Data Leakage Prevention

User Guide
September 2021

SIEMENS

Data Leakage Prevention

Growing importance of data protection and evolving compliance requirements require a comprehensive Data Leakage Prevention strategy

Narrative behind Data Protection

- **Data** is an essential **asset** and property of any organisation.
- **Loss** of data may lead to dramatic **consequences**: productivity disruption, ruined business reputation, regulatory fines, lost of customer trust and loyalty, permanent business failure.
- Therefore, it is in the highest **interest of an organisation** to treat data as a property and **protect**, especially given constantly increase of outside threats and attacks as well as inside threats.
- At the same time, **supervisory bodies** demand companies to develop data loss prevention and protection measurements and lay down strict guidelines (e.g. EBA ICT Guidelines 2019, BAIT 2020) and penalties, in the event of its leakage or loss.

What is Data Leakage Prevention?

- Data theft can happen while data is in use (endpoint actions), in-motion (network traffic), and at rest (data storage). Attackers often find data in use and at rest a more valuable target than data in motion.
- Implementation of a comprehensive **Data Leakage Prevention** (DLP) **strategy** can mitigate data breaches and risk of data loss:
  - DLP strategy is a set of processes and tools used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users.
  - DLP ensures enforcement of security policies, it helps to meet compliance requirements, and it increases data visibility within the organisation.

To address these challenges effectively, you are included in the rollout of the Siemens owned Data Leakage Prevention (DLP) service in your organization

SIEMENS

Data Leakage Prevention

DLP controls designed on the basis of assisting compliant user behavior, without significantly impacting daily work

Medium			SFS DLP Conrols
Re-movable media	USB (e.g. USB flash drive / smartphone / HDD)	USB → PC (Upload)	—
		PC → USB (Download)	⊘
	CD / DVD	CD / DVD → PC (Upload)	—
		PC → CD / DVD (Download)	⊘
Transfer of documents via Remote Sharing (file sharing via network, WIFI, AirDrop, FastShare, Cable)			👁
Upload on Websites			👁
Data transfer via non-authorized applications			👁
PowerShell run by users			👁
E-Mail (Outlook) – mail sent to non-siemens mail addresses with at least one attachment (incl. screenshots)			👁
Bluetooth data transfer			👁
Printing (Private Printer, except for virtual pdf printing)			👁
Printing (Corporate Printer, except for virtual pdf printing)			👁
Messenger (Document upload to Yammer)			👁

„–“ No measure ⊘ Block 👁 Monitoring

Comments

- The DLP service relies on user of the software **Digital Guardian Agent** – DG Agent is a client-based software that starts with operating system and runs in the background.
- DG Agent is **Siemens-wide proven** tool aiming to
  - assist you in processing data accurately and becoming more sensible to data security (compliance behavior) and
  - prevent loss and disclosure of company data to unauthorized persons.
- **SFS DLP controls** are defined as DLP Minimum Standard for SFS with the focus on monitoring of data movements / data transfer executed by users; attempts to copy / save data to a removable media will be blocked (work-related temporary exceptions are subject to approvals).
- Every action related to a **data transfer**, such as uploading a document to the web, is logged. Any other actions that are not related to data movements are not recorded (e.g. copy documents from USB drive to your computer, visit any website, contents download from Web, emails sent without attachment and within Siemens).
- No performance or behavior controls take place.

SIEMENS

Data Leakage Prevention
Typical questions related to DLP (English Version)

Question	Answer
Will I notice an installation, and will I have to re-start my computer?	DG Agent will be installed in the background without any user interaction or participation.
Will DG Agent installation affect my computer performance?	DG Agent should not affect your computer and its performance – if you experience any issues, please contact your local IT help desk.
What happens after the installation?	Shortly after the DG Agent installation is complete, the DLP controls will be activated.
How does DLP controls work?	DLP controls can block a data transfer before it is performed (e.g., saving data on a USB drive) or monitor and log the data transfer activity (e.g., uploading files to Web or sending an email to non-Siemens recipients with at least one document attached).
What information is exactly recorded?	Every action related to a data transfer, such as uploading a document to the web, is logged. Any other actions that are not related to data movements are not recorded (e.g., copy documents from UBS drive to your computer, visiting any website or downloading contents from Web).
How long are logs kept?	Retention period for logs is 26 weeks after the date of the recording.
Who has access to logs?	Only DLP admins have access to your logs. DLP admins are allowed to view logs only in IT incident cases to provide you with technical support. No one in your organisation has access to the collected DLP logs.
Who will receive DLP reports?	Your local DLP coordinator receives DLP event reports, reports are created only in (at entity level) aggregated and anonymized form.
Where will be logs stored?	DLP records are stored on the central DLP server located in Germany.
Who can support me if I have questions related to DLP?	If you have technical issues, you can contact your local IT help desk. If you have any other type of questions, please contact your local DLP coordinator.

SIEMENS