## Skyhigh DLP Incident Notes

The following Omnibar facets are used exclusively in on the DLP Incidents page.

|  |  |  |
| --- | --- | --- |
| Search Term | Description | Available Options |
| File Size | The detected file size of the file matching the DLP policy rule. You can use this Omnibar facet to filter results around the size of the file. Transfers of unusually large files may indicate potential data exfiltration events. Excessive transfers of unusually small files may indicate attempts to test security measures in preparation of a data theft incident. | Equal To Greater Than Less Than Between |
| File Type | The format of the file matching the DLP policy rule. You can use this Omnibar facet to filter results around a specific file format in order to better tune policies that control which formats can be shared. For example, if you have a policy that only allows PDFs to be shared, you could use the File Type filter to confirm that .DOC or .XLS files are triggering policy violations. | [One or more formats can be selected from any of the Skyhigh CASB supported formats.](https://success.myshn.net/Start_Here_with_Skyhigh/Skyhigh_Overview/Supported_File_Formats) |
| Incident ID | This Omnibar facet is reserved for internal functionality. | N/A |
| Match Count | The number of policy rule matches were found in the document that triggered the policy violation. You can use this Omnibar facet to filter results to investigate files that violate a policy in many places (as those indicate the highest risk violations) or to review files that have a small number of matches as those may indicate false positives or accidental violations. | Enter any integer to filter to the number of policy matches. |
| Policy | The name of the violated policy. You can use this Omnibar facet to review all policy violations from a specific policy. | [Select from any of your existing DLP policies.](https://success.myshn.net/Policy_Management/Data_Loss_Prevention_Policies/DLP_Policy_Rules_and_Rule_Groups) |
| Remediator | The remediator is the CASB user who has been assigned to investigate the policy violation. You can use this Omnibar facet to view the workflow of your remediators. | [Select from any CASB user with the Policy Manager role to view any policy violations where that user is assigned as a remediator.](https://success.myshn.net/Setup_and_Configuration/RBAC_and_User_Management/aAbout_User_Access_Levels) |

|  |  |  |
| --- | --- | --- |
| Search Term | Description | Available Options |
| Response | The response action taken as a result of the policy violation. You can use this Omnibar facet to review policy responses and see how many policy violations are responded to in a certain way. | [Select from Skyhigh's DLP response actions.](https://success.myshn.net/Policy_Management/Data_Loss_Prevention_Policies/DLP_Policy_Response_Actions) |
| Scan Name | The name of the On-Demand Scan that detected the policy violation. You can use this Omnibar facet to review your On-Demand Scans; if an On-Demand Scan consistently runs without triggering any policy violations it may not be configured correctly. Conversely, if an On-Demand Scan produces excessive false positives you may need to adjust the scan criteria. | [Select from your active On-Demand Scans.](https://success.myshn.net/Policy_Management/On-Demand_Scanning) |
| Severity | The recorded severity level of the policy violation. Severity level is defined by the user during DLP policy creation. You can use this Omnibar facet to manage your remediation workflow; filtering based on severity level allows your remediators to focus on the highest priority violations first. | High |
| Sharing | If the content is included in a shared folder or external link within the CSP. Some companies view policy violations for files shared outside of the company more harshly than files that remain internal. You can use this Omnibar facet to provide better insight on how your users are interacting with the cloud and better determine the significance of the policy violation. | Content Not Shared Externally |
| Status | The current state of the policy violation. Status is set by the user in the policy violation platform. You can use this Omnibar facet to manage your remediation workflow; remediators can filter to only New policies to tackle the incoming violations or filter out any violations that have been marked as False Positive. | New Open False Positive Resolved Archived |
| User | The user who triggered the policy violation. You can use this Omnibar facet to investigate specific users. If a single user is generating excessive policy violations, they may need to be investigated. | Select between all users who have triggered a DLP policy violation. |
| File Name | The name of the file matching the DLP policy rule. You can use this Omnibar facet to locate policy violations centering on a specific file. | All detected files can be used in this search filter. |

|  |  |  |
| --- | --- | --- |
| Search Term | Description | Available Options |
| File Size | The detected file size of the file matching the DLP policy rule. You can use this Omnibar facet to filter results around the size of the file. Transfers of unusually large files may indicate potential data exfiltration events. Excessive transfers of unusually small files may indicate attempts to test security measures in preparation of a data theft incident. | Filter on file size based on KB, MB or GB. The filter can compare files against the user-entered value based on the following criteria:  Equal To  Greater Than  Less Than  Between |
| File Type | The format of the file matching the DLP policy rule. You can use this Omnibar facet to filter results around a specific file format in order to better tune policies that control which formats can be shared. For example, if you have a policy that only allows PDFs to be shared, you could use the File Type filter to confirm that .DOC or .XLS files are triggering policy violations. | One or more formats can be selected from any of the Skyhigh CASB supported formats. |
| Incident ID | This Omnibar facet is reserved for internal functionality. | N/A |
| Match Count | The number of policy rule matches were found in the document that triggered the policy violation. You can use this Omnibar facet to filter results to investigate files that violate a policy in many places (as those indicate the highest risk violations) or to review files that have a small number of matches as those may indicate false positives or accidental violations. | Enter any integer to filter to the number of policy matches. |
| Policy | The name of the violated policy. You can use this Omnibar facet to review all policy violations from a specific policy. | Select from any of your existing DLP policies. |
| Remediator | The remediator is the CASB user who has been assigned to investigate the policy violation. You can use this Omnibar facet to view the workflow of your remediators. | Select from any CASB user with the Policy Manager role to view any policy violations where that user is assigned as a remediator. |
| Response | The response action taken as a result of the policy violation. You can use this Omnibar facet to review policy responses and see how many policy violations are responded to in a certain way. | Select from Skyhigh's DLP response actions. |

|  |  |  |
| --- | --- | --- |
| Search Term | Description | Available Options |
| Scan Name | The name of the On-Demand Scan that detected the policy violation. You can use this Omnibar facet to review your On-Demand Scans; if an On-Demand Scan consistently runs without triggering any policy violations it may not be configured correctly. Conversely, if an On-Demand Scan produces excessive false positives you may need to adjust the scan criteria. | Select from your active On-Demand Scans. |
| Severity | The recorded severity level of the policy violation. Severity level is defined by the user during DLP policy creation. You can use this Omnibar facet to manage your remediation workflow; filtering based on severity level allows your remediators to focus on the highest priority violations first. | High Medium Low |
| Sharing | If the content is included in a shared folder or external link within the CSP. Some companies view policy violations for files shared outside of the company more harshly than files that remain internal. You can use this Omnibar facet to provide better insight on how your users are interacting with the cloud and better determine the significance of the policy violation. | Content Shared Externally Content Not Shared Externally |
| Status | The current state of the policy violation. Status is set by the user in the policy violation platform. You can use this Omnibar facet to manage your remediation workflow; remediators can filter to only New policies to tackle the incoming violations or filter out any violations that have been marked as False Positive. | New Open False Positive Resolved Archived |
| User | The user who triggered the policy violation. You can use this Omnibar facet to investigate specific users. If a single user is generating excessive policy violations, they may need to be investigated. | Select between all users who have triggered a DLP policy violation. |
| File Name | The name of the file matching the DLP policy rule. You can use this Omnibar facet to locate policy violations centering on a specific file. | All detected files can be used in this search filter. |
| File Type | The format of the file matching the DLP policy rule. You can use this Omnibar facet to filter results around a specific file format in order to better tune policies that control which formats can be shared. For example, if you have a policy that only allows PDFs to be shared, you could use the File Type filter to confirm that .DOC or .XLS files are triggering policy violations. | [One or more formats can be selected from any of the Skyhigh CASB supported formats.](https://success.myshn.net/Start_Here_with_Skyhigh/Skyhigh_Overview/Supported_File_Formats) |

|  |  |  |
| --- | --- | --- |
| Search Term | Description | Available Options |
| File Size | The detected file size of the file matching the DLP policy rule. You can use this Omnibar facet to filter results around the size of the file. Transfers of unusually large files may indicate potential data exfiltration events. Excessive transfers of unusually small files may indicate attempts to test security measures in preparation of a data theft incident. | Filter on file size based on KB, MB or GB. The filter can compare files against the user-entered value based on the following criteria: |
|  |  | * Equal To |
|  |  | * Greater Than |
|  |  | * Less Than |
|  |  | * Between |
| Incident ID | This Omnibar facet is reserved for internal functionality. | N/A |
| Match Count | The number of policy rule matches were found in the document that triggered the policy violation. You can use this Omnibar facet to filter results to investigate files that violate a policy in many places (as those indicate the highest risk violations) or to review files that have a small number of matches as those may indicate false positives or accidental violations. | Enter any integer to filter to the number of policy matches. |
| Policy | The name of the violated policy. You can use this Omnibar facet to review all policy violations from a specific policy. | [Select from any of your existing DLP policies.](https://success.myshn.net/Policy_Management/Data_Loss_Prevention_Policies/DLP_Policy_Rules_and_Rule_Groups) |
| Remediator | The remediator is the CASB user who has been assigned to investigate the policy violation. You can use this Omnibar facet to view the workflow of your remediators. | Select from any CASB user with the Policy Manager role to view any policy violations where that user is assigned as a remediator. |
| Response | The response action taken as a result of the policy violation. You can use this Omnibar facet to review policy responses and see how many policy violations are responded to in a certain way. | Select from Skyhigh's DLP response actions. |
| Scan Name | The name of the On-Demand Scan that detected the policy violation. You can use this Omnibar facet to review your On-Demand Scans; if an On-Demand Scan consistently runs without triggering any policy violations it may not be configured correctly. Conversely, if an On-Demand Scan produces excessive false positives you may need to adjust the scan criteria. | Select from your active On-Demand Scans. |

|  |  |  |
| --- | --- | --- |
| Search Term | Description | Available Options |
| Severity | [The recorded severity level of the policy violation. Severity level is defined by the user during DLP policy creation. You can use this Omnibar facet to manage your remediation workflow; filtering based on severity level allows your remediators to focus on the highest priority violations first.](https://success.myshn.net/Policy_Management/Data_Loss_Prevention_Policies/Creating_a_New_DLP_Policy) | High  Medium  Low |
| Sharing | If the content is included in a shared folder or external link within the CSP. Some companies view policy violations for files shared outside of the company more harshly than files that remain internal. You can use this Omnibar facet to provide better insight on how your users are interacting with the cloud and better determine the significance of the policy violation. | Content Shared Externally |
|  |  | Content Not Shared Externally |
| Status | [The current state of the policy violation. Status is set by the user in the policy violation platform. You can use this Omnibar facet to manage your remediation workflow; premeditators can filter to only New policies to tackle the incoming violations or filter out any violations that have been marked as False Positive.](https://success.myshn.net/Incident_Management_and_Threat_Protection/Policy_Incidents/Understanding_DLP_Violation_Statuses) | New |
|  |  | * Open * False Positive * Resolved * Archived |
| User | The user who triggered the policy violation. You can use this Omnibar facet to investigate specific users. If a single user is generating excessive policy violations, they may need to be investigated. | Select between all users who have triggered a DLP policy violation. |