

Acronis SCS

Acronis Cyber Backup 12.5 SCS Hardened Edition Server

v12.5

Guidance Documentation Supplement

Document Version: 0.10

Prepared for:

The logo for Acronis SCS, featuring the word "Acronis" in blue with a red and white striped graphic to the left of the 'A', followed by "SCS" in blue.

Acronis SCS
6370 East Thomas Road
Suite 250
Scottsdale, AZ 85251
United States of America

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

Prepared by:



Corsec Security, Inc.
13921 Park Center Road
Suite 460
Herndon, VA 20171
United States of America

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

Revision History

Version	Modification Date	Modified By	Description of Changes
0.1	2019-10-08	Lea Giovannello	Initial draft.
0.2	2019-12-20	Manil Trivedi	Updated naming information to Acronis SCS Cyber Backup. Added information about the compiler flags. Added information about performing an update. Clarified how sensitive information repositories are used.
0.3	2020-01-15	Manil Trivedi	Removed Best Practices Guide from section 1.2. Updated the information about the update process and verifying the installer. Updated naming information to Acronis Cyber Backup SCS 12.5 Hardened Edition.
0.4	2020-01-24	Mark Kasulaitis	Updated naming information. Updated download link.
0.5	2020-02-10	Mark Kasulaitis	Updated download link.
0.6	2020-05-18	Mark Kasulaitis	Updated download link. Updated the guidance document reference. Updated the steps about checking for updates and performing an update. Added a section for reporting security flaws.
0.7	2020-06-19	Mark Kasulaitis	Updated download link.
0.8	2020-06-26	Mark Kasulaitis	Updated download link.
0.9	2020-07-16	Mark Kasulaitis	Updated download link. Fixed a typo.
0.10	2020-08-19	Mark Kasulaitis	Removed the restrictions from the footer.

Table of Contents

- 1. Introduction4
 - 1.1 Purpose4
 - 1.2 Target Audience4
 - 1.3 Evaluated TOE Configuration4
 - 1.4 Assumptions.....5
 - 1.5 Conventions5
- 2. Installation6
 - 2.1 Introduction6
 - 2.2 Secure Installation.....6
 - 2.2.1 Phase 1 – Initial Preparation6
 - 2.2.2 Phase 2 – Download and Verify the TOE.....7
 - 2.2.3 Phase 3 – Install the TOE8
 - 2.2.4 Phase 4 – Post Installation.....8
- 3. Administrative Guidance 10
 - 3.1 Clarifications..... 10
 - 3.1.1 Cryptographic Support 10
 - 3.1.2 Modes of Operation 10
 - 3.1.3 Check for Updates and TOE Version 10
 - 3.1.4 Hardware Resources 11
 - 3.1.5 Sensitive Information Repositories 11
 - 3.1.6 Reporting a Security Flaw..... 11
 - 3.2 Exclusions..... 11
- 4. Acronyms 12

List of Tables

- Table 1 – TOE Guidance Documents4
- Table 2 – Acronyms 12

List of Figures

- Figure 1 – Deployment Configuration of the TOE5

1. Introduction

The Target of Evaluation (TOE) is the Acronis Cyber Backup 12.5 SCS Hardened Edition Server developed by Acronis SCS and is a software-only application that runs on a Windows operating system (OS). The TOE is the Management Server component of the Acronis Cyber Backup 12.5 SCS Hardened Edition solution, which consists of a Management Server and multiple Backup Agents. The Management Server provides a web UI¹ called the Management Console with customizable dashboards, advanced reporting, and auditing for managing backups.

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 v1.3; March 01, 2019 (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 Cyber Backup 12.5 SCS 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
<i>Acronis SCS Acronis Cyber Backup 12.5 SCS Hardened Edition User Guide</i>	<i>User Guide</i>	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:

¹ UI – User Interface

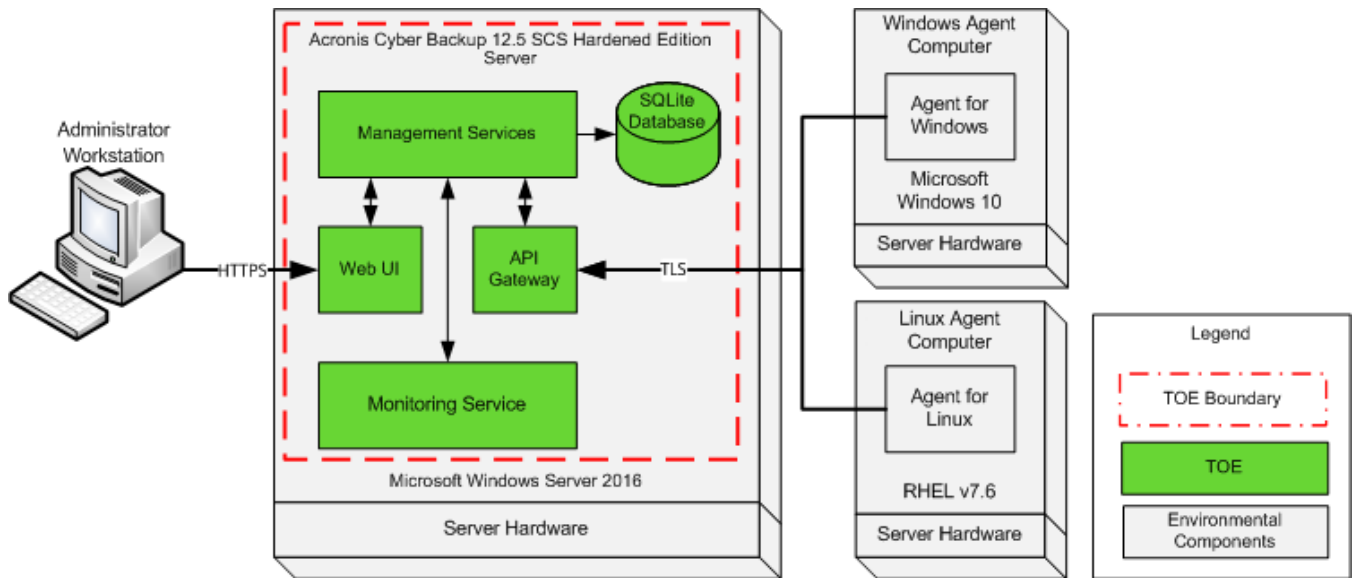


Figure 1 – Deployment Configuration of the TOE

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.

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 Cyber Backup 12.5 SCS Hardened Edition Server software v12.5
- For the Windows Agent Computer:
 - Microsoft Windows 10 OS
 - Acronis Cyber Backup 12.5 SCS Hardened Edition Agent for Windows software v12.5
- For the Linux Agent Computer:
 - RHEL 7.6 OS
 - Acronis Cyber Backup 12.5 SCS Hardened Edition Agent for Linux software v12.5
- For the Administration workstation:
 - Web browser:
 - Google Chrome 29 or later
 - Mozilla Firefox 23 or later
 - Opera 16 or later
 - Windows Internet Explorer 10 or later
 - Microsoft Edge 25 or later
 - Safari 8 or later running in the macOS and iOS operating systems

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 Acronis*

Cyber Backup 12.5 SCS Hardened Edition Server Security Target. Before beginning, please review section 2.6 *On Premise Deployment* of the *User Guide*. The sections below contain information about configuring the TOE environment.

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.

2.2.1.2 Windows Agent Computer

The administrator installs the Microsoft Windows 10 OS on this computer to prepare for the installation of the 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.

2.2.1.3 Linux Agent Computer

The administrator installs the RHEL 7.6 OS on this computer to prepare for the installation of the Backup Agent software. Please see the RHEL website at https://access.redhat.com/downloads/content/69/ver=/rhel---7/7.6/x86_64/product-software for RHEL installation instructions.

2.2.1.4 Administration Workstation

The administration workstation is a general-purpose computer with a web browser listed in 2.1 above. The workstation's browser is used by administrators to manage the TOE.

2.2.2 Phase 2 – Download and Verify the TOE

The delivery process includes downloading the TOE, verifying its signature, and registering its license.

2.2.2.1 Download the 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.

2.2.2.2 Verify the 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.

2.2.2.3 Register the TOE

Acronis SCS sends customers an email containing the license reference, license key, and a link to register the product. The TOE 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.

2.2.3 Phase 3 – Install the TOE

The section below details the steps required to install the TOE.

2.2.3.1 Install the TOE

Follow the steps below to install the TOE.

1. Log on to the Windows Server 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. **Management Server**
 - b. **Monitoring Service**
7. Click the **Modify** button and check that the Management Server and Monitoring Service options appear under **What to Install**.
8. For the **Logon account for management server service** line, click on the **Change** link.
9. Select the radio button for **User Service User Accounts** and click on the **Done** button.
10. Click the **Install** button.
11. After the installation completes, a big checkmark within a circle is displayed.
12. Click the **Close** button and the *Sign in as current Windows user* login screen is displayed in the browser to confirm successful installation.

The TOE 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.

2.2.4 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 Configure the SSL Certificate Settings

The Management Server uses a self-signed TLS key pair to establish TLSv1.2 communications with the Agents and the Administrator workstation 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. No other TLS configuration changes are needed to meet the security claims outlined in the *Security Target*.

2.2.4.2 Browser Configuration

Depending on the certificate used for the Management Server and the OS of the workstation, configuration of the browser may be needed to trust the console page. If a user is already able to use the **SIGN IN** button on a Windows

Acronis Cyber Backup 12.5 SCS Hardened Edition Server v12.5

machine to log into the TOE, then continue to the next section. Otherwise, see section *3.1 Configuring a web browser for Integrated Windows Authentication* for the instructions specific to the browser installed on a Windows workstation.

2.2.4.3 Install the Agents

After the TOE is installed the Backup Agents are installed on their respective computers. The Windows Agent is installed on the Windows Agent Computer and the Linux Agent is installed on the Linux Agent Computer. For instructions on installing the Backup Agents please refer to sections *2.6.3.1 Installation in Windows* and *2.6.3.2 Installation in Linux*.

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

Only accounts that are part of the Administrators Organization can check for updates. To check for updates to the TOE, click the question mark icon in the top right corner and then click **Check for updates**. A new window is displayed that will note if a new version is available or if the latest version is installed.

To view the currently installed version of the TOE software, click the question mark icon in the top right corner and then click **About**. A pop-up is displayed that will note the version information for the installed software.

3.1.3.1 Performing an Update

If an update is available after following the steps to check for an update, use the download link below the output of the version check to navigate to download a copy of the installation file. Note that the download links for the current version are available even if a new version is available as these links will always point to the most recent version. If downloaded to a machine that the TOE is not running on, transfer the file to the TOE's host before continuing. Verification the installation file following the same process outlined in section 2.2.2.2 above. 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 Windows Firewall is 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 TOE communicates with the Backup Agents to establish secure communications using TLSv1.2 over TCP port 7780. The Backup Agents are TLS clients to the TOE.

The TOE is accessed via a web browser on TCP port 9877. By default, the TOE supports both HTTP and HTTPS (using TLSv1.2), on the same TCP port 9877. An administrator configures the TOE to redirect HTTP traffic to HTTPS by changing the **auto_redirect** value from **false** to **true** in section 2.2.4.1 above.

3.1.5 Sensitive Information Repositories

The TOE accesses the Window's Event logs to store audit information about the authentication of the administrator. No other information repositories on the platform are used.

3.1.6 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
- Managing agents for hypervisors, applications, and mobile devices

4. Acronyms

This section defines the acronyms and terms 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 v1.3; March 01, 2019
CA	Certificate Authority
CC	Common Criteria
CLR	Command Line Reference
CS	Certificate Services
CEP	Customer Experience Program
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
TLS-PKG	Functional Package for Transport Layer Security (TLS), Version 1.1, 12 February 2019
TOE	Target of Evaluation
TSF	TOE Security Functionality
UI	User Interface
VM	Virtual Machine

Prepared by:
Corsec Security, Inc.



13921 Park Center Road, Suite 460
Herndon, VA 20171
United States of America

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

