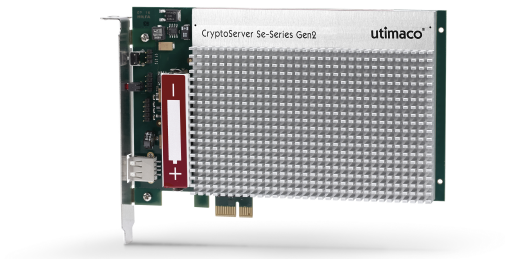
Security Server Segen2

Release Notes



utimaco®

Imprint

Copyright 2023	Utimaco IS GmbH Germanusstr. 4 D-52080 Aachen Germany
Phone	AMERICAS +1-844-UTIMACO (+1 844-884-6226) EMEA +49 800-627-3081 APAC +81 800-919-1301
Internet	https://support.hsm.utimaco.com/
e-mail	support@utimaco.com
Document Version	Working version
Product Version	4.70
Date	2024-03-15
Document No.	2023-0032
Status	**PUBLISHED**

Table of Contents

1 Introduction

SecurityServer 4.70 introduces various enhancements and fixes issues found in previous releases. Please consult the following sections for details.

Please review this document to be informed of any new features and changes introduced by this new release, and especially any pre-conditions to notice.

2 List of bug fixes

The following bugs were fixed in this release.

Reference	Component	Issue
PHX-1150	Simulator	Fixed memory allocation in Simulator
PHX-1279	SDK	SDK headers for CRYPT built with platform are missing information (cmake build)
PHX-999	SDK	CryptoServer SDK exmp_host.c does not build - Old reference to cs_xtrace
PHX-998	CXI	Fixed memory allocation error
PHX-320	cxi,cxitool	cxitool BackupKey: The same successfully imported keys cannot be backed up (error: os_mem_failed)
PHX-225	p11tool2	p11tool2 PIN-related commands: Examples in help text use deprecated 6-digit PIN
DOC-719	DOC	New paramter in CS_PKCS11_R3.cfg for ODBC reconnections
PHX-1073	EKM	cssqlekm.cfg mentions ucapi in the example for KeyStorageConfig
DOC-875	DOC	Fixed error in documentation saying ECDSA was not supported for user authentication
PHX-175	SDK	[FW] PATHDEFS in Windows make_clean.bat in SDK\... \mak
PHX-1637	P11CAT	P11CAT | Generate keypair from file' using key Templates(key_SM2) is not working
PHX-1580	SDK	CS-SDK envsetup.sh script does not work (wrong path using Linux/x86-64)
PHX-1579	SDK	CS-SDK Build exmp using make CFG=sim5 does not work on Linux
PHX-1400	p11tool2	p11tool2: Wrong Error text during setpin
PHX-1339	p11tool2	[Host] p11tool2 SetPIN wrong behavior
PHX-1242	cng	Default log path for cs_cng.cfg does not work
PHX-1019	CXI	[FW] CXI DeriveKey with ECDH_COF, SHA-256 should allow longer AES output keys
PHX-636	P11CAT	[Host] P11CAT shows wrong data type for Unique ID
PHX-532	cngtool	[Host] cngtool: No output when stdout is e.g. send through a pipe
PHX-173	cxi	[FW] cxi GenerateKeyPair: Public exponent of public template is ignored
PHX-128	p11tool2	[Host] p11tool2 GenerateKeyPair: Generating a key pair with a template file and oid:secp256r1 returns CKR_CURVE_NOT_SUPPORT (while executing without a template works)

Reference	Component	Issue
PHX-121	pkcs11	[Host] Fallback in PKCS11 R3 not working/breaks failover
PHX-117	cxitool	[Host] cxitool SelfSignedCert: Supported KeyUsage parameter is said unknown
PHX-107	pkcs11	[Host] PKCS11: Re-Initialize Slot does not delete keys in external keystore
PHX-84	pkcs11	[Host] PKCS#11 R3: Error when accessing slots with ID > 255
OCTO-148	Driver	PCIe driver: resynch after external erase

3 List of enhancements

New operating systems

This version of SecurityServer 4.70 has been tested on the operating systems RHEL/CentOS 9, and Ubuntu 22.04LTS.

Versioning

Starting with this release, firmware modules and host side utilities will report the same version number as the product CD (i.e. 4.70) to ease version identification of the product.

Support of Edward curves

This release adds support of Edward curves: Ed25519 and Ed448. This release supports both variants (Pure and Pre-Hashed) with or without context data.

The schemes supported are Ed25519, Ed25519cts,Ed25519ph, Ed448, and Ed448ph.

Prevent weak mechanisms for HMAC users

If an HSM user cannot login due deprecated hash algorithms (HMAC-PBKDF with hash=MD5 or Rd160), the administrator will see an audit log entry that helps to understand the issue.

It is no longer possible to create or restore users with md5 and Rd160 hash algorithms.

4 List of firmware packages

ID	name	type	version	initialization level
0	SMOS	SIM	5.6.12.0	INIT_OK
4	POST	SIM	4.70.0.0	INIT_OK
68	CXI	SIM	4.70.0.0	INIT_OK
81	VDES	SIM	4.70.0.0	INIT_OK
82	PP	SIM	4.70.0.0	INIT_OK
83	CMDS	SIM	4.70.0.0	INIT_OK
84	VRSA	SIM	4.70.0.0	INIT_OK
85	SC	SIM	4.70.0.0	INIT_OK
86	UTIL	SIM	4.70.0.0	INIT_OK
87	ADM	SIM	4.70.0.0	INIT_OK
88	DB	SIM	4.70.0.0	INIT_OK
89	HASH	SIM	4.70.0.0	INIT_OK
8a	STUN	SIM	4.70.0.0	INIT_OK
8b	AES	SIM	4.70.0.0	INIT_OK
8d	DSA	SIM	4.70.0.0	INIT_OK
8e	LNA	SIM	4.70.0.0	INIT_OK
8f	ECA	SIM	4.70.0.0	INIT_OK
91	ASN1	SIM	4.70.0.0	INIT_OK
96	MBK	SIM	4.70.0.0	INIT_OK
9c	ECDSA	SIM	4.70.0.0	INIT_OK
9f	CRYPT	SIM	4.70.0.0	INIT_OK
a1	OSCCA	SIM	4.70.0.0	INIT_OK

5 Hardware platform - Cryptoserver Models

The table below lists the compatible hardware platforms for this release.

Hardware model	*Hardware platform*
CryptoServer Se12/52/500/1500 PCIe	CryptoServer Se-Series Gen2 PCIe card, hardware version >= 5.1.0.0, Bootloader >= 5.00.0.0
CryptoServer Se12/52/500/1500 LAN	CryptoServer LAN V5, UTISYS003-AC, 19“ / 1U housing; redundant power supply, integrated CryptoServer Se-Series Gen2 PCIe card
CryptoServer CSe10/CSe100 PCIe	CryptoServer CSe-Series PCIe card, hardware version >= 4.0.2.0, Bootloader >= 4.0.0.0
CryptoServer CSe10/CSe100 LAN	CryptoServer LAN V5, UTISYS003-AC, 19“ / 1U housing; redundant power supply, integrated CryptoServer CSe-Series PCIe card

6 Supported operating systems

The following table lists the operating systems supported by SecurityServer.

Windows	***Version***
Windows	10,11
Windows Server	2016, 2019, 2022

Linux	***Version***
RHEL	8,9
CentOS	7,9
SUSE LES	12,15
Ubuntu	18.04LTS, 20.04LTS 22.04LTS

Notice: Only 64-bit versions of these operating systems are supported. 32-bit applications running on such 64-bit operating systems are still supported, but 32-bit versions of tools and libraries are not shipped with the product bundle anymore; please download the 32-bit Add-on bundle for SecurityServer 4.70.0. from our customer support portal when executing a 32-bit application.

7 Supported Java runtime environments

The following table lists the Java Runtime Environments supported by SecurityServer.

Java Runtime Environment	*Version*
Oracle Java	8,11,15
OpenJDK	8,11,15

8 Administration tools

The following table lists the administration tools shipped with SecurityServer.

Tool	*Version*
Csadm	4.70
gladm	4.70
CAT (GUI for HSM administration)	4.70
p11tool2	4.70
P11CAT (GUI for pkcs#11 administration)	4.70
cngtool	4.70
cxitool	4.70
Remote pin pad daemon (PPD)	4.70

9 Cryptographic libraries

The following table lists the cryptographic interface libraries shipped with SecurityServer.

Cryptographic Interface Library	*Version*
PKCS #11 R3 library “cs_pkcs11_R3.dll” (Windows), “libcs_pkcs11_R3.so” (Linux)	4.70
JCE Provider “CryptoServerJCE.jar” (Windows, Linux)	4.70
CSP Provider “cs2csp.dll” (Windows)	4.70
CNG Provider “cs2cng.dll” (Windows)	4.70
MS SQL Extensible Key Management Provider “cssqlekm.dll” (Windows)	4.70
CXI library for C/C++ “cxi.dll” (Windows), “libcxi.so” (Linux)	4.70
CXI library for Java “CryptoServerCXI.jar” (Windows, Linux)	4.70

10 Driver (PCIe card)

The following table lists the PCIe card driver shipped with SecurityServer.

Driver	*Version*
Windows Driver	5.2.0.0
Linux Driver	5.28.0

11 Technical support

You can find technical support for Utimaco products in any of these ways:

Download product information from Utimaco website[1].

Consult the Utimaco support portal[2] or find here contact information[3] to contact us via email or telephone. Please make sure to have your HSM information at hand, including your hardware serial number(s), software version number(s), operating system(s) and patch level(s), as well as the text of any error messages.

1 https://utimaco.com/products/categories/hardware-security-modules-hsm/hsms-general-purpose-use-cases/securityserver
2 https://support.hsm.utimaco.com/support
3 https://support.hsm.utimaco.com/support/contact/

12 Legal Notices

13 Older Releases - 4.60.0.2

13.1 List of bug fixes - 4.60.0.2

The following issues have been resolved in SecurityServer.

Reference	Component	Issue
PHX-1150	Firmware	Fixed memory allocation error

13.2 List of enhancements - 4.60.0.2

This is a maintenance release. It only contains bug fixes.

14 Older Releases - 4.60.0.1

14.1 List of bug fixes - 4.60.0.1

This release only contains changes for another hardware platform.

14.2 List of enhancements - 4.60.0.1

This release only contains changes for another hardware platform.

15 Older Releases - 4.60

15.1 List of bug fixes 4.60

The following issues have been resolved in SecurityServer.

Reference	Component	Issue
PHX-735	CryptoServer JCE	u.trust_anchor_product_bundle CryptoServerJCE.jar shows wrong version information in MANIFEST.MF
PHX-735	CryptoServer JCE	Wrong version in CXI_JAVA and JCE sample
PHX-733	Cmds,csadm	Error in User Database changing user password after user invalid authentication attemp
PHX-835	csadm	Unexpected error trying to perform FW downgrade after installing feature that requires change of Initial ADMIN credentials
PHX-916	Csadm,pkcs11	Access cHSMs via host using the Windows driver
PHX-389	PKCS#11	PCKS#11 C_Sign: Resulting MAC has double of the expected size with CKM_AES_MAC and CKM_DES3_MAC
PHX-637	PKCS#11	PKCS #11 C_SignUpdate: C_Verify on a C_SignUpdate created signature fails (ECDSA)
PHX-560	gladm	gladm system-clear: Interruption of u.trust Anchor after repeated system-clear executions
PHX-775	CXI	cxi: Memory allocation error when encrypting several (large) files
PHX-970	SDK,vdx	vdx_host sample cannot run due to p11 initial credentials unchanged (SO, User)
PHX-934	SDK	VDX example module does not build under linux & Windows (obsolete memutil.h)
PHX-344	CryptoServer CXI	JVM crash from CP5.getchallenge and pkcs11 reports secure messaging failed
PHX-709	gladm	gladm tests failing on Windows for Release 4.55 - device_ready test
PHX-731	gladm	gladm tests failing on Windows for Release 4.55 - test_quorum_requirements_unparsable_values
PHX-704	gladm	CSAR - error CHAI_SNAPSHOT_TEMPLATE_UNAVAILABLE while cloning snapshot on v4.51.0.1
PHX-783	Csadm	csadm test for connection timeouts failing on Linux side
PHX-638	PKCS#11	PKCS#11 R3: No errorcode in C_OpenSession when err != CKR_OK
PHX-831	CAT	The I Attribute of Users Display I[$01] Instead of I[1]

Reference	Component	Issue
PHX-799	CryptoServer CXI	CryptoServerCXI: Linux CXI_Java reproducible JVM crash when ignoring timeout on session
PHX-823	cmds	Possible to add multiple users with the same long name - Shortname displayed to users
PHX-829	CAT	It is Not Possible to Get I=0 Only Using CAT
PHX-830	CAT	After Failing to Login a User with Unchanged Credentials on CAT the Connection to the Hsm is terminated
PHX-832	csadm	Load File shadow.msc visible in AuditLogs
PHX-991	PKCS#11	ucapi: Key replication error - CKR_GENERAL_ERROR when creating PKCS #11 keys on CSAR and SeXk (with multiple cHSMs configured in the configuration file)

15.2 List of enhancements 4.60

15.2.1 Replacement of Default Authentication data

No authentication can be done using the ADMIN key provided in the product CD. Customers cannot execute any commands before changing
the default credentials.

Further implications:

- Existing customers that have an ADMIN user with the default key are not impacted.
- Ready to use simulator already has a replaced ADMIN key. The key named ADMIN_SIM should be used.
- New credentials for the ADMIN user must not be same or equal to old credentials.
- It is possible to change credentials in alarm state.

- If a command does not require authentication and credentials are provided, then first the authentication takes place and it is checked if the
credentials are changed or not. If the credentials are not changed, the command execution will not take place.

15.2.2 Replacement of HMAC Authentication Data Set by Administrator

HMAC users are now required to change their password. Users cannot execute any commands without changing their password.
Further implications are:
- Existing users are not impacted. Restored users are not considered new users. However, if a new user is restored without changing
the password, then a password change is required.
- Whilst changing the password, the password cannot be same as the previous one.

15.2.3 HMAC Authentication with PBKDF

The HMAC Authentication has been replaced by the HMAC-PBKDF Authentication. This functionality is not visible externally. The iteration
count of PBKDF was chosen to lead to an authentication delay of no more than ~0.5secs. It is recommended to use keep alive sessions. The
functionality is implemented with backward compatibility, which means an older version of host software with firmware 4.60 and an older
version of firmware with software 4.60 will fall back to the old HMAC authentication. In the August release of 2024, this backward compatibility
will be deprecated as part of deprecation roadmap.

15.2.4 Reconnection to lost external key storage connection

PKCS#11 uses ODBC to connect to a database on the host side. If the connection with the database is lost, PKCS#11 did not try to re-
establish a connection. This means that the application needed to be restarted to re-establish a connection. Now, PKCS#11 tries to
automatically re-establish lost connections with the database.