Acronis SCS

Acronis SCS Cyber Backup 12.5 Hardened Edition Agent

v12.5

Guidance Documentation Supplement

Document Version: 0.7

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

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2022-09-22	Manil Trivedi	Initial draft.
0.2	2022-10-05	Ryan Butler	Updated TOE name.
0.3	2022-11-02	Kathleen Moyer	Updated version check procedures and TOE diagram.
0.4	2023-07-17	Cole Murphy	Command-line Tool removed during installation in section 2.2.3. CLI section 3.1.5 removed. Check for Updates Section 3.1.3 removed.
0.5	2023-09-14	Cole Murphy	Address Updated Backup features of the Agent added to exclusions list Version-Check version updated to 1.19 CRL info added to 2.2.1.2 Aakore.yaml section 2.2.6.2 added
0.6	2023-09-21	Cole Murphy	Address Updated RHEL 7.6 updated to RHEL 7.9 Section 3.1.3 re-added
0.7	2023-10-11	Cole Murphy	HTTP updated to HTTPS in Section 3.1.4 App PP updated from 1.3 to 1.4 Windows and Agent Step Section Order Updated

Table of Contents

List of Tables

List of Figures

1. Introduction

The TOE is the Acronis SCS Cyber Backup 12.5 Hardened Edition Agent developed by Acronis SCS and will hereafter be referred to as the TOE throughout this document. The TOE is the Backup Agent component of the Acronis SCS Cyber Backup 12.5 Hardened Edition solution, which consists of a Management Server and multiple Backup Agents. Backup Agents are responsible for performing specific backup, recovery, replication and data-manipulation tasks on their host machines. The Backup Agents are able to work independently from the Management Server to run their scheduled backup operations.

1.1 Purpose

This document provides guidance on the secure installation and secure use of the TOE for the Common Criteria (CC) evaluated configuration that is conformant to the Protection Profile for Application Software v1.4; October 07, 2021 (AS PP) and Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019 (TLS-PKG). This document provides clarifications and changes to the Acronis SCS Cyber Backup 12.5 Hardened Edition documentation and should be used as the guiding document for the installation and administration of the TOE in the CC-evaluated configuration.

Table 1 below lists the guidance documents relevant to the installation and configuration of the TOE.

Table 1 – TOE Guidance Documents

Document Name	Short Name	Description
Acronis SCS Acronis Cyber Backup 12.5 SCS Hardened Edition User Guide	*User Guide*	Contains steps for the basic initialization and setup of the TOE. These documents also provide information about the Acronis Backup components, architecture, deployment, and installation, and services.

1.2 Target Audience

The audience for this document consists of the end-user, the Acronis SCS development staff, the Common Criteria Evaluation Laboratory staff, and the Government Certifier.

1.3 Evaluated TOE Configuration

The TOE is installed in an on-premise deployment with all the product components stored on the local network. Figure 1 depicts the evaluation configuration of the TOE: In the evaluated configuration, the TOE is setup in two configurations: one where the Windows Agent TOE is on a network connected to the Management Server in the TOE environment, and the other is where the Linux Agent TOE is on a network connected to the Management Server in the TOE environment. Note that both of these configurations can be setup and used on the same network and use the same Management Server without interfering with each other.

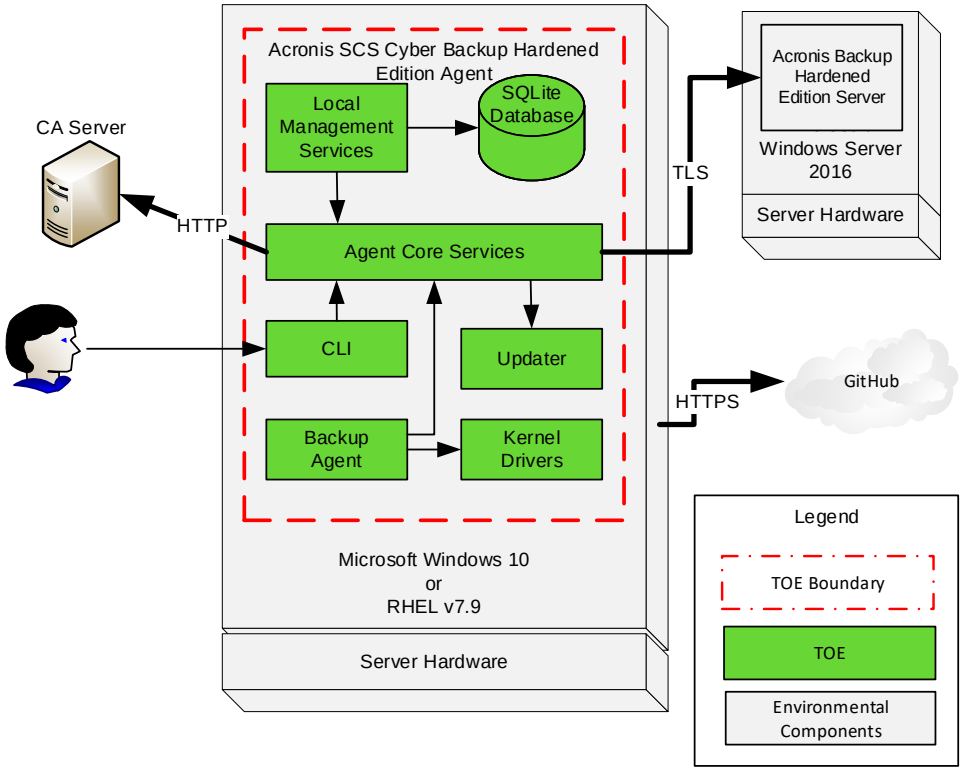

Figure 1 – Deployment Configuration of the TOE

1.4 Assumptions

The writers of this document assume the following:

- The TOE relies upon a trustworthy computing platform for its execution. This includes the underlying platform and whatever runtime environment it provides to the TOE.
- 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.
- The user of the application software is not willfully negligent or hostile and uses the software in compliance with the applied enterprise security policy.

1.5 Conventions

The following font conventions are used throughout this document:

- *Italics font is used for Document titles, files, and references.*
- ***Bold text*** *is used for* ***general emphasis*** *and selected* ***elements****.*
- ***Bold text*** *with the greater-than symbol, "**>**", is used to separate navigation steps or selections.*
- `Courier New font` is used for commands. Text that needs to be provided in a command is bracketed by "<" ">" symbols, e.g., an <IP address>.

2. Installation

This section describes the installation procedure notes and changes.

2.1 Introduction

This section provides guidance for how to properly step through the installation instructions documented in the *User Guide* along with additions and changes to the instructions contained therein, in order to allow the installer to properly install the evaluated configuration of the TOE.

Only users with administrator privileges can install the TOE. Before beginning the installation, the administrator must make certain that all the necessary platform components are in place. The *User Guide* document contains the detailed requirements for all the components necessary to install the TOE. The following items will be needed and must be acquired before continuing with this guidance.

- For the Management Server:
  - Microsoft Windows Server 2016 operating system (OS)
  - Acronis SCS Cyber Backup 12.5 Hardened Edition Server software v12.5
- For the Windows Agent Computer:
  - Microsoft Windows 10 OS
  - Acronis SCS Cyber Backup 12.5 Hardened Edition Agent for Windows software v12.5
  - Acronis SCS Version-check v1.19
- For the Linux Agent Computer
  - RHEL v7.9 OS
  - Acronis SCS Cyber Backup 12.5 Hardened Edition Agent for Linux software v12.5
  - Acronis SCS Version-check v1.19
- For the CA server:
  - Any CA server software that can be used for certificate creation/signing and to host the CRL[1] for certificate validation. No specific CA server is required as long as it follows RFC 5280.

2.2 Secure Installation

Note: Throughout this section, the reader will be instructed to read certain passages from the documents in Table 1 above. The *section number* and *section title* or *heading* of the referenced passage are *italicized*. It is assumed that the passage is from the *User Guide* unless otherwise noted. Passages from other documents are noted using the short name of the document as listed in Table 1 above.

2.2.1 Phase 1 – Initial Preparation

Section 2.1 above specifies the required components for the evaluated configuration of the TOE and TOE environment. For more information on the evaluated configuration, please refer to *1.4* of the *Acronis SCS Cyber Backup 12.5 Hardened Edition Agent Security Target.* Before beginning, please review section *1.6 On Premise Deployment* of the *User Guide*. The sections below contain information about configuring the TOE environment.

[1] CRL – Certificate Revocation List

2.2.1.1 Management Server

The administrator installs a clean version of the Microsoft Windows Server 2016 OS. Please follow the documentation on the Microsoft website https://docs.microsoft.com/en-us/windows-server/get-started/installation-and-upgrade for instructions on installing Microsoft Windows Server 2016.

Then the administrator installs the Acronis Cyber Backup 12.5 SCS Hardened Edition Server software v12.5 for only the **Management Server** and **Monitoring Service** components. Please refer to section *1.6.1 Installing the management server* of the *User Guide* for instructions on installing the software for the Management Server.

To ensure sensitive data is protected by TLS between the TOE and Management Server, the Management Server must be set to always use TLS. The Management Server uses a self-signed TLS key pair to establish TLSv1.2 communications with the TOE that must be replaced. Configure the Management Server to use a new key pair as instructed in section *3.2 Changing the SSL certificate settings* of the *User Guide*. When making these changes, also use the **auto_redirect** value of **true** to redirect HTTP traffic.

2.2.1.2 CA Server

There are no requirements to use a specific CA server. If desired, Microsoft's Windows Server can provide this functionality. Microsoft's documentation for installing and setting up the CA server can be found here: https://docs.microsoft.com/en-us/windows-server/networking/core-network-guide/cncg/server-certs/server-certificate-deployment. Otherwise, refer to the documentation for any other CA server.

The CA server will need to be setup to publish a certificate revocation list (CRL) for the TOE to check certificates against. The RootCA must include a CrlDistributionPoint extension pointing to a URI which produces DER-encoded CRLs signed by the RootCA.

2.2.1.3 Windows Agent Computer

The administrator installs the Microsoft Windows 10 OS on this computer to prepare for the installation of the Agent for Windows v12.5 Backup Agent software. Please follow the documentation located on the Microsoft website https://www.microsoft.com/en-us/software-download/windows10startfresh for instructions on installing Microsoft Windows 10.

2.2.1.4 Linux Agent Computer

The administrator installs the RHEL 7.9 OS on this computer to prepare for the installation of the Agent for Linux v12.5 Backup Agent software. Please see the RHEL website at https://access.redhat.com/downloads/content/69/ver=/rhel---7/7.9/x86_64/product-software for RHEL installation instructions.

Using terminal, install the below prerequisites for the TOE software with the following commands:

```
yum install dbus-x11
yum install gnome-keyring
```

2.2.2 Phase 2 – Preparation of the Agent

2.2.2.1 Windows Agent

The delivery process includes downloading the Windows Agent and verifying its signature.

2.2.2.1.1 Download the Windows TOE

Access the Acronis Cyber Backup 12.5 SCS Hardened Edition download page by clicking on the link, https://download.acronisscs.com/AB-12.5.4.16720/Windows64/AcronisCyberBackupSCS_12_64-bit_16720.exe. Click **Save** on the popup message.

2.2.2.1.2 Verify the Windows TOE

Locate the downloaded file and complete the following steps to verify the file signature:

1. Right-click the file, click on **Properties**, and select the **Digital Signatures** tab.
2. Select the row that contains the signer **ACRONIS SCS, INC** and digest algorithm **sha256**. Click on the **Details** button. Under **Digital Signature Information**, the **This digital signature is OK** message should be displayed.

If the certificate information does not match the above information or if the message **This digital signature is OK** is not displayed, do not install the software and contact Acronis SCS support.

2.2.2.2 Linux Agent

The delivery process includes downloading the Linux Agent and verifying its signature.

2.2.2.2.1 Download the Linux TOE

Access the Acronis Cyber Backup 12.5 SCS Hardened Edition download page by clicking on the link, https://download.acronisscs.com/AB-12.5.4.16720/Linux64/AcronisBackupSCS_12_64-bit_16720.x86_64. Click **Save** on the popup message.

2.2.2.2.2 Verify the Linux TOE

Locate the downloaded file and complete the following steps to verify the file signature:

1. Download the key used to sign the Linux package from the Acronis SCS GitHub located here: https://github.com/acronisscs/Linux_Signing_Cert.
2. Import the Acronis SCS public key by running the following command:

```
gpg --import <public key name>
```

3. Verify the signature of the signed file by running the following command:

```
gpg --verify <signed file name>
```

If the output of the command does not contain **Good signature**, do not install the software and contact Acronis SCS support.

2.2.3 Phase 3 – Installation of the Agent

2.2.3.1 Windows Agent

Follow the steps below to install the Windows Agent.

1. Log on to the Windows Agent Computer as an administrator.
2. Locate the downloaded *AcronisBackup_64-bit.exe* file, then double-click the file to start the Acronis Backup setup program. Click the **Yes** button if prompted by User Access Control.

3. The **Welcome to Acronis Backup Setup** page is displayed. Click the **I accept the terms of this license agreement** check box and then click the **Proceed** button.
4. In the **Install Acronis Backup** pane, click the **Customize installation settings** link below the green **Install Acronis Backup** button to configure the setup.
5. Under **Installation settings** for the **What to Install** line, click on the **Change** link.
6. Scroll through the list and check or uncheck the boxes so that only the following options are checked:
    a. **Agent for Windows**
7. Click the **Specify** button next to the **Acronis Backup Management Server** line.
8. In the **Server name or IP address** field, enter either the host name or the IP address of the machine where the management server is installed. Note that using the IP address of the management machine is allowed but discouraged.
9. Select the **Use the following account** radio button, then enter the <username and password> of the Management Server's administrator and click on the **Done** button.
10. The *Connecting with the management server* animation briefly appears, followed by the *Installation settings* pane. Check that the selections under *What to Install* and *Acronis Backup Management Server* are correct.
11. Click on the **Install** button.
12. After the installation completes, a big checkmark within a circle is displayed.
13. Click the **Close** button.

The Windows Agent was built with stack buffer overflow protection using the /GS flag and automatically installs the required Microsoft Visual C++ files in the operating environment. These files are needed for the TOE to operate correctly. There are no manual steps for configuring stack buffer overflow protection and it is enabled automatically.

2.2.3.2 Linux Agent

Follow the steps below to install the Linux Agent.

1. Log on to the Linux Agent Computer as an administrator.
2. Using terminal, locate the downloaded installation file and add execute permissions to it with the following command:
   `chmod +x AcronisBackupSCS_12_64-bit.x86_64`
3. Execute the installation with the following command:
   `sudo ./AcronisBackupSCS_12_64-bit.x86_64`
4. If asked to check for updates, push the **space bar** to go to the next page instead.
5. On the License Agreement page, push **shift** + **tab** to highlight *Accept* and push the **space bar**.
6. In the *Component Selection* window, ensure that only the **Acronis Backup Agent for Linux** is selected, tab to the *Next* button, and press the **space bar**.
7. On the next window, enter the **Server name** or **IP address** of the machine where the Management Server is installed. Note that using the IP address of the management machine is allowed but discouraged.
8. Select the *Register under the following account* option and specify the <username and password> of the Management Server's administrator.
9. Tab to the *Next* button and push the **space bar**.
10. If prompted with a message about missing packages, choose to continue and let the program use yum to install the packages.
11. After the required packages are installed, the installation will continue and complete. Once done, push the **space bar** on the *Exit* button.

The Linux Agent was built with stack buffer overflow protection using the __stack_chk_fail symbol in ELF executable files. There are no manual steps for configuring stack buffer overflow protection and it is enabled automatically.

2.2.4 Phase 4 – Post Installation

After installation of the TOE, the below configuration steps must be completed before the TOE is in the evaluated configuration.

2.2.4.1 Check the License of the Agents

Acronis SCS sends customers an email containing the license reference, license key, and a link to register the product. Registration is required for customer support. Click the link in the email to access the Register page, then enter the Acronis SCS-provided credentials to register the license.

Check that the Agents are recognized by the Management Server with the following steps:

1. Login to the Management Server as an administrator.
2. From a browser, access the Web UI by entering "https://<Management server IP address>:9877".
3. From the Dashboard click **Devices** > **Machines with Agents.**
4. Click the **Settings** icon in the upper right corner for the Agent, then click **Details.**
5. Confirm that the license is assigned by scrolling down to **Assigned License.**

2.2.4.2 Configure aakore.yaml on the Agent

The 'aakore.yaml' file must be updated in the following manners to enforce certain functionalities. The file is located at 'C:\ProgramData\Acronis\agent\etc' or '/opt/acronis/etc/':

- `enable-crl-verify: true`
  - This must be set to enable CRL checking.
- `insecure-skip-verify: false`
  - This must be set to enable checking of the presented certificate CN/SAN against the reference id.

3. Administrative Guidance

This section provides additional guidance not found in the guides listed in Table 1. Any clarifications, exclusions, or additions are detailed here to allow the administrator to properly configure and maintain the evaluated configuration of the TOE. The administrator should have successfully completed the installation procedures listed in section 2 above before applying the guidance found in the below sections.

3.1 Clarifications

This section contains clarifications that need to be made to existing guidance documentation. The below sections may also provide extra guidance for administering or managing the TOE.

3.1.1 Cryptographic Support

There are no management options to change the settings for the implemented cryptographic libraries. The TOE is already configured with the appropriate setting to meet the security requirements outlined in the *Security Target*.

3.1.2 Modes of Operation

The TOE only provides one mode of operation (its normal operation) and does not support a maintenance mode.

3.1.3 Check for Updates and TOE Version

The TOE provides the ability to check for updates and patches to the application software. Acronis SCS provides a script for both Linux and Windows to check for updates (installed in section 2.2.6). The script conducts a version check of the installed Acronis SCS software and compares it to the latest version. If no update is found, the script will report the current version of the TOE and that no update is available. If an update is found, the script will report the current version and that an update is available.

On Linux, to check for an update, the user of the platform runs the shell script “Update.sh”. Note that execute permissions may need to be added to the script with the “chmod +x Update.sh” command before running it.

On Windows, to check for an update, the user of the platform runs the Windows PowerShell script “Update.ps1”. If an update is available after following the steps to check for an update, use the Management Server’s web interface to check for an update from the top menu and download a copy of the installation files. If downloaded to a machine that is not the TOE’s host, transfer the file to the TOE’s host before continuing. Verify the installation file following the same process outlined in section 2.2.2.2 or 2.2.4.2 above, depending on the OS. If verified successfully, launch the installer and select “Install or update Acronis Backup”. Then select “Update” to perform an update of the existing product. If the update process is complete and the TOE software has maintained the same dialog screens, a big checkmark within a circle is displayed to show that the update was successful. If a red circle with a white X in it is displayed, this would indicate that the update failed and to contact Acronis SCS support.

3.1.4 Hardware Resources

The TOE will leverage the platform's networking hardware to communicate with other systems in the environment. The firewalls are configured automatically during installation to allow the TOE to communicate with the systems in the environment over HTTPS and TLS.

3.1.4.1 TLSv1.2 and Certificates

The backup agent establishes secure communications with the Management Server using TLSv1.2 over TCP ports 7770-7800 after validating the X.509 certificate received from the Management Server. When the TOE cannot establish a connection to determine the CRL status and validity of a certificate, the TOE will not accept the certificate. If a certificate's revocation status cannot be determined, the connection will be rejected.

3.1.5 Reporting a Security Flaw

Customers that purchase the TOE may 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.

3.2 Exclusions

Features and functionality that are not part of the evaluated configuration of the TOE are the following:

- Remote and cloud storage locations
- Cloud configuration deployments
- Functionality of the Management Server
- The backup features of the Agent

4. Acronyms

This section defines the acronyms used throughout this document.

Table 2 – Acronyms

Acronym	Definition or Meaning
ACEP	Acronis Customer Experience Program
AD	Active Directory
AGD	Guidance Documents
API	Application Programming Interface
AS PP	Protection Profile for Application Software v1.4; October 07, 2021
CA	Certificate Authority
CC	Common Criteria
CLR	Command Line Reference
CS	Certificate Services
CEP	Customer Experience Program
CRL	Certificate Revocation List
FIPS	Federal Information Processing Standard
GB	Gigabyte
HTTP	Hyper Text Transport Protocol
HTTPS	Hyper Text Transport Protocol Secure
MB	Megabyte
OS	Operating System
RAM	Random Access Memory
TLS	Transport Layer Security
TOE	Target of Evaluation
TSF	TOE Security Functionality
UI	User Interface
VM	Virtual Machine

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