



Seqrite Endpoint Security 7.6

Administrator's Guide

วิธีการตั้งค่าการใช้งาน DLP

SEPS SME
SEPS Business
SEPS Total
SEPS Enterprise Suit

วิธีการตั้งค่าการใช้งาน DLP

* Data Loss Prevention (DLP) เป็นฟีเจอร์ป้องกันข้อมูลสูญหาย หรือถูกขโมย สามารถตั้งค่าการใช้งานของฟีเจอร์ ได้ดังนี้

1. เข้าสู่หน้า Console Seqrite Endpoint Security Management

ไปที่เมนู Clients > แถบ Manage Policies > เลือก Policy ที่ต้องการตั้งค่า

The screenshot shows the Seqrite Endpoint Security 7.6 console interface. The top navigation bar includes 'Admin Settings', 'Support', 'Help', and 'Logout'. The main navigation bar has 'Home', 'Clients', 'Settings', and 'Reports'. The 'Clients' section is active, and the 'Manage Policies' tab is selected. Below the navigation, there is a table of policies:

Policy Name	Groups	Access	Policy Applied On	Policy Pending On	Action
Default	-	Default	-	-	[Icon]
Import_Policy	Default	Default	-	1 Endpoint	[Icon]
Client_Policy	Client	Default	1 Endpoint	-	[Icon]

2. ไปที่ Data Loss Prevention (DLP) > ดึงช่องสี่เหลี่ยม Enable Data Loss Prevention

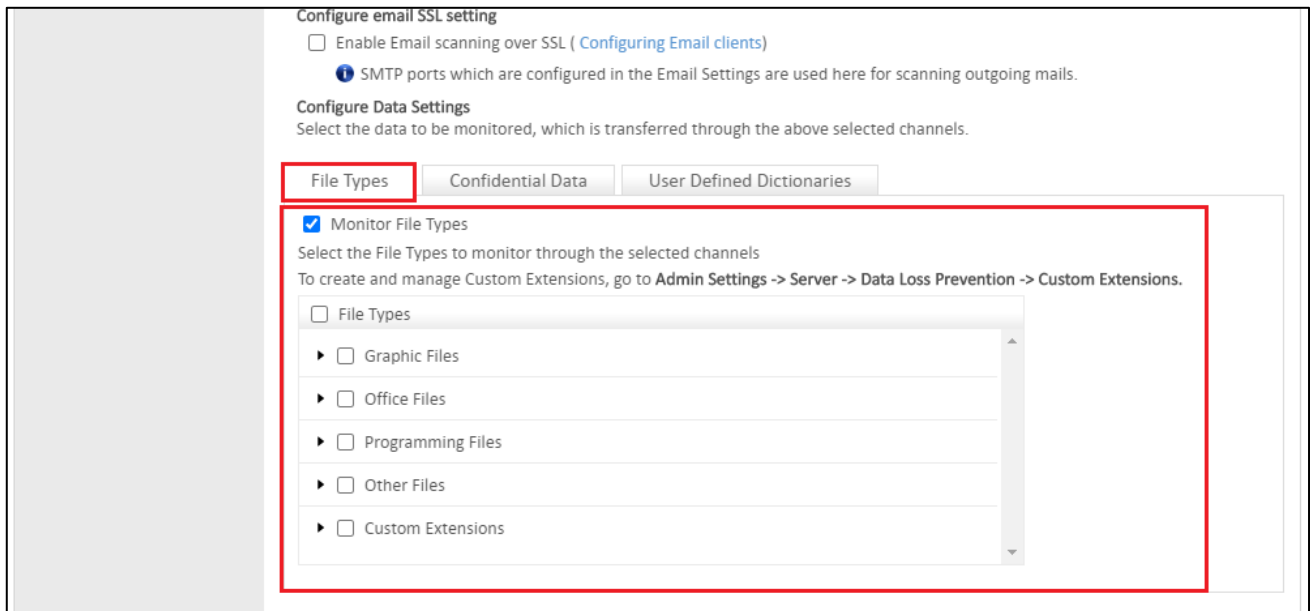
The screenshot shows the 'Data Loss Prevention (DLP)' settings page in the Seqrite console. The left sidebar has 'Data Loss Prevention (DLP)' selected. The main content area includes:

- Data Loss Prevention (DLP)**: Ensure you have enabled Data Loss Prevention on the endpoints. To enable DLP, go to Admin settings -> Client -> Data Loss Prevention. Here you can monitor and control the data transfer through various channels. Select the channels and data to be monitored from the following settings:
 - Enable Data Loss Prevention
 - Display alert message on DLP policy violations
- Data Transfer Channels**:
 - Print Screen
 - Removable Devices
 - Network Share
 - Clipboard
 - Printer Activity
 - Application/Online Services
- Applications**:
 - Web Browsers
 - Email
 - Instant Messaging
 - File Sharing / Cloud Services
 - Social Media / Others

- หัวข้อ Data Transfer Channels เลือกช่องทางที่ต้องการจะป้องกันไม่ให้นำไฟล์ออกจากเครื่อง

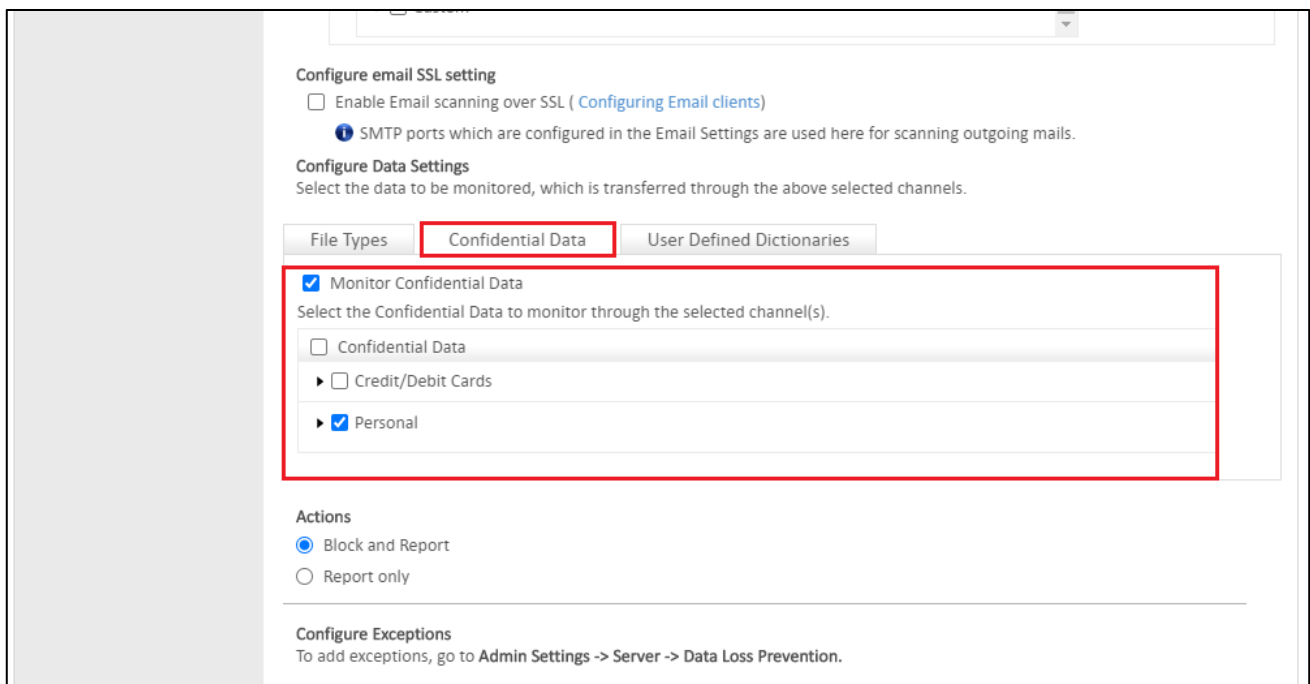
3. กำหนดข้อมูลที่ต้องการป้องกัน ได้ 3 แบบ

3.1 File Type กำหนดเป็น นามสกุลไฟล์ ตีกล่อง Monitor File Types > เลือกนามสกุลไฟล์ที่ต้องการ (สามารถเพิ่มนามสกุลได้ โปรดดูคู่มือ “วิธีการเพิ่มนามสกุลไฟล์ในพีเจอร์ DLP”)



3.2 Confidential Data กำหนดแบบ Pattern > Monitor Confidential Data

- Credit/Debit ข้อมูลเครดิต/เดบิต หมายเลขบัญชีธนาคาร การเงินต่างๆ
- Personal ข้อมูลส่วนบุคคล เช่น หมายเลขบัตรประชาชน เบอร์โทรศัพท์ เป็นต้น



- 3.3 Use Defined Dictionaries กำหนดเป็น Keyword คำ > Monitor Use Defined Dictionaries > เลือก Keyword ที่ทำการเพิ่มไว้ (สามารถกำหนด เพิ่ม Keyword ได้ โปรดดูคู่มือ “วิธีการเพิ่ม Keyword ในพีเจอร์ DLP”)

The screenshot shows the 'Configure Data Settings' page for 'User Defined Dictionaries'. The 'User Defined Dictionaries' tab is selected. The 'Monitor User Defined Dictionaries' checkbox is checked. Below this, a table lists the dictionaries:

User Defined Dictionaries	Number of Words
<input checked="" type="checkbox"/> DLP-Keywords_Test View Details	3

Below the table, the 'Match Whole Word' and 'Match Case' checkboxes are checked. In the 'Actions' section, the 'Block and Report' radio button is selected.

- Match Whole Word ตรงกับคำทั้งหมด
- Match Case ตรงกับกรณีหรือ บางส่วน (สามารถเลือกได้ทั้งสองอย่าง)

Actions

- Block and Report บล็อกการนำข้อมูลออกและเก็บรีพอร์ต
- Report Only สามารถนำข้อมูลออกได้ แต่เก็บรีพอร์ตไว้

**ทำการ Save Policy หลังการตั้งค่าทุกครั้ง (ปุ่ม Save จะอยู่ด้านล่างสุดของเพจ)