Seqrite Endpoint Security 8.2

Steps to Apply SP

www.seqrite.com

Copyright Information

Copyright © 2008–2024 Quick Heal Technologies Ltd. All Rights Reserved.

No part of this publication may be reproduced, duplicated, or modified in any form or incorporated into any information retrieval system, electronic or any other media or transmitted in any form without prior permission of Quick Heal Technologies Limited, Marvel Edge, Office No.7010 C & D, 7th Floor, Viman Nagar, Pune 411014, Maharashtra, India.

Marketing, distribution or use by anyone barring the people authorized by Quick Heal Technologies Ltd. is liable to legal prosecution.

Trademarks

Seqrite and DNAScan are registered trademarks of Quick Heal Technologies Ltd. while Microsoft and Windows are registered trademarks of Microsoft Corporation. Other brands and product titles are trademarks of their respective holders.

License Terms

Installation and usage of Seqrite Endpoint Security is subject to user's unconditional acceptance of the Seqrite end-user license terms and conditions.

To read the license terms, visit <u>http://www.seqrite.com/eula</u> and check the End-User License Agreement for your product.

Contents

Overview	2
Execution Flow	2
What does SP 1.0 Contain?	.2
	`- ``
Prerequisites	3
Steps to Apply the Patch	3
Application of Infra Service Pack 1.0	4
Apply SP Manually	. 5
Apply SP Automatically	.8
	Execution Flow What does SP 1.0 Contain? Prerequisites Steps to Apply the Patch Application of Infra Service Pack 1.0. Apply SP Manually

Overview

EPS 8.2.1 release includes the BitLocker Encryption feature which will be applicable for EPS 8.2 and delivered as a bundle via Infra Service Pack.

Execution Flow



What does SP 1.0 Contain?

The service pack comprises the following items:

Policy Encryption

- eps.war
- cs-pushdata.war
- cs-pushaction.war
- cs-consumer.jar
- localization json file
- epscloudapi.property file
 - o qh.epscloud.requestConnectionTimeout=180000
 - Mongo url Quartz password encryption.
 - Property Name: qh.platform.quartz.scheduler.jobStoreMongoUri

Help Content

Policy Encryption

Health Monitor

• Code for restarting consumer in case of policy pending issue.

Location:

/opt/Seqrite_EndPoint_Security/health_monitoring/health_monitoring_distributed_file /<u>communication.sh</u>

Database Mongo

NA. Only SP specific collection changes

Redis

Code change for resolving critical vulnerability.

Prerequisites

Apply a patch script, **servicepack.sh** before applying SP 1.0. The purpose of applying this patch is to enable Infra SP.

Steps to Apply the Patch

To apply the patch, follow these steps:

- Go to the following path to get the SP 0.1 patch <u>http://download.quickheal.com/builds/seqrite/82/en/build</u>/ctrldservicepack/sp01/servi cepack.sh
- 2. Login to the server machine as root user.
- 3. Place this **servicepack.sh** script into server machine /opt/ directory.
- 4. Open terminal or console and go to **/opt/ directory** from console and type **bash servicepack.sh** command and hit [Enter].



5. Once you hit [enter], the script executes. It takes around three to four minutes to complete the execution.

You can check the execution status of patch script by checking logs present at the following location: **/opt/Seqrite_EndPoint_Security/log/SP_Logs.txt**

Note: In case of any failure, the script will roll back itself. No human intervention is required. Same can be checked in Rollback logs:

/opt/Seqrite_EndPoint_Security/log/SP_Rollback.txt

- 6. Now, you can verify whether the patch has been applied by checking the logs and also by accessing the database.
 - a. Before accessing the mongo db by robo-3t or studio-3t, run this command to disable the authorization.

sed -i -e 's,authorization: enabled,authorization: disabled,g' /etc/mongod.conf systemctl restart mongod

- b. Now access the mongo db by using host IP [for eg:- 172.18.14.100]
- c. Go to global collection > server information and check **spv =0.1**. We can assure that patch has been successfully applied.



Application of Infra Service Pack 1.0

There are two ways to apply the SP:

Apply SP Manually

- Access following path to get the SP 1.0 <u>http://download.quickheal.com/builds/seqrite/82/en/build/ctrldservicepack/sp10/servicepack/servicepack/sp10/servicepack/servicepack/sp10/servicepack/service</u>
- 2. Login to server machine as root.
- 3. Place this **servicepack.sh** SP script into server machine.
- Copy servicepack.sh file to /opt/Seqrite_EndPoint_Security/deployment/clientpackager/servicepack/server/ folder [If server folder does not exist then create it and place the servicepack.sh]
- 5. Assign permission 644 to servicepack.sh file [chmod 644 servicepack.sh]
- 6. Go to */opt/Seqrite_EndPoint_Security/deployment/clientpackager/servicepack/* folder and assign permission 644.
 - a. Edit servicepack.json
 - b. change "sspv": "0.1" to "sspv": "1.0"
 - c. Save it.



7. The json file looks like:



- 8. Execute **bash servicepack.sh** from terminal/ console from this path: /opt/Seqrite_EndPoint_Security/deployment/clientpackager/servicepack/server/
- 9. Once the user executes the command then human interaction is not recommended. Here is the successful execution snap:



- 10. Wait for the installation successful or rollback message.
- 11. If a rollback message is displayed, it indicates that the Service Pack was not applied due to errors. In such cases, the Service Pack will initiate contingency measures to restore the server to its original state.
- 12. You can check the execution status of SP script by checking logs present at this location: /opt/Seqrite_EndPoint_Security/log/SP_Logs.txt

Note: In the event of any failure, the script will automatically initiate a rollback process. [No human intervention is required]. Same can be checked in Rollback logs: /opt/Seqrite_EndPoint_Security/log/SP_Rollback.txt

- 13. You can verify whether the patch has been applied by checking the logs and also by accessing the database.
 - a. Before accessing the mongo db by robo-3t or studio-3t, run this command to disable the authorization.
 sed -i -e 's,authorization: enabled,authorization: disabled,g' /etc/mongod.conf systemctl restart mongod
 - b. Access the mongo db by using host IP [for example: 172.18.14.100]
 - c. Go to global collection > server information and check **spv =1.0.** The patch has successfully been applied.

Studio 37 Free for MongoDB					
e Edit Database Collection index Document Vere 	Help wethout Ward More?				
A	intellShell DS_x × IntellShell DS-149 × IntellShell DS-149 × IntellShell DS-149 × IntellShell DS_x × IntellShell DS_x × IntellShell DS_x				
> Et tenantiele *	5 112.18.18.20027017 > 🕞 gener				
5 (3) turning(00) 5 (3) uar 5 (3) uar juntimencis 5 (3) uar juntimencis 5 (3) uar juntimencis (3) System (1) 1) Years (1)	Image: Second				
	<pre></pre>				

d. Same can be verified by accessing server console on login page.

O Test answer (Ampril /172.18.14.100/spr	utopin			÷ 0 0
Child D Sever Lage				
	We have updated our Privacy Pully as a	Pjan 14, 3121. If you commute to		
	our services after set 15, 2021, you will Privacy Policy.	in descend to have accepted the		
	SECT	TE		
	Sign into your Se	oprite account		
	Drug (D			
	Research	+		
		- M		
	Perget Passare P			
and provide formation (Target	nanana (magney) agenesi			Segurar Endpoint Security 8.2.1.6
- C O Sature Manuf	Art partment Missoy Marty Supp Antone		Terter	Segura Sedgeson Security 82118
 Contraction of the second secon	nd contenen Misso Pring segnitations TETA NOVeptypp/Anthones		1000	Sequite Endpoint Security 1.2.1.0
+ C • Notice • Interview + C • Notice • Interview Values laps • O file • Interview • Second • • S	nd particuré Minag Yoly supp Solices 18:54-300 (spalage) Adultion of m		maar maare quit Bygensteen = A	Segura Endjanos Security 1.21.0 (* 0) 0
+ C • Not seen in the office of the office o	nd conterne frivacy frank segn factore TE 54 X00 (spc) (spc) (deathins and provided Scott)		neuro qui departante - A	Septer Industri Society 2008 vi Cli C L C. A- El C
Constant interesting of the second seco	nd containte 1 Million Maring 1 Junge Saltone. 18 54-300 kept tege (deaththeard) m 19 Million South Contained	0 ×	Tencine apid.29poperations or 4	Septe Folgers Socray 1311
+ C International Internation	Ad cardwork Minag Yong sope Solices III 54 500 hps/spp/Additionant m spenness South C Connected Endpoints Last Connected	0.X	ansare spall drygenations in A Annual Strygenations in A Annual Strygenations (Constanting (Constanting) (Constanting) (Constanting)	Septe Legen Soury 1318
C Materia Marcal Trees	Ad containes () Minacy Mary () supplications TR 54-300(Next/Spp)(Additionant) P P P P P P P P P P P P P	•.×	Server and Department of A	Septe Intern Tour 1911
A set of the transmission of the set of the set of the transmission of the set of t	Ad contained Privacy Table Suppr Safetion TR 54-300/Hps/rapp/dat/files/and Privacy Safetion S Suppr Reported C Connected Environment Safetion Safetion C Connected Environment Safetion C Connected Environment C C C Connected Environment C C C C C C C C C C C C C C C C C C C	• ×	encore epoil.25/poperations = .4 Another Pool 1 and the speed (Training Pool 1 and the speed	Segue Logens Socrey 1316
	Ad conductini Minacy Tribuy Suppr Subtract ISE SA 2000 Input page/Admitteriant ISE SA 2000 Input page/Admitteriant ISE SA 2000 Input page Admitteriant ISE SA 2000 Input page Admitteriant	0.×	secon epol 20 years and a proto Part of the Say and a proto Part of the	Segure Solgers Source 1318
Province Services of Services Province Services Service Services	At container Marcy Yotay supprisings TR 54.500(keps/spg)(AastHonerd P Revealed South Convected Trefpoints Care Convected Trefpoints Care Convect	0.×	encore and dependence of a second and dependence of a second and dependence of the second and the second and the second second and the second and the second and the second and the second and the second and the second and the second	Segure Logens Secury 1318
Construction of the second secon	Ad conducting Marco Tables Suppr Safetion IN 54-500 Paper page (deal thinking) IN 54-500 Paper page	0 ×	teners end Dependence + 4	Segular Endpaires Encourty 2011 (*) (2) (*) (*) (*) (*
A Constraint of the second secon	Ad contained Privacy Telay Surger Salaton III: La 2000/epin/app/dat/filesand III: La 2000/epin/app/dat/filesand Connected Environment Connected Environm	0 × 1944 (0) 1944 (0) 1944 (0) 1944 (0)	encore and Directore and A	Singhie Kolganie Society 2018
Province Services and Services Province Services Service Services Services Service Services Service Services Service Services Service Services Service Services Services Service Services Se	Ad cardwork Minag Ming supp Salina III 14 300 kps/sps/Adm/Minage Revealed South Conversion State Conversion Stat	0 × 100 1 feer (0) 6 dege (0) 8 dege (0)	encore and Dependence of a second and Dependence of a se	Segure Lobjert Secury 1318

Apply SP Automatically

- 1. After patch [servicepack.sh] is applied to system, edit **epscloudapi.properties** in /opt/Seqrite_EndPoint_Security/config/.
 - a. Edit epscloudapi.properties.
 - b. Change

qh.epscloud.cdnServerUrl=<u>http://download.quickheal.com/builds/seqrite/82/en</u>/build/ to

qh.epscloud.cdnServerUrl=<u>http://download.quickheal.com/builds/seqrite/82/en/build</u>/ctrldservicepack/sp10/ [This url used for local testing & can be used for controlled SP].



2. The epscloudapi.properties file looks like this:



- After making changes in properties, redeploy the eps war from /opt/Seqrite_EndPoint_Security/wildfly/standalone/deployments/
- 4. Steps to redeploy eps war:
 - a. Remove the existing eps.war.deployed or from console [rm eps.war.deployed]



b. Now after refresh remove eps.war.undeployed also or from console [**rm** eps.war.undeployed].



Now, upon refreshing, you should be able to observe that eps.war is deploying.



c. Please wait for some time. You will notice that eps.war has been deployed.



5. Make sure that serivepack.json with "sspv": "1.0" is uploaded at: http://14.141.38.197:8765/qaupload/jitendra/epsng8.2/ SP.



5. Now access mongo db from Robo 3T and go to global > quartz_triggers and trigger the Cron named Keyname > **CheckUpdateTrigger**.

	Pleast open connections (Cbi+P) at	Quickstart	serverinformation	serverleformation	+ quetz_bigges	< quartz_triggers ×			
> By BissandboulConfigSetting: > > By genericRyportBass > > By gelobal_polois > > By collastion >) 🔂 filesandboxConfigSettings 🗠	15 db147 (172.19 100.147.27017) >							
	> 56 global_policies	⊳ Run •	Load query	Save query -	Oury history	Erset default query 👻 🔒	Copy Paste	Q Al Helper (TVsual Query Build	ł.
	> (ii) localization > (iii) cnDemandAppOt/Settings	Query ~	0						ŝ.
	Projection	0			Sort 0		1	Ϊ.	
	Skip				Umit				
	> onDemandVulScnSettings	Result Qu	ery Code Explain						
	> 🔂 esinto	0 1-	e− → → [50		Documents 1 to 26	66628 2 8		Table View 👻 🕄 Customize view 🛡	
> (g) p3pconfig) (g) packager_delete_info	> (ji) popconfig > (ji) packager_delete_info	quartz_	triggers > keyName						
Wy resour) filt prins, compatible, ver) filt quartz_celenders) filt quartz_jobs	artz impl	description	endTime Invit	finalFireTime	feeinstanceid ruit ruit ruit	jobid 65:0359:d97:08 65:c1359:d97:08	keyName	2
	> 🗟 quartz_locks > 🗟 quartz_schedulers	artzimpl		lun 🗌	Ind	In rul	(iii) 65ct359d97c08	ManageGdprStatusTrigger	i.
2	✓ (i) quartz_biggers	artz impl	Dat	E nul	E null	D nut	LEE 65cf359d97c08_	ManagelleactivateLicenseEeysTripger	1
Operation	> III indexes (2)	artz impl.	E mil	E muñ	El null	in rul	G 65ct359d97c08	EpsManageBaseIneRoFalkarCasesT	
	> B reportFilterCategories	artz.hopd.	Ind .	I null	D null	ind.	10 65ct359d97c08_	CheckUpdateTragger	
	> B sequential sequences	utrimed K	[] ad	Clad	[] nul	- Ded	1771 65e1359e92e08	The Interior Securities files fiscar	1
	· Characteria V	1.45	comment subsetset					Court Documents () on connects	ŝ

6. After the cronjob is triggered, it will compare servicepack.json file on machine and one on cdn and after finding latest on CDN it will create a folder name server at this location: /opt/Seqrite_EndPoint_Security/deployment/clientpackager/servicepack/



7. The ServicePack file gets downloaded in this folder.



- 8. After downloading the ServicePack, it automatically executes the ServicePack.
- You can check the execution status of SP by checking logs which is present in following location:

/opt/Seqrite_EndPoint_Security/log/SP_Logs.txt

- 10. Now you can check the SP is applied on logs and also can verify by accessing DB.
 - Before accessing the mongo db by robo-3t or studio-3t, run following command to disable the authorization.
 sed -i -e 's,authorization: enabled,authorization: disabled,g' /etc/mongod.conf systemctl restart mongod
 - b. Now access the mongo db by using host IP [for example: 172.18.14.100]
 - c. Now go to global collection > server information and check **spv =1.0.** The patch has been successfully applied.



d. Same can be verified by accessing server console on login page.



Note: In the event of any failure, the script will automatically initiate a rollback process. /opt/Seqrite_EndPoint_Security/log/SP_Rollback.txt