JMCS Northern Light Video Conferencing System Security Target

Common Criteria: EAL2

Version 1.2

22-FEB-12

Document management

Document identification

Document ID	NLVC_ST_EAL2
Document title	JMCS Northern Light Video Conferencing System Security Target
Product version	NLVC System version which consist of: - NLVC Client (version 6.3.0.0) - NLVC Server Webadmin Tool (version 7.0.0.1) - NLVC Server (version 6.1-0.21)

Document history

Version	Date	Description
0.1	25-08-2010	Released for internal review.
0.2	22-09-2010	Additional SFRs: FDP_IFC, FDP_IFF, FDP_ITT.
0.3	1-10-2011	Addressing EORs.
1.0	21-11-2011	Final release
1.1	13-JAN-12	Final release for MyCB review
1.2	22-FEB-12	Final release for MyCB review

Table of Contents

1 Security Target introduction (ASE_INT)

1.1 ST and TOE identification

ST Title	JMCS Northern Light Video Conferencing System Security Target
ST Version	1.2, 22-FEB-12
TOE Name	Northern Light Video Conferencing System
TOE Version	NLVC System version which consist of: - NLVC Client (version 6.3.0.0) - NLVC Server Webadmin Tool (version 7.0.0.1) - NLVC Server (version 6.1-0.21)
Assurance Level	EAL2
CC Identification	Common Criteria for Information Technology (IT) Security Evaluation, Version 3.1, July 2009, incorporating: • Part One – Introduction and General Model, Revision Three, July 2009; • Part Two – Security Functional Components, Revision Three, July 2009; and • Part Three – Security Assurance Components, Revision Three, July 2009. Common Methodology for Information Technology Security Evaluation, Evaluation methodology, July 2009, Version 3.1, Revision 3, CCMB-2009-07-004

1.2 Document organization

This document is organized into the following sections:

- Section 1 provides the introductory material for the ST as well as the TOE description including the physical and logical scope of the TOE.

- Section 2 provides the conformance claims for the evaluation.

- Section 3 provides the security problem to be addressed by the TOE and the operational environment of the TOE.
- Section 4 defines the security objectives for the TOE and the environment.
- Section 5 contains the functional and assurance requirements derived from the Common Criteria, Part 2 and 3, respectively that must be satisfied by the TOE.
- Section 6 provides a summary of the TOE specification, identifying the IT security functions provided by the TOE.

1.3 TOE Overview

1.3.1 TOE type and usage

The Target of Evaluation (TOE) is the Northern Light Video Conferencing System and is referred to as the TOE or NLVC System in this document.

NLVC is a multipoint-to-multipoint video conferencing system. It allows conferencing of any desired number of people around the world using existing LAN infrastructure, without affecting current applications. It is software based and uses non-proprietary hardware.

NLVC uses multicast technology within the LAN and unicast technology within the WAN. This enables NLVC to keep the conference bandwidth constant no matter how many users are connected to that conference.

NLVC also uses the RSW (Real Time Switching) Control Criteria. RSW Control Criteria is an advanced set of controls for Multimedia Conferencing that focused more on bandwidth reduction and prioritizes the participants to avoid confusion when everybody speaks up during conference.

1.3.2 TOE security functions

The following table highlights the range of security functions and features implemented by the TOE.

Security function	Description
Secure Communication	The TOE provides a secure SSL session between the client and the server.

Security function	Description
Identification and authentication	The TOE provides identification and authentication of users before users are allowed to access the functionality of the TOE.
Security Management	The TOE provides functions that allow management of the TOE and its security functions. The TOE restricts access to the management functions based on the role of the user.
User Data Protection	The TOE manages access control on configuration data and functions based on user roles and access control lists.

1.3.3 Supporting hardware, software and/or firmware

The requirements for each of the component of the TOE are described as below:

1. **NLVC Server and NLVC Server Webadmin Tool**

   The minimum hardware requirements:

   - X86 based processor
   - Intel core 2 Duo processor
   - Minimum 1 Gigabyte of RAM
   - Minimum 20 Gigabyte of Hard Disk Space
   - 2 x10/100/1000 network interface port

   Software requirements:

   - Operating System; Linux CentOS 5.4
   - Supporting Software; SSH Server v4.3, Apache Web Server v2.2.3-6, Yum v3.0.5-1 and OpenVPN v2.0.9-1 (for secure version Only)

2. **NLVC Client using NLVC Boardroom Codec System**

   Software requirements:

- NLVC Boardroom Codec System is a standalone customized Windows based application and can be installed on the following windows platform; Windows 2000, Windows XP, Windows 2003, Windows Vista and Windows 7.

1.4 TOE description

1.4.1 Physical scope of the TOE

The TOE is a client-server based video conferencing system. A typical installation of the TOE can be found in Figure 1 below and identifies the various components of the NLVC architecture.

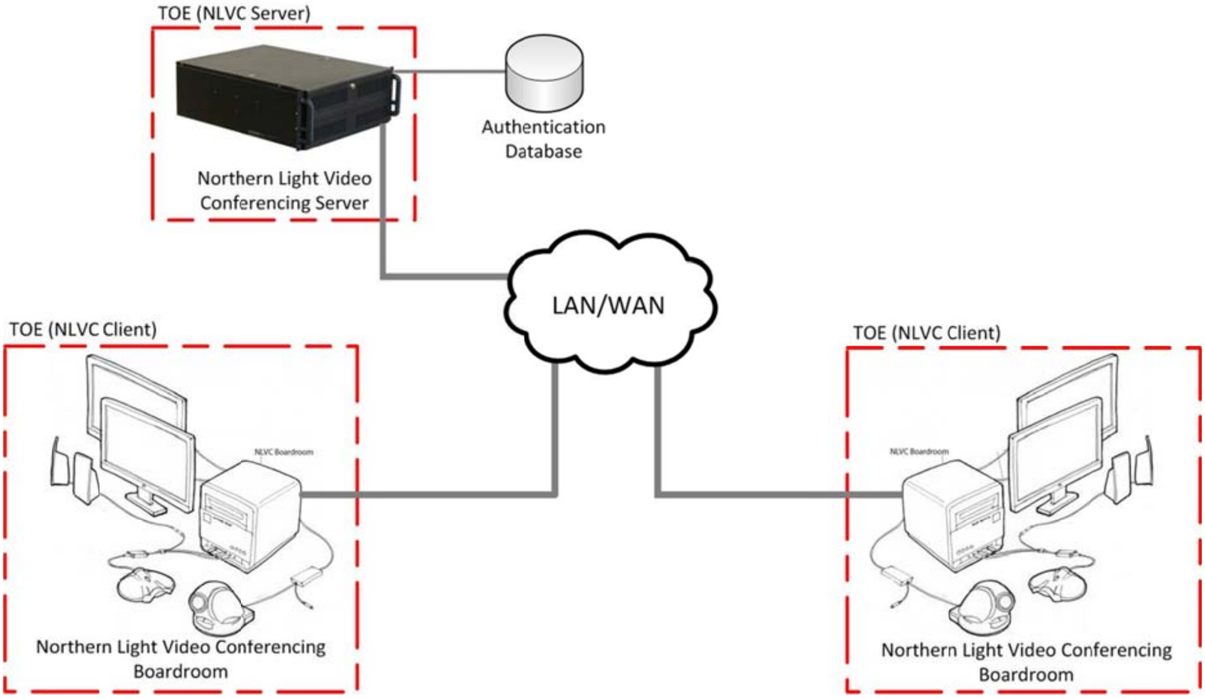
TOE (NLVC Server)
Northern Light Video Conferencing Server
Authentication Database
LAN/WAN
TOE (NLVC Client)
NLVC Boardroom
Northern Light Video Conferencing Boardroom
TOE (NLVC Client)
NLVC Boardroom
Northern Light Video Conferencing Boardroom

Figure 1 – NLVC architecture

1.4.1.1 NLVC System Server

NLVC server employs the RSW control criteria, which is a set of rules that uses the client-server style of communications. The main purpose of the NLVC server is to maintain and control conference according to the RSW control criteria used.

The functions of the server include:

- Controlling the conference using the chosen RSW control criteria

- Allowing users to login into the system
- Allowing users to change passwords
- Establishing inter-server links (during multi-server conferences)

The scope of the TOE will not include the multi-server conferencing and will only have 1 NLVC server in the evaluated configuration.

1.4.1.2 NLVC System Client

NLVC client is the user based GUI application that works on the end user's PC or NLVC boardroom codec system as shown in Figure 1 above.

The NLVC boardroom codec system is a standalone platform with a high resolution monitor, Windows system, camera, and advanced echo cancellation system whereas the desktop can be any windows based system. NLVC client (TOE) runs on these 2 types of platforms.

There are 2 main modules of the client. They are NLVC Main Control and NLVC Conference Monitor.

Functions of Main Control:

- Provides controls to create conference and join conferences (NLVC mode)
- Provides controls to call and hang up for H.322 mode
- Provides communication interface with NLVC server
- Provides secure communication with NLVC server
- Provides control for login and logout
- Provides feedback of client and server messages to users
- Loads and handles synchronization of NLVC conference monitor and H323 module
- Provides controls to switch between H.323 mode, normal NLVC mode and secure NLVC mode (only secure NLVC mode will be in the evaluated configuration)

Functions of Conference Monitor

- Loads and handles synchronization of audio, video and document conferencing modules (only video conferencing module will in the scope of the evaluation)
- Provides controls to access video conferencing audio/video/document conferencing features
- Provides controls to Start/Stop transmission for the Chairman role and active users
- Aligns video windows relative to the screen
- Provides the control for muting the speaker/microphone
- Shows Mic In Peakmeter/indicator
- Set Video resolution/frame rate/property

- Provides controls for conference for users
- Provides user status information (eg. Participant/observer/joined active)

1.4.2 Logical scope of the TOE

The logical boundary consists of the security functionality of TOE is summarized below.

1.4.2.1 Identification & Authentication

The TOE requires that the users identify and authenticate themselves before performing any TSF mediated action on behalf of the user. The TOE checks the credentials presented by the user upon the login module of the client against the authentication information in the database.

The TOE also identifies and authenticates NLVC Clients through the use of certificates.

1.4.2.2 Secure Communication

The TOE protects the video feeds and command data when they are transmitted between the server and the client through the establishment of a SSL channel.

1.4.2.3 Security Management

The TOE contains various management functions to ensure efficient and secure management of the TOE.

The TOE maintains 4 roles within the TOE to ensure that the functions are restricted to only those users that need to have access to privileged functions. The roles maintained by the TOE are: Chairman, Participant, Observer and Administrator.

1.4.2.4 User Data Protection

The access control function permits a user to access configuration data and functions only if a user role of the user has permission to perform the requested action.

It also permits a NLVC client with a valid certificate to request to establish a secure SSL channel with the NLVC Server.

2 Conformance Claim (ASE_CCL)

The ST and TOE are conformant to version 3.1 (REV 3) of the Common Criteria for Information Technology Security Evaluation.

The following conformance claims are made for the TOE and ST:

- Part 2 conformant. Conformant with Common Criteria for Information Technology Security Evaluation Part 2: Security functional requirements, version 3.1 (REV 3) July 2009.
- Part 3 conformant, EAL2. Conformant with Common Criteria for Information Technology Security Evaluation Part 3: Security assurance requirements, version 3.1, (REV 3). Evaluation is EAL2, July 2009

3 Security Problem Definition

3.1 Threats

Identifier	Statements
T.ACCESS	A valid user obtains or modifies stored user data that they are not authorised to access resulting in a loss of confidentiality or integrity of the data.
T.SNIFFING	An attacker may get access to the user data over the WAN/LAN when a video conferencing session is taking place.
T.MANAGEMENT	A valid user or external attacker modifies management data that they are not authorised to access resulting in a loss of integrity of the data that the TOE uses to enforce the security functions.
T.PASSWORD	An unauthorized user gains access to the passwords in the database and use them to authenticate to the TOE resulting in a loss of confidentiality or integrity of user or management data.

3.2 Assumptions

The following assumptions govern the operational environment of the TOE:

Identifier	Statements
A.ENVIRONMENT	The TOE environment will provide appropriate authentication and authorisation controls for all users and administrators in the underlying environment (including the Operating System, RDBMS)
A.TRUST	The TOE environment is free of vulnerabilities that allow an attacker to bypass the TOE security functions.
A.ADMIN	It is assumed that the administrator who manages the TOE is not hostile and is competent.
A.PHYSICAL	It is assumed that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by

	the TOE.
A.DATABASE	It is assumed that the databases in the TOE environment have been correctly configured according to the principle of least privilege.
A.MANAGEMENT	All management of the TOE will be performed through the management interfaces of the TOE and not through the underlying environment.
A.CRYPTO	It is assumed that the encryption of user password in the TOE environment have been performed to ensure confidentiality or integrity of user or management data.

4 Security objectives (ASE_OBJ)

4.1 Security objectives for the TOE

Identifier	Objective statements
O.ACCESS	The TOE must ensure that only authorised users and NLVC clients are able to access the TOE functions.
O.USER	The TOE must ensure that all users and NLVC Clients are identified and authenticated before they access the TOE functions.
O.MANAGE	The TOE must allow administrators to effectively manage the TOE, while ensuring that appropriate control is maintained over those functions. .
O.PASSWORD	The TOE must ensure that passwords stored in the database are not in clear plaintext.
O.COMMS	The TOE must ensure that the user data is protected against disclosure when transmitting between the client and the server.

4.2 Security objectives for the environment

Identifier	Objective statements
OE.ENVIRONMENT	Those responsible for the TOE must ensure that appropriate authentication and authorisation controls for all users and administrators in the underlying environment (including the Operating System, RDBMS, and Web Server)
OE.TRUST	Those responsible for the TOE must ensure that the TOE environment is free of vulnerabilities that allow an attacker to bypass the TOE security functions.
OE.ADMIN	The owners of the TOE must ensure that the administrator who manages the TOE is not hostile and is competent.
OE.PHYSICAL	Those responsible for the TOE must ensure that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.

OE.DATABASE	Those responsible for the TOE must ensure that the databases in the TOE environment have been correctly configured according to the principle of least privilege.
OE.MANAGEMENT	Those responsible for the TOE must ensure that all management of the TOE is performed through the management interfaces of the TOE and not through the underlying environment.
OE. CRYPTO	Those responsible for TOE must ensure the Users' passwords in the TOE environment are encrypted.

5 Security requirements (ASE_REQ)

5.1 Overview

This section defines the security requirements satisfied by the TOE. Each requirement has been extracted from version 3.1 of the Common Criteria, part 2 providing functional requirements and part 3 providing assurance requirements.

5.2 SFR conventions

Part 2 of the Common Criteria defines an approved set of operations that may be applied to security functional requirements. Following are the approved operations and the document conventions that are used within this ST to depict their application:

- **Assignment.** The assignment operation provides the ability to specify an identified parameter within a requirement. Assignments are depicted using bolded text and are surrounded by square brackets as follows [**assignment**].

- **Selection.** The selection operation allows the specification of one or more items from a list. Selections are depicted using bold italics text and are surrounded by square brackets as follows [***selection***].

- **Refinement.** The refinement operation allows the addition of extra detail to a requirement. Refinements are indicated using bolded text, for **additions**, and strike-through, for ~~deletions~~.

- **Iteration.** The iteration operation allows a component to be used more than once with varying operations. Iterations are depicted by placing a slash "/" at the end of the component identifier and a unique name for the iteration FDP_IFF.1/xxx and FDP_IFF.1/yyy.

5.3 Security functional requirements

5.3.1 Overview

The security functional requirements are expressed using the notation stated in Section 5.2 and summarized in the table below.

Identifier	Title
FCS_COP.1	Cryptographic operation
FDP_ACC.1	Subset access control
FDP_ACF.1	Security attribute based access control
FDP_IFC.1	Subset information flow control
FDP_IFF.1	Simple security attributes
FDP_ITT.1	Basic internal transfer protection
FIA_UAU.2/User	User authentication before any action
FIA_UAU.2/ NLVC Client	User identification before any action
FIA_UID.2/User	User identification before any action
FIA_UID.2/NLVC Client	User identification before any action
FMT_MOF.1	Management of security functions behaviour
FMT_MSA.1/Access Control SFP	Management of security attributes
FMT_MSA.1/Communication SFP	Management of security attributes
FMT_MSA.3/Access Control SFP	Static attribute initialisation

Identifier	Title
FMT_MSA.3/Communication SFP	Static attribute initialisation
FMT_MTD.1/Default	Management of TSF data
FMT_MTD.1/Users	Management of TSF data
FMT_MTD.1/Password	Management of TSF data
FMT_SMF.1	Specification of management functions
FMT_SMR.1	Security roles
FPT_ITT.1	Basic internal TSF data transfer protection

5.3.2 FCS_COP.1 Cryptographic operation

Hierarchical to:	No other components.
FCS_COP.1.1	The TSF shall perform [**hashing**] in accordance with a specified cryptographic algorithm [**SHA256**] and cryptographic key sizes [**none**] that meet the following: [**FIPS 180-2**].
Dependencies:	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction
Notes:	This cryptographic operation does not use key. The password of the users is hashed and compare with the values stored in the authentication data database.

5.3.3 FDP_ACC.1 Subset access control

Hierarchical to:	No other components.
FDP_ACC.1.1	The TSF shall enforce the [**Access Control SFP**] on [**Subjects:** **a) TOE users** **Objects:** **a) TOE configuration data** **b) Functions** **Operations:** **a) Manipulate**]
Dependencies:	FDP_ACF.1 – Security attribute based access control
Notes:	None.

5.3.4 FDP_ACF.1 Security attribute based access control

Hierarchical to:	No other components.
FDP_ACF.1.1	The TSF shall enforce the [**Access Control SFP**] to objects based on the following: [**Subject attribute:** **a) ID of the user** **b) corresponding user role** **Object attributes:** **a) Access Control List**]
FDP_ACF.1.2	The TSF shall enforce the following rules to determine if an operation among controlled subjects and controlled objects is allowed: [**The operation is allowed, if:** **a) The Access Control List for an object permits the user ID to access that object; AND** b) **The Access Control List for an object permits the User Role to access that Object.**]
FDP_ACF.1.3	The TSF shall explicitly authorise access of subjects to objects based on the following additional rules: [**the Administrator role can access all functions and data**].
FDP_ACF.1.4	The TSF shall explicitly deny access of subjects to objects based on the following additional rules: [**None**].
Dependencies:	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation
Notes:	None.

5.3.5 FDP_IFC.1 Subset information flow control

Hierarchical to:	No other components.
FDP_IFC.1.1	The TSF shall enforce the [**Communication SFP**] on [**NLVC server and client when**

	the client machine requests a secure channel between the NLVC server and client for transmitting and receiving and transmitting user data].
Dependencies:	FDP_IFF.1 Simple security attributes
Notes:	None.

5.3.6 FDP_IFF.1 Simple security attributes

Hierarchical to:	No other components.
FDP_IFF.1.1	The TSF shall enforce the [**Communication SFP**] based on the following types of subject and information security attributes: [**a) Identification and authentication of the client machine**].
FDP_IFF.1.2	The TSF shall permit an information flow between a controlled subject and controlled information via a controlled operation if the following rules hold: [**a) For the transmission of user data from the NLVC server and the NLVC client; the requesting client machine has been identified as authorised by the server using certificates.**]
FDP_IFF.1.3	The TSF shall enforce the [**no additional information flow control SFP rules**].
FDP_IFF.1.4	The TSF shall explicitly authorise an information flow based on the following rules: [**none**].
FDP_IFF.1.5	The TSF shall explicitly deny an information flow based on the following rules: [**none**].
Dependencies:	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation
Notes:	None.

5.3.7 FDP_ITT.1 Basic internal transfer protection

Hierarchical to:	No other components.
FDP_ITT.1.1	The TSF shall enforce the [***access control SFP(s)***] to prevent the [***disclosure, modification, loss of use***] of user data when it is transmitted between physically-separated parts of the TOE.
Dependencies:	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control
Notes:	None.

5.3.8 FIA_UAU.2/User - User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication
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
Notes:	User Credentials for Employees and Supervisors only exist within a specific organisation.

5.3.9 FIA_UAU.2/ NLVC Client - User authentication before any action

Hierarchical to:	FIA_UAU.1 Timing of authentication
FIA_UAU.2.1	The TSF shall require each NLVC Client to be successfully authenticated before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

5.3.10 FIA_UID.2/User - User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
FIA_UID.2.1	The TSF shall require each user to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	No dependencies.
Notes:	None.
Notes:	None.

5.3.11 FIA_UID.2/NLVC Client - User identification before any action

Hierarchical to:	FIA_UID.1 Timing of identification
FIA_UID.2.1	The TSF shall require each NLVC Client to be successfully identified before allowing any other TSF-mediated actions on behalf of that user.
Dependencies:	No dependencies.
Notes:	None.

5.3.12 FMT_MOF.1 Management of security functions behaviour

Hierarchical to:	No other components.
FMT_MOF.1.1	The TSF shall restrict the ability to [***determine the behaviour of, disable, enable, modify the behaviour of***] the functions [**all functions**] to [**the users with appropriate permissions**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.3.13 FMT_MSA.1/Access Control SFP - Management of security attributes

Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the [**Access Control SFP**] to restrict the ability to [***write or delete***] the security attributes [**that map user Ids to roles only the users that are mapped**] to [**None**].
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.3.14 FMT_MSA.1/Communication SFP - Management of security attributes

Hierarchical to:	No other components.
FMT_MSA.1.1	The TSF shall enforce the [**Communication SFP**] to restrict the ability to [***create, modify, delete***] the security attributes [**identification and authentication of NLVC clients**] to [**Administrator**].
Dependencies:	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.3.15 FMT_MSA.3/Access Control SFP - Static attribute initialisation

Hierarchical to:	No other components.

FMT_MSA.3.1	The TSF shall enforce the [**Access Control SFP**] to provide [***restrictive***] default values for security attributes that are used to enforce the SFP.
FMT_MSA.3.2	The TSF shall allow [**none**] 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
Notes:	None.

5.3.16 FMT_MSA.3/Communication SFP - Static attribute initialisation

Hierarchical to:	No other components.
FMT_MSA.3.1	The TSF shall enforce the [**Communication 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 [**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
Notes:	None.

5.3.17 FMT_MTD.1/Default – 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***] the [**TOE configuration data**] to [**Users with appropriate permission**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	User: Administrator.

5.3.18 FMT_MTD.1/Users – Management of TSF data

Hierarchical to:	No other components
FMT_MTD.1.1	The TSF shall restrict the ability to [***query, modify, delete, clear*** **[Create]**] the [**User accounts**] to [**Administrator**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	None.

5.3.19 FMT_MTD.1/Password – Management of TSF data

Hierarchical to:	No other components
FMT_MTD.1.1	The TSF shall restrict the ability to [***modify***] the [**User Password**] to [**users (that is related to the password)**].
Dependencies:	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions
Notes:	User: Administrator

5.3.20 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 management functions: [**security attribute management, TSF data management, and security function management**]
Dependencies:	No dependencies.
Notes:	None.

5.3.21 FMT_SMR.1 Security roles

Hierarchical to:	No other components.
FMT_SMR.1.1	The TSF shall maintain the roles [**chairman, participant, observer and administrator**].
FMT_SMR.1.2	The TSF shall be able to associate users with roles.
Dependencies:	FIA_UID.1 Timing of identification
Notes:	None.

5.3.22 FPT_ITT.1 Basic internal TSF data transfer protection

Hierarchical to:	No other components.
FPT_ITT.1.1	The TSF shall protect TSF data from [***disclosure***] when it is transmitted between separate parts of the TOE.
Dependencies:	No dependencies.
Notes:	None.

5.4 TOE security assurance requirements

Assurance class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.2 Security-enforcing functional specification
	ADV_TDS.1 Basic design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life cycle support	ALC_CMS.2 Use of a CM system
	ALC_CMC.2 Parts of the TOE CM coverage
	ALC_DEL.1 Delivery procedures
ASE: Security Target evaluation	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST Introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security Problem Definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_IND.2 Independent testing - sample
	ATE_FUN.1 Functional testing
	ATE_COV.1 Evidence of coverage
AVA: Vulnerability assessment	AVA_VAN.2 Vulnerability analysis

5.5 Defined terms

The following table defines all subjects, objects, operations, security attributes, external entities and other key terms that are used within the statements of security functional and assurance requirements. It also describes the acronym used in this documentation.

Term/Acronym	Definition
NLVC	Northern Light Video Conferencing System
RSW (Real Time Switching) Control Criteria	RSW Control Criteria is an advanced set of controls for Multimedia Conferencing that focused more on bandwidth reduction and prioritizes the participants to avoid confusion when everybody speaks up during conference.
Hashing	A procedure or mathematical function that changes large data into smaller data. Mostly, the value is used to check for any modification in the data and to ensure that an attacker cannot see sensitive information in plain text.
Unicast Technology	Data transmission technology that transmit the same data to all possible destinations.
Multicast Technology	Data transmission technology that transmit data only to interested destinations by using special address assignments
SSL (Secure Sockets Layer)	Protocol that helps to protect data integrity that is transmitting in the network by encrypting the data itself.
SHA-256	Types of cryptographic hash function.
WAN (Wide Area Network)	A computer network that covers a broad area / public telecommunication infrastructure, such as internet.
LAN (Local Area Network)	A computer network that interconnects computers in a limited area such as a home, school, computer laboratory, or office building.
VPN (Virtual Private Network)	A techniques for creating secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities.
OpenVPN	A free and open source software application that implements virtual private network .

6 TOE summary specification (ASE_TSS)

6.1 Overview

This section provides the TOE summary specification, a high-level definition of the security functions claimed to meet the functional and assurance requirements.

The TOE security functions include the following:

- User Data Protection
- Identification and Authentication
- Security Management
- Secure Communication

6.1.1 Secure Communication

The TOE uses the OpenVPN library to create a secured VPN tunnel between the client and server ensuring that the video feeds and TSF data are protected against disclosure (**FDP_ITT.1, FPT_ITT.1**)

6.1.2 Identification and Authentication

When a user logon using the NLVC client, the TOE requires that the user identify and authenticate themselves before performing any TSF mediated action on behalf of the user (**FIA_UID.2/User, FIA_UAU.2/User**). The TOE checks the credentials presented by the user against the authentication information in the database.

All users presented passwords are hashed before being used to authenticate the user or when users change their passwords (**FMT_MTD.1/Password**) and is being written to the database. This is all done by the TOE (**FCS_COP.1**).

Administrators will login to the NLVC server through another interface. This is a web interface and can only be accessed by the administrator.

The TOE also checks the authenticity of the NLVC clients when they are requesting to establish a secure channel to the NLVC Server. This is done through the use of digital certificates which are pre-installed on the client side (**FIA_UAU.2/NLVC Client, FIA_UID.2/NLVC Client**).

6.1.3 Security Management

The TOE contains various management functions to ensure efficient and secure management of the TOE (**FMT_SMF.1**):

a) **User Management**

The TOE only Administrator to query, create, delete, and modify users (**FMT_MTD.1/Users**). All users can change their password only (**FMT_MTD.1/Users**).

b) **Permission Management for Functions and Data**

The one who starts the video session will have the chairman role. Only the chairman can invite users to the video conferencing session and assign them roles (participants or observers) (**FMT_MTD.1/Default, FMT_MSA.1/Access Control SFP**). The administrator of the TOE can configure the certificate settings on the NLVC server side for identification and authentication of NLVC Clients (**FMT_MSA.1/Communication SFP**).

c) **Configuration of session**

When the user setup the video conferencing session, he/she can edit the settings of the video conferencing (SSL, protocols, etc) (**FMT_MTD.1/Default**).

The TOE maintains 4 roles (**FMT_SMR.1**) within the TOE to ensure that the functions are restricted to only those users that need to have access to privileged functions. The functions above, and indeed, aspects of these functions, are restricted based on these roles.

The TOE allows no one to change the default values of the TSF data and security attributes of the TOE (**FMT_MSA.3/ Access Control SFP**) but only allows the administrator to change the security attributes for the identification and authentication of NLVC client through digital certificates (**FMT_MSA.3/Communication SFP**).

6.1.4 User Data Protection

The TOE enforces an access control policy on TOE configuration data and functions. After a user identifies and authenticates to the TOE, he or she can establish a video conferencing session. The one who creates the session will be the chairman.

Only the chairman can invite users to the session and choose the role the other users can take. They can be a participant where the users can speak during the session, or an observer where the user can only hear and see the session but not speak at all. The Chairman also set up the configuration for the video conferencing session. (**FDP_ACC.1, FDP_ACF.1**).

The TOE also enforces a Communication SFP on the establishment of a secure channel between the NLVC Clients and the NLVC server. Only a NLVC client with a valid certificate can establish a secure VPN channel with the NLVC server (**FDP_IFF.1, FDP_IFC.1**).

There are 4 types of users maintained by the TOE. They are Chairman, Participant, Observer and Administrator (**FMT_SMR.1**). Chairman, Participant and Observer are conference users with different access rights to TOE functions during the conference session. Administrator is a user that can only access the management functions through web interface that has access rights to TOE configuration data and TOE Functions.

7 Rationale

7.1 Security objectives rationale

Security objectives rationale is provided to demonstrate that the treats are countered and the assumptions are met.

7.1.1 Threat Rationale

Threats	Objective	Justification
T.ACCESS	O.ACCESS	The objective ensures that the TOE restricts access to the TOE objects to the authorized users and NLVC clients.
T.MANAGEMENT	O.USER O.MANAGE O.ACCESS	The objective ensures that the TOE restricts access to the TOE objects to the authorized users This objective ensures that the TOE provides the tools necessary for the authorized administrator to manage the security-related functions and that those tools are usable only by users with appropriate authorizations. The objective ensures that the TOE restricts access to the TOE objects to the authorized users
T.SNIFFING	O.COMMS	The objective ensures that the user data and TSF data are protected against disclosure when transmitting between the client and the server.
T.PASSWORD	O.PASSWORD	The objective ensures that all passwords stored in the database are hashed using SHA256 before written to the database. No one can see the password in plaintext and will not be able to use the password to authenticate to the TOE.

7.1.2 Assumption Rationale

Below provides a mapping of the Security objectives for the environment of the TOE to relevant assumptions, as well as a justification for the mapping.

Assumptions	Objective	Justification
A.ADMIN	OE.ADMIN	This objective ensures that those responsible for the TOE are competent and trustworthy individuals, capable of managing the TOE and the security of the information it contains.
A.ENVIRONMENT	OE.ENVIRONMENT	This objective ensures that there are appropriate authentication and authorisation controls for all users and administrators in the underlying environment (including the Operating System, RDBMS.
A.PHYSICAL	OE.PHYSICAL	This objective ensures that the IT environment provides the TOE with appropriate physical security, commensurate with the value of the IT assets protected by the TOE.
A.DATABASE	OE.DATABASE	This objective ensures that the databases in the TOE environment have been correctly configured according to the principle of least privilege.
A.MANAGEMENT	OE.MANAGEMENT	This objective ensures that all management of the TOE is performed through the management interfaces of the TOE and not through the underlying environment.
A.TRUST	OE.TRUST	This objective ensures that the TOE environment is free of vulnerabilities that allow an attacker to bypass the TOE security functions.
A.CRYPTO	OE.CRYPTO	This objective ensures that the users passwords in the TOE environment have been encrypted to ensure users credential are protected.

7.2 Security requirements rationale

7.2.1 SFR dependency rationale

Below demonstrates the mutual supportiveness of the SFR's for the TOE by demonstrating how the SFR dependencies are fulfilled by the TOE, and by justifying those dependencies that are not fulfilled.

The SARs relevant to the TOE constitute an evaluation assurance level EAL2 as defined in Common Criteria and include no extensions or augmentations. Therefore, as a complete evaluation assurance level, they are a mutually supportive set and require no further justification.

SFR	Dependency	Inclusion
FCS_COP.1	[FDP_ITC.1 Import of user data without security attributes, or FDP_ITC.2 Import of user data with security attributes, or FCS_CKM.1 Cryptographic key generation] FCS_CKM.4 Cryptographic key destruction	None. Hashing does not include any cryptographic keys.
FDP_ACC.1	FDP_ACF.1 Security attribute based access control	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1 Subset access control FMT_MSA.3 Static attribute initialisation	FDP_ACC.1 FMT_MSA.3/Access Control SFP
FDP_IFC.1	FDP_IFF.1 Simple security attributes	FDP_IFF.1
FDP_IFF.1	FDP_IFC.1 Subset information flow control FMT_MSA.3 Static attribute initialisation	FDP_IFC.1 FMT_MSA.3/Communication SFP
FDP_ITT.1	FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control	FDP_IFC.1
FIA_UAU.2/Users	FIA_UID.1 Timing of identification	FIA_UID.2/User

SFR	Dependency	Inclusion
FIA_UAU.2/NLVC Clients	FIA_UID.1 Timing of identification	FIA_UID.2/NLVC Client
FIA_UID.2/Users	No dependencies	N/A
FIA_UID.2/NLVC Clients	No dependencies	N/A
FMT_MOF.1	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 FMT_SMR.1
FMT_MSA.1/Access Control SFP	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_ACC.1 FMT_SMF.1 FMT_SMR.1
FMT_MSA.1/Communication SFP	[FDP_ACC.1 Subset access control, or FDP_IFC.1 Subset information flow control] FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FDP_IFC.1 FMT_SMF.1 FMT_SMR.1
FMT_MSA.3/Access Control SFP	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1/Access Control SFP FMT_SMR.1
FMT_MSA.3/Communication SFP	FMT_MSA.1 Management of security attributes FMT_SMR.1 Security roles	FMT_MSA.1/Communication SFP FMT_SMR.1

SFR	Dependency	Inclusion
FMT_MTD.1/Default	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 FMT_SMR.1
FMT_MTD.1/Users	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 FMT_SMR.1
FMT_MTD.1/Password	FMT_SMR.1 Security roles FMT_SMF.1 Specification of Management Functions	FMT_SMF.1 FMT_SMR.1
FMT_SMF.1	No dependencies	N/A
FMT_SMR.1	FIA_UID.1 Timing of identification	FIA_UID.2/User
FPT_ITT.1	No dependencies	N/A

7.2.2 Tracing of SFR to security objectives

Below provides the mapping of the TOE SFRs and the security objectives for the TOE.

Objective	SFR and Demonstration
O.ACCESS	**FDP_ACC.1**: The requirement helps meets the objective by identifying the objects and users subjected to the access control policy. **FDP_ACF.1**: The requirement meets this objective by ensuring the TOE only allows access to objects based on the defined access control policy. **FDP_IFC.1:** The requirement helps meets the objective by identifying the objects and users subjected to the Communicate SFP. **FDP_IFF.1:** The requirement meets this objective by ensuring the TOE only allows request for secure VPN channel establishment based on the defined Communicate SFP.
O.USER	**FIA_UID.2/User**: The requirement helps meets the objective by identifying the users before any TSF mediated actions.

Objective	SFR and Demonstration
	FIA_UID.2/NLVC Client: The requirement helps meets the objective by identifying NLVC Clients before any TSF mediated actions. **FIA_UAU.2/User**: The requirement helps meets the objective by authenticating the users before any TSF mediated actions. **FIA_UAU.2/NLVC Client**: The requirement helps meets the objective by authenticating the NLVC Clients before any TSF mediated actions. **FMT_SMR.1**: The TOE manages 4 roles: Chairman, participant, observer and Administrator.
O.PASSWORD	**FCS_COP.1:** The requirement helps to meet the objective by hashing all the passwords using SHA256 before they are written into the database.
O.MANAGE	**FMT_MSA.1/Access Control SFP**: The TOE allows the super administrator to determine who will have access to the folder and the folder's contents and what actions the user can be perform. **FMT_MSA.1/Communication SFP**: The TOE allows the administrator to determine who will have access to the establishment of secure VPN channel function. **FMT_MSA.3/Access Control SFP**: The TOE enforces a restrictive access when a new object is created. The TOE has a default ACL which is assigned to all newly-created objects. This default ACL cannot be altered by any user. **FMT_MSA.3/Communication SFP**: Only administrator has access to the TOE for the purposes of initializing security attributes. The security attributes are used for mutual identification and authentication between the NLVC Server and NLVC clients. **FMT_MTD.1/Default:** This requirements helps meet the objective by allowing no one to change the default values of the TSF data. **FMT_MTD.1/Password:** This requirement helps meet the objective by allowing users to change their passwords. **FMT_MTD.1/Users:** This requirements helps meet the objective by allowing only the Administrators roles to create, delete, modify user accounts. **FMT_SMF.1**: The TOE provides the functions for security attribute management, TSF data management, and security function management. **FMT_SMR.1**: The TOE manages 4 roles: Chairman, participant, observer and

Objective	SFR and Demonstration
	Administrator.
O.COMMS	**FDP_ITT.1:** The TOE provides a SSL channel protecting the user data from disclosure and modification when it is transmitting between the NLVC client and NLVC Server. **FPT_ITT.1:** The TOE provides a SSL channel protecting the TSF data from disclosure when it is transmitting between the NLVC client and NLVC Server.

7.2.3 SAR justification

The assurance package for the evaluation of the TOE is Evaluation Assurance Level 2 (EAL2).

The TOE is intended to protect confidential information related to a business's employees. This information, while sensitive within an organization, the value to an attacker is relatively low. As such, it is considered that the average motivation of attackers will be low, which implies that the overall attack potential for this TOE will be LOW. EAL2 is sufficient to demonstrate that the TOE is resistant to attackers with a LOW attack potential.