-basic)
14.	FIA_UAU.7	Protected authentication feedback	IA-3	Specifies that the TOE displays only the typed in user account name and asterisks for the password during password authentication.
15.	FIA_UID.2	User identification before any action	IA-4	Specifies that the TOE requires each user to identify himself/herself before being allowed to perform any other actions.
16.	FMT_MSA.3	Static attribute initialization	SM-1	Specifies that the StillSecure Safe Access provides restrictive default values for security attributes and the System administrator and Cluster administrator can specify alternative initial values.
17.	FMT_MTD.1	Management of TSF data	SM-2	Specifies that the TOE restricts the ability to access data.
18.	FMT_SMR.1	Security roles	SM-3	Specifies the roles maintained in the TOE.
19.	FMT_SMF.1	Specification of Management Functions	SM-4	Specifies that the users in specific roles can define the parameters that control the operation of security-related aspects of the TOE.
20.	FPT_RVM_EXP.1-1	Non-bypassability of the TSP	PT-1	Specifies that the StillSecure Safe Access security policy enforcement functions are invoked and succeed before each function is allowed to proceed.
21.	FPT_SEP_EXP.1-1	TSF domain separation	PT-2	Specifies that the StillSecure Safe Access maintains a security domain for its own execution and enforces separation between security domains of the users.
22.	FSR_SRG_EXP.1	StillSecure Report Generation	SR-1	Specifies that the StillSecure Safe Access generates different kinds of reports about the security status information.
23.	FSR_SRR_EXP.1	StillSecure Report Review	SR-2	Specifies that the reports about the security status generated by StillSecure Safe Access can be reviewed.
24.	FTP_TRP_EXP.1-1	Partial trusted channel	TC-1	Specifies that the TOE to establish and maintain trusted communication to or from users and the TSF.

8.3.2 Assurance Measures

The assurance measures rationale shows how all assurance requirements are satisfied. The rationale is provided in Table 8-10: .

Table 8-10: Assurance Measures Rationale

Component	Evidence Requirements	How Satisfied	Rationale
ACM_CAP.2	CM Documentation • CM Proof • Configuration Item List	StillSecure Safe Access V5.0 Configuration Management, and configuration listing obtained from the configuration management system.	• CM Proof - Shows the CM system is being used. • Configuration Item List(s) - is comprised of a list of the source code files and version numbers - is comprised of a list of design documents with version numbers - is comprised of test documents with version numbers - user and administrator documentation with version numbers
ADO_DEL.1	Delivery Procedures	StillSecure Safe Access V5.0 Delivery Procedures	Provides a description of all procedures that are necessary to maintain security when distributing TOE software to the user's site. SAR is applicable across all phases of delivery from packaging, storage, distribution
ADO_IGS.1	Installation, generation, and start-up procedures	StillSecure Safe Access V5.0 Installation Guidance StillSecure Safe Access V5.0 Common Criteria Supplement to the Guidance Documentation	Provides detailed instructions on how to install the TOE.
ADV_FSP.1	Functional Specification	StillSecure Safe Access V5.0 Development Specification (FSP/HLD/RCR) Common Criteria Evaluation v1.0	Provides rationale that the TSF is fully represented Describes the TSF interfaces and TOE functionality
ADV_HLD.1	High-Level Design	StillSecure Safe Access V5.0 Development Specification (FSP/HLD/RCR) Common Criteria Evaluation v1.0	Describes the TOE subsystems and their associated security functionality
ADV_RCR.1	Representation Correspondence	StillSecure Safe Access V5.0 Development Specification (FSP/HLD/RCR) Common Criteria Evaluation v1.0	Provides the following two dimensional mappings: 1. TSS and functional specification; 2. Functional specification and high-level design.
AGD_ADM.1	Administrator Guidance	Safe Access® v5.0 Users' Guide StillSecure Safe Access V5.0 Release Notes	Describes how to administer the TOE securely.

Component	Evidence Requirements	How Satisfied	Rationale
AGD_USR.1	User Guidance	Not Applicable	Describes the secure use of the TOE.
ATE_COV.1	Test Coverage Analysis	StillSecure Safe Access V5.0 Evaluation Test Coverage Analysis	Shows correspondence between the tests identified in the test documentation and the TSF as described in the functional specification.
ATE_FUN.1	Test Documentation	StillSecure Safe Access V5.0 Common Criteria Test cases	Test documentation includes test plans and procedures and expected and actual results.
ATE_IND.2	TOE for Testing	TOE for Testing	The TOE will be provided for testing.
AVA_SOF.1	SOF Analysis	StillSecure Safe Access V5.0 SOF Analysis	Provides a rationale that each mechanism identified in the ST as having an SOF meets or exceeds the minimum strength level specified there.
AVA_VLA.1	Vulnerability Analysis	StillSecure Safe Access V5.0 Vulnerability Analysis	Provide an analysis of the TOE deliverables for obvious ways in which a user can violate the TSP, including the disposition of obvious vulnerabilities.

8.4 PP Claims Rationale

Not applicable. There are no PP claims.