IBM MaaS360 2.106.500.016 Cloud Extender Security Target

Version:	**1.4**
Status:	**Final**
Last Update:	**2022-07-20**
Classification:	**Public**

Trademarks

IBM, the IBM logo, ibm.com, Cloud Extender, MaaS360, the MaaS360 logo, MobileFirst Protect, and Domino are trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at https://www.ibm.com/legal/us/en/copytrade.shtml.

Common Criteria is a registered trademark of the National Security Agency, a federal agency of the United States.

Entrust is a trademark or a registered trademark of Entrust, Inc. in the United States and certain countries. All Entrust product names and logos are trademarks or registered trademarks of Entrust.

Microsoft, Windows, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

Novell is a registered trademark of Novell Inc.

OpenSSL is a trademark of The OpenSSL Software Foundation, Inc.

Oracle is a registered trademark of Oracle Corporation.

Other product and service names might be trademarks of IBM or other companies.

Legal Notice

This document is provided AS IS with no express or implied warranties. Use the information in this document at your own risk.

This document may be reproduced or distributed in any form without prior permission provided the copyright notice is retained on all copies. Modified versions of this document may be freely distributed provided that they are clearly identified as such and this copyright is included intact.

Revision History

Revision	Date	Author(s)	Changes to Previous Revision
1.4	2022-07-20	Alejandro Masino	Final

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Security Target Identification

Title:	IBM MaaS360 2.106.500.016 Cloud Extender Security Target
Version:	1.4
Status:	Final
Date:	2022-07-20
Sponsor:	IBM Corp.
Developer:	IBM Corp.
Validation Body:	NIAP
Validation ID:	VID11113
Keywords:	IBM Corp.

1.2 TOE Identification

The TOE is IBM MaaS360 version 2.106.500.016 Cloud Extender.

1.3 TOE Type

The TOE type is a software application.

1.4 TOE Overview

The TOE consists of the IBM Cloud Extender (CE) application. It includes four modules enabling communications functionality with various customer-provided services as well as the supporting documentation and a Configuration Tool, the IBM MaaS360 Cloud Extender Configuration Tool. The major security features of the TOE include cryptographic support, user data protection, Trusted Paths, and Trusted Channels.

The TOE is installed within the customer's network in order to enable services offered by the IBM MaaS360 Enterprise Mobility Management (EMM), a cloud-based multi-tenant platform that provides a mobile device management (MDM) solution. The TOE is a small Windows application (approx. 12MB) that is installed behind the customer firewall with network access to the appropriate internal systems. The TOE is not a distributed application. The TOE is not a mobile application.

Figure 1 shows the IBM MaaS360 Enterprise Mobility Management (EMM), depicting the TOE enclosed by the blue line perimeter and the trusted communication channels which are part of this evaluation. Those communication channels represented by a broken line are not part of this TOE and are not covered by the evaluation.

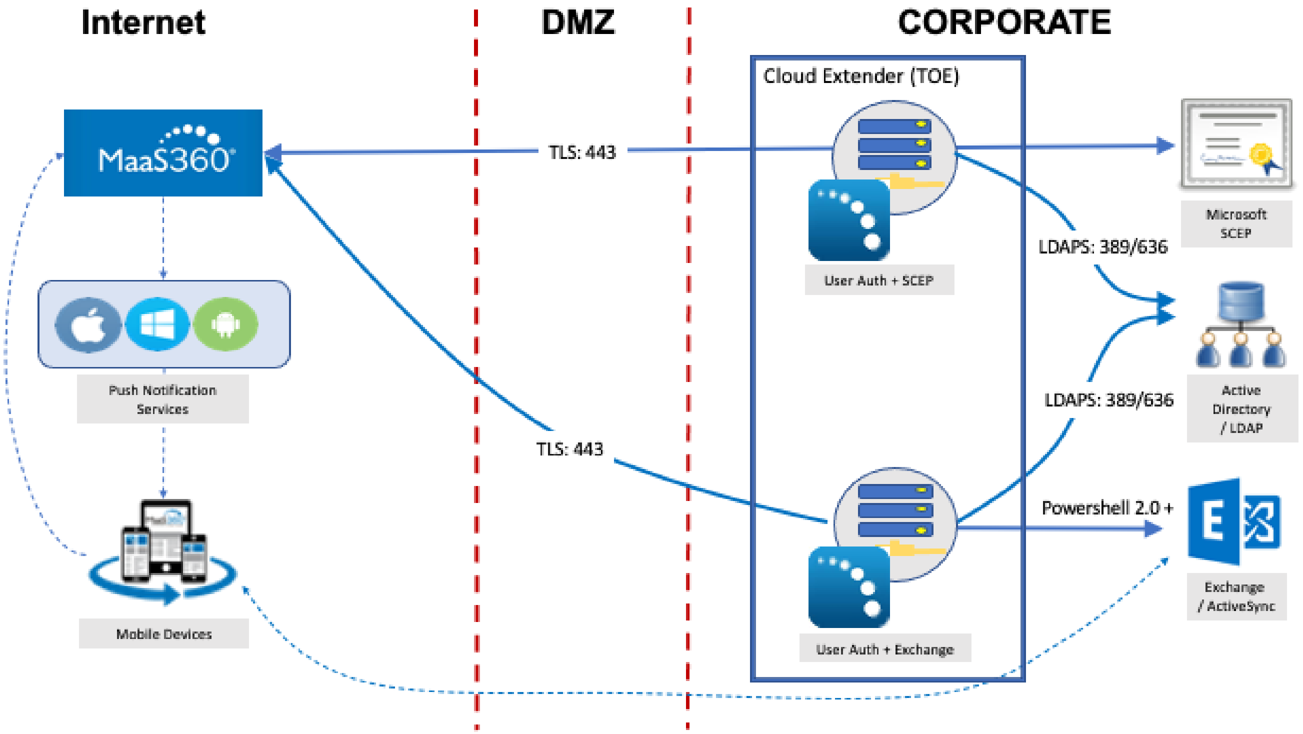

Figure 1: Trusted Communication Channels for a Cloud Extender

The TOE makes an outbound connection to the MaaS360 Software as a Service (SaaS) application (labeled as MaaS360 in the left-top blue box) over port 443 using the Transport Layer Security (TLS) protocol and uses the Extensible Messaging and Presence Protocol (XMPP) protocol to maintain the connection with the MaaS360 Cloud.

The TOE falls under use case 3 ("Communication") scenario, described in section 1.4 of [ASPPv1.3]☝ as follows:

> *"The application allows for communication interactively or non-interactively with other users or applications over a communications channel. Example communications include instant messages, email, and voice."*

1.5 TOE Description

The TOE is a software application that is installed and runs as a service on a Microsoft® Windows® operating system. In this case, Microsoft Windows Server 2019 Standard version 1809 (x64), which has been evaluated for conformance with the U.S. Government Protection Profile (PP) for General Purpose Operating Systems Version 4.1, and is listed on the NIAP Product Compliant List [NIAP-PCL]☝.

The TOE is used in support of the IBM MaaS360 SaaS for mobile device management. Various modules are supplied by IBM, each of which integrates with service components of the MaaS360 customer's infrastructure. For this evaluation, the following modules are the only modules included:

- Exchange Integration for Active Sync Devices Module.
- Corporate Directory Authentication Module.

- Corporate User Visibility Module.
- Certificate Authority Module.

1.5.1 Architecture

The Cloud Extender is a Windows application and service comprised of:

- The Core Installer, which is a Windows service.
- The four CE modules mentioned above.
- The Cloud Extender Configuration Tool.

The Cloud Extender consists of multiple processes running simultaneously. It uses the following cryptographic libraries:

- The Windows Cryptography API Next Generation (CNG) cryptographic library accessed via the .NET Framework (provided by the operational environment).
- OpenSSL for the IBM MaaS360 Cloud Extender

CNG is used for communication and data-at-rest purposes while Open (Secure Sockets Layer) SSL is used for HTTPS connections. OpenSSL for the IBM MaaS360 Cloud Extender is also used to encrypt configuration templates generated by the IBM MaaS360 Cloud Extender Configuration Tool should TOE administrators wish to similarly configure another Cloud Extender. As this template is stored by default in an encrypted file system (EFS) volume, the TOE platform is thusly providing the overall data-at-rest capability.

The Core Installer communicates with the MaaS360 SaaS. It uses Client for URLs (cURL) and Windows crypto for protecting the communications channel between the MaaS360 SaaS application and the Cloud Extender. The Core installer uses TLS 1.2 and initiates all communication with the MaaS360 SaaS application. Thus, the TOE acts as a TLS client.

The TOE is packaged with several third-party libraries, which are listed in FPT_LIB_EXT.1.

The IBM MaaS360 Cloud Extender Configuration Tool is supplied with the Cloud Extender installation package, which can be used during the initial installation as well as on-demand when configuration changes are necessary.

The evaluated configuration includes four CE modules, which are packages of scripts and actions that integrate with components of the MaaS360 customer’s infrastructure and provides full integration service with that component. Table 1 provides descriptions of each of the CE modules.

CE Module	Description
Exchange Integration for Active Sync Devices Module	The Exchange Integration module interacts with the Exchange Server to automatically discover ActiveSync-connected devices and uploads that device information to the MaaS360® Cloud. The Exchange Integration module automatically quarantines devices, allows only MaaS360 enrolled devices, carries out actions (such as Approve, Block, or Remove device from the Mailbox) sent from MaaS360, and applies ActiveSync device policies. This module supports MS Exchange 2007, 2010, 2013, 2016, Office 365, and Microsoft Business Productivity Online Suite (BPOS)-D.

CE Module	Description
Corporate Directory Authentication Module	The User Authentication module interacts with Active Directory and LDAP directories to provide user authentication service for various MaaS360 functions, such as self-service device enrollment with corporate credentials, MaaS360 Portal login, and user management portal. The Cloud Extender supports integration with Lightweight Directory Access Protocol (LDAP) implementations, including Active Directory, Domino® LDAP, Oracle® LDAP, Novell® eDirectory LDAP, and OpenLDAP.
Corporate User Visibility Module	The User Visibility module synchronizes user and group information from LDAP or Active Directory directories to the MaaS360 SaaS application.
Certificate Authority Module	The Certificate Integration module facilitates the automatic provisioning, distribution, and renewal of digital identity certificates to managed mobile devices by using existing Microsoft Certificate Authority (CA), Symantec® CA, or Entrust® Admin Services and Identity Guard. The Cloud Extender interacts with the CA and then pushes the issued certificates down to enrolled devices by using the following method: • It receives certificate requests from the MaaS360 Portal for all enrolled devices that require an identity certificate. • It authenticates against the CA or Registration Authority (RA) as a part of the certificate request process. • It requests ID certificates by passing the details of the device or user and corresponding attributes as a part of the certificate request. • It encrypts the received certificate by using the public key of the requesting device and pushes the encrypted payload to the MaaS360 Portal, which is then delivered to the device. • It supports auto-renewals of certificates and makes sure that devices receive the new certificates before the current certificate expires.

Table 1: Description of the Cloud Extender Modules

1.5.2 TOE boundaries

1.5.2.1 Physical boundary of the TOE

The Physical Boundary of the TOE consists of the application installer executable and guidance documents. Each of these assets is distributed digitally via the IBM MaaS360 portal.

1.5.2.1.1 Hardware / Firmware Components

The hardware platform used during the evaluation was a Dell PowerEdge R740 with an Intel Xeon Gold 5118 processor (SkyLake microarchitecture).

1.5.2.1.2 TOE Guidance

The following documentation comprises the TOE guidance and is available on the IBM MaaS360 Mobile Device Management website.

- MasS360 Cloud Extender Admin Guide [ADM_GUIDE]
- MaaS360 Cloud Extender Common Criteria Guide [CC-CFG]

1.5.2.2 Logical

The figure below describes the logical boundary of the TOE, which includes the TOE Security Functions (TSF) as specified in [ASPPv1.3].

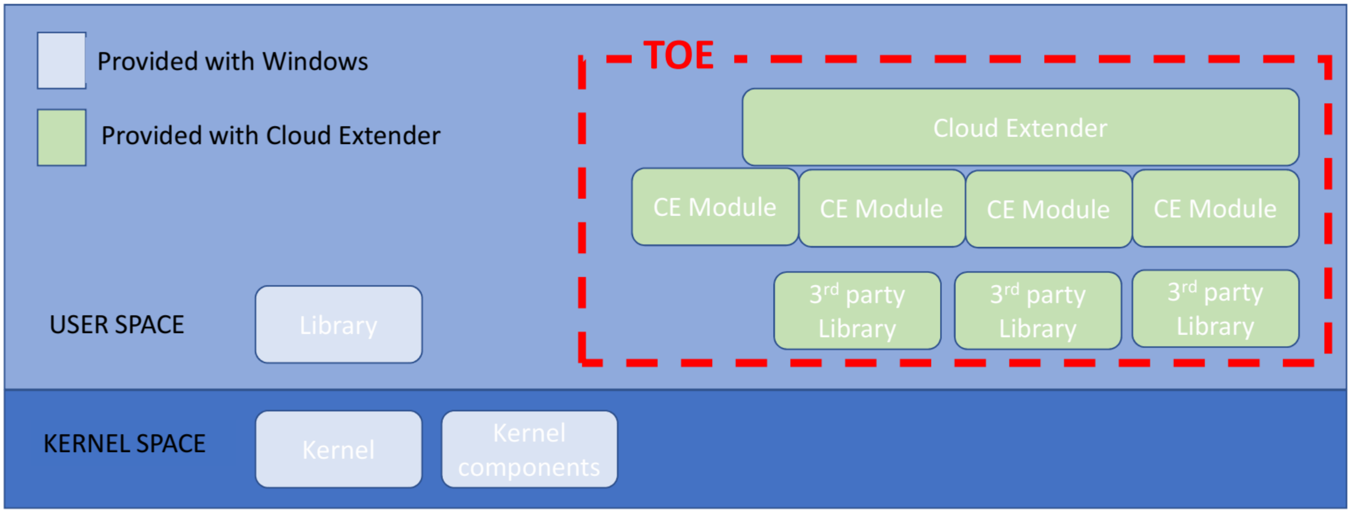

Figure 2: The Logical Boundary of the Cloud Extender TOE

1.5.2.3 Security Functions provided by the TOE

The TOE provides the security functionality required by [ASPPv1.3] and [TLSPKGv1.1], which is described briefly in the following sections.

1.5.2.3.1 Cryptographic Support (FCS)

The Cloud Extender provides cryptographic support using the Windows platform provided cryptographic services via the Cryptography API: Next Generation (CNG) for the following.

1. TLS connections: CNG is used by Secure Channel (SChannel), enabling the Cloud Extender to communicate with the Exchange Server, Domain Controller, and PKI Certificate Servers using HTTPS, limiting the protocol to TLS 1.2, and only using a subset of the TLS 1.2 ciphers.
2. Protecting data-at-rest using the Encrypted File System (EFS) to the C:\ProgramData\MaaS360\ directory that contains all configuration and log information.
3. Encrypting registry entries using the Data Protection Application Programming Interface (DAPI).
4. Generating an Exchange Server certificate during the installation process.

The inclusion of the OpenSSL libraries with the TOE provides cryptographic functionality for the following functions.

1. TLS connections to the MaaS360 Portal and SCEP certificate servers only (HTTPS using cURL).

2. Encryption of configuration profiles, but as these are stored within an EFS directory above it is not the enforcing SFR.
3. Device and User Certificate generation for certificate signing requests to a SCEP server using the Device and User templates. These requests are completed by the SCEP server and certificates returned to the IBM MaaS360 Cloud Extender, as detailed in Table 2.

Type	Explanation
Mobile Device	The Cloud Extender generates a certificate based on requirements and pushes that certificate to the mobile device. The Cloud Extender uses certificate templates to pass user attributes as part of the Subject Name/Alternate Name, which links the certificate to the user and is used as a device certificate. Devices treat all certificates as user certificates. Most commonly used certificate template type that supports Microsoft, Symantec, Entrust, and Verizon MCS. Mostly used for authentication.
User	Support for Microsoft certificates stored in AD, Entrust, and IDnomic – Mobile Guard (OpenTrust) Mostly used for S/MIME certificates to deliver signing and encryption certificates. For user certificates that are used for authentication, choose the device certificate template, and provide user attributes to pass to the CA for certificate generation.

Table 2: Device and User Certificate Related Functionality

The entropy used to seed the SP800-90A DRBG provided by the TOE is obtained from the underlying platform.

The SP800-90A DRBG implemented in the TOE by the OpenSSL for the IBM MaaS360 Cloud Extender obtains a 384-bit seed from the underlying platform by calling the BCryptGenRandom() API function. Similarly, the cryptographic functionality provided by the underlying platform obtains entropy from the same source.

The TOE obtains an entropy equal to or greater than 256 bits. The Entropy Assessment Report [CE-EAR] provides a more detail description of the entropy source.

1.5.2.3.2 User Data Protection (FDP)

The application provides user data protection services through restricting access by the application to only those platform-based resources (sensitive data repositories, and network communications) that are needed in order to provide the needed application functionality.

Sensitive application data is encrypted using platform-provided encrypted file system (EFS) services, when stored in non-volatile memory, such as the hard disk drive(s).

1.5.2.3.3 Identification and Authentication (FIA)

The TOE supports authentication by X.509 certificates by the application and using the platform API. Certificate validation, supported properties, and usage are described in section 7.1.3.

1.5.2.3.4 Security Management (FMT)

The Cloud Extender application provides the ability to set various configuration options for the TOE. These options are stored, as recommended by Microsoft, in the Windows Registry and are protected using the Data Protection application programming interface (DPAPI).

During installation, the files installed on the platform are allocated appropriate file-permissions, supporting the protection of the application, and its data from unauthorized access.

1.5.2.3.5 Privacy (FPR)

The Cloud Extender application does not specifically request Personally Identifiable Information (PII).

1.5.2.3.6 Protection of the TSF (FPT)

The Cloud Extender application uses only documented Windows APIs. It is packaged with third-party libraries which provide supporting functionality. These are listed in section 6.1.6.5.

The Cloud Extender application does not write user-modifiable files to directories that contain executable files.

The Cloud Extender application is compiled using stack buffer overrun protection and uses Address Space Layout Randomization (ASLR) techniques, it does not generally request to map memory at explicit addresses. Exceptions are listed in section 7.1.6.

The Cloud Extender application is packaged and delivered in the Windows Application Software (.EXE) format signed using the Microsoft Authenticode process using the Microsoft Sign Tool.exe (v6.3). It is compiled by IBM with stack-based buffer overflow protection enabled.

1.5.2.3.7 Trusted Path/Channels (FTP)

The Cloud Extender application protects all transmitted data by using TLS 1.2 protected trusted channels. Protocols used within these trusted channels may include additional protection and include HTTPS, and LDAPS.

1.5.2.4 Excluded TOE Features

The following modules are not delivered with the TOE and therefore the services they provide are not part of the evaluated configuration.

- IBM Traveler module
- Exchange Integration for Real-time Mail Notifications module
- BlackBerry Enterprise Server (BES) module
- Mobile Enterprise Gateway (MEG) module
- MaaS360 VPN module
- Zebra Printer Management module

1.5.2.5 Operational Environment

The TOE requires the following in its operational environment.

- A configured and operational instance of the MaaS360 SaaS application.
- One or more enrolled mobile devices.
- A network connection to the MaaS360 SaaS application and the customer's internal network.
- A Microsoft Windows Server 2019 Standard version 1809 (x64) platform on which it runs.
- A MS Exchange Server.
- An Active Directory Server.
- A Network Device Enrollment Server Certificate Authority (NDES CA) server and/or An Entrust Certificate server.

The TOE was tested in the environment described in Figure 3.

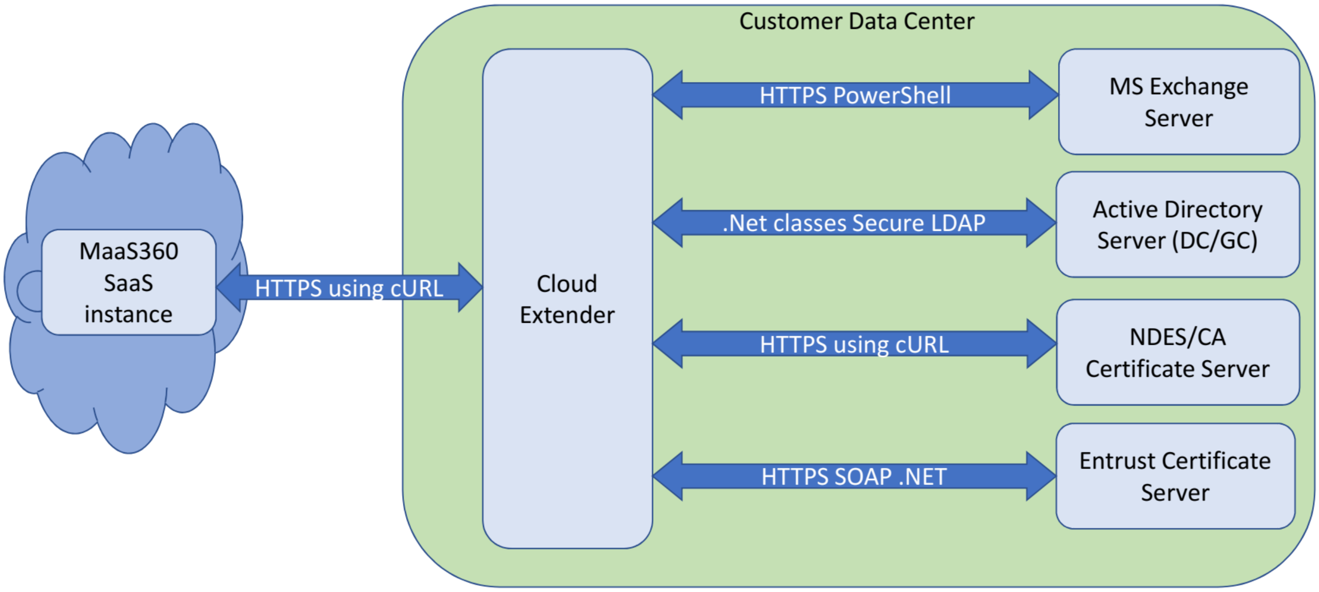

Figure 3: Operational Environment for the Cloud Extender TOE

2 CC Conformance Claim

This Security Target is CC Part 2 extended and CC Part 3 extended.

This Security Target claims conformance to the following Protection Profile:

- [ASPPv1.3]: Protection Profile for Application Software. Version 1.3 as of 2019-03-01; exact conformance.
- [TLSPKGv1.1]: Functional Package for TLS. Version 1.1 as of 2019-03-01; exact conformance.

Common Criteria [CC] version 3.1 revision 5 is the basis for this conformance claim.

Table 3 below contains the NIAP Technical Decisions (TDs) for the [ASPPv1.3] at the time of the creation of this Security Target and a statement of applicability to the evaluation.

TD	Description	Applicability	Reference
TD0601	X.509 SFR Applicability in App PP	Replace RFC5759 with RFC8603 (this TD supersedes TD0444, TD0473, TD0521, and TD0587).	[CCEVS-TD0601]
TD0600	Conformance claim sections updated to allow for MOD_VPNC_V2.3	Not applicable to this evaluation as the PP module for VPN client is not part of the conformance claims.	[CCEVS-TD0600]
TD0598	Expanded AES Modes in FCS_COP for App PP	New AES modes do not affect this evaluation.	[CCEVS-TD0598]
TD0582	PP-Configuration for Application Software and Virtual Private Network (VPN) Clients now allowed	Not applicable to this evaluation.	[CCEVS-TD0582]
TD0561	Signature verification update	Changes in FPT_TUD_EXT.1 and FPT_TUD_EXT.2	[CCEVS-TD0561]
TD0554	iOS/iPadOS/Android AppSW Virus Scan	Not applicable to this evaluation as the TOE does not run in these platforms.	[CCEVS-TD0554]
TD0548	Integrity for installation tests in AppSW PP 1.3	Not applicable to this evaluation as the TOE does not run in an iOS platform.	[CCEVS-TD0548]
TD0544	Alternative testing methods for FPT_AEX_EXT.1.1	Not applicable to this evaluation as the TOE runs in only one platform.	[CCEVS-TD0544]
TD0543	FMT_MEC_EXT.1 evaluation activity update	This technical decision affects only the testing assurance activity.	[CCEVS-TD0543]
TD0519	Linux symbolic links and FMT_CFG_EXT.1	Not applicable to this evaluation as the TOE does not run on this platform.	[CCEVS-TD0519]
TD0515	Use Android APK manifest in test	Not applicable to this evaluation as the TOE does not run on this platform.	[CCEVS-TD0515]
TD0510	Obtaining random bytes for iOS/macOS	Not applicable to this evaluation as the TOE does not run on this platform.	[CCEVS-TD0510]
TD0498	Application Software PP Security Objectives and Requirements Rationale	Update of mapping between security objectives and SFRs.	[CCEVS-TD0498]

TD	Description	Applicability	Reference
TD0495	FIA_X509_EXT.1.2 Test Clarification	This technical decision affects only the testing assurance activity.	[CCEVS-TD0495]
TD0465	Configuration Storage for .NET Apps	This technical decision affects only the testing assurance activity.	[CCEVS-TD0465]
TD0445	User Modifiable File Definition	This technical decision affects only the testing assurance activity.	[CCEVS-TD0445]
TD0437	Supported Configuration Mechanism	Updates in FMT_MEC_EXT.1.1.	[CCEVS-TD0437]
TD0435	Alternative to SELinux for FPT_AEX_EXT.1.3	Not applicable to this evaluation as the TOE does not run on this platform.	[CCEVS-TD0435]
TD0434	Windows Desktop Applications Test	This technical decision affects only the testing assurance activity.	[CCEVS-TD0434]
TD0427	Reliable Time Source	Updates in A.PLATFORM.	[CCEVS-TD0427]
TD0416	Correction to FCS_RBG_EXT.1 Test Activity	This technical decision affects only the testing assurance activity.	[CCEVS-TD0416]

Table 3: NIAP Technical Decisions for ASPPv1.3

Table 4 below contains the NIAP Technical Decisions (TDs) for the [TLSPKGv1.1] at the time of the creation of this Security Target and a statement of applicability to the evaluation.

TD	Description	Applicability	Reference
TD0588	Session Resumption Support in TLS package	Not applicable to this evaluation as session resumption is not supported by the TOE.	[CCEVS-TD0588]
TD0513	CA Certificate loading	This technical decision affects only the testing assurance activity.	[CCEVS-TD0513]
TD0499	Testing with pinned certificates	This technical decision affects only the testing assurance activity.	[CCEVS-TD0499]
TD0469	Modification of test activity for FCS_TLSS_EXT.1.1 test 4.1	Not applicable as this SFR is not claimed in the evaluation.	[CCEVS-TD0469]
TD0442	Updated TLS Ciphersuites for TLS Package	The list of cipher suites is updated for FCS_TLSC_EXT.1.	[CCEVS-TD0442]

Table 4: NIAP Technical Decisions for Functional Package v1.1 for TLS

3 Security Problem Definition

The following sections describe security problem definition as stated in [ASPPv1.3]☝.

3.1 Threat Environment

3.1.1 Threats countered by the TOE

T.NETWORK_ATTACK

An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may engage in communications with the application software or alter communications between the application software and other endpoints in order to compromise it.

T.NETWORK_EAVESDROP

An attacker is positioned on a communications channel or elsewhere on the network infrastructure. Attackers may monitor and gain access to data exchanged between the application and other endpoints.

T.LOCAL_ATTACK

An attacker can act through unprivileged software on the same computing platform on which the application executes. Attackers may provide maliciously formatted input to the application in the form of files or other local communications.

T.PHYSICAL_ACCESS

An attacker may try to access sensitive data at rest.

3.1.2 Threats countered by the Operational Environment

3.2 Assumptions

3.2.1 Intended usage of the TOE

A.PLATFORM

The TOE relies upon a trustworthy computing platform with a reliable time clock for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.

A.PROPER_USER

The user of the application software is not willfully negligent or hostile, and uses the software in compliance with the applied enterprise security policy.

A.PROPER_ADMIN

The administrator of the application software is not careless, willfully negligent or hostile, and administers the software in compliance with the applied enterprise security policy.

3.3 Organizational Security Policies

There are no Organizational Security Policies for the TOE.

4 Security Objectives

4.1 Objectives for the TOE

O.INTEGRITY

Conformant TOEs ensure the integrity of their installation and update packages, and also leverage execution environment-based mitigations. Software is seldom, if ever, shipped without errors. The ability to deploy patches and updates to fielded software with integrity is critical to enterprise network security. Processor manufacturers, compiler developers, execution environment vendors, and operating system vendors have developed execution environment-based mitigations that increase the cost to attackers by adding complexity to the task of compromising systems. Application software can often take advantage of these mechanisms by using APIs provided by the runtime environment or by enabling the mechanism through compiler or linker options.

O.QUALITY

To ensure quality of implementation, conformant TOEs leverage services and APIs provided by the runtime environment rather than implementing their own versions of these services and APIs. This is especially important for cryptographic services and other complex operations such as file and media parsing. Leveraging this platform behavior relies upon using only documented and supported APIs.

O.MANAGEMENT

To facilitate management by users and the enterprise, conformant TOEs provide consistent and supported interfaces for their security-relevant configuration and maintenance. This includes the deployment of applications and application updates through the use of platform-supported deployment mechanisms and formats, as well as providing mechanisms for configuration. This also includes providing control to the user regarding disclosure of any PII.

O.PROTECTED_STORAGE

To address the issue of loss of confidentiality of user data in the event of loss of physical control of the storage medium, conformant TOEs will use data-at-rest protection. This involves encrypting data and keys stored by the TOE in order to prevent unauthorized access to this data. This also includes unnecessary network communications whose consequence may be the loss of data.

O.PROTECTED_COMMS

To address both passive (eavesdropping) and active (packet modification) network attack threats, conformant TOEs will use a trusted channel for sensitive data. Sensitive data includes cryptographic keys, passwords, and any other data specific to the application that should not be exposed outside of the application.

4.2 Objectives for the Operational Environment

OE.PLATFORM

The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying operating system and any discrete execution environment provided to the TOE.

OE.PROPER_USER

The user of the application software is not willfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy.

OE.PROPER_ADMIN

The administrator of the application software is not careless, willfully negligent or hostile, and administers the software within compliance of the applied enterprise security policy.

4.3 Security Objectives Rationale

4.3.1 Coverage

The following table provides a mapping of TOE objectives to threats and policies, showing that each objective counters or enforces at least one threat or policy, respectively.

Objective	Threats / OSPs
O.INTEGRITY	T.NETWORK_ATTACK
O.QUALITY	T.NETWORK_EAVESDROP T.LOCAL_ATTACK
O.MANAGEMENT	T.NETWORK_ATTACK T.NETWORK_EAVESDROP
O.PROTECTED_STORAGE	T.PHYSICAL_ACCESS
O.PROTECTED_COMMS	T.NETWORK_ATTACK T.NETWORK_EAVESDROP

Table 5: Mapping of security objectives to threats and policies

The following table provides a mapping of the objectives for the Operational Environment to assumptions, threats and policies, showing that each objective holds, counters or enforces at least one assumption, threat or policy, respectively.

Objective	Assumptions / Threats / OSPs
OE.PLATFORM	A.PLATFORM
OE.PROPER_USER	A.PROPER_USER
OE.PROPER_ADMIN	A.PROPER_ADMIN

Table 6: Mapping of security objectives for the Operational Environment to assumptions, threats and policies

4.3.2 Sufficiency

The following rationale provides justification that the security objectives are suitable to counter each individual threat and that each security objective tracing back to a threat, when achieved, actually contributes to the removal, diminishing or mitigation of that threat.

Threat	Rationale for security objectives
T.NETWORK_ATTACK	The threat T.NETWORK_ATTACK is countered by O.PROTECTED_COMMS as this provides for integrity of transmitted data. The threat T.NETWORK_ATTACK is countered by O.INTEGRITY as this provides for integrity of software that is installed onto the system from the network. The threat T.NETWORK_ATTACK is countered by O.MANAGEMENT as this provides for the ability to configure the application to defend against network attack.
T.NETWORK_EAVESDROP	The threat T.NETWORK_EAVESDROP is countered by O.PROTECTED_COMMS as this provides for confidentiality of transmitted data. The objective O.QUALITY ensures use of mechanisms that provide protection against network-based attack. The threat T.NETWORK_EAVESDROP is countered by O.MANAGEMENT as this provides for the ability to configure the application to protect the confidentiality of its transmitted data.
T.LOCAL_ATTACK	The objective O.QUALITY protects against the use of mechanisms that weaken the TOE with regard to attack by other software on the platform.
T.PHYSICAL_ACCESS	The objective O.PROTECTED_STORAGE protects against unauthorized attempts to access physical storage used by the TOE.

Table 7: Sufficiency of objectives countering threats

The following rationale provides justification that the security objectives for the environment are suitable to cover each individual assumption, that each security objective for the environment that traces back to an assumption about the environment of use of the TOE, when achieved, actually contributes to the environment achieving consistency with the assumption, and that if all security objectives for the environment that trace back to an assumption are achieved, the intended usage is supported.

Assumption	Rationale for security objectives
A.PLATFORM	The operational environment objective OE.PLATFORM is realized through A.PLATFORM.
A.PROPER_USER	The operational environment objective OE.PROPER_USER is realized through A.PROPER_USER.
A.PROPER_ADMIN	The operational environment objective OE.PROPER_ADMIN is realized through A.PROPER_ADMIN.

Table 8: Sufficiency of objectives holding assumptions

5 Extended Components Definition

This Security Target uses the extended components defined in [ASPPv1.3]☝ .

6 Security Requirements

6.1 TOE Security Functional Requirements

The table below summarizes the SFRs for the TOE and the operations performed on the components according to CC part 1. Operations in the SFRs use the following convention:

- Iterations (Iter.) are identified by appending a suffix to the original SFR.
- Refinements (Ref.) added to the text are shown in *italic text*, deletions are shown as ~~strikethrough text~~.
- Assignments (Ass.) are shown in **bold text**.
- Selections (Sel.) are shown in **bold text**.

Security functional class	Security functional requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
FCS - Cryptographic support	FCS_CKM_EXT.1 Cryptographic Key Generation Services	ASPPv1.3	No	No	No	Yes
	FCS_CKM.1(1) Cryptographic Asymmetric Key Generation	ASPPv1.3	No	No	No	Yes
	FCS_CKM.2 Cryptographic Key Establishment	ASPPv1.3	No	No	No	Yes
	FCS_COP.1(1) Cryptographic Operation - Encryption/Decryption	ASPPv1.3	No	No	No	Yes
	FCS_COP.1(2) Cryptographic Operation - Hashing	ASPPv1.3	No	No	No	Yes
	FCS_COP.1(3) Cryptographic Operation - Signing	ASPPv1.3	No	No	No	Yes
	FCS_COP.1(4) Cryptographic Operation - Keyed-Hash Message Authentication	ASPPv1.3	No	No	Yes	Yes
	FCS_RBG_EXT.1 Random Bit Generation Services	ASPPv1.3	No	No	No	Yes
	FCS_RBG_EXT.2 Random Bit Generation from Application	ASPPv1.3	No	No	No	Yes
	FCS_STO_EXT.1 Storage of Credentials	ASPPv1.3	No	No	Yes	Yes
	FCS_HTTPS_EXT.1 / Client HTTPS Protocol	ASPPv1.3	No	No	No	Yes
FDP - User data protection	FDP_DEC_EXT.1 Access to Platform Resources	ASPPv1.3	No	No	Yes	Yes
	FDP_NET_EXT.1 Network Communications	ASPPv1.3	No	No	Yes	Yes
	FDP_DAR_EXT.1 Encryption Of Sensitive Application Data	ASPPv1.3	No	No	No	Yes
FIA - Identification and authentication	FIA_X509_EXT.1 X.509 Certificate Validation	ASPPv1.3	No	No	No	Yes
	FIA_X509_EXT.2 X.509 Certificate Authentication	ASPPv1.3	No	No	No	Yes

Security functional class	Security functional requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
FMT - Security management	FMT_MEC_EXT.1 Supported Configuration Mechanism	ASPPv1.3	No	No	No	Yes
	FMT_CFG_EXT.1 Secure by Default Configuration	ASPPv1.3	No	No	No	No
	FMT_SMF.1 Specification of Management Functions	ASPPv1.3	No	No	Yes	Yes
FPR - Privacy	FPR_ANO_EXT.1 User Consent for Transmission of Personally Identifiable Information	ASPPv1.3	No	No	No	Yes
FPT - Protection of the TSF	FPT_API_EXT.1 Use of Supported Services and APIs	ASPPv1.3	No	No	No	No
	FPT_AEX_EXT.1 Anti-Exploitation Capabilities	ASPPv1.3	No	No	Yes	Yes
	FPT_TUD_EXT.1 Integrity for Installation and Update	ASPPv1.3	No	No	No	Yes
	FPT_TUD_EXT.2 Integrity for Installation and Update	ASPPv1.3	No	No	No	No
	FPT_LIB_EXT.1 Use of Third Party Libraries	ASPPv1.3	No	No	Yes	No
	FPT_IDV_EXT.1 Software Identification and Versions	ASPPv1.3	No	No	Yes	Yes
FTP - Trusted path/channels	FTP_DIT_EXT.1 Protection of Data in Transit	ASPPv1.3	No	No	No	Yes
FCS - Cryptographic support	FCS_TLS_EXT.1 TLS Protocol	TLSPKGv1.1	No	No	No	Yes
	FCS_TLSC_EXT.1 TLS Client Protocol	TLSPKGv1.1	No	No	No	Yes
	FCS_TLSC_EXT.5 TLS Client Support for Supported Groups Extension	TLSPKGv1.1	No	No	No	Yes

Table 9: SFRs for the TOE

6.1.1 Cryptographic support (FCS)

6.1.1.1 Cryptographic Key Generation Services (FCS_CKM_EXT.1)

FCS_CKM_EXT.1.1 The application shall **invoke platform-provided functionality for asymmetric key generation, implement asymmetric key generation**.

6.1.1.2 Cryptographic Asymmetric Key Generation (FCS_CKM.1(1))

FCS_CKM.1.1(1) The application shall **invoke platform-provided functionality, implement functionality** to generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm

- **RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following FIPS PUB 186-4, "Digital Signature Standard (DSS), Appendix B.3"**

- **ECC schemes using "NIST curves" P-256, P-384 and no other curves that meet the following: FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4**

.

Application Note: *RSA key generation is implemented in the application to generate certificate signing requests (CSR). ECDSA key generation is both implemented in the application and the underlying platform for ephemeral keys created for TLS protocol establishment.*

6.1.1.3 Cryptographic Key Establishment (FCS_CKM.2)

FCS_CKM.2.1 The application shall **invoke platform-provided functionality, implement functionality** to perform cryptographic key establishment in accordance with a specified cryptographic key establishment method:

- **Elliptic curve-based key establishment schemes that meets the following: NIST Special Publication 800-56A, "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"**

.

Application Note: *Key establishment is implemented in the application and the underlying platform for TLS protocol establishment.*

6.1.1.4 Cryptographic Operation - Encryption/Decryption (FCS_COP.1(1))

FCS_COP.1.1(1) The application shall perform encryption/decryption in accordance with a specified cryptographic algorithm

- **AES-CBC (as defined in NIST SP 800-38A) mode**
- **AES-GCM (as defined in NIST SP 800-38D) mode**

and cryptographic key sizes **128-bit, 256-bit** .

Application Note:

AES-CBC with 256-bit keys is required for the CTR_DRBG method used by the SP800-90A DRBG implemented in the OpenSSL for the IBM MaaS360 Cloud Extender cryptographic module, which is part of the TOE. AES-GCM with 128-bit keys is required for the TLS cipher suites supported by the TOE and implemented in both the TOE and the underlying platform.

6.1.1.5 Cryptographic Operation - Hashing (FCS_COP.1(2))

FCS_COP.1.1(2) The application shall perform cryptographic hashing services in accordance with a specified cryptographic algorithm

- **SHA-256**
- **SHA-384**
- **no other**

and message digest sizes

- **256**
- **384**
- **no other**

bits that meet the following: FIPS Pub 180-4.

Application Note:

Message digest algorithms are implemented in both the TOE and the underlying platform to support TLS communications.

6.1.1.6 Cryptographic Operation - Signing (FCS_COP.1(3))

FCS_COP.1.1(3) The application shall perform cryptographic signature services (generation and verification) in accordance with a specified cryptographic algorithm

- **RSA schemes using cryptographic key sizes of 2048-bit or greater that meet the following: FIPS PUB 186-4, “Digital Signature Standard (DSS)”, Section 4**

.

Application Note:

Signature generation and verification algorithms are implemented in both the TOE and the underlying platform to support TLS communications and certificate validation.

6.1.1.7 Cryptographic Operation - Keyed-Hash Message Authentication (FCS_COP.1(4))

FCS_COP.1.1(4) The application shall perform keyed-hash message authentication in accordance with a specified cryptographic algorithm

a) HMAC-SHA-256

and

- **no other algorithms**

with key sizes **256 bits** and message digest sizes 256 and **no other size** bits that meet the following: FIPS Pub 198-1 The Keyed-Hash Message Authentication Code and FIPS Pub 180-4 Secure Hash Standard.

Application Note:

Message authentication algorithms are implemented in both the TOE and the underlying platform to support TLS communications.

6.1.1.8 Random Bit Generation Services (FCS_RBG_EXT.1)

FCS_RBG_EXT.1.1 The application shall

- **implement DRBG functionality**

for its cryptographic operations.

Application Note:

DRBG is implemented in the TOE to support key generation and support TLS communications.

6.1.1.9 Random Bit Generation from Application (FCS_RBG_EXT.2)

FCS_RBG_EXT.2.1 The application shall perform all deterministic random bit generation (DRBG) services in accordance with NIST Special Publication 800-90A using **CTR_DRBG (AES)**

FCS_RBG_EXT.2.2 The deterministic RBG shall be seeded by an entropy source that accumulates entropy from a platform-based DRBG and

- **no other noise source**

with a minimum of

- **256 bits**

of entropy at least equal to the greatest security strength (according to NIST SP 800-57) of the keys and hashes that it will generate.

6.1.1.10 Storage of Credentials (FCS_STO_EXT.1)

FCS_STO_EXT.1.1 The application shall **invoke the functionality provided by the platform to securely store**

- **certificates for MaaS360 SaaS application;**
- **customer's instantiation credentials for Microsoft SCEP;**
- **customer's instantiation credentials for Active Directory and/or LDAP server;**
- **customer's instantiation credentials for Microsoft Exchange and/or Active Sync**

to non-volatile memory.

Application Note:

Certificates for MaaS360 SaaS application are stored in the Windows Certificate Store. The credentials (username, password) instantiated by the customer to authenticate against the Microsoft SCEP, the Active Directory and/or LDAP server, and Microsoft Exchange and/or Active Sync are stored in the Windows Registry in encrypted form.

6.1.1.11 HTTPS Protocol (FCS_HTTPS_EXT.1 / Client)

FCS_HTTPS_EXT.1.1 / Client The application shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2 / Client The application shall implement HTTPS using TLS as defined in the TLS package.

FCS_HTTPS_EXT.1.3 / Client The application shall **notify the user and not establish the user-initiated connection** if the peer certificate is deemed invalid.

6.1.1.12 TLS Protocol (FCS_TLS_EXT.1)

FCS_TLS_EXT.1.1 The product shall implement **TLS as a client**.

6.1.1.13 TLS Client Protocol (FCS_TLSC_EXT.1)

FCS_TLSC_EXT.1.1 The product shall implement TLS 1.2 (RFC 5246) and **no earlier TLS versions** as a client that supports the cipher suites

- **TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289**

and also supports functionality for

- **none**

.

FCS_TLSC_EXT.1.2 The product shall verify that the presented identifier matches the reference identifier according to RFC 6125.

FCS_TLSC_EXT.1.3 The product shall not establish a trusted channel if the server certificate is invalid

- **with no exceptions**

.

6.1.1.14 TLS Client Support for Supported Groups Extension (FCS_TLSC_EXT.5)

FCS_TLSC_EXT.5.1 The product shall present the Supported Groups Extension in the Client Hello with the supported groups **secp256r1, secp384r1**.

6.1.2 User data protection (FDP)

6.1.2.1 Access to Platform Resources (FDP_DEC_EXT.1)

FDP_DEC_EXT.1.1 The application shall restrict its access to **network connectivity**.

FDP_DEC_EXT.1.2 The application shall restrict its access to

- **no sensitive information repositories**
- **address book**
- **calendar**
- **call lists**
- **system logs**
- **the Windows Credential Store**
- **system logs and Windows Event logs-application with the following folders and sub-folders:**
    - **C:\Program Files (x86)\MaaS360\Cloud Extender**
    - **C:\ProgramData\MaaS360\Cloud Extender**
    - **C:\Program Files (x86)\Common Files\MaaS360\Visibility_2.106.500.016.002**

.

6.1.2.2 Network Communications (FDP_NET_EXT.1)

FDP_NET_EXT.1.1 The application shall restrict network communication to

- **MaaS360 SaaS application,**
- **customer’s instantiation of Microsoft NDES CA,**
- **customer’s instantiation of Entrust CA,**
- **customer’s instantiation of Active Directory and/or LDAP server,**
- **customer’s instantiation of Microsoft Exchange and/or Active Sync**

.

6.1.2.3 Encryption Of Sensitive Application Data (FDP_DAR_EXT.1)

FDP_DAR_EXT.1.1 The application shall **leverage platform-provided functionality to encrypt sensitive data** in non-volatile memory.

6.1.3 Identification and authentication (FIA)

6.1.3.1 X.509 Certificate Validation (FIA_X509_EXT.1)

FIA_X509_EXT.1.1 The application shall **invoke platform-provided functionality, implement functionality** to validate certificates in accordance with the following rules:

a) RFC 5280 certificate validation and certificate path validation.

b) The certificate path must terminate with a trusted CA certificate.

c) The application shall validate a certificate path by ensuring the presence of the basicConstraints extension, that the CA flag is set to TRUE for all CA certificates, and that any path constraints are met.

d) The application shall validate that any CA certificate includes caSigning purpose in the key usage field.

e) The application shall validate the revocation status of the certificate using **CRL as specified in RFC 8603** .

f) The application shall validate the extendedKeyUsage field according to the following rules:

1. Certificates used for trusted updates and executable code integrity verification shall have the Code Signing Purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
2. Server certificates presented for TLS shall have the Server Authentication purpose (id-kp 1 with OID 1.3.6.1.5.5.7.3.1) in the EKU field.
3. Client certificates presented for TLS shall have the Client Authentication purpose (id-kp 2 with OID 1.3.6.1.5.5.7.3.2) in the EKU field.
4. S/MIME certificates presented for email encryption and signature shall have the Email Protection purpose (id-kp 4 with OID 1.3.6.1.5.5.7.3.4) in the EKU field.
5. OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-dp 9 with OID 1.3.6.1.5.5.7.3.9) in the EKU field.
6. Server certificates presented for EST shall have the CMC Registration Authority (RA) purpose (id-kp-cmcRA with OID 1.3.6.1.5.5.7.3.28) in the EKU field.

Application Note:

Notice that item 5 above is not applicable, as OCSP is not claimed by this SFR.

FIA_X509_EXT.1.2 The application shall treat a certificate as a CA certificate only if the basicConstraints extension is present and the CA flag is set to TRUE.

6.1.3.2 X.509 Certificate Authentication (FIA_X509_EXT.2)

FIA_X509_EXT.2.1 The application shall use X.509v3 certificates as defined by RFC 5280 to support authentication for **HTTPS, TLS**.

FIA_X509_EXT.2.2 When the application cannot establish a connection to determine the validity of a certificate, the application shall **not accept the certificate**.

6.1.4 Security management (FMT)

6.1.4.1 Supported Configuration Mechanism (FMT_MEC_EXT.1)

FMT_MEC_EXT.1.1 The application shall **invoke the mechanisms recommended by the platform vendor for storing and setting configuration options**.

6.1.4.2 Secure by Default Configuration (FMT_CFG_EXT.1)

FMT_CFG_EXT.1.1 The application shall provide only enough functionality to set new credentials when configured with default credentials or no credentials.

FMT_CFG_EXT.1.2 The application shall be configured by default with file permissions which protect the application binaries and data files from modification by normal unprivileged users.

6.1.4.3 Specification of Management Functions (FMT_SMF.1)

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

- **configure cryptographic functionality**

.

6.1.5 Privacy (FPR)

6.1.5.1 User Consent for Transmission of Personally Identifiable Information (FPR_ANO_EXT.1)

FPR_ANO_EXT.1.1 The application shall **not transmit PII over a network** .

6.1.6 Protection of the TSF (FPT)

6.1.6.1 Use of Supported Services and APIs (FPT_API_EXT.1)

FPT_API_EXT.1.1 The application shall use only documented platform APIs.

6.1.6.2 Anti-Exploitation Capabilities (FPT_AEX_EXT.1)

FPT_AEX_EXT.1.1 The application shall not request to map memory at an explicit address except for **OpenSSL for the IBM MaaS360 Cloud Extender and FIPS Object Modules**.

FPT_AEX_EXT.1.2 The application shall

- **not allocate any memory region with both write and execute permissions**

.

FPT_AEX_EXT.1.3 The application shall be compatible with security features provided by the platform vendor.

FPT_AEX_EXT.1.4 The application shall not write user-modifiable files to directories that contain executable files unless explicitly directed by the user to do so.

FPT_AEX_EXT.1.5 The application shall be built with stack-based buffer overflow protection enabled.

6.1.6.3 Integrity for Installation and Update (FPT_TUD_EXT.1)

FPT_TUD_EXT.1.1 The application shall **provide the ability** to check for updates and patches to the application software.

FPT_TUD_EXT.1.2 The application shall **leverage the platform** to query the current version of the application software.

FPT_TUD_EXT.1.3 The application shall not download, modify, replace or update its own binary code.

FPT_TUD_EXT.1.4 Application updates shall be digitally signed such that the application platform can cryptographically verify them prior to installation.

FPT_TUD_EXT.1.5 The application is distributed **as an additional software package to the platform OS**.

6.1.6.4 Integrity for Installation and Update (FPT_TUD_EXT.2)

FPT_TUD_EXT.2.1 The application shall be distributed using the format of the platform-supported package manager.

FPT_TUD_EXT.2.2 The application shall be packaged such that its removal results in the deletion of all traces of the application, with the exception of configuration settings, output files, and audit/log events.

FPT_TUD_EXT.2.3 The application installation package shall be digitally signed such that its platform can cryptographically verify them prior to installation.

6.1.6.5 Use of Third Party Libraries (FPT_LIB_EXT.1)

FPT_LIB_EXT.1.1 The application shall be packaged with only **the third-party libraries provided in Table 10**.

Library	Version
SQLLite	3.35.5
OpenSSL	1.0.2za
OpenSSL FIPS Module	2.0.16
libcURL	7.83.0
Zlib vc	1.1.4
Protobuf	2.6.1
Boost	1.5.9
BitWise Operation Library	5.2.0
Lua	5.1

Library	Version
Lua cURL	1.6
luasql	2.1
DotNetZip	1.9.1.8
NSIS	2.46
CMarkUp	11.2
Gloox Library	1.0.1
InstallShield	2015 + SP1 professional

Table 10: Third-party Libraries

6.1.6.6 Software Identification and Versions (FPT_IDV_EXT.1)

FPT_IDV_EXT.1.1 The application shall be versioned with **"Product Name" and "Product Version" file properties** .

6.1.7 Trusted path/channels (FTP)

6.1.7.1 Protection of Data in Transit (FTP_DIT_EXT.1)

FTP_DIT_EXT.1.1 The application shall

- **encrypt all transmitted sensitive data with**
  - **HTTPS in accordance with FCS_HTTPS_EXT.1 / Client**
  - **TLS as defined in the TLS Package**
- **invoke platform-provided functionality to encrypt all transmitted sensitive data with HTTPS, TLS**

between itself and another trusted IT product.

6.2 Security Functional Requirements Rationale

6.2.1 Coverage

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

Security functional requirements	Objectives
FCS_CKM_EXT.1	O.QUALITY
FCS_CKM.1(1)	O.PROTECTED_COMMS, O.QUALITY

Security functional requirements	Objectives
FCS_CKM.2	O.PROTECTED_COMMS, O.QUALITY
FCS_COP.1(1)	O.PROTECTED_COMMS, O.PROTECTED_STORAGE
FCS_COP.1(2)	O.PROTECTED_COMMS, O.PROTECTED_STORAGE
FCS_COP.1(3)	O.MANAGEMENT, O.PROTECTED_COMMS
FCS_COP.1(4)	O.PROTECTED_COMMS, O.PROTECTED_STORAGE
FCS_RBG_EXT.1	O.PROTECTED_COMMS, O.PROTECTED_STORAGE, O.QUALITY
FCS_RBG_EXT.2	O.PROTECTED_COMMS, O.PROTECTED_STORAGE
FCS_STO_EXT.1	O.PROTECTED_STORAGE, O.QUALITY
FCS_HTTPS_EXT.1 / Client	O.PROTECTED_COMMS
FDP_DEC_EXT.1	O.INTEGRITY
FDP_NET_EXT.1	O.PROTECTED_COMMS
FDP_DAR_EXT.1	O.PROTECTED_STORAGE, O.QUALITY
FIA_X509_EXT.1	O.PROTECTED_COMMS, O.QUALITY
FIA_X509_EXT.2	O.PROTECTED_COMMS
FMT_MEC_EXT.1	O.QUALITY
FMT_CFG_EXT.1	O.INTEGRITY
FMT_SMF.1	O.MANAGEMENT
FPR_ANO_EXT.1	O.MANAGEMENT
FPT_API_EXT.1	O.QUALITY
FPT_AEX_EXT.1	O.INTEGRITY
FPT_TUD_EXT.1	O.INTEGRITY, O.MANAGEMENT
FPT_TUD_EXT.2	O.QUALITY
FPT_LIB_EXT.1	O.QUALITY

Security functional requirements	Objectives
FPT_IDV_EXT.1	O.MANAGEMENT
FTP_DIT_EXT.1	O.PROTECTED_COMMS, O.QUALITY
FCS_TLS_EXT.1	O.PROTECTED_COMMS
FCS_TLSC_EXT.1	O.PROTECTED_COMMS
FCS_TLSC_EXT.5	O.PROTECTED_COMMS

Table 11: Mapping of security functional requirements to security objectives

6.2.2 Sufficiency

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

Security objectives	Rationale
O.INTEGRITY	FDP_DEC_EXT.1 limits access to platform hardware resources, which limits the methods by which an attacker can attempt to compromise the integrity of the TOE. FMT_CFG_EXT.1 limits unauthorized access to itself by preventing the use of default authentication credentials and by ensuring that the TOE uses appropriately restrictive platform permissions on its binaries and data. FPT_AEX_EXT.1 adds complexity to the task of compromising systems by ensuring that application is compatible with security features provided by the platform vendor and that the application implements platform-provided anti-exploitations such as ASLR and stack overflow protection. FPT_TUD_EXT.1 ensures that the TOE can be patched and that any updates to the TOE have appropriate integrity protection.
O.QUALITY	FCS_CKM_EXT.1 specifies that the TSF may rely on platform-provided key generation services. FCS_RBG_EXT.1 specifies that the TSF may rely on platform-provided random bit generation services. FCS_STO_EXT.1 specifies that the TSF may rely on platform-provided credential storage services. FDP_DAR_EXT.1 specifies that the TSF may rely on platform-provided data-at-rest protection services. FMT_MEC_EXT.1 ensures that the TOE can use platform services to store and set configuration options. FPT_API_EXT.1 requires the TOE to leverage platform functionality by using only documented and supported APIs.

Security objectives	Rationale
	FPT_LIB_EXT.1 ensures that the TOE does not include any unnecessary or unexpected third-party libraries that could present a privacy threat or vulnerability. FTP_DIT_EXT.1 specifies that the TSF may rely on platform-provided services to implement trusted communications. FCS_CKM.1(1) specifies that the TSF may rely on platform-provided asymmetric key generation services. FCS_CKM.2 specifies that the TSF may rely on platform-provided key establishment services. FIA_X509_EXT.1 specifies that the TSF may rely on platform-provided X.509 certificate validation services. FPT_TUD_EXT.2 specifies that the TOE may leverage the platform-supported package manager for application distribution and leverages platform-provided mechanisms to remove all traces of itself when removed from the platform system.
O.MANAGEMENT	FMT_SMF.1 defines the security-relevant management functions that are supported by the TOE. FPR_ANO_EXT.1 defines how the TSF provides control to the user regarding the disclosure of any PII. FPT_IDV_EXT.1 provides a methodology for identifying the TOE versioning. FPT_TUD_EXT.1 defines how updates to the TOE are deployed and verified. FCS_COP.1(3) defines the mechanism used to verify TOE updates if the TOE implements this functionality rather than the underlying platform.
O.PROTECTED_STORAGE	FCS_RBG_EXT.1 defines whether random bit generation services are implemented by the TSF or the platform. Depending on how data at rest is protected, the TOE may rely on the use of a random bit generator to create keys that are subsequently used for data protection. FCS_STO_EXT.1 defines the mechanism that the TSF uses or relies upon to protect stored credential data. FDP_DAR_EXT.1 defines the mechanism that the TSF uses or relies upon to protect sensitive data at rest. FCS_COP.1(1) defines the AES cryptographic algorithm that may be used to encrypt stored credential data based on the claims made in FCS_STO_EXT.1. FCS_COP.1(2) defines integrity mechanisms that may be used by the TOE as part of ensuring that data at rest is protected. FCS_COP.1(4) to defines HMAC mechanisms that may be used by the TOE as part of ensuring that data at rest is protected. FCS_RBG_EXT.2 defines the TOE’s implementation of random bit generation functionality in the event that the TOE provides this function in support of generating keys that are used for data protection.

Security objectives	Rationale
O.PROTECTED_COMMS	FCS_RBG_EXT.1 defines whether the random bit generation services used in establishing trusted communications are implemented by the TSF or by the platform. FCS_CKM_EXT.1 specifies whether the TOE or the platform is responsible for generation of any asymmetric keys that may be used for establishing trusted communications. FTP_DIT_EXT.1 defines the trusted channels used to protect data in transit, the data that is protected, and whether the trusted channels are implemented by the TSF or the platform. FCS_CKM.1(1) defines whether the TSF or the platform generates asymmetric keys that are used in support of trusted communications. FCS_CKM.2 defines whether the TSF or the platform performs key establishment for trusted communications. FCS_COP.1(1) defines the symmetric encryption algorithms used in support of trusted communications. FCS_COP.1(2) defines the hash algorithms used in support of trusted communications. FCS_COP.1(3) defines the digital signature algorithms used in support of trusted communications. FCS_COP.1(4) defines the HMAC algorithms used in support of trusted communications. FCS_RBG_EXT.2 defines the DRBG algorithms used in support of trusted communications. FCS_HTTPS_EXT.1 / Client defines the TOE’s support for the HTTPS trusted communications protocol. FDP_NET_EXT.1 defines the TOE’s usage of network communications, which may include the transmission or receipt of data over a trusted channel. FIA_X509_EXT.1 defines X.509 certificate validation activities in support of trusted communications. FIA_X509_EXT.2 defines the trusted communications that X.509 certificate services support as well as the extent to which trusted communications can be established when using a certificate with unknown validity. FCS_TLS_EXT.1 defines the TOE’s support for the TLS communication protocol. FCS_TLSC_EXT.1 defines the TLS communication protocol as a client. FCS_TLSC_EXT.5 defines the supported groups extension in the TLS communication protocol.

Table 12: Security objectives for the TOE rationale

6.2.3 Security Requirements Dependency Analysis

The following table demonstrates the dependencies of the SFRs modeled in [ASPPv1.3]☝ and [TLSPKGv1.1]☝, and how the SFRs for the TOE resolve those dependencies.

Security functional requirement	Dependencies	Resolution
FCS_CKM_EXT.1	No dependencies	
FCS_CKM.1(1)	FCS_CKM_EXT.1	FCS_CKM_EXT.1
FCS_CKM.2	FTP_DIT_EXT.1	FTP_DIT_EXT.1
FCS_COP.1(1)	FTP_DIT_EXT.1	FTP_DIT_EXT.1
FCS_COP.1(2)	FTP_DIT_EXT.1	FTP_DIT_EXT.1
FCS_COP.1(3)	FTP_DIT_EXT.1	FTP_DIT_EXT.1
FCS_COP.1(4)	FTP_DIT_EXT.1	FTP_DIT_EXT.1
FCS_RBG_EXT.1	No dependencies	
FCS_RBG_EXT.2	FCS_RBG_EXT.1	FCS_RBG_EXT.1
	FCS_COP.1(1)	FCS_COP.1(1)
FCS_STO_EXT.1	No dependencies	
FCS_HTTPS_EXT.1 / Client	FTP_DIT_EXT.1	FTP_DIT_EXT.1
FDP_DEC_EXT.1	No dependencies	
FDP_NET_EXT.1	No dependencies	
FDP_DAR_EXT.1	No dependencies	
FIA_X509_EXT.1	FTP_DIT_EXT.1	FTP_DIT_EXT.1
FIA_X509_EXT.2	FTP_DIT_EXT.1	FTP_DIT_EXT.1
FMT_MEC_EXT.1	No dependencies	
FMT_CFG_EXT.1	No dependencies	
FMT_SMF.1	No dependencies	
FPR_ANO_EXT.1	No dependencies	
FPT_API_EXT.1	No dependencies	
FPT_AEX_EXT.1	No dependencies	
FPT_TUD_EXT.1	No dependencies	
FPT_TUD_EXT.2	FPT_TUD_EXT.1	FPT_TUD_EXT.1
FPT_LIB_EXT.1	No dependencies	

Security functional requirement	Dependencies	Resolution
FPT_IDV_EXT.1	No dependencies	
FTP_DIT_EXT.1	No dependencies	
FCS_TLS_EXT.1	No dependencies	
FCS_TLSC_EXT.1	FCS_TLS_EXT.1	FCS_TLS_EXT.1
	FCS_CKM.1	FCS_CKM.1(1)
	FCS_CKM.2	FCS_CKM.2

	FCS_COP.1	FCS_COP.1(1)
		FCS_COP.1(2)
		FCS_COP.1(3)
		FCS_COP.1(4)

	FCS_RBG_EXT.1	FCS_RBG_EXT.1 FCS_RBG_EXT.2
	FIA_X509_EXT.1	FIA_X509_EXT.1
	FIA_X509_EXT.2	FIA_X509_EXT.2
FCS_TLSC_EXT.5	FCS_TLSC_EXT.1	FCS_TLSC_EXT.1

Table 13: TOE SFR dependency analysis

6.2.4 Internal consistency and mutual support of SFRs

6.3 Security Assurance Requirements

The security assurance requirements (SARs) for the TOE are defined in the ASPPV1.3 protection profile.

The following table shows the SARs, and the operations performed on the components according to CC part 3: iteration (Iter.), refinement (Ref.), assignment (Ass.) and selection (Sel.).

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
ASE Security Target evaluation	ASE_CCL.1 Conformance claims	ASPPV1.3	No	No	No	No
	ASE_ECD.1 Extended components definition	ASPPV1.3	No	No	No	No
	ASE_INT.1 ST introduction	ASPPV1.3	No	No	No	No
	ASE_OBJ.1 Security objectives for the operational environment	ASPPV1.3	No	No	No	No
	ASE_REQ.1 Stated security requirements	ASPPV1.3	No	No	No	No

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
	ASE_SPD.1 Security problem definition	ASPPV1.3	No	No	No	No
	ASE_TSS.1 TOE summary specification	ASPPV1.3	No	No	No	No
ADV Development	ADV_FSP.1 Basic functional specification	ASPPV1.3	No	No	No	No
AGD Guidance documents	AGD_OPE.1 Operational user guidance	ASPPV1.3	No	No	No	No
	AGD_PRE.1 Preparative procedures	ASPPV1.3	No	No	No	No
ALC Life-cycle support	ALC_CMC.1 Labelling of the TOE	ASPPV1.3	No	No	No	No
	ALC_CMS.1 TOE CM coverage	ASPPV1.3	No	No	No	No
	ALC_TSU_EXT.1	ASPPV1.3	No	No	No	No
ATE Tests	ATE_IND.1 Independent testing - conformance	ASPPV1.3	No	No	No	No
AVA Vulnerability assessment	AVA_VAN.1 Vulnerability survey	ASPPV1.3	No	No	No	No

Table 14: SARs

6.4 Security Assurance Requirements Rationale

The [ASPPv1.3]☝ specifies the security assurance requirements (SARs) individually. Any and all rationale for this protection profile's selection of SARs is provided by the protection profile. No modifications and no augmentations have been made to the protection profile's SARs.

7 TOE Summary Specification

7.1 TOE Security Functionality

As per [ASPPv1.3]☝ and [TLSPKGv1.1]☝, the TOE supports the following major security features.

- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- Privacy
- Protection of the TSF
- Trusted path/channels

7.1.1 Cryptographic Support

7.1.1.1 Crytographic Algorithms

The TOE includes the OpenSSL for the IBM MaaS360 Cloud Extender cryptographic module which provides the necessary cryptographic algorithms to implement certificate signing requests (CSR) and supports secure communication using TLS. The application also invokes platform-provided functionality for secure communication using TLS.

The table below shows the cryptographic algorithms including their supported key sizes, the applicable standard and purpose, and whether it is implemented in the TOE, the underlying application, or both.

Cryptographic Service	Algorithm	Key sizes	Standard	Purpose	TOE	Platform Provided
Asymmetric Key Generation	RSA	2048 bit or greater	[FIPS186-4]☝	Certificate signing request	✓	
	Elliptic Curve Cryptography (ECC)	P-256, P-384	[FIPS186-4]☝	Ephemeral asymmetric key generation and validation for TLS key exchange	✓	✓
Key Establishment	Elliptic Curve	P-256, P-384	[SP800-56A-Rev3]☝	TLS key exchange	✓	✓
Data Encryption and Decryption	AES in CBC mode	256 bits	[SP800-38A]☝	DRBG	✓	✓
Data Encryption and Decryption	AES in GCM mode	128 bits	[SP800-38D]☝	Authenticated encryption	✓	✓
Message Digest	SHA-256, SHA-384	N/A	[FIPS180-4]☝	Pseudorandom function (PRF) Digital Signature Generation and Verification	✓	✓

Cryptographic Service	Algorithm	Key sizes	Standard	Purpose	TOE	Platform Provided
Digital Signature Generation and Verification	RSA digital generation and verification	2048 bits or greater	[FIPS186-4]	TLS server authentication	✓	✓
Message Authentication	HMAC	256 bits	[FIPS186-4]	Pseudorandom function (PRF)	✓	✓
Random Number Generator	DRBG_CTR	256 bits	[SP800-90A-Rev1]	TLS key exchange	✓	

Table 15: Cryptographic algorithms

Related SFRs:

- FCS_CKM.1(1)
- FCS_CKM.2
- FCS_COP.1(1)
- FCS_COP.1(2)
- FCS_COP.1(3)
- FCS_COP.1(4)
- FCS_RBG_EXT.1
- FCS_RBG_EXT.2

7.1.1.2 Random Bit Generation Services

The TOE implements its own deterministic random bit generator (DRBG) functionality. As mentioned in the previous section, the TOE includes the OpenSSL for the IBM MaaS360 Cloud Extender cryptographic module, which provides an implementation of the CTR_DRBG (AES). The TOE invokes this cryptographic service for random bit generation services by default, and there is no ability to specify the use of an alternative DRBG.

The TOE obtains entropy from the underlying platform to seed and reseed the DRBG. A seed of 384 bits is collected by invoking the BCryptGenRandom API function; the amount of entropy used for seeding the DRBG is always equal or greater than 256 bits.

The entropy source is described in more detail in the proprietary Entropy Assessment Report [CE-EAR].

Related SFRs:

- FCS_RBG_EXT.1
- FCS_RBG_EXT.2

7.1.1.3 Storage of credentials

The TOE relies on the underlying platform for securely storing credentials. The following table shows the credentials necessary for the operation of the TOE, their purpose, and their storage.

Credential	Purpose	Storage
Private PKI keys	EFS encryption	Windows certificate store
Private keys	Backup/transfer of Cloud Extender configuration file	EFS protected directory
	Registration request encryption	EFS protected directory
	License key	EFS protected directory
Credentials (username, password) for customer's instantiation	Authentication to Microsoft SCEP	Encrypted in Windows Registry
	Authentication to Active Directory and/or LDAP server	Encrypted in Windows Registry
	Authentication to Microsoft Exchange and/or Active Sync	Encrypted in Windows Registry

Table 16: Credential List

Related SFRs:

- FCS_STO_EXT.1

7.1.1.4 HTTPS and TLS Protocols

The TOE implements the HTTPS and TLS protocols to connect (as a TLS client) to the MaaS360 Cloud, and to Certificate Enrollment servers using the Simple Certificate Enrollment Protocol (SCEP). The HTTPS protocol is provided by the cURL library, whereas the TLS protocol is provided by the OpenSSL for the IBM MaaS360 Cloud Extender.

The TOE also invokes the underlying platform (via Powershell and .NET API classes) to establish secure communications as a TLS client with the rest of the endpoints: Microsoft Exchange Server, Active Directory Server and Entrust Certificate Server.

In both cases, the TLS protocol supports the following ciphersuites in the evaluated configuration:

- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289

The TOE validates the peer certificate used for the connection.

When negotiating the TLS v1.2 elliptic curve cipher suite, the TOE includes as part of the TLS handshake the supported group extension using elliptic curves based on the ciphersuites selected by the administrator of the endpoint. The TOE supports Supported Groups Extension in the Client Hello message per [RFC8422]☝. Elliptic curves secp256r1 and secp384r1 defined in [RFC7919]☝ are the only ones supported by default; no additional configuration is available.

The TOE also verifies during the TLS handshake that the identifying information in the TLS server certificate matches what is expected; this verification includes checking the expected Distinguished Name (DN), Subject Name (SN), or Subject Alternative Name (SAN) attributes along with any applicable extended key usage identifiers.

The Common Name (CN) (which is part of the DN or SN) and SAN referenced identifiers are verified against the identity of the remote computer’s DNS entry to ensure that it matches. The use of IP addresses is not supported.

Wildcards are accepted only in the leftmost portion of the resource identifier (i.e., *.contoso.com), otherwise the certificate will be deemed invalid. The CN and SAN are the only supported reference identifiers that can be forced as part of the certificate validation, and this behavior is not configurable.

The TOE does not provide a general-purpose capability to "pin" TLS certificates.

The TOE implements HTTP over TLS (HTTPS) as described in [RFC2818]☝ so that system applications executing on the TOE can securely connect to external servers using HTTPS.

Related SFRs:

- FTP_DIT_EXT.1
- FCS_HTTPS_EXT.1 / Client
- FCS_TLS_EXT.1
- FCS_TLSC_EXT.1
- FCS_TLSC_EXT.5

7.1.2 User Data Protection

7.1.2.1 Encryption of Sensitive Application Data

The Cloud Extender utilizes platform-provided functionality to encrypt sensitive data in non-volatile memory. In particular, it uses the Windows EFS to store sensitive data. Users are instructed to ensure that EFS is enabled for the folders identified in FDP_DAR_EXT.1.

The following sensitive information is stored:

- The C:\ProgramData\MaaS360\ directory that contains all configuration and log information.
- Registry entries using the Data Protection Application Programming Interface (DAPI).
- Private PKI keys
- Private keys
- User Modifiable Files

Related SFRs:

- FDP_DAR_EXT.1

7.1.2.2 Access to Platform Resources

With the exception of network connectivity, the TOE application does not restrict any access to platform hardware resources or peripherals. Additionally, the following sensitive information repositories are applicable to the TOE:

- Windows Credential Store (Protected by Platform DAC)
- TOE Windows Registry assets (Protected by DPAPI)

Restriction of access to the directories and files identified in FDP_DEC_EXT.1.2 is provided by the TOE platform's discretionary access controls.

Related SFRs:

- FDP_DEC_EXT.1

7.1.2.3 Network Communications

Network communications are established between the Cloud Extender and the customer's internal services as described in Figure 3.

The Cloud Extender (the TOE) acts as a bridge between the customer's servers and the SaaS-based cloud portal. The customer will configure which servers will be integrated into the solution and since exact DNS or URLs cannot be provided, example URLs and port addresses are given in the below table.

Network Communication Type	**Information**	**Example Port**
MS Exchange	https://[Exchange]/powershell https://mail01f35.forest35.fiberlinkqa.local/powershell	
User Auth/ Vis Secure LDAP	domaincontroller forest35.fiberlinkqa.local	636
Entrust	https://[Entrust Server]:Port/mdmws/services/AdminServiceV9 https://asmobileenrolldemo.entrust.com:19443/mdmws/services/AdminServiceV9	
NDES	https://[NDES Server]/certsrv/mscep/mscep.dll https://ca01f35.forest35.fiberlinkqa.local/certsrv/mscep/mscep.dll https://[NDES Server]/certsrv/mscep_admin https://ca01f35.forest35.fiberlinkqa.local/certsrv/mscep_admin	

Table 17: Cloud Extender Connections to Customer's Services

The Cloud Extender makes an outbound connection to the MaaS360 SaaS application. The following table outlines the outbound connection requirements for each instance of MaaS360 Cloud. Every customer will be assigned to a single MaaS360 SaaS application instance.

Network Communication Type	**Information**	**Example Port**
MaaS360 SaaS application	maas-central.maas360.com 208.76.130.120	443
	maas-central-##.maas360.com (where ## is an instance number) 208.76.128.150	443
M1 (portal.fiberlink.com)	services.fiberlink.com 208.76.128.153 208.76.130.181	443
	mpns.maas360.com 208.76.128.168 208.76.131.110	443

Network Communication Type	Information	Example Port
	https://license.fiberlink.com/internettest 208.76.128.58 208.76.130.58	443
	upload.fiberlink.com 54.224.0.0/12 54.230.0.0/15 54.192.0.0/11	443
	dl.maas360.com (no IP range)	-
M2 (m2.maas360.com)	services.m2.maas360.com 88.205.104.145 217.112.145.234	443
	mpns.m2.maas360.com 88.205.104.154 217.112.145.235	443
	https://license.fiberlink.com/internettest 208.76.128.58 208.76.130.58	443
	upload.fiberlink.com 54.224.0.0/12 54.230.0.0/15 54.192.0.0/11	443
	dl.m2.maas360.com (no IP range)	-
M3 (m3.maas360.com)	services.m3.maas360.com 208.76.133.30 50.204.34.212	443
	mpns.m3.maas360.com 208.76.133.28 50.204.34.211	443
	https://license.fiberlink.com/internettest 208.76.128.58	443

Network Communication Type	Information	Example Port
	208.76.130.58	
	upload.fiberlink.com 54.224.0.0/12 54.230.0.0/15 54.192.0.0/11	443
	dl.m3.maas360.com (no IP range)	-
M4 (m4.maas360.com)	services.m4.maas360.com 119.81.110.141 119.81.173.174	443
	mpns.m4.maas360.com 119.81.110.140 119.81.173.173	443
	https://license.fiberlink.com/internettest 208.76.128.58 208.76.130.58	443
	upload.fiberlink.com 54.224.0.0/12 54.230.0.0/15 54.192.0.0/11	443
	dl.m4.maas360.com (no IP range)	-
M5 (m5.maas360.com)	services.m5.maas360.com 59.144.107.12 169.38.87.152	443
	mpns.m5.maas360.com 59.144.107.15.140 169.38.87.155	443
	https://license.fiberlink.com/internettest 208.76.128.58 208.76.130.58	443
	upload.fiberlink.com	443

Network Communication Type	Information	Example Port
	54.224.0.0/12 54.230.0.0/15 54.192.0.0/11	
	dl.m5.maas360.com (no IP range)	-

Table 18: Cloud Extender Connections to MaaS360 SaaS Application

Related SFRs:

- FDP_NET_EXT.1

7.1.3 Identification and Authentication

7.1.3.1 X.509 Certificate Validation

The TOE conducts certificate validation by performing the following:

- Certificate validation and certificate path validation conforms to RFC 5280.
- The certificate path must terminate with a trusted CA certificate.
- All CA certificates must have the basicConstraints extension present and the CA flag set to TRUE.
- The certificate must not be revoked. This is established by a certificate revocation list (CRL) that is referenced by the TOE.
- The extendedKeyUsage field must be valid based on the following rules:
    - Certificates used for trusted updates and executable code integrity verification must have the Code Signing purpose (id-kp 3 with OID 1.3.6.1.5.5.7.3.3) in the extendedKeyUsage field.
    - Server certificates presented for TLS must have the Server Authentication purpose (id-kp with OID 1.3.6.1.5.5.7.3.1) in the extendedKeyUsage field.
    - Client certificates presented for TLS must have the Client Authentication purpose (id-kp2 with OID 1.3.6.1.5.5.7.3.2) in the extendedKeyUsage field.
    - Server certificates presented for EST must have the CMC Registration Authority (RA) purpose (id-kp-cmcRA with OID 1.3.6.1.5.5.7.3.28) in the extendedKeyUsage field.
- The SAN/CN checks follow all other certificate checks (e.g. signature validation, expiry, certificate purpose etc.)
    - If SAN is defined in the configuration file:
        - If the SAN defined in the presented certificate exactly matches the SAN defined in the configuration file the certificate is accepted.
        - Otherwise the certificate is rejected.
    - If CN is defined and SAN is not present:
        - the CN in the presented certificate must match CN defined in the configuration file.

- If there are no CNs listed in the configuration file, the certificate is accepted.

The use of IP addresses is not supported.

The TOE uses X.509 in support of TLS authentication. The use of certificates is enabled by default. TOE administrators may also specify the path to a certificate revocation list so that revocation status can be checked during authentication. The actual certificates and keys to be used by the TOE can be specified through the use of the Windows Credential Store for the platform-provided TLS. The TOE implementation of OpenSSL, OpenSSL for the IBM MaaS360 Cloud Extender, does not support the addition or configuration of additional TLS certificates. While the HTTPS implementation will automatically reject a certificate if it is found to be invalid, a certificate with unknown revocation status (because the TSF is unable to read or obtain the CRL) is rejected. In this case, an error message is generated and logged for TOE administrator.

Related SFRs:

- FIA_X509_EXT.1
- FIA_X509_EXT.2

7.1.4 Security Management

7.1.4.1 Secure By Default Configuration

The Cloud Extender does not require any credentials for access control to the application. A license key must be obtained from IBM in order to install the application.

Default credentials installed as a result of the Cloud Extender installation include the following:

- Credential Name
- ComodoCA.pem
- DigiCert_High_Assurance_EV_Root_CA.pem
- DigitCert_Global_Root_CA.pem
- DigiCert_SHA2_High_Assurance_Server_CA.pem
- DigiCert_SHA2_Secure_Server_CA.pem
- entrustsecureserver.pem
- GTECyberTrustGlobalRoot.pem
- VerisignCAG2.pem
- VerisignCAG3.pem
- VerisignCAG5.pem
- Certificate for accessing the MaaS360 SaaS application

Related SFRs:

- FMT_CFG_EXT.1

7.1.4.2 Supported Configuration Mechanism

The Cloud Extender is supplied along with the IBM MaaS360 Cloud Extender Configuration Tool. The configuration data for the Cloud Extender application is stored in the platform's Windows Registry and may optionally be exported to an encrypted file that is stored in an EFS protected folder on the platform. The following table details settings that pertain to SFR functionality:

Configuration Options	**Method**	
	Manually (see [CC-CFG])	**CE Configuration Tool**
TLS 1.2 System default	✓	
Limit HTTPS to TLS 1.2	✓	
Configure and enable the EFS Service	✓	
Use Proxy Authentication		✓
Mode		✓
Exchange ActiveSync Manager	✓	✓
User Authentication		✓
User Visibility		✓
Certificates Integration		✓
Configure Service Account		✓
Configure Certificate Templates		✓
Configure Cloud Extender Configuration		✓

Table 19: Cloud Extender Configuration Options

Additionally, the application relies on platform-provided access control mechanisms (user permissions) for securing access to TOE components outside of the EFS such as the installation directory where TOE binaries are located. The configuration of these elements is defined in the [ADM_GUIDE].

No other TOE management functions are applicable to the Cloud Extender.

Related SFRs:

- FMT_MEC_EXT.1
- FMT_SMF.1

7.1.5 Privacy

7.1.5.1 User Consent for Transmission of PII

The application does not contain any functionality that relates to Personally Identifiable Information (PII).

Related SFRs:

- FPR_ANO_EXT.1

7.1.6 Protection of the TSF

7.1.6.1 Anti-exploitation Capabilities

The following compiler flag and linker option is used to enable ASLR when the TOE is built:

`/DYNAMICBASE` (Use address space layout randomization)

The ASLR enabling option modifies the header of an executable to indicate that the application should be randomly rebased at load time. An explanation of the linker option can be found in the Microsoft Developer Network (MSDN) library at the following link: https://msdn.microsoft.com/en-us/library/bb384887.aspx. All the Dynamic Linked Libraries (DLLs) are compiled with this option.

The building procedure also uses the `/GS` flag set (default compiler option), which instructs the compiler to perform buffer security checks.

Two Cloud Extender components (luaCrypto and luaPKIExtender) contain support for enabling Federal Information Processing Standard (FIPS) 140-2 conformance via the OpenSSL for the IBM MaaS360 Cloud Extender. Please note that this implementation of the OpenSSL cryptographic module was not submitted for CMVP validation and such status is not being claimed. Both components statically link the OpenSSL library. It is a requirement of OpenSSL that the statically linked libraries specify a base address. The actual address is specified in the linker options. There is no specific address required, just that the address chosen is specified during the FIPS link step. IBM uses the following addresses:

```
luaCrypto: /BASE:0xFD00000
luaPKIExtender: /BASE:0x1A000000
```

Additionally, all executable files are located in the Cloud Extender installation directory while all user-modifiable files are written to a separate location within the EFS volume described in the [ADM_GUIDE].

Related SFRs:

- FPT_AEX_EXT.1

7.1.6.2 Use of Supported Services and APIs

The table below lists the APIs provided by the TOE platform.

API Category	Windows APIs
PowerShell Commandlets	• Get-ItemProperty • Get-Item • Remove-Item • Get-Command • Add-Type • New-Object • Get-PSSession • Remove-PSSession • ConvertTo-SecureString • New-PSSessionOption • Connect-ExchangeOnline

API Category	Windows APIs
	• Start-Sleep • Import-PSSession • Get-Content • get-childitem • Export-CSV • Get-PSSnapin • Add-PSSnapin • Remove-Variable • Get-ActiveSyncOrganizationSettings • Set-ActiveSyncOrganizationSettings • Get-ExchangeServer • Get-ActiveSyncMailboxPolicy • Get-MobileDeviceMailboxPolicy • Set-ActiveSyncMailboxPolicy • Set-MobileDeviceMailboxPolicy • New-ActiveSyncMailboxPolicy • New-MobileDeviceMailboxPolicy • Remove-ActiveSyncMailboxPolicy • Remove-MobileDeviceMailboxPolicy • Get-CASMailbox • Set-CASMailbox • Get-ActiveSyncDeviceStatistics • Get-ActiveSyncDevice • Get-MobileDeviceStatistics • Get-MobileDevice • Clear-ActiveSyncDevice • Clear-MobileDevice • Remove-ActiveSyncDevice • Remove-MobileDevice • Get-OrganizationalUnit • Get-Recipient • Remove-RoleGroup • Remove-ManagementRoleAssignment • Remove-ManagementRole • New-ManagementRole • Get-ManagementRoleEntry • Read-Host • Write-Host • New-RoleGroup
Active Directory	• System.DirectoryServices.ActiveDirectory.Forest.GetCurrentForest • System.DirectoryServices.DirectoryEntry.Properties • System.DirectoryServices.DirectorySearcher.FindAll

API Category	Windows APIs
	• System.DirectoryServices.DirectorySearcher.PropertiesToLoad.Add • System.DirectoryServices.ActiveDirectory.Forest.GetCurrentForest().GetAllTrustRelationships • System.DirectoryServices.ActiveDirectory.Domain.GetDomain
LDAP	• SearchRequest • DirectoryAttributeModification • ModifyRequest • LdapConnection • VerifyServerCertificateCallback • DirectoryAttribute • PageResultRequestControl
Windows Registry	• RegOpenCurrentUser • RegCreateKey • RegOpenKey • RegCloseKey • RegDeleteKey • RegDeleteValue • RegQueryInfoKey • RegQueryValue • RegSetValue • RegEnumValue • RegEnumKey
Windows Management Instrumentation (WMI)	• ExecQuery • CoInitializeEx • CoUninitialize • GetObjectText • ExecMethod • SpawnInstance • ConnectServer • CreateObjectStub • ExecNotificationQueryAsync • CancelAsyncCall • GetObjectW
Process	• CreateProcess • GetProcAddress • GetExitCodeProcess • CloseHandle • AdjustTokenPrivileges • LookupPrivilegeValue • OpenProcessToken • OpenProcess

API Category	Windows APIs
	• OpenThreadToken • CreateToolhelp32Snapshot • Process32First • Process32Next • TerminateProcess • WaitForMultipleObjects • WaitForSingleObject • CreateMutex • OpenMutex • Sleep • ReleaseMutex • ReleaseSemaphore • CreateSemaphore • OpenSemaphore • CreateEvent • ResetEvent • GetCurrentProcess • GetProcessIoCounters • GetProcessMemoryInfo • SetThreadPriority • SetEvent • GetCurrentThreadId • RegisterEventSource • ReportEvent • DeregisterEventSource • PeekMessage • TranslateMessage • DispatchMessage • EnterCriticalSection • LeaveCriticalSection • IsWow64Process • CoCreateInstance
Windows OS HTTP (Networking)	• WinHttpSendRequest • WinHttpWriteData • WinHttpReceiveResponse • WinHttpQueryDataAvailable • WinHttpReadData • WinHttpOpen • WinHttpSetTimeouts • WinHttpCrackUrl • WinHttpConnect • WinHttpOpenRequest

API Category	Windows APIs
	• WinHttpCloseHandle • WinHttpSetOption • WinHttpSetCredentials • WinHttpAddRequestHeaders • WinHttpQueryHeaders • WinHttpQueryAuthSchemes • WSACloseEvent • WSAGetLastError • WSACreateEvent • NotifyAddrChange • CoSetProxyBlanket • WinHttpGetIEProxyConfigForCurrentUser • InternetQueryOptionW • InternetCrackUrlA • WinHttpGetProxyForUrl • WinHttpDetectAutoProxyConfigUrl • WlanQueryInterface • WlanCloseHandle • WlanOpenHandle • WlanFreeMemory • WlanGetProfile • GetAdaptersAddresses
SOAP http	System.Web.Services.Protocols.SoapHttpClientProtocol methods • Invoke • BeginInvoke • EndInvoke • InvokeAsync
Windows Service	• OpenSCManagerW • OpenServiceW • QueryServiceStatus • CloseServiceHandle • StartServiceW • ControlService • QueryServiceConfigW • DeleteService • EnumServicesStatusW
Microsoft Certificate Store	• CertAddCertificateContextToStore • CertCloseStore • CertComparePublicKeyInfo • CertEnumCertificatesInStore • CertEnumCRLsInStore

API Category	Windows APIs
	• CertFindCertificateInStore • CertNameToStr • CertOpenStore • CertOpenSystemStore • CertSetCertificateContextProperty • PFXExportCertStore
Microsoft CryptoAPI	• CryptAcquireContext • CryptBinaryToString • CryptCreateHash • CryptDecryptMessage • CryptDeriveKey • CryptEncrypt • CryptDestroyHash • CryptDestroyKey • CryptExportPublicKeyInfo • CryptGetUserKey • CryptHashData • CryptImportKey • CryptMsgOpenToDecode • CryptMsgUpdate • CryptMsgGetParam • CryptReleaseContext • CryptGenRandom • BCryptGenRandom

Table 20: Windows APIs Used by the Cloud Extender

The Cloud Extender installation package is signed by IBM using a Symantec certificate issued to IBM. Instructions for viewing the certificate are found in the [ADM_GUIDE]. The Cloud Extender is not subject to updates.

The version of the core installer can be determined via the *Control Panel » Program and Features* facility in Windows.

The version of the modules can be inspected through the Windows File Manager. Right click on the emsagent.exe file and select *Properties*.

The module versions are displayed on one of the final IBM MaaS360 Cloud Extender Configuration Tool screens.

Related SFRs:

- FPT_API_EXT.1

7.1.6.3 Use of Third-party Libraries

The TOE is comprised with the third-party libraries shown in the following table.

Library	Version	URL
SQLite	3.35.5	https://sqlite.org
OpenSSL with OpenSSL FIPS Module	1.0.2za and 2.0.16	https://www.openssl.org
libcURL	7.83.0	https://curl.haxx.se
Zlibc	1.1.4	https://zlibc.linux.lu
Protobuf	2.6.1	https://code.google.com/p/protobuf
Boost	1.5.9	http://www.boost.org
Bitwise operation library	5.2.0	https://github.com/mcschroeder/lua-5.2.0-special/blob/master/src/lbitlib.c
Lua	5.1	http://www.lua.org
Lua cURL	1.6	https://github.com/Lua-cURL
LuaSQL	2.1	https://keplerproject.github.io/luasql
DotNetZip	1.9.1.8	https://dotnetzip.codeplex.com
NSIS	2.46	http://nsis.sourceforge.net
CMarkup	11.2	http://www.firstobject.com/dn_markup.htm
Gloox Library	1.0.1	https://camaya.net/gloox
InstallShield	2015 + SP1 professional	https://www.revenera.com/install/products/installshield.html

Table 21: Third-party Libraries

Related SFRs:

- FPT_LIB_EXT.1

7.1.6.4 TOE Identification

The identification of the TOE can be verified by looking at the Product Name and Product Version properties of the emsagent.exe program (e.g. by using the Windows File Manager, right clicking on the emsagent.exe file and selecting *Properties*).

The module version is also displayed on one of the final IBM MaaS360 Cloud Extender Configuration Tool screens.

Related SFRs:

- FPT_IDV_EXT.1

7.1.6.5 Timely Security Updates

7.1.6.5.1 TOE installation

The TOE can be downloaded and installed from the MasS360 portal (https://login.maas360.com), following the instructions provided in the guidance documentation ([CC-CFG] and [ADM_GUIDE]).

7.1.6.5.2 Security Update Process for the Cloud Extender

The TOE is not subject to updates. If security updates are identified, a new version of the TOE must be installed. Installers for the TOE are signed by IBM in accordance with the Microsoft Authenticode process using a Class 3 SHA-256 certificate provided by Symantec. This signature is the only authorized source for the TOE.

The TOE provides capabilities for checking the current version and if updates are available through the IBM MaaS360 Cloud Extender Configuration Tool as documented in the [CC-CFG], section 6.2. If an update is available, the new installer must be obtained from the customer portal which requires authentication.

Automatic updates are not available and the TOE has no capacity to download, modify, or replace its own binary code. Additionally, uninstall procedures provided in the [CC-CFG] will result in the complete removal of the TOE from the underlying platform including all log and configuration data.

Related SFRs:

- FPT_TUD_EXT.1
- FPT_TUD_EXT.2

7.1.6.5.3 Process for handling security vulnerabilities

The IBM Product Security Incident Response Team (PSIRT) process is described at: https://www.ibm.com/security/secure-engineering/process.html.

The process for creating and deploying security updates is as follows.

1. Internal or external testing or a third-party report discovers a vulnerability.
2. The IBM X-Force team provides CVSS scoring.
3. Development teams investigate and remediate the issue.
4. A fix is tested and validated in QA and Staging.
5. The fix is deployed via the appropriate distribution channels (SaaS continuous integration / continuous deployment (CI/CD) release window or publishing apps to the relevant app stores).

During the analysis of the vulnerability, IBM identifies which part of the TOE or third-party libraries are involved. Any necessary updates to third-party components are included and distributed with the updated CE application. Hence no third-party processes need to be considered by users.

Users are notified when updates change security properties or configuration of the product.

IBM request that sensitive information is encrypted and supply a Pretty Good Privacy (PGP) public key for the purpose.

The length of time in days between public disclosure of a vulnerability and the public availability of the security update for the TOE can vary based on their severity as follows.

Time frames are set by IBM PSIRT based on CVSS scoring as follows:

- CVSS Effective Score between 7 and 10 - Resolve as soon as possible, not to exceed 90 days, less than 30 days preferred
- CVSS Effective Score between 0 and 6.9 - Resolve as soon as possible, not to exceed 180 days

The PSIRT team may also flag vulnerabilities to be expedited regardless of CVSS Effective Score of a finding if circumstances warrant a faster resolution.

7.1.6.5.4 Notification of updates and security related fixes

Customers can use any or all of the following notification mechanisms.

1. The Cloud Extender heartbeats into the MaaS360 platform every 5 minutes. If updates are available, there will be an event written to the Windows System Event log. The log can be viewed by an administrator. Additionally, administrators may manually check for updates using the procedure described in the [ADM_GUIDE].
2. All release communication is found on the IBM Support page: https://www.ibm.com/support/pages/maas360-release-notes.
3. Whenever IBM elevates new code, the site is updated and customers are notified to review these updates.

Information about how and where security bulletins are published is found at: https://www-03.ibm.com/security/secure-engineering/bulletins.html

7.1.7 Trusted path/channels

The TOE provides protection of data in transit by enforcing all network communication (mentioned in FDP_NET_EXT.1 to use HTTPS and TLS.

The following APIs provided by the TOE platform provides protection of the network channels. The list of API function can be found in Table 20.

- PowerShell Commandlets
- Active Directory API
- LDAP API
- Windows OS HTTP API
- SOAP http

Related SFRs:

- FTP_DIT_EXT.1

8 Abbreviations, Terminology and References

8.1 Abbreviations

AES
Advanced Encryption System

API
Application Program Interface

ASLR
Address Space Layout Randomization

CA
Certificate Authority

CAVP
Cryptographic Algorithm Validation Program

CAVS
Cryptographic Algorithm Validation System

CBC
Cypher Block Chaining

CC
Common Criteria

CCM
Counter with CBC-MAC

CE
Cloud Extender

CI/CD
Continuous Integration/Continuous Deployment

CN
Common Name

CNG
Cryptography API: Next Generation

CRL
Certificate Revocation List

cURL
Client for URLs

CVL
Component Validation List

CVSS
Common Vulnerability Scoring System

DLL
Dynamic Link Library

DMZ
De-militarized Zone

DN
Distinguished Name

DPAPI
Data Protection Application Programming Interface

DRBG
Deterministic Random Bit Generator

EAR
Entropy Analysis Report

ECC
Elliptic Curve Cryptography

ECDSA
Elliptic Curve Digital Signature Algorithm

EFS
Encrypted File System

EMM
Enterprise Mobility Management

EMS
Endpoint Management System

FIPS
Federal Information Processing Standard

GCM
Galois/Counter Mode

HMAC
Keyed-hash Message Authentication Code

HTTPS
Hypertext Transfer Protocol over TLS

IBM
International Business Machines

LDAP
Lightweight Directory Access Protocol

LDAPS
Secure LDAP

MSDN
Microsoft Developers Network

NDES
Network Device Enrollment Service

NIAP
National Information Assurance Partnership

OSP
Organizational Security Policies

PCL
Product Compliant List

PGP
Pretty Good Privacy

PII
Personally Identifiable Information

PP
Protection Profile

PSIRT
Product Security Incident Response Team

RBG
Random Bit Generator

RSA
Rivest-Shamir-Adleman

SaaS
Software as a Service

SAN
Subject Alternative Name

SCEP
Simple Certificate Enrollment Protocol

SN
Subject Name

SSL
Secure Sockets Layer

ST
Security Target

SWID
Software ID

TLS
Transport Layer Security

TOE
Target of Evaluation

TSF
TOE Security Function

TSFI
TOE Security Function Interfaces

TSS
TOE Security Summary

VPN
Virtual Private Network

XMPP
Extensible Messaging and Presence Protocol

8.2 Terminology

8.3 References

ADM_GUIDE **MaaS360 Cloud Extender Admin Guide**
Version 1.0
Date 2022-07-20

ASPPv1.3 **Protection Profile for Application Software Version 1.3**
Version 1.3
Date 2016-02-22
Location https://www.niap-ccevs.org/MMO/pp/pp_app_v1.3.pdf

CC **Common Criteria for Information Technology Security Evaluation**
Version 3.1R5
Date April 2017
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART1V3.1R5.pdf
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART2V3.1R5.pdf
Location http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R5.pdf

CC-CFG **MaaS360 Cloud Extender Common Criteria Guide**
Version 1.0
Date 2022-07-20

CCEVS-TD0416 **Correction to FCS_RBG_EXT.1 Test Activity**
Date 2019-04-24
Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0416

CCEVS-TD0427 **Reliable Time Source**
Date 2019-06-11
Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0427

CCEVS-TD0434 **Windows Desktop Applications Test**
Date 2019-07-22
Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0434

CCEVS-TD0435 **Alternative to SELinux for FPT_AEX_EXT.1.3**
Date 2019-07-26
Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0435

CCEVS-TD0437 **Supported Configuration Mechanism**
Date 2019-07-23
Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0437

CCEVS-TD0442	**Updated TLS Ciphersuites for TLS Package**	
	Date	2019-08-21
	Location	https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0442
CCEVS-TD0445	**User Modifiable File Definition**	
	Date	2019-10-09
	Location	https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0445
CCEVS-TD0465	**Configuration Storage for .NET Apps**	
	Date	2019-11-08
	Location	https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0465
CCEVS-TD0469	**Modification of test activity for FCS_TLSS_EXT.1.1 test 4.1**	
	Date	2019-11-20
	Location	https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0469
CCEVS-TD0495	**FIA_X509_EXT.1.2 Test Clarification**	
	Date	2020-01-29
	Location	https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0495
CCEVS-TD0498	**Application Software PP Security Objectives and Requirements Rationale**	
	Date	2020-01-31
	Location	https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0498
CCEVS-TD0499	**Testing with pinned certificates**	
	Date	2020-02-04
	Location	https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0499
CCEVS-TD0510	**Obtaining random bytes for iOS/macOS**	
	Date	2020-03-03
	Location	https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0510
CCEVS-TD0513	**CA Certificate loading**	
	Date	2020-05-26
	Location	https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0513
CCEVS-TD0515	**Use Android APK manifest in test**	
	Date	2020-06-08
	Location	https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0515

CCEVS-TD0519 **Linux symbolic links and FMT_CFG_EXT.1**
Date 2020-06-18
Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0519

CCEVS-TD0543 **FMT_MEC_EXT.1 evaluation activity update**
Date 2020-09-15
Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0543

CCEVS-TD0544 **Alternative testing methods for FPT_AEX_EXT.1.1**
Date 2020-09-15
Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0544

CCEVS-TD0548 **Integrity for installation tests in AppSW PP 1.3**
Date 2020-09-30
Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0548

CCEVS-TD0554 **iOS/iPadOS/Android AppSW Virus Scan**
Date 2020-10-30
Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0554

CCEVS-TD0561 **Signature verification update**
Date 2021-01-15
Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0561

CCEVS-TD0582 **PP-Configuration for Application Software and Virtual Private Network (VPN) Clients now allowed**
Date 2021-04-16
Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0582

CCEVS-TD0588 **Session Resumption Support in TLS package**
Date 2021-05-12
Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0588

CCEVS-TD0598 **Expanded AES Modes in FCS_COP for App PP**
Date 2021-08-03
Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0598

CCEVS-TD0600 **Conformance claim sections updated to allow for MOD_VPNC_V2.3**
Date 2021-08-10
Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0600

CCEVS-TD0601 **X.509 SFR Applicability in App PP**
Date 2021-09-22
Location https://www.niap-ccevs.org/Documents_and_Guidance/view_td.cfm?TD=0601

CE-EAR **MaaS360 Cloud Extender Entropy Assessment Report**
Version 2.0
Date 2020-08-17

FIPS180-4 **Secure Hash Standard (SHS)**
Date 2015-08-04
Location https://csrc.nist.gov/publications/detail/fips/180/4/final

FIPS186-4 **Digital Signature Standard (DSS)**
Date 2013-07-19
Location https://csrc.nist.gov/publications/detail/fips/186/4/final

NIAP-PCL **NIAP Product Compliant List**
Date received 2019-10-26
Location https://www.niap-ccevs.org/Product/CompliantCC.cfm?CCID=2019.1244

RFC2818 **HTTP Over TLS**
Author(s) E. Rescorla
Date 2000-05-01
Location http://www.ietf.org/rfc/rfc2818.txt

RFC7919 **Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS)**
Author(s) D. Gillmor
Date 2016-08-01
Location http://www.ietf.org/rfc/rfc7919.txt

RFC8422 **Elliptic Curve Cryptography (ECC) Cipher Suites for Transport Layer Security (TLS) Versions 1.2 and Earlier**
Author(s) Y. Nir, S. Josefsson, M. Pegourie-Gonnard
Date 2018-08-01
Location http://www.ietf.org/rfc/rfc8422.txt

SP800-38A **Recommendation for Block Cipher Modes of Operation: Methods and Techniques**
Date 2001-12-01
Location https://csrc.nist.gov/publications/detail/sp/800-38a/final

SP800-38D **Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC**
Date 2007-11-28
Location https://csrc.nist.gov/publications/detail/sp/800-38d/final

SP800-56A-Rev3 **Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography**
Date 2018-04-16
Location https://csrc.nist.gov/publications/detail/sp/800-56a/rev-3/final

SP800-90A-Rev1 **Recommendation for Random Number Generation Using Deterministic Random Bit Generators**
Date 2015-06-24
Location https://csrc.nist.gov/publications/detail/sp/800-90a/rev-1/final

TLSPKGv1.1 **Functional Package for Transport Layer Security (TLS)**
Version 1.1
Date 2019-02-12
Location https://www.niap-ccevs.org/MMO/PP/PKG_TLS_V1.1.pdf