Swedish Certification Body for IT Security

Certification Report - NetMotion Mobility 12.14

Issue: 1.0, 2021-dec-08

Authorisation: Ulf Noring, Lead Certifier , CSEC

SWEDAC · ACKREDITERING ·
Accred. no. 1917
Certification of
Products
ISO/IEC 17065

Table of Contents

1 Executive Summary

The Target of Evaluation (TOE) is NetMotion Mobility 12.14, a client/server-based software Virtual Private Network (VPN) that secures communications between the enterprise network and the mobile environment.

The TOE consists of the following software components:

- NetMotion Mobility Server 12.14.09178
- NetMotion Mobility 12.12 Client for Windows (12.12.16943)
- NetMotion Mobility 12.12 Client for Android (12.12.16943)
- NetMotion Mobility 12.13 Client for macOS (12.13.23250)
- NetMotion Mobility 12.13 Client for iOS (12.13.05677)

The main security features of the TOE are:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF

The Windows components are obtained from the NetMotion Software portal at http://www.netmotionwireless.com/customerportal. The Android, macOS and iOS clients are obtained from their respective app stores.

The TOE guidance documentation is provided in Hypertext Markup Language (HTML) format and is available to customers at:

https://help.netmotionsoftware.com/support/docs/MobilityXG/1210/help/mobilityhelp.htm

The following Common Criteria Guidance Supplement is also available to customers, in Portable Document Format (PDF), upon request:

- NetMotion Mobility® 12.14 Common Criteria Guidance Supplement
  - NetMotion_Mobility_12_EAL4_AGD0.6.pdf

The TOE claims conformance to the EAL4 package of security assurance requirements, augmented with ALC_FLR.2. It does not claim conformance to any Protection Profile (PP).

Four threats and eight assumptions are specified in chapter three in the security target [ST]. No organizational security policies (OSP) are included.

The evaluation has been performed by Intertek EWA-Canada in Kista, Sweden. The evaluation was completed on 2021-10-29. The evaluation was conducted in accordance with the requirements of Common Criteria (CC), version. 3.1 release 5.

Intertek EWA-Canada is accredited in accordance with ISO/IEC 17025 to perform evaluations against the Common Criteria standard. Accreditation was issued by the Standards Council of Canada, and has been accepted by SWEDAC, the Swedish accreditation body. This evaluation was performed as a trial evaluation for licensing with the Swedish Certification Body for IT Security (CSEC).

The certifier monitored the activities of the evaluator by reviewing all successive versions of the evaluation reports and by observing a site visit and performing testing oversight. The certifier determined that the evaluation results confirm the security claims in the Security Target (ST) and the Common Methodology for evaluation assurance level EAL 4 augmented by ALC_FLR.2. The technical information in this report is based on the Security Target [ST] and the Final Evaluation Report (FER) produced by Intertek EWA-Canada.

The certification results only apply to the version of the product indicated in the certificate, and on the condition that all the stipulations in the Security Target are met. This certificate is not an endorsement of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT product by CSEC or any other organisation that recognises or gives effect to this certificate is either expressed or implied.

As specified in the security target of this evaluation, the invocation of cryptographic primitives has been included in the TOE, while the implementation of these primitives has been located in TOE environment. Therefore the invocation of cryptographic primitives has been in the scope of this evaluation, while correctness of implementation of cryptographic primitives been excluded from the TOE. Correctness of implementation is done through third party certification using the CAVP certificates referred to in tables 11, 12 and 13 of the Security Target.

Users of this product are advised to consider their acceptance of this third party affirmation regarding the correctness of implementation of the cryptographic primitives.

2 Identification

Certification Identification	
Certification ID	CSEC2020018
Name and version of the certified IT product	NetMotion Mobility 12.14
Security Target Identification	NetMotion Mobility 12.14 Security Target, NetMotion Software Inc., 2021-10-15, document version 0.15
EAL	EAL 4 + ALC_FLR.2
Sponsor	NetMotion Software, Inc.
Developer	NetMotion Software, Inc.
ITSEF	Intertek EWA-Canada
Common Criteria version	3.1 revision 5
CEM version	3.1 revision 5
QMS version	2.0
Scheme Notes Release	18.0
Recognition Scope	CCRA, SOGIS and EA/MLA
Certification date	2021-12-10

3 Security Policy

The main security features of the TOE are:

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Protection of the TSF

A brief description of these features is provided below. A more detailed description can be found in chapter 7 in the [ST].

3.1 Security Audit

The TOE generates audit records for security events. Only those roles that have been granted specific access to the audit trail are able to view the audit records. For the purpose of this evaluation, only users in the Administrator role have been granted this access.

3.2 Cryptographic Support

The TOE supports secure communications between TOE components. This encrypted traffic prevents modification and disclosure of user information. Cryptographic functionality is provided by FIPS 140-2 validated modules in the operating systems of the server and client components. Cryptography is also supported for the authentication of users.

3.3 User Data Protection

The TOE provides an information flow security policy. The security policy limits access to internal protected resources based on policy settings. The TOE provides a secure connection between mobile users and the internal network. Traffic is protected from disclosure and modification.

3.4 Identification and Authentication

The TOE verifies that users are identified and authenticated before permitting access. Additionally, administrators must be identified and authenticated before access to administrative functions is permitted.

3.5 Security Management

The TOE provides security management functions through the Mobility Console. Administrators manage users, information flow policies, and audit records.

3.6 Protection of the TSF

Reliable timestamps are provided on the Mobility Server in support of TOE functions, including the generation of audit records.

4 Assumptions and Clarification of Scope

4.1 Usage Assumptions

The Security Target [ST] makes two assumptions on the usage of the TOE:

A.MANAGE

A management console computer is available on the internal protected network for the purposes of managing the TOE. Administrators will access the Mobility Console only from a management console computer on the internal network.

A.NOEVIL

Authorized administrators are non-hostile and follow all administrative guidance.

4.2 Environmental Assumptions

The Security Target [ST] makes six assumptions on the operational environment of the TOE.

A.AUTH

The operational environment provides authentication services to the TOE.

A.CERTIFICATE

A PKI is available to issue certificates to users and servers. Root trust exists for the certificate chain.

A.INTERNAL

The internal network and its assets are protected from unauthorized access. A firewall must be in place to ensure that only authorized connections from Mobility Clients to the Mobility Server are permitted.

A.OS

The services, including cryptographic services, provided by the underlying operating system work correctly, and the operating system does not introduce any negative side effects to the TSF.

A.PHYSICAL

The server resources of the TOE will be located within controlled access facilities, which will prevent unauthorized physical access.

A.SECCOM

The communications between the TOE’s Mobility Server and the authentication services, and between the TOE’s Mobility Server and the management console computer are secured on an internal network.

4.3 Clarification of Scope

The Security Target contains four threats which have been considered during the evaluation.

T.ACCESS

An unauthorized individual on an external network may access and exploit protected application data resources on an internal network.

T.NOAUTH

An unauthorized individual may gain access to the TOE security management functions and use this to allow unauthorized access to application data protected by the TOE.

T.SENSDATA

An unauthorized individual may be able to view or alter sensitive application data passed between a client and a server.

T.UNAUTH

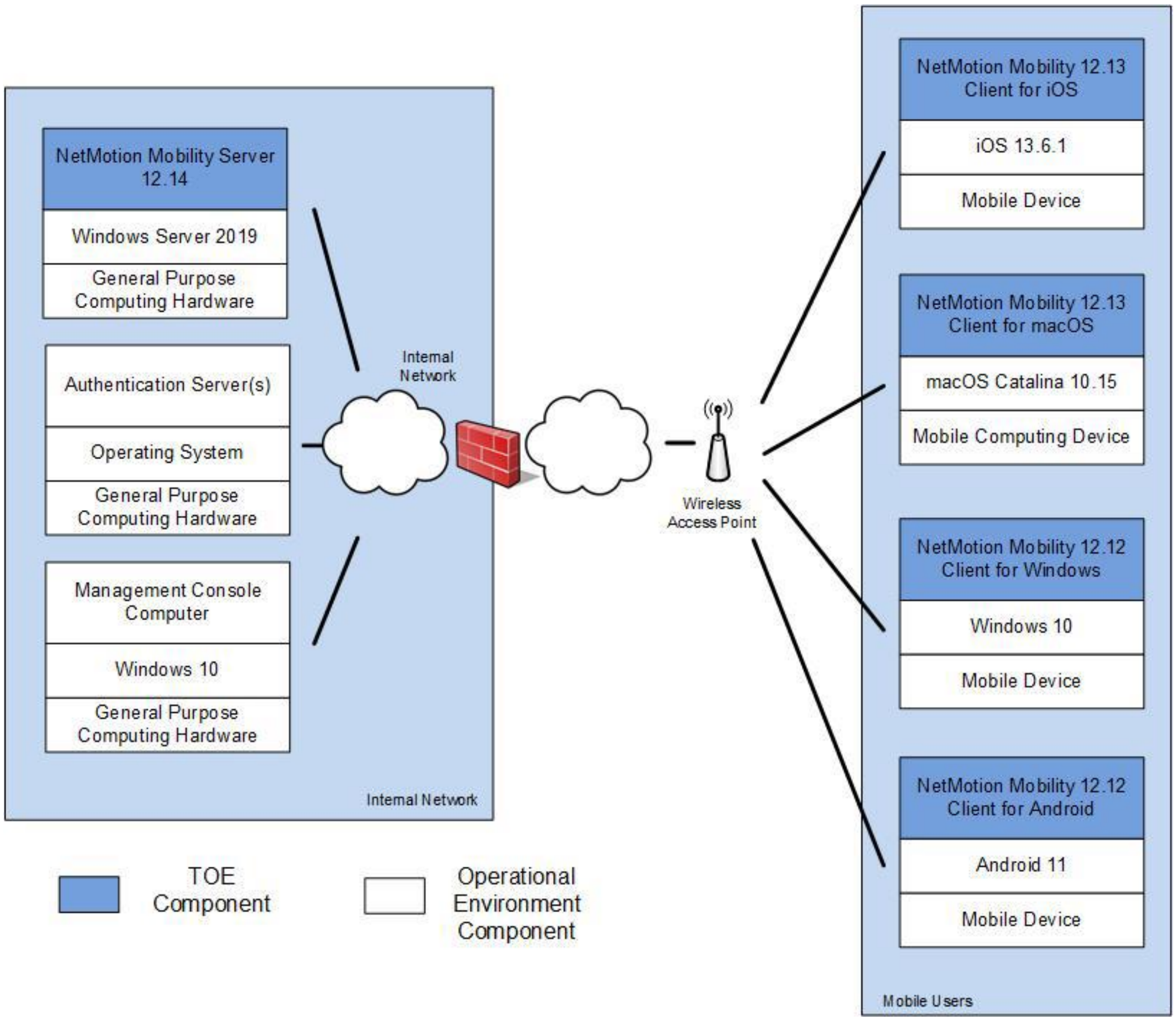
An unauthorized user may gain access to the TOE and exploit system privileges to gain access to TOE security functions and application data.

The Security Target does not include Organizational Security Policies.

5 Architectural Information

The TOE is a VPN solution that consists of a server and client architecture. Clients from various platforms connect to the NetMotion Mobility Server to establish a secure encrypted tunnel to the enterprise network.

The below diagram shows the TOE architecture and required hardware and software.


NetMotion Mobility Server 12.14
Windows Server 2019
General Purpose Computing Hardware
Authentication Server(s)
Operating System
General Purpose Computing Hardware
Management Console Computer
Windows 10
General Purpose Computing Hardware
Internal Network
Internal Network
Wireless Access Point
NetMotion Mobility 12.13 Client for iOS
iOS 13.6.1
Mobile Device
NetMotion Mobility 12.13 Client for macOS
macOS Catalina 10.15
Mobile Computing Device
NetMotion Mobility 12.12 Client for Windows
Windows 10
Mobile Device
NetMotion Mobility 12.12 Client for Android
Android 11
Mobile Device
Mobile Users
TOE Component
Operational Environment Component

6 Documentation

The following documentation comprise the TOE guidance:

HELP	NetMotion Mobility 12.1X Help
CCGS	NetMotion Mobility® 12.14 Common Criteria Guidance Supplement

7 IT Product Testing

7.1 Developer Testing

The developer tested the TSF with full coverage and depth for all TOE components. All cryptographic components have been CAVP certified. For more information on the CAVP testing, see tables 11, 12 and 13 as well as section 7.2 in the [ST]

7.2 Evaluator Testing

The evaluators repeated all of the developer test cases. The evaluators devised five independent test cases. The Windows, iOS and macOS clients were used for independent testing. This is because the Android client was used extensively for developer testing. Independent testing was performed at the Intertek EWA-Canada Common Criteria lab in Kista, Sweden during September and October 2021.

7.3 Penetration Testing

An internet search of potential vulnerabilities and scanning of the TOE using several tools was used to determine potential vulnerabilities. Penetration testing was performed to verify that these vulnerabilities were not exploitable in the evaluated configuration. Penetration testing focused on the Mobility Server component. Penetration testing was performed at the Intertek EWA-Canada Common Criteria lab in Kista, Sweden during September and October 2021.

8 Evaluated Configuration

The following hardware and software components are required to support the operation of the TOE in the evaluated configuration:

TOE Component	Required Software	Required Hardware
NetMotion Mobility 12.14 Server, version 1809	Windows Server 2019	General Purpose Computing Platform with x64-compatible dual-core processor, 2.0 GHz, 16 GB RAM
NetMotion Mobility 12.12 Windows Client, version 1909	Windows 10	General Purpose Computing Platform
NetMotion Mobility 12.13 iOS Client	iOS 13.6.1	iPad, iPhone (Apple devices with Apple A8 to A12X CPUs)
NetMotion Mobility 12.13 macOS Client	macOS 10.15	Mac mini, iMac, MacPro or MacBook hardware (Intel CPUs)
NetMotion Mobility 12.12 Android Client	Android 11	General Purpose Android device

The following environmental components are required for operation of the TOE in the evaluated configuration:

Component	Required Software	Required Hardware
Management Console	Windows 10 with Microsoft Edge 52 or later	General Purpose Computing Platform
RADIUS Authentication Server (provided as a service to the TOE)	Software supporting PEAP MS-CHAPv2 and EAP-TLS	General Purpose Computing hardware that meets the requirements of the authentication server
Public Key Infrastructure (provided as a service to the TOE)	Dependent upon the authentication server	General Purpose Computing hardware that meets the requirements of the authentication server
Firewall	Dependent on the selected appliance	General Purpose Firewall appliance

For more information, see chapter 1.4 in the [ST]. For even more detail, see the evaluated configuration guidance supplement [CCGS].

The following features are excluded from this evaluation:

- The data publisher

- NetMotion Republication Services
- Web Services API
- Unattended authentication mode
- Mobility Client API
- Mobility Event Viewer (on the Mobility Client)
- Mobility Network Access Control Module

9 Results of the Evaluation

The evaluators applied each work unit of the Common Methodology [CEM] within the scope of the evaluation, and concluded that the TOE meets the security objectives stated in the Security Target [ST] for an attack potential of Enhanced Basic.

The certifier reviewed the work of the evaluator and determined that the evaluation was conducted in accordance with the Common Criteria [CC].

The evaluators overall verdict is PASS.

The verdicts for the assurance classes and components are summarised in the following table:

Assurance Class Name / Assurance Family Name	Short name (including component identifier for assurance families)	Verdict
Security Target Evaluation	ASE	PASS
ST Introduction	ASE_INT.1	PASS
Conformance claims	ASE_CCL.1	PASS
Security Problem Definition	ASE_SPD.1	PASS
Security objectives	ASE_OBJ.2	PASS
Extended components definition	ASE_ECD.1	PASS
Derived security requirements	ASE_REQ.2	PASS
TOE summary specification	ASE_TSS.1	PASS
Life-cycle support	ALC	PASS
Use of a CM system	ALC_CMC.4	PASS
Parts of the TOE CM Coverage	ALC_CMS.4	PASS
Delivery procedures	ALC_DEL.1	PASS
Developer Security	ALC_DVS.1	PASS
Flaw reporting procedures	ALC_FLR.2	PASS
Life-cycle definition	ALC_LCD.1	PASS
Tools and Techniques	ALC_TAT.1	PASS
Development	ADV	PASS
Security architecture description	ADV_ARC.1	PASS
Security-enforcing functional specification	ADV_FSP.4	PASS
Implementation representation	ADV_IMP.1	PASS
Basic design	ADV_TDS.3	PASS
Guidance documents	AGD	PASS
Operational user guidance	AGD_OPE.1	PASS
Preparative procedures	AGD_PRE.1	PASS
Tests	ATE	PASS
Evidence of coverage	ATE_COV.2	PASS
Depth	ATE_DPT.1	PASS
Functional testing	ATE_FUN.1	PASS
Independent testing - sample	ATE_IND.2	PASS
Vulnerability Assessment	AVA	PASS
Vulnerability analysis	AVA_VAN.3	PASS

10 Evaluator Comments and Recommendations

None.

11 Glossary

CEM	Common Methodology for Information Technology Security, document describing the methodology used in Common Criteria evaluations
ITSEF	IT Security Evaluation Facility, test laboratory licensed to operate within a evaluation and certification scheme
ST	Security Target, document containing security requirements and specifications , used as the basis of a TOE evaluation
TOE	Target of Evaluation
VPN	Virtual Private Network
CAVP	Cryptographic Algorithm Validation Program

12 Bibliography

12.1 General

CC Combination of CCp1, CCp2, CCp3, and CEM (see below)

CCp1 Common Criteria for Information Technology Security Evaluation, Part 1, version 3.1, revision 5, April 2017, CCMB-2017-04-001

CCp2 Common Criteria for Information Technology Security Evaluation, Part 2, version 3.1, revision 5, April 2017, CCMB-2017-04-002

CCp3 Common Criteria for Information Technology Security Evaluation, Part 3:, version 3.1, revision 5, April 2017, CCMB-2017-04-003

CEM Common Methodology for Information Technology Security Evaluation, version 3.1, revision 5, April 2017, CCMB-2017-04-004

ST NetMotion Mobility 12.14 Security Target, NetMotion Software Inc., 2021-10-15, document version 0.15

EP-002 EP-002 Evaluation and Certification, CSEC, 2021-10-26, document version 34.0

EP-188 SP-188 Scheme Crypto Policy, CSEC, 2021-10-26, document version 12.0

12.2 Documentation

HELP NetMotion Mobility 12.1X Help, NetMotion Software Inc., 2021

CCGS NetMotion Mobility® 12.14 Common Criteria Guidance Supplement, NetMotion Software Inc., 2021-10-12, document version 0.6

Appendix A Scheme Versions

During the certification the following versions of the Swedish Common Criteria Evaluation and Certification scheme have been used.

A.1 Scheme/Quality Management System

Version	Introduced	Impact of changes
2.0	2021-11-24	None
1.25	2021-06-17	None
1.24	2020-11-19	None
1.23.2	Application	Original version

A.2 Scheme Notes

Scheme Note	**Version**	**Title**	**Applicability**
SN-15	3.0	Demonstration of test coverage	Clarify demonstration of test coverage at EAL4.
SN-18	3.0	Highlighted Requirements on the Security Target	Clarifications on the content of the ST.
SN-22	3.0	Vulnerability Assessment	Vulnerability assessment needs to be redone if 30 days or more has passed between AVA and the final version of the final evaluation report.
SN-28	1.0	Updated procedures application, evaluation and certification	Evaluator reports should be received in two batches.
SN-31	1.0	New procedures for site visit oversight and testing oversight	Site visit performed remotely.