IT Analytics™

Symantec Data Loss Prevention Content Pack Administrator Guide

Version 2.9.1

IT Analytics Symantec Data Loss Prevention Content Pack Administrator Guide

Product version 2.9.1

Documentation version: 1

This document was last updated on: April 22, 2020.

Copyright Statement

About this guide

Foreword

IT Analytics complements and expands upon the reporting and analytics offered by Symantec Data Loss Prevention. The capabilities provided within the IT Analytics Symantec Data Loss Prevention Content Pack allow customers to extract maximum value from the data contained within their Symantec Data Loss Prevention database(s). This product relies on a functional implementation of the IT Analytics Server version 2.9. The IT Analytics Server is the underlying technology that serves as a foundation for all the IT Analytics Content Packs.

By implementing the IT Analytics Symantec Data Loss Prevention Content Pack, you attain the following benefits:

- Unified view of data from multiple Symantec Data Loss Prevention databases
- Powerful on-the-fly forensic analysis through ad-hoc reports and charts, with pivot tables
- Out-of-the-box visually informative KPI scorecards, dashboards, and reports
- Replace time-consuming & complex customreporting

For more information about the IT Analytics Server version 2.9 installation guidelines, refer to the IT Analytics Server Administrator Guide. For more information about using the IT Analytics Portal, refer to the IT Analytics Portal User Guide.

This document provides guidance on how to install the IT Analytics Symantec Data Loss Prevention Content Pack into an IT Analytics Server. For additional assistance with the deployment of IT Analytics, please contact Support.

Style Conventions

This guidance uses the style conventions that are described in the following table.

Table 1-1 Style conventions for this document

Element	Meaning	
	Bold font	Signifies characters typed exactly as shown, including commands, switches, and file names. User interface elements also appear in bold.
	Italic font	Titles of books and other substantial publications appear in italic.
	Italic	Placeholders set in italic represent variables.

`Monospace font`	Defines code and script samples.
NOTE	Alerts the reader to supplementary information.

System Requirements

Deployment Infrastructure

IT Analytics Symantec Data Loss Prevention Content Pack requires a functional implementation of the IT Analytics Server version 2.9.1. For more information about the IT Analytics Server installation guidelines, please refer to the *IT Analytics Server Administrator Guide*. The IT Analytics Symantec Data Loss Prevention Content Pack supports existing implementations of Symantec Data Loss Prevention version 11.x, 12.x, 14.x, and 15.x.

Installing and Configuring the Content Pack

Configuring the Content Pack

Configure the Content Pack

To take advantage of your Content Pack you now have to configure it using the IT Analytics Portal and create at least one data source to associate with the Content Pack.

Adding a Connection

1. To configure connections to the Content Packs open the IT Analytics Portal in a browser at: http://*servername*:port/ITAnalytics/, where *servername* is the name of the IT Analytics Server.
1. Clicking on the Setting button in the toolbar, navigate to **Settings > Data Sources**. Under the Symantec Data Loss Prevention Content Pack, you should see the following text:

   IT Analytics Symantec Data Loss Prevention requires a connection to a Symantec Data Loss Prevention Database as data source before related cubes can be installed.

2. To the right of that text, click the **Settings** button and then **Add Connection** to access the connection wizard, then click **Next**.
3. On the **Database Settings Page**:
   - Enter the **Oracle Host Name** where the DLP database resides.
   - Enter the **Oracle Database Service Name (default is 'Protect')** where you want to pull the DLP data from.
   - Either select the default port to connect on, or if DLP was installed on a different port, enter that information.
   - The last section enter the proper **Symantec Data Loss Prevention Credentials** necessary to connect to the Oracle database.
4. Review the information on the Summary Page before clicking **Next** to create the connection.
5. Verify that the connection has been configured successfully and click **Finish**.
6. You can now install cubes and reports from the Symantec Data Loss Prevention Content Pack. To do so, please refer to the Cubes Installation and Reports Installation sections of this guide.
7. To add additional connections to other Symantec Data Loss Prevention Databases, click the **Settings** button to the right of the DLP Connections dropdown menu and select **Add Connection**. Follow steps 3 through 5 above to add an additional connection.

For more information about installing cubes and reports and processing cubes, please refer to the *IT Analytics Server Administrator Guide*.

Removing a Connection

1. To remove connections to the Content Packs open the IT Analytics Portal and navigate to Settings > Data Sources.
2. In the DLP Connections dropdown menu, select the connection you want to remove then click the Settings

button to the right and click Remove Connection.

3. Click OK to confirm the removal of that connection and the data sources page should refresh. Verify that connection is no longer displaying on the data sources page.

Note that removing a data source connection does not remove the cubes or cube data (if cubes are already installed and processed). However, if you have any processing jobs scheduled to run that utilize a connection that has been deleted, the processing jobs will fail.

Cubes Installation

Now that a connection to the Symantec Data Loss Prevention Manager database has been established, you will need to install the cubes from the Symantec Data Loss Prevention Content Pack.

Installing Cubes from the Content Pack

1. Once the appropriate data source connections have been established, you can install cubes available from the Content Packs you have already implemented. To install cubes in the IT Analytics Portal, navigate to **Settings > Cubes Installation**.

2. Select the Symantec Data Loss Prevention cubes you would like to install from the **Not Installed** section, or click **Select All** to specify all available cubes. You can select multiple cubes by holding down CTRL or SELECT and clicking on the cubes you want to install.
3. Click the **Install** to begin the installation the selected cubes.
4. You can monitor the progress of cube installation in the **IT Analytics Event Viewer**. When the status message **Cube install process has completed** appears, click **Close**.
5. On the **Cube Installation** tab, review that the selected cubes now appear in the **Installed** section. Click the **Refresh** button if necessary to ensure the latest update. Once installed, there should be a message next to each cube that states they require processing.

Reports Installation

Similar to installing the cubes, the out-of-the-box reports and dashboards can also be installed from the Symantec Data Loss Prevention Content Pack.

Installing Reports from a Content Pack

1. Once the appropriate data source connections have been established, you can install reports available from the Content Packs you have already implemented. To install reports in the IT Analytics Portal, navigate to **Settings > Reports Installation**.
2. Select the Symantec Data Loss Prevention reports you would like to install from the **Available for installation** section, or click **Select All** to choose all available reports. You can select multiple reports by holding down CTRL or SELECT and clicking on the reports you want to install.
3. Click the **Install** button to install the selected reports.
4. Monitor the progress of reports installation in the **IT Analytics Event Viewer**. When the status message
   Report install process has completed appears, click Close.
5. On the **Report Installation** tab, review that the selected reports now appear in the Installed section. Click the Refresh button if necessary to ensure the latest update. Once installed, there should be a message next to each report that states it is installed.

For more information about processing cubes, please refer to *the IT Analytics Server Administrator Guide*.

Content Pack Reporting Examples

This section is intended to provide step-by-step examples of using IT Analytics reporting specifically for the Symantec Data Loss Prevention Content Pack. Note that these examples do not cover all the reporting features of the IT Analytics Portal. For more information about using the IT Analytics Portal, refer to the *IT Analytics Portal User Guide*.

Example 1: Using the Cube Browser with the Symantec Data Loss Prevention Content Pack

The IT Analytics Cube Browser provides an interactive view of an OLAP cube. You can use it to dynamically analyze data from within the IT Analytics Portal and create views by easily dragging and dropping fields in place. The cube browser lets you view, organize, and summarize data into on-demand, personalized reports.

Creating a cube view using the DLP Incident Summary Cube

NOTE: To follow this example you must have IT Analytics Symantec Data Loss Prevention Content Pack installed on your system and all cubes must be processed. While this is just one example, you can apply similar configuration tactics to create any cube views.

To create a DLP Incident Summary cube view

1. Open the IT Analytics Portal in a browser at: http://*servername:port*/ITAnalytics/, where *servername* is the name of the IT Analytics Server.
2. In the left navigation, expand the **Cubes** folder.
3. Choose the **DLP Incident Summary** cube to load the cube in the browser.

4. In the Field List section on the right, expand **Measures** (denoted by the icon) and then expand **Incidents**.
5. Click **Incident Count** to select the measure value and drag it to the left-hand portion of the window, where it states “Add measures from the field list to view data from this cube.” Measures, or totals, are the aggregate summary counts for each cube. Alternatively, you can drag the **Incident Count** measure into the **Measures** window in the Cube View Configuration Section at the bottom of the screen.
6. From the Field List, expand the **DLP Incident Severity** dimension (denoted by the icon) then click **Incident - Severity**, and drag it over the value cell for the **Incident Count** measure you displayed in the previous step to display these values across rows. This field indicates the severity of all incidents. Alternatively, you can drag the **Incident – Severity** dimension to the **Rows** window in the Cube View Configuration section.
7. From the Field List, expand the **DLP Incident Status** dimension, click **Incident - Status**, and drag it in between **Incident - Severity** and **Incident Count** in the cube viewer window. Alternatively, you can drag **Incident - Status** to the **Rows** window in the Cube View Configuration section, underneath **Incident - Severity.**
8. Because you already have an existing field (**Incident - Severity**), you have the option to place the new field before or after the existing field. Simply click on the column header and move it in front, or rearrange the order in the Cube View Configuration section below. You can move the field to different places in order to dynamically change how your data is presented.
9. From the Field List expand the **DLP Incident Type** dimension, click **Incident - Type**, and then drag it over the **Incident Count** header to display values across columns. This field displays a breakdown of incident type (Discover, Endpoint or Network). Alternatively, you can drag **Incident - Type** to the **Columns** window in the Cube View Configuration section.

10. From the Field List expand the **DLP Policy Summary** dimension, click **Policy - Name**, and drag it to the **Filters** window in the Cube View Configuration section. This field displays the list of DLP policies enabled in your environment. Dropping it into the Filter area allows you to filter the report by specific policy.
11. To filter on a specific value, right-click on the **Policy - Name** dimension in the **Filters** window and select **Manage Filters**. Choose to include or exclude specific policies by checking or unchecking specific values, then click **OK**. The data in the cube view will refresh to reflect your filter selection.
12. Expand the **Incident - Severity** row by clicking the plus sign (+) next to the 'Yes' or 'No' value. You can now view a breakdown of incident count by severity and status across incident types, for the policy you filtered on.

Using additional features of the cube browser

1. Using the example above, you can hover your mouse over any value cell in the report to display a contextually aware pop-up chart to get a different view of your data.
2. For more robust charting options, right-click on the cell that represents the total number of clients in the report (lower-right hand corner) and select a chart format (pie, bar, column, etc.). This will pop-up a new window to display the chart and that window can be minimized and saved within the cube view for easy access.
3. To display the data in the report in a more grid like fashion (rather than expanding each dimension to see the data) you can opt for a details view. For example, expand the **DLP Incident** dimension and click on **Incident - ID** and drag it to the Details window of the Cube View Configuration section.
4. Right-click on the cell that represents the total number of incidents in the report (lower-right hand corner) and select **View Details**. This will pop-up a new window to display the data in a more tabular or grid format, and you have the ability to sort columns, search for data strings or export this data to Excel or as a CSV file. As with the chart windows, you can minimize this details view to the cube view or convenient access.

For more information on additional features within the IT Analytics Portal, refer to the *IT Analytics Portal User Guide*.

Example 2: Creating a Key Performance Indicator (KPI) with the Symantec Data Loss Prevention Content Pack

IT Analytics Symantec Data Loss Prevention Content Pack lets you create Key Performance Indicators (KPIs) by manually defining them in the cube viewer. KPIs are defined as quantifiable measures that represent a critical success factor in an organization. The emphasis is on the action of quantifying something in the environment. For example, the KPIs must be measurable to successfully be monitored and compared against a given objective.

Creating a Key Performance Indicator using the DLP Incident Summary Cube

In the IT Analytics Symantec Data Loss Prevention Content Pack, KPIs are created from existing measures. However, not all measures are good candidates for KPI utilization. A measure should be leveraged in a KPI only if it represents a critical success factor to gauge performance. Besides being measurable and
performance-oriented, KPIs should be used to track progress against the strategic and typically long-

term goals that remain fairly static in nature.

NOTE: To follow this example you must have IT Analytics Symantec Data Loss Prevention Content Pack installed on your system and all cubes must be processed. While this is just one example, you can apply similar configuration tactics to create other KPIs.

To create Key Performance Indicators

1. Open the IT Analytics Portal in a browser at: http://<servername:port>/ITAnalytics/, where <servername> is the name of the IT Analytics Server.
2. In the left navigation, expand the Cubes folder.
3. Choose the **DLP Incident Summary** cube to load the cube in the browser.
4. In the Field List section on the right, expand **Measures** (denoted by the icon) and then expand **Incident Count**.
5. Click **Incident Count** to select the measure value and drag it to the left-hand portion of the window, where it states “Add measures from the field list to view data from this cube.” Measures, or totals, are the aggregate summary counts for each cube. Alternatively, you can drag the **Incident Count** measure into the **Measures** window in the Cube View Configuration Section at the bottom of the screen.
6. From the Field List, expand the **DLP Incident Severity** dimension (denoted by the icon) then click **Incident - Severity**, and drag it over the value cell for the **Incident Count** measure you displayed in the previous step to display these values across rows. This field indicates the severity level across all incidents. Alternatively, you can drag the **Incident - Severity** dimension to the **Rows** window in the Cube View Configuration section.
7. Right-click the cell in the cube view that represents incident count with high severity and click **Create KPI from Selected Cell**.
8. In the resulting New KPI pop-up window, you will see the following options:
   - **Selected value with no goal** - Select this KPI if you simply want to tag a value and watch it.
   - **Selected value with a goal of zero** - Select this KPI if the goal is for the selected value to equal zero.
   - **Percentage of a selected value with a goal of zero percent** - Select this KPI if the goal is for the selected value to be as close to zero percent as possible. If you select this KPI you will be asked to select another cell to use as the denominator in order to determine the percentage.
   - **Percentage of a selected value with a goal of 100%** - Select this KPI if the goal is for the selected value to be equal to hundred percent. If you select this KPI you will be asked to select another cell to use as the denominator in order to determine the percentage.
9. For this example, we will choose **Percentage of a selected value with a goal of 100%** since our goal is to have all machines with firewall enabled, then click **Next**.
10. We now need to choose a second value, which will represent the total number of incidents in our environment. Click **Select Second Cell** and then right-click the value for total **Incident Count** and select **Add selected cell to new KPI definition**. You should see a confirmation that the second cell was successfully selected, then click **Next**.
11. For the status graphic, select **Gauge – Descending**. You can leave the threshold values as is, or modify the percentages as needed. For example, you can input 5 for green and 20 for yellow.
12. For the trend indicator, select **Compare Current Period to Previous Period**, then ensure the following are filled out:
    - **Date Attribute:** Detection - Date
    - **Number of Days in Period Comparison:** 30

- **Graphic:** Standard Arrow – Descending (this denotes that you want the trend to be going down, and as such the arrow will be colored accordingly – red for increasing, green for decreasing)

13. Click **Next** to save the KPI and give it a relevant name, such as **Percent of DLP High Severity Incidents** Then click **Next**.
14. Review the KPI settings and if satisfied, click **Next**.
15. Verify the KPI has been saved successfully and click **Finish** to close the wizard.
16. On the left navigation menu, click **Key Performance Indicators**. The new KPI should now display in the list under the DLP Incident Summary cube, with the current value and trend graphic already defined.

For more information on additional features within the IT Analytics Portal, refer to the IT Analytics Portal User Guide.

Content PackDescription

Cubes

The following is a list of default cubes provided within the IT Analytics Symantec Data Loss Prevention Content Pack, with their associated fields and KPIs (if applicable) as reference.

DLP Agent Status Cube

Contains information about the status of the DLP agents in the Data Lost
Prevention environment, including details about agents that didn't violate any of the DLP policies. Information specific to this cube includes the total number of incidents, number of agents, agent status, agent name, IP address and more.

Dimensions

- **Agent - AD User Name**: User logged on to the endpoint computer at the time AD resolution is run
- **Agent – Investigating**: Denotes whether or not the agent's status is set to Under Investigation
- **Agent – IP Address**: IP Address on the endpoint computer
- **Agent – Is Deleted**: Denotes whether or not the agent has been deleted from the endpoint server
- **Agent – Name**: Endpoint computer name
- **Agent On or Off the Network**: Indicates whether the agent is on or off the corporate network
- **Agent – Status**: Endpoint agent's status
- **Agent – Version**: Endpoint agent's full version number
- **Agent – Major Version**: Endpoint agent's version number up to the third decimal place. This allows minor versions to be grouped more easily.
- **DLP Agent Last Connection Date – Date**: Date the agent last connected to the endpoint server
- **DLP Agent Last Connection Date – Date Range**: Date range the agent last connected to the endpoint server

- **DLP Agent Last Connection Date – Day of Week**: Day the agent last connected to the endpoint server
- **DLP Agent Last Connection Date – Month**: Month the agent last connected to the endpoint server
- **DLP Agent Last Connection Date – Quarter**: Quarter the agent last connected to the endpoint server
- **DLP Agent Last Connection Date – Week Number**: Week number the agent last connected to the endpoint server
- **DLP Agent Last Connection Date – Year**: Year the agent last connected to the endpoint server
- **DLP Last Connection – Hour**: Hour the agent last connected to the endpoint server
- **DLP Last Connection – Minute**: Minute the agent last connected to the endpoint server
- **DLP Last Connection – Second**: Second the agent last connected to the endpoint server
- **DLP Last Connection – Time**: Time the agent last connected to the endpoint server
- **Endpoint Server – Name**: Endpoint server name
- **Oracle Database - Host Name**: Denotes the oracle database name and instance name from which the data is obtained

Measures

Agents Count	Total number of agents.
Incidents Count	Total number of Endpoint incidents.

DLP Discover Incident Details Cube

Contains information about incidents discovered by a Discover Data Loss
Prevention scan as well as the conditions that triggered those incidents. Information specific to this cube includes the total number of incidents, number of violations, the name of the policy that generated the incident, the conditions within those policies, the incident severity, status, and all custom attributes with its corresponding attribute values given during the remediation process.

Dimensions

- **Condition – Detection or Group**: Indicates whether the condition belongs to one of two rule types
- **Condition – ID**: Condition ID
- **Condition – Is Latest**: Indicates whether or not this is the latest version of the condition
- **Condition – Minimum Matches**: Specifies the minimum number of matches required to trigger the condition and generate an incident
- **Condition – Processing Order**: Denotes the order in which conditions are processed
- **Condition – Rule or Exception**: Indicates whether the condition was added as a rule or as an exception
- **Condition - Status**: Captures historical changes of the condition status
- **Condition – Type**: Describes the type of matching used in the condition
- **Condition – Unique or Multiple Matches**: Indicates the match counting type selected in the condition
- **Rule – Name**: Name given to the detection or exception rule.
- **Custom Attribute – Name**: Lists all user-defined custom attributes
- **Custom Attribute – Value**: Lists values assigned to the custom attributes
- **Data Owner – Name**: Name of the person responsible for remediating the incident
- **Data Owner – Email**: Email address of the person responsible for

remediating the incident.

- **Detection – Date**: Incident detection date as reported by the detection server
- **Detection – Date Range**: Incident detection date range as reported by the detection server
- **Detection – Day of Week**: Incident detection day as reported by the detection server
- **Detection – Month**: Incident detection month as reported by the detection server
- **Detection – Quarter**: Incident detection quarter as reported by the detection server
- **Detection – Week Number**: Incident detection week number as reported by the detection server
- **Detection – Year**: Incident detection year as reported by the detection server
- **Detection – Hour**: Incident detection hour as reported by the detection server
- **Detection – Minute**: Incident detection minute as reported by the detection server
- **Detection – Second**: Incident detection second as reported by the detection server
- **Detection – Time**: Incident detection time as reported by the detection server
- **Discover Incident – ContentRoot**: Lists Content Roots that were scanned by the discover server
- **Discover Incident – Document Name**: Name of the file that triggered the incident
- **Discover Incident – File Owner**: Creator of the file or item that triggered the incident
- **Discover Incident – Repository Location**: Full path of the file that triggered the incident
- **Discover Incident – Scanned Machine**: Host name of the scanned computer
- **Discover Incident – Target Type**: Discover target type
- **Discover Incident – File Location**: Full path of the file that triggered the incident
- **Discover Incident – ACL Type**: ACL permission type Note: Possible values are: File

- **Discover Incident – Grant or Deny**: Indicates whether the ACL type assigned permission is grant or deny
- **Discover Incident – File Permission**: Permission assignment corresponding to the Grant or Deny dimension
- **Discover Incident – File Permission Username**: Username or group granted the given file permission
- **Discover Incident – Protect Status**: Indicates the remediation action taken on the discovered file
- **Discover Scan – In Process Scan**: Indicates whether or not the scan is in progress
- **Discover Scan – Initial Scan**: Indicates whether or not this is the first scan performed on the discover target
- **Discover Scan – Instance ID**: Discover scan instance ID
- **Discover Scan – Last Completed Scan**: Indicates whether or not this is the last scan performed on the discover target
- **Discover Scan – Target Type**: Denotes the type of data repository being scanned
- **Discover Server – Name**: Discover server name
- **Discover Target – Name**: Discover target name as shown in the Enforce console
- **Incident – ID**: Incident – ID
- **Message Component – Document Format**: File format used in the message
- **Message Component – MIME Type**: MIME type used in the message
- **Message Component – Name**: Name used in the message
- **Incident – Severity**: Incident severity
- **Incident – Status**: Incident status as shown in the incident snapshot
- **Incident – Status Group**: Incident status group as defined in the Enforce console
- **Message – Date**: Date the message was received by the detection server or endpoint client
- **Message – Date Range**: Date range the message was received by the detection server or endpoint client
- **Message – Day of Week**: Day the message was received by the detection server or endpoint client

- **Message – Month**: Month the message was received by the detection server or endpoint client
- **Message – Quarter**: Quarter the message was received by the detection server or endpoint client
- **Message – Week Number**: Week number the message was received by the detection server or endpoint client
- **Message – Year**: Year the message was received by the detection server or endpoint client
- **Message – Hour**: Hour the message was received by the detection server or endpoint client
- **Message – Minute**: Minute the message was received by the detection server or endpoint client
- **Message – Second**: Second the message was received by the detection server or endpoint client
- **Message – Time**: Time the message was received by the detection server or endpoint client
- **Oracle Database – Host Name**: Denotes the oracle database name and instance name from which the data is obtained
- **Policy – Description**: Policy description as displayed in the Enforce console
- **Policy – ID**: Policy ID
- **Policy – Is Deleted**: Indicates whether or not the policy has been deleted
- **Policy – Is Latest Version**: Indicates whether or not the policy version is the latest
- **Policy – Name**: Policy name
- **Policy – Status**: Indicates whether the policy is active or inactive
- **Policy – Version**: Policy version number
- **Policy – Group Name**: Policy Group names as defined in the Enforce console

Measures

Match	Total number of Discover matches. Count

Incidents Count	Total number of Discover incidents.

DLP Discover Incident Summary Cube

Contains information about incidents discovered by a Discover Data Loss
Prevention scan. Information specific to this cube includes the total number of incidents and matches, the name of the policy that generated the incident, the incident severity and status.

Dimensions

- **Custom Attribute – Name:** Lists all user-defined custom attributes
- **Custom Attribute – Value:** Lists values assigned to the custom attributes
- **Data Owner – Name:** Name of the person responsible for remediating the incident.
- **Data Owner – Email:** Email address of the person responsible for remediating the incident.
- **Detection – Date:** Incident detection date as reported by the detection server
- **Detection – Date Range:** Incident detection date range as reported by the detection server
- **Detection – Day of Week:** Incident detection day as reported by the detection server
- **Detection – Month:** Incident detection month as reported by the detection server
- **Detection – Quarter:** Incident detection quarter as reported by the detection server
- **Detection – Week Number:** Incident detection week number as reported by the detection server
- **Detection – Date:** Incident detection date as reported by the detection server
- **Detection – Date Range:** Incident detection date range as reported by the detection server
- **Detection – Day of Week:** Incident detection day as reported by the detection server
- **Detection – Month:** Incident detection month as reported by the detection server
- **Detection – Quarter:** Incident detection quarter as reported by the detection server

- **Detection – Week Number:** Incident detection week number as reported by the detection server
- **Detection – Year:** Incident detection year as reported by the detection server
- **Detection – Hour:** Incident detection hour as reported by the detection server
- **Detection – Minute:** Incident detection minute as reported by the detection server
- **Detection – Second:** Incident detection second as reported by the detection server
- **Detection – Time:** Incident detection time as reported by the detection server
- **Discover Incident – ContentRoot:** Lists Content Roots that were scanned by the discover server
- **Discover Incident – Document Name:** Name of the file that triggered the incident
- **Discover Incident – File Owner:** Creator of the file or item that triggered the incident
- **Discover Incident – Repository Location:** Full path of the file that triggered the incident
- **Discover Incident – Scanned Machine:** Host name of the scanned computer
- **Discover Incident – Target Type:** Discover target type
- **Discover Incident – File Location:** Full path of the file that triggered the incident
- **Discover Incident – ACL Type:** ACL permission type Note: Possible values are: File
- **Discover Incident – Grant or Deny:** Indicates whether the ACL type assigned permission is grant or deny
- **Discover Incident – File Permission:** Permission assignment corresponding to the Grant or Deny dimension
- **Discover Incident – File Permission Username:** Username or group granted the given file permission
- **Discover Incident – Protect Status:** Indicates the remediation action taken on the discovered file
- **Discover Scan – In Process Scan:** Indicates whether or not the scan is in progress

- **Discover Scan – Initial Scan:** Indicates whether or not this is the first scan performed on the discover target
- **Discover Scan – Instance ID:** Discover scan instance ID
- **Discover Scan – Last Completed Scan:** Indicates whether or not this is the last scan performed on the discover target
- **Discover Scan – Target Type:** Denotes the type of data repository being scanned
- **Discover Server – Name:** Discover server name
- **Discover Target – Name:** Discover target name as shown in the Enforce console
- **Incident – ID:** Incident – ID
- **Message Component – Document Format:** File format used in the message
- **Message Component – MIME Type:** MIME type used in the message
- **Message Component – Name:** Name used in the message
- **Incident – Severity:** Incident severity
- **Incident – Status:** Incident status as shown in the incident snapshot
- **Incident – Status Group:** Incident status group as defined in the Enforce console
- **Message – Date:** Date the message was received by the detection server or endpoint client
- **Message – Date Range:** Date range the message was received by the detection server or endpoint client
- **Message – Day of Week:** Day the message was received by the detection server or endpoint client
- **Message – Month:** Month the message was received by the detection server or endpoint client
- **Message – Quarter:** Quarter the message was received by the detection server or endpoint client
- **Message – Week Number:** Week number the message was received by the detection server or endpoint client
- **Message – Year:** Year the message was received by the detection server or endpoint client
- **Message – Hour:** Hour the message was received by the detection server or endpoint client

- **Message – Minute:** Minute the message was received by the detection server or endpoint client
- **Message – Second:** Second the message was received by the detection server or endpoint client
- **Message – Time:** Time the message was received by the detection server or endpoint client
- **Oracle Database – Host Name:** Denotes the oracle database name and instance name from which the data is obtained
- **Policy – Group Name:** Policy Group names as defined in the Enforce console
- **Policy – Description:** Policy description as displayed in the Enforce console
- **Policy – ID:** Policy ID
- **Policy – Name:** Policy name
- **Policy – Status:** Indicates whether the policy is active or inactive

Measures

Match Count	Total number of Discover matches.
Incidents Count	Total number of Discover incidents.

DLP Discover Scans Cube

Contains information about discover scans that were performed on the environment, as well as the documents that were scanned. Information specific to this cube includes the number of scans performed, number of documents scanned, the time and duration of the scan, as well as the date and time the documents were last accessed and more.

Dimensions

- **Content Root Scan Started – Date:** Date the content root scan started
- **Content Root Scan Started – Date Range:** Date range the content root scan started
- **Content Root Scan Started – Day of Week:** Day the content root scan started
- **Content Root Scan Started – Month:** Month the content root scan started
- **Content Root Scan Started – Quarter:** Quarter the content root scan started
- **Content Root Scan Started – Week Number:** Week number the content root scan started
- **Content Root Scan Started – Year:** Year the content root scan started
- **Content Root Scan Started – Hour:** Hour the content root scan started
- **Content Root Scan Started – Minute:** Minute the content root scan started
- **Content Root Scan Started – Second:** Second the content root scan started
- **Content Root Scan Started – Time:** Time the content root scan started
- **Discover Incident – ContentRoot:** Lists Content Roots that were scanned by the discover server
- **Discover Incident – Document Name:** Name of the file that triggered the incident
- **Discover Incident – File Owner:** Creator of the file or item that triggered the incident
- **Discover Incident – Repository Location:** Full path of the file that triggered the incident

- **Discover Incident – Scanned Machine:** Host name of the scanned computer
- **Discover Incident – Target Type:** Discover target type
- **Discover Scan – In Process Scan:** Indicates whether or not the scan is in progress
- **Discover Scan – Initial Scan:** Indicates whether or not this is the first scan performed on the discover target
- **Discover Scan – Instance ID:** Discover scan instance ID
- **Discover Scan – Last Completed Scan:** Indicates whether or not this is the last scan performed on the discover target
- **Discover Scan – Target Type:** Denotes the type of data repository being scanned
- **Discover Server – Name:** Discover server name
- **Discover Target – Name:** Discover target name as shown in the Enforce console
- **File Created – Date:** Date the discovered file was created
- **File Created – Date Range:** Date range the discovered file was created
- **File Created – Day of Week:** Day the discovered file was created
- **File Created – Month:** Month the discovered file was created
- **File Created – Quarter:** Quarter the discovered file was created
- **File Created – Week Number:** Week number the discovered file was created
- **File Created – Year:** Year the discovered file was created
- **File Created – Hour:** Hour the discovered file was created
- **File Created – Minute:** Minute the discovered file was created
- **File Created – Second:** Second the discovered file was created
- **File Created – Time:** Time the discovered file was created
- **File Last Accessed – Date:** Date the discovered file was last accessed
- **File Last Accessed – Date Range:** Date range the discovered file was last accessed
- **File Last Accessed – Day of Week:** Day the discovered file was last accessed
- **File Last Accessed – Month:** Month the discovered file

was last accessed

- **File Last Accessed – Quarter:** Quarter the discovered file was last accessed
- **File Last Accessed – Week Number:** Week number the discovered file was last accessed
- **File Last Accessed – Year:** Year the discovered file was last accessed
- **File Last Accessed – Hour:** Hour the discovered file was last accessed
- **File Last Accessed – Minute:** Minute the discovered file was last accessed
- **File Last Accessed – Second:** Second the discovered file was last accessed
- **File Last Accessed – Time:** Time the discovered file was last accessed
- **Incident – Severity:** Incident – Severity
- **Last State Changed – Date:** Date the scan status last changed
- **Last State Changed – Date Range:** Date range the scan status last changed
- **Last State Changed – Day of Week:** Day of the week the scan status last changed
- **Last State Changed – Month:** Month the scan status last changed
- **Last State Changed – Quarter:** Quarter the scan status last changed
- **Last State Changed – Week Number:** Week number the scan status last changed
- **Last State Changed – Year:** Year the scan status last changed
- **Last State Changed – Hour:** Hour the scan status last changed
- **Last State Changed – Minute:** Minute the scan status last changed
- **Last State Changed – Second:** Second the scan status last changed
- **Last State Changed – Time:** Time the scan status last changed
- **Oracle Database – Host Name:** Denotes the oracle database name and instance name from which the data is obtained

- **Policy – Description:** Policy description as displayed in the Enforce console
- **Policy – ID:** Policy ID
- **Policy – Name:** Policy name

- **Policy – Status:** Indicates whether the policy is active or inactive
- **Scan Started – Date:** Date the discover target scan started
- **Scan Started – Date Range:** Date range the discover target scan started
- **Scan Started – Day of Week:** Day the discover target scan started
- **Scan Started – Month:** Month the discover target scan started
- **Scan Started – Quarter:** Quarter the discover target scan started
- **Scan Started – Week Number:** Week number the discover target scan started
- **Scan Started – Year:** Year the discover target scan started
- **Scan Started – Hour:** Hour the discover target scan started
- **Scan Started – Minute:** Minute the discover target scan started
- **Scan Started – Second:** Second the discover target scan started
- **Scan Started – Time:** Time the discover target scan started

Measures

Discovered File Count	Total number of files with sensitive information.
Bytes Filtered	Total number of bytes filtered during scanning.
Bytes Scanned	Total number of bytes scanned.
Content Root Elapsed Time	Total scan time.
Items Filtered	Total number of items skipped during scanning.

Items Unprocessable	Total number of unprocessable items.
Mbytes Filtered	Total number of MB filtered during scanning.

Mbytes Scanned	Total number of MB scanned.
Scan Count	Total number of discover scans.
Scanned File Count	Total number of scanned files.

Key Performance Indicators

Files Discovered in Last 30 Days Files

Scanned in Last 30 Days Gigabytes

Scanned in Last 30 Days

DLP Endpoint Incident Details Cube

Contains information about incidents generated by the Endpoint Data Loss Prevention product as well as the conditions that triggered those incidents. Information specific to this cube includes the total number of incidents, number of violations, the name of the policy that generated the incident, the conditions within those policies, the incident severity and status.

Dimensions

- **Agent – AD User Name:** User logged on to the endpoint computer at the time AD resolution is run
- **Agent – Investigating:** Denotes whether or not the agent's status is set to Under Investigation
- **Agent – IP Address:** IP Address on the endpoint computer
- **Agent – Is Deleted:** Denotes whether or not the agent has been deleted from the endpoint server
- **Agent – Name:** Endpoint computer name
- **Agent On or Off the Network:** Indicates whether the agent is on or off the corporate network
- **Agent – Status:** Endpoint agent's status
- **Agent – Version:** Endpoint agent's full version number
- **Agent – Major Version:** Endpoint agent's version number up to the third decimal place. This allows minor versions to be grouped more easily.
- **Condition – Detection or Group:** Indicates whether the condition belongs to one of two rule types
- **Condition – ID:** Condition ID
- **Condition – Is Latest:** Indicates whether or not this is the latest version of the condition
- **Condition – Minimum Matches:** Specifies the minimum number of matches required to trigger the condition and generate an incident
- **Condition – Processing Order:** Denotes the order in which conditions are processed
- **Condition – Rule or Exception:** Indicates whether the condition

was added as a rule or as an exception

- **Condition - Status:** Captures historical changes of the condition status
- **Condition – Type:** Describes the type of matching used in the condition
- **Condition – Unique or Multiple Matches:** Indicates the match counting type selected in the condition
- **Rule – Name:** Name given to the detection or exception rule.
- **Custom Attribute – Name:** Lists all user-defined custom attributes
- **Custom Attribute – Value:** Lists values assigned to the custom attributes
- **Data Owner – Name:** Name of the person responsible for remediating the incident
- **Data Owner – Email:** Email address of the person responsible for remediating the incident.
- **Detection – Date:** Incident detection date as reported by the detection server
- **Detection – Date Range:** Incident detection date range as reported by the detection server
- **Detection – Day of Week:** Incident detection day as reported by the detection server
- **Detection – Month:** Incident detection month as reported by the detection server
- **Detection – Quarter:** Incident detection quarter as reported by the detection server
- **Detection – Week Number:** Incident detection week number as reported by the detection server
- **Detection – Year:** Incident detection year as reported by the detection server
- **Detection – Hour:** Incident detection hour as reported by the detection server
- **Detection – Minute:** Incident detection minute as reported by the detection server
- **Detection – Second:** Incident detection second as reported by the detection server
- **Detection – Time:** Incident detection time as reported by the detection server
- **Endpoint Incident – Application Name:** The name of the application employed by the end user

- **Endpoint Incident – Device Type:** Lists the endpoint monitoring channel that triggered the incident
- **Endpoint Incident – File Name:** Destination name of the file or item that triggered the incident
- **Endpoint Incident – File Owner:** Creator of the file or item that triggered the incident
- **Endpoint Incident – File Path:** Full destination path of the file that triggered the incident
- **Endpoint Incident – Instance ID:** Endpoint device identifier on which the violation occurred
- **Endpoint Incident – IP Address:** IP address of the endpoint at the time the violation occurred
- **Endpoint Incident – Machine Name:** Name of the computer that triggered the incident
- **Endpoint Incident – On or Off the Network:** Indicates the agent location at the time the violation occurred
- **Endpoint Incident – Source File Name:** Name of the file or item that triggered the incident
- **Endpoint Incident – Source File Path:** Full path of the file that triggered the incident
- **Endpoint Incident – User Name:** Logged on user on the computer that triggered the incident
- **Endpoint Incident – Agent Response:** Response or action taken by the endpoint agent
- **Endpoint Incident – User Justification Response:** Justification response as defined in the Enforce console
- **Endpoint Incident – User Justification Type:** Justification type as defined in the Enforce console
- **Endpoint Server - Name:** Endpoint server name
- **Incident – ID:** Incident ID
- **Message Component – Document Format:** File format used in the message
- **Message Component – MIME Type:** MIME type used in the message
- **Message Component – Name:** Name used in the message
- **Incident – Severity:** Incident severity
- **Incident – Status:** Incident status as shown in the incident snapshot

- **Incident – Status Group:** Incident status group as defined in the Enforce console
- **Message – Date:** Date the message was received by the detection server or endpoint client
- **Message – Date Range:** Date range the message was received by the detection server or endpoint client
- **Message – Day of Week:** Day the message was received by the detection server or endpoint client
- **Message – Month:** Month the message was received by the detection server or endpoint client
- **Message – Quarter:** Quarter the message was received by the detection server or endpoint client
- **Message – Week Number:** Week number the message was received by the detection server or endpoint client
- **Message – Year:** Year the message was received by the detection server or endpoint client
- **Message – Hour:** Hour the message was received by the detection server or endpoint client
- **Message – Minute:** Minute the message was received by the detection server or endpoint client
- **Message – Second:** Second the message was received by the detection server or endpoint client
- **Message – Time:** Time the message was received by the detection server or endpoint client
- **Oracle Database – Host Name:** Denotes the oracle database name and instance name from which the data is obtained
- **Policy – Group Name:** Policy Group names as defined in the Enforce console
- **Policy – Description:** Policy description as displayed in the Enforce console
- **Policy – ID:** Policy ID
- **Policy – Name:** Policy name
- **Policy – Status:** Indicates whether the policy is active or inactive
- **Policy – Version:** Policy version number
- **Policy – Group Name:** Policy Group names as defined in the Enforce console

Measures

Agents Count	Total number of agents that generated incidents.
Incident Count	Total number of Endpoint incidents.
Match Count	Total number of Endpoint matches.

DLP Endpoint Incident Summary Cube

Contains information about incidents generated by the Endpoint Data Loss
Prevention product. Information specific to this cube includes the total number of incidents, number of violations, the name of the policy that generated the incident, the incident severity and status.

Dimensions

- **Agent – AD User Name:** User logged on to the endpoint computer at the time AD resolution is run
- **Agent – Investigating:** Denotes whether or not the agent's status is set to Under Investigation
- **Agent – IP Address:** IP Address on the endpoint computer
- **Agent – Is Deleted:** Denotes whether or not the agent has been deleted from the endpoint server
- **Agent – Name:** Endpoint computer name
- **Agent On or Off the Network:** Indicates whether the agent is on or off the corporate network
- **Agent – Status:** Endpoint agent's status
- **Agent – Version:** Endpoint agent's full version number
- **Agent – Major Version:** Endpoint agent's version number up to the third decimal place. This allows minor versions to be grouped more easily.
- **Custom Attribute – Name:** Lists all user-defined custom attributes
- **Custom Attribute – Value:** Lists values assigned to the custom attributes
- **Data Owner – Name:** Name of the person responsible for remediating the incident
- **Data Owner – Email:** Email address of the person responsible for remediating the incident.
- **Detection – Date:** Incident detection date as reported by the detection server
- **Detection – Date Range:** Incident detection date range as reported by the detection server
- **Detection – Day of Week:** Incident detection day as reported by the detection server
-

- ■ **Detection – Month:** Incident detection month as reported by the detection server
-
-
- ■ **Detection – Quarter:** Incident detection quarter as reported by the detection server
-
- ■ **Detection – Week Number:** Incident detection week number as reported by the detection server
-
- ■ **Detection – Year:** Incident detection year as reported by the detection server
-
- ■ **Detection Server – Name:** Detection server name as shown in the Systems Overview page
-
- ■ **Detection Server – Type:** Detection Server channel name as shown in the System Overview page
-
- ■ **Detection – Hour:** Incident detection hour as reported by the detection server
-
- ■ **Detection – Minute:** Incident detection minute as reported by the detection server
-
- ■ **Detection – Second:** Incident detection second as reported by the detection server
-
- ■ **Detection – Time:** Incident detection time as reported by the detection server
-
- ■ **Endpoint Incident – Application Name:** The name of the application employed by the end user
-
- ■ **Endpoint Incident – Device Type:** Lists the endpoint monitoring channel that triggered the incident

- **Endpoint Incident – File Name:** Destination name of the file or item that triggered the incident
- **Endpoint Incident – File Owner:** Creator of the file or item that triggered the incident
- **Endpoint Incident – File Path:** Full destination path of the file that triggered the incident
- **Endpoint Incident – Instance ID:** Endpoint device identifier on which the violation occurred
- **Endpoint Incident – IP Address:** IP address of the endpoint at the time the violation occurred
- **Endpoint Incident – Machine Name:** Name of the computer that triggered the incident
- **Endpoint Incident – On or Off the Network:** Indicates the agent location at the time the violation occurred
- **Endpoint Incident – Source File Name:** Name of the file or item that triggered the incident
- **Endpoint Incident – Source File Path:** Full path of the file that triggered the incident
- **Endpoint Incident – User Name:** Logged on user on the computer that triggered the incident
- **Endpoint Incident – Agent Response:** Response or action taken by the endpoint agent
- **Endpoint Incident – User Justification Response:** Justification response as defined in the Enforce console
- **Endpoint Incident – User Justification Type:** Justification type as defined in the Enforce console
- **Endpoint Server - Name:** Endpoint server name
- **Incident – ID:** Incident ID
- **Incident – Severity:** Incident severity
- **Incident – Status:** Incident status as shown in the incident snapshot
- **Incident – Status Group:** Incident status group as defined in the Enforce console
- **Message Component – Document Format:** File format used in the message
- **Message Component – MIME Type:** MIME type used in the message
- **Message Component – Name:** Name used in the message

- **Message – Date:** Date the message was received by the detection server or endpoint client
- **Message – Date Range:** Date range the message was received by the detection server or endpoint client
- **Message – Day of Week:** Day the message was received by the detection server or endpoint client
- **Message – Month:** Month the message was received by the detection server or endpoint client
- **Message – Quarter:** Quarter the message was received by the detection server or endpoint client
- **Message – Week Number:** Week number the message was received by the detection server or endpoint client
- **Message – Year:** Year the message was received by the detection server or endpoint client
- **Message – Hour:** Hour the message was received by the detection server or endpoint client
- **Message – Minute:** Minute the message was received by the detection server or endpoint client
- **Message – Second:** Second the message was received by the detection server or endpoint client
- **Message – Time:** Time the message was received by the detection server or endpoint client
- **Oracle Database – Host Name:** Denotes the oracle database name and instance name from which the data is obtained
- **Policy – Group Name:** Policy Group names as defined in the Enforce console
- **Policy – Description:** Policy description as displayed in the Enforce console
- **Policy – ID:** Policy ID
- **Policy – Name:** Policy name
- **Policy – Status:** Indicates whether the policy is active or inactive

Measures

Agents Count	Total number of agents that generated incidents.

Incident Count	Total number of Endpoint incidents.
Match Count	Total number of Endpoint matches.

DLP Incident Details Cube

Contains information about incidents generated by any Data Loss Prevention product as well as the conditions that triggered those incidents. Information specific to this cube includes the total number of incidents, number of violations, the name of the policy that generated the incident, the conditions within those policies, the incident severity, status and type.

Dimensions

- **Condition – Detection or Group**: Indicates whether the condition belongs to one of two rule types
- **Condition – ID**: Condition ID
- **Condition – Is Latest**: Indicates whether or not this is the latest version of the condition
- **Condition – Minimum Matches**: Specifies the minimum number of matches required to trigger the condition and generate an incident
- **Condition – Processing Order**: Denotes the order in which conditions are processed
- **Condition – Rule or Exception**: Indicates whether the condition was added as a rule or as an exception
- **Condition - Status**: Captures historical changes of the condition status
- **Condition – Type**: Describes the type of matching used in the condition
- **Condition – Unique or Multiple Matches**: Indicates the match counting type selected in the condition
- **Custom Attribute – Name**: Lists all user-defined custom attributes
- **Custom Attribute – Value**: Lists values assigned to the custom attributes
- **Data Owner – Name**: Name of the person responsible for remediating the incident
- **Data Owner – Email**: Email address of the person responsible for remediating the incident.
- **Detection – Date**: Incident detection date as reported by the detection server
- **Detection – Date Range**: Incident detection date range as reported by the detection server

- **Detection – Day of Week**: Incident detection day as reported by the detection server
- **Detection – Month**: Incident detection month as reported by the detection server
- **Detection – Quarter**: Incident detection quarter as reported by the detection server
- **Detection – Week Number**: Incident detection week number as reported by the detection server
- **Detection – Year**: Incident detection year as reported by the detection server
- **Detection Server – Name**: Detection server name as shown in the Systems Overview page
- **Detection Server – Type**: Detection Server channel name as shown in the System Overview page
- **Detection – Hour**: Incident detection hour as reported by the detection server
- **Detection – Minute**: Incident detection minute as reported by the detection server
- **Detection – Second**: Incident detection second as reported by the detection server
- **Detection – Time**: Incident detection time as reported by the detection server
- **Incident – ID**: Incident ID
- **Incident – Severity**: Incident severity
- **Incident – Status**: Incident status as shown in the incident snapshot
- **Incident – Status Group**: Incident status group as defined in the Enforce console
- **Incident – Product Area**: Incident type
- **Message Component – Document Format**: File format used in the message
- **Message Component – MIME Type**: MIME type used in the message
- **Message Component – Name**: Name used in the message
- **Message – Date**: Date the message was received by the detection server or endpoint client
- **Message – Date Range**: Date range the message was received by the detection server or endpoint client

- **Message – Day of Week**: Day the message was received by the detection server or endpoint client
- **Message – Month**: Month the message was received by the detection server or endpoint client
- **Message – Quarter**: Quarter the message was received by the detection server or endpoint client
- **Message – Week Number**: Week number the message was received by the detection server or endpoint client
- **Message – Year**: Year the message was received by the detection server or endpoint client
- **Message – Hour**: Hour the message was received by the detection server or endpoint client
- **Message – Minute**: Minute the message was received by the detection server or endpoint client
- **Message – Second**: Second the message was received by the detection server or endpoint client
- **Message – Time**: Time the message was received by the detection server or endpoint client
- **Oracle Database – Host Name**: Denotes the oracle database name and instance name from which the data is obtained
- **Policy – Description**: Policy description as displayed in the Enforce console
- **Policy – ID**: Policy ID
- **Policy – Is Deleted**: Indicates whether or not the policy has been deleted
- **Policy – Is Latest Version**: Indicates whether or not the policy version is the latest
- **Policy – Name**: Policy name
- **Policy – Status**: Indicates whether the policy is active or inactive
- **Policy – Version**: Policy version number
- **Policy – Group Name**: Policy Group names as defined in the Enforce console
- **Rule – Name**: Name given to the detection or exception rule

Measures

Incident Count Total number of incidents for all incident types.

Match Count	Total number of matches for all incident types.

DLP Incident History Cube

Contains historical information about incident actions (either by DLP user or by a DLP server) within the Data Loss Prevention system, including details about the type and the nature of the action. Information specific to this cube includes the total number of incident actions, date when the action was performed, who performed the action and more.

Dimensions

- **Incident – ID:** Incident ID
- **Incident History – Date:** Date the event occurred
- **Incident History – Date Range:** Date range the event occurred
- **Incident History – Day of Week:** Day the event occurred
- **Incident History – Month:** Month the event occurred
- **Incident History – Quarter:** Quarter the event occurred
- **Incident History – Week Number:** Week number the event occurred
- **Incident History – Year:** Year the event occurred
- **Incident History – Detail:** Free text description of the event
- **Incident History – Submitted By:** DLP user name who performed the action
- **Incident History – Hour:** Hour the event occurred
- **Incident History – Minute:** Minute the event occurred
- **Incident History – Second:** Second the event occurred
- **Incident History – Time:** Time the event occurred
- **Incident History – Type:** Type of event as shown in the history tab of the incident snapshot
- **Oracle Database – Host Name:** Denotes the oracle database name and instance name from which the data is obtained
- **Role – Description:** Role description as displayed in the Enforce console
- **Role – Name:** Role name as displayed in the Enforce console

Measures

Action Count	Total number of incident actions.

DLP Incident Status History

Contains historical information about incident status changes within the
Data Loss Prevention system, including details about who performed the change and when. Information specific to this cube includes the total number of incident actions, change date, username and more.

Dimensions

- **Change – Date:** Date the incident status was changed
- **Change – Date Range:** Date range the incident status was changed
- **Change – Day of Week:** Day the incident status was changed
- **Change – Month:** Month the incident status was changed
- **Change – Quarter:** Quarter the incident status was changed
- **Change – Week Number:** Week number the incident status was changed
- **Change – Year:** Year the incident status was changed
- **Change – Hour:** Hour the incident status was changed
- **Change – Minute:** Minute the incident status was changed
- **Change – Second:** Second the incident status was changed
- **Change – Time:** Time the incident status was changed
- **Change – User:** DLP user name that performed the change
- **Detection – Date:** Incident detection date as reported by the detection server
- **Detection – Date Range:** Incident detection date range as reported by the detection server
- **Detection – Day of Week:** Incident detection day as reported by the detection server
- **Detection – Month:** Incident detection month as reported by the detection server
- **Detection – Quarter:** Incident detection quarter as reported by the detection server
- **Detection – Week Number:** Incident detection week number as reported by the detection server
- **Detection – Year:** Incident detection year as reported by the detection server
- **Detection Server – Name:** Detection server name as shown in the Systems Overview page

- **Detection Server – Type:** Detection Server channel name as shown in the System Overview page
- **Detection – Hour:** Incident detection hour as reported by the detection server
- **Detection – Minute:** Incident detection minute as reported by the detection server
- **Detection – Second:** Incident detection second as reported by the detection server
- **Detection – Time:** Incident detection time as reported by the detection server
- **Incident – ID:** Incident ID
- **Incident – Next Status:** Next status assigned to the incident. If the incident status is not changed, next status will be set to unknown
- **Incident – Next Status Group:** Next status group as defined in the Enforce console
- **Incident – Severity:** Incident severity
- **Incident – Status:** Incident status as shown in the incident snapshot
- **Incident – Status Group:** Incident status group as defined in the Enforce console
- **Incident – Product Area:** Incident type
- **Next Change – Date:** Date when the Incident Next Status value was changed. If the status remains unchanged, this will show up as unknown
- **Next Change – Date Range:** Date range when the Incident Next Status value was changed. If the status remains unchanged, this will show up as unknown
- **Next Change – Day of Week:** Day when the Incident Next Status value was changed. If the status remains unchanged, this will show up as unknown
- **Next Change – Month:** Month when the Incident Next Status value was changed. If the status remains unchanged, this will show up as unknown
- **Next Change – Quarter:** Quarter when the Incident Next Status value was changed. If the status remains unchanged, this will show up as unknown

- **Next Change – Week Number:** Week number when the Incident Next Status value was changed. If the status remains unchanged, this will show up as unknown
- **Next Change – Year:** Year when the Incident Next Status value was changed. If the status remains unchanged, this will show up as unknown
- **Next Change – Hour:** Hour when the Incident Next Status value was changed. If the status remains unchanged, this will show up as unknown
- **Next Change – Minute:** Minute when the Incident Next Status value was changed. If the status remains unchanged, this will show up as unknown
- **Next Change – Second:** Second when the Incident Next Status value was changed. If the status remains unchanged, this will show up as unknown
- **Next Change – Time:** Time when the Incident Next Status value was changed. If the status remains unchanged, this will show up as unknown
- **Next Change – User:** DLP user who set the Incident Next Status value
- **Oracle Database – Host Name:** Denotes the oracle database name and instance name from which the data is obtained
- **Policy – Description:** Policy description as displayed in the Enforce console
- **Policy – ID:** Policy ID
- **Policy – Name:** Policy name
- **Policy – Status:** Indicates whether the policy is active or inactive
- **Role – Description:** Role description as displayed in the Enforce console
- **Role – Name:** Role name as displayed in the Enforce console

Measures

Incident Count Total number of incidents.

Seconds in Status	Total number of seconds in a given status
Second to Status	Total number of seconds to get to next status
Status Changes	Total number of status changes

DLP Incident Summary Cube

Contains information about incidents generated by any Data Loss Prevention product. Information specific to this cube includes the total number of incidents, number of violations, the name of the policy that generated the incident, the incident severity, status and type.

Dimensions

- **Custom Attribute – Name:** Lists all user-defined custom attributes
- **Custom Attribute – Value:** Lists values assigned to the custom attributes
- **Data Owner – Name:** Name of the person responsible for remediating the incident
- **Data Owner – Email:** Email address of the person responsible for remediating the incident.
- **Detection – Date:** Incident detection date as reported by the detection server
- **Detection – Date Range:** Incident detection date range as reported by the detection server
- **Detection – Day of Week:** Incident detection day as reported by the detection server
- **Detection – Month:** Incident detection month as reported by the detection server
- **Detection – Quarter:** Incident detection quarter as reported by the detection server
- **Detection – Week Number:** Incident detection week number as reported by the detection server
- **Detection – Year:** Incident detection year as reported by the detection server
- **Detection Server – Name:** Detection server name as shown in the Systems Overview page
- **Detection Server – Type:** Detection Server channel name as shown in the System Overview page
- **Detection – Hour:** Incident detection hour as reported by the detection server
- **Detection – Minute:** Incident detection minute as reported by the detection server

- **Detection – Second:** Incident detection second as reported by the detection server
- **Detection – Time:** Incident detection time as reported by the detection server
- **Endpoint Incident – Application Name:** The name of the application employed by the end user
- **Endpoint Incident – Device Type:** Lists the endpoint monitoring channel that triggered the incident
- **Endpoint Incident – File Name:** Destination name of the file or item that triggered the incident
- **Endpoint Incident – File Owner:** Creator of the file or item that triggered the incident
- **Endpoint Incident – File Path:** Full destination path of the file that triggered the incident
- **Endpoint Incident – Instance ID:** Endpoint device identifier on which the violation occurred
- **Endpoint Incident – IP Address:** IP address of the endpoint at the time the violation occurred
- **Endpoint Incident – Machine Name:** Name of the computer that triggered the incident
- **Endpoint Incident – On or Off the Network:** Indicates the agent location at the time the violation occurred
- **Endpoint Incident – Source File Name:** Name of the file or item that triggered the incident
- **Endpoint Incident – Source File Path:** Full path of the file that triggered the incident
- **Endpoint Incident – User Name:** Logged on user on the computer that triggered the incident
- **Incident – ID:** Incident ID
- **Incident – Severity:** Incident severity
- **Incident – Status:** Incident status as shown in the incident snapshot
- **Incident – Status Group:** Incident status group as defined in the Enforce console
- **Incident – Product Area:** Incident type
- **Message Component – Document Format:** File format used in the message

- **Message Component – MIME Type:** MIME type used in the message
- **Message Component – Name:** Name used in the message
- **Message – Date:** Date the message was received by the detection server or endpoint client
- **Message – Date Range:** Date range the message was received by the detection server or endpoint client
- **Message – Day of Week:** Day the message was received by the detection server or endpoint client
- **Message – Month:** Month the message was received by the detection server or endpoint client
- **Message – Quarter:** Quarter the message was received by the detection server or endpoint client
- **Message – Week Number:** Week number the message was received by the detection server or endpoint client
- **Message – Year:** Year the message was received by the detection server or endpoint client
- **Message – Hour:** Hour the message was received by the detection server or endpoint client
- **Message – Minute:** Minute the message was received by the detection server or endpoint client
- **Message – Second:** Second the message was received by the detection server or endpoint client
- **Message – Time:** Time the message was received by the detection server or endpoint client
- **Network Incident – Message Subject:** Subject line of email message. In the case of a web violation, this will show as HTTP incident.
- **Network Incident – Sender Name:** Sender email address or IP address
- **Oracle Database – Host Name:** Denotes the oracle database name and instance name from which the data is obtained
- **Policy – Group Name:** Policy Group names as defined in the Enforce console
- **Policy – Description:** Policy description as displayed in the Enforce console
- **Policy – ID:** Policy ID

- **Policy – Name:** Policy name

- **Policy – Status:** Indicates whether the policy is active or inactive

Measures

Incident Count	Total number of incidents for all incident types.
Match Count	Total number of matches for all incident types.

Key Performance Indicators

Incidents Detected in Last 30 Days New High Severity Incidents

Number of False Positives in last 30 days

DLP Network Incident Details Cube

Contains information about incidents generated by the Network Data Loss
Prevention product as well as the conditions that triggered those incidents. Information specific to this cube includes the total number of incidents, number of violations, the name of the policy that generated the incident, the conditions within those policies, the incident severity and status and more.

Dimensions

- **Condition – Detection or Group:** Indicates whether the condition belongs to one of two rule types
- **Condition – ID:** Condition ID
- **Condition – Is Latest:** Indicates whether or not this is the latest version of the condition
- **Condition – Minimum Matches:** Specifies the minimum number of matches required to trigger the condition and generate an incident
- **Condition – Processing Order:** Denotes the order in which conditions are processed
- **Condition – Rule or Exception:** Indicates whether the condition was added as a rule or as an exception
- **Condition - Status:** Captures historical changes of the condition status
- **Condition – Type:** Describes the type of matching used in the condition
- **Condition – Unique or Multiple Matches:** Indicates the match counting type selected in the condition
- **Custom Attribute – Name:** Lists all user-defined custom attributes
- **Custom Attribute – Value:** Lists values assigned to the custom attributes
- **Data Owner – Name:** Name of the person responsible for remediating the incident
- **Data Owner – Email:** Email address of the person responsible for remediating the incident.
- **Detection – Date:** Incident detection date as reported by the detection server

- **Detection – Date Range:** Incident detection date range as reported by the detection server
- **Detection – Day of Week:** Incident detection day as reported by the detection server
- **Detection – Month:** Incident detection month as reported by the detection server
- **Detection – Quarter:** Incident detection quarter as reported by the detection server
- **Detection – Week Number:** Incident detection week number as reported by the detection server
- **Detection – Year:** Incident detection year as reported by the detection server
- **Detection Server – Name:** Detection server name as shown in the Systems Overview page
- **Detection Server – Type:** Detection Server channel name as shown in the System Overview page
- **Detection – Hour:** Incident detection hour as reported by the detection server
- **Detection – Minute:** Incident detection minute as reported by the detection server
- **Detection – Second:** Incident detection second as reported by the detection server
- **Detection – Time:** Incident detection time as reported by the detection server
- **Incident – ID:** Incident ID
- **Incident – Severity:** Incident severity
- **Incident – Status:** Incident status as shown in the incident snapshot
- **Incident – Status Group:** Incident status group as defined in the Enforce console
- **Message Component – Document Format:** File format used in the message
- **Message Component – MIME Type:** MIME type used in the message
- **Message Component – Name:** Name used in the message
- **Network Incident – Message Subject:** Subject line of email message. In the case of a web violation, this will show as HTTP incident.

- **Network Incident – Sender Name:** Sender email address or IP address
- **Network Incident – Recipient Domain:** Recipient domain name or IP address
- **Network Incident – Recipient Name:** Recipient email address, IP address, or web address
- **Network Incident – Prevent Action:** Action taken by the Network Prevent server
- **Network Incident – Protocol:** Network protocol name
- **Oracle Database – Host Name:** Denotes the oracle database name and instance name from which the data is obtained
- **Policy – Description:** Policy description as displayed in the Enforce console
- **Policy – ID:** Policy ID
- **Policy – Is Deleted:** Indicates whether or not the policy has been deleted
- **Policy – Is Latest Version:** Indicates whether or not the policy version is the latest
- **Policy – Name:** Policy name
- **Policy – Status:** Indicates whether the policy is active or inactive
- **Policy – Version:** Policy version number
- **Policy – Group Name:** Policy Group names as defined in the Enforce console
- **Rule – Name:** Name given to the detection or exception rule

Measures

Incident Count	Total number of Network incidents.
Match Count	Total number of Network matches.

DLP Network Incident Summary Cube

Contains information about incidents generated by the Network Data Loss
Prevention product. Information specific to this cube includes the total number of incidents, number of violations, the name of the policy that generated the incident, the incident severity and status.

Dimensions

- **Custom Attribute – Name:** Lists all user-defined custom attributes
- **Custom Attribute – Value:** Lists values assigned to the custom attributes
- **Data Owner – Name:** Name of the person responsible for remediating the incident
- **Data Owner – Email:** Email address of the person responsible for remediating the incident.
- **Detection – Date:** Incident detection date as reported by the detection server
- **Detection – Date Range:** Incident detection date range as reported by the detection server
- **Detection – Day of Week:** Incident detection day as reported by the detection server
- **Detection – Month:** Incident detection month as reported by the detection server
- **Detection – Quarter:** Incident detection quarter as reported by the detection server
- **Detection – Week Number:** Incident detection week number as reported by the detection server
- **Detection – Year:** Incident detection year as reported by the detection server
- **Detection Server – Name:** Detection server name as shown in the Systems Overview page
- **Detection Server – Type:** Detection Server channel name as shown in the System Overview page
- **Detection – Hour:** Incident detection hour as reported by the detection server
- **Detection – Minute:** Incident detection minute as reported by the detection server

- **Detection – Second:** Incident detection second as reported by the detection server
- **Detection – Time:** Incident detection time as reported by the detection server
- **Incident – ID:** Incident ID
- **Incident – Severity:** Incident severity
- **Incident – Status:** Incident status as shown in the incident snapshot
- **Incident – Status Group:** Incident status group as defined in the Enforce console
- **Message Component – Document Format:** File format used in the message
- **Message Component – MIME Type:** MIME type used in the message
- **Message Component – Name:** Name used in the message
- **Message – Date:** Date the message was received by the detection server or endpoint client
- **Message – Date Range:** Date range the message was received by the detection server or endpoint client
- **Message – Day of Week:** Day the message was received by the detection server or endpoint client
- **Message – Month:** Month the message was received by the detection server or endpoint client
- **Message – Quarter:** Quarter the message was received by the detection server or endpoint client
- **Message – Week Number:** Week number the message was received by the detection server or endpoint client
- **Message – Year:** Year the message was received by the detection server or endpoint client
- **Message – Hour:** Hour the message was received by the detection server or endpoint client
- **Message – Minute:** Minute the message was received by the detection server or endpoint client
- **Message – Second:** Second the message was received by the detection server or endpoint client
- **Message – Time:** Time the message was received by the detection server or endpoint client
- **Network Incident – Message Subject:** Subject line of email message. In the case of a web violation, this will show as

HTTP incident.

- **Network Incident – Sender Name:** Sender email address or IP address
- **Network Incident – Recipient Domain:** Recipient domain name or IP address
- **Network Incident – Recipient Name:** Recipient email address, IP address, or web address
- **Network Incident – Prevent Action:** Action taken by the Network Prevent server
- **Oracle Database – Host Name:** Denotes the oracle database name and instance name from which the data is obtained
- **Policy – Group Name:** Policy Group names as defined in the Enforce console
- **Policy – Description:** Policy description as displayed in the Enforce console
- **Policy – ID:** Policy ID
- **Policy – Name:** Policy name
- **Policy – Status:** Indicates whether the policy is active or inactive

Measures

Incident Count	Total number of Network incidents.
Match Count	Total number of Network matches.

DLP Network Statistics Cube

Contains information about statistics for network messages. Information
specific to this cube includes the total number of incidents and messages by protocol and detection server.

Dimensions

- **Captured – Date:** Date the message was captured by the detection server
- **Captured – Date Range:** Date range the message was captured by the detection server
- **Captured – Day of Week:** Day the message was captured by the detection server
- **Captured – Month:** Month the message was captured by the detection server
- **Captured – Quarter:** Quarter the message was captured by the detection server
- **Captured – Week Number:** Week number the message was captured by the detection server
- **Captured – Year:** Year the message was captured by the detection server
- **Detection Server – Name:** Detection server name as shown in the Systems Overview page
- **Detection Server – Type:** Detection Server channel name as shown in the System Overview page
- **Incident – Severity:** Incident severity
- **Network Incident – Protocol:** Network protocol name
- **Oracle Database – Host Name:** Denotes the oracle database name and instance name from which the data is obtained
- **Policy – Description:** Policy description as displayed in the Enforce console
- **Policy – ID:** Policy ID
- **Policy – Name:** Policy name
- **Policy – Status:** Indicates whether the policy is active or inactive

Measures

Incident Count Total number of Network incidents.

Match Count	Total number of Network matches.

DLP Policy History Cube

Contains historical information about policies and conditions setup within
the Data Loss Prevention system, including details of what elements of a condition changed from version to version. Information specific to this cube includes the total number of policies, total number of conditions, policy creation date, condition creating date, responsible user, document, keywords, patterns and more.

Dimensions

- **Condition – Detection or Group:** Indicates whether the condition belongs to one of two rule types
- **Condition – ID:** Condition ID
- **Condition – Is Latest:** Indicates whether or not this is the latest version of the condition
- **Condition – Minimum Matches:** Specifies the minimum number of matches required to trigger the condition and generate an incident
- **Condition – Processing Order:** Denotes the order in which conditions are processed
- **Condition – Rule or Exception:** Indicates whether the condition was added as a rule or as an exception
- **Condition - Status:** Captures historical changes of the condition status
- **Condition – Type:** Describes the type of matching used in the condition
- **Condition – Unique or Multiple Matches:** Indicates the match counting type selected in the condition
- **Condition Change Audit – Attribute Name:** Condition attribute name that was changed
- **Condition Change Audit – Change Details**: Details regarding the actual change in the condition
- **Database Info Condition – ClauseID:** ID number in the condition WHERE clause. This is only applicable to policies which use Exact Data Matching (EDM)
- **Database Info Condition – DataSourceID:** EDM profile ID number
- **Database Info Condition – Threshold:** Number of selected fields to match on EDM profile
- **Condition Created – Date:** Date the condition was created

- **Condition Created – Day of Week:** Day the condition was created
- **Condition Created – Month:** Month the condition was created
- **Condition Created – Quarter:** Quarter the condition was created
- **Condition Created – Year:** Year the condition was created
- **Condition Edited – Date:** Date the condition was edited (shows historical data)
- **Condition Edited – Day of Week:** Day the condition was edited (shows historical data)
- **Condition Edited – Month:** Month the condition was edited (shows historical data)
- **Condition Edited – Quarter:** Quarter the condition was edited (shows historical data)
- **Condition Edited – Year:** Year the condition was edited (shows historical data)
- **Policy Created – Date:** Date the policy was created
- **Policy Created – Date Range:** Date range the policy was created
- **Policy Created – Day of Week:** Day the policy was created
- **Policy Created – Month:** Month the policy was created
- **Policy Created – Quarter:** Quarter the policy was created
- **Policy Created – Week Number:** Week number the policy was created
- **Policy Created – Year:** Year the policy was created
- **Policy Edited – Date:** Date the policy was edited (shows historical data)
- **Policy Edited – Date Range:** Date range the policy was edited (shows historical data)
- **Policy Edited – Day of Week:** Day the policy was edited (shows historical data)
- **Policy Edited – Month:** Month the policy was edited (shows historical data)
- **Policy Edited – Quarter:** Quarter the policy was edited (shows historical data)
- **Policy Edited – Week Number:** Week number the policy was edited (shows historical data)
- **Policy Edited – Year:** Year the policy was edited (shows historical data)

- **Document Meta Info Condition – MIMEType:** Message attachment or file type MIME type
- **Document Name Condition – Filenames:** Files names used in the Message Attachment or File Name Match condition
- **Document Profile Condition – DocSourceID:** Indexed Document Matching (IDM) profile ID number
- **Document Profile Condition – Similarity:** Document Profile Condition – Similarity: IDM similarity threshold
- **Document Size Condition – Document Size:** Document size specified within Message attachment or file size match condition type
- **Document Size Condition – Size Comparator:** Size comparator type specified within Message attachment or file size match condition type
- **Document Size Condition – Size Magnitude:** Unit type used within Message Attachment or File Size Match condition type
- **Keyword Condition – Case Sensitive:** Match type used within the Content Matches Keyword condition type
- **Keyword Condition – Delimiter:** Keyword separator used within the Content Matches Keyword condition type
- **Keyword Condition – Is Tokenized Search: I**ndicates whether or not keyword searches are tokenized. The default value is yes.
- **Keyword Condition – Keyword List:** Keyword list specified within the Content Matches Keyword condition type
- **Oracle Database – Host Name:** Denotes the oracle database name and instance name from which the data is obtained
- **Pattern Condition – Pattern:** Regular expression defined within the Content Matches Regular Expression condition type
- **Policy – Description:** Policy description as displayed in the Enforce console
- **Policy – ID:** Policy ID
- **Policy – Is Deleted:** Indicates whether or not the policy has been deleted

- **Policy – Is Latest Version:** Indicates whether or not the policy version is the latest
- **Policy – Name:** Policy name
- **Policy – Status:** Indicates whether the policy is active or inactive
- **Policy – Version:** Policy version number

- **Protocol Condition – Protocols:** Protocol ID used within the Protocol or Endpoint Destination condition type
- **Recipient Condition – Email Address:** Email address specified within the Recipient Matches Pattern condition type
- **Recipient Condition – IP Address:** IP address specified within the Recipient Matches Pattern condition type
- **Recipient Condition – URL:** URL specified within the Recipient Matches Pattern condition type
- **Recipient Profile Condition – DataSourceID:** Data source ID for the directory profile
- **Role – Description:** Role description as displayed in the Enforce console.
- **Role – Name:** Role name as displayed in the Enforce console
- **Rule – Name:** Name given to the detection or exception rule
- **Sender Condition – IP Address:** IP address specified within the Sender/User Matches Pattern condition type
- **Sender Condition – Sender Identifier:** Email address, windows username, or IM screen name specified within the Sender/user Matches Pattern condition type
- **Sender Profile Condition – DataSourceID: profile** Data source ID for the directory
- **Condition Created – Hour:** Hour the condition was created
- **Condition Created – Minute:** Minute the condition was created
- **Condition Created – Second:** Second the condition was created
- **Condition Created – Time:** Time the condition was created
- **Condition Edited – Hour:** Hour the condition was edited (shows historical data)
- **Condition Edited – Minute:** Minute the condition was edited (shows historical data)
- **Condition Edited – Second:** Second the condition was edited (shows historical data)
- **Condition Edited – Time:** Time the condition was edited (shows historical data)
- **Policy Created – Hour:** Hour the policy was created
- **Policy Created – Minute:** Minute the policy was created

- **Policy Created – Second:** Second the policy was created
- **Policy Created – Time:** Time the policy was created

- **Policy Edited – Hour:** Hour the policy was edited (shows historical data)
- **Policy Edited – Minute:** Minute the policy was edited (shows historical data)
- **Policy Edited – Second:** Second the policy was edited (shows historical data)
- **Policy Edited – Time:** Time the policy was edited (shows historical data)
- **Universal Metadata Condition – Metadata Key:** Indicates the type of the rule.
- Possible values: NetworkLocation
- **Universal Metadata Condition – Metadata Source:** A constant value of 1.
- **Universal Metadata Condition – Metadata Value:** Indicates the endpoint location. Possible values: 0 and 1 where 0 = ‘On the corporate network’ and 1 = ‘Off the corporate network’
- **Universal Metadata Condition – Metadata Value Operand:** A constant value of ‘CSVSTRING’
- **User – Created By:** DLP user who created the policy
- **User – Edited By:** DLP user who modified the policy

Measures

Condition Change Count	Total number of policy changes.
Condition Count	Total number of conditions.
Policy Count	Total number of policies.

Key Performance Indicators

Policies Edited in Last 30 Days

DLP User Actions Audit Cube

Contains historical information about administrative events within the Data Loss Prevention system, including details about the type of the entity that was changed as well as the nature of the change. Information specific to this cube includes the total number of administrative events, event creation date, username, source IP address and more.

Dimensions

- **Oracle Database – Host Name**: Denotes the oracle database name and instance name from which the data is obtained
- **User Action – Category:** Action taken when the even occurred
- **User Action – Detail:** Free text details for the event
- **User Action – Entity:** Object or component name on which the event occurred
- **User Action – IP Address:** IP Address of the PC that triggered the event
- **User Action – Role:** Role assigned to the user who triggered the event
- **User Action – User Name:** DLP user who triggered the event
- **User Action – Date:** Date the event occurred
- **User Action – Date Range:** Date range the event occurred
- **User Action – Day of Week:** Date of the week the event occurred
- **User Action – Month:** Month the event occurred
- **User Action – Quarter:** Quarter the event occurred
- **User Action – Week Number:** Week number the event occurred
- **User Action – Year:** Year the event occurred
- **User Action – Hour:** Hour the event occurred
- **User Action – Second:** Second the event occurred
- **User Action – Minute:** Minute the event occurred
- **User Action – Time:** Time the event occurred

Measures

Administrative events.	Total number of administrative events. Events Count

Reports

The following is a list of default reports provided within the IT Analytics Symantec Data Loss Prevention Content Pack, with their associated descriptions as reference.

DLP Auditing – User Event Details

Displays a chart showing the user events month over month along with a detailed table of user actions by user name, including role, date, category and event detail. The report allows the user to filter the data by start/end date, category, entity, role and user name.

DLP Auditing – User Incident Event Summary

Displays a breakdown of events by username. The report allows the user to filter the data by start/end date, category, role and username.

DLP Deployment – Agent Search

Displays a list of agents by endpoint name with additional details such as IP address, whether it has been deleted, its major version, version, status, on or off network, last connection date and incident count. The report allows the user to filter the data by endpoint server, IP address, is deleted, on or off network, name, status, version, and major version.

DLP Auditing – User Action Auditing

Displays a trend of user actions by category, along with a detailed chart including username, role, date, entity, category, detail and event count. The report allows the user to filter the data by start/end date, entity, category, role and username.

DLP Deployment – Agent Version by Server

Displays a graph of agents by server and the agent version, along with a detailed table showing total agents associated with each endpoint server. The report allows the user to filter the data by deleted, status and version.

DLP Deployment – Policy Evolution Trend

Displays a trend graph showing the number of policies over time (monthly) and a detailed table including the creator of each policy. The report allows the user to filter the data by start/end date, policy name, rule name and user.

DLP Deployment – Scan Summary

Displays a graph showing the number of gigabytes scanned over time for each server. The report allows the user to filter the data by start/end date, detection server, discover target, policy, scan type and severity.

DLP Remediation – Discover Incident Details

Displays a list of discover incidents with various details including detection date, policy, severity, status and others. The report allows the user to filter the data by start/end date, custom attribute name/value, discover server/target, Oracle database, policy, severity, status and target type.

DLP Remediation – Endpoint Incident Details

Displays a list of endpoint incidents with various details including detection date, policy, agent name/status, severity, status and others. The report allows the user to filter the data by start/end date, agent name/status, agent version, agent response, custom attribute name/value, device type, IP Address, policy name, severity and username.

DLP Statistics – Discover Scanned Storage Trend

Displays a chart showing the number of gigabytes scanned over time, along with a detail chart denoting the number of discover incidents generated. The report allows the user to filter the data by start/end date, content root, discover server and target, Oracle database, policy and severity.

DLP Statistics – Endpoint Incident Trend byChannel

Displays a trending chart showing the incidents per channel over time, as well as a detailed chart broken down by month. The report allows the user to filter the data by start/end date, agent response, monitoring channel, detection server, policy name, severity, custom attribute name and value.

DLP Statistics – Incident Trend by Product Area

Displays a trending chart showing incidents per product area over time, as well as a detailed chart broken down by month. The report allows the user to filter the data by start/end date, custom attribute name/value, Oracle host name, policy name, product area and severity.

DLP Statistics – Organizational Incident Trend

Displays a trending chart showing incidents over time by the specific custom attribute name selected. The report allows the user to filter the data by start/end date, custom attribute name, detection server, policy name, product area and severity.

DLP Remediation – Incidents Search

Displays a summary of incident data by severity, status and product area, as well as a detailed chart listing detection date and policy. The report allows the user to filter the data by start/end date, custom attribute name/value, policy, version, status, product area and severity.

DLP Remediation - Incident Status History Details

Displays a table including historical details for incidents by status. The report allows the user to filter the data by start/end date, detection server, changed from/to status, change user, next status group, Oracle database, policy, product area, role, and severity

DLP Statistics – Incidents by Policy

Displays a graph showing the number incidents by policy name, as well as a detailed table. The report allows the user to filter the data by start/end date and custom attribute name/value.

DLP Statistics – Incidents by Product Area

Displays a graph showing a high level view of incidents for each product area, as well as a detailed table. The report allows the user to filter the data by start/end date and custom attribute name/value.

DLP Statistics – Incidents by Severity

Displays a graph showing a high level view of incidents by severity, as well as a detailed table. The report allows the user to filter the data by start/end date and custom attribute name/value.

DLP Statistics – Incidents by Status

Displays a graph showing a high level view of incidents by status, as well as a detailed table. The report allows the user to filter the data by start/end date and custom attribute name/value.

DLP Remediation – Discover Incident Search

Displays a summary of discover incidents by severity, status and target type, as well as detailed table. The report allows the user to filter the data by start/end date, custom attribute name/value, discover server/target, Oracle database, policy, severity, status and target type.

DLP Remediation – Endpoint Incident Search

Displays a summary of endpoint incidents by severity and device type, as well as detailed table. The report allows the user to filter the data by start/end date, agent name/status, custom attribute name/value, agent version/response, device type, IP address, policy, severity and username.

DLP Investigations – Discover File Incidents by File Owner Trend

Displays a graph showing the number of incidents over time by file owner. The report allows the user to filter the data by start/end date, filename, policy, Oracle host and severity.

DLP Investigations – Networking File Incidents by Networking User Trend

Displays a graph showing the number of incidents for a designated file over time by networking user. The report allows the user to filter the data by start/end date, filename, policy, Oracle host and severity.

DLP Remediation – Network Incident Search

Displays a summary of network incidents by severity and status, as well as detailed table. The report allows the user to filter the data by start/end date, custom attribute name/value, detection server, filename, policy, protocol, severity, status and user.

DLP Investigations – User Incident Details

Displays a detailed table showing specifics for incidents by a given user. The report allows the user to filter the data by start/end date, custom attribute name/value, email/IP address, machine name, policy, product area, severity and username.

DLP Investigations – User Incident Search

Displays a chart showing top policies with incidents and a detailed table showing specifics for incidents by a given user. The report allows the user to filter the data by start/end date, custom attribute name/value, email/IP address, machine name, policy, severity and username.

DLP Remediation – Network Incident Details

Displays a list of network incidents with various details including detection date, policy, sender name, severity, status and others. The report allows the user to filter the data by start/end date, custom attribute name/value, detection server, filename, policy, protocol, severity, status and user.

DLP Normalized Risk – Frequency of Discover Incidents vs. Files Scanned Trend Displays a chart showing incidents by policy over time and a detailed table including the ratio values between the number of discover incidents and the number of files scanned. The report allows the user to filter the data by start/end date, discover target/server, policy and severity.

DLP Normalized Risk – Frequency of Discover Incidents vs. GB Scanned Trend

Displays a chart showing the avg number of Discover incidents per DB scanned over time with a further breakdown by policy. Also displays a detailed table including the total number of DB scanned and incident used to calculate the ratios across all incident severity values. The report allows the user to filter the data by start/end date, discover target/server, policy and severity.

DLP Normalized Risk – Frequency of Email Incidents (Email Prevent)

Displays a chart showing the avg number of SMTP incidents per emails scanned over time with a further breakdown by detection server. Also displays a detailed table including the total number of emails scanned and incident used to calculate the ratios across all incident severity values.

The report allows the user to filter the data by start/end date, detection server, policy and severity.

DLP Normalized Risk – Frequency of Web Incidents

Displays a chart showing the avg number of HTTP and HTTPS incidents per web message scanned over time with a further breakdown by policy. Also displays a detailed table including the total number of web messages scanned and incident used to calculate the ratios across all incident severity values. The report allows the user to filter the data by start/end date, detection server, policy and severity.

DLP Policy Optimization - Policy Change Audit

Displays a detail report of all the changes performed on any given policy during the specified time period. The report includes the name of the attribute that was changed as well as the name of the user responsible for the change and the time stamp of the change.

DLP Policy Optimization – Policy Change Impact

Displays a chart showing the number incidents by policy version over time, as well as a table listing the number of incidents per policy version on a monthly basis. The report allows the user to filter the data by start/end date, policy name and user.

DLP Policy Optimization – Policy Change Trend

Displays a chart showing the number of policy changes over time, as well as a table listing the number of changes per policy on a monthly basis. The report allows the user to filter the data by start/end date, policy name and user.

DLP Policy Optimization – Policy Changes

Displays a detailed table listing the policy changes made, along with relevant information such as: policy name, date, version, user, condition and attribute name and detail on the change that was applied. The report allows the user to filter the data by start/end date, Oracle database, policy name/status/version, rule name and user.

DLP Remediation – Remediator Productivity

Displays a pie showing number of incidents that changed by user, such as Closed, over time, as well as a detailed table displaying a breakdown of the statuses changed and severity. This allows the user to measure which users are responsible for managing incidents. This report allows the user to filter the data by start/end date, detection server, policy, severity, status group, role and user.

DLP Statistics – Scans

Displays a detailed table showing information on scans by Discover target and content root, along with relevant information such as: status, elapsed time, total items/bytes, items/bytes scanned and others. The report allows the user to filter the data by start/end date, Content Root, Discover target, Discover server, Oracle Database, Scan Type, policy name, and severity.

DLP Statistics – Discover Scanned File Trend

Displays a chart showing number of files scanned and detailed table showing information on scans by Month and Date along with relevant information such as: Scan Count, Megabytes Scanned, Total Scanned Files, and Discovered Files. The report allows the user to filter the data by start/end date, Discover target, Discover server and policy name.

DLP System Management – Agent Summary by Status

Displays a graph that shows the number of agents by status and broken down by major version, as well as a detailed table. The report allows the user to filter the data by start/end date, is deleted, status and major version.

DLP System Management – Agent Summary by Version

Displays a graph that shows the number of agents major version broken down by status, as well as a detailed table. The report allows the user to filter the data by is deleted, status and major version.

Dashboards

The following is a list of default dashboards provided within the IT Analytics Symantec Data Loss Prevention Content Pack, with their associated description as reference.

DLP Incidents Dashboard

Displays a graphical representation of the incidents within the Data Loss Prevention environment. Specific charts include the open incidents by policy, open incidents by type, and incidents by status and severity.

Dimension Attributes

The following is a list of default cube dimensions and their associated attributes provided within the IT Analytics Symantec Data Loss Prevention Content Pack, as reference.

DLP Agent

DLP Agent Last Connection Date

Applicable cubes:

- DLP Agent Status

DLP Agent Last Connection Date contains the following dimension attributes:

- **Agent Last Connection Date – Date:** Date the agent last connected to the endpoint server
- **Agent Last Connection Date – Date Range:** Date range the agent last connected to the endpoint server

Note: Possible values are: Today, yesterday, 2 – 7 days ago, 8 – 14 days ago, etc.

- **Agent Last Connection Date – Day of Week:** Day the agent last connected to the endpoint server
- **Agent Last Connection Date – Month:** Month the agent last connected to the endpoint server
- **Agent Last Connection Date – Quarter:** Quarter the agent last connected to the endpoint server
- **Agent Last Connection Date – Week Number:** Week number the agent last connected to the endpoint server
- **Agent Last Connection Date – Year:** Year the agent last connected to the endpoint server

DLP Agent Last Connection

Applicable cubes:

- DLP Agent Status

DLP Agent Last Connection contains the following dimension attributes:

- **Agent Last Connection – Hour:** Hour the agent last connected to the endpoint server
- **Agent Last Connection – Minute:** Minute the agent last connected to the endpoint server
- **Agent Last Connection – Second:** Second the agent last connected to the endpoint server
- **Agent Last Connection – Time:** Time the agent last connected to the endpoint server

DLP Captured Date

Applicable cubes:

- DLP Network Statistics

DLP Captured Date contains the following dimension attributes:

- **Captured – Date:** Date the message was captured by the detection server
- **Captured – Date Range:** Date range the message was captured by the detection server

Note: Possible values are: Today, yesterday, 2 – 7 days ago, 8 – 14 days ago, etc.

- **Captured – Day of Week:** Day the message was captured by the detection server
- **Captured – Month:** Month the message was captured by the detection server
- **Captured – Quarter:** Quarter the message was captured by the detection server
- **Captured – Week Number:** Week number the message was captured by the detection server
- **Captured – Year:** Year the message was captured by the detection server

DLP Captured Time

Applicable cubes:

- DLP Network Statistics

DLP Captured Time contains the following dimension attributes:

- **Captured – Hour:** Hour the message was captured by the detection server
- **Captured – Minute:** Minute the message was captured by the detection server

- **Captured – Second:** Second the message was captured by the detection server
- **Captured – Time:** Time the message was captured by the detection server

DLP Change Date

Applicable cubes:

- DLP Incident Status History

DLP Change Date contains the following dimension attributes:

- **Change – Date:** Date the incident status was changed
- **Change – Date Range:** Date range the incident status was changed

Note: Possible values are: Today, yesterday, 2 – 7 days ago, 8 – 14 days ago, etc

- **Change – Day of Week:** Day the incident status was changed
- **Change – Month:** Month the incident status was changed
- **Change – Quarter:** Quarter the incident status was changed
- **Change – Week Number:** Week number the incident status was changed
- **Change – Year:** Year the incident status was changed

DLP Change Time

Applicable cubes:

- DLP Incident Status History

DLP Change Time contains the following dimension attributes:

- **Change – Hour:** Hour the incident status was changed
- **Change – Minute:** Minute the incident status was changed
- **Change – Second:** Second the incident status was changed

- **Change – Time:** Time the incident status was changed

DLP Change User

Applicable cubes:

- DLP Incident Status History

DLP Change User contains the following dimension attributes:

- **Change – User:** DLP user name that performed the change

DLP Condition

Applicable cubes:

- DLP Discover Incident Details
- **DLP Endpoint Incident Details**
- **DLP Incident Details**
- **DLP Network Incident Details**
- **DLP Policy History**

DLP Condition contains the following dimension attributes:

- **Condition - Status:** Captures historical changes of the condition status

Note: Possible values are: Created, Changed, Unchanged, and Deleted. The unchanged status will appear when a section/element of a compound condition is changed.

- **Condition – Is Latest:** Indicates whether or not this is the latest version of the condition
- **Condition – Detection or Group:** Indicates whether the condition belongs to one of two rule types
- **Condition – ID:** Condition ID
- **Condition – Unique or Multiple Matches:** Indicates the match counting type selected in the condition

Note: Possible values are: 1 – Check for existence, 2 – Count all matches, and 3 – Count all unique matches. A value of 1 will also be assigned if match counting is not applicable to the condition

- **Condition – Minimum Matches:** Specifies the minimum number of matches required to trigger the condition and generate an incident
- **Rule – Name:** Name given to the detection or exception rule.
- **Condition – Processing Order:** Denotes the order in which conditions are processed
- **Condition – Rule or Exception:** Indicates whether the condition was added as a rule or as an exception
- **Condition – Type:** Describes the type of matching used in the condition

Note: Possible values are: Content Matches Data Identifier, Message Attachment or File Type Match, Content Matches Keyword, Sender/User Matches Pattern, and Protocol or Endpoint Destination

DLP Condition Change Audit

Applicable cubes:

- DLP Policy History

DLP Condition Change Audit contains the following dimension attributes:

- **Condition Change Audit – Attribute Name:** Condition attribute name that was changed

Note: Possible values are: Data Source ID, Email Address, File Names, IP Address, Protocols, etc.

- **Condition Change Audit – Change Details**: Details regarding the actual change in the condition

DLP Content Root Scan Started Date

Applicable cubes:

- DLP Discover Scans

DLP Content Root Scan Started Date contains the following dimension attributes:

- **Content Root Scan Started – Date:** Date the content root scan started
- **Content Root Scan Started – Date Range:** Date range the content root scan started
- **Content Root Scan Started – Day of Week:** Day the content root scan started
- **Content Root Scan Started – Month:** Month the content root scan started
- **Content Root Scan Started – Quarter:** Quarter the content root scan started
- **Content Root Scan Started – Week Number:** Week number the content root scan started
- **Content Root Scan Started – Year:** Year the content root scan started

DLP Content Root Scan Started Time

Applicable cubes:

- DLP Discover Scans

DLP Content Root Scan Started Time contains the following dimension attributes:

- **Content Root Scan Started – Hour:** Hour the content root scan started
- **Content Root Scan Started – Minute:** Minute the content root scan started
- **Content Root Scan Started – Second:** Second the content

root scan started

- **Content Root Scan Started – Time:** Time the content root scan started

DLP Custom Attribute Name

Applicable cubes:

- DLP Discover Incident Details
- **DLP Discover Incident Summary**
- **DLP Endpoint Incident Details**
- **DLP Endpoint Incident Summary**
- **DLP Incident Details**
- **DLP Incident Summary**
- **DLP Network Incident Details**
- **DLP Network Incident Summary**

DLP Custom Attribute Name contains the following dimension attributes:

- **Custom Attribute – Name:** Lists all user-defined custom attributes

DLP Custom Attribute Value

Applicable cubes:

- DLP Discover Incident Details
- **DLP Discover Incident Summary**
- **DLP Endpoint Incident Details**
- **DLP Endpoint Incident Summary**
- **DLP Incident Details**
- **DLP Incident Summary**
- **DLP Network Incident Details**
- **DLP Network Incident Summary**

DLP Custom Attribute Value contains the following dimension attributes:

- **Custom Attribute – Value:** Lists values assigned to the custom attributes

DLP Data Owner

Applicable cubes:

- DLP Discover Incident Details
- **DLP Discover Incident Summary**
- **DLP Endpoint Incident Details**
- **DLP Endpoint Incident Summary**
- **DLP Incident Details**
- **DLP Incident Summary**
- **DLP Network Incident Details**
- **DLP Network Incident Summary**

DLP Data Owner contains the following dimension attributes:

- **Data Owner – Name:** Name of the person responsible for remediating the incident.

Note: This field must be set manually, or with a lookup plug-in such as Data Insight.

DLP Data Owner Email

Applicable cubes:

- DLP Discover Incident Details
- **DLP Discover Incident Summary**
- **DLP Endpoint Incident Details**
- **DLP Endpoint Incident Summary**
- **DLP Incident Details**
- **DLP Incident Summary**
- **DLP Network Incident Details**

- DLP Network Incident Details

DLP Data Owner Email contains the following dimension attributes:

- **Data Owner – Email:** Email address of the person responsible for remediating the incident.

Note: This field must be set manually, or with a lookup plug-in such as Data Insight.

DLP Database Info Condition

Applicable cubes:

- DLP Policy History

DLP Database Info Condition contains the following dimension attributes:

- **Database Info Condition – ClauseID:** ID number in the condition WHERE clause. This is only applicable to policies which use Exact Data Matching (EDM)
- **Database Info Condition – DataSourceID:** EDM profile ID number
- **Database Info Condition – Threshold:** Number of selected fields to match on EDM profile

DLP Date Condition Created

Applicable cubes:

- DLP Policy History

DLP Date Condition Created contains the following dimension attributes:

- **Condition Created – Date:** Date the condition was created
- **Condition Created – Date Range:** Date range the condition was created
- **Condition Created – Day of Week:** Day the condition was created
- **Condition Created – Month:** Month the condition was created
- **Condition Created – Quarter:** Quarter the condition was created

- **Condition Created – Week Number:** Week number the condition was created
- **Condition Created – Year:** Year the condition was created

DLP Date Condition Edited

Applicable cubes:

- DLP Policy History

DLP Date Condition Edited contains the following dimension attributes:

- **Condition Edited – Date:** Date the condition was edited (shows historical data)
- **Condition Edited – Day of Week:** Day the condition was edited (shows historical data)
- **Condition Edited – Date Range:** Date range the condition was edited (shows historical data)
- **Condition Edited – Month:** Month the condition was edited (shows historical data)
- **Condition Edited – Quarter:** Quarter the condition was edited (shows historical data)
- **Condition Edited – Week Number:** Week number the policy was created (shows historical data)
- **Condition Edited – Year:** Year the condition was edited (shows historical data)

DLP Date Policy Created

Applicable cubes:

- DLP Policy History

DLP Date Policy Created contains the following dimension attributes:

- **Policy Created – Date:** Date the policy was created

- **Policy Created – Date Range:** Date range the policy was created
- **Policy Created – Day of Week:** Day the policy was created
- **Policy Created – Month:** Month the policy was created
- **Policy Created – Quarter:** Quarter the policy was created
- **Policy Created – Week Number:** Week number the policy was created
- **Policy Created – Year:** Year the policy was created

DLP Date Policy Edited

Applicable cubes:

- DLP Policy History

DLP Date Policy Edited contains the following dimension attributes:

- **Policy Edited – Date:** Date the policy was edited (shows historical data)
- **Policy Edited – Day of Week:** Day the policy was edited (shows historical data)
- **Policy Edited – Month:** Month the policy was edited (shows historical data)
- **Policy Edited – Quarter:** Quarter the policy was edited (shows historical data)
- **Policy Edited – Year:** Year the policy was edited (shows historical data)

DLP Detection Date

Applicable cubes:

- DLP Discover Incident Details
- **DLP Discover Incident Summary**
- **DLP Endpoint Incident Details**
- **DLP Endpoint Incident Summary**

- **DLP Incident Details**

- DLP Incident Status History
- **DLP Incident Summary**
- **DLP Network Incident Details**
- **DLP Network Incident Summary**

DLP Detection Date contains the following dimension attributes:

- **Detection – Date:** Incident detection date as reported by the detection server
- **Detection – Date Range:** Incident detection date range as reported by the detection server
- **Detection – Day of Week:** Incident detection day as reported by the detection server
- **Detection – Month:** Incident detection month as reported by the detection server
- **Detection – Quarter:** Incident detection quarter as reported by the detection server
- **Detection – Week Number:** Incident detection week number as reported by the detection server
- **Detection – Year:** Incident detection year as reported by the detection server

Note: These values correspond to the 'Reported On' timestamp in the Endpoint Incident Snapshot, which represents the date/time when the incident was processed by the endpoint server.

DLP Detection Server

Applicable cubes:

- DLP Incident Details
- **DLP Incident Status History**
- **DLP Incident Summary**
- **DLP Network Incident Details**

- DLP Network Incident Summary
- **DLP Network Statistics**

DLP Detection Server contains the following dimension attributes:

- **Detection Server – Name:** Detection server name as shown in the Systems Overview page
- **Detection Server – Type:** Detection Server channel name as shown in the System Overview page

DLP Detection Time

Applicable cubes:

- DLP Discover Incident Details
- **DLP Discover Incident Summary**
- **DLP Endpoint Incident Details**
- **DLP Endpoint Incident Summary**
- **DLP Incident Details**
- **DLP Incident Status History**
- **DLP Incident Summary**
- **DLP Network Incident Details**
- **DLP Network Incident Summary**

DLP Detection Time contains the following dimension attributes:

- **Detection – Time:** Incident detection time as reported by the detection server
- **Detection – Hour:** Incident detection hour as reported by the detection server
- **Detection – Minute:** Incident detection minute as reported by the detection server
- **Detection – Second:** Incident detection second as reported by the detection server

Note: These values map to the 'Reported On' timestamp in the Oracle database, which represents when the incident was processed by the endpoint server.

DLP Discover Incident

Applicable cubes:

- DLP Discover Incident Details
- **DLP Discover Incident Summary**
- **DLP Discover Scans**

DLP Discover Incident contains the following dimension attributes:

- **Discover Incident – Content Root:** Lists Content Roots that were scanned by the discover server

Note: This list only contains content roots in which at least one sensitive file was found

- **Discover Incident – Document Name:** Name of the file that triggered the incident
- **Discover Incident – File Owner:** Creator of the file or item that triggered the incident
- **Discover Incident – Repository Location:** Full path of the file that triggered the incident
- **Discover Incident – Scanned Machine:** Host name of the scanned computer
- **Discover Incident – Target Type:** Discover target type

Note: Possible values are File System, Lotus Notes, SQL Database, SharePoint, Exchange, File System Endpoint, Web Services, and Scanner (SharePoint, Exchange, Web Server, File System, Documentum, LiveLink, and Generic)

DLP Discover Incident File Location

Applicable cubes:

- DLP Discover Incident Details
- **DLP Discover Incident Summary**

DLP Discover Incident File Location contains the following dimension attributes:

- **Discover Incident – File Location:** Full path of the file that triggered the incident

DLP Discover Incident File Permission ACL Type

Applicable cubes:

- DLP Discover Incident Details
- **DLP Discover Incident Summary**

DLP Discover Incident File Permission ACL Type contains the following dimension attributes:

- **Discover Incident – ACL Type:** ACL permission type Note: Possible values are: File and SP (SharePoint)

DLP Discover Incident File Permission Grant or Deny

Applicable cubes:

- DLP Discover Incident Details
- **DLP Discover Incident Summary**

DLP Discover Incident File Permission Grant or Deny contains the following dimension attributes:

- **Discover Incident – Grant or Deny:** Indicates whether the ACL type assigned permission is grant or deny

DLP Discover Incident File Permission Permission

Applicable cubes:

- DLP Discover Incident Details
- **DLP Discover Incident Summary**

DLP Discover Incident File Permission Permission contains the following dimension attributes:

- **Discover Incident – File Permission:** Permission assignment corresponding to the Grant or Deny dimension

Note: Possible values are: Read and write

DLP Discover Incident File Permission Username

Applicable cubes:

- DLP Discover Incident Details
- **DLP Discover Incident Summary**

DLP Discover Incident File Permission Username contains the following dimension attributes:

- **Discover Incident – File Permission Username:** Username or group granted the given file permission

DLP Discover Incident Protect Status

Applicable cubes:

- DLP Discover Incident Details
- **DLP Discover Incident Summary**

DLP Discover Incident Protect Status contains the following dimension attributes:

- **Discover Incident – Protect Status:** Indicates the remediation action taken on the discovered file

Note: Possible values are: Endpoint File Quarantine, Protect File Copied, No Remediation, etc.

DLP Discover Scan

Applicable cubes:

- DLP Discover Incident Details
- **DLP Discover Incident Summary**
- **DLP Discover Scan**

DLP Discover Scan contains the following dimension attributes:

- **Discover Scan – In Process Scan:** Indicates whether or not the scan is in progress
- **Discover Scan – Initial Scan:** Indicates whether or not this is the first scan performed on the discover target
- **Discover Scan – Last Completed Scan:** Indicates whether or not this is the last scan performed on the discover target
- **Discover Scan – Scan Instance ID:** Discover scan instance ID
- **Discover Scan – Target Type:** Denotes the type of data repository being scanned

DLP Discover Server

Applicable cubes:

- DLP Discover Incident Details
- **DLP Discover Incident Summary**
- **DLP Discover Scan**

DLP Discover Server contains the following dimension attributes:

- **Discover Server – Name:** Discover server name

DLP Discover Scan Content Root

Applicable cubes:

- DLP Discover Scans

DLP Discover Scan Content Root contains the following dimension attributes:

- **Discover Scan – Content Root:** Lists all Content Roots scanned by the discover server

Note: The list includes content roots that have not sensitive data

DLP Discover Target

Applicable cubes:

- DLP Discover Incident Details
- **DLP Discover Incident Summary**
- **DLP Discover Scans**

DLP Discover Target contains the following dimension attributes:

- **Discover Target – Name:** Discover target name as shown in the Enforce console

DLP Document Meta Info Condition

Applicable cubes:

- DLP Policy History

DLP Document Meta Info Condition contains the following dimension attributes:

- **Document Meta Info Condition – MIMEType:** Message attachment or file type MIME type

DLP Document Name Condition

Applicable cubes:

- DLP Policy History

DLP Document Name Condition contains the following dimension attributes:

- **Document Name Condition – Filenames:** Files names used in the Message Attachment or File Name Match condition

DLP Document Profile Condition

Applicable cubes:

- DLP Policy History

DLP Document Profile Condition contains the following dimension attributes:

- **Document Profile Condition – DocSourceID:** Indexed Document Matching (IDM) profile ID number
- **Document Profile Condition – Similarity:** Document Profile Condition – Similarity: IDM similarity threshold

DLP Document Size Condition

Applicable cubes:

- DLP Policy History

DLP Document Size Condition contains the following dimension attributes:

- **Document Size Condition – Document Size:** Document size specified within Message attachment or file size match condition type
- **Document Size Condition – Size Comparator:** Size comparator type specified within Message attachment or file size match condition type

Note: Possible values are: 1 means greater than and 2 means less than

- **Document Size Condition – Size Magnitude:** Unit type used within Message Attachment or File Size Match condition type

Note: Possible values are: 0 means bytes, 1 means kilobytes, 2 means megabytes, and 3 means gigabytes

DLP Endpoint Incident

Applicable cubes:

- DLP Endpoint Incident Details
- **DLP Endpoint Incident Summary**
- **DLP Incident Summary**

DLP Endpoint Incident contains the following dimension attributes:

- **Endpoint Incident – Application Name:** The name of the application employed by the user
- **Endpoint Incident – Device Type:** Lists the endpoint monitoring channel that triggered the incident
- **Endpoint Incident – File Name:** Destination name of the file or item that triggered the incident
- **Endpoint Incident – File Owner:** Creator of the file or item that triggered the incident
- **Endpoint Incident – File Path:** Full destination path of the file that triggered the incident
- **Endpoint Incident – Instance ID:** Endpoint device identifier on which the violation occurred
- **Endpoint Incident – IP Address:** IP address of the endpoint at the time the violation occurred
- **Endpoint Incident – Machine Name:** Name of the computer that triggered the incident
- **Endpoint Incident – On or Off the Network:** Indicates the agent

location at the time the violation occurred

- **Endpoint Incident – Source File Name:** Name of the file or item that triggered the incident
- **Endpoint Incident – Source File Path:** Full path of the file that triggered the incident
- **Endpoint Incident – User Name:** Logged on user on the computer that triggered the incident

DLP Endpoint Incident Agent Response

Applicable cubes:

- DLP Endpoint Incident Details
- **DLP Endpoint Incident Summary**

DLP Endpoint Incident Agent Response contains the following dimension attributes:

- **Endpoint Incident – Agent Response:** Response or action taken by the endpoint agent

DLP Endpoint Incident User Justification

Applicable cubes:

- DLP Endpoint Incident Details
- **DLP Endpoint Incident Summary**

DLP Endpoint Incident User Justification contains the following dimension attributes:

- **Endpoint Incident – User Justification Response:** Justification response as defined in the Enforce console
- **Endpoint Incident – User Justification Type:** Justification type as defined in the Enforce console

Note: The four possible default values are User Education, Broken Business Process, Manager Approved, and False Positive

DLP Endpoint Server

Applicable cubes:

- DLP Endpoint Incident Details
- **DLP Endpoint Incident Summary**

DLP Endpoint Server contains the following dimension attributes:

- **Endpoint Server - Name:** Endpoint server name

DLP File Created Date

Applicable cubes:

- DLP Discover Scans

DLP File Created Date contains the following dimension attributes:

- **File Created – Date:** Date the discovered file was created
- **File Created – Date Range:** Date range the discovered file was created
- **File Created – Day of Week:** Day the discovered file was created
- **File Created – Month:** Month the discovered file was created
- **File Created – Quarter:** Quarter the discovered file was created
- **File Created – Week Number:** Week number the discovered file was created
- **File Created – Year:** Year the discovered file was created

DLP File Created Time

Applicable cubes:

- DLP Discover Scans

DLP File Created Time contains the following dimension attributes:

- **File Created – Hour:** Hour the discovered file was created
- **File Created – Minute:** Minute the discovered file was created
- **File Created – Second:** Second the discovered file was created
- **File Created – Time:** Time the discovered file was created

DLP File Last Accessed Date

Applicable cubes:

- DLP Discover Scans

DLP File Last Accessed Date contains the following dimension attributes:

- **File Last Accessed – Date:** Date the discovered file was last accessed
- **File Last Accessed – Date Range:** Date range the discovered file was last accessed
- **File Last Accessed – Day of Week:** Day the discovered file was last accessed
- **File Last Accessed – Month:** Month the discovered file was last accessed
- **File Last Accessed – Quarter:** Quarter the discovered file was last accessed
- **File Last Accessed – Week Number:** Week number the discovered file was last accessed
- **File Last Accessed – Year:** Year the discovered file was last accessed

DLP File Last Accessed Time

Applicable cubes:

- DLP Discover Scans

DLP File Last Accessed Time contains the following dimension attributes:

- **File Last Accessed – Hour:** Hour the discovered file was last accessed

- **File Last Accessed – Minute:** Minute the discovered file was last accessed

- **File Last Accessed – Second:** Second the discovered file was last accessed
- **File Last Accessed – Time:** Time the discovered file was last accessed

DLP Incident

Applicable cubes:

- DLP Discover Incident Details
- **DLP Discover Incident Summary**
- **DLP Endpoint Incident Details**
- **DLP Endpoint Incident Summary**
- **DLP Incident Details**
- **DLP Incident History**
- **DLP Incident Status History**
- **DLP Incident Summary**
- **DLP Network Incident Details**
- **DLP Network Incident Summary**

DLP Incident contains the following dimension attributes:

- **Incident – ID:** Incident ID

DLP Incident History Date

Applicable cubes:

- DLP Incident History

DLP Incident History Date contains the following dimension attributes:

- **Incident History Date – Date:** Date the event occurred
- **Incident History Date – Date Range:** Date range the event occurred
- **Incident History Date – Day of Week:** Day the event occurred

- **Incident History Date – Month:** Month the event occurred
- **Incident History Date – Quarter:** Quarter the event occurred
- **Incident History Date – Week Number:** Week number the event occurred
- **Incident History Date – Year:** Year the event occurred

DLP Incident History Detail

Applicable cubes:

- DLP Incident History

DLP Incident History Detail contains the following dimension attributes:

- **Incident History – Detail:** Free text description of the event

DLP Incident History Submitted By

Applicable cubes:

- DLP Incident History

DLP Incident History Submitted By contains the following dimension attributes:

- **Incident History – Submitted By:** DLP user name who performed the action

DLP Incident History Time

Applicable cubes:

- DLP Incident History

DLP Incident History Time contains the following dimension attributes:

- **Incident History – Hour:** Hour the event occurred
- **Incident History – Minute:** Minute the event occurred
- **Incident History – Second:** Second the event occurred

- **Incident History – Time:** Time the event occurred

DLP Incident History Type

Applicable cubes:

- DLP Incident History

DLP Incident History Type contains the following dimension attributes:

- **Incident History – Type:** Type of event as shown in the history tab of the incident snapshot

Note: Possible values are: Action Blocked, Attribute Lookup Completed, Attribute Set, Detected, Severity Change, Status Change, User Notified, etc

DLP Incident Message Component Document Format

Applicable cubes:

- DLP Discover Incident Details
- **DLP Discover Incident Summary**
- **DLP Endpoint Incident Details**
- **DLP Endpoint Incident Summary**
- **DLP Incident Details**
- **DLP Incident Summary**
- **DLP Network Incident Details**
- **DLP Network Incident Summary**

DLP Incident Message Component Document Format contains the following dimension attributes:

- **Message Component – Document Format:** File format used in the message

DLP Incident Message Component Mime Type

Applicable cubes:

- DLP Discover Incident Details
- **DLP Discover Incident Summary**
- **DLP Endpoint Incident Details**
- **DLP Endpoint Incident Summary**
- **DLP Incident Details**
- **DLP Incident Summary**
- **DLP Network Incident Details**
- **DLP Network Incident Summary**

DLP Incident Message Component Mime Type contains the following dimension attributes:

- **Message Component – MIME Type:** MIME type used in the message

DLP Incident Message Component Name

Applicable cubes:

- DLP Discover Incident Details
- **DLP Discover Incident Summary**
- **DLP Endpoint Incident Details**
- **DLP Endpoint Incident Summary**
- **DLP Incident Details**
- **DLP Incident Summary**
- **DLP Network Incident Details**
- **DLP Network Incident Summary**

DLP Incident Message Component Name contains the following dimension attributes:

- **Message Component – Name:** Name used in the message

DLP Incident Next Status

Applicable cubes:

- DLP Incident Status History

DLP Incident Next Status contains the following dimension attributes:

- **Incident – Next Status:** Next status assigned to the incident. If the incident status is not changed, next status will be set to unknown

DLP Incident Next Status Group

Applicable cubes:

- DLP Incident Status History

DLP Incident Next Status Group contains the following dimension attributes:

- **Incident – Next Status Group:** Next status group as defined in the Enforce console

DLP Incident Severity

Applicable cubes:

- DLP Discover Incident Details
- **DLP Discover Incident Summary**
- **DLP Discover Scans**
- **DLP Endpoint Incident Details**
- **DLP Endpoint Incident Summary**
- **DLP Incident Details**
- **DLP Incident Status History**
- **DLP Incident Summary**

- **DLP Network Incident Details**
- **DLP Network Incident Summary**
- **DLP Network Statistics**

DLP Incident Severity contains the following dimension attributes:

- **Incident – Severity:** Incident severity

Note: Possible values are: Info, Low, Med, and High

DLP Incident Status

Applicable cubes:

- DLP Discover Incident Details
- **DLP Discover Incident Summary**
- **DLP Endpoint Incident Details**
- **DLP Endpoint Incident Summary**
- **DLP Incident Details**
- **DLP Incident Status History**
- **DLP Incident Summary**
- **DLP Network Incident Details**
- **DLP Network Incident Summary**

DLP Incident Status contains the following dimension attributes:

- **Incident – Status:** Incident status as shown in the incident snapshot

DLP Incident Status Group

Applicable cubes:

- DLP Discover Incident Details
- **DLP Discover Incident Summary**

- **DLP Endpoint Incident Details**
- **DLP Endpoint Incident Summary**
- **DLP Incident Details**
- **DLP Incident Status History**
- **DLP Incident Summary**
- **DLP Network Incident Details**
- **DLP Network Incident Summary**

DLP Incident Status Group contains the following dimension attributes:

- **Incident – Status Group:** Incident status group as defined in the Enforce console

DLP Incident Type

Applicable cubes:

- DLP Incident Details
- **DLP Incident Status History**
- **DLP Incident Summary**

DLP Incident Type contains the following dimension attributes:

- **Incident – Product Area:** Incident type

Note: Possible values are: Network, Endpoint, and Data at rest

DLP Keyword Condition

Applicable cubes:

- DLP Policy History

DLP Keyword Condition contains the following dimension attributes:

- **Keyword Condition – Case Sensitive:** Match type used within the Content Matches Keyword condition type

Note: Possible values are: Case Sensitive and Case Insensitive

- **Keyword Condition – Delimiter:** Keyword separator used within the Content Matches Keyword condition type

Note: Possible values are: Newline and comma

- **Keyword Condition – Is Tokenized Search: I**ndicates whether or not keyword searches are tokenized. The default value is yes.
- **Keyword Condition – Keyword List:** Keyword list specified within the Content Matches Keyword condition type

DLP Last State Changed Date

Applicable cubes:

- DLP Discover Scans

DLP Last State Changed Date contains the following dimension attributes:

- **Last State Changed – Date:** Date the scan status last changed
- **Last State Changed – Date Range:** Date range the scan status last changed
- **Last State Changed – Day of Week:** Day of the week the scan status last changed
- **Last State Changed – Month:** Month the scan status last changed
- **Last State Changed – Quarter:** Quarter the scan status last changed
- **Last State Changed – Week Number:** Week number the scan status last changed
- **Last State Changed – Year:** Year the scan status last changed

DLP Last State Changed Time

Applicable cubes:

- DLP Discover Scans

DLP Last State Changed Time contains the following dimension attributes:

- **Last State Changed – Hour:** Hour the scan status last changed
- **Last State Changed – Minute:** Minute the scan status last changed
- **Last State Changed – Second:** Second the scan status last changed
- **Last State Changed – Time:** Time the scan status last changed

DLP Message Date

Applicable cubes:

- DLP Discover Incident Details
- **DLP Discover Incident Summary**
- **DLP Endpoint incident Details**
- **DLP Endpoint Incident Summary**
- **D LP Incident Details**
- **DLP Incident Summary**
- **DLP Network Incident Summary**
- **DLP Network Incident Details**

DLP Message Date contains the following dimension attributes:

- **Message – Date:** Date the message was received by the detection server or endpoint client
- **Message – Date Range:** Date range the message was received by the detection server or endpoint client
- **Message – Day of Week:** Day the message was received by the detection server or endpoint client
- **Message – Month:** Month the message was received by the detection server or endpoint client
- **Message – Quarter:** Quarter the message was received by the detection server or endpoint client

- **Message – Week Number:** Week number the message was

received by the detection server or endpoint client

- **Message – Year:** Year the message was received by the detection server or endpoint client
- **Message – Hour:** Hour the message was received by the detection server or endpoint client
- **Message – Minute:** Minute the message was received by the detection server or endpoint client
- **Message – Second:** Second the message was received by the detection server or endpoint client
- **Message – Time:** Time the message was received by the detection server or endpoint client

Note: These values map to the 'Occurred On' timestamp in the Endpoint Incident snapshot, which represents when the message was received by the detection server or endpoint client.

DLP Network Incident Message

Applicable cubes:

- DLP Incident Summary
- **DLP Network Incident Details**
- **DLP Network Incident Summary**

DLP Network Incident Message contains the following dimension attributes:

- **Network Incident – Message Subject:** Subject line of email message. In the case of a web violation, this will show as HTTP incident.
- **Network Incident – Sender Name:** Sender email address or IP address

DLP Network Incident Message Recipient

Applicable cubes:

›

- DLP Network Incident Details
- **DLP Network Incident Summary**

DLP Network Incident Message Recipient contains the following dimension attributes:

- **Network Incident – Recipient Domain:** Recipient domain name or IP address
- **Network Incident – Recipient Name:** Recipient email address, IP address, or web address

DLP Network Incident Prevent Action

Applicable cubes:

- DLP Network Incident Details
- **DLP Network Incident Summary**

DLP Network Incident Prevent Action contains the following dimension attributes:

- **Network Incident – Prevent Action:** Action taken by the Network Prevent server

Note: Possible values are: Blocked, Content Removed, Modified, Passed, etc.

DLP Network Incident Protocol

Applicable cubes:

- DLP Network Incident Details
- **DLP Network Incident Summary**
- **DLP Network Statistics**

DLP Network Incident Protocol contains the following dimension attributes:

- Network Incident – Protocol: Network protocol name

Note: Possible values are: FTP, HTTP, HTTPS, SMTP, IM, etc.

DLP Next Change Date

Applicable cubes:

- DLP Incident Status History

DLP Next Change Date contains the following dimension attributes:

- **Next Change – Date:** Date when the Incident Next Status value was changed.

If the status remains unchanged, this will show up as unknown

- **Next Change – Date Range:** Date range when the Incident Next Status value was changed. If the status remains unchanged, this will show up as unknown
- **Next Change – Day of Week:** Day when the Incident Next Status value was changed. If the status remains unchanged, this will show up as unknown
- **Next Change – Month:** Month when the Incident Next Status value was changed. If the status remains unchanged, this will show up as unknown
- **Next Change – Quarter:** Quarter when the Incident Next Status value was changed. If the status remains unchanged, this will show up as unknown
- **Next Change – Week Number:** Week number when the Incident Next Status value was changed. If the status remains unchanged, this will show up as unknown
- **Next Change – Year:** Year when the Incident Next Status value was changed.

If the status remains unchanged, this will show up as unknown

DLP Next Change Time

Applicable cubes:

- DLP Incident Status History

DLP Next Change Time contains the following dimension attributes:

- **Next Change – Hour:** Hour when the Incident Next Status value was changed.

If the status remains unchanged, this will show up as unknown

- **Next Change – Minute:** Minute when the Incident Next Status value was changed. If the status remains unchanged, this will show up as unknown
- **Next Change – Second:** Second when the Incident Next Status value was changed. If the status remains unchanged, this will show up as unknown
- **Next Change – Time:** Time when the Incident Next Status value was changed.

If the status remains unchanged, this will show up as unknown

DLP Next Change User

Applicable cubes:

- DLP Incident Status History

DLP Next Change User contains the following dimension attributes:

- **Next Change – User:** DLP user who set the Incident Next Status value

DLP Oracle Database

Applicable cubes:

- DLP Agent Status

- **DLP Discover Incident**

- **DLP Discover Incident Summary**
- **DLP Endpoint Incident Details**
- **DLP Endpoint Incident Summary**
- **DLP Incident Details**
- **DLP Incident History**
- **DLP Incident Status History**
- **DLP Incident Summary**
- **DLP Network Incident Details**
- **DLP Network Incident Summary**
- **DLP Network Statistics**
- **DLP Policy History**
- **DLP User Actions Audit**
- **DLP Discover Scans**

DLP Oracle Database contains the following dimension attributes:

- **Oracle Database – Host Name:** Denotes the oracle database name and instance name from which the data is obtained

DLP Pattern Condition

Applicable cubes:

- DLP Policy History

DLP Pattern Condition contains the following dimension attributes:

- **Patter Condition – Pattern:** Regular expression defined within the Content Matches Regular Expression condition type

DLP Policy Details

Applicable cubes:

- **DLP Discover Incident**

- DLP Endpoint Incident Details
- **DLP Incident Details**
- **DLP Network Incident Details**
- **DLP Policy History**

DLP Policy Details contains the following dimension attributes:

- **Policy – Is Deleted:** Indicates whether or not the policy has been deleted
- **Policy – Description:** Policy description as displayed in the Enforce console
- **Policy – ID:** Policy ID
- **Policy – Is Latest Version:** Indicates whether or not the policy version is the latest
- **Policy – Name:** Policy name
- **Policy – Status:** Indicates whether the policy is active or inactive
- **Policy – Version:** Policy version number

DLP Policy Group

Applicable cubes:

- DLP Discover Incident Details
- **DLP Discover Incident Summary**
- **DLP Endpoint Incident Details**
- **DLP Endpoint Incident Summary**
- **DLP Incident Details**
- **DLP Incident Summary**
- **DLP Network Incident Details**
- **DLP Network Incident Summary**

DLP Policy Group contains the following dimension attributes:

- **Policy – Group Name:** Policy Group names as defined in the Enforce console

DLP Policy Summary

Applicable cubes:

- DLP Discover Incident Summary
- **DLP Discover Scans**
- **DLP Endpoint Incident Summary**
- **DLP Incident Status History**
- **DLP Incident Summary**
- **DLP Network Incident Summary**
- **DLP Network Statistics**

DLP Policy Summary contains the following dimension attributes:

- **Policy – Description:** Policy description as displayed in the Enforce console
- **Policy – ID:** Policy ID
- **Policy – Name:** Policy name
- **Policy – Status:** Indicates whether the policy is active or inactive

DLP Protocol Condition

Applicable cubes:

- DLP Policy History

DLP Protocol Condition contains the following dimension attributes:

- **Protocol Condition – Protocol:** Protocol ID used within the Protocol or Endpoint Destination condition type

DLP Recipient Condition

Applicable cubes:

- DLP Policy History

DLP Recipient Condition contains the following dimension attributes:

- **Recipient Condition – Email Address:** Email address specified within the Recipient Matches Pattern condition type
- **Recipient Condition – IP Address:** IP address specified within the Recipient Matches Pattern condition type
- **Recipient Condition – URL:** URL specified within the Recipient Matches Pattern condition type

DLP Recipient Profile Condition

Applicable cubes:

- DLP Policy History

DLP Recipient Profile Condition contains the following dimension attributes:

- **Recipient Profile Condition – DataSourceID:** Data source ID for the directory profile

DLP Role

Applicable cubes:

- DLP Incident History
- **DLP Incident Status History**
- **DLP Policy History**

DLP Role contains the following dimension attributes:

- **Role – Description:** Role description as displayed in the Enforce console.
- **Role – Name:** Role name as displayed in the Enforce console

DLP Scan Started Date

Applicable cubes:

- DLP Discover Scans

DLP Scan Started Date contains the following dimension attributes:

- **Scan Started – Date:** Date the discover target scan started
- **Scan Started – Date Range:** Date range the discover target scan started
- **Scan Started – Day of Week:** Day the discover target scan started
- **Scan Started – Month:** Month the discover target scan started
- **Scan Started – Quarter:** Quarter the discover target scan started
- **Scan Started – Week Number:** Week number the discover target scan started
- **Scan Started – Year:** Year the discover target scan started

DLP Scan Started Time

Applicable cubes:

- DLP Discover Scans

DLP Scan Started Time contains the following dimension attributes:

- **Scan Started – Hour:** Hour the discover target scan started
- **Scan Started – Minute:** Minute the discover target scan started
- **Scan Started – Second:** Second the discover target scan started
- **Scan Started – Time:** Time the discover target scan started

DLP Sender Condition

Applicable cubes:

- DLP Policy History

DLP Sender Condition contains the following dimension attributes:

- **Sender Condition – IP Address:** IP address specified within the Sender/User Matches Pattern condition type
- **Sender Condition – Sender Identifier:** Email address, windows username, or IM screen name specified within the Sender/user Matches Pattern condition type

DLP Sender Profile Condition

Applicable cubes:

- DLP Policy History

DLP Sender Profile Condition contains the following dimension attributes:

- **Sender Profile Condition – DataSourceID: profile** Data source ID for the directory

DLP Time Condition Created

Applicable cubes:

- DLP Policy History

DLP Time Condition Created contains the following dimension attributes:

- **Condition Created – Hour:** Hour the condition was created
- **Condition Created – Minute:** Minute the condition was created
- **Condition Created – Second:** Second the condition was created
- **Condition Created – Time:** Time the condition was created

DLP Time Condition Edited

Applicable cubes:

- DLP Policy History

DLP Time Condition Edited contains the following dimension attributes:

- **Condition Edited – Hour:** Hour the condition was edited (shows historical

data)

- **Condition Edited – Minute:** Minute the condition was edited (shows historical data)
- **Condition Edited – Second:** Second the condition was edited (shows historical data)
- **Condition Edited – Time:** Time the condition was edited (shows historical data)

DLP Time Policy Created

Applicable cubes:

- DLP Policy History

DLP Time Policy Created contains the following dimension attributes:

- **Policy Created – Hour:** Hour the policy was created
- **Policy Created – Minute:** Minute the policy was created
- **Policy Created – Second:** Second the policy was created
- **Policy Created – Time:** Time the policy was created

DLP Time Policy Edited

Applicable cubes:

- DLP Policy History

DLP Time Policy Edited contains the following dimension attributes:

- **Policy Edited – Hour:** Hour the policy was edited (shows historical data)
- **Policy Edited – Minute:** Minute the policy was edited (shows historical data)
- **Policy Edited – Second:** Second the policy was edited (shows historical data)
- **Policy Edited – Time:** Time the policy was edited (shows historical data)

DLP Universal Metadata Condition

Applicable cubes:

- DLP Policy History

DLP Universal Metadata Condition contains the following dimension attributes:

- **Universal Metadata Condition – Metadata Key:** Indicates the type of the rule.

  Possible values: NetworkLocation
- **Universal Metadata Condition – Metadata Source:** A constant value of 1.
- **Universal Metadata Condition – Metadata Value:** Indicates the endpoint location. Possible values: 0 and 1 where 0 = 'On the corporate network' and 1

  = 'Off the corporate network'
- **Universal Metadata Condition – Metadata Value Operand:** A constant value of 'CSVSTRING'

DLP User Action

Applicable cubes:

- DLP User Actions Audit

DLP User Action contains the following dimension attributes:

- **User Action – Category:** Action taken when the event occurred
- **User Action – Detail:** Free text details for the event
- **User Action – Entity:** Object or component name on which the event occurred
- **User Action – IP Address:** IP Address of the PC that triggered the event
- **User Action – Role:** Role assigned to the user who triggered the event

›

- **User Action – User Name:** DLP user who triggered the event

DLP User Action Date

Applicable cubes:

- DLP User Actions Audit

DLP User Action Date contains the following dimension attributes:

- **User Action – Date:** Date the event occurred
- **User Action – Date Range:** Date range the event occurred
- **User Action – Day of Week:** Date of the week the event occurred
- **User Action – Month:** Month the event occurred
- **User Action – Quarter:** Quarter the event occurred
- **User Action – Week Number:** Week number the event occurred
- **User Action – Year:** Year the event occurred

DLP User Action Time

Applicable cubes:

- DLP User Actions Audit

DLP User Action Time contains the following dimension attributes:

- **User Action – Hour:** Hour the event occurred
- **User Action – Second:** Second the event occurred
- **User Action – Minute:** Minute the event occurred
- **User Action – Time:** Time the event occurred

DLP User Created By

Applicable cubes:

- DLP Policy History

DLP User Created By contains the following dimension attributes:

- **User – Created By:** DLP user who created the policy

DLP User Edited By

Applicable cubes:

- DLP Policy History

DLP User Edited By contains the following dimension attributes:

- **User – Edited By:** DLP user who modified the policy