DLP-WATERMARK SERVICE PACK [V8.3.3]

INSTALLATION GUIDE

Contents

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 upgrade to v8.3.
- 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

1. **Download the Script**: You can download the "SP – Endpoint_Protection_8_3_3.sh" script from the following location:
   Path: http://download.quickheal.com/builds/seqrite/83/en/build/sp/watermark/Endpoint_Protection_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:

1. **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 → 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.
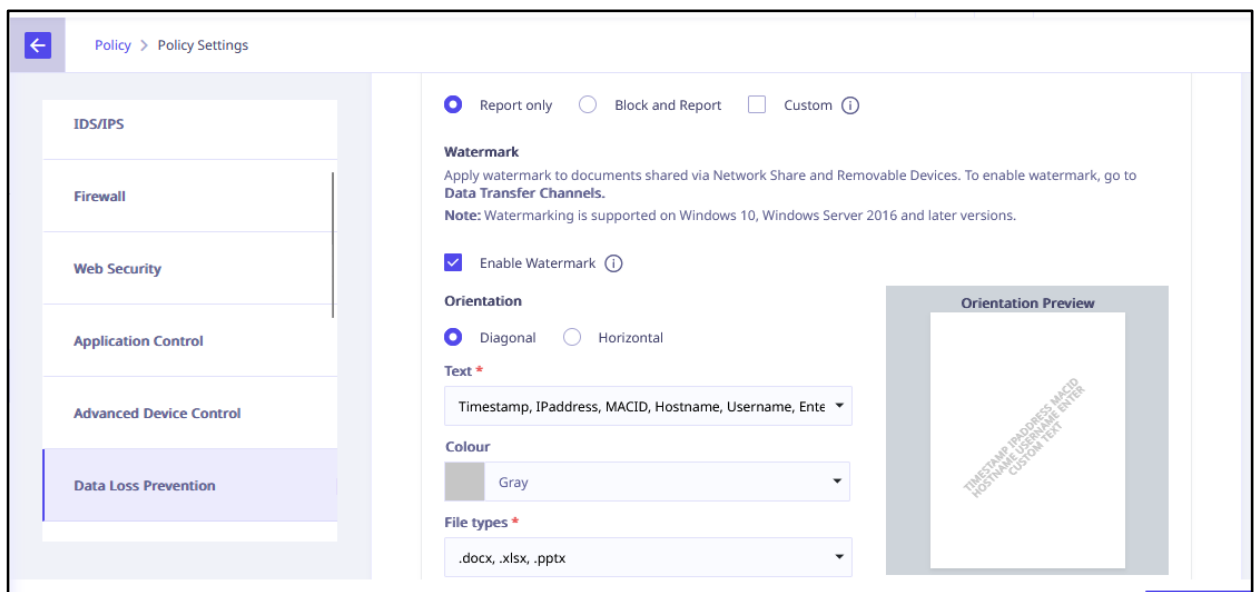
Note: After the successful application of the Service Pack, the server version will remain as 8.3 in the server console.

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.

```
2024-10-24 05:37:39 : [Info] checkDBServerReachable_fun Entry
2024-10-24 05:37:39 : [Info] checkDBServerReachable_fun Exit
2024-10-24 05:37:44 : [Error] User terminated service pack with ctrl+c action or Rebooted/Powered Off the machine
2024-10-24 05:37:44 : [Info] updateSPFailReasonInDB_fun Entry
SP fail reason : 3.0 - Date : 2024-10-24 05:37:44 : [Error] User terminated service pack with ctrl+c action or Rebooted/Powered
Off the machine
2024-10-24 05:37:44 : [Info] Updating SP fail version in telemetryInfo collection Entry
2024-10-24 05:37:44 : [Info] versionUpdateStatus in DB : MongoDB shell version v4.2.2 connecting to: mongodb://localhost:27017/?
authSource=sqepsng80&compressors=disabled&gssapiServiceName=mongodb Implicit session: session { "id" : UUID("e489c153-dea3-418c-
bd3a-80abcd432c6d") } MongoDB server version: 6.0.4 WARNING: shell and server versions do not match { "acknowledged" : true, "ma
tchedCount" : 1, "modifiedCount" : 1 }
2024-10-24 05:37:44 : [Info] Updating SP fail version in telemetryInfo collection Exit
2024-10-24 05:37:44 : [Info] updateSPFailReasonInDB_fun Exit
```

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

```
        }
    ],
    "spMode" : NumberInt(1),
    "spDownload" : NumberInt(1),
    "Version" : "",
    "FailReason" : "3.0 - Date : 2024-11-05 11:06:35 : [Error] User terminated service pack with ctrl+c action or Rebooted/Powered Off the machine",
    "features" : {
        "idsIps" : {
            "idsIpsStatus" : NumberInt(1),
            "detectPortScanAttack" : NumberInt(0)
```

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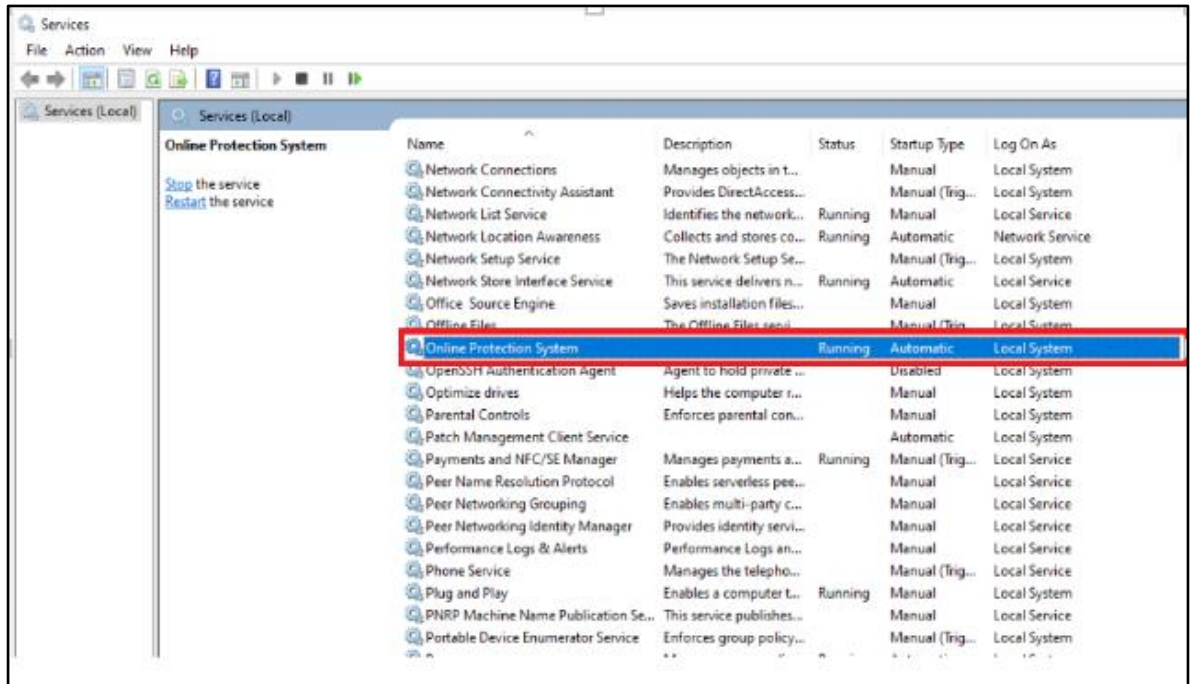
2. **Missing CSSDLP Driver**:
   - Open Command Prompt with administrative privileges.
   - Type the command *fltmc* and press Enter.
   - Check if the *cssdlp* driver is listed under "Filter Name".

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.
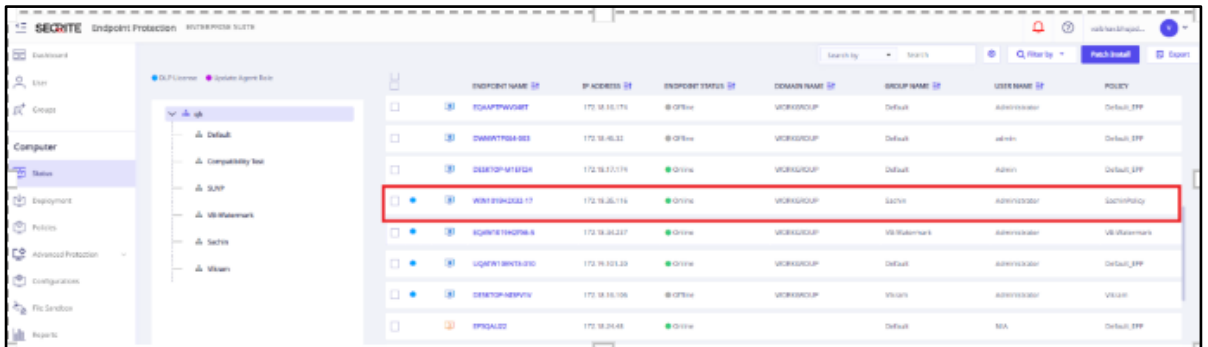
4. **No DLP License?**
   - Log in to the EPP 8.3 server, go to **Status**, and check for your client. If no DLP license is assigned, log in to the EPP 8.3 server, go to **Status**, select the **Endpoint**, click **Client Action** > **DLP** > **Assign DLP License** > **Submit**, and verify by the blue dot next to the client (as shown in the screenshot).
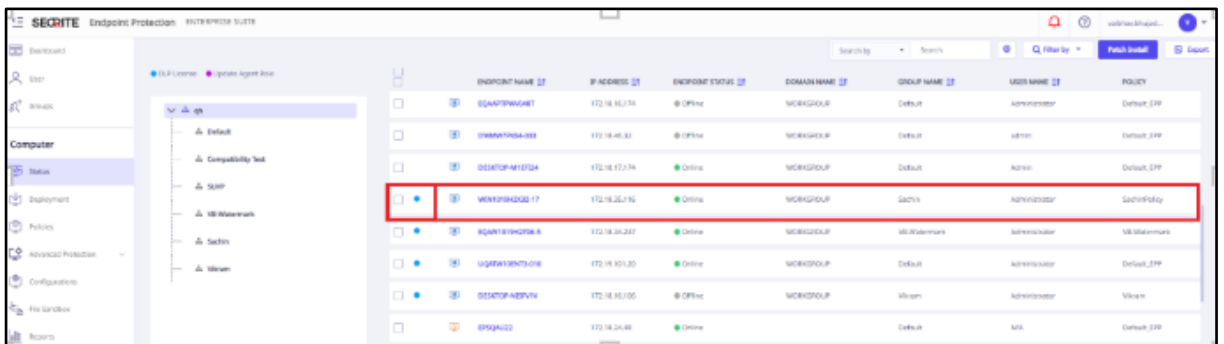
5. **Verify .NET Framework Version**
   To verify that the .NET Framework version 4.8 is enabled on the client operating system, follow these steps:

   1. **Check .NET Framework Version**:
      o Open **Control Panel** and navigate to **Programs and Features**.
      o Click on **Turn Windows features on or off**.
      o In the list that appears, look for **.NET Framework 4.8**.
      o 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**.
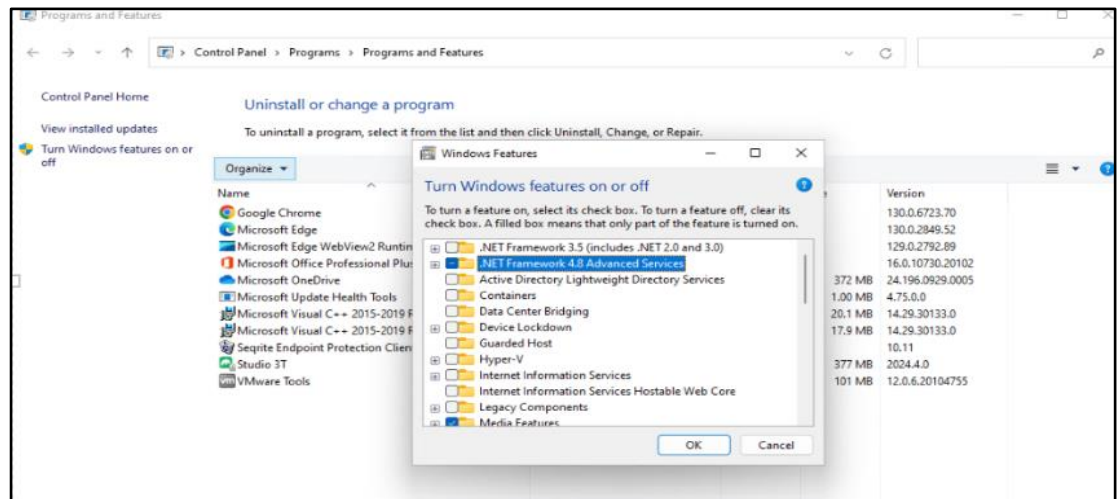
   2. **Service Check**:
      o If the service is not enabled, follow these additional steps:
         ▪ Disable **Self Protection**.
         ▪ Right-click on **Online Protection System** and select **Start**.

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.

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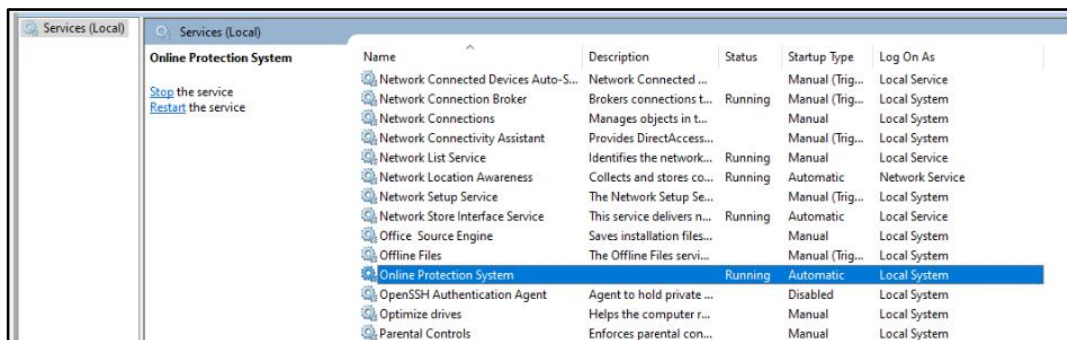**1. Creating the eppclient.log File**
By default, the **eppclient.log** file is not created. However, since the watermarking feature processes a large number of files, it could grow very large. To manually create the **eppclient.log** file, follow these steps:

- 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.
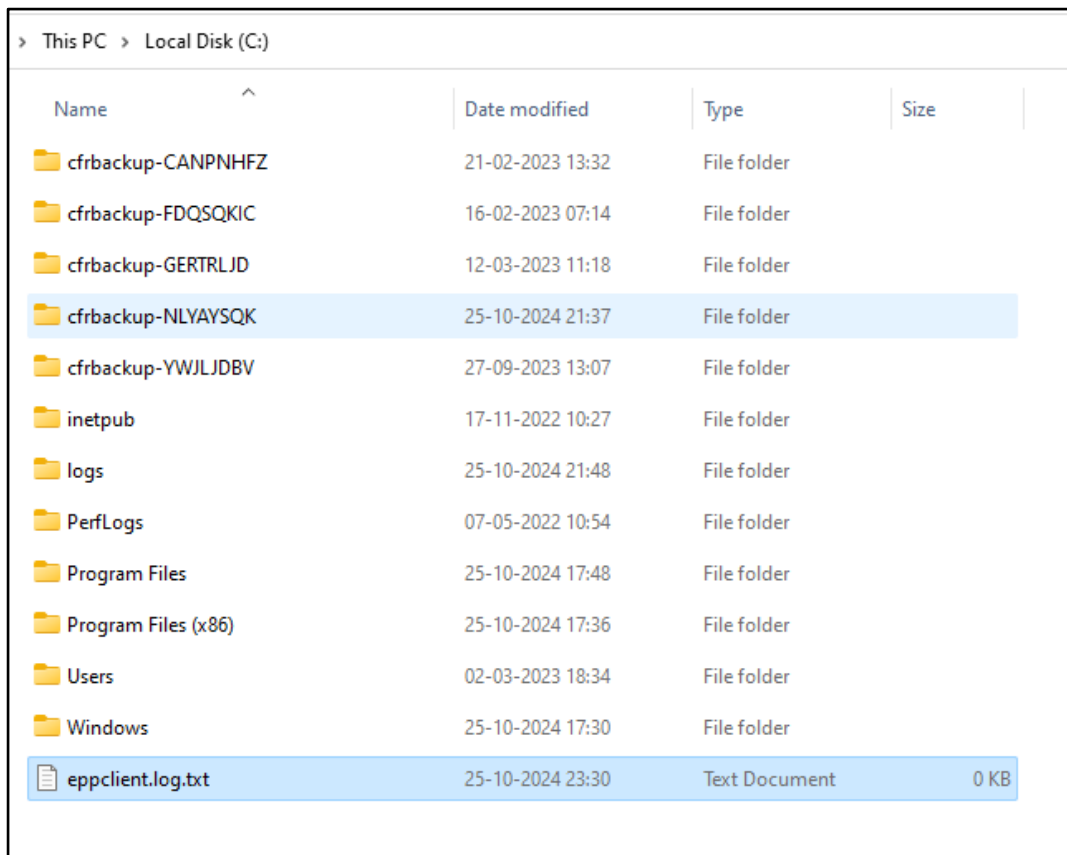
2. Restarting the "Online Protection System" Service

- 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**.

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.