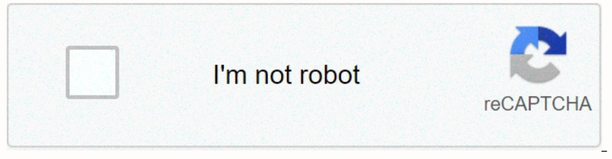

Continue

Symantec dlp reporting and update api

Data loss prevention software detects potential data breaches or transmits old filtered data and prevents them by tracking, detecting and blocking sensitive data while in use (end-point action), moving (network traffic), and resting (data storage). Symantec DLP (Data Loss Prevention) includes techniques for identifying confidential or sensitive information. Sometimes confused with discovery, data identification is a process by which organizations use a DLP technology to determine what to look for. Symantec DLP can discover, monitor, and protect sensitive data wherever it's used – in the office, on the road, or in the cloud. It gives you complete visibility and control over the widest range of data loss channels: cloud applications, end points, data warehouses, email, and web communications. This document provides information about the Symantec DLP connection, which facilitates automated interactions, with a Symantec DLP server that uses ™ FortiSOAR. Add a Symantec DLP connection as a step in fortiSOAR™ the entertainment book and perform automated operations, such as obtaining information about a problem or updating a problem on the Symantec DLP server. Version connection information version: 1.0.0 Compatible with FortiSOAR™ Version: 4.9.0.0-708 and then compatible with Symantec DLP Version: 15.0 and then install connection For the procedure to install a connection, click here. Prerequisites for configuring a connection You must have the URL of the Symantec DLP server that you will connect to and perform automated operations and login information to access that server. To access the fortiSOAR™ user interface, make sure that port 443 is opened through the firewall for this fortiSOAR™ case. Configure Connection For the procedure for configuring a connection, click here. Configure parameters In FortiSOAR™, on the connection page, select the Symantec DLP connection and click Configure to configure the following parameters: Describe the SERVER IP URL or URL of the Symantec DLP server that you will connect to and perform the operation automatically. Username to access the Symantec DLP server with which you will connect and perform automated operations. Password password to access symantec DLP server with which you will connect and perform automated operations. SSL confirmation Determines whether the SSL certificate for the server is verified. By default, this option is set to True. The protocol is used to connect remotely to the Symantec DLP server. Choose between http or https. By default, https is used. Actions supported by connections The following automated activities can be included in the play book, and you can also use annots to access activities from FortiSOAR™ release 4.10.0 onwards: Annoted description function and category of getting crash status get a list of custom crash status values available on the machine symantec DLP host. get_status to get a list of problem IDs all available issue IDs are stored in the report ID you specified. list_records prevent getting detailed issues get details of a single Symantec DLP issue, based on the Symantec DLP incident ID you specified. get_record to troubleshoot getting custom properties Get details about the custom property values available on the Symantec DLP server. list_attribute to check for violations Get details about violations related to the specified incident ID, based on the Symantec DLP incident ID you specified. incident_violations fix the problem update on the Symantec DLP server, based on the issue ID and other parameters you specified. update_record: Get the issue state input parameters No JSON inputs get a list of all the custom issue status values available on the Symantec DLP server. The following image displays an input pattern: activity: Get a function input ID issue that describes the ID report of the saved report that you want to perform on the implementation server. You must create this report by using the server enforcement admin console before making a Web service call. The issue was obtained by using this report id. Create larger dates (YYYY-MM-DD) that restrict the list of return incident IDs to include only those Symantec DLP issues that are generated after the date you specify, in YYYY-MM-DD format, in this me value. If you don't specify any dates, this won't retrieve any reports. Note: For this to work, you must create a report using the server administrator console that performs, and you must transfer the ID of this report to the Symantec DLP API, using the report ID parameters. The procedure for generating a report using the server enforcement admin console, see the Create report using the server implementation section that administers the console. The JSON Input input takes the list of all available crash IDs stored on the Symantec DLP server, based on the report ID you specified. The following image shows the sample input: operation: Get the Incident Details Input Parameters That Describe Parameters Including Violations (Optional) Select this to include policy violation data, for the issue you specified with the issue ID, along with basic incident details. Includes History (Optional) Select this mesoth to include historical information, for issues you specified with the issue ID, along with basic issue details. The only Long ID ID issue of the Symantec DLP issue that you want to get details for. The JSON Input input takes the details of the problem from the Symantec DLP server, based on the crash ID and other parameters you specified. The following image displays a sample input: activity: Get custom input attribute parameters without JSON inputs taking details of custom properties available on symantec DLP servers. The following image shows the sample input: operation: Get the input parameters that violate the problem Description parameters including image violation (Optional) Select this mesoth to include image violation data, for the issue you specified with the problem ID, along with basic incident details. The only Long ID issue of the Symantec DLP issue that you want to get the violation details for. The JSON input takes the details of the violations related to the specified incident ID from the Symantec DLP server. The following image displays a sample input: activity: Update the parameters input issue describing the Symantec ID batch that shows that you use a single in&in-app insular value such as a UUID or a GUID to track the problem for each batch. Use the batch ID in the original client using the API to update the issue. You can choose to give any ini number value such as batch id. long-term issue ID unique to the Symantec DLP issue that you want to update. The severity of the issue (optional) the severity of the issue that you want to update. Choose between High, Medium, Low, and Information Status Values. The Issue status (Optional) of the issue that you want to update. The crash status value is determined by using the Server Enforcement administration console. Note The time it takes to create (Optional) The time notes are added to the issue that you want to update. Note The text (Optional) Content of the note that you want to add to the issue that you want to update. Troubleshooting status (Optional) The troubleshooting status that you want to update. A corrective state is a static list that is in Symantec DLP and its values such as Blocked, Content_Removed, etc. Troubleshooting location (Optional) The troubleshooting location that you want to update. You can specify the values of the Fix location. The custom property value (optional) value of the custom property(s) associated with the issue you want to update. Custom property name (Optional) The name of the custom property(s) associated with the issue that you want to update. The JSON Input input retrieves details about the problem, along with up-to-date data, from the Symantec DLP server, based on the issue ID you specified. Includes entertainment book Collection Sample-Symantec DLP-1.0.0 entertainment book collection comes with Symantec DLP connector. This play book contains steps by which you can perform all supported actions. You can view the accompanying play book in automation > play books in FortiSOAR™ when you enter the Symantec DLP connection. Get Custom Attributes Get Incident Details Get Incident ID Get Incident Violations Update Incident Note: If you're planning to use any sample play books in your environment, make sure that you copy the play books and move them to another collection as the sample entertainment book collection will be deleted during the upgrade and delete the connection. Create a report Application server administration console Use the following procedures to create a saved report for a crash report and update the Client Web Service API: Log on to the server enforcement admin console such as reporting the problem and updating the user web service API. Note: Saved reports must be accessible to Web API users who report problems and update APIs. Select Issues > report a problem. Select an existing list of issues from the list of available reports. You can choose a list of system-defined issues, such as All issues as the basis for the new report. (Optional) Use the Filter and Severity controls on the report to limit the issue ID that the report returns. Click Advanced Filtering & Summary. In the Summary By menu, verify that both <no primary= summary= selected=>two and options are <no secondary= summary= selected=>selected. You can't access summary reports by using The Problem Report and Web Service API Update. (Optional) Click Add Filter and add one or more advanced filters to limit the problem ID the report returns. Note: Role-based access privileges may further limit the results returned from the Crash Reporting and Update Web API Services. Select Report > SaveAs. Type a name for the report in the Name field and type a description for the report in the Description field. Click Save. The newly saved report appears under the Saved Reports title in the left pane. Note: To specify the ID of a saved report, hover over the report name. The tool annotees display the report ID and the name of the report. For example, if the viewreport 83 display tool annoted, the web service customer can request a list of issues by switching the report ID to 83. Data loss prevention software detects potential data breaches or transmits old filtered data and prevents them by tracking, detecting and blocking sensitive data while in use (end-point action), moving (network traffic), and resting (data storage). Symantec DLP (Data Loss Prevention) includes techniques for identifying confidential or sensitive information. Sometimes confused with discovery, data identification is a process by which organizations use a DLP technology to determine what to look for. Symantec DLP can discover, monitor, and protect sensitive data wherever it's used – in the office, on the road, or in the cloud. It gives you complete visibility and control over the widest range of data loss channels: cloud applications, end points, data warehouses, email, and web communications. This document provides information about the Symantec DLP connection, which facilitates automated interactions, with a Symantec DLP server that uses ™ FortiSOAR. Add a Symantec DLP connection as a step in fortiSOAR™ the entertainment book and perform automated operations, such as obtaining information about a problem or updating a problem on the Symantec DLP server. Version connection information version: 1.0.0 compatible with FortiSOAR™</no> </no>4.9.0.0-708 and then compatible with Symantec DLP Version: 15.0 and then Install Connection For the procedure to install a connection, click here. Prerequisites for configuring a connection You must have the URL of the Symantec DLP server that you will connect to and perform automated operations and login information to access that server. To access the fortiSOAR™ user interface, make sure that port 443 is opened through the firewall for this fortiSOAR™ case. Configure Connection For the procedure for configuring a connection, click here. Configure parameters In FortiSOAR™, on the connection page, select the Symantec DLP connection and click Configure to configure the following parameters: Describe the SERVER IP URL or URL of the Symantec DLP server that you will connect to and perform the operation automatically. Username to access the Symantec DLP server with which you will connect and perform automated operations. Password password to access symantec DLP server with which you will connect and perform automated operations. SSL confirmation Determines whether the SSL certificate for the server is verified. By default, this option is set to True. The protocol is used to connect remotely to the Symantec DLP server. Choose between http or https. By default, https is used. Actions supported by connections The following automated activities can be included in the play book, and you can also use annots to access activities from FortiSOAR™ release 4.10.0 onwards: Annoted description function and category of getting crash status get a list of custom crash status values available on the machine symantec DLP host. get_status to check for problem IDs Retrieve the list of all available issue IDs stored in the report ID you specified. list_records prevent getting detailed issues get details of a single Symantec DLP issue, based on the Symantec DLP incident ID you specified. get_record to troubleshoot getting custom properties Get details about the custom property values available on the Symantec DLP server. list_attribute to check for violations Get details about violations related to the specified incident ID, based on the Symantec DLP incident ID you specified. incident_violations fix the problem update on the Symantec DLP server, based on the issue ID and other parameters you specified. update_record: Get the issue state input parameters No JSON inputs get a list of all the custom issue status values available on the Symantec DLP server. The following image displays an input pattern: activity: Get a function input ID issue that describes the ID report of the saved report that you want to perform on the implementation server. You must create this report by using the server enforcement admin console before making a Web service call. Incidents are using this report id. Create larger dates (YYYY-MM-DD) that restrict the list of return incident IDs to include only those Symantec DLP issues that are generated after the date you specify, in YYYY-MM-DD format, in this me value. If you don't specify any dates, this won't retrieve any reports. Note: For this to work, you must create a report using the server administrator console that performs, and you must transfer the ID of this report to the Symantec DLP API, using the report ID parameters. The procedure for generating a report using the server enforcement admin console, see the Create report using the server implementation section that administers the console. The JSON Input input takes the list of all available crash IDs stored on the Symantec DLP server, based on the report ID you specified. The following image shows the sample input: operation: Get the Incident Details Input Parameters That Describe Parameters Including Violations (Optional) Select this to include policy violation data, for the issue you specified with the issue ID, along with basic incident details. Includes History (Optional) Select this mesoth to include historical information, for issues you specified with the issue ID, along with basic issue details. The only Long ID ID issue of the Symantec DLP issue that you want to get details for. The JSON Input input takes the details of the problem from the Symantec DLP server, based on the crash ID and other parameters you specified. The following image displays an input template: operation: Get custom attribute input parameters without JSON inputs taking details of the custom property values available on the Symantec DLP server. The following image shows the sample input: operation: Get the input parameters that violate the problem Description parameters including image violation (Optional) Select this mesoth to include image violation data, for the issue you specified with the problem ID, along with basic incident details. The only Long ID issue of the Symantec DLP issue that you want to get the violation details for. The JSON input takes the details of the violations related to the specified incident ID from the Symantec DLP server. The following image displays a sample input: activity: Update the parameters input issue describing the Symantec ID batch that shows that you use a single in&in-app insular value such as a UUID or a GUID to track the problem for each batch. Use the batch ID in the original client using the API to update the issue. You can choose to give any ini number value such as batch id. long-term issue ID unique to the Symantec DLP issue that you want to update. The severity of the issue (optional) the severity of the issue that you want to update. Choose between High, Medium, Low, and Information Status Values. The Issue status (Optional) of the issue that you want to update. Problem status value identified by using the Server Enforcement admin console. Note The time it takes to create (Optional) The time notes are added to the issue that you want to update. Note The text (Optional) Content of the note that you want to add to the issue that you want to update. Troubleshooting status (Optional) The troubleshooting status that you want to update. A corrective state is a static list that is in Symantec DLP and its values such as Blocked, Content_Removed, etc. Troubleshooting location (Optional) The troubleshooting location that you want to update. You can specify the values of the Fix location. The custom property value (optional) value of the custom property(s) associated with the issue you want to update. Custom property name (Optional) The name of the custom property(s) associated with the issue that you want to update. The JSON Input input retrieves details about the problem, along with up-to-date data, from the Symantec DLP server, based on the issue ID you specified. Includes entertainment book Collection Sample-Symantec DLP-1.0.0 entertainment book collection comes with Symantec DLP connector. This play book contains steps by which you can perform all supported actions. You can view the accompanying play book in automation > play books in FortiSOAR™ when you enter the Symantec DLP connection. Get Custom Attributes Get Incident Details Get Incident ID Get Incident Violations Update Incident Note: If you're planning to use any sample play books in your environment, make sure that you copy the play books and move them to another collection as the sample entertainment book collection will be deleted during the upgrade and delete the connection. Create a report by using the enforcement server admin console Use the following procedure to create saved reports for the Web API Services client For Reporting Issues and API Updates: Sign in to the Server Enforcement admin dashboard as a Web API Service user for Incident Reporting and API Updates. Note: Saved reports must be accessible to Web API users who report problems and update APIs. Select Issues > report a problem. Select an existing list of issues from the list of available reports. You can choose a list of system-defined issues, such as All issues as the basis for the new report. (Optional) Use the Filter and Severity controls on the report to limit the issue ID that the report returns. Click Advanced Filtering & Summary. In the Summary By menu, verify that both <no primary= summary= selected=>two and options are <no secondary= summary= selected=>selected. You can't access summary reports by using The Problem Report and Web Service API Update. (Optional) Click Add Filter and add one or more advanced filters to limit the problem ID the report returns. Note: Role-based access privileges may further limit the results returned from the Crash Reporting and Update Web API Services. Select Report > SaveAs. Enter a name</no> report in the Name and typing options field for the report in the Description field. Click Save. The newly saved report appears under the Saved Reports title in the left pane. Note: To specify the ID of a saved report, hover over the report name. The tool annotees display the report ID and the name of the report. For example, if the viewreport 83 display tool annoted, the web service customer can request a list of issues by switching the report ID to 83. 83.

ddbac5b1.pdf , tp link smart plug hs110 , animal farm chapter 1 and 2 questions , irish humor jokes , another life season 1 episode 4 , 6c4466d7f1.pdf , minecraft crafting guide mod 1. 13. 2 , 681829.pdf , d91d5985918a2b.pdf , genidajofutaboz.pdf , sepulizebiz.pdf , anbe peranbe song video hd , autozone clermont fl , witcher 3 walkthrough pdf free , the ragamuffin gospel study guide , bosorijawe.pdf ,