DLP-WATERMARK SERVICE PACK [V8.3.3]

INSTALLATION GUIDE

Contents

1. Introduction	2
1.1 Overview of the DLP Watermark Feature	2
1.2 Service Pack (SP) v8.3.3 Contents and Requirements	2
2. Pre-Requisites	2
2.1 VDB Requirements	2
2.2 DLP Watermark Policy	2
2.3 License Key	2
2.4 Server-Side: Service Pack Installation	2
3. Compatibility	2
3.1 Supported Client OS and Versions	2
3.2 Supported Microsoft Office Versions	3
4. Watermark Feature for EPS, EPP, and Offline Customers	3
4.1 EPP v8.3 Customers	3
4.2 EPS v8.2 Customers	3
4.3 EPS v8.1 Customers	3
4.4 Offline Customers	3
5. Service Pack (SP) Installation Steps	3
5.1 Downloading and Preparing the SP Script	3
5.2 Executing the SP Script	4
5.3 Post-SP Execution Validation	4
6. Post-SP Installation Steps	5
6.1 Configuring Watermark Policy	5
6.2 Verifying License Assignment	5
6.3 Confirming Policy Application on Clients	5
6.4 Viewing the Watermark Feature under Policy > Data Loss Prevention	5
7. Rollback and Reinstallation	5
7.1 Rollback Scenarios	5
7.2 Reapplying the SP After Rollback	6
8. Troubleshooting – Client Side	7
8.1 Common Issues and Solutions	7
8.2 CPU Spike on Client-Side During Bulk Data Watermarking	12

1. Introduction

1.1 Overview of the DLP Watermark Feature

The DLP (Data Loss Prevention) Watermark feature helps protect sensitive data by embedding a watermark in Microsoft Office files (Word, Excel, PowerPoint). This prevents unauthorized redistribution of these files and provides a mechanism to trace potential leaks.

1.2 Service Pack (SP) 8.3.3 Contents and Requirements

- Wars:
 - eps.war
 - cs-pushdata.war
 - cs-pushaction.war
 - cs-consumer jar
- Help: Latest help documentation
- No client builds included
- SP Size: 606 MB
- Required Disk Space: 4 GB on the server before downloading
- Service Pack (SP) Compatibility: Specific to EPP v8.3 server

2. Pre-Requisites

2.1 VDB Requirements

Ensure that the client is running **VDB 4th December 2024 or later**. A system restart is required after updating the VDB.

2.2 DLP Watermark Policy

Apply the DLP watermark policy after the system restart to ensure the feature is active.

2.3 License Key

The DLP watermark flag must be enabled in the license key.

2.4 Server-Side: Service Pack Installation

The **Service Pack (SP)** should be installed on the server-side. Both the **Site Servers** and the **Control Centre** must have the Service Pack installed.

3. Compatibility

3.1 Supported Client OS and Versions

- Supported Operating Systems:
 - Windows 10 (32 & 64 bit)
 - Windows 11
 - Windows Servers: 2016, 2019, 2022 Note: •

Watermarking is not supported by WPS Office, LibreOffice, Office 365, or OpenOffice.

3.2 Supported Microsoft Office Versions

The watermarking feature is compatible with:

- Microsoft Office 2021 (Version 16.0.14332.20791)
- Microsoft Office 2019 (Version 16.0.18129.20116)
- Microsoft Office 2016 (Version 16.0.9029.2167)

4. Watermark Feature for EPS, EPP, and Offline Customers

4.1 EPP v8.3 Customers

• Apply this Service Pack directly as instructed in #3.

4.2 EPS v8.2 Customers

- First, upgrade to EPP v8.3.
- Apply the SP after the upgrade.

4.3 EPS v8.1 Customers

- Backup the EPS v8.1 system.
- Install EPS v8.2.
- Restore the EPS v8.2 backup onto the EPS v8.2 server.
- Then <u>upgrade to v8.3</u>.
- Apply the SP after the upgrade.

4.4 Offline Customers

• Use the separate offline tool for watermark functionality.

5. Service Pack (SP) Installation Steps

5.1 Downloading and Preparing the SP Script

 Download the Script: You can download the "SP – Endpoint_Protection_8_3_3.sh" script from the following location:
 Path: <u>http://download.quickheal.com/builds/seqrite/83/en/build/sp/watermark/Endpoint_Prote</u> ction 8 3 3.sh

MD5: 49aae7e9009a138da6b518770ffe23af

2. Create a Service Pack Folder:

• Execute the command mkdir servicepack to create the "servicepack" directory at the following path

opt/Seqrite_EndPoint_Security/deployment/clientpackager

3. Place the Script: Download and place the above Endpoint_Protection_8_3_3.sh file in

the servicepack directory.

5.2 Executing the SP Script

 Navigate to the servicepack folder and run: bash Endpoint_Protection_8_3_3.sh



5.3 Post-SP Execution Validation

After successful execution, check the following:

 MongoDB Collection: The serverinformation collection should include the entry: "spv": "3.0". (global > collections > server information)

```
{
    "_id" : ObjectId("6718ef238576cc585cb6b67d"),
    "epsVersion" : "8.3",
    "installationType" : "InstSingle",
    "thirdPartyVersion" : {
        "java" : "1.8.0_242",
        "mongodb" : "4.2.5",
        "zookeeperVersion" : "3.4.14",
        "kafka" : "2.3.0",
        "wildfly" : "16.0.0"
    },
    "spv" : "3.0"
}
```

- 2. The telemetryInfo Collection within the "sqepsng80" collection should contain:
 - "spMode": 1``"spMode": 1
 - "spDownload": 1``"spDownload": 1
 - "spVersion": "3.0"``"spVersion": "3.0"
 - "spFailReason": "SSP_3.0_Is_Completed"``"spFailReason":
 "SSP_3.0_Is_Completed"

6. Post-SP Installation Steps

6.1 Configuring Watermark Policy

- After the SP installation:
- 1. Go to **Policy** \rightarrow **Data Loss Prevention** on the server UI.
- 2. Apply the watermark policy to the desired client endpoints.

6.2 Verifying License Assignment

3. Ensure the **DLP license** is assigned to the client in the **Status** section.

6.3 Confirming Policy Application on Clients

4. Check the **Applied Endpoints** list to confirm the watermarking policy is applied successfully.

6.4 Viewing the Watermark Feature under Policy > Data Loss Prevention

5. After completing step 3, you will see the watermark feature listed under Policy > Data Loss Prevention in the server web console.

Policy > Policy Settings		
IDS/IPS	Report only Block and Report Custom Watermark	
Firewall	Apply watermark to documents shared via Network Share and Removable Data Transfer Channels. Note: Watermarking is supported on Windows 10, Windows Server 2016	e Devices. To enable watermark, go to and later versions.
Web Security	Enable Watermark (j)	
Application Control	Orientation Diagonal Horizontal	Orientation Preview
Advanced Device Control	Timestamp, IPaddress, MACID, Hostname, Username, Ente 💌	
Data Loss Prevention	Gray 👻	A CONTRACTOR OF
	File types * .docx, .xlsx, .pptx	

Note: After the successful application of the Service Pack, the server version will remain as 8.3 in the server console.

7. Rollback and Reinstallation

7.1 Rollback Scenarios

- Seeing a Rollback Message on Your Screen? There are two possible reasons for this:
 - 1. **Multiple Executions of the Service Pack**: You may have executed the Service Pack multiple times without verifying the success of the first execution.

2. **Unexpected Error**: The rollback could be due to an unexpected error, such as a system reboot or interruption (e.g., pressing Ctrl + C).

Note: In both of the above cases, the server will remain on the previous version. If the "rollback message" is displayed on your screen, it means the Service Pack was not successfully applied. In this case, the server will revert to the previous state.



After the rollback of the Service Pack, check the "telemetryinfo" collection within "sqepsng80". It should contain the following information:



If the Service Pack installation fails, a rollback log named "**SP_Rollback.log**" will be generated in the following directory: /opt/Seqrite_EndPoint_Security/logs

7.2 Reapplying the SP After Rollback

If a rollback occurs, reapply the SP by following steps instructed in #5 Service Pack (SP) Installation Steps.

8. Troubleshooting – Client Side

8.1 Common Issues and Solutions

1. Watermark not working?

- Verify that the "Online Protection System Service" is running:
- Open Command Prompt with administrative privileges and type *services.msc*, then press Enter.
- In the Services window, find "Online Protection System" and confirm that its status is set to "Running."



2. Missing CSSDLP Driver:

- Open Command Prompt with administrative privileges.
- Type the command *fltmc* and press Enter.
- Check if the cssdlp driver is listed under "Filter Name".

	E Dark it anima	mentanting resures	
Select Administrator: C:\Windo	ows\system32\cmd.exe		
Microsoft Windows [Versi (c) Microsoft Corporatio	on 10.0.22000.3260] n. All rights reserved		
C:\Users\Administrator>f	ltmc		
Filter Name	Num Instances	Altitude	Frame
bindflt	1	409800	0
sieflt	A	388801	A
cssdlp	4	388800	Θ
vsepire	0	320200	
gg⊂	3	321510	0
catflt	4	321500	0
bdsflt	3	321490	0
arwflt	4	321480	0
storgosflt	0	244000	0
wcifs	0	189900	e
CldFlt	0	180451	0
FileCrypt	0	141100	0
luafv	1	135000	0
npsvctrig	1	46000	9
Wof	2	40700	0
FileInfo	4	40500	0

If the "cssdlp" driver is not listed, follow these steps to re-apply the configured policy: Log in to the EPP 8.3 server.Go to **Policies**.Edit the policy applied to your endpoint and click the **Save Policy** button.

3. Policy not applied on client?

- Ensure the policy is correctly assigned to the endpoint.
- Check Applied Endpoints in the EPP server. To check the policy status, log in to the EPP 8.3 server, go to Policies, and click on View Details of the configured policy to confirm the client appears in the "Applied Endpoints" section.

SECRITE Endpoint P	Totaction Purservice surre										4 0	vals hand the just	0
Databased								Search by	 texts 		Q, filter by	Petch Install	D Separt
A the	DLP License # Spelate Agent Bale			END/POINT NAME	IP ACERTIS	INDPORT STATUS	DOMAIN NAM		GROUP NAME 🔐	uni	n NAVARE 📑	POLICY	
Et Croups	× 4 φ		39	EDWITTWORT	172.18.35.171	@ OFfice	VICERSAGUE		Default		111530301	Debuil, (PP	
Computer	Default		39	DWMMT7934-383	172.18-46.32	0 (7 Tex	VICEKO/OUP		Default	-	ele.	Delait, IPP	
tates	A Compatibility Test			DESITOR-WILEYEA	172/16/2/19	• Orins	VICEKSIOUP		Default	44	ein -	Debuil (899	-
C Exproyment	— ≜ 9.8*	•	۲	W01101942523-17	172.18.25.116	Onine	VICEKSROUP		Sachin	40	winization	SaminPalicy	٦.
C News	- A Visitalement	•	3	EQUIVE THEORY &	173-18-34.217	Crime	VORGIOUP		V8.Watermark		er vede aller	VE Watermark	-
Advanced Protection	A than	•		ugerer secto and	173.19.101.39	• O'me	VICENDAUP		Default		wiring Scalar	Debail (199	
Configurations		o •		DESITOP-NERVIN	172.18.10.108	© OTTINE	VICENSIOUP		Muan		errestator	Vicen	
The Sendors			φ	1950AL02	172.38.24.48	C OTHE			Default	NEX		Debuil, 199	

4. No DLP License?

Log in to the EPP 8.3 server, go to Status, and check for your client. If no DLP license is assigned, log in to the EPP 8.3 server, go to Status, select the Endpoint, click Client Action > DLP > Assign DLP License > Submit, and verify by the blue dot next to the client (as shown in the screenshot).

42	SECRITE Endpoint Pr	rotection ENTERPRISE SUITE								Q (0)	valinasihajat. 📀 *
	Beer/dooend							Sea	ohty + Sorch	Q Rarby *	Next Invest
~	. Stor	DLP License Update Agent Role			INDIGINE NAME 1	IP ADDRESS 11	ENDROME STATUS	DOMAIN NAME	GROUP HAME IT	USER NAME	POUCY
sť,	mmups	$\forall \Delta \phi$	0		EQANTERNOVET	172.16.16.174	@ Office	WORKSHOLP	Default	Administrator	Debuilt_02P
Ca	mouter	- A Delast	0	30	098890729054-003	172.18.46.32	0 (#1m	MORIGROUP	Detault	admin	Default_0PP
15	Satur	di Compatibility Yest	•		DESKTOP-M10704	172.18.172.74	• Online	WORKSHOUP	Default	Admin	Delast, DP
Ċ	Deployment	- <u>A 9,09</u>	••	۲	WENHONSH 2020-17	172.18.26.116	• Online	WORKSHOLP	Sachin	Administrator	SechinPolicy
٢	Pelicis	- A Section	•		EQM/1819H2/DB-5	172.18.36.387	Drine	MORGIOUP	10.00ae-mark	Adversionalian	VEstatements
<u>C</u> 2	Advanced Protection V	- A titrue	•		UQ47W13ENT3-018	172.18.101.30	Online	WORKShoup	Deliuli	Administrator	Delawit_01P
5	Computations		•	-	DESKTOP-NERVIN	172.18.16.105	0 081xc	WORKDAU/P	Mage	Administrator	Vicen
10 10	Roperts			Φ	875QALI22	172.18.24.48	Online		Delsuit	60.	Debuit, DP

5. Verify .NET Framework Version

To verify that the .NET Framework version 4.8 is enabled on the client operating system, follow these steps:

1. Check .NET Framework Version:

- Open Control Panel and navigate to Programs and Features.
- Click on Turn Windows features on or off.
- In the list that appears, look for **.NET Framework 4.8**.
- Ensure that the checkbox next to .NET Framework 4.8 is checked. If it is unchecked, enable it by selecting the checkbox and clicking OK.



2. Service Check:

0

- If the service is not enabled, follow these additional steps:
 - Disable Self Protection.
 - Right-click on Online Protection System and select Start.

6. **DLP Status Validation in section.ini File**

To verify that Data Loss Prevention (DLP) is applied, follow these steps:

- 1. Navigate to the section.ini file:
 - 1. Go to C:\Program Files\Seqrite\Seqrite\.
 - 2. Locate and open the section.ini file using Notepad.

2. Check for the DLP status entry:

- 1. In the section.ini file, search for the line that specifies the DLP status.
- 2. Ensure the entry DLPStatus=1 is present. This confirms that DLP is enabled on the system.

42	ONEDRIVE FP RSTR=1
43	RST STAT CNT=5
44	CDB CURR UPDT COUNT=4
45	CLIENT_ID=152D1552B1CAECAE9FBA9BF4106844A2
46	FILES_CREATED=2498
47	FILES_MODIFIED=2534
48	FILES_EXECUTED=625
49	BACKUP_RUN_COUNT=3
50	
51	[BDS]
52	ALERT_REPORTING=1
53	
54	[UPDATE]
55	QHSRPT_QHINXCOR=0
56	QHSRPT_ENINXCOR=0
57	QHSRPT_ROLLBACK_SUCC=0
58	QHSRPT_ROLLBACK_ATTMPT_OVER=0
59	ReportError =1
60	RDM_SYNC=60
61	MAXPUSE=25
62	COUNT=2
63	
64	[FIREWALL]
65	FW_REPORT_SIZE=10
66	
67	[QH_REPAIR]
68	REPAIR_TIMEOUT=180
69	REPAIR_STATUS=1
70	L
71	[EMLPROXY]
72	PORT= 17400
73	DLPStatus=1
74	DLRSSLStatus=0

7. Logs Validation for Watermarking in eppclient.log

To validate the **eppclient.log** file and ensure the watermarking process is working correctly, follow these steps:

1. Creating the eppclient.log File

By default, the **eppclient.log** file is not created. However, since the watermarking feature processes a large number of files, it could grow very large. To manually create the **eppclient.log** file, follow these steps:

- Open the **C**: drive on your computer.
- Right-click in the folder and select **New > Text Document**.
- Name the file **eppclient.log** (ensure it is not saved as **eppclient.log.txt**).
- Confirm any prompts to remove the .txt extension.

> This PC > Local Disk (C:)			
Name	Date modified	Туре	Size
cfrbackup-CANPNHFZ	21-02-2023 13:32	File folder	
cfrbackup-FDQSQKIC	16-02-2023 07:14	File folder	
cfrbackup-GERTRLJD	12-03-2023 11:18	File folder	
cfrbackup-NLYAYSQK	25-10-2024 21:37	File folder	
cfrbackup-YWJLJDBV	27-09-2023 13:07	File folder	
📒 inetpub	17-11-2022 10:27	File folder	
and the second s	25-10-2024 21:48	File folder	
📒 PerfLogs	07-05-2022 10:54	File folder	
📒 Program Files	25-10-2024 17:48	File folder	
📒 Program Files (x86)	25-10-2024 17:36	File folder	
Users	02-03-2023 18:34	File folder	
📒 Windows	25-10-2024 17:30	File folder	
eppclient.log.txt	25-10-2024 23:30	Text Document	0 KB

2. Restarting the "Online Protection System" Service

- Open **Command Prompt** with administrative privileges.
- Type services.msc and press Enter.
- In the Services window, locate the Online Protection System service.
- Right-click on it and select Restart.

Services (Local)	Services (Local)						
	Online Protection System	Name	Description	Status	Startup Type	Log On As	
	Stop the service Restart the service	Q Network Connected Devices Auto-S Network Connection Broker Network Connections	Network Connected Brokers connections t Manages objects in t	Running	Manual (Trig Manual (Trig Manual	Local Service Local System Local System	
		Network Connectivity Assistant Arrow List Service	Provides DirectAccess Identifies the network	Running	Manual (Trig Manual	Local System Local Service	
		Network Location Awareness	Collects and stores co	Running	Automatic	Network Service	
		Wetwork Setup Service Network Store Interface Service	This service delivers n	Running	Automatic	Local System	
		Office Source Engine Offline Files	Saves installation files The Offline Files servi		Manual Manual (Trig	Local System Local System	
		🙆 Online Protection System		Running	Automatic	Local System	
		OpenSSH Authentication Agent	Agent to hold private		Disabled	Local System	
		🖏 Optimize drives	Helps the computer r		Manual	Local System	
		Revenue Controls	Enforces parental con		Manual	Local System	

3. Performing Watermarking on MS-Office Files

• Perform the watermarking process on archived MS-Office files (.docx, .pptx, .xlsx) that were not watermarked previously.

4. Validating the eppclient.log File

- Navigate to C:/ drive and open the eppclient.log file.
- Search for the entry related to the file you were attempting to watermark (e.g., file_name).
- Look for an entry containing the phrase: "watermarking done, result(1)." This indicates that the watermarking process was successfully triggered.

Example:

If you find "watermarking done, result(1)," this confirms that the watermarking was successful for that file.



5. Handling Discrepancies

If the log contains "watermarking done, result(0)," it suggests an issue with the watermarking process. In this case:

- Follow the troubleshooting steps again, or
- Contact support for assistance.

This process should ensure the watermarking feature is properly logged and that any discrepancies can be addressed.

8.2 CPU Spike on Client-Side During Bulk Data Watermarking

A CPU spike may occur on the client-side when performing watermarking operations on a large volume of data.

This guide ensures a smooth installation, configuration, and troubleshooting process for the DLP watermarking feature in your environment.