IBM MaaS360 Cloud Extender version 3.000.800 Security Target

Version:	**1.3**
Status:	**Final**
Last Update:	**2025-08-12**
Classification:	**Public**
Authors:	**atsec**

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/copyright-trademark.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

Version	Date	Author(s)	Changes to Previous Revision
1.0	2024-12-06	atsec	First version
1.1	2025-02-25	atsec	Address ECR comments
1.2	2025-07-21	atsec	Update TOE version and address evaluator's comments. Update library list aligned with SBOM. Apply TD0931.
1.3	2025-08-12	atsec	Update bibliographic reference for CC guide.

Table of Contents

List of Tables

List of Figures

1 Introduction

1.1 Security Target Identification

Title:	IBM MaaS360 Cloud Extender version 3.000.800 Security Target
Version:	1.3
Status:	Final
Date:	2025-08-12
Sponsor:	International Business Machines Corporation
Developer:	International Business Machines Corporation
Validation Body:	NIAP
Validation ID:	VID11531
Keywords:	IBM Corporation

1.2 TOE Identification

The TOE is IBM MaaS360 Cloud Extender version 3.000.800.038.

1.3 TOE Type

The TOE type is a software application.

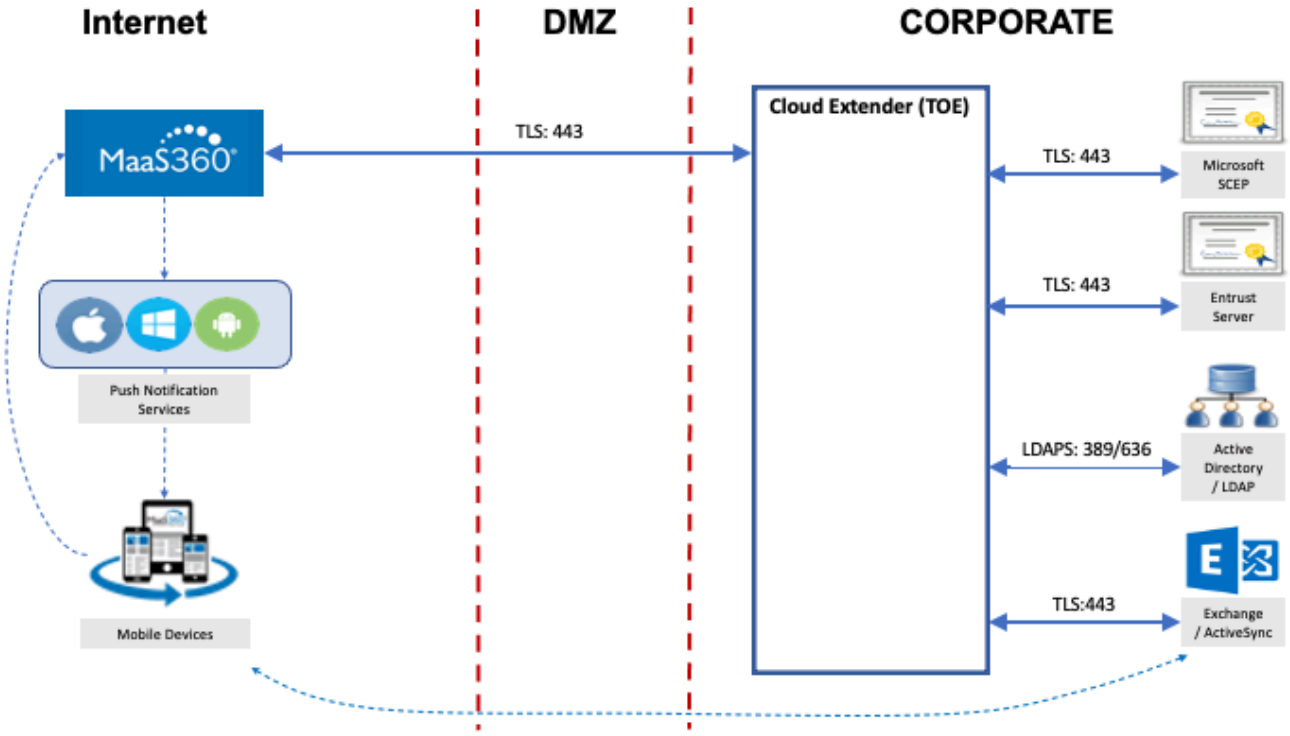
1.4 TOE Overview

The TOE is the IBM Cloud Extender (CE) application. It consists of four modules enabling communications functionality with various customer-provided services and the IBM MaaS Cloud Extender Configuration Tool, hereafter refers to as Configuration Tool. The TOE also includes guidance documentation as described in section 1.5.2.1.2. The major security features of the TOE include cryptographic support, user data protection, identification and authentication, security management, protection of the TOE security functionality, and the establishment of trusted paths using the TLS protocol.

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. Specificially, the TOE is installed behind the customer firewall with network access to appropriate internal systems. The TOE is available as a small Windows application (approx. 12MB). The TOE is not a distributed application or 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 dashed lines are not part of the TOE and thus are not covered by the evaluation.

Figure 1: Trusted Communication Channels for a Cloud Extender



The TOE makes an outbound connection to the IBM MaaS360 Cloud (labeled as MaaS360 in the left-top blue box) over port 443 using the Transport Layer Security (TLS) protocol and the Message Queuing Telemetry Transport (MQTT) protocol to maintain the connection with the MaaS360 Cloud.

The TOE falls under use case 3 ("Communication") scenario, described in section 1.4 of [PP_APP_V1.4] as follows:

> "*The TOE 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 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, only the following modules are covered:

- Exchange Integration Module
- User Authentication Module
- User Visibility Module
- Certificate Integration Module

1.5.1 Architecture

The Cloud Extender consists of multiple processes running simultaneously. The TOE is comprised of:

- The Core Installer, which is a Windows service.

- The four CE modules mentioned above.
- The Cloud Extender Configuration Tool.

The TOE uses the following cryptographic libraries:

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

The Windows CNG is used for HTTPs connections and data-at-rest purposes.

OpenSSL is used for HTTPS connections and 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 IBM MaaS360 Cloud and other endpoints. The Core installer uses TLS 1.2 and initiates all communication. Thus, the TOE acts as a TLS client. For IBM MaaS360 Cloud and the NDES/CA Certificate Server endpoint, the Core installer uses Client for URLs (cURL) and the TLS layer provided by OpenSSL, for the rest of the endpoints (MS Exchange Server, Active Directory Server or LDAP Server, Entrust Certificate Server), the Core Installer uses the functionality provided by the underlying platform (i.e. the Windows CNG).

The TOE is also 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.

Table 1: Description of the Cloud Extender Modules

CE Module	Description
Exchange Integration module	The Exchange Integration module interacts with the Exchange Server to automatically discover ActiveSync-connected devices, and uploads that device information to the IBM 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 2010, 2013, 2016, and Office 365.
User Authentication module	The User Authentication module interacts with Active Directory or 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. Cloud Extender supports integration with Lightweight Directory Access Protocol (LDAP) implementations, including Active Directory, Domino® LDAP, Oracle® LDAP, Novell® eDirectory LDAP, and OpenLDAP.
User Visibility Module	The User Visibility module uses the corporate directory groups to allow for the assignment and distribution of policies, apps, and content to mobile devices.

CE Module	Description
	These groups are imported by the MaaS360 Administrator to control administrator access to manage a subset of devices. LDAP filters are used to limit the groups and organizations imported. Devices are managed based on corporate directory structure.
Certificate Integration 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 TOE 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.

1.5.2 TOE boundaries

1.5.2.1 Physical boundary of the TOE

The physical boundary of the TOE consists of the TOE software, which is the application installer executable. The TOE is distributed as electronic download 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 5120 processor (SkyLake microarchitecture).

1.5.2.1.2 TOE Guidance

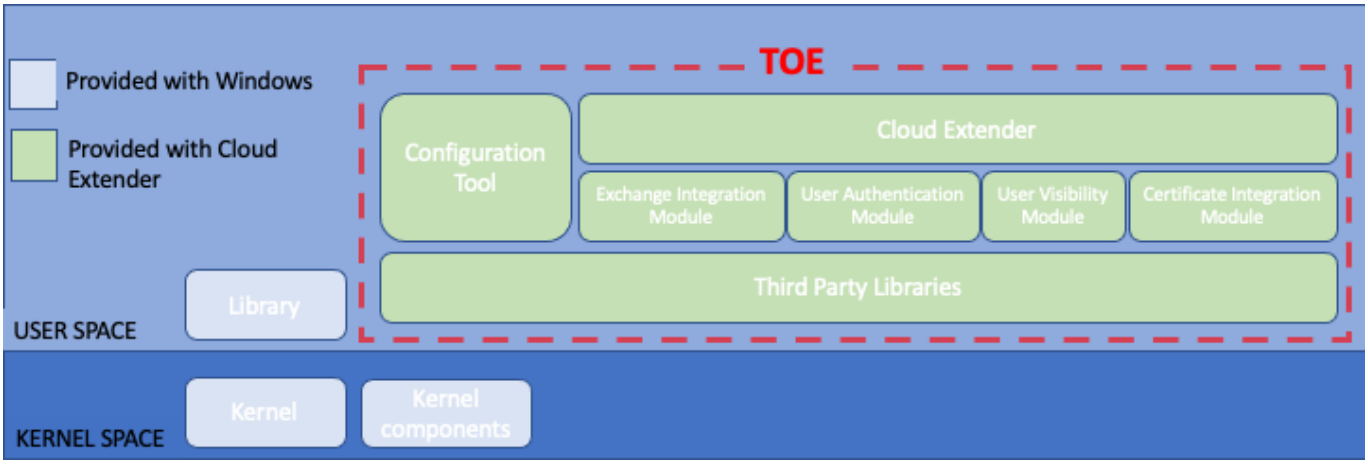
The TOE guidance documentation, which consists of the following guides, is available on the IBM MaaS portal.

- 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 Functionality (TSF) as specified in [PP_APP_V1.4].

Figure 2: Logical Boundary of the TOE



1.5.2.3 Security Functions provided by the TOE

The TOE provides the security functions required by [PP_APP_V1.4] and [PKG_TLS_V1.1], which is summarized in the following sections.

1.5.2.3.1 Cryptographic Support (FCS)

The TOE provides the following cryptographic functions via the Microsoft Cryptography API: Next Generation (CNG) cryptographic library from the underlying Microsoft Windows Server platform on which the TOE runs:

1. TLS connections: the TOE communicates with the Exchange Server, Domain Controller, and PKI Certificate Servers using HTTPS and the Microsoft Secure Channel (SChannel) Security Service Provider, using Windows CNG for cryptographic functionality. The TOE limits the protocol to TLS 1.2, with only a subset of the TLS 1.2 cipher suites.
2. Protecting data-at-rest using the Encrypted File System (EFS) to the `C:\ProgramData\MaaS360\Cloud Extender` directory that contains all configuration and log information.
3. Encrypting registry entries using the Data Protection Application Programming Interface (DPAPI).

In addition, the TOE comes with its own OpenSSL cryptographic module version 1.0.2zh, which provides the following cryptographic services:

1. TLS connections to the MaaS360 Portal and SCEP certificate servers (HTTPS using cURL). The protocol is also limited to TLS 1.2, and only using a subset of the TLS 1.2 cipher suites.
2. 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 TOE, as outlined in Table 2.

Table 2: Device and User Certificate Related Functionality

Type	Explanation
Mobile Device	The TOE generates a certificate based on requirements and pushes that certificate to the mobile device. The TOE 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.

Type	Explanation
	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	Supported only by Microsoft CA. 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.

The TOE implements its own SP800-90A DRBG through OpenSSL. The entropy used to seed this DRBG provided by the TOE is obtained from the Microsoft Windows Server platform on which the TOE runs. The DRBG 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 proprietary Entropy Assessment Report provides additional details on the entropy source.

1.5.2.3.2 User Data Protection (FDP)

The TOE provides user data protection services by restricting its access to specific platform-based resources (sensitive data repositories, and network communications) that are strictly needed to support the necessary TOE functionality.

Sensitive application data is protected 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 TOE and by 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 TOE provides the ability to set a number of its configuration options. 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 TOE platform are allocated with appropriate file permissions, supporting the protection of the TOE and its data from unauthorized access.

1.5.2.3.5 Privacy (FPR)

The TOE does not specifically request Personally Identifiable Information (PII).

1.5.2.3.6 Protection of the TSF (FPT)

The TOE only uses documented Windows APIs. The TOE is packaged with third-party libraries which provide supporting functionality. The third-party libraries are listed in section 6.1.6.6.

The TOE does not write user-modifiable files to directories that contain executable files.

The TOE implements anti-exploitation capabilities including stack buffer overrun protection (through compilation by IBM) and Address Space Layout Randomization (ASLR) techniques. Also, the TOE does not generally request to map memory at explicit addresses, except for those listed in section 7.1.6.

The TOE is packaged and delivered in the Windows Application Software (.EXE) format signed with Microsoft Authenticode using the Microsoft Sign Tool.

1.5.2.3.7 Trusted Path/Channels (FTP)

The TOE protects all transmitted data via trusted channels over TLS 1.2. 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 part of the MaaS360 Cloud Extender product but are not delivered with the TOE and therefore the services they provide are excluded from the evaluated configuration.

- Email Notification module
- IBM Traveler Integration module
- Mobile Enterprise Gateway (MEG) module

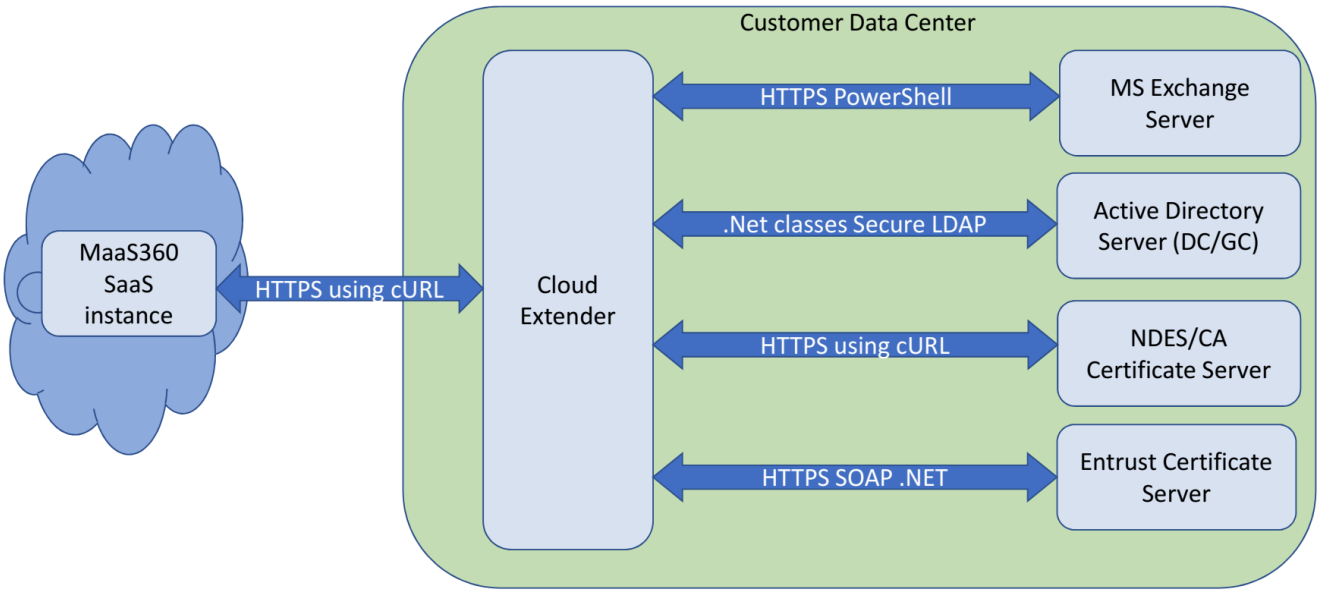
1.5.2.5 Operational Environment

The TOE requires the following in its operational environment.

- A configured and operational instance of the IBM MaaS360 Cloud.
- One or more enrolled mobile devices.
- A network connection to the IBM MaaS360 Cloud 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 or LDAP Server (connected in LDAP mode).
- A Network Device Enrollment Server Certificate Authority (NDES CA) server and/or An Entrust Certificate server.

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

Figure 3: Operational Environment for the 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:

- [PP_APP_V1.4]: Protection Profile for Application Software. Version 1.4 as of 2021-10-07; exact conformance.
- [PKG_TLS_V1.1]: 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 [PP_APP_V1.4] at the time of the creation of this Security Target and a statement of applicability to the evaluation.

Table 3: NIAP Technical Decisions for [PP_APP_V1.4]

TD #	Description	Applicable?	Non-applicability rationale
TD0931	Clarification when CTR_DRBG is Selected for FCS_RBG_EXT.2.2 in PP_APP_V1.4	Yes	
TD0893	Addition of Recommended Configuration Locations for Windows in FMT_MEC_EXT.1.1	No	The TOE is not a .NET application
TD0865	Consistency of Cryptographic Key Sizes	No	The ST does not claim conformance to FCS_CKM.1.1/ PBKDF
TD0860	Updating FIPS 186-4 to 186-5 in PP_APP_V1.4	Yes	
TD0844	Addition of Assurance Package for Flaw Remediation V1.0 Conformance Claim	No	The ST does not claim conformance to Assurance Package for Flaw Remediation V1.0.
TD0823	Update to Microsoft Windows Exploit Protection link in FPT_AEX_EXT.1.3	Yes	
TD0822	Correction to Windows Manifest File for FDP_DEC_EXT.1	Yes	
TD0815	Addition of Conditional TSS Activity for FPT_AEX_EXT.1.5	Yes	
TD0798	Static Memory Mapping Exceptions	Yes	
TD0780	FIA_X509_EXT.1 Test 4 Clarification	Yes	
TD0756	Update for platform-provided full disk encryption	Yes	
TD0747	Configuration Storage Option for Android	No	The TOE's platform is not Android.
TD0743	FTP_DIT_EXT.1.1 Selection exclusivity	Yes	
TD0736	Number of elements for iterations of FCS_HTTPS_EXT.1	No	The ST does not claim conformance to FCS_HTTPS_EXT.1/Server.
TD0719	ECD for PP APP V1.3 and 1.4	Yes	
TD0717	Format changes for PP_APP_V1.4	Yes	

TD #	Description	Applicable?	Non-applicability rationale
TD0664	Testing activity for FPT_TUD_EXT.2.2	Yes	
TD0650	Conformance claim sections updated to allow for MOD_VPNC_V2.3 and 2.4	No	The ST does not claim MOD_VPNC_V2.3 and 2.4
TD0628	Addition of Container Image to Package Format	Yes	

Table 4 below contains the NIAP Technical Decisions (TDs) for the [PKG_TLS_V1.1] at the time of the creation of this Security Target and a statement of applicability to the evaluation.

Table 4: NIAP Technical Decisions for [PKG_TLS_V1.1]

TD #	Description	Applicable?	Non-applicability rationale
TD0779	Updated Session Resumption Support in TLS package V1.1	Yes	
TD0770	TLSS.2 connection with no client cert	No	The ST does not claim TLSS SFRs.
TD0739	PKG_TLS_V1.1 has 2 different publication dates	Yes	
TD0726	Corrections to (D)TLSS SFRs in TLS 1.1 FP	No	The ST does not claim TLSS SFRs.
TD0513	CA Certificate loading	Yes	
TD0499	Testing with pinned certificates	No	The TOE does not support pinned certificates.
TD0469	Modification of test activity for FCS_TLSS_EXT.1.1 test 4.1	No	The ST does not claim FCS_TLSS_EXT.1.
TD0442	Updated TLS Ciphersuites for TLS Package	Yes	

3 Security Problem Definition

The following sections describe security problem definition as stated in [PP_APP_V1.4].

3.1 Threat Environment

3.1.1 Threats countered by the TOE

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.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.PHYSICAL_ACCESS
An attacker may try to access sensitive data at rest.

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_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.

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.

3.3 Organizational Security Policies

[PP_APP_V1.4] and [PKG_TLS_V1.1] define no Organizational Security Policies (OSPs).

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.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_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.

O.PROTECTED_STORAGE

TTo 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.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.

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_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.

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.

4.3 Security Objectives Rationale

The security objectives rationale is defined in the [PP_APP_V1.4] protection profile.

5 Extended Components Definition

This Security Target claims exact conformance to [PP_APP_V1.4] and [PKG_TLS_V1.1]; therefore, it does not extend the security requirements defined by these documents.

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**.

Table 5: SFRs for the TOE

Security functional class	Security functional requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
FCS - Cryptographic support	FCS_CKM_EXT.1 Cryptographic Key Generation Services	PP_APP_V1.4	No	No	No	Yes
	FCS_CKM.1/AK Cryptographic Asymmetric Key Generation	PP_APP_V1.4	No	No	No	Yes
	FCS_CKM.2 Cryptographic Key Establishment	PP_APP_V1.4	No	No	No	Yes
	FCS_COP.1/SKC Cryptographic Operation - Encryption/Decryption	PP_APP_V1.4	No	No	No	Yes
	FCS_COP.1/HASH Cryptographic Operation - Hashing	PP_APP_V1.4	No	No	No	Yes
	FCS_COP.1/SIG Cryptographic Operation - Signing	PP_APP_V1.4	No	No	No	Yes
	FCS_COP.1/KEYEDHASH Cryptographic Operation - Keyed-Hash Message Authentication	PP_APP_V1.4	No	No	Yes	Yes
	FCS_RBG_EXT.1 Random Bit Generation Services	PP_APP_V1.4	No	No	No	Yes
	FCS_RBG_EXT.2 Random Bit Generation from Application	PP_APP_V1.4	No	No	No	Yes
	FCS_STO_EXT.1 Storage of Credentials	PP_APP_V1.4	No	No	Yes	Yes
	FCS_HTTPS_EXT.1/CLIENT HTTPS Protocol	PP_APP_V1.4	No	No	No	Yes
	FCS_TLS_EXT.1 TLS Protocol	PKG_TLS_V1.1	No	No	No	Yes
	FCS_TLSC_EXT.1 TLS Client Protocol	PKG_TLS_V1.1	No	No	No	Yes
	FCS_TLSC_EXT.5 TLS Client Support for Supported Groups Extension	PKG_TLS_V1.1	No	No	No	Yes
FDP - User data protection	FDP_DEC_EXT.1 Access to Platform Resources	PP_APP_V1.4	No	No	Yes	Yes
	FDP_NET_EXT.1 Network Communications	PP_APP_V1.4	No	No	Yes	Yes
	FDP_DAR_EXT.1 Encryption Of Sensitive Application Data	PP_APP_V1.4	No	No	No	Yes

Security functional class	Security functional requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
FIA - Identification and authentication	FIA_X509_EXT.1 X.509 Certificate Validation	PP_APP_V1.4	No	No	No	Yes
	FIA_X509_EXT.2 X.509 Certificate Authentication	PP_APP_V1.4	No	No	No	Yes
FMT - Security management	FMT_MEC_EXT.1 Supported Configuration Mechanism	PP_APP_V1.4	No	No	No	Yes
	FMT_CFG_EXT.1 Secure by Default Configuration	PP_APP_V1.4	No	No	No	No
	FMT_SMF.1 Specification of Management Functions	PP_APP_V1.4	No	No	No	Yes
FPR - Privacy	FPR_ANO_EXT.1 User Consent for Transmission of Personally Identifiable Information	PP_APP_V1.4	No	No	No	Yes
FPT - Protection of the TSF	FPT_API_EXT.1 Use of Supported Services and APIs	PP_APP_V1.4	No	No	No	No
	FPT_AEX_EXT.1 Anti-Exploitation Capabilities	PP_APP_V1.4	No	No	Yes	Yes
	FPT_TUD_EXT.1 Integrity for Installation and Update	PP_APP_V1.4	No	No	No	Yes
	FPT_TUD_EXT.2 Integrity for Installation and Update	PP_APP_V1.4	No	No	No	Yes
	FPT_IDV_EXT.1 Software Identification and Versions	PP_APP_V1.4	No	No	Yes	Yes
	FPT_LIB_EXT.1 Use of Third Party Libraries	PP_APP_V1.4	No	No	Yes	No
FTP - Trusted path/channels	FTP_DIT_EXT.1 Protection of Data in Transit	PP_APP_V1.4	No	No	Yes	Yes

6.1.1 Cryptographic support (FCS)

6.1.1.1 FCS_CKM_EXT.1 Cryptographic Key Generation Services

Origin: PP_APP_V1.4

FCS_CKM_EXT.1.1 The application shall

- **invoke platform-provided functionality for asymmetric key generation**
- **implement asymmetric key generation**

.

TD Note:: *TD0717 has been applied to this SFR.*

6.1.1.2 FCS_CKM.1/AK Cryptographic Asymmetric Key Generation

Origin: PP_APP_V1.4

FCS_CKM.1.1/AK 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 186-5, "Digital Signature Standard (DSS)", Appendix B.3**
- **[ECC schemes] using [“NIST curves” P-384 and P-256] that meet the following: [FIPS PUB 186-5, “Digital Signature Standard (DSS)”, Appendix B.4]**

.

Application Note: *RSA key generation is implemented by the TOE to generate certificate signing requests (CSR). ECC key generation is implemented by both the TOE and TOE platform for ephemeral keys for TLS protocol establishment.*

TD Note:: *TD0860 has been applied to this SFR; however, the platform-provided cryptographic algorithms (i.e. Windows CNG cryptographic library) have not been tested against* [FIPS186-5] *but* [FIPS186-4].

6.1.1.3 FCS_CKM.2 Cryptographic Key Establishment

Origin: PP_APP_V1.4

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 by both the TOE and TOE platform for TLS protocol establishment.*

6.1.1.4 FCS_COP.1/SKC Cryptographic Operation - Encryption/Decryption

Origin: PP_APP_V1.4

FCS_COP.1.1/SKC 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 provided by the TOE's OpenSSL. AES-GCM with 128-bit keys, which is provided by both the TOE and the TOE platform, is required for the TLS cipher suites.

6.1.1.5 FCS_COP.1/HASH Cryptographic Operation - Hashing

Origin: PP_APP_V1.4

FCS_COP.1.1/HASH The application shall perform [cryptographic hashing services] in accordance with a specified cryptographic algorithm

- **SHA-256**

and message digest sizes

- **256**

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

Application Note:

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

6.1.1.6 FCS_COP.1/SIG Cryptographic Operation - Signing

Origin: PP_APP_V1.4

FCS_COP.1.1/SIG 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 186-5, “Digital Signature Standard (DSS)”, Section 5]**

.

Application Note:

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

TD Note:: *TD0860 has been applied to this SFR; however, the platform-provided cryptographic algorithms (i.e. Windows CNG cryptographic library) have not been tested against* [FIPS186-5] *but* [FIPS186-4].

6.1.1.7 FCS_COP.1/KEYEDHASH Cryptographic Operation - Keyed-Hash Message Authentication

Origin: PP_APP_V1.4

FCS_COP.1.1/KEYEDHASH The application shall perform [keyed-hash message authentication] in accordance with a specified cryptographic algorithm

- **HMAC-SHA-256**

and

- **no other algorithms**

with key sizes **256 bits** and message digest sizes **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 by both the TOE and TOE platform to support TLS communications.

6.1.1.8 FCS_RBG_EXT.1 Random Bit Generation Services

Origin: PP_APP_V1.4

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 TLS communications.

6.1.1.9 FCS_RBG_EXT.2 Random Bit Generation from Application

Origin: PP_APP_V1.4

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

- **384 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 FCS_STO_EXT.1 Storage of Credentials

Origin: PP_APP_V1.4

FCS_STO_EXT.1.1 The application shall

- **invoke the functionality provided by the platform to securely store**
  - **CA certificates;**
  - **Proxy server credentials;**

to non-volatile memory.

6.1.1.11 FCS_HTTPS_EXT.1/CLIENT HTTPS Protocol

Origin: PP_APP_V1.4

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 Functional Package for TLS.

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

6.1.1.12 FCS_TLS_EXT.1 TLS Protocol

Origin: PKG_TLS_V1.1

FCS_TLS_EXT.1.1 The product shall implement

- **TLS as a client**

.

6.1.1.13 FCS_TLSC_EXT.1 TLS Client Protocol

Origin: PKG_TLS_V1.1

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**

.

TD Note:: *TD0442 has been applied to this SFR.*

6.1.1.14 FCS_TLSC_EXT.5 TLS Client Support for Supported Groups Extension

Origin: PKG_TLS_V1.1

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 FDP_DEC_EXT.1 Access to Platform Resources

Origin: PP_APP_V1.4

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 **the Windows Credential Store** , **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\3.000.800**

.

6.1.2.2 FDP_NET_EXT.1 Network Communications

Origin: PP_APP_V1.4

FDP_NET_EXT.1.1 The application shall restrict network communication to

- **the following application-initiated network communication:**
  - **IBM MaaS360 Cloud,**
  - **Microsoft NDES CA,**
  - **Entrust CA,**
  - **Active Directory or LDAP server,**
  - **Microsoft Exchange**

.

6.1.2.3 FDP_DAR_EXT.1 Encryption Of Sensitive Application Data

Origin: PP_APP_V1.4

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 FIA_X509_EXT.1 X.509 Certificate Validation

Origin: PP_APP_V1.4

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

- RFC 5280 certificate validation and certificate path validation.
- The certificate path must terminate with a trusted CA certificate.
- The application shall validate a certificate path by ensuring the presence of the basicConstraints extension and that the CA flag is set to TRUE for all CA certificates, and that any path constraints are met.
- The application shall validate that any CA certificate includes caSigning purpose in the key usage field
- The application shall validate the revocation status of the certificate using **CRL as specified in RFC 8603**.
- The application shall validate the extendedKeyUsage field according to the following rules:
  a) The application shall validate the extendedKeyUsage (EKU) field according to the following rules:
     - 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.
     - 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.
     - 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.
     - 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.
     - OCSP certificates presented for OCSP responses shall have the OCSP Signing purpose (id-kp 9 with OID 1.3.6.1.5.5.7.3.9) in the EKU field.
     - 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:

Although all rules above are implemented, only the first and second rules are applicable for the TOE when performing certificate validation for trusted updates and TLS server certificates.

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 FIA_X509_EXT.2 X.509 Certificate Authentication

Origin: PP_APP_V1.4

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 FMT_MEC_EXT.1 Supported Configuration Mechanism

Origin: PP_APP_V1.4

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 FMT_CFG_EXT.1 Secure by Default Configuration

Origin: PP_APP_V1.4

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 FMT_SMF.1 Specification of Management Functions

Origin: PP_APP_V1.4

FMT_SMF.1.1 The TSF shall be capable of performing the following management functions **no management functions**.

6.1.5 Privacy (FPR)

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

Origin: PP_APP_V1.4

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 FPT_API_EXT.1 Use of Supported Services and APIs

Origin: PP_APP_V1.4

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

6.1.6.2 FPT_AEX_EXT.1 Anti-Exploitation Capabilities

Origin: PP_APP_V1.4

FPT_AEX_EXT.1.1 The application shall not request to map memory at an explicit address except for **IBM MaaS360 Cloud Extender (OpenSSL) 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 FPT_TUD_EXT.1 Integrity for Installation and Update

Origin: PP_APP_V1.4

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 **provide the ability** 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 FPT_TUD_EXT.2 Integrity for Installation and Update

Origin: PP_APP_V1.4

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.

TD Note:: *TD0628 has been applied to this SFR.*

6.1.6.5 FPT_IDV_EXT.1 Software Identification and Versions

Origin: PP_APP_V1.4

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

6.1.6.6 FPT_LIB_EXT.1 Use of Third Party Libraries

Origin: PP_APP_V1.4

FPT_LIB_EXT.1.1 The application shall be packaged with only **the third-party libraries provided in Table** 6.

Table 6: Third-party Libraries

Library	Version
Apache log4net for .NET Framework 4.5	2.0.16
bitlib	26
Boost	1.88
Eclipse Paho C Library	1.3.8
Eclipse Paho C++ Library	1.3.1
Gloox	1.0.4
Google Protocol Buffers	2.4.1.521
libcurl	8.13.0
libest	r3.2.0
Lua	5.1.4
Lua cURL	0.2.2
LuaSql	2.1.1
lua-winreg	v1.0.0
Microsoft C Runtime Library	14.28.29918.0
Microsoft Concurrency Runtime Library	14.28.29918.0
Microsoft Visual C++ Redistributable	14.28.29918.0
OpenSSL	1.0.2zh

OpenSSL FIPS Module	2.0.16
SharpZipLib	1.3.3
SQLite	3.35.5
Zlibc	1.3.1

6.1.7 Trusted path/channels (FTP)

6.1.7.1 FTP_DIT_EXT.1 Protection of Data in Transit

Origin: PP_APP_V1.4

FTP_DIT_EXT.1.1 The application shall

- **encrypt all transmitted data with HTTPS as a client in accordance with FCS_HTTPS_EXT.1/Client for exchanging data with the IBM MaaS360 Cloud, exchanging data with the NDES/CA Certificate Server, TLS as a client as defined in the Functional Package for TLS for exchanging data with the IBM MaaS360 Cloud, exchanging data with the NDES/CA Certificate Server**
- **invoke platform-provided functionality to encrypt all transmitted data with HTTPS, TLS for connecting to Microsoft Exchange/ ActiveSync using HTTPS, connecting to Active Directory or LDAP server using LDAP over TLS, connecting to the Entrust Certificate Server using HTTPS**

between itself and another trusted IT product.

TD Note:: *TD0743 has been applied to this SFR.*

6.2 Security Functional Requirements Rationale

The SFR rationale is defined in the [PP_APP_V1.4] protection profile.

6.3 Security Assurance Requirements

The security assurance requirements (SARs) for the TOE are defined in the PP_APP_V1.4 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.).

Table 7: SARs

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
ADV Development	ADV_FSP.1 Basic functional specification	PP_APP_V1.4	No	No	No	No
AGD Guidance documents	AGD_OPE.1 Operational user guidance	PP_APP_V1.4	No	No	No	No
	AGD_PRE.1 Preparative procedures	PP_APP_V1.4	No	No	No	No

Security assurance class	Security assurance requirement	Source	Operations			
			Iter.	Ref.	Ass.	Sel.
ALC Life-cycle support	ALC_CMC.1 Labelling of the TOE	PP_APP_V1.4	No	No	No	No
	ALC_CMS.1 TOE CM coverage	PP_APP_V1.4	No	No	No	No
	ALC_TSU_EXT.1	PP_APP_V1.4	No	No	No	No
ATE Tests	ATE_IND.1 Independent testing - conformance	PP_APP_V1.4	No	No	No	No
AVA Vulnerability assessment	AVA_VAN.1 Vulnerability survey	PP_APP_V1.4	No	No	No	No
ASE Security Target evaluation	ASE_CCL.1 Conformance claims	PP_APP_V1.4	No	No	No	No
	ASE_ECD.1 Extended components definition	PP_APP_V1.4	No	No	No	No
	ASE_INT.1 ST introduction	PP_APP_V1.4	No	No	No	No
	ASE_OBJ.1 Security objectives for the operational environment	PP_APP_V1.4	No	No	No	No
	ASE_REQ.1 Stated security requirements	PP_APP_V1.4	No	No	No	No
	ASE_SPD.1 Security problem definition	PP_APP_V1.4	No	No	No	No
	ASE_TSS.1 TOE summary specification	PP_APP_V1.4	No	No	No	No

6.4 Security Assurance Requirements Rationale

The SAR rationale is defined in the [PP_APP_V1.4] protection profile.

7 TOE Summary Specification

7.1 TOE Security Functionality

As per [PP_APP_V1.4] and [PKG_TLS_V1.1], 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 comes with the OpenSSL cryptographic module which provides the necessary cryptographic algorithms to implement certificate signing requests (CSR) and supports secure communication with TLS. The TOE also invokes platform-provided crypto services implemented in the Windows Cryptographic API Next Generation (CNG) library for secure communication with TLS.

The table below lists all cryptographic services, including the algorithms, supported key sizes, applicable standard, purpose. The table also indicates whether the algorithm is implemented by the TOE, by the underlying TOE platform, or both. The last two columns provide the certificates obtained from the Cryptographic Algorithm Validation Program (CAVP) in the evaluated configuration for each of the cryptographic algorithms; grayed cells indicate that the algorithm is not implemented.

Table 8: Cryptographic algorithms

Cryptographic Service	Algorithm	Key sizes	Standard	Purpose	CAVP Certs.	
					TOE	Platform Provided
FCS_CKM.1/AK - Asymmetric Key Generation	RSA	2048, 3072, 4096 bits	[FIPS186-5]	Certificate signing request	A5499	
	Elliptic Curve Cryptography (ECC)	P-256, P-384	[FIPS186-4]	Ephemeral asymmetric key generation for TLS key exchange		C211 C348
			[FIPS186-5]		A5499	
FCS_CKM.2 - Key Establishment	Elliptic Curve	P-256, P-384	[SP800-56A-Rev3]	TLS key exchange	A5499	C211
FCS_COP.1/SKC - Data Encryption and Decryption	AES in CBC mode	256 bits	[SP800-38A]	DRBG	A5499	C211
	AES in GCM mode	128 bits	[SP800-38D]	Authenticated encryption	A5499	C211
FCS_COP.1/Hash - Message Digest	SHA-256	N/A	[FIPS180-4]	Hash function in Pseudorandom function (PRF) for the TLS protocol	A5499	C211

Cryptographic Service	Algorithm	Key sizes	Standard	Purpose	CAVP Certs.	
					TOE	Platform Provided
				Hash function in RSA Digital Signature Generation and Verification Hash function in Message Authentication		
FCS_COP.1/Sig - Digital Signature Generation and Verification	RSA	2048, 3072 bits	[FIPS186-4]	TLS server authentication		C211 C348
		2048, 3072, 4096 bits	[FIPS186-5]		A5499	
FCS_COP.1/ KeyedHash - Message Authentication	HMAC-SHA-256	256 bits	[FIPS198-1]	Pseudorandom function (PRF)	A5499	C211
FCS_RBG_EXT.2 - Random Number Generator	CTR_DRBG	256 bits	[SP800-90A-Rev1]	TLS key exchange	A5499	

Related SFRs:

- FCS_CKM_EXT.1
- FCS_CKM.2
- FCS_COP.1/SKC
- FCS_COP.1/HASH
- FCS_COP.1/SIG
- FCS_COP.1/KEYEDHASH
- 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 OpenSSL, which provides an implementation of the CTR_DRBG (AES). The TOE invokes this DRBG by default, and there is no ability to specify the use of an alternative DRBG.

The TOE obtains entropy from the TOE 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 sufficient to ensure a security strength of 256 bits.

Detailed description of the entropy source is provided in the proprietary Entropy Assessment Report.

Related SFRs:

- FCS_RBG_EXT.1
- FCS_RBG_EXT.2

7.1.1.3 Storage of credentials

The TOE relies on the TOE platform for securely storing credentials. The following table lists the credentials necessary for the operation of the TOE, where they are stored and protected.

Table 9: Credential List

Credential	Storage	Protection
CA certificates	Windows Certificate Store	Windows Certificate Store
Proxy server credentials	Stored encrypted in Windows registry under Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Fiberlink\V360\FibAuthInfo	DPAPI

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 IBM MaaS360 Cloud, and to Certificate Enrollment servers using the Simple Certificate Enrollment Protocol (SCEP). The HTTPS protocol is provided by the cURL library while the TLS protocol is provided by the OpenSSL.

The TOE also invokes the TOE platform (via Powershell and .NET API classes) to establish HTTPS connections with the rest of the endpoints: Microsoft Exchange Server, Active Directory or LDAP Server, and Entrust Certificate Server. For TLS protocol support, the TOE platform provides the Microsoft Secure Channel (Schannel) Security Service Provider (SSP), which uses the Windows CNG library for cryptographic algorithms.

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 its peer X.509 certificate used for TLS connection with the endpoint.

When negotiating 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 required.

The TOE also verifies during the TLS handshake that the identifying information in the TLS server certificate matches the expected information. 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 reference identifiers are verified against the identity of the endpoint’s DNS entry to ensure that it matches. The use of Internet Protocol (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 via 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 TOE utilizes TOE platform-provided functionality to encrypt sensitive data in non-volatile memory. In particular, it uses the Windows Encrypting File System (EFS) to store sensitive data. Users are instructed to ensure that EFS is enabled for the folders specified in FDP_DAR_EXT.1.

The following table shows how sensitive information is stored and protected.

Table 10: Storage of Sensitive data

Sensitive Data	Storage	Protection
Configuration Information	Stored as encrypted files in C:\ProgramData\MaaS360\Cloud Extender directory.	EFS
Log Information	Stored as encrypted files in C:\ProgramData\MaaS360\Cloud Extender\logs directory.	EFS
Authentication data for Microsoft SCEP	Stored in encrypted file C:\ProgramData\MaaS360\Cloud Extender \Data\EMSAgent.db	EFS
Authentication data for Active Directory		
Authentication data for LDAP server		
Authentication data for Microsoft Exchange		

Related SFRs:

- FDP_DAR_EXT.1

7.1.2.2 Access to Platform Resources

With the exception of network connectivity, the TOE 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)

The TOE leverages the TOE platform to restrict accss to the directories and files specified in FDP_DEC_EXT.1.2. The TOE platform provides discretionary access controls.

Related SFRs:

- FDP_DEC_EXT.1

7.1.2.3 Network Communications

Network communications are established between the TOE and the customer's internal services as illustrated in Figure 3.

The TOE acts as a bridge between the customer's servers and the SaaS-based cloud portal. The customer will configure which servers to 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.

Table 11: TOE Connections to Customer's Services

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	

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

Table 12: TOE Connections to the IBM MaaS360 Cloud

Network Communication Type	Information	Example Port
IBM MaaS360 Cloud	maas-central.maas360.com	443
	maas-central-##.maas360.com (where ## is an instance number)	443
M1 (portal.fiberlink.com)	services.fiberlink.com	443
	mpns.maas360.com	443
	https://license.fiberlink.com/internettest	443
	upload.fiberlink.com	443
	dl.maas360.com (no IP range)	-
M2 (m2.maas360.com)	services.m2.maas360.com	443
	mpns.m2.maas360.com	443
	https://license.fiberlink.com/internettest	443
	upload.fiberlink.com	443

Network Communication Type	Information	Example Port
	dl.m2.maas360.com (no IP range)	-
M3 (m3.maas360.com)	services.m3.maas360.com	443
	mpns.m3.maas360.com	443
	https://license.fiberlink.com/internettest 208.76.128.58 208.76.130.58	443
	upload.fiberlink.com	443
	dl.m3.maas360.com (no IP range)	-
M4 (m4.maas360.com)	services.m4.maas360.com	443
	mpns.m4.maas360.com	443
	https://license.fiberlink.com/internettest	443
	upload.fiberlink.com	443
	dl.m4.maas360.com (no IP range)	-
M5 (m5.maas360.com)	services.m5.maas360.com	443
	mpns.m5.maas360.com	443
	https://license.fiberlink.com/internettest	443
	upload.fiberlink.com	443
	dl.m5.maas360.com (no IP range)	-

Related SFRs:

- FDP_NET_EXT.1

7.1.3 Identification and Authentication

7.1.3.1 X.509 Certificate Validation

TOE connects securely to the external entities (Microsoft SCEP, Entrust Server, Active Directory/LDAP, Exchange/ActiveSync, MaaS360 cloud) by establishing a secure channel using the TLS protocol. When the TOE starts a TLS connection as a client, it obtains the certificate from the TLS server during the handshake. As part of the final steps of the TLS handshake process, the TOE verifies the identity of the server by validating the X.509 certificate.

X.509 certificate validation is implemented in the TOE by OpenSSL and in the provided-platform by the Microsoft Secure Channel (SChannel) Security Service Provider.

The TOE performs X.509 certificate validation as follows:

- Certificate validation and certificate path validation conforming 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 a revoked certificate. The TOE uses the certificate revocation list (CRL) referenced by the TOE to check the revocation status. The CRL conforms to RFC 8603.

- The CA certificate must include caSigning purpose in the key usage field.
- The certificate presented by the TLS server must have the Server Authentication purpose 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 TOE does not support the use of IP addresses.

The certificates the TOE uses for certificate path validation can be specified through the use of the Windows Credential Store for the TOE platform-provided TLS. The TOE's OpenSSL implementation uses its own certifiate bundle, and does not support adding or configurating additional TLS certificates. The TOE administrators may also specify the path to a certificate revocation list so that revocation status can be checked during authentication.

The TOE will automatically reject a certificate if it is found to be invalid. The TOE also rejects a certificate with unknown revocation status (due to the TOE unable to read or obtain the CRL). In this case, an error message is generated and logged for TOE administrator.

If the validation of the server certificate fails, the TOE closes the connection and the communication with the external entity is not established. The TOE does not provide a means for defining an alternative action in case of the certificate validation failure.

Related SFRs:

- FIA_X509_EXT.1
- FIA_X509_EXT.2

7.1.4 Security Management

7.1.4.1 Secure By Default Configuration

The TOE does not require any credentials to access it. A license key must be obtained from IBM in order to install the TOE on the TOE platform.

An installation of the TOE will include the following default credentials:

- 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 IBM MaaS360 Cloud

Related SFRs:

- FMT_CFG_EXT.1

7.1.4.2 Supported Configuration Mechanism

The IBM MaaS360 Cloud Extender Configuration Tool is supplied with the TOE installation package. Configuration data for the TOE is stored in the TOE platform's Windows Registry and may optionally be exported to an encrypted file stored in an EFS-protected folder on the TOE Windows platform. The following table outlines the settings relevant to the TSF:

Table 13: TOE Configuration Options

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		✓

Additionally, the TOE relies on TOE platform-provided access control mechanisms (i.e., user permissions) for protecting access to the TOE components outside of the EFS such as the installation directory where TOE binaries are located.

No other TOE management functions are applicable to the TOE.

Related SFRs:

- FMT_MEC_EXT.1
- FMT_SMF.1

7.1.5 Privacy

7.1.5.1 User Consent for Transmission of PII

The TOE does not specifically request 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 enablement option modifies the header of an executable to indicate that the TOE is to be randomly rebased at load time. Additional information about 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 Dynamic Linked Libraries (DLLs) are compiled with this option.

The TOE build 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) support Federal Information Processing Standard (FIPS) 140-2 conformance, which is provided through the TOE's OpenSSL. However, please note that this particular TOE's OpenSSL module is not FIPS 140-2 or FIPS 140-3 validated. Both components statically link the OpenSSL library. OpenSSL requires the statically linked libraries to 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 140-2 link step. IBM uses the following addresses:

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

Additionally, all executable files are located in the TOE's installation directory. All user-modifiable files are written to a separate location within the EFS volume described in the [CC-CFG].

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.

Table 14: Windows APIs used by the TOE

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 • Start-Sleep • Import-PSSession • Get-Content • get-childitem

API Category	Windows APIs
	• 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 • Connect-ExchangeOnline • Disconnect-ExchangeOnline • Get-ConnectionInformation • Get-InstalledModule
Active Directory	• System.DirectoryServices.ActiveDirectory.Forest.GetCurrentForest • System.DirectoryServices.DirectoryEntry.Properties • System.DirectoryServices.DirectorySearcher.FindAll • System.DirectoryServices.DirectorySearcher.PropertiesToLoad.Add • System.DirectoryServices.ActiveDirectory.Forest.GetCurrentForest().GetAllTrustRelationships

API Category	Windows APIs
	• System.DirectoryServices.ActiveDirectory.Domain.GetDomain
LDAP	• System.DirectoryServices.Protocols.SearchRequest • DirectoryAttributeModification • ModifyRequest • LdapConnection • VerifyServerCertificateCallback • DirectoryAttribute • PageResultRequestControl • SearchRequest
Windows Registry	• RegOpenCurrentUser • RegCreateKey • RegOpenKey • RegCloseKey • RegDeleteKey • RegDeleteValue • RegQueryInfoKey • RegQueryValue • RegSetValue • RegEnumValue • RegEnumKey
Windows Management Instrumentation (WMI)	• ExecQuery • GetObjectText • ExecMethod • Get • SpawnInstance • ConnectServer • CreateObjectStub • ExecNotificationQueryAsync • CancelAsyncCall • GetObjectW
Process	• CreateProcess • GetProcAddress • GetExitCodeProcess • CloseHandle • AdjustTokenPrivileges • LookupPrivilegeValue • OpenProcessToken • OpenProcess • OpenThreadToken • CreateToolhelp32Snapshot • Process32First • Process32Next • TerminateProcess

API Category	Windows APIs
	• WaitForMultipleObjects • WaitForSingleObject • CreateMutex • OpenMutex • Sleep • ReleaseMutex • ReleaseSemaphore • CreateSemaphore • OpenSemaphore • GetProcAddress • CreateEvent • ResetEvent • GetCurrentProcess • GetProcessIoCounters • GetProcessMemoryInfo • SetThreadPriority • SetEvent • GetCurrentThreadId • RegisterEventSource • ReportEvent • DeregisterEventSource • Source PeekMessage • TranslateMessage • DispatchMessage • EnterCriticalSection • LeaveCriticalSection • IsWow64Process • CoCreateInstance
FileSystem	• FindFirstFile • FindNextFile • FindClose • CreateFile • CopyFile • GetFileSize • ReadFile • WriteFile • MoveFileExW • DeleteFile • CreateDirectory • SetCurrentDirectoryW • GetFileVersionInfoW • GetFileTime • GetVolumeInformationW • GetDiskFreeSpaceExW

API Category	Windows APIs
	• GetLogicalDriveStringsA • SHGetFolderPathW • FindFirstVolumeW • FindNextVolumeW • FindVolumeClose • GetVolumePathNamesForVolumeNameW • Fseek • Ftell • Fread • Fclose • _wfopen • fwrite • Fflush • SHGetFolderPath • _wsplitpath • fstream • Tellg • __CLR_OR_THIS_CALL fail • FindFirstFile • FindNextFile • FindClose • ReadDirectoryChangesW • CreateFileA • GetFileTime • FileTimeToSystemTime • GetSystemTime • RemoveDirectoryW • SetFileAttributesW • GetFileVersionInfoSizeW • GetVolumeInformationW • GetSystemDirectoryW
Windows OS HTTP (Networking)	• WinHttpSendRequest • WinHttpWriteData • WinHttpReceiveResponse • WinHttpQueryDataAvailable • WinHttpReadData • WinHttpOpen • WinHttpSetTimeouts • WinHttpCrackUrl • WinHttpConnect • WinHttpOpenRequest • WinHttpCloseHandle • WinHttpSetOption • WinHttpSetCredentials

API Category	Windows APIs
	• WinHttpAddRequestHeaders • WinHttpQueryHeaders • WinHttpQueryAuthSchemes • WSACloseEvent • WSAGetLastError • WSACreateEvent • NotifyAddrChange • CoSetProxyBlanket • WinHttpGetIEProxyConfigForCurrentUser • InternetQueryOptionW • WinHttpCrackUrl • InternetCrackUrlA • WinHttpOpen • WinHttpGetProxyForUrl • WinHttpDetectAutoProxyConfigUrl • WlanQueryInterface • WlanCloseHandle • WlanOpenHandle • WlanFreeMemory • WlanGetProfile • GetAdaptersAddresses
Windows Service	• OpenSCManagerW • OpenServiceW • QueryServiceStatus • CloseServiceHandle • StartServiceW • ControlService • QueryServiceConfigW • DeleteService • EnumServicesStatusW
Windows Certificate Store	• CertAddCertificateContextToStore • CertCloseStore • CertComparePublicKeyInfo • CertEnumCertificatesInStore • CertEnumCRLsInStore • CertFindCertificateInStore • CertNameToStr • CertOpenStore • CertOpenSystemStore • CertSetCertificateContextProperty • PFXExportCertStore
Windows CryptoAPI	• CryptAcquireContext • CryptBinaryToString

API Category	Windows APIs
	• CryptCreateHash • CryptDecryptMessage • CryptDeriveKey • CryptEncrypt • CryptDestroyHash • CryptDestroyKey • CryptEncrypt • CryptExportPublicKeyInfo • CryptGetUserKey • CryptHashData • CryptImportKey • CryptMsgOpenToDecode • CryptMsgUpdate • CryptMsgGetParam • CryptReleaseContext • CryptGenRandom • BCryptGenRandom
COM	• CoCreateInstance • CoSetProxyBlanket • SysFreeString • CoGetClassObject • CreateInstanceLic
String Manupilation	• find • substr • tolower • wcslen • strncpy • wcscpy • wcscat • wcstok • wcscmp • vfprintf • strftime • strlen • strcpy • sscanf • _tprintf • strcpy_s
Memory Management	• free • malloc • memset • memcpy • realloc

API Category	Windows APIs
	• ZeroMemory • calloc • CopyMemory
Data Conversion	• strtoul • _wtoi • _ultow • WINBASEAPI int WINAPI WideCharToMultiByteMultiByteToWideChar • WINBASEAPI int WINAPI WideCharToMultiByte • _itow
Localization	• WINBASEAPI LCID WINAPI GetThreadLocale • WINBASEAPI BOOL WINAPI IsValidLocale • WINBASEAPI BOOL WINAPI SetThreadLocale
SOAP http	System.Web.Services.Protocols.SoapHttpClientProtocol methods • Invoke • BeginInvoke • EndInvoke • InvokeAsync
C# (Used by Certificate Integration Module)	• System.Threading.Mutex.OpenExisting • System.Net.Http.HttpResponseMessage • System.Net.Http.HttpRequestMessage • System.Net.Http.HttpClient.SendAsync • System.Net.WebProxy • System.Text.Encoding.UTF8.GetString • System.Convert.FromBase64String • System.Security.Cryptography.SHA256.ComputeHash • System.Security.Cryptography.MD5.ComputeHash • System.Security.Cryptography.SHA1CryptoServiceProvider.ComputeHash • System.BitConverter.ToString

The TOE installation package is signed by IBM using a IBM-issued Symantec certificate. Instructions for viewing the certificate are found in the [CC-CFG]. The TOE is not subject to updates.

The TOE version is displayed via the Configuration Tool window.

Related SFRs:

- FPT_API_EXT.1

7.1.6.3 TOE Identification

The TOE is identified by using file properties of the emsagent.exe program. The TOE name (i.e. "IBM MaaS360 Cloud Extender") is assigned to the Product Name property; the TOE version (i.e. 3.000.800.038) is assigned to the Product Version property. The TOE version follows the following convention: `majorVersion.minorVersion`; the first three period-separated numbers correspond to the major version, the last number to the minor version.

The administrator can see the TOE name and version by using the IBM MaaS360 Cloud Extender Configuration Tool.

Related SFRs:

- FPT_IDV_EXT.1

7.1.6.4 Timely Security Updates

7.1.6.4.1 TOE installation

The TOE can be installed following the instructions from the administrative guidance documentation ([CC-CFG].

The TOE can be obtained by following the downloading instructions provided by IBM when the product is purchased and a license is obtained.

7.1.6.4.2 Security Update Process for the TOE

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 Configuration Tool . If an update is available, the new installer must be obtained from the IBM MaaS portal, which requires an IBM user account.

Automatic updates are disabled in the evaluated configuration and therefore 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 TOE platform including all log and configuration data.

Related SFRs:

- FPT_TUD_EXT.1
- FPT_TUD_EXT.2

7.1.6.4.3 Process for handling security vulnerabilities

The IBM Product Security Incident Response Team (PSIRT) process is described at: https://www.ibm.com/support/pages/ibm-security-vulnerability-management.

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 Common Vulnerability Scoring System (CVSS) scoring.
3. Development teams investigate and remediate the issue.
4. A fix is tested and validated in Quality Assurance (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 Cloud Extender 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 requests 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.

7.1.6.4.4 Notification of updates and security related fixes

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

1 The TOE 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 [CC-CFG].

2 All release communication is found on the IBM Support page: https://www.ibm.com/docs/sk/maas360?topic=notes-cloud-extender-release.

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.ibm.com/support/pages/ibm-security-vulnerability-management

7.1.7 Trusted path/channels

The TOE protects data in transit by enforcing all network communication (specified 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 14.

- 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

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

MQTT
Message Queuing Telemetry Transport

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

8.2 References

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 1.1
Date 2025-08-12
Location https://public.dhe.ibm.com/software/security/products/maas360/CE/IBM_MaaS360_v3.000.800_CE_CommonCriteria_Guide_v1.1.pdf

FIPS180-4 **Secure Hash Standard (SHS)**
Date 2015-08-04
Location https://csrc.nist.gov/pubs/fips/180-4/upd1/final

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

FIPS186-5 **Digital Signature Standard (DSS)**
Date 2023-02-03
Location https://csrc.nist.gov/pubs/fips/186-5/final

FIPS198-1 **The Keyed-Hash Message Authentication Code (HMAC)**
Date 2008-07-16
Location https://csrc.nist.gov/pubs/fips/198-1/final

PKG_TLS_V1.1 **Functional Package for TLS Version 1.1**
Version 1.1
Date 2019-03-01
Location https://www.niap-ccevs.org/protectionprofiles/439

PP_APP_V1.4 **Protection Profile for Application Software Version 1.4**
Version 1.4
Date 2021-10-07
Location https://www.niap-ccevs.org/protectionprofiles/462

RFC2818 **HTTP Over TLS**
Author(s) E. Rescorla
Date 2000--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--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--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/pubs/sp/800/38/a/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/pubs/sp/800/38/d/final
SP800-56A-Rev3	**Recommendation for Pair-Wise Key-Establishment Schemes Using Discrete Logarithm Cryptography** Date 2018-04-16 Location https://csrc.nist.gov/pubs/sp/800/56/a/r3/final
SP800-90A-Rev1	**Recommendation for Random Number Generation Using Deterministic Random Bit Generators** Date 2015-06-24 Location https://csrc.nist.gov/pubs/sp/800/90/a/r1/final