Acronis SCS

Acronis SCS Cyber Backup 12.5 Hardened Edition Server

v12.5

Security Target

Document Version: 0.14

Prepared for:

Acronis SCS

Acronis SCS
1225 W. Washington St., Suite 250
Tempe, AZ 85288
United States of America

Phone: +1 781 782 9000
www.acronisscs.com

Prepared by:

Corsec

Corsec Security, Inc.
12600 Fair Lakes Drive, Suite 210
Fairfax, VA 22003
United States of America

Phone: +1 703 267 6050
www.corsec.com

Table of Contents

1. Introduction 4
1.1 Purpose 4
1.2 Security Target and TOE References 4
1.3 Product Overview 5
1.3.1 Product Components 5
1.4 TOE Overview 6
1.4.1 TOE Environment 7
1.5 TOE Description 8
1.5.1 Physical Scope 8
1.5.2 Logical Scope 8
1.5.3 Product Features and Functionality not included in the TOE 10
1.5.4 Scope of Evaluation 10
2. Conformance Claims 11
3. Security Problem Definition 13
3.1 Threats 13
3.2 Assumptions 13
3.3 Organizational Security Policies 13
4. Security Objectives 14
4.1 Security Objectives for the TOE 14
4.2 Security Objectives for the Operational Environment 15
4.3 Security Objectives Rationale 15
5. Extended Components 16
5.1 Extended TOE Security Functional Components 16
5.2 Extended TOE Security Assurance Components 16
6. Security Assurance Requirements 17
7. Security Functional Requirements 18
7.1 Conventions 18
7.2 Security Functional Requirements 18
7.2.1 Class FCS: Cryptographic Support 19
7.2.2 Class FDP: User Data Protection 23
7.2.3 Class FMT: Security Management 23
7.2.4 Class FPR: Privacy 24
7.2.5 Class FPT: Protection of the TSF 24
7.2.6 Class FTP: Trusted Path/Channel 25
8. TOE Summary Specification 27
8.1 TOE Security Functionality 27
8.1.1 Cryptographic Support 28
8.1.2 User Data Protection 30
8.1.3 Security Management 30
8.1.4 Privacy 31
8.1.5 Protection of the TSF 31
8.1.6 Trusted Path/Channels 32
8.2 Timely Security Updates 32
9. Rationale 34

9.1 Conformance Claims Rationale 34
9.1.1 Variance Between the PP and this ST 34
9.1.2 Security Assurance Requirements Rationale 34
10. Acronyms 35
Appendix A: Supported Platform APIs 37
Appendix B: Included Third-party Libraries 38

List of Figures

Figure 1 – Physical TOE Boundary 8

List of Tables

Table 1 – ST and TOE References 4
Table 2 – Environmental Components 7
Table 3 – Guidance Documentation 8
Table 4 – CC and PP Conformance 11
Table 5 - Relevant Technical Decisions 11
Table 6 – Threats 13
Table 7 – Assumptions 13
Table 8 – Security Objectives for the TOE 14
Table 9 – Security Objectives for the Operational Environment 15
Table 10 – Extended TOE Security Assurance Components 16
Table 11 – Security Assurance Requirements 17
Table 12 – TOE Security Functional Requirements 18
Table 13 – Mapping of TOE Security Functionality to Security Functional Requirements 27
Table 14 – Cryptographic Algorithms and Key Sizes 28
Table 15 – Acronyms 35
Table 16 – Included Third-party Libraries 38

1. Introduction

This section identifies the Security Target (ST), Target of Evaluation (TOE), and the organization of the ST. The TOE is the Acronis SCS Cyber Backup 12.5 Hardened Edition Server developed by Acronis SCS and will hereafter be referred to as the TOE or the Management Server throughout this document. The TOE is the Management Server component of the Acronis SCS Backup Server solution, which consists of a Management Server and multiple Backup Agents. The Management Server provides a web UI[1] called the Management Console with customizable dashboards, advanced reporting, and auditing for managing backups.

1.1 Purpose

This ST is divided into 10 sections, as follows:

- Introduction (Section 1) – Provides a brief summary of the ST contents and describes the organization of other sections within this document. It also provides an overview of the TOE security functionality and describes the physical and logical scope for the TOE as well as the ST and TOE references.
- Conformance Claims (Section 2) – Provides the identification of any Common Criteria (CC), Protection Profile (PP), and Evaluation Assurance Level (EAL) package claims. It also identifies whether the ST contains extended security requirements.
- Security Problem (Section 3) – Describes the threats, organizational security policies, and assumptions that pertain to the TOE and its environment.
- Security Objectives (Section 4) – Identifies the security objectives that are satisfied by the TOE and its environment.
- Extended Components (Section 5) – Identifies new components (extended Security Functional Requirements (SFRs) and extended Security Assurance Requirements (SARs)) that are not included in CC Part 2 or CC Part 3.
- Security Assurance Requirements (Section 6) – Presents the SARs met by the TOE.
- Security Functional Requirements (Section 7) – Presents the SFRs met by the TOE.
- TOE Summary Specification (Section 8) – Describes the security functions provided by the TOE that satisfy the SFRs and objectives.
- Rationale (Section 9) – Presents the conformance claims rationale for the selected PP.
- Acronyms (Section 10) – Defines the acronyms used within this ST.

1.2 Security Target and TOE References

Table 1 shows the ST and TOE references.

Table 1 – ST and TOE References

ST Title	*Acronis SCS Cyber Backup 12.5 Hardened Edition Server v12.5 Security Target*
ST Version	Version 0.14
ST Author	Corsec Security, Inc.
ST Publication Date	October 11, 2023

[1] UI – User Interface

TOE Reference	Acronis SCS Cyber Backup 12.5 Hardened Edition Server v12.5

1.3 Product Overview

The Product Overview provides a high-level description of the product that is the subject of the evaluation. The following section, TOE Overview, will provide the introduction to the parts of the overall product offering that are specifically being evaluated.

Acronis SCS Cyber Backup 12.5 Hardened Edition Server (also known as Acronis SCS Backup Server) is an advanced data protection solution that provides reliable backup and recovery of physical, virtual, and cloud workloads with a wide range of storage options. It may be used to protect data residing on-premises, in remote locations, in the cloud, and on mobile devices. Centralized and remote management of backups is performed via the Management Server's web-based Management Console, with customizable dashboards, advanced reporting, and auditing. Backup Agents installed on protected platforms perform data backup and recovery of physical or virtual machines, hypervisors, applications, and mobile devices. Acronis SCS Backup Server supports application-aware backup and recovery features for Oracle database, Microsoft Office 365, Microsoft Exchange, Microsoft SQL[2] Server, Microsoft SharePoint, and Microsoft Active Directory.

Acronis SCS Backup Server may be deployed in an on-premise or cloud configuration. With the on-premise configuration, the Management Server is installed on a customer's local network. With the cloud configuration, it is installed in a secure Acronis Data Center.

Acronis SCS Backup Server includes the Acronis SCS Cryptographic Library and Acronis SCS Protocol Library in both the Management Server and Backup Agents. They provide the underlying cryptographic and protocol functionality necessary to support the use of secure communications protocols, encrypted backups, and secure file sharing.

1.3.1 Product Components

The following paragraphs provide a brief description of the product components.

1.3.1.1 Management Server

The Management Server provides the means to configure, monitor, and manage backups and provides the web server (Web UI) for the Management Console. The Management Server is comprised of a number of management services responsible for management functions of Acronis SCS Backup Server. The Management Server also includes an API[3] Gateway to communicate with the Backup Agents. The Management Server does not actually perform backup, recovery, or other data-manipulation operations. These are performed by the Backup Agents installed on each protected machine. The management server uses port 7780 to asynchronously exchange management messages between the management server and the agents.

The Management Console allows an administrator to create a backup plan, or set of rules, to specify how data will be backed up on a given machine. This includes specifying what to back up (for example, disks or volumes), where to back it up to, and the schedule (by event or time) for backups. The same backup plan can be applied to groups of machines of the same type to simplify management of a large number of machines. Backup infrastructures can be organized into departments allowing for role-based administration of separate resources. The Management Server also allows a user to recover an entire machine or individual files, folders, VM[4]s, or databases from a backup.

[2] SQL – Structured Query Language
[3] API – Application Programming Interface
[4] VM – Virtual Machine

The Management Server uses a built-in SQLite database by default to store its operational data but may be configured at installation to use Microsoft SQL server instead.

The Acronis SCS Backup Server Monitoring Service provides monitoring and reporting features. Its dashboard provides a number of customizable, dynamic widgets that give an overview of a backup infrastructure and backed-up devices, allowing an administrator to easily monitor the current state of a backup infrastructure. The reporting feature generates on-demand and scheduled reports about the backup infrastructure. The Reports section is available only with an Advanced license. The option to install the Monitoring Service component is provided through a custom install. If installed, the Management Console will show Dashboard and Reports sections under the Overview tab.

Only the features described in Section 1.5 are included in the evaluation.

1.3.1.2 Backup Agents

Backup Agents, which are an environmental components, are installed as a number of services to perform the actual backup and recovery operations on each machine that requires protection. They are typically installed on each machine that requires protection and then added to the Management Server. However, they are able to operate independently from the Management Server. Backup Agents are supported on both Windows and Linux OS[5]s. Different agent types are used to protect different data sources, but they all share the same architecture, communication protocols, and the vast majority of the functionality.

A command-line interface (CLI) is installed with the Backup Agents to allow for management of the Backup Agents separately from the Management Console.

1.4 TOE Overview

The TOE Overview summarizes the usage and major security features of the TOE. The TOE Overview provides a context for the TOE evaluation by identifying the TOE type, describing the product, and defining the specific evaluated configuration.

The software-only TOE is the Acronis SCS Cyber Backup 12.5 Hardened Edition Server. It is a standalone software application that runs on a Windows OS and provides a web-based centralized Management Console with customizable dashboards, advanced reporting, and auditing for managing backups. Its security features include securely storing the TLS private key, checking for updates and patches to the application software, using a digital signature to protect the integrity of the installation and update files, versioning the software with SWID tags, and using anti-exploitation capabilities such as not mapping memory to explicit addresses, file permission protections, and stack buffer overflow protections. It also secures remote access to its Management Console and communications between the TOE and Backup Agents. The TOE implements the cryptographic functionality for cryptographic services, including HTTPS[6] and TLS[7] v1.2, through its embedded Acronis SCS Cryptographic Library and Acronis SCS Protocol Library. Licenses are allocated to Backup Agents in the TOE environment that allow access to more functionality in the Management Console.

In the evaluated configuration, the TOE is installed on a Microsoft Windows Server 2016 machine that is on a network connected to two Backup Agents in the TOE environment, an Agent for Windows and an Agent for Linux.

[5] OS – Operating System
[6] HTTPS – Hypertext Transfer Protocol Secure
[7] TLS – Transport Layer Security

The Protection Profile for Application Software specifies several use cases that may be implemented by conformant TOEs. Acronis SCS Cyber Backup 12.5 Hardened Edition Server is considered to implement both content creation and content consumption.

1.4.1 TOE Environment

Table 2 defines the environmental component requirements. In the evaluated configuration, the TOE is provided as an Acronis SCS Backup Server setup program. The TOE is installed on a Windows Server running Microsoft Windows Server 2016. It is installed with custom installation settings to install the following components of the Acronis SCS Backup Server solution: Management Server and Monitoring Service.

Table 2 – Environmental Components

Component	Requirements
Management Server	This machine is used to host the Management Server software and Monitoring Service. The following are required: • Microsoft Windows Server 2016 OS • Acronis SCS Backup Server v12.5 software with licenses • 200 MB[8] of RAM[9] and 1.7 GB[10] of free space on the system volume • Intel Xeon E-2136 (Coffee Lake) CPU[11] with AES-NI
Administrator Workstation	This machine is a general-purpose computer used by administrators for remote management of the TOE via one of the following web browsers: • Google Chrome 76 or later • Mozilla Firefox 68 or later • Opera 62 or later • Microsoft Edge 88 or later • Safari 14.1.2 or later
Windows Agent Computer	This machine is a general-purpose computer that will have the Windows Agent installed on it. The following are required: • Microsoft Windows 10 OS • Acronis SCS Backup Agent for Windows v12.5 software • 720 MB disk space and 130 MB RAM • Intel Core i7-8650U CPU with AES-NI
Linux Agent Computer	This machine is a general-purpose computer that will have the Linux Agent installed on it. The following are required: • RHEL v7.9 OS • Acronis SCS Backup Agent for Linux v12.5 software • 850 MB disk space and 150 MB RAM • Intel Core i5-8350U CPU with AES-NI

The TOE relies on an embedded SQLite database to store configuration data. This database is part of the TOE.

[8] MB – Megabyte
[9] RAM – Random-Access Memory
[10] GB – Gigabyte
[11] CPU – Central Processing Unit

1.5 TOE Description

This section primarily addresses the physical and logical components of the TOE that are included in the evaluation.

1.5.1 Physical Scope

Figure 1 illustrates the physical scope and the physical boundary of the overall solution and ties together all of the components of the software-only TOE and the constituents of the TOE environment.

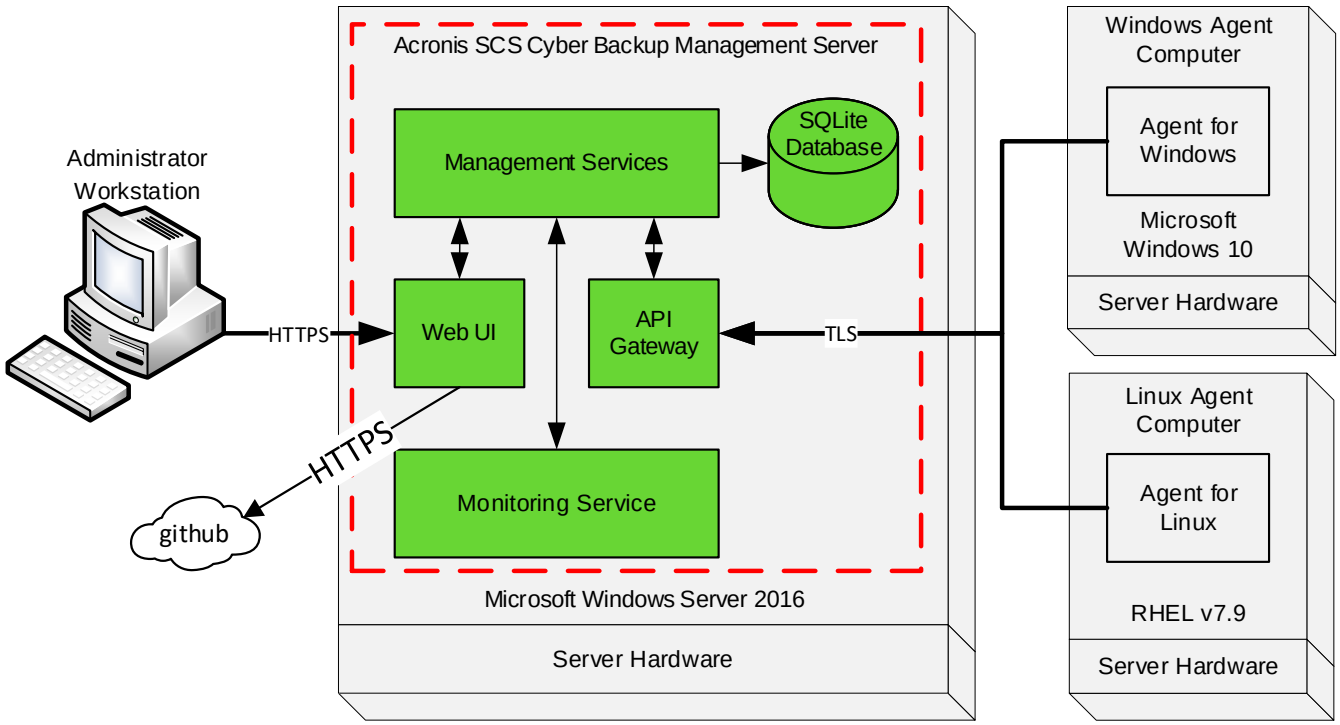

Figure 1 – Physical TOE Boundary

The TOE Boundary includes all the Acronis SCS developed parts of the Acronis SCS Cyber Backup 12.5 Hardened Edition Server product. Any third-party source code or software that Acronis SCS has modified is considered to be TOE Software.

1.5.1.1 Guidance Documentation

Table 3 lists the TOE Guidance Documentation to install, configure, and maintain the TOE.

Table 3 – Guidance Documentation

Document Name	Description
Acronis SCS Backup Server User Guide	Includes steps for the basic initialization and setup of the TOE.
Acronis SCS Cyber Backup 12.5 Hardened Edition Server Guidance Documentation Supplement Document Version: 0.5	Contains information regarding specific configuration for the TOE evaluated configuration.

1.5.2 Logical Scope

The logical boundary of the TOE is broken down into the following security classes, which are further described in Sections 7 and 8 of this ST. The logical scope also provides the description of the security features of the TOE. The SFRs implemented by the TOE are usefully grouped under the following Security Function Classes.

1.5.2.1 Cryptographic Support

The TOE provides cryptographic functions to secure sessions between the administrator workstation connecting via a web browser to the Management Console of the TOE using HTTPS and TLS v1.2. Cryptographic functions are also used to secure communications between the TOE and the Backup Agents in the TOE environment using TLS v1.2. The Acronis SCS Cryptographic Library and Acronis SCS Protocol Library are used to provide the required algorithms and protocols for all cryptographic operations. The TOE also stores its sensitive data in the Windows Data Protection API.

1.5.2.2 User Data Protection

The TOE protects sensitive data in non-volatile memory according to the requirements in FCS_STO_EXT.1. The TOE restricts its access to network connectivity provided by the platform's hardware resources. Specifically, it will only use network connectivity for administrative actions over trusted paths to its Management Console and connections via trusted channels from Backup Agents in the TOE environment. The TOE accesses the platform's system logs to store audit information and does not access any other sensitive information repositories.

1.5.2.3 Security Management

The TOE does not provide default credentials. It uses the existing administrator accounts on the platform for authentication. The TOE creates a group that is assigned to administrators and used to identify the accounts that have access. The application invokes the mechanisms recommended by the platform vendor for storing and setting configuration options. The TOE and its data are protected against unauthorized access by default file permissions. Section 8.1.3 provides a list of security-relevant management functions provided by the TOE.

1.5.2.4 Privacy

The TOE does not transmit Personally Identifiable Information (PII).

1.5.2.5 Protection of the TSF

The TOE does not allocate memory with both write and execute permissions and does not write user-modifiable files to directories that contain executable files. The TOE is compiled with the /GS flag to enable stack-based buffer overflow protection and is compatible with the platform's security features. The TOE uses standard platform APIs and includes only the third-party libraries it needs to perform its functionality. The TOE is versioned with SWID[12] tags that comply with the minimum requirements from ISO[13]/IEC[14] 19770-2:2015 and provides the ability to check for updates to the application software.

The TOE is distributed as an additional software package to the platform OS. The TOE is packaged such that its removal results in the deletion of all traces of the application, except for configuration settings, output files, and audit/log events. The TOE does not download, modify, replace or update its own binary code.

1.5.2.6 Trusted Path/Channels

The TOE provides trusted paths and trusted channels using its cryptographic functions. The TOE secures administrative communications using HTTPS over TLS v1.2 to its Management Console. The TOE provides trusted communications channels between the TOE and Backup Agents using TLS v1.2.

[12] SWID – Software Identification
[13] ISO – International Organization for Standardization
[14] IEC – International Electrotechnical Commission

1.5.3 Product Features and Functionality not included in the TOE

Features and Functionality that are not part of the evaluated configuration of the TOE are as follows:

- Remote and cloud storage locations
- Cloud configuration deployments
- Managing agents for hypervisors, applications, and mobile devices
- Backup functionality

1.5.4 Scope of Evaluation

The evaluation is limited in scope to the secure features described in the *Protection Profile for Application Software v1.4; October 07, 2021* (App PP) and the *Functional Package for Transport Layer Security (TLS),* Version 1.1, 12 February 2019 (TLS-PKG) and detailed in Section 1.5.2.

2. Conformance Claims

This section provides the identification for any CC, PP, Technical Decisions (TD), and EAL package conformance claims. Rationale is provided for any extensions or augmentations to the conformance claims. Rationale for CC and PP conformance claims can be found in Section 9.1.

Table 4 – CC and PP Conformance

Common Criteria (CC) Identification and Conformance	Common Criteria for Information Technology Security Evaluation, Version 3.1, Revision 5, April 2017; CC Part 2 extended; CC Part 3 extended; PP claim to the *Protection Profile for Application Software v1.4; October 07, 2021* conformant; *Functional Package for Transport Layer Security (TLS),* Version 1.1, 12 February 2019.
PP Identification	Exact Conformance[15] to the *Protection Profile for Application Software v1.4; October 07, 2021* and the *Functional Package for Transport Layer Security (TLS),* Version 1.1, 12 February 2019.

Table 5 - Relevant Technical Decisions

Technical Decisions	Applicable (Y/N)	Exclusion Rationale (if applicable)
AS PP		
TD0780 – FIA_X509_EXT.1 Test 4 Clarification	No	The TOE does not make use of X.509v3 certificates
TD0756 – Update for platform-provided full disk encryption	Yes	
TD0747 – Configuration Storage Option for Android	Yes	
TD0743 – FTP_DIT_EXT.1.1 Selection exclusivity	Yes	
TD0736 – Number of elements for iterations of FCS_HTTPS_EXT.1	Yes	
TD0719 – ECD for PP APP V1.3 and V1.4	Yes	
TD0717 – Format changes for PP_APP_V1.4	Yes	
~~TD0669 – FIA_X509_EXT.1 Test 4 Interpretation~~	~~No~~	Archived by NIAP
TD0664 – Testing activity for FPT_TUD_EXT.2.2	Yes	
~~TD0659 – Change to Required NIST Curves for FCS_CKM.1/AK~~	~~No~~	Archived by NIAP
~~TD0655 – Mutual authentication in FTP_DIT_EXT.1 for SW App~~	~~No~~	Archived by NIAP
TD0650 – Conformance claim sections updated to allow for MOD_VPNC_V2.3 and 2.4	No	The PP-Module added is not claimed by the TOE
TD0628 – Addition of Container Image to Package Format	Yes	
~~TD0626 – FCS_COP.1 Keyed Hash Selections~~	~~No~~	Archived by NIAP
~~TD0624 – Addition of DataStore for Storing and Setting Configuration Options~~	~~No~~	Archived by NIAP
TLS-PKG		
TD0770 – TLSS.2 connection with no client cert	No	The TOE only acts as a TLS server and does not verify X.509v3 certificates
TD0739 – PKG_TLS_V1.1 has 2 different publication dates	Yes	
TD0726 – Corrections to (D)TLSS SFRs in TLS 1.1 FP	Yes	
TD0588 – Session Resumption Support in TLS package	Yes	

[15] Exact Conformance is a type of strict conformance such that the set of SFRs and the SPD/Objectives are exactly as presented within the accepted PP and Extended PP without changes.

Technical Decisions	Applicable (Y/N)	Exclusion Rationale (if applicable)
TD0513 – CA Certificate loading	No	The TOE only acts as a TLS server and does not verify X.509v3 certificates
TD0499 – Testing with pinned certificates	No	The TOE only acts as a TLS server and does not verify X.509v3 certificates
TD0469 – Modification of test activity for FCS_TLSS_EXT.1.1 test 4.1	Yes	
TD0442 – Updated TLS Ciphersuites for TLS Package	Yes	

3. Security Problem Definition

This section describes the security aspects of the environment in which the TOE will be used and the manner in which the TOE is expected to be employed. It provides the statements for the TOE security environment's threats, assumptions, and Organizational Security Policies (OSPs) as identified in the App PP.

3.1 Threats

Table 6 describes the threats that the TOE is expected to address as defined in the App PP.

Table 6 – Threats

Threat	Description
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

Table 7 describes the assumptions that are assumed to exist in the TOE's operating environment as defined in the App PP.

Table 7 – Assumptions

Assumption	Description
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

There are no OSPs defined in the App PP.

4. Security Objectives

This section identifies the security objectives for the TOE and its supporting environment.

4.1 Security Objectives for the TOE

Table 8 describes the security objectives that the TOE is required to meet as defined in the App PP.

Table 8 – Security Objectives for the TOE

Objective	Description
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. **Addressed by:** FDP_DEC_EXT.1, FMT_CFG_EXT.1, FPT_AEX_EXT.1, FPT_TUD_EXT.1
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. **Addressed by:** FMT_SMF.1, FPR_ANO_EXT.1, FPT_IDV_EXT.1, FPT_TUD_EXT.1, FCS_COP.1/Sig
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. **Addressed by:** FCS_RBG_EXT.1, FCS_CKM_EXT.1, FTP_DIT_EXT.1, FCS_CKM.1/AK, FCS_CKM.2, FCS_COP.1/SKC, FCS_COP.1/Hash, FCS_CKM.1/Sig, FCS_COP.1/KeyedHash, FCS_RBG_EXT.2, FCS_HTTPS_EXT.1/Server, FDP_NET_EXT.1
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. **Addressed by:** FCS_RBG_EXT.1, FCS_STO_EXT.1, FDP_DAR_EXT.1, FCS_CKM.1/SK, FCS_COP.1/SKC, FCS_COP.1/Hash, FCS_COP.1/KeyedHash, FCS_RBG_EXT.2
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. **Addressed by:** FCS_CKM_EXT.1, FCS_RBG_EXT.1, FCS_STO_EXT.1, FMT_MEC_EXT.1, FPT_API_EXT.1, FPT_LIB_EXT.1, FTP_DIT_EXT.1, FCS_CKM.1/AK, FCS_CKM.2, FPT_TUD_EXT.2

4.2 Security Objectives for the Operational Environment

Table 9 describes the security objectives that the TOE's operating environment is required to meet as defined in the App PP.

Table 9 – Security Objectives for the Operational Environment

Assumption	Description
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

Please refer to section 4.3 of the App PP for a description of how the assumptions, threats, and organizational security policies map to the security objectives defined in the App PP.

5. Extended Components

This section defines the extended SFRs and extended SARs met by the TOE.

5.1 Extended TOE Security Functional Components

Table 12 in section 7.2 below identifies the extended SFRs implemented by the TOE. These extended SFRs' definitions are not repeated in this ST because they are taken directly from the App PP and TLS-PKG.

5.2 Extended TOE Security Assurance Components

Table 10 identifies the extended SARs claimed for the TOE. These extended SARs' definitions are taken directly from the App PP and are not repeated in this ST.

Table 10 – Extended TOE Security Assurance Components

Name	Description
ALC_TSU_EXT.1	Timely Security Updates

6. Security Assurance Requirements

The App PP identifies the SARs to frame the extent to which the evaluator assesses the documentation applicable for the evaluation and performs independent testing.

This section lists the set of SARs that are required in evaluations against the App PP. The App PP is conformant to Parts 2 (extended) and 3 (extended) of CC V3.1, Revision 5.

As a functional package, the TLS Package does not define its own SARs. The expectation is that all SARs required by the App PP will apply to the entire TOE, including the portions addressed by the TLS Package. Consequently, the evaluation activities specified in the App PP apply to the entire TOE evaluation, including any changes made to them by subsequent NIAP Technical Decisions as summarized in Section 1.2.

The TLS Package does contain evaluation activities for how to evaluate its SFR claims as part of the evaluation of AES_TSS.1, AGD_OPE.1, AGD_PRE.1, and ATE_IND.1. All Security Functional Requirement specified by the TLS Package will be evaluated in the manner specified in that package.

The TOE security assurance requirements are identified in Table 11.

Table 11 – Security Assurance Requirements

Assurance Requirements	
Security Target (ASE)	Conformance claims (ASE_CCL.1)
	Extended components definition (ASE_ECD.1)
	ST introduction (ASE_INT.1)
	Security objectives (ASE_OBJ.1)
	Security requirements (ASE_REQ.1)
	Security problem definition (ASE_SPD.1)
	TOE summary specification (ASE_TSS.1)
Development (ADV)	Basic functional specification (ADV_FSP.1)
Guidance documents (AGD)	Operational user guidance (AGD_OPE.1)
	Preparative procedures (AGD_PRE.1)
Life Cycle Support (ALC)	Labeling of the TOE (ALC_CMC.1)
	TOE CM[16] coverage (ALC_CMS.1)
	Timely Security Updates (ALC_TSU_EXT.1)
Tests (ATE)	Independent testing – Conformance (ATE_IND.1)
Vulnerability assessment (AVA)	Vulnerability survey (AVA_VAN.1)

[16] CM – Configuration Management

7. Security Functional Requirements

The individual SFRs are specified in the sections below. SFRs in this section are mandatory SFRs that any conformant TOE must meet. Based on selections made in these SFRs, it will also be necessary to include some of the selection-based SFRs in Appendix B. Optional or Objective SFRs may also be adopted from those listed in Appendix A and Appendix C respectively.

The Assurance Activities defined in App PP describe actions that the evaluator will take in order to determine compliance of a particular TOE with the SFRs. The content of these Assurance Activities will therefore provide more insight into deliverables required from TOE Developers.

7.1 Conventions

The conventions used in descriptions of the SFRs are as follows:

- Refinement: Indicated with bold text (e.g., [**refinement**]).
- Selection: Indicated with underlined text surrounded by brackets (e.g., [selection]).
- Assignment: Indicated with italicized text surrounded by brackets (e.g., [*assignment*]).
- Assignment within a Selection: Indicated with italicized and underlined text surrounded by brackets (e.g., [*assignment within a selection*]).
- Refinement within a Selection: Indicated with bold and underlined text surrounded by brackets (e.g., [**assignment within a selection**]).
- **Iteration** operation: is indicated by appending the SFR name with a slash and unique identifier suggesting the purpose of the operation, e.g. "/EXAMPLE1."
- Extended SFRs are identified by having a label 'EXT' at the end of the SFR name.

Operations such as assignments and selections performed by the PP author are identified as shown above; however, they do not appear within brackets. This is done intentionally to delineate between selections or assignments made by the PP author and those made by the ST author. No refinements have been made by the ST author other than grammatical and formatting corrections, or those made in places where a table reference differs from that of the PP.

7.2 Security Functional Requirements

This section specifies the SFRs for the TOE and organizes the SFRs by CC class. Table 12 identifies all SFRs implemented by the TOE and indicates the ST operations performed on each requirement. Note that some column headers use the following abbreviations: S=Selection; A=Assignment; R=Refinement; I=Iteration.

Table 12 – TOE Security Functional Requirements

Name	Description	S	A	R	I
Required SFRs					
FCS_RBG_EXT.1	Random Bit Generation Services	✓			
FCS_CKM_EXT.1	Cryptographic Key Generation Services	✓			
FCS_STO_EXT.1	Storage of Credentials	✓	✓		
FDP_DAR_EXT.1	Encryption of Sensitive Application Data	✓			
FDP_DEC_EXT.1	Access to Platform Resources	✓			

Name	Description	S	A	R	I
FDP_NET_EXT.1	Network Communications	✓	✓		
FMT_CFG_EXT.1	Secure by Default Configuration				
FMT_MEC_EXT.1	Supported Configuration Mechanism				
FMT_SMF.1	Specification of Management Functions	✓	✓		
FPR_ANO_EXT.1	User Consent for Transmission of Personally Identifiable Information	✓			
FPT_AEX_EXT.1	Anti-Exploitation Capabilities	✓	✓		
FPT_API_EXT.1	Use of Supported Services and APIs				
FPT_IDV_EXT.1	Software Identification and Versions	✓			
FPT_LIB_EXT.1	User of Third Party Libraries		✓		
FPT_TUD_EXT.1	Integrity for Installation and Update	✓			
FTP_DIT_EXT.1	Protection of Data in Transit	✓			
Selection-based SFRs					
FCS_CKM.1/AK	Cryptographic Asymmetric Key Generation	✓		✓	✓
FCS_CKM.2	Cryptographic Key Establishment	✓		✓	
FCS_COP.1/SKC	Cryptographic Operation – Encryption/Decryption	✓		✓	✓
FCS_COP.1/Hash	Cryptographic Operation – Hashing	✓		✓	✓
FCS_COP.1/Sig	Cryptographic Operation – Signing	✓		✓	✓
FCS_COP.1/KeyedHash	Cryptographic Operation – Keyed-Hash Message Authentication	✓	✓	✓	✓
FCS_HTTPS_EXT.1/Server	HTTPS Protocol	✓			
FCS_RBG_EXT.2	Random Bit Generation from Application	✓			
FCS_TLS_EXT.1	TLS Protocol	✓			
FCS_TLSS_EXT.1	TLS Server Protocol	✓			
FCS_TLSS_EXT.4	TLS Server Support for Renegotiation				
FPT_TUD_EXT.2	Integrity for Installation and Update				

7.2.1 Class FCS: Cryptographic Support

FCS_CKM.1/AK Cryptographic Asymmetric Key Generation

FCS_CKM.1/AK

The application shall [implement functionality] **to generate asymmetric cryptographic keys in accordance with a specified cryptographic key generation algorithm** [

- ***RSA[17] schemes*** *using cryptographic key sizes of [**2048 bit or greater]** that meet the following: [**FIPS[18] PUB[19] 186-4**, **"Digital Signature Standard (DSS)", Appendix B.3]**,*
- ***[ECC[20] schemes]*** *using [**"NIST[21] curves" ~~P-256,~~ P-384 and [P-256, P-521]]** that meet the following: [**FIPS PUB 186-4, "Digital Signature Standard (DSS)", Appendix B.4[22]]***

].

[17] RSA – Rivest, Shamir, Adleman
[18] FIPS – Federal Information Processing Standards
[19] PUB – Publication
[20] ECC – Elliptic Curve Cryptography
[21] NIST – National Institute of Standards and Technology
[22] TD0717: Format changes for PP_APP_V1.4 applies

FCS_CKM.2 Cryptographic Key Establishment

FCS_CKM.2.1

The application shall [implement functionality] to perform cryptographic key establishment in accordance with a specified cryptographic key establishment method: [

- **RSA-based key establishment schemes** that meets the following: **RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017, "Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1"**,
- **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",**

].[23]

FCS_CKM_EXT.1 Cryptographic Key Generation Services

FCS_CKM_EXT.1.1

The application shall [

- implement asymmetric key generation

].[24]

FCS_COP.1/SKC Cryptographic Operation – Encryption/Decryption

FCS_COP.1.1/SKC

The **application** shall perform [*encryption/decryption*] in accordance with a specified cryptographic algorithm [

- *AES[25]-GCM[26] (as defined in NIST SP[27] 800-38D) mode*

] and cryptographic key sizes [*128-bit, 256-bit*].[28]

FCS_COP.1/Hash Cryptographic Operation – Hashing

FCS_COP.1.1/Hash

The **application** shall perform [*cryptographic hashing services*] in accordance with a specified cryptographic algorithm [

- SHA[29]-256
- SHA-384

] and **message digest** sizes [

- 256
- 384

] **bits** that meet the following: [FIPS Pub 180-4].[30]

[23] TD0717: Format changes for PP_APP_V1.4 applies
[24] TD0717: Format changes for PP_APP_V1.4 applies
[25] AES – Advanced Encryption Standard
[26] GCM – Galois Counter Mode
[27] SP – Special Publication
[28] TD0717: Format changes for PP_APP_V1.4 applies
[29] SHA – Secure Hash Algorithm
[30] TD0717: Format changes for PP_APP_V1.4 applies

FCS_COP.1/Sig Cryptographic Operation – Signing

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 186-4, "Digital Signature Standard (DSS)", Section 5]*

].[31]

FCS_COP.1/KeyedHash Cryptographic Operation – Keyed-Hash Message Authentication

FCS_COP.1.1/KeyedHash

The **application** shall perform [*keyed-hash message authentication*] in accordance with a specified cryptographic algorithm [

- *HMAC[32]-SHA-256*

] and [

- SHA-384

] **with** key sizes [*256, 384*] and **message digest sizes** [256, 384, 512] 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'*[33]].

FCS_HTTPS_EXT.1/Server HTTPS Protocol

FCS_HTTPS_EXT.1.1/Server

The application shall implement the HTTPS protocol that complies with RFC 2818.

FCS_HTTPS_EXT.1.2/Server

The application shall implement HTTPS using TLS as defined in the Functional Package for TLS.

FCS_HTTPS_EXT.1.3/Server

The application shall [not establish the connection] if the peer certificate is deemed invalid.[34]

FCS_RBG_EXT.1 Random Bit Generation Services

FCS_RBG_EXT.1.1

The application shall [

- *implement DRBG[35] functionality*

] for its cryptographic operations.

[31] TD0717: Format changes for PP_APP_V1.4 applies
[32] HMAC – Hash-based Message Authentication Code
[33] TD0717: Format changes for PP_APP_V1.4 applies
[34] TD0736: Number of elements for iterations of FCS_HTTPS_EXT.1 applies
[35] DRBG – Deterministic Random Bit Generator

FCS_RBG_EXT.2 Random Bit Generation from Application

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[36] DRBG (AES)].

FCS_RBG_EXT.2.2

The deterministic RBG[37] shall be seeded by an entropy source that accumulates entropy from a platform-based DRBG and [

- a hardware-based 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.

FCS_STO_EXT.1 Storage of Credentials

FCS_STO_EXT.1.1

The application shall [

- invoke the functionality provided by the platform to securely store [*the TLS private key, registration token, Backup Agent application token*]

] to non-volatile memory.

FCS_TLS_EXT.1 TLS Protocol

FCS_TLS_EXT.1.1

The product shall implement [TLS as a server].

FCS_TLSS_EXT.1 TLS Server Protocol

FCS_TLSS_EXT.1.1

The product shall implement TLS 1.2 (RFC 5246) and [no earlier TLS versions] as a server that supports the cipher suites [

- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288,
- TLS_ECDHE[38]_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289,
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289[39],

] and also supports functionality for [session renegotiation].[40]

FCS_TLSS_EXT.1.2

The product shall deny connections from clients requesting SSL[41] 2.0, SSL 3.0, TLS 1.0, and [TLS 1.1].

FCS_TLSS_EXT.1.3

The product shall perform key establishment for TLS using [

- RSA with size [2048 bits, 3072 bits, 4096 bits] and no other sizes,

[36] CTR – Counter Mode
[37] RBG – Random Bit Generation
[38] ECDHE – Elliptic Curve Diffie Hellman Ephemeral
[39] TD0442: Updated TLS Ciphersuites for TLS Package applies
[40] TD0588: Session Resumption Support in TLS package applies
[41] SSL – Secure Sockets Layer

- ECDHE parameters using elliptic curves [secp521r1] and no other curves

].[42]

FCS_TLSS_EXT.4 TLS Server Support for Renegotiation

FCS_TLSS_EXT.4.1

The product shall support the "renegotiation_info" TLS extension in accordance with RFC 5746.

FCS_TLSS_EXT.4.2

The product shall include the renegotiation_info extension in ServerHello messages.

7.2.2 Class FDP: User Data Protection

FDP_DAR_EXT.1 Encryption of Sensitive Application Data

FDP_DAR_EXT.1.1

The application shall [

- protect sensitive data in accordance with FCS_STO_EXT.1[43]

] in non-volatile memory.

FDP_DEC_EXT.1 Access to Platform Resources

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 [system logs].

FDP_NET.EXT.1 Network Communications

FDP_NET_EXT.1.1

The application shall restrict network communication to [

- user-initiated communication for [*HTTPS over TLS connections to the TOE's Management Console (Web UI) to include download of a trusted update*],
- respond to [*remotely initiated TLS communication from Backup Agents in the TOE environment*]

].

7.2.3 Class FMT: Security Management

FMT_CFG_EXT.1 Secure by Default Configuration

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.

FMT_MEC_EXT.1 Supported Configuration Mechanism

FMT_MEC_EXT.1.1

The application shall [

[42] TD0726: Corrections to TLSS SFRs in TLS 1.1 FP applies

[43] TD0756: Update for platform-provided full disk encryption applies

- invoke the mechanisms recommended by the platform vendor for storing and setting configuration options.][44]

FMT_SMF.1 Specification of Management Functions

FMT_SMF.1.1

The TSF shall be capable of performing the following management functions [

- [*Query the version of the TOE,*
- *Check for updates to the TOE,*
- *Manage the list of Backup Agents allowed to connect to the TOE*
- *Manage registration tokens used by Backup Agents to connect to the TOE.*]

].

7.2.4 Class FPR: Privacy

FPR_ANO_EXT.1 User Consent for Transmission of Personally Identifiable Information

FPR_ANO_EXT.1.1

The application shall [

- not transmit PII over a network

].

7.2.5 Class FPT: Protection of the TSF

FPT_AEX_EXT.1 Anti-Exploitation Capabilities

FPT_AEX_EXT.1.1

The application shall not request to map memory at an explicit address except for [*OpenSSL runtime integrity test*].

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.

FPT_API_EXT.1 Use of Supported Services and APIs

FPT_API_EXT.1.1

The application shall use only documented platform APIs.

[44] Non-impactful updates as a result of TD0747: Configuration Storage Option for Android as there is no change to how it is evaluated

FPT_IDV_EXT.1 Software Identification and Versions

FPT_IDV_EXT.1.1

The application shall be versioned with [SWID tags that comply with minimum requirements from ISO/IEC 19770-2:2015].

FPT_LIB_EXT.1 User of Third Party Libraries

FPT_LIB_EXT.1.1

The application shall be packaged with only [*the list of third-party libraries in Appendix B: Included Third-Party Libraries*].

FPT_TUD_EXT.1 Integrity for Installation and Update

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

~~The~~ Application ~~installation package and its~~ updates shall be digitally signed such that ~~it's~~ the application platform can cryptographically verify them prior to installation.[45]

FPT_TUD_EXT.1.5

The application is distributed [as an additional software package to the platform OS].

FPT_TUD_EXT.2 Integrity for Installation and Update

FPT_TUD_EXT.2.1

The application shall be distributed using [the format of the platform-supported package manager].[46]

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.[47]

7.2.6 Class FTP: Trusted Path/Channel

FTP_DIT_EXT.1 Protection of Data in Transit

FTP_DIT_EXT.1.1

The application shall [

- encrypt all transmitted [data] with [

[45] Non-impactful updates as a result of TD0561: Signature verification update
[46] Updated as per TD0628: Addition of Container Image to Package Format
[47] Non-impactful addition as a result of TD0561: Signature verification update

- HTTPS as a server in accordance with FCS_HTTPS_EXT.1/Server for [*management traffic*],
- TLS as a server as defined in the Functional Package for TLS and also supports functionality for [none] for [*Backup Agents*][48]]

] between itself and another trusted IT[49] product.

[48] Updated as per TD0743: FTP_DIT_EXT.1.1 Selection Exclusivity

[49] IT – Information Technology

8. TOE Summary Specification

This section presents information to detail how the TOE meets the functional requirements described in previous sections of this ST.

8.1 TOE Security Functionality

Each of the security requirements and the associated descriptions correspond to the security functions. Hence, each function is described by how it specifically satisfies each of its related requirements. This serves to both describe the security functions and rationalize that the security functions satisfy the necessary requirements.

Table 13 – Mapping of TOE Security Functionality to Security Functional Requirements

TOE Security Function	SFR ID[50]	Description
Cryptographic Support	FCS_CKM.1/AK	Cryptographic Asymmetric Key Generation
	FCS_CKM.2	Cryptographic Key Establishment
	FCS_CKM_EXT.1	Cryptographic Key Generation Services
	FCS_COP.1/SKC	Cryptographic Operation – Encryption/Decryption
	FCS_COP.1/Hash	Cryptographic Operation – Hashing
	FCS_COP.1/Sig	Cryptographic Operation – Signing
	FCS_COP.1/KeyedHash	Cryptographic Operation – Keyed-Hash Message
	FCS_HTTPS_EXT.1/Server	HTTPS Protocol
	FCS_RBG_EXT.1	Random Bit Generation Services
	FCS_RBG_EXT.2	Random Bit Generation from Application
	FCS_STO_EXT.1	Storage of Credentials
	FCS_TLS_EXT.1	TLS Protocol
	FCS_TLSS_EXT.1	TLS Server Protocol
	FCS_TLSS_EXT.4	TLS Server Support for Renegotiation
User Data Protection	FDP_DAR_EXT.1	Encryption of Sensitive Application Data
	FDP_DEC_EXT.1	Access to Platform Resources
	FDP_NET_EXT.1	Network Communications
Security Management	FMT_CFG_EXT.1	Secure by Default Configuration
	FMT_MEC_EXT.1	Supported Configuration Mechanism
	FMT_SMF.1	Specification of Management Functions
Privacy	FPR_ANO_EXT.1	User Consent for Transmission of Personally Identifiable Information
Protection of the TSF	FPT_AEX_EXT.1	Anti-Exploitation Capabilities
	FPT_API_EXT.1	Use of Supported Services and APIs
	FPT_IDV_EXT.1	Software Identification and Versions
	FPT_LIB_EXT.1	User of Third Party Libraries
	FPT_TUD_EXT.1	Integrity for Installation and Update
	FPT_TUD_EXT.2	Integrity for Installation and Update
Trusted Path / Channels	FTP_DIT_EXT.1	Protection of Data in Transit

[50] ID – Identification

8.1.1 Cryptographic Support

The TOE implements the Acronis SCS Cryptographic Library to provide the required algorithms for all cryptographic operations. Each of the cryptographic algorithms supported by the TOE have been tested and certified by the CAVP[51]. See Table 14 below for the cryptographic operations implemented by the TOE.

Table 14 – Cryptographic Algorithms and Key Sizes

Cryptographic Operation	Usage	Algorithm	Key Lengths / Curves / Moduli	Certificate
Encryption/Decryption	TLS, HTTPS	AES-GCM	128, 256	CAVP C1351
Key Pair Generation	TLS, HTTPS	RSA	2048, 3072	CAVP C1351
		ECDSA	NIST P curve with size 521	CAVP C1351
Digital Signature Generation Digital Signature Verification	TLS, HTTPS	RSA	2048, 3072	CAVP C1351
Key Establishment	TLS, HTTPS	RSA	2048, 3072, 4096	None
		ECDHE	NIST P curve with size 521	CAVP C1351
Message Digest	TLS, HTTPS	SHA-256, SHA-384	256, 384	CAVP C1351
Message Authentication	TLS, HTTPS	HMAC-SHA-256, HMAC-SHA-384	256, 384	CAVP C1351
Deterministic Random Bit Generation	DRBG	CTR_DRBG (AES)	256	CAVP C1351

FCS_CKM_EXT.1 and FCS_CKM.1/AK

The TOE implements asymmetric key generation. The schemes implemented by the TOE to generate asymmetric cryptographic keys for key establishment and entity authentication are the RSA and ECC schemes. The RSA keys and key sizes listed in Table 14 are generated for key establishment and entity authentication for TLS and HTTPS. The ECDHE keys and NIST P curve listed in Table 14 are generated for key establishment and entity authentication for TLS and HTTPS. Both RSA and ECC key generation schemes that are implemented by the TOE meet FIPS PUB 186-4.

FCS_CKM.2

The TOE implements both RSA and elliptic curve-based key establishment schemes for TLS and HTTPS. The RSA-based schemes meet RSAES-PKCS1-v1_5 as specified in Section 7.2 of RFC 8017. The TOE acts as a recipient for RSA-based key establishment schemes. The elliptic-curve based scheme for ECDHE meet NIST SP-800 56A. The key sizes and curve used for the key establishment schemes are listed in Table 14.

FCS_COP.1/SKC

The TOE performs AES encryption and decryption for HTTPS and TLS v1.2 trusted path and channel communications. The AES algorithm operates in GCM mode with key sizes of 128 and 256 bits. In TLS and HTTPS sessions, the TOE acts as a TLS server for connections to itself from the Backup Agents and users connecting from a browser. Please refer to **FCS_TLSS_EXT.1** for more information on the implementation of the TLS protocol.

[51] CAVP – Cryptographic Algorithm Validation Program

FCS_COP.1/Hash and FCS_COP.1/KeyedHash

Hashing services are performed by the TOE with the SHA-256 and SHA-384 algorithms and the message digest sizes of 256 and 384 in accordance with FIPS Pub 180-4. The hash functions are used with other TOE cryptographic functions, including digital signature verification and MACs[52]. The HMAC-SHA-256 cryptographic algorithm uses the SHA-256 hash function with a cryptographic key size of 256 bits and 256-bit message digest size in accordance with FIPS Pub 198-1. The HMAC-SHA-384 cryptographic algorithm uses the SHA-384 hash function with a cryptographic key size of 384 bits and 384-bit message digest size in accordance with FIPS Pub 198-1.

FCS_COP.1/Sig

For signature generation and verification, the TOE uses the RSA algorithm. The RSA algorithm meets FIPS PUB 186-4 Section 4 and uses the key sizes of 2048 and 3072 bits. The RSA algorithm is used for HTTPS and TLS connections.

FCS_HTTPS_EXT.1/Server

The TOE implements HTTPS on trusted paths in compliance with RFC 2818. Acting as a server during remote administration TLS connections, the TOE requires the peer to initiate the connection. The TOE does not support mutual authentication and will not request the peer's certificate.

FCS_RBG_EXT.1 and FCS_RBG_EXT.2

The TOE implements the SP 800-90A CTR_DRBG (AES) for all deterministic random bit generation services. The CTR_DRBG is seeded with a minimum of 256 bits of entropy via RDRAND that accumulates entropy from the Intel DRNG. The entropy received from the Intel DRNG is assumed to be 100% entropic. The amount of entropy used to seed the CTR_DRBG corresponds to the greatest security strength of the algorithms included in the ST (AES-256). Refer to Tables 2 and 3 of NIST SP 800-57A for more information on the algorithm security strengths.

FCS_STO_EXT.1

The TOE leverages the Windows Data Protection API to securely store the TOE's TLS private key, Backup Agent application token, and registration token. The TLS private key is used to decrypt TLS and HTTPS traffic. The registration token is used as an alternative to an administrator's credentials when installing a Backup Agent while the Backup Agent application token is used by connecting Backup Agents to download the correct configuration and license information.

FCS_TLS_EXT.1, FCS_TLSS_EXT.1, and FCS_TLSS_EXT.4

The TOE only implements TLS as a server and is not a TLS client.

The TOE implements server-side TLS v1.2 for secure connections from the management workstation to the Management Console (HTTPS) and from the Backup Agents to the Management Server (TLS). The server-side TLS v1.2 connections support the following cipher suites:

- TLS_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5288
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 as defined in RFC 5289
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 as defined in RFC 5289

The TOE only accepts TLS v1.2 requests and denies connections from clients requesting SSL 2.0, SSL 3.0, TLS 1.0, or TLS 1.1.

[52] MAC – Message Authentication Code

The TOE uses its Acronis SCS Cryptographic Library to generate key establishment parameters for the server Key Exchange message using RSA with key size 2048, 3072, and 4096 bits and ECDHE over NIST curve secp521r1.

The TOE supports functionality for session renegotiation. The TOE supports the `renegotiation_info` TLS extension in accordance with RFC 5746. It includes the `renegotiation_info` extension in `ServerHello` messages. The TOE also supports TLS 1.2 Session Tickets.

TOE Security Functional Requirements Satisfied: FCS_CKM.1/AK, FCS_CKM.2, FCS_CKM_EXT.1, FCS_COP.1/SKC, FCS_COP.1/Hash, FCS_COP.1/Sig, FCS_COP.1/KeyedHash, FCS_HTTPS_EXT.1/Server, FCS_RBG_EXT.1, FCS_RBG_EXT.2, FCS_STO_EXT.1, FCS_TLS_EXT.1, FCS_TLSS_EXT.1, FCS_TLSS_EXT.4

8.1.2 User Data Protection

FDP_DAR_EXT.1

The TOE protects sensitive data in accordance with FCS_STO_EXT.1 when it is stored in non-volatile memory. The TOE utilizes the Windows Data Protection API to store a TLS private key that is used for HTTPS and TLS connections, the Backup Agent application tokens for downloading configuration and licensing information, and registration tokens that are used as an alternative to credential when installing the Backup Agents. No other forms of sensitive data are stored by the TOE. Users that authenticate through the TOE are validated by the OS. The TOE only reacts to the returned responses and does not store these credentials.

FDP_DEC_EXT.1 and FDP_NET_EXT.1

The TOE restricts its access to platform hardware resources to network connectivity for the TLS connections described in FCS_TLSS_EXT.1. This includes users initiating HTTPS connections to the TOE's Management Console (via the Web UI) and Backup Agents initiating TLS v1.2 connections to the TOE's API Gateway. From the TOE's Management Console, an authorized user can download a software update to the platform. The ports utilized by the TOE are as follows:

- Port 9877: Administrative interface to the TOE
- Port 7780: Asynchronous communication between the TOE and Agents

The TOE accesses the system logs to store audit information. It does not access any other sensitive information repositories.

TOE Security Functional Requirements Satisfied: FDP_DAR_EXT.1, FDP_DEC_EXT.1, FDP_NET_EXT.1

8.1.3 Security Management

FMT_CFG_EXT.1

The TOE does not install with any default credentials. Rather, it uses the credentials of the platform for user authentication. The TOE software must be installed using a local administrator account. During installation all members of the Administrators group are added to the Acronis Centralized Admins group. Any account with the Acronis Centralized Admins group can be used to access the TOE once the installation is complete. The TOE is also configured by default with file permissions that protect the application binaries and data files from modification by normal unprivileged users. This prevents a standard user from modifying the application or its data files.

FMT_MEC_EXT.1
The application invokes the mechanisms recommended by the platform vendor for storing and setting configuration options. Application specific settings are stored using the Windows Registry and the `C:\ProgramData\` directory.

The following features can be used to configure the TOE and the settings saved to the above locations:

- Add or delete an agent machine to or from the managed devices.
- Manage registration tokens for automated deployment of agent software.

FMT_SMF.1
The TOE provides a web UI that is used for all management functionality it provides. If the default port is kept, it can be accessed using either https://localhost:9877/ or at a machine name from the local machine. This is configured during the initial setup and can be accessed by any existing account that is in the Acronis Centralized Admins group. Administrators that are part of the top-level organization in the TOE are able to manage any feature. The TSF is capable of performing the following management functions:

- Query the version of the TOE. To check current version, click the question mark icon in the top-right corner and then About.
- Check for updates to the TOE. To check for updates manually, click the question mark icon in the top-right corner > About > Check for updates or the question mark icon > Check for updates.
- Manage the list of Backup Agent devices allowed to connect to the TOE. To get license information and backup settings, Backup Agents must connect to the TOE. The Devices tab in the web UI allows administrators to add or remove devices from the list of allowed devices.
- Manage tokens used by Backup Agents for the initial connection to the TOE when adding a device. A token can be used during the installation of a Backup Agent instead of using the TOE's administrator account information. Active tokens are listed in the Manage Tokens menu that is viewable when adding a device.

TOE Security Functional Requirements Satisfied: FMT_CFG_EXT.1, FMT_MEC_EXT.1, FMT_SMF.1

8.1.4 Privacy

FPR_ANO_EXT.1
The TOE's primary function is to backup and restore data, which may include PII. The TOE does not prompt for or require user-supplied PII to perform its designed functionality, nor does it transmit any such PII over a network; therefore, the requirement does not apply to this PII.

TOE Security Functional Requirements Satisfied: FPR_ANO_EXT.1

8.1.5 Protection of the TSF

FPT_AEX_EXT.1
The TOE does not make requests to map memory at an explicit address, except for the OpenSSL integrity test, and is compiled with ASLR enabled. The TOE does not allocate any memory regions with write and execute permissions. The TOE is compatible with the platform's security features. More specifically, the application can run successfully with Windows Defender Exploit Guard configured with the following minimum mitigations enabled: Control Flow Guard (CFG), Randomize memory allocations (Bottom-Up ASLR), Export address filtering (EAF), Import address filtering (IAF), and Data Execution Prevention (DEP). The TOE does not write user-modifiable files to directories

that contain executable files. The TOE is compiled with the `/GS` flag enabled by default for stack-based buffer overflow protection and the `/NXCOMPAT` flag to enable DEP protections for the application.

FPT_API_EXT.1
The TOE uses only the documented platform APIs listed in Appendix A: Supported Platform APIs.

FPT_IDV_EXT.1
The TOE is versioned with SWID tags that comply with the minimum requirements from ISO/IEC 19770-2:2015.

FPT_LIB_EXT.1
The TOE is packaged with the third-party libraries listed in Appendix B: Included Third-Party Libraries.

FPT_TUD_EXT.1 and FPT_TUD_EXT.2
The TOE provides the ability to check for updates and patches to the application software. An organization administrator can check for updates by clicking the question mark icon in the top-right corner and then **Check for updates**.

The TOE provides the ability to query the current version of the application software by clicking the question mark icon in the top-right corner and then **About**.

The TOE does not download, modify, replace or update its own binary code. The TOE's installation package and its updates are digitally signed so that the platform can verify their signatures before installation. The packages are digitally signed using a 2048-bit RSA key and SHA-256 digest algorithm. The authorized source of this signature is ACRONIS SCS, INC issued by DigiCert.

The TOE is distributed as an additional software package to the platform OS. It is packaged in the standard executable (.exe) format. It is 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.

TOE Security Functional Requirements Satisfied: FPT_AEX_EXT.1, FPT_API_EXT.1, FPT_IDV_EXT.1, FPT_LIB_EXT.1, FPT_TUD_EXT.1, FPT_TUD_EXT.2

8.1.6 Trusted Path/Channels

FTP_DIT_EXT.1
The TOE encrypts all transmitted data between itself and a workstation with HTTPS in accordance with HTTPS and TLSv1.2. It also encrypts all transmitted data between itself and Backup Agents with TLSv1.2. Please refer to the sections **FCS_HTTPS_EXT.1** and **FCS_TLSS_EXT.1** for more details.

TOE Security Functional Requirements Satisfied: FTP_DIT_EXT.1

8.2 Timely Security Updates

To keep the TOE secure, Acronis SCS issues security fixes depending on the following severity:

- Critical: hotfix and workaround are immediately required.
- High: hotfix or nearest update, if update is within 3-4 weeks (15-20 business days).
- Low-Medium: next major version or update.

Issue severity is calculated according to CVSSv3 methodology. For some issues a custom severity can be set by the Acronis SCS security team when CVSSv3 is not appropriate. For example, privacy issues may be prioritized far higher than the CVSS score.

If the issue was reported by a 3rd-party and therefore is subject to public disclosure, the fixes are released within the negotiated disclosure period.

Acronis SCS discloses the following information for vulnerabilities:

- Release Notes will contain information that security issues were fixed in a specific release or update.
- Release Notes will contain issue IDs and severity in a qualitative form if they are worth mentioning.
- In special cases, the details of security issues may be disclosed to customers when it's important to let customers know if their systems/data are at risk.
- Acronis SCS will not disclose details of vulnerabilities in documentation.

The Acronis SCS Support team notifies customers about security issues related to the TOE in the following cases:

1. Issue severity is Critical
2. Issue severity is High and the issue is known to 3rd-party (external report or a known exploitation).

The notification is sent to the most relevant group of customers and include enough information to understand the following:

1. The risk associated with the issue
2. Conditions under which a customer's system is vulnerable
3. Necessary steps to mitigate the risk

Customers that purchase the TOE can email appsupport@acronisscs.com to report security issues pertaining to the TOE. A public key and disclosure policy are posted to the Acronis SCS GitHub (https://github.com/acronisscs/public_disclosure) for use in securing the contents of any security related email.

Any update that is released, related to security fixes or not, is deployed to the Acronis SCS website for download. Customers may refer to the email or use the check for update process to see if a new version is available for their installation. Updates can then be downloaded and applied to the TOE as needed.

9. Rationale

9.1 Conformance Claims Rationale

This Security Target extends Part 2 and extends to Part 3 of the Common Criteria Standard for Information Technology Security Evaluations, Version 3.1 Revision 5. This ST conforms to the App PP and TLS-PKG.

9.1.1 Variance Between the PP and this ST

There is no variance between the App PP, TLS-PKG, and this ST.

9.1.2 Security Assurance Requirements Rationale

The assumptions, threats, OSPs, and objectives defined in this ST are those specified in the App PP and TLS-PKG. This ST maintains exact conformance to the App PP and TLS-PKG, including the assurance requirements listed in Section 5 of the App PP. The TOE is a standalone application that runs on a Windows Server platform and is applicable to the App PP and TLS-PKG.

10. Acronyms

Table 15 defines the acronyms used throughout this document.

Table 15 – Acronyms

Acronym	Definition
AES	Advanced Encryption Standard
API	Application Programming Interface
App PP	Protection Profile for Application Software v1.4; October 07, 2021
ASLR	Address Space Layout Randomization
CAVP	Cryptographic Algorithm Validation Program
CC	Common Criteria
CEM	Common Evaluation Methodology
CFG	Control Flow Guard
CLI	Command Line Interface
CM	Configuration Management
CTR	Counter Mode
DEP	Data Execution Protection
DRBG	Deterministic Random Bit Generator
DSS	Digital Signature Standard
EAF	Export address filtering
EAL	Evaluation Assurance Level
ECC	Elliptic Curve Cryptography
ECDHE	Elliptic Curve Diffie Hellman Ephemeral
FIPS	Federal Information Processing Standard
GB	Gigabyte
GCM	Galois Counter Mode
HMAC	Hash-based Message Authentication Code
HTTP	Hypertext Transport Protocol
HTTPS	Hypertext Transport Protocol Secure
IAF	Import address filtering
ID	Identification
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
IT	Information Technology
CCTL	Common Criteria Testing Laboratory
MAC	Message Authentication Code
MB	Megabyte
N/A	Not Applicable

Acronym	Definition
NIST	National Institute of Standards and Technology
OS	Operating System
OSP	Organizational Security Policy
PII	Personally Identifiable Information
PP	Protection Profile
PUB	Publication
RAM	Random Access Memory
RBG	Random Bit Generation
RFC	Request for Comments
RSA	Rivest, Shamir, Adleman
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
SHA	Secure Hash Algorithm
SP	Special Publication
SQL	Structured Query Language
SSL	Secure Sockets Layer
ST	Security Target
SWID	Software Identification
TD	Technical Decisions
TLS	Transport Layer Security
TLS-PKG	Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019
TOE	Target of Evaluation
UI	User Interface
VM	Virtual Machine

Appendix A: Supported Platform APIs

The following is a list of the supported platform APIs that the TOE uses:

- CreateFile
- ReadFile
- WriteFile
- LockFile
- UnlockFile
- FILE_NETWORK_OPEN_INFORMATION
- NtQueryInformationFile
- RegQueryInfoKeyA
- RegOpenKey
- RegQueryValue
- RegCloseKey
- Recv
- Send
- ExitThread
- CreateThread

Appendix B: Included Third-party Libraries

Table 16 provides a list of the included third-party libraries that the TOE uses.

Table 16 – Included Third-party Libraries

Library	Library	Library
curl.dll	iconv.dll	mspack.dll
expat.dll	intl.dll	python35.dll
glib-2.0.dll	libcurl.dll	re2.dll
gobject-2.0.dll	liblber.dll	sqlite3.dll
gthread-2.0.dll	libldap_r.dll	tcmalloc.dll
gvmomi-vix-1.11.0.dll	libcrypto10.dll	ulxmlrpcpp.dll
winpthreads4.dll	libevent.dll	vix.dll
icu38.dll	libxml2.dll	
icudt38.dll	zlib1.dll	

Prepared by:
Corsec Security, Inc.

12600 Fair Lakes Drive, Suite 210
Fairfax, VA 22003
United States of America

Phone: +1 703 267 6050
Email: info@corsec.com
http://www.corsec.com