Click 'Settings' > 'Data Loss Prevention'

- Data loss prevention (DLP) rules let you prevent files being copied to external devices and prohibit screen captures when certain applications are running.
- Discovery rules let you scan Windows devices for files that contain sensitive information and to block sensitive data being leaked from your device.
- For example, the scan finds card numbers, social security numbers, bank account numbers, bank routing numbers, and more.
- You can review all files identified by DLP events from the 'Logs' interface. You can then take actions to secure that data where required.

Use the following links to jump to the task you need help with:

Overview

Monitoring rules:

- Monitoring rules let you prevent sensitive information from being copied to external devices like USB keys and block screenshots of running applications, documents and so on.
- You create monitoring rules at ‘Settings' > 'Data Loss Prevention' > 'DLP Monitoring'.
- There are two types of monitoring rules:
    - **Removable storage access rules** let you specify the actions taken when files are copied / moved to external storage devices like USB drives
    - **Screenshot rules** let you specify the action to be taken when screenshots are taken from certain applications.

You can view the logs of monitored events at 'Logs' > 'Data Loss Prevention Events'.

Discovery rules:

- Discovery scan rules are configured by your Endpoint Manager admin.
- You can run discovery scans from 'Tasks' > 'DLP Tasks' > 'Data Loss Prevention Scan'

- Results – you can view scan results at 'Logs' > 'Data Loss Prevention Events'.

Create monitoring rules

- Click ‘Settings’ > ‘Data Loss Prevention’ > ‘DLP Monitoring’

- Select 'Enable DLP Monitoring'

You can create two types of monitoring rules:

- Removable storage access rules - Block or allow copy/move operations to USB data devices
- Screenshot rules - Prevent screen captures using various screenshot tools and applications. when certain applications are running or when sensitive documents are open on the device.

Removable storage access rules

- Click ‘Settings’ > ‘Data Loss Prevention’ > ‘DLP Monitoring’
- Ensure 'Enable DLP Monitoring' is selected
- Click 'Add' > 'Removable Storage Access Rule'

- Choose the action and device targets:

Action – What CCS should do if it detects data being moved to the target devices:

- **Block** – The storage device is set to ‘Read-only’ mode. Users cannot copy data to / from the storage device.
- **Ignore** – Data transfers to the device are allowed.

Criteria – Select the type of device to which the rule applies. The only option available is:

- USB data devices

Options – Choose whether you want to create an event log whenever the rule is enforced.

- You can view the logs in via the 'Logs' > 'Data Loss Prevention Events' interface

- Click ‘Ok’

The monitoring rule is added.

- Click ‘Save’ to apply your changes.

- CCS allows or blocks the file transfer operations to external devices as per the rules. You can view the event logs in the 'Logs' > 'Data Loss Prevention Events' interface. See View scan results and logs for more details.

Screenshot rules

- Click ‘Settings’ > ‘Data Loss Prevention’ > ‘DLP Monitoring’

- Ensure 'Enable DLP Monitoring' is selected

- Click 'Add' > 'Screenshot Rule'

- Choose the action and criteria for the rule:

Action – What CCS should do if it detects a screenshot operation when an application meeting the rule criteria is running on the device:

- **Block** – The screen shots are not allowed.

- **Ignore** – The screen shots are allowed.

Criteria – Select the rule targets.

The targets are the files/folders/groups that are covered by the rule.

- Click ‘Edit’

There are three types of criteria you can specify for a rule:

- Criteria 1 – Application(s) / executable file(s)

- Criteria 2 – Application rating
- Criteria 3 – Application vendor

Criteria 1 – Application(s) / executable file(s)

- Click ‘Add’ in the ‘Running application’ row

There are six types of target you can add:

- Files - Apply the rule to specific files on your drive.
- Running Processes - Apply the rule to a process that is currently running on your computer.
- File Groups - Apply the rule to predefined file groups.
    - A file group is a collection of files which (usually) share similar attributes and/or functionality. For example, the 'Executables' group is a list of file types that can run code on your computer.
    - You can view and manage file groups in 'Settings' > 'Fie Rating' > 'File Groups' interface.
- Folder - Apply the rule to a folder or drive.
- File Hash - Create a hash value from a file and use it as the rule target. A hash value is a large number which is generated by passing the file through a hashing algorithm. The number uniquely identifies the file, and it is extremely unlikely that two files will ever generate the same hash. The benefit of using a file hash is that the rule will still work even if the file name changes.
- Process Hash - Create a hash value of a process and use it as the rule target. Please see description above if required.

Add an individual File

- Choose 'Files' from the 'Add' drop-down.
- Navigate to the file you want to target then click 'Open'

The file is added the as the rule target.

- Repeat the process to add more files.
- Click 'OK' if you want to simply apply the selected action
- Alternatively, select criteria 2 to refine the rule with more filters.

Add a currently running application by choosing its process

- Choose 'Running Processes' from the 'Add' drop-down.

A list of currently running processes in your computer is shown:

- Select the process of the target application then click ‘OK’.

The parent application of the process is added as the target.

- Click 'OK'.
- Repeat the process to add more targets
- Click 'OK' if you want to simply apply the selected action to the target
- Alternatively, select criteria 2 to refine the rule with more filters.

Add a File Group

- Choose 'File Groups' from the 'Add' drop-down.

- Select the group from the drop-down.

All files in the group are added as targets.

- Click 'OK'.
- Repeat the process to add more targets
- Click 'OK' if you want to simply apply the selected action to the target
- Alternatively, select criteria 2 to refine the rule with more filters.

Add a folder/drive partition

- Choose 'Folder' from the 'Add' drop-down.

- Navigate to the drive partition or folder you want to add as target and click 'OK'

All files in the folder / drive are added as targets.

- Click 'OK'.
- Repeat the process to add more targets
- Click 'OK' if you want to simply apply the selected action to the target
- Alternatively, select criteria 2 to refine the rule with more filters.

Add a file based on its hash value

- Choose 'File Hash' from the 'Add' drop-down
- Navigate to the file whose hash value you want to target.
- Click 'Open'.
- CCS generates the hash of the parent file and stores it as the target.
- The advantage is that the rule will catch the file even if the file name changes.
- Repeat the process to add more targets
- Click 'OK' if you want to simply apply the selected action to the target
- Alternatively, select criteria 2 to refine the rule with more filters.

Add target by creating a hash from a running process

- Choose 'Process Hash' from the 'Add' drop-down.
- This shows a list of currently running processes on your computer:
- Select the target process and click 'OK'

- CCS generates a hash of the parent file and stores it as the target.
- The advantage is that the rule will catch the file even if the file name changes.
- Repeat the process to add more targets
- Click 'OK' if you want to simply apply the selected action to the target
- Alternatively, select criteria 2 to refine the rule with more filters.

Criteria 2 – Application rating

You can narrow the scope of the rule by adding another condition for the selected application(s) in criteria 1. Note – If you choose to add application rating to the rule, both criteria 1 AND criteria 2 should be met for the rule to trigger.

- Click the 'Select' button in the 'Running application rating' stripe:

- This applies the rule to files which match the trust rating you set. You can choose from the following trust ratings:
    - Trusted - Applications are categorized as 'Trusted' if:
        - The file is on the global whitelist of safe files
        - The file is signed by a vendor with 'Trusted' rating in local vendor List
        - The file was installed by a trusted installer
        - The file was given a trusted rating by an administrator or user.
    - Unrecognized - Files that do not have a current trust rating. The file is on neither the blacklist nor the whitelist, so is given an 'unknown' trust rating.
    - Malware - Malicious files - those that are on the blacklist of known harmful files.
- Click 'OK' if you want to apply the selected action to the target(s)
- Alternatively, select criteria 3 to refine the rule with more filters.

Criteria 3 – Application vendor

- You can apply an action to a file based on the vendor who digitally signed the file. The vendor is the software company that created the file.

- There are three ways you can add a vendor:

1. Directly select a vendor

  - Choose 'Vendor from a Vendor List' from the drop-down
  - The 'Add Vendor' dialog opens with a list of vendors in the local 'Vendor List' in CCS
    - You can view and manage list of vendors and their trust ratings from the Vendor List interface
    - Click 'Settings' > 'File Rating' 'Vendor List' to open the 'Vendor List' interface
  - Use the sort and filter options in the column headers to search for the vendor to be specified
  - Choose the vendor and click 'OK'. The vendor will be added to the filters.

2. Specify an executable file on your local drive

  - Choose 'File Signer' from the drop-down
  - Navigate to the executable file whose publisher you want to add as the criteria and click 'Open'.
  - CCS checks that the .exe file is signed by the vendor and counter-signed by a Trusted CA. If so, the vendor is added as a criteria

3. Select a currently running process

    - Choose 'Running Process Signer' from the drop-down
    - A list of all processes running at present on your computer is shown
    - Select the process to specify the publisher of the application that started the process and click 'OK'
    - CCS checks that the .exe file that started the process is signed by the vendor and counter-signed by a Trusted CA. If so, the vendor is added as a criteria

- Click ‘OK’ in the rule criteria screen.

Options – Choose whether you want to create an event log whenever the rule is enforced. Click ‘Logs’ on the home-screen to view DLP logs.

- Click ‘OK’ and again in the settings screen to save the rule.
- Repeat the process to add more rules.

CCS allows or blocks the screen capture operations as per the rules. You can view the event logs in the 'Logs' > 'Data Loss Prevention Events' interface. See View scan results and logs for more details.

DLP discovery scan rules

- Click 'Settings' > 'Data Loss Prevention' > ‘Discovery Rules’

- DLP discovery rules are created by your Endpoint Mnager admin ad added to the configuration profiles active on the device.
- The discovery rules interface shows the rules applied to your device by the profiles active on it
    - See this wiki if you need help to create DLP discovery rules and add them to profiles.
- You can run manual scans using these rules from CCS by clicking 'Tasks' > 'DLP Tasks' > 'Data Loss Prevention Scan'
    - See Manually run a DLP scan for help to run an on-demand DLP scan.

Manually run a DLP scan

You can run DLP scans on-demand from the 'DLP Tasks' interface:

- Click 'Tasks' on the CCS home screen
- Click 'DLP Tasks' > 'Data Loss Prevention Scan'

- Click 'DLP Tasks' > 'Data Loss Prevention Scan'

The scan interface shows all rules added to your device by the EM profile active on your device.

- Start button - Run a scan with all rules at once

  Or

- Use the start buttons on the left to run a scan with a specific rule.

View scan results and logs

- Click 'Logs' in the CCS menu bar

  OR

- Click ‘Tasks’ > ‘Advanced Tasks’ > ‘View Logs’
- Select 'Data Loss Prevention Events’ in the drop-down at top-left

The logs show items flagged by data loss prevention scans and monitoring events:

- **Date & Time** - When the event occurred.
- **Target** - The item affected by the rule.
- **Rule**- The DLP rule that found the target item. This could be a DLP discovery rule or a monitoring rule.
- **Action** - How the file was handled in the DLP event.
- **Status** – Shows whether the rule executed successfully or not
- **Details** – The specifics of the data found. See View details of a file for more details.

You can use the filter options at the top to search the logs by time, location of the file, rule or action.

View file details

- The details column shows different information depending on the type of DLP event:
    - DLP quarantine – Shows the name of the rule that quarantined the file.
    - DLP monitoring rule – Shows the removable storage device affected by the rule.
    - Discovery rule – Has a ‘Show details’ link which opens the specifics of the event:

- The screen shows the name of the file, and the rule/pattern which discovered sensitive data in the file.
- The ‘match’ column shows the first and last characters of the actual discovered data. The option to show this should be enabled in the discovery rule.
- Click ‘Jump to Folder’ to view the document itself.