

User Guide – KeyScaler SAT API

INSTALL AND USER GUIDE

Security Level:	External
Author:	Nirmal Misra
Last Edit Date:	19 August 2024

© 2024 Device Authority

This document contains proprietary and confidential information of Device Authority and shall not be reproduced or transferred to other documents, disclosed to others, or used for any purpose other than that for which it is furnished, without the prior written consent of Device Authority. It shall be returned to the respective Device Authority companies upon request.

The trademark and service marks of Device Authority, including the Device Authority mark and logo, are the exclusive property of Device Authority, and may not be used without permission. All other marks mentioned in this material are the property of their respective owners.



Table of Contents

1	This	s Document	3								
	1.1	Document History	3								
	Refere	Referenced Documents									
	Glossa	ary of Terms	3								
	Pre-Re	equisites	3								
2	Intr	oduction	5								
	2.1	SAT Feature Overview	5								
3	Inst	allation	7								
	3.1	Configuration	9								
	3.2	Run the Application	11								
	3.3	Script Output	15								
	3.4	Change Password Script	16								
	3.5	Log Files	17								
4	Key	Scaler Control Panel View	19								
5	Арр	plication Uninstallation Process	21								
6	Арр	endix A – Create a HSM Signing Key	23								
7	Арр	endix B – Create a new FreeMarker Service Connector	26								
8	Арр	pendix C – Create a new SAT Policy	28								
9	Арр	pendix D – SAT Scripts Configuration	30								



1 This Document

1.1 Document History

Version	Description	Date	Who
1.0	Initial Document Creation	28/06/2024	Nirmal Misra
2.0	Add KeyScaler Configuration to Appendices	08/07/2024	Nirmal Misra
3.0	Changes to App User interface, updated screenshots	12/08/2024	Nirmal Misra

Referenced Documents

#	Document Name	Comment
1	SAT API One Pager	
2	Credential Manager User Guide	
3	Generate HSM Key API Document	SAC API - HSM Generate Key Pair.pdf

Glossary of Terms

Term	Description
ΑΡΙ	Application Programming Interface
СР	KeyScaler Control Panel
СМ	Credential Manager
DAE	Device Authority Engine
EC Keys	Elliptic Curve
KS	KeyScaler
HSM	Hardware Security Module
ют	Internet Of Things
MQTT	Message Queuing Telemetry Transport
PAM	Privileged Access Management
Pld	Password Identity
PSecret	Password Secret
RSA Keys	Rivest–Shamir–Adleman Key
SAC	Service Access Controller
SAT	Secure Asset Transfer
URL	Universal Resource Locator
UUID	Universal Unique Identifier aka GUID – Globally Unique Identifier

Pre-Requisites

- 1. Access to KeyScaler System version 7.0.4 or above configured with a SAC MQTT as the front end.
- 2. An RSA or EC Key available in the KeyStore for Signing the assets. Please Refer to Appendix A for how this can be done.
- 3. Freemarker Service Connector configured. See Appendix B for configuration guide
- 4. KeyScaler Configured with SAT Policy and Signing Key. For configuration guide , see Appendix C
- 5. Cyber Ark Account and access to CyberArk Vault to store credentials
- 6. Device Authority's Credential Manager agent software configured (MQTT Mode enabled) running on the IoT device. For Device Configuration and Registration please Refer to Credential Manager User Guide.



7. Sample Script available . Some sample scripts are available from Device Authority. How to configure scripts are described in Appendix D.



2 Introduction

This user guide document is intended for System Administrators who would like to install, configure and use KeyScaler's Synchronous Asset Transfer (SAT) feature to securely deliver an asset (for example, a Unix- or Windows- script) to a remote IoT device.

Sample applications to use KeyScaler's SAT API are provided, and their installation to a System Administrator's Windows computer is explained in this document. Sample Unix scripts are also provided. For other platforms, please contact cyberarkcustomer@deviceauthority.com.

2.1 SAT Feature Overview

Device Authority's SAT feature for KeyScaler integrated with CyberArk's Privileged Access Management (PAM) product enables CyberArk customers to easily and securely conduct PAM operations on IoT devices. The primary use case for this is to grant field service engineers temporary access, and then revoke such access, through password rotation. This is achieved by securely executing scripts on these IoT devices to set, and verify, user passwords. This is enabled by a new KeyScaler API (the SAT API) that enables users to securely send scripts for immediate execution on specified remote IoT devices. The device returns the execution output log to KeyScaler.

The transfer is visible in KeyScaler's Control Panel (CP) as a device job and, when successful, a corresponding log showing the script's execution output.

This SAT feature enables CyberArk users to:

- 1. Store script templates (with placeholders for execution-time values) in KeyScaler via KeyScaler's CP.
- 2. Designate target device(s), nominate the script template, and provide payload values (to be merged with the script template to replace placeholders) via the SAT API.
- 3. Deliver the composed script to the target device(s) via KeyScaler's MQTT channel.
- 4. View device execution output log (returned to KeyScaler via the MQTT channel) in KeyScaler's CP.

Sample Unix scripts available are:

- Change User Password.
- Verify User Password.

An overview of the SAT feature flow is shown in figure 1 below:





Figure 1- System overview diagram for KeyScaler's SAT feature



3 Installation

To install the Windows base KeyScaler SAT API application (this is the "External DAE API Client" shown in figure 1), download the file **CyberArk_KsAPI_Setup-1.0.0.0.0.exe** from the CyberArk Marketplace to your Windows machine:

🖊 I 🖸 📙 🖛 I	Manage	Downloads						- 🗆 ×	
File Home Share View	App Tools							^	?
Pin to Quick Copy Paste access	Move to ▼	Copy to	New item *	Properties	Select all Select none				
Clipboard		Organise	New	Open	Select				
← → × ↑ 🕹 > This PC > Downle	pads					ٽ _~	Search Downloads	م	
✓ Quick access	^	Name V Today (1)				Date modified Size	Туре	CyberArk_KsAPI_Setup-1.0.0.0 Application	
- Documents		🎯 CyberArk_KsAPI_Setu	ip-1.0.0.0.exe			28/06/2024 13:15 1	,011 KB Applic		
Pictures	*	 Earlier this week (9) 						NINIS	
Google Drive 427 items 1 item selected 12.7 MB St	💉 🗸 ate: 🎎 Share	< ed					>		ł
Figure 2 – KeyScaler	SAT	API exe file							

Next, Double Click on the file to start the installation process. You may need to allow your windows firewall to add the file as an exception.

Click on 'YES' button to continue with the installation and follow the steps below:

User Account Control X	\$
Do you want to allow this app from an unknown publisher to make changes to your device?	
KeyScaler_SecureAssetTransfer_Setup-1.0.0.0. exe	
Publisher: Unknown File origin: Hard drive on this computer	
Show more details	
Yes No	

Figure 3 – Allow Windows to install the application



Figure 4 – Click Next to start the installation process



🌍 Device Authority KeyScaler API Setup — 🗌	×
License Agreement Please review the license terms before installing Device Authority KeyScaler API.	٩
Press Page Down to see the rest of the agreement.	
Device Authority END USER LICENSE AGREEMENT ("EULA") This EULA (also available online at <http: assets="" eula.pdf="" www.deviceauthority.com=""> as updated from time to time, is a legal agreement between you, the end user customer, and the applicable Device Authority entity identified below ("Device Authority") and governs your use of the Software (as defined below). BY DOWNLOADING, INSTALLING, OR OTHERWISE ACCESSING OR USING THE SOFTWARE, YOU AGREE THAT YOU HAVE READ, UNDERSTOOD, AND AGREE TO E BOUND BY THIS EULA. IF YOU DO NOT AGREE, DO NOT USE THE SOFTWARE.</http:>	FE V
If you accept the terms of the agreement, click I Agree to continue. You must accept th agreement to install Device Authority KeyScaler API.	e
Nullsoft Install System v3.08 - Ca	ncel
Figure 5 – Click 'I Agree' to the End User License Agreement	

🌍 Device Authority KeyScaler API Setup		_	
Installing Please wait while Device Authority KeyScaler API is being			0
installed.			
Extract: flagup.xbm 100%			
Show details			
Nullsoft Install System v3.08			
< Back	Next >		Cancel

Figure 6 – Wait for the installation process to complete – it should only take a few seconds

Device Authority KeyScaler API Setu	р	-		>
Installation Complete				
Setup was completed successfully.				Ŷ
Completed				
Output folder: C:\Program Files\Devic	eAuthority∖KeyScaler API			^
Extract: DeviceAuthority.ico 100%				
Extract: DeviceAuthority-Grayscale.ic	o 100%			
Extract: DeviceAuthority - EULA.rtf	100%			
Extract: config.json 100%				
Create shortcut: C:\Program Files\De	viceAuthority\KeyScaler API	(Keyscaler AF	I.exe.ln	k
Created uninstaller: C:\Program Files\	DeviceAuthority\KeyScaler	API\uninstall.	exe	
Create folder: C:\ProgramData\Micros	oft\Windows\Start Menu\Pr	rograms\Devi	ceAuth.	
Create shortcut: C: ProgramData Micr	rosoft\Windows\Start Menu	\Programs\De	eviceA	•
Completed				\mathbf{v}
uisort Install System V3,08				
	< Pack	Next >	Car	ncel

Figure 7 – Click on 'Show Details' to view the files being installed



Device Authority KeyScaler	_		\times	
	Completing Device A KeyScaler API Setu Device Authority KeyScaler API h computer. Click Finish to dose Setup.	Authority p as been install	ed on you	r
	< <u>B</u> ack	<u>F</u> inish	Cano	el

Figure 8 – Click on 'Finish' once Setup is completed

3.1 Configuration

Next, navigate to the following folder:

. 🗹 🛄 🖛		Manage	Manage	KeyScaler AP	1					- 🗆	×
File Home	Share View Sho	rtcut Tools	App Tools								^ 🕐
Pin to Quick Copy access	Cut Maste Copy path Paste Paste shortcut	Move to •	Copy to	name New folder	The New item •	Properties	Select all	1			
CI	ipboard		Organise		New	Open	Select				
$\leftarrow \rightarrow \cdot \uparrow$	→ This PC → Windows	(C:) → Pro	ogram Files → Dev	iceAuthority >	KeyScaler API	>	~	ට Search KeyScal	er API		Q
🖈 Quick access		^	Name	^		Date modified	Туре	Size	KeyscalerAPI.ex	œ	
			dist			28/06/2024 13:19	File folder		Shortcut		
👖 Device Autho	rity		config.json			24/06/2024 14:03	JSON Source File	1 KB			
👝 OneDrive - De	evice Authority Inc		DeviceAuthori	ty - EULA.rtf		14/06/2024 14:42	Rich Text Format	167 KB			
			🎯 DeviceAuthori	ty.ico		14/06/2024 14:42	lcon	15 KB			
💻 This PC			DeviceAuthori	ty-Grayscale.ico	D	14/06/2024 14:42	lcon	15 KB			
🧊 3D Objects			ô KeyscalerAPI.e	xe		28/06/2024 13:19	Shortcut	2 KB			
E Desktop			🎯 uninstall.exe			28/06/2024 13:19	Application	62 KB	Date modified: 28/	/06/2024 13:19	
Documents									Size: 1.6	6 KB	
L Downloads									Date created: 28/	/06/2024 13:19	
- Downloads											
J Music		~									
7 items 1 item s	elected 1.66 KB										

Figure 9 – File Manager showing the installation files for the SAT API application.

Next, edit the *config.json* file to modify the log location and file to match your environment:

C:\Prog	ram Files\DeviceAuthority\KeyScaler Secure Asset Transfer\config.json - Notepad++	_		×
File Edit	Search View Encoding Language Settings Tools Macro Run Plugins Window ?		+	• ×
🕞 📑 🔚	🖻 🗟 🕼 🎒 🎸 🖺 🌔 🗩 C 🆛 🍢 🔍 🔍 🖫 💁 1 🗸 🧮 🐼 🚳 🖉 🔊 🔍 🔍		🔤	 >>
🔚 config.js	on 🗵			
1				^
2	<pre>"log_file" : "C:\\Users\\Public\\logs\\sat_log.log",</pre>			
3	"log_level" : 20,			
4				
5	"verify_tls" : false,			
6	"host" : "tenant.mykeyscaler.com",			
7	"tenant_name" : "tenant",			- 11
8				
9	"sat_policy_id" : "b127ba96-3057-496b-a2c0-61188c5d1297",			
10	"use tpc prompts" : true			
11	L}			~
JSON file	length : 268 lines : 12 Ln : 1 Col : 1 Pos : 1 Windows (CR LF) UTF-	8	1	NS

Figure 10 – Edit config.json file to match your environment



For the fields *host, tenant* and *sat_policy_id*, these will be available once your KeyScaler system is available.

The host will be the tenant domain, for example:



Figure 11 – Host value for config.json

The *sat_policy_id* is created after a SAT policy is created in the KeyScaler tenant, for example:



Figure 12 – KeyScaler Control Panel – View sat_policy_id

G	M SNot secure	https://tenant.m	nykeyscaler.com/cp/a	admin/policies/sit/edit/ <mark>b1</mark>	27ba96-3057-496b	-a2c0-61188c5d1297/1
Ke	yScaler™ Dashboard	Manage Devices 👻	Manage Policies 👻	HSM Access Controller 👻	KeyScaler Edge 👻	Reports & Notification -
	MANAGE KEY	SCALER SYN	CHRONOUS A	SSET TRANSFER P	OLICIES	
	Edit Synchro	nous Asset Tra	nsfer Policy			
	Policy Name *			SAT Policy		0
	Policy Descrip	tion		CyberArk test		
	Timeout (ms) *			900000		0
	Signing Key *			CyberarkPair000	0001 🗸	Θ
	SAC Hostname	*		http://localhost:80	081	0
	Template Servi	ce Connector		FreeMarker Tem	plate Connec 🗸	0
					·	

Figure 13 – KeyScaler Control Panel View sat_policy_id



Sample, config.json:



Figure 14 – Sample config.json file

Next, Save and exit the config.json file.

3.2 Run the Application

To run the application on the System Administrator's computer that will operate the KeyScaler SAT feature, double click on the *KeyScaler_SecureAssetTransfer.exe* file:

User Account Control	×
Do you want to allow the unknown publisher to r	his app from an nake changes to your
device?	₽
KeyScaler_SecureAssetTra Publisher: Unknown File origin: Hard drive on this con	nsfer.exe
Show more details	
Yes	No

Figure 15 – Click on 'Yes' button to continue

A terminal window pop up will appear, prompting the user for some inputs:





Figure 16 – Launch the SAT API application

Enter the config file config.json or just hit return to use the default config file that was edited above:



Figure 17 – Enter the values prompted by the application

Once the **config file**, **device-name**, have been entered, the App prompts the user to enter the **pid** and **psecret**, either manually (m) or from file (f). If (f) is selected, user can just hit enter to use the default file *credentials.json* to enter the Pid/Psecret from file.

The SAT API Application then returns a list of possible scripts that can be executed on the target device.

The *pid* and *psecret* value may also be obtained from the KeyScalar system. Once logged into the Control Panel, navigate to **Account Settings**:



C 🔝 Not secure https://tenant.mykeyscaler.com/cp/adr	nin/policies/sat/edit/b127ba96-3057-496b-a2c0-61188c5d1297/1	
KeyScaler™ Dashboard Manage Devices ∞ Manage Policies マ	ISM Access Controller + KeyScaler Edge + Reports & Notification +	Help - Tenant ma
		Account Settings
		🖬 Customize Account Logo
MANAGE KEYSCALER SYNCHRONOUS ASS	ET TRANSFER POLICIES	Manage System Settings
		Manage KeyScaler Certificate Author
		Manage Service Connectors
Edit Synchronous Asset Transfer Policy		Manage Administrators
		Manage Users
		★ Manage Customer Accounts
Policy Name *	SAT Policy	L Manage Authorization IDs
		C Manage Key Rotation
Policy Description	CyberArk test	
		St Product License
Timeout (ms) *	900000	Manage DAE API Settings
		Manage Denice Autobale Feed
Signing Key *	CyberarkPair000001	L Download Software
		_
SAC Hostname *	http://localhost:8081	
Template Service Connector	FreeMarker Template Connec 🗸 🛛	

Figure 18 – KeyScaler Control Panel – Navigate to Account Settings

KeyScaler™ Dashboard	Manage Devices –	Manage Policies 👻	HSM Access Controller 👻	KeyScaler Edge 👻	Reports & Notification -
ACCOUNT SE	TTINGS TENAM	NT MAIN			
Integration Info					
The following information	on is typically used whe	n integrating the DAE (Connector with your server.		
Account Number	r				
358813731					
Participant ID					
42051594-baa7	7-478c-ba5d-1c908d	e528b8			
Participant Secre	et				
ef1b0476-593b	-4a6c-ab95-98b885	dae6ca			

Figure 19 – KeyScaler Control Panel – Pid and psecret settings

Select a script to run, for example 'list', and enter the **target_username**, and **target_password** (note these are not required for the list command) a sample output is shown below:



KeyScaler_SecureAssetTransfer.exe	_		×
C:\Program Files\DeviceAuthority\KeyScaler Secure Asset Transfer			^
configFilePath: config.json			
2024-08-13 12:19:50,635 [INFO] ***********			
2024-08-13 12:19:50,636 [INFO] Created Logger			
2024-08-13 12:19:50,636 [INFO] ************			
Checking regex pattern for sat policy id			
2024-08-13 12:19:50,636 [INFO] ************************************			
2024-08-13 12:19:50,637 [INFO] * System: tenant.mykeyscaler.com			
2024-08-13 12:19:50.637 [INFO] ************************************			
device name:			
2024-08-13 12:19:55.059 [INFO] Device: Iot Device 01			
Do you want to input pid manually (m) or read from file (f)? f			
Enter the path to the credentials.ison file:			
Checking regex pattern for pid			
Do you want to input psecret manually (m) or read from file (f)? f			
Enter the path to the credentials.ison file:			
Checking regex pattern for psecret: ef1b0476-593b-4a6c-ab95-98b885dae6ca			
2024-08-13 12:20:14.434 [INFO] Server certificate verification is disabled!			
2024-08-13 12:20:15.036 [INFO]			
2024-08-13 12:20:15.036 [INFO] Scripts			
2024-08-13 12:20:15,036 [INFO]			
2024-08-13 12:20:15.036 INFO Searching for all Scripts available for Device: Iot Device 01			
2024-08-13 12:20:15.036 [INFO] Scripts for Device: Iot Device 01(bc5bb6fa-a38a-4d56-abdf-47fbf64281c1)			
2024-08-13 12:20:15.036 INFO Script changepass script 1 : Description changepass script 1			
2024-08-13 12:20:15.036 INFOI Script Cyberark SAT Script : Description Cyberark Echo test			
2024-08-13 12:20:15.036 [INFO] Script diskspace : Description diskspace			
2024-08-13 12:20:15.036 [INFO] Script ifconfig : Description get the IP			
2024-08-13 12:20:15.036 [INFO] Script list : Description basic director listing and echo user name			
2024-08-13 12:20:15.036 [INFO] Script verifypass script 1 : Description verifypass script 1			
2024-08-13 12:20:15,036 [INFO] End of Scripts List			
scriptToRun: list			
target username: sat user			
Enter Password: net1234			
Enter value for 'path': .			
Script: list - ID 39f3c31c-0e31-48e6-aa4c-c21c91e757bd - True			
2024-08-13 12:32:55,712 [INFO] Supplied parameters from user: {'user': 'sat user', 'path': '.', 'password': '	*****	***'}	
Running SAT Script			
2024-08-13 12:32:55,749 [INFO] Server certificate verification is disabled!			
			×

Figure 20 – SAT API Application Execution



3.3 Script Output

The SAT API application returns the script output (as executed on the target device) to the application's console and to the log file (if configured – see section 3.5). An example of the console output is shown below, continuing with the previous section's use of the "list" script:

KeyScaler_SecureAssetTransfer.exe	- 0	×	
Enter value for 'path': . Script: list - ID 39f3c31c-0e31-48e6-aa4c-c21c91e757bd - True 2024-08-13 12:32:55,712 [INFO] Supplied parameters from user: {'user': 'sat_user', 'path': '.', 'password': '********'}		^	•
Running SAT Script			
2024-08-13 12:32:55,749 [INFO] Server certificate verification is disabled! 2024-08-13 12:32:49,625 [INFO] SAT Response Output: { 'req_id': '7fbdbeb2-6f5e-4e99-9379-cbc75dbb2406', 'response_ts': 1723548829687, 'ht status_code': 0, 'response_data': { 'data': 'sat_user\ntotal 124\ndrwxr-xr-x 23 root root 4096 Apr 25 19:16 .\ndrwxr-xr-x 23 root root 16 .\n-rwwrwxrwx 1 root root 12976 Apr 25 19:16 auth_test\n-rwr-rw-rw-rw- 1 root root 2404 Apr 25 19:16 auth_test.\ndrwxr-xr-x 2 root root 4096 Apr 25 19:16 auth/test.\ndrwxr-xr-x 2 root root 4096 Apr 24 13:53 dev\n-rw-rw-rw- 1 root 7 2021 deviceCert.cert\n-rw-rw-rw- 1 root root 1675 Sep 17 2021 deviceKey.pem\ndrwxr-xr-x 102 root root 4096 Jul 30 17:48 et<\n-rw root 0 Apr 25 18:59 gcc_output.tst\ndrwxr-xr-x 6 root root 4096 Apr 24 13:53 ome\nlwxr-xr-x 102 root root 32 Aug 11 2022 i t/initrd.img-5.4.0-1089-azure\nlrwxrwxrwx 1 root root 32 Aug 11 2022 initrd.img.old -> bot/initrd.img-5.4.0-1086-azure\ndrwxr-xr-x 4096 Nov 17 2022 lib\ndrwxr-xr-x 3 root root 4096 Nov 17 2022 libC4Ndrwxr-xr-x 2 root root 16384 Jan 21 2020 lost+found\ndrwxr-xr- 0 Apr 24 13:52 proc\ndrwxr-xr-x 3 root root 4096 Apr 24 13:53 nmt\ndrwxr-xr-x 2 root root 16096 Jan 21 2020 lost+found\ndrwxr-xr-x 2 80 Nov 17 2022 lib\ndrwxr-xr-x 7 root root 4096 Apr 24 202 sapp\ndrwxr-xr-x 24 root root 860 Aug 12 13:40 run\ndrwxr-xr-x 2 80 Nov 17 2022 sy\ndrwxrwxrwx 1 root root 4096 Aug 13 06:27 tmp\ndrwxr-xr-x 10 root root 4096 Jan 21 2020 usr\ndrwxr-xr-x 14 root 6 2022 var\nlrwxrwxrwx 1 root root 29 Aug 11 2022 rmlinuz -> boot/vmlinuz-5.4.0-1089-azure\nlrwxrwxrwx 1 root root 29 Aug 11 6 dat -> boot/vmlinuz-5.4.0-1086-azure\n', 'success': True} Result:	tp_code': 4096 Apr oot root root 3714 -rw-rw- nitrd.img x 22 root -xr-x 2 -x 167 roo 2 root root root 409 1 2022 vm	200, ' 25 19 4096 N Sep 1 1 root root root root root t root 2 0 6 Nov nlinuz.	
sat_user total 124			
Markinsky 2 3 root root 4095 Apr 25 19:16 . -rwarkwarku 1 root root 12976 Apr 25 19:16 auth_test -rwarkwarku 1 root root 2404 Apr 25 19:16 auth_test.c drwark-xr-x 2 root root 4096 Nov 17 2022 bin drwar-xr-x 15 root root 4096 Nov 17 2022 boot drwar-xr-x 15 root root 4096 Apr 24 13:53 dev			
-rw-rw-rw 1 root root 3714 Sep 17 2021 deviceCert.cert -rw-rw-rw - 1 root root 1675 Sep 17 2021 deviceKey.pem			
drwxr-xr-x 102 root root 4096 Jul 30 17:48 etc -rw-rw-rw- 1 root root 0 Apr 25 18:59 gcc_output.txt drwxr-xr-x 6 root root 4096 Apr 24 13:53 home Irwxrwxrwx 1 root root 32 Aug 11 2022 initrd.img -> boot/initrd.img-5.4.0-1089-azure			
lrwxrwxrwx 1 root root 32 Aug 11 2022 initrd.img.old -> boot/initrd.img-5.4.0-1086-azure drwxr-xr-x 22 root root 4096 Nov 17 2022 lib			
drwxr-xr-x 2 root root 4096 Nov 17 2022 lib64			
drwxr-xr-x 2 root root 4096 Jan 21 2020 media			
dmwxr-xr-x 2 root root 4096 Jan 21 2020 opt			
dr-xr-xr-x 16/ root root 0 Apr 24 13:52 proc drwx 7 root root 4006 Aug 12 20:06 root			
drwxr-xr-x 24 root root 860 Aug 12 13:40 run			
ulwar-Ar-A 2 root root 406 Jan 29 2020 snap			
drwxr-xr-x 2 root root 4096 Jan 21 2020 srv			
ar-xr-xr-x 12 root root 0 Apr 24 13:22 Sys			
drwxr-xr-x 10 root root 4096 Jan 21 2020 usr			
drwxr-xr-x 14 root root 4006 Nov 6 2022 var			
InwxrwxrWx 1 root root 29 Aug 11 2022 vmlinuz -> boot/vmlinuz-5.4.0-1089-azure lrwxrwxrwx 1 root root 29 Aug 11 2022 vmlinuz.old -> boot/vmlinuz-5.4.0-1086-azure			
Completed			
Press a key to close			
Figure 24 CAT ADI application actives the equiptication of a start of a device			-

Figure 21 – SAT API application returns the script output as executed on the device



3.4 Change Password Script

Other scripts available are for changing a password and verifying the password change. Sample outputs of these two scripts are shown below:



Figure 22 – Output for a sample change password script

8 KeyScaler_SecureAssetTransfer.exe	-		×
<pre>cv kcycale_SecureAsedInniet.exe configFilePath: config.json 2024-07-01 20:46:06,162 [INFO] ************************************</pre>	_	L	× •
Running SAT Script			
2024-07-01 20:48:15,520 [INFO] Server certificate verification is disabled! 2024-07-01 20:48:14,082 [INFO] SAT Response Output: {'req_id': 'c0e8270f-f9bb-4eaa-b6dd-b3e303ba23af', 'response_ts': 1719863 ode': 200, 'status_code': 0, 'response_data': {'data': '{"message": "verifying user sat_user"}\n{\'success\': true}\'Passw '}\n', 'success': True} Result: {"message": "verifying user sat_user"} {'success': true} {'Password is correct'}	325165, ord is	'http correc	_c t\
Completed			
Press a key to close			~

Figure 23 – Output for a sample verify password script



3.5 Log Files

Log files can be viewed in the file defined in the config.json configuration file:

"log_file" : "C:\\Users\\Public\\Logs\\log.log",

📕 🕗 📑 🖛 Logs							_		×
File Home Share View									^ ?
Pin to Quick Copy access	ut Move Copy to Copy	New item ▼ ↑ New folder	Properties	Select all Select none					
Clipboard	Organise	New	Open	Select					
← → ∽ ↑ 📙 > This PC > Windo	ws (C:) > Users > Public > Logs				~ Ō	Search Logs			P
📌 Ouick access	^ Name ^	Da	te modified Type	Size		log.log			
	credentialmanager.le	og 03,	/05/2024 10:52 Text E	ocument	19 KB	Text Document			
	log.log	01,	/07/2024 20:02 Text E	ocument	17 KB				
Documents	X log.out	11,	/11/2023 20:46 OUT I	ile 18	9,906 KB				
Pictures	* 📄 test.log	24,	/10/2019 10:45 Text [ocument	2 KB				
🝐 Google Drive	*								
↓ Downloads 4 items 1 item selected 16.6 KB State	r ¥ ¥ a Shared							B	==
Figure 24 – Location of	SAT API app log file								

The default log level in **config.json** is 10, however this can be configured to the following levels for additional troubleshooting:

- CRITICAL = 50
- ERROR = 40
- WARNING = 30
- INFO = 20
- DEBUG = 10
- NOTSET = 0

Sample content of a log file is shown in the next figure.



📔 C:\l	Users\Public\Logs\log.log - Note	epad++ [Administrator]					_		×
File Ed	dit Search View Encoding	Language Settings	Tools Macro Run	Plugins Window	?			+	▼ ×
🕞 🖨	🗄 🖻 🗟 🕼 📥 🖌 👘	6 2 C # 4	🔍 🔍 🖪 🔂	1 🗐 1	🖪 🕗 🖿 🖉	•	🖻 🔍 🎫 🕞	Z A V	, »
🔚 conf	ig.ison 🛛 🔲 credentials.ison								
	var\nlrwxrwxrwx l roo	t root 29 Aug	1 2022 vmlinuz	-> boot/vmlinuz-	5.4.0-1089-azur	e\nlrwxrwxrwx	1 root root	29 Auc	
	11 2022 vmlinuz.old ->	boot/vmlinuz-5.4	0-1086-azure\n',	'success': True	}}	- (,
90	2024-07-01 19:52:31,050	[INFO] ********	****						
91	2024-07-01 19:52:31,050	[INFO] Created L	gger						
92	2024-07-01 19:52:31,050	[INFO] ********	****						
93	2024-07-01 19:52:31,050	[INFO] ********	*****	*****					
94	2024-07-01 19:52:31,050	[INFO] * System:	tenant.mykeyscal	er.com					
95	2024-07-01 19:52:31,050	[INFO] *********	****	*****					
96	2024-07-01 19:53:25,805	[INFO] Created I							
97	2024-07-01 19:53:25,805	(INFO) *********	****						
99	2024-07-01 19:53:25,820	[INFO] ********	*****	*****					
100	2024-07-01 19:53:25.820	[INFO] * System:	tenant.mvkevscal	er.com					
101	2024-07-01 19:53:25,820	[INFO] ********	*****	*****					
102	2024-07-01 19:53:52,096	[INFO] ********	****						
103	2024-07-01 19:53:52,097	[INFO] Created L	gger						
104	2024-07-01 19:53:52,097	[INFO] ********	* * * *						
105	2024-07-01 19:53:52,097	[INFO] ********	*****	*****					
106	2024-07-01 19:53:52,097	[INFO] * System:	tenant.mykeyscal	er.com					
107	2024-07-01 19:53:52,098	[INFO] ********	*****	*****					
108	2024-07-01 19:54:35,910	[INFO] Server ce	tificate verific	ation is disable	d!				
109	2024-07-01 19:54:36,509	[INFO]							
110	2024-07-01 19:54:36,509	[INFO]	Scripts						
111	2024-07-01 19:54:36,509	(INFO)				- 01			
112	2024-07-01 19:54:36,509	(INFO) Searching	TOT ALL SCRIPTS	available for De	vice: lot Device	e UI 47fbf64201c1)			
114	2024-07-01 19:54:36,509	(INFO) Scripts 1	ngenage ecript 1	· Script change	-assa-4ust-abur	-4/1010420101)			
115	2024-07-01 19:54:36,509	[INFO] Script Cu	erark SAT Script_1	: Script Cubera	rk Echo test				
116	2024-07-01 19:54:36,509	[INFO] Script di	kspace : Script	diskspace	IN LONG CCSC				
117	2024-07-01 19:54:36,509	[INFO] Script if	onfig : Script g	et the IP					
118	2024-07-01 19:54:36,509	[INFO] Script li	t : Script basic	director listin	g and echo user	name			
119	2024-07-01 19:54:36,509	[INFO] Script ve	ifypass_script_l	: Script verify	pass_script_l				
120	2024-07-01 19:54:36,509	[INFO]	End of Scripts	List					
121	2024-07-01 20:02:04,254	[INFO] Supplied	arameters from u	ser: {'user': 's	at_user', 'path	': '.', 'passw	ord': '******	*** }	
122	2024-07-01 20:02:04,277	[INFO] Server ce	tificate verific	ation is disable	d!				
123	2024-07-01 20:02:09,910	[INFO] SAT Respo	se Output: {'req	_id': 'lab45c9c-	8a7e-4f81-87bb-:	2500a791686e',	'response_ts'	(:	
	1719860530944, 'http_co	de': 200, 'status	code': 0, 'respo	nse_data': {'dat	a': 'sat_user\n	total 124\ndrw	xr-xr-x 23 ro	ot root	
	4096 Apr 25 19:16 .\ndr	wxr-xr-x 23 root	root 4096 Apr 2	5 19:16\n-rwx	rwxrwx 1 root	root 12976 Ap	r 25 19:16		
	autn_test\n-rw-rw-rw-	1 root root 240	Apr 25 19:16 au	th_test.c\ndrwxr	-xr-x 2 root :	root 4096 Nov	17 2022	1	
	bin\ndrwxr-xr-x 4 roo	deviceCert cert)	zuzz boot\ndr	war-ar-a 15 room	t root 4060 Ap: ap 17 2021 day:	r 24 13:53 dev iceVeu nem\ndm	\n-rw-rw-rw-	I root	
	4096 May 21 17:33 etc/m	-rw-rw-rw- 1 ro	troot 0 Apr	25 18:59 gec out	tput tyt\ndrwyr.	-vr-v 6 root	root 4096 br	nr 24 13.5	13
	home\nlrwxrwxrwx l ro	ot root 32 Aug	11 2022 initrd.	img -> boot/init	rd.img-5.4.0-10	89-azure\nlrwx	rwxrwx l roc	nt root	~
	32 Aug 11 2022 initrd.	img.old -> boot/i	itrd.img-5.4.0-1	086-azure\ndrwxr	-xr-x 22 root :	root 4096 Nov	17 2022		
	lib\ndrwxr-xr-x 2 roo	t root 4096 Nov	7 2022 lib64\nd	rwx 2 ro	ot root 16384 Ja	an 21 2020 10	st+found\ndrwx	r-xr-x	2
	root root 4096 Jan 21	2020 media\ndrwx	-xr-x 3 root r	oot 4096 Apr 24	13:53 mnt\ndrw	xr-xr-x 2 ro	ot root 4096	Jan 21	
	2020 opt\ndr-xr-xr-x 17	7 root root 0	Apr 24 13:52 pro	c\ndrwx	7 root root 40	96 Jun 28 20:3	7 root\ndrwxr-	-xr-x 24	
	root root 860 Jul 1	09:10 run\ndrwxr-	r-x 2 root roo	t 12288 Nov 17	2022 sbin\ndrwx	r-xr-x 2 roo	t root 4096 J	fan 29	
	2020 snap\ndrwxr-xr-x	2 root root 409	Jan 21 2020 sr	v\ndr-xr-xr-x 1	2 root root	0 Apr 24 13:5	2 sys\ndrwxrwx	trwt 9	
	root root 4096 Jul 1	13:40 tmp\ndrwxr-	r-x 10 root roo	t 4096 Jan 21	2020 usr\ndrwxr	-xr-x 14 root	root 4096 No	ov 6 202	22
	var\nlrwxrwxrwx l roo	t root 29 Aug	1 2022 vmlinuz	-> boot/vmlinuz-	5.4.0-1089-azur	e\nlrwxrwxrwx	l root root	29 Aug	1
104	11 2022 vmlinuz.old ->	boot/vmlinuz-5.4	0-1086-azure\n',	'success': True	}}				
124									~
Normalit	tevt file	length 17.062 lines	24	1 Colul Porti		Windows (CD)		r	
promait	LEAT THE	iengui : 17,005 illies :	24 LN :	COLL POST		windows (CK	011-0		CVI.





4 KeyScaler Control Panel View

On KeyScaler System, Login using login Credentials, and navigate to Managed Devices page:

	Manage Devices				
DEVICE STATE :	Manage Device Groups Provision New Devices Manage Pending Registra Manage PKI Signature+ R	Manage Devices		8	Provision A Device
Authorized	 Manage DSM Public Keys Manage X.509 Registratio 	n		8	
Blacklisted				0	

Figure 26- KeyScaler Control Panel – Managed Devices

For a specific device, the jobs for that device can be viewed by clicking on the ellipse, as shown:

MAN	NAGE DEVICES						
Auth	norized Quarantined Blacklisted	±					Record
	Device Name 1	Registered Identifier	Authentication Method	DDKG Library 1	Date Registered 1	Certificate Status	View
	IoT Device 02		DDKG	Linux-L1	05/13/2024 18:05:25	N/A	
	lot Device 01		DDKG	Linux-L1	05/13/2024 17:29:36	N/A	(
	dustaptop-001		DDKG	Windows	01/04/2024 12:17:58	Revoked Details	
	the second se		DDKG	Windows	12/24/2023 12:18:21	N/A View Jo	bs
	CyberArkSTLab13		DDKG	Windows	12/13/2023 17:10:59	N/A Certifica	ates
	Laptop		DDKG	Linux-L1	12/08/2023 14:13:05	N/A Reques	t Logs

Figure 27- KeyScaler Control Panel – View Jobs for Device

Clicking on the 'view jobs' provides a list of status of those jobs for the elected device:

JOBS FOR DEVICE IOT	DEVICE 01		
-			
Status	Date Created 1	Date Updated 1	Actions
Status COMPLETED	Date Created 1 07/01/2024 19/02/06	Date Updated 1 07/01/2024 19.02.10	Actions View Parent Job
Status COMPLETED COMPLETED	Date Created 1 6701/2024 19 02 06 6707/2024 16 23 42	Date Updated 1 07/01/2024 19:02:10 07/01/2024 19:02:10	Actions View Parent Job View Parent Job

Figure 28- KeyScaler Control Panel – View Status of Jobs

Also, the Logs for the device can also be seen:

<u>)</u>	KeyScaler ^m Dashboard	Manage Devices +	Manage Policies -	HSM Access Controller -	KeyScaler Edge -	Reports & Notification -	Help -	Tenant main - admin@deviceaut
	DEVICE LOGS	FOR IOT DEV	/ICE 01					
	Log ID 1				so	rript ID 🚦	Created 1	Actions
	a6a9sac0-16e0-4609-	95ba-fe2067d19e1c			04	1b8541-9f7d-4faf-8fd1-9df183ce2cc0	07/01/2024 19:02:10	View
	8feca6a8-a3fc-48dd-t	b273-a04ta9235913			88	4dc900-dcbd-4889-a952-3!5b51854d5a	07/01/2024 16:24:26	View
	1b5e349e-57cd-4224	-b1e6-870a3c820fc9			64	0bb666-fa5f-4ebc-8e51-735bb6fa98c1	06/28/2024 16:50:58	View
	75ab1b75-d619-4b13	I-afe8-988714f5ac7a			12:	2a05a3-e451-4634-b6d3-ef53bd728a74	06/28/2024 16:30:47	View

Figure 29 – KeyScaler Control Panel – View Logs



youan Dashu	new manager of mouth a manager runder ** how roccess controler ** hog ocume cope ** helpons a how manager **	nop -	Tenant man +	aum
DEVICE L	OGS FOR IOT DEVICE 01			
LOGS				
Line	Detail			
1	sat_user			
2	total 124			
3	dmxxr-xr-x 23 root root 4096 Apr 25 19:16 .			
4	dmxxr-xx-x 23 root root 4006 Apr 25 19:16			
5	-rwwrwonwx 1 root root 12978 Apr 25 19:16 auth_test			
6	-nw-nw-1 root root 2404 Apr 25 19-16 auth_best.c			
7	drivsr-xr-x 2 root root 4098 Nov 17 2022 bin			
8	drivsr-xr-x 4 root root 4096 Nov 17 2022 boot			
9	drivsr-xr-x 15 root root 4080 Apr 24 13:53 dev			
10	-nw-nw-nu-1 root root 3714 Sep 17 2021 deviceCert.cert			
11	-nw-nw-nw-1 root 1675 Sep 17 2021 deviceKey.pem			
12	drwxr-xr-x 102 root root 4096 May 21 17:33 etc			
13	-nw-nw-1 root to 0 Apr 25 18:59 gcc_output bit			
14	drwxr-xr-x 6 root root 4096 Apr 24 13:53 home			
15	Invorvorvex 1 root root 32 Aug 11 2022 initrd img -> boot/initrd img-5.4.0-1089-azure			
16	Inversevence: 1 root root 32 Aug 11 2022 initrd img old -> boot/initrd img-5.4.0-1086-azure			
17	dmxr-xr-x 22 root root 4096 Nov 17 2022 lib			
18	drwxr-vr-x 2 root root 4096 Nov 17 2022 ib64			
19	drwx 2 root root 16384 Jan 21 2020 lost+found			
20	drwxr-vr-vt 2 root root 4096 Jan 21 2020 media			
21	drivsr-xr-x 3 root root 4096 Apr 24 13:53 mnt			
22	dmxr-xr-x 2 root root 4096 Jan 21 2020 opt			

Figure 30 – KeyScaler Control Panel – View logs of a specific Log ID



5 Application Uninstallation Process

To uninstall the SAT API application, double click the uninstall file:

L I 2 ↓ There Mar	KeyScaler Secure	Asset Transfer						- 0	×
Pine Poine Snate View App Pin to Quick Copy Paste access	Move Copy to to to to	ename New folder	Properties	Select all					
Clipboard	Organise	New	Open	Select					
\leftarrow \rightarrow \checkmark \uparrow \blacksquare > This PC > Windows (0)	C:) → Program Files → De	viceAuthority > KeyScaler Secu	re Asset Transfer			ٽ ~	Search KeyScaler Secure Asset Transfe	r	P
OneDrive - Device Authority Inc	^ Name	^ I	Date modified	Туре	Size		uninstall.exe	9	
This PC	dist	(01/07/2024 18:05	File folder			Application		
2D Objects	config.json	(01/07/2024 19:52	JSON Source File	1 KB				
J SD Objects	credentials.js	on	28/06/2024 16:46	JSON Source File	1 KB		NUMBER OF STREET		
Desktop	😥 DeviceAutho	rity - EULA.rtf	14/06/2024 14:42	Rich Text Format	167 KB				
at Documents	BeviceAutho	rity.ico	14/06/2024 14:42	lcon	15 KB				
🕂 Downloads	DeviceAutho	rity-Grayscale.ico	14/06/2024 14:42	lcon	15 KB				
👌 Music	6 KeyScaler_Se	cureAssetTransfer.exe	01/07/2024 19:47	Shortcut	3 KB		Date modified:	01/07/2024 18:05	
Pictures	🞯 uninstall.exe	(01/07/2024 18:05	Application	62 KB		Size:	61.4 KB	
Videos							Date created:	28/06/2024 16:44	
Windows (C:)									
Seagate Backup Plus Drive (E:) 8 items 1 item selected 61.4 KB	~								
- Figure 31 – Uninstall t	he SAT API o	application						Ľ	
5									

KeyScaler Secure Asset Transfer Uninstall	\times
Are you sure you want to uninstall KeyScaler Secure Asset Transfer?	
Yes No	

Figure 32 – Click 'YES' to continue the Uninstall of the application

left KeyScaler Secure Asset Transfer Uninstall: Uninstalling	_		\times
Delete file: C:\Program Files\DeviceAuthority\KeyScaler Sec	ure Asset Transfer\	dist\lib\tk\t	earc
Show details			
Nullsoft Install System v3.08			
	Close	Canc	el

Figure 33 – The SAT API App files start to get deleted from the system



stall	-		\times
	2		
	stall	stall —	stall — D

Figure 34 – Click on 'show details'

KeyScaler Secure Asset Transfer Uninsta	ill	-		\geq
Completed				
Completed				
Delete file: C:\Program Files\DeviceAutho	rity KeyScaler Sec	ure Asset Transfe	r\dist\i	^
Delete file: C:\Program Files\DeviceAutho	rity KeyScaler Sec	ure Asset Transfe	r\dist\li	
Delete file: C:\Program Files\DeviceAutho	rity KeyScaler Sec	ure Asset Transfe	r\dist\li	
Remove folder: C: Program Files DeviceA	uthority (KeyScaler	Secure Asset Tra	nster (d	
Delete file: C: Program Files Device Autho	rity KeyScaler Sec rity KeyScaler Sec	ure Asset Transfe	r (aist (i	
Remove folder: C:\Program Files\DeviceA	uthority\KeyScaler Sec	Secure Asset Transie	nefer\d	
Remove folder: C:\Program Files\DeviceA	uthority\KeyScaler	Secure Asset Tra	nsfer\d	
Remove folder: C:\Program Files\DeviceA	uthority KeyScaler	Secure Asset Tra	nsfer\d	
Completed				
				*
ullsoft Install System v3.08				
	< Pack	Class	Con	rol
		Giose	Cano	Jer

Figure 35 – Details of the files being uninstalled

This completes the uninstall process.



6 Appendix A – Create a HSM Signing Key

On KeyScaler CP, navigate to HSM Access Controller> Key Access Policies and create a new HSM Policy:

	Secure Repositories Key Access Policies	
DEVICE STATE SUMMARY	Key Management Manage HSM Policies Provision A Device	CONTROL P/
Total Registered	8	07/08/2024 16:30
Authorized	8	07/08/2024 14:47
Quarantined	0	07/08/2024 11:57
Blacklisted	0	07/08/2024 11:31

Figure 36- KeyScaler Control Panel – HSM Access Controller>Key Access Policies

In the sample below, a couple of policies are listed:

HARDWARE SE	CURITY MODULE POLI	CIES											
Name 1	Description	Encrypt	Decrypt	Generate	Delete	Import	Export	Rotate	Sign	Auto-rotate	Created O	Updated 1	Actions
QApy HSM Policy DC	QApy HSM testing Policy	All keys	All keys	Yes	All keys	Yes	All keys	All keys	All keys	Never	01/04/2024	01/04/2024	View Edit
	A 17 1 A 1 A 1 A 1 A 1 A 1 A 1 A 1 A 1 A	Manual Issue	Named Keys	Vac	This policy/s know	Vac	This policy/s know	This policy/s know	Named keys	Mauar	00/09/2022	12/18/2022	Manu I Edit

Figure 37- KeyScaler Control Panel – HSM Access Controller>Key Access Policies>List Policies

Click on **+New Policy** button to give a page as shown below:

MANAGE HARDWARE SECURITY MODULE POLICIES Create New Hardware Security Module Policy Policy Name * Policy Name • Policy Description Description Use Service Connector • Encrypt Not available • Description • Description • Description • Encrypt Not available • Description • Not available • Sign Not available Sign Not available Auto. Rotate every * 0 Days • Auto. Rotate every * 0 Days • Expont •	KeyScaler [™] Dashboard	Manage Devices - Manage Policies -	HSM Access Controller - KeyScaler Edge - Reports & Notification -	
Create New Hardware Security Module Policy Policy Name * Policy Name • Policy Description Description Use Service Connector	MANAGE HAS			
Create New Hardware Security Module Policy Policy Name * Policy Name • Policy Description Description Use Service Connector - Encrypt Not available • Decrypt Not available • Generate - Export Not available • Kotare - Sign Not available • Auto-Rotate every * 0 One on fulle * -	MANAGE HAP	DWARE SECORITY MODUL	E POLICIES	
Policy Name Policy Name Policy Description Description Use Service Connector Image: Connector Encrypt Not available Decrypt Not available Sport Not available Sign Not available Auto-Rotate every* Not available SIGN POLICY TO THESE DEVICE GROUP(S)	Create New	Hardware Security Module Po	licy	
Policy Description Description Les Service Connector Not available Encrypt Not available Decrypt Not available Delete Not available Import Not available Export Not available Sign Not available Auto-Rotate every* 0 SIGN POLICY TO THESE DEVICE GROUP(S) Hot available	Policy Name *		Policy Name	
Use Service Connector Instandade Encrypt Instandade Decrypt Instandade Generate Instandade Import Instandade Export Instandade Sign Not available Auto-Rotate every* Instandade SIGN POLICY TO THESE DEVICE GROUP(S) Instandade	Policy Descrip	ition	Description	
Encrypt Not available Decrypt Not available Generate Delete Not available Import Export Not available Rotate Sign Not available Auto-Rotate every* 0 Desse	Use Service C	onnector		
Decrypt Not available Generate Import Import Import Export Not available Sign Not available Auro-Rotate every* Import AssiGN POLICY TO THESE DEVICE GROUP(S) Import	Encrypt		Not available	
Generate Import Import Import Export Not available Rotate Not available Sign Not available Auto-Rotate every* Import SIGN POLICY TO THESE DEVICE GROUP(S) Import	Decrypt		Not available	
Delete Not available Import Import Export Not available Rotate Not available Sign Not available Auto-Rotate every* 0 Days ©	Generate			
Import Import Export Not available Rotate Not available Sign Not available Auto-Rotate every* Import Assign POLICY TO THESE DEVICE GROUP(S) Import	Delete		Not available	
Export Not available Rotate Not available Sign Not available Auto-Rotate every* 0 Assign Policy To THESE DEVICE GROUP(S)	Import			
Rotate Not available Sign Not available Auto-Rotate every* 0 Days C	Export		Not available	
Sign Not available Auto-Rotate every* 0 Days O	Rotate		Not available	
Auto-Rotate every * 0 Days ASSIGN POLICY TO THESE DEVICE GROUP(S)	Sign		Not available 🗸	
ASSIGN POLICY TO THESE DEVICE GROUP(S)	Auto-Rotate e	very *	0 Days 🖌	
	ASSIGN PO	LICY TO THESE DEVICE GR	OUP(S)	
Pavice Group(e) Policy recipient group	Device Cround	(e)	Policy recipient aroun	

Figure 38- KeyScaler Control Panel – HSM Access Controller>Key Access Policies> Create New Policy



This policy allows users to control what access and control can be given to devices. In this case, we need to give 'Sign' permissions, so fill in the form as shown in the example below:

ANAGE HARDWARE SECURITY MODULE POLICIE	ES
Edit Hardware Security Module Policy	
Policy Name *	SAT HSM Policy
Policy Description	SAT HSM Policy
Encrypt	Named keys 🗸
Keys for Encryption	x Cyberarl/Pair000001
Decrypt	Named keys 🗸
Keys for Decryption	x CyberarkPair000001
Generate	8
Delete	This policy's keys
Import	8
Export	This policy's keys 🗸
Rotate	This policy's keys 🗸
Sign	Named keys
Keys for signing	x CyberarkPair000001
Auto-Rotate every *	0 Days O
ASSIGN POLICY TO THESE DEVICE GROUP(S)	
Device Group(s)	(# SAT-Scripts-Group) (# SATDemoGroup)

Figure 39- KeyScaler Control Panel – HSM Access Controller>Key Access Policies> Create new Policy

The 'Named Keys' as shown, can be added later by editing the policy. For now, select the option 'This Policies Keys' from the pull-down menu for 'Sign'.

Next, navigate to HSM Access Controller>Key Management.

KeyScaler™ Dash	board Manage Devic	ces - Manage Policies -	HSM Access Controller +	KeyScaler Edge -	Reports & Notification -
			Secure Repositories		
MANAGE	HARDWARE S	ECURITY MODUL	Key Management Key Management Key Man	hagement	
Edit Ha	rdware Security	Module Policy			

Figure 40- KeyScaler Control Panel – HSM Access Controller>Key Management

In the sample below a couple of keys are already Listed. For generating a new HSM key, this can only be done by REST API, and not via the KeyScaler Control Panel as the key need to be tied to a specific device(s) that have registered with KeyScaler. For generating a Signing Key follow the HSM Generate Key Pair API documentation. In summary, the following inputs are required:

- Key Alias
- Type of Key, either RSA or EC
- Size of Key
- HSM Policy UUID

The HSM Policy UUID can be taken from the URL as highlighted below:



$\leftarrow \rightarrow$	C û	8 Not secur	re <u>https</u> ://ter	nant.mykeyscaler.c	om/cp/admin/hsm/po	licies/edit <mark>/ff346433</mark>	3-6cbb-447a-bc83-6d9a70619541/1	
	KeyScaler™ D	ashboard Ma	anage Devices -	Manage Policies -	HSM Access Controller +	KeyScaler Edge -	Reports & Notification ~	
	MANAG	GE HARDV	WARE SECU		POLICIES			
	Edit I	Hardware S	Security Mod	lule Policy				
	Polic	y Name *			SA	FHSM Policy	Θ	
	Polic	y Description	1		SA	FHSM Policy		

Figure 41Key – Scaler Control Panel – HSM Access Controller>HSM Policy UUID

Then refresh this page to view the new key.

KeyScaler™ Dashboard Manage Devices - Manage Policie	s - HSM Access Controller - I	KeyScaler Edge - R	ports & Notification -				Help -	Tenant main
HARDWARE SECURITY MODULE KEYS	1							
Alias	Key Pair	Key Size	Version	Policy 1	Last Rotated Date O	Active	Actions	
RSAKey01ForEncryption	true	2048	0	SAT HSM Policy	12/18/2023	true	Export	Delete
CyberarkPair000001	true	2048	0	SAT HSM Policy	09/08/2022	true	Export 1	Delete

Figure 42- KeyScaler Control Panel – HSM Access Controller>List Keys

This completes the HSM Key Generation.



Appendix B – Create a new FreeMarker Service Connector

On KeyScaler CP, navigate to Tenant Main> Manage Service Connectors:

KeyScaler™ Dashboard Manage Devices - Manage	HSM Access Controller - KeyScaler Edge - Reports & Notification -	Help - Tenant mai
MANAGE KEYSCALER SYNCHRON	DUS ASSET TRANSFER POLICIES	Account Settings Customer Account Logo Manage KeyScare Certificate Authorst Manage KeyScare Certificate Authorst
Edit Synchronous Asset Transfer Po	icy	ref Manage Notifications & Reports
Policy Name *	SAT Policy	Manage Users Ar Manage Customer Accounts Manage Authorization IDs Manage Authorization IDs
Policy Description	CyberArk test	S Manage Key Hotation
Timeout (ms) *	900000	Ber - Vesse Vanage DAE API Settings 國 Manage Device Attribute Feed
Signing Key *	CyberarkPair000001	

Figure 43- KeyScaler Control Panel – Manage Service Connectors

Next, click on **+Add New**, to create a new service connector:

MANA	GE SERVICE CONNECTORS TENANT MAIN			
	Drofile Name +	Service Drovider	Date Created 1	Actions
	FreeMarker Template Connector	Other Template	09/08/2022 10:45:48	View Edit Delete
				Add New Sync Services

Figure 44- KeyScaler Control Panel – Manage Service Connectors>List Connectors

This will provide a form to fill-in with the service connector details.

SERVICE CONNECTORS			
New Service Connector Pr	ofile		
Service Provider			
Other Template	\sim		
The following information is used to con	nect to the service provider.		
Profile Name			
Key			
Value	x	+	
URL			
Custom API Secret			
Service Connector Uses TLS			

Figure 45- KeyScaler Control Panel – Manage Service Connectors>Create New Connector

A sample form is provided below:



SERVICE CON	INECTORS				
Edit Service Co	nnector Profile	9			
Service Provider					
Other Template	~				
The following information	on is used to connect	to the service pr	ovider.		
Profile Name					
FreeMarker Ter	nplate Connector				
URL					
http://localhost:	8082/sc				
API Secret					
		•			
Show Characte	ers				
Service Connect	or Uses TLS				

Figure 46- KeyScaler Control Panel – Manage Service Connectors>Create New Connector

- Service Connector: Select Other Template
- Profile Name: Free text for the service connector name
- URL: The URL of where the FreeMarker Service Connector¹ application is deployed. This could be the same VM as KeyScaler System, in which case use local host, as shown above.
- **API Secret**: This is used by the Service connector to authenticate to KeyScaler System. You can use your own API Secret, however, leaving it blank and saving, KeyScaler will generate one automatically for you.
- Service Connector Uses TLS: This should be enabled for Production Systems. When enabled, enter the service connector TLS certificate in the pop-up text field:

Profile Name FreeMarker Template Connector URL http://tocahosts 8082/sc Street Canacters S	Server Authentication (potional) The following information is used to connect to the service provider. The following information is used to connect to the service provider. Full enabloundaries. To disable leave blank.	
Service Connector Less TLS	Somer Authentication (grinder) The following information is used to connect to the service provider. The following information is used to connect to the service provider. The tablound antem To disable leave starts. The tablound antem To disable leave starts.	
Profile Name FreeMarker Template Connector URL http://localhost.8082/sc API Secret Service Connector Liss		
FreeMarker Template Connector URL http://locathost.8082/sc API Secret Stroic Charactere Storic Charactere Storic Charactere Storic Charactere Storic Charactere	Profile Name	
URL http://localhost.8082/sc API Secret Store Characters	FreeMarker Template Connector	
http://localhost.8082/sc API Secret Sthow Charactere Stroke Charactere		
API Secret Stow Charactere Service Connector Uses TLS	http://localhost.8082/sc	
Service Connector Uses TLS	API Secret	
Stow Characters Service Connector Uses TLS		
Service Connector Uses TLS	Show Characters	
	Service Connector Uses TLS	
	⊴←	

Figure 47 – KeyScaler Control Panel – Manage Service Connectors>Create New Connector> Enable TLS

Next, click on **Save** button to complete the service connector configuration.

¹ For any question and support on the connector, please contact <u>cyberarkcustomer@deviceauthority.com</u>



7 Appendix C – Create a new SAT Policy

To create a new Secure Asset Transfer Policy, login to KeyScaler CP and navigate to Manage Policies>Synchronous Asset Transfer Policies, as shown below:

KeyScaler™ Dashboard	Manage Devices 👻	Manage Policies 👻	HSM Access Controller	- KeyScaler Edge -	Reports & Notification -	
DEVICE STATE	SUMMARY	Agent Crypto P Automated Pas KeyScaler Issu	olicies sword Policies ed Certificate Policies olicies		Provision A Device	CONTROL PANE
Total Registered		C Authentication I	Policies Policies sset Transfer Policies		8	07/08/2024 14:47:17 07/08/2024 11:57:04
Quarantined Blacklisted			Manage	Synchronous Asset Transf	er Policies	07/08/2024 11:31:27 07/02/2024 15:44:03
RECENT EVEN	rs				_	
07/08/2024 14:46:41	lot Device 01		Successful device aut	horization	Device	Authenticated and Authorized

Figure 48 – KeyScaler CP> Manage Policies > SAT Policies

Next, click on +New Policy Button:

SYNCHRONOUS ASSET TRAN	ISFER POLICIES						
Policy Name 1	Policy Description	Transfer Timeout	HSM Key	SAC Hostname	Date Created 1	Date Updated 1	Actions
Nirmal_SAT_Policy_Non_MQTT_SAC	Nirmal_SAT_Policy_Non_MQTT_SAC	360000	CyberarkPair000001	http://localhost.8081/	10/03/2023 10:40:30	10/05/2023 17 42 43	View Edit /
NirmalSATPolicy (separate sac-mqtt)	NirmalSATPolicy	360000	CyberarkPair000001	http://51.140.81.51.8081/	09/27/2022 09:05:15	12/02/2023 19:25:51	View Edit I
RAT Bolieu	Cubardak Inst	900000	Cuberark/Pair000001	http://jocalhost.8081	09/08/2022 11 22 29	12/06/2023 10:02:30	View 1Edit 11

Figure 49 – KeyScaler CP> Manage Policies > SAT Policies> Create New Policy

Fill in the SAT Policy form as shown in the example below, selecting the signing key generated in Appendix A and Template Service connector from Appendix C from the pull-down menus:

	KeyScaler [™] Dashboard	Manage Devices 👻	Manage Policies 👻	HSM Access Controller -	KeyScaler Edge –	Reports & Notification -
	MANAGE KEY	SCALER SYNG	CHRONOUS AS	SET TRANSFER F	OLICIES	
	Edit Synchro	nous Asset Trar	nsfer Policy			
	Policy Name *			SAT Policy		Θ
	Policy Description Timeout (ms) *			CyberArk tes	t	
				900000		Θ
	Signing Key *			CyberarkPa	ir000001 •	• •
	SAC Hostname	•		http://localho	st:8081	Θ
	Template Servi	ice Connector		FreeMarker	Template Connec 🔹	~ 0

Figure 50 – KeyScaler CP> Manage Policies > SAT Policies> Fill in New SAT Policy form

For SAC Hostname², this could be hosted on the same VM as KeyScaler, in which case enter local host, as shown above.

² For any question and support on SAC Hostname, please contact <u>cyberarkcustomer@deviceauthority.com</u>



Click on the '?' to get additional help for each field, for example for Timeout (ms)

Policy Description	CyberArk test		
	000000		Timeout (ms)
Timeout (ms) *	90000		Timeout for asset transfer in milliseconds.
Signing Key *	CyberarkPair000001	0	

Figure 51 – KeyScaler CP> Manage Policies > SAT Policies> Popup Help for filling in SAT policy form

Click on Save Policy, to complete the SAT policy set up. Next, view the policy, just created:

HSM Key	SAC Hostname	Date Created 1	Date Updated 1	Actions
CyberarkPair000001	http://localhost:8081/	10/03/2023 10:40:30	10/05/2023 17:42:43	View Edit Delete
CyberarkPair000001	http://51.140.81.51:8081/	09/27/2022 09:05:15	12/02/2023 19:25:51	View Edit Delete
CyberarkPair000001	http://localhost:8081	09/08/2022 11:22:29	12/06/2023 10:02:30	View Edit Delete
			New Policy	Manage SAT Scripts

Figure 52 – KeyScaler CP> Manage Policies > SAT Policies>View Policy

And make a note of the SAT policy UUID, highlighted below, this will be needed for the SAT API application.

C 🕅 O Not secure https://ten	ant.mykeyscaler.co	om/cp/admin/policies/	sat/detail <mark>/b127ba</mark>	96-3057-496b-a2c0-61188c5d1297/1
KeyScaler [™] Dashboard Manage Devices →	Manage Policies +	HSM Access Controller -	KeyScaler Edge -	Reports & Notification ~
VIEW SYNCHRONOUS ASSE	T TRANSFER I	POLICY		
View SAT Policy				
Policy Name		SATI	Policy	
Policy Description		Cybe	rArk test	
Timeout (ms)		9000	00	
Signing Key		Cybe	rarkPair000001	
SAC Hostname		http://	localhost:8081	
Template Service Connector		Free	Marker Template Conne	ector

Figure 53 – KeyScaler CP> Manage Policies > SAT Policies>SAT Policy UUID



8 Appendix D – SAT Scripts Configuration

On KeyScaler CP, from the SAT Policy list Page, click on the **Manage SAT Scripts** button:

SYNCHRONOUS ASSET TRANSI	FER POLICIES						
Policy Name 1	Policy Description	Transfer Timeout	HSM Key	SAC Hostname	Date Created 1	Date Updated 1	Actions
Nirmal_SAT_Policy_Non_MQTT_SAC	Nirmal_SAT_Policy_Non_MQTT_SAC	360000	CyberarkPair000001	http://localhost.8081/	10/03/2023 10:40:30	10/05/2023 17:42:43	View Edit Dek
NemalSATPolicy (separate sac-mgtt)	NirmalSATPolicy	360000	Cyberark/Pair000001	http://51.140.81.51.8081/	09/27/2022 09:05:15	12/02/2023 19:25:51	View Edit Dei
SAT Policy	CyberArk lest	900000	CyberarkPair000001	http://localhost.8081	09/08/2022 11:22:29	12/06/2023 10:02:30	View Edit Dele

Figure 54 – KeyScaler Control Panel> Manage SAT Policy>Manage SAT Scripts

Next Click on +New Script, to give the following form to fill-in for the script set up:

KeyScaler [™] Dash	board	Manage Devices -	Manage Policies	HOM Access Controller	- Keyficaler Edge -	Paparta & NetKozón -	Halp - 1	Tenant main -	admin@devicea
MANAGE	EKEYS	CALER SYN	CHRONOUS	ASSET TRANSFER	SCRIPTS				
Create	New S	ynchronous A	sset Transfer	Script					
Script N	lame *				Script Name	0			
Script D	escriptio	in			Description				
OS Type					Any	v			
Script P	lacehold	ers							Ŀ
Script *									ŀ
ASSIG	N SCR	IPT TO THES	E DEVICE GR	ROUP(S)					
Device 0	Group(s)				Script recipient	pro 0			
							c	ancel Cre	ate Script

Figure 55 – KeyScaler Control Panel> Manage SAT Policy>Manage SAT Scripts>New Script

Fill in the form as shown in the example below, for list script.



KeyScaler™ Dashboard Manage	Devices • Manage Policies •	HSM Access Controller	KeyScaler Edge 👻	Reports & Notificatio	n •			
MANAGE KEYSCALE	R SYNCHRONOUS A	SSET TRANSFER	SCRIPTS					
Edit Synchronous As	sset Transfer Script							
Script Name *			list		0			
Script Description			basic director	listing and echo use				
OS Type			Linux	~				
Script Placeholders			['user', 'path']					
Script *			echo \${user} Is -al \${path} # which ssh					
ASSIGN SCRIPT TO	THESE DEVICE GRO	OUP(S)						
Device Group(s)			× SATDemoGr	oup				

Figure 56 – KeyScaler Control Panel> Manage SAT Policy>Manage SAT Scripts>New Script for List

- Script Name: Free text field to enter a name for the script
- Script Description: Free text field to enter the description of what the script does
- **OS Type**: Pull down list of the supported OS where the script can be executed, e.g. Linux
- **Script Placeholders**: The script fields to be substituted by the service connector from the data model defined in the SAT API.
- Script: The script itself to be executed on the device via the SAT API.
- **Device Group(s)**: The Device Group (whose devices) have permission to have these scripts executed on them.

Click the **Save** button to complete the script configuration.

----- End of Document