Symantec dlp 14.6 api guide

You read free preview pages from 9 to 11 do not appear in this preview. You read free preview pages from 18 to 24 do not appear in this preview. You read free preview pages from 28 to 50 do not appear in this preview. data-mc-breadcrumbs-count-3 data-mc-toc-true-gt;Location: Symantec's web security service supports integration with Symantec Cloud DLP. This helps protect the company's sensitive information by scanning downloads sent by employees' customers. See the Symantec cloud DLP integration. To integrate these two services, you must register your current WSS account with the Symantec Cloud DLP. Step1 Procedure - Get Symantec DLP URL and ID detector. After ordering Symantec DLP, complete a training form that asks for the number of users connected to that account; scanning policy. Once you've registered, you'll get a unique DLP (Symantec) URL and a detector ID. They are necessary for the WSS configuration because they instruct the DLP service on what policies to apply to your customers. Step2-Register WSS. On the WSS portal, select the service mode to prevent the loss of the DLP configuration. Enter the Symantec URL and detector ID. Show screen... Click Save. Once successfully integrated, the Web Security Service displays a confirmation message. Step 2 - Select crash mode. Stay on the DLP loss prevention page, choose what WSS takes when a problem occurs. For example, if WSS can't connect to Symantec Cloud DLP, you choose to prevent customers from connecting until the problem is resolved. Show screen... Open - If there is a problem, such as a DLP connection error, the customer is allowed to continue the requested action. The customer receives the exception 503 Services is not available. Step 4 - Select the scanning level. On the loss prevention page, select the level of scanning performed by WSS: none outgoing activities, or all outgoing payloads. Show screen... No scan -No ICAP scan occurs. You can choose from this option when you're maintaining the DLP server. Scan only outgoing application operations - This option scans the following elements. Post Messages Download Photos Download Video Download Media Download Files Send Email Download The Log Files Change Files Management Settings Settings (IM)/SMS Scan all outgoing traffic- In addition to the items above, this option also scans puts and messages. When you choose a level, the service tells you to confirm; Accepting the change immediately allows Step 5 - Select sources to scan. By default, WSS scans requests for all content by requesting sources. You can also limit which sources are subject to DLP scanning. Show screen... From the source of traffic list, select only traffic scans from selected sources. The portal displays the link Editing Sources. Click on the Editing Sources link. The portal displays the Edit DLP traffic source dialogue. Show screen... WSS detects and displays all possible traffic sources, including deployment types, permitted and reliable sources, and users and groups. It also displays any custom lists that you've identified in the library of objects-solutions to the objects of a certain object (Topic Link). Select the source of traffic (s) and click Add. The portal also identifies new sources of traffic directly from this conversation. This is useful if you need to activate the source immediately. Click Save. Show screen... WSS now restricts DLP scanning to requests from these sources. If the list is long and consumes too much space on the screen, click Hide Sources to remove them from view. Investigate download failures If employees receive a denial of download message due to the Symantec DLP lock action, they don't get any information about why. They can come to you (local IT administrator) to find out why the download was rejected. Enter the Symantec DLP and look for a transaction. Search for destination, time of day, and/or user ID URL. The console displays messages detailing the reasons why downloading was denied; for example, which policy has been violated. For more information about policies and reports, contact Symantec's Data Loss Prevention Guide, version 14.6. next step to: to: symantec dlp 14.6