How to Protect Confidential Data Using Cisco Web Security Appliance with Digital Guardian
## Contents

<table>
<thead>
<tr>
<th>Topic</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>About This Document</td>
<td>3</td>
</tr>
<tr>
<td>Product Description</td>
<td>3</td>
</tr>
<tr>
<td>Configuration on the Cisco WSA</td>
<td>3</td>
</tr>
<tr>
<td>Configuration on Digital Guardian</td>
<td>5</td>
</tr>
</tbody>
</table>
About This Document
This document is for Cisco and Digital Guardian engineers, partners and customers who want to integrate the Cisco® Web Security Appliance (WSA) with a Digital Guardian appliance. The aim is to protect confidential data, customer data and intellectual property from leaving the organization through the web channel.

Product Requirement for Interoperability

<table>
<thead>
<tr>
<th>Product</th>
<th>Model</th>
<th>Software Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Web Security Appliance</td>
<td>S690, S390, S190, S680, S380, S670, S370, S170,S600v, S300v, S100v, S000v</td>
<td>8.x, 9.x, 10.x</td>
</tr>
<tr>
<td>Digital Guardian Appliance</td>
<td>Appliance or virtual appliance</td>
<td>8.x, 9.x</td>
</tr>
</tbody>
</table>

Product Description
Cisco Web Security Appliance (WSA) with Advanced Malware Protection (AMP) is an all-in-one highly secure web gateway that offers broad protection, extensive controls, and investment value. It offers an array of competitive web security deployment options, each of which includes Cisco’s market-leading global threat intelligence infrastructure. WSA offers an integrated approach to help disparate security point solutions to work together, to triangulate information for faster identification, and to more effectively mitigate and remediate threats.

Digital Guardian offers a complete data loss prevention (DLP) solution that allows companies to effectively discover, monitor, control, and secure sensitive data. Digital Guardian’s DLP solution uses content and context awareness to support complex use cases that involve intellectual property, trade secrets, customer lists, customer credit card information, and other data.

Cisco WSA and Digital Guardian’s DLP solution are integration tested to provide a comprehensive, easy-to-deploy data loss prevention solution that helps organizations effectively monitor, control and prevent sensitive data from leaving their network. The solution enforces policies to ensure protection, whether HTTP/HTTPS, File Transfer Protocol (FTP) or Secure Sockets Layer (SSL) is used for data transfer over the Web. It also protects data in applications such as webmail, blogs, and wikis.

Cisco WSA communicates with Digital Guardian’s Network DLP appliance by means of plain or secure Internet Content Adaptation Protocol (ICAP). By directing all outbound HTTP, HTTPS and FTP traffic to Digital Guardian’s Network DLP appliance, you can allow or block the traffic based on the configured rules and policies. You can also conduct deep content inspection for regulatory compliance and intellectual property (IP) protection, incident severity definition, case management and performance optimization.

Configuration on the Cisco WSA

Summary
1. Define an external DLP system on the Cisco WSA that works with the Digital Guardian appliance in your network.
2. Create one or more external DLP policies that define which traffic the WSA sends to Digital Guardian for content scanning.
3. Configure the minimum ICAP Request body size.

Step 1: Configure an External DLP Server
Open the Cisco WSA appliance management console. In the menu that appears, click “Network → External DLP Servers”. The External DLP Servers page appears, as shown below.
Click on the Edit Settings

Edit the External DLP Servers settings and add the correct Server Address and Port with the correct Service URL. Click on Start Test to verify the connectivity. Select the appropriate Failure Handling option and then click Submit.

Note:

• For the Server Address, provide the hostname of the DLP system. The Server Address can be a URL/string or an IP address. From an overall functional perspective, both the URL and IP address work fine with the Content Inspection (CI) Appliance.

• For Reconnection Attempts, use 5 or an appropriate number of times that you want WSA to try to reconnect to the DLP system.

• For the Service URL, type the IP address that is assigned to eth4 on the CI Appliance. Use the icap prefix and specify request: icap://<dlp_eth4_IP>/request.

Click Submit and Commit all changes to save.

Step 2: Configure an External DLP Server Policy

Open the WSA appliance management console. In the menu that appears, click Web Security Manager > External Data Loss Prevention.

In the External DLP Policies page you will find Global Policy by default.
Under Destinations, click in the **Scan:** None field to edit the settings.
Change None → **Scan all uploads**

Click **Submit** and then **Commit** changes

**Step 3: Configure the Minimum ICAP Request Body Size on CLI**
Configure the minimum ICAP request body size that will be sent to Digital Guardian appliance for ICAP scanning. The default is 4096 bytes. Change it to around 20 bytes (or the size you want) and commit the changes. The CLI changes are captured in the following screen. Use the command `externaldlpconfig` to modify the minimum ICAP request body size. Make sure the settings are properly saved and applied to the WSA device.

**Configuration on Digital Guardian**

**Summary**
1. Define the basic configuration on Digital Guardian to integrate with WSA.
2. Configure PCI compliance policy in Digital Guardian.
3. Testing the client to make sure it blocks credit cards.
4. Checking the logs and reports on Digital Guardian.

**Step 1: Configure the Digital Guardian Server**
Choose Manager System → Configuration → Network

**Note:** Please configure eth4 as the interface that will be listening for the ICAP protocol

Choose the **Enable** checkbox for ICAP Server with the default port number.
Step 2: Configure PCI Compliance

An example: Create a new policy and name it as PCI Web. Under Select Actions, choose Workflow → Log High, and under Remediation choose Block transaction.

Click Next

In the Registered Data field, choose the option Specify Registered Data that will be used as a content constraint in this Policy.

Under Pattern, choose CCN. In the Constraints dialog box, for the Enter Range field, enter 1 and then click Next.
Assign this policy to only specific appliances or to all the appliances, depending upon your mode of deployment, and click Next.

Preview the policy configuration and then click on Finish.

The policy PCI Web will now be displayed and enabled.

Step 3: Testing the Client for PCI Compliance
From the client, browse to https://alt.org/post or http://dlp.cloud/ for non-SSL testing, or go to any external webmail website and try to add some credit card information.

Step 4: Checking Logs and Reports on the Digital Guardian Console
Under Incidents, go to the top two incidents which are hitting the PCI Web policy.
Click on the incident to view the details: The Tabs are HTTPS, Workflow, History, and Related Incidents. For example, in the HTTPS Tab, you can view:

- Policy
- Sample Match
- Inspection Service
- Source and Destination
- User
- Server Name
- HTTPS Details – Date/Time, File Size, and URL

Lastly, you can also choose option in the View File menu.

This wraps up our configuration on Cisco Web Security Appliance and Digital Guardian.