Cisco Systems, Inc
IronPort

RSA Secured Implementation Guide for RSA DLP Network

Last Modified: December 5th, 2012

Partner Information

Product Information	
Partner Name	Cisco Systems, Inc
Web Site	www.cisco.com
Product Name	Cisco IronPort S-Series
Version & Platform	7.5
Product Description	The Cisco IronPort S-Series Web Security Appliance addresses security risks by combining innovative technologies on a single platform. It employs advanced tools including acceptable-use-policy controls, reputation filtering, malware filtering, data security, and application visibility and control.

Solution Summary

In the Information Age, your organization's data is one of its most prized possessions. Your organization spends a lot of money making data available to your employees, customers, and partners. Data is always on the move by traveling over the web and email. This increased access poses challenges for information security professionals to figure out how to prevent the malicious, accidental, or unintentional loss of sensitive and proprietary information. To better protect your corporate data, the Cisco IronPort S-Series can integrate with RSA DLP Network via the ICAP protocol to identify sensitive data and enforce corporate policies.

Partner Integration Overview	
Protocols Supported	HTTP POST/GET/PUT, HTTPS POST/GET/PUT, FTP
Webmail Supported	Gmail, Yahoo! Mail, Microsoft Outlook (Hotmail)
ICAP Service	Request Mode
Remediation Actions Available	Allow, Audit, Block, Encrypt

IRONPORT

Partner Product Configuration

Introduction

The Cisco IronPort Web Security appliance integrates with RSA Data Loss Prevention to identify and protect sensitive data. The Web Proxy uses the Internet Content Adaptation Protocol (ICAP) which is a lightweight HTTP based protocol that allows proxy servers to offload content scanning to external systems. By offloading to dedicated external systems, the Web Proxy can take advantage of the deep content scanning in RSA DLP Network, while being free to perform other Web Proxy functions with minimal performance impact.

Before You Begin

This section provides instructions for integrating the partners' product with the RSA Data Loss Prevention (DLP) Suite. This document is not intended to suggest optimum installations or configurations.

It is assumed that the reader has both working knowledge of all products involved, and the ability to perform the tasks outlined in this section. Administrators should have access to the product documentation for all products in order to install the required components.

All vendor products/components must be installed and working prior to the integration. Perform the necessary tests to confirm that this is true before proceeding.

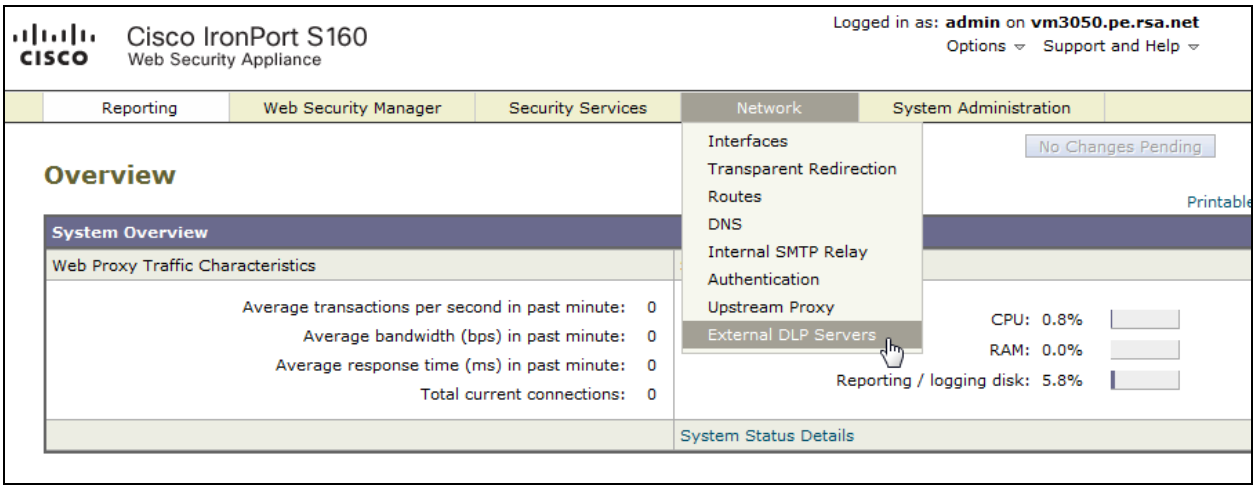
Configuring the Cisco IronPort S-Series

In order the integrate Cisco IronPort with RSA DLP you must first define the RSA DLP ICAP Server as an **External DLP Server**. Next, you will create an **External DLP Policy** so that data can be forwarded to the RSA DLP ICAP Server for content inspection.

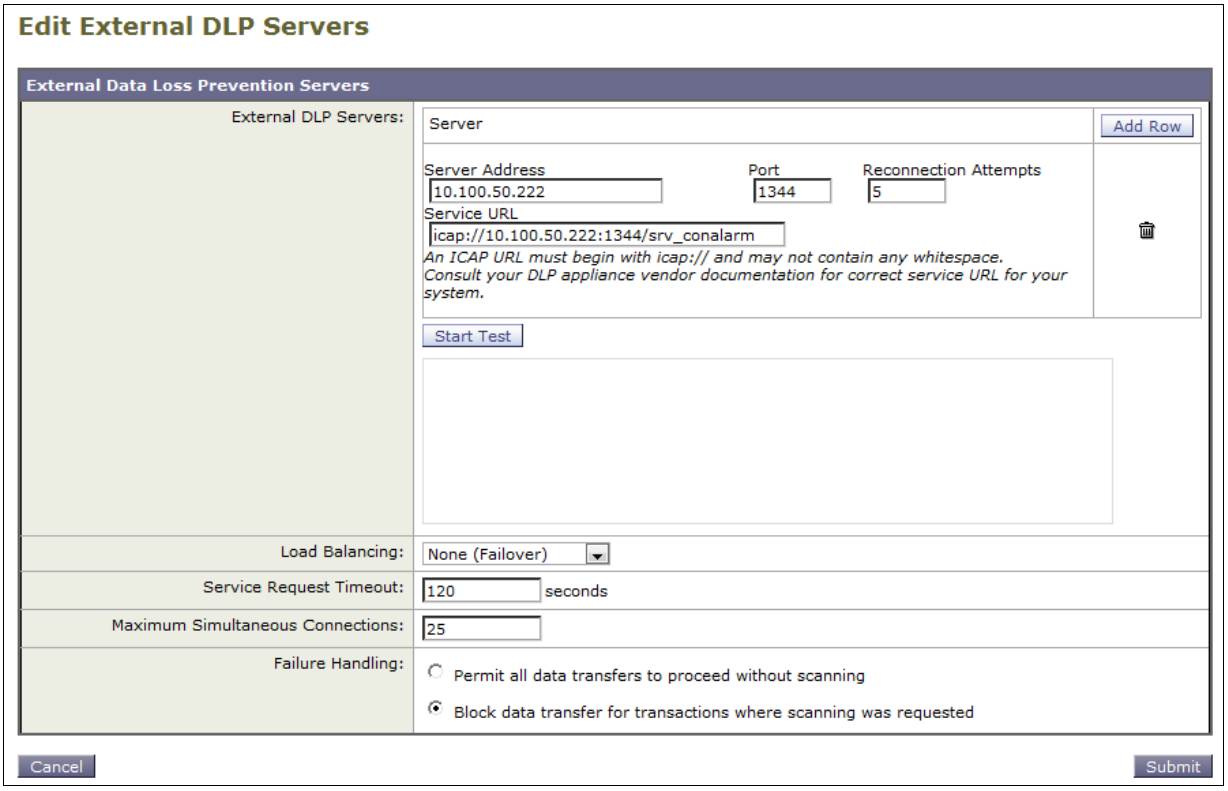
Adding an External DLP Server

The Cisco IronPort Web Security appliance can integrate with multiple external RSA DLP ICAP servers by defining multiple External DLP servers in the appliance. To do this, perform the following steps:

1. Log into the IronPort admin console and select **Network → External DLP Servers**.



2. Click **Edit Settings** and enter the connection details for your RSA DLP ICAP Server.



The Service URL should be in the format:

`icap://<Your_DLP_ICAP_Server>:1344/srv_conalarm`

3. Click **Submit** to save the changes. You may also add additional ICAP Servers by clicking the **Add Row** button.

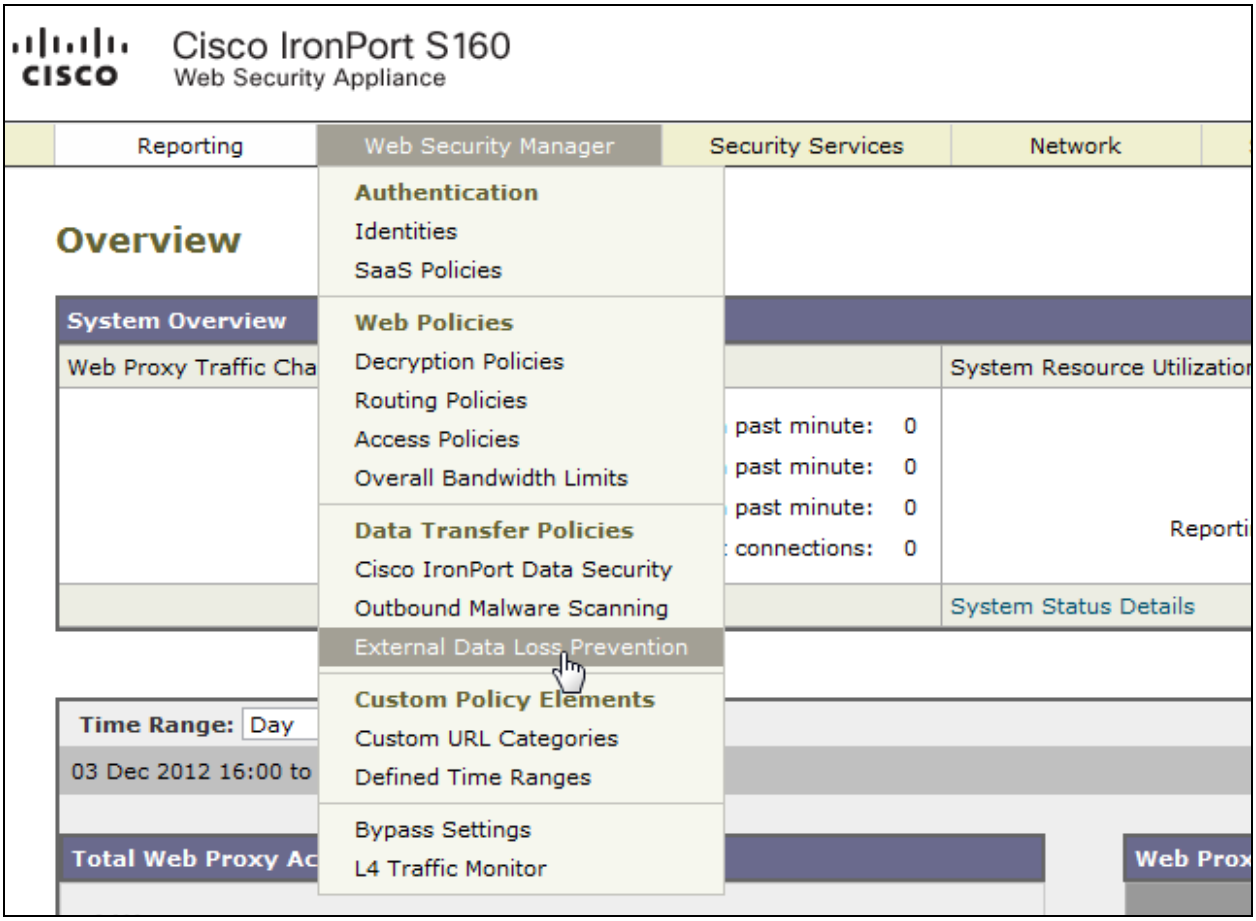
Adding an External DLP Policy

! Important: Cisco IronPort has a minimum request body size, below which upload requests are NOT scanned by the external DLP server. The default minimum request body size is 4KB (4096 bytes). For more information, please consult the *Bypassing Upload Requests Below a Minimum Size* section of the Cisco IronPort Online Help or User Guide.

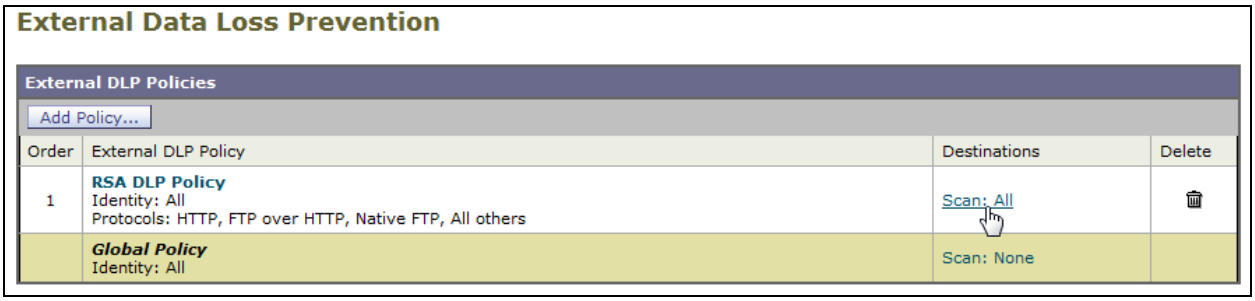
When you configure the appliance to work with an external DLP system, you can create External DLP Policies to pass data leaving the network to the external DLP system which scans the content and determines whether or not to block the request. To do this, perform the following steps:

To configure control settings for an External DLP Policy group:

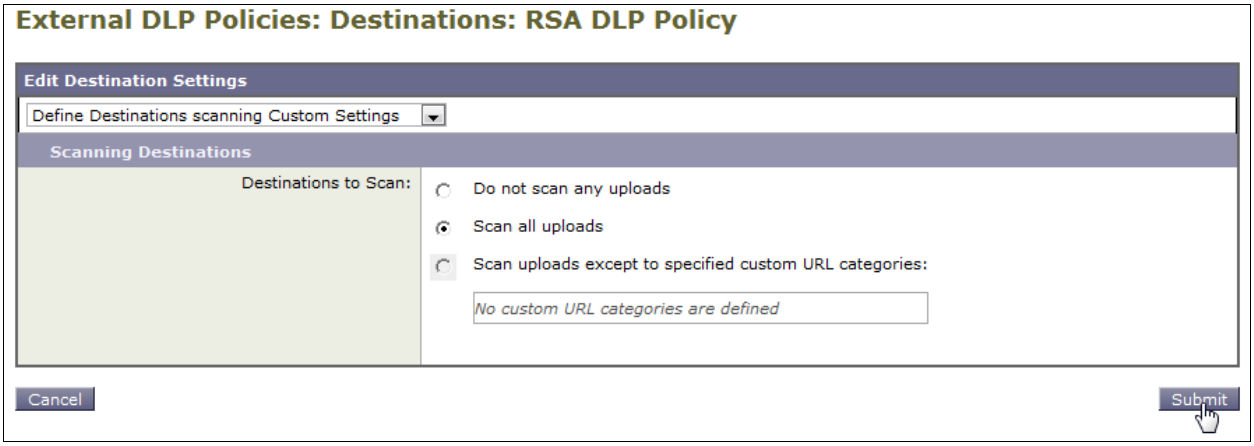
1. Navigate to **Web Security Manager → External Data Loss Prevention**.



2. Click the link under the **Destinations** column for the policy group you want to configure.



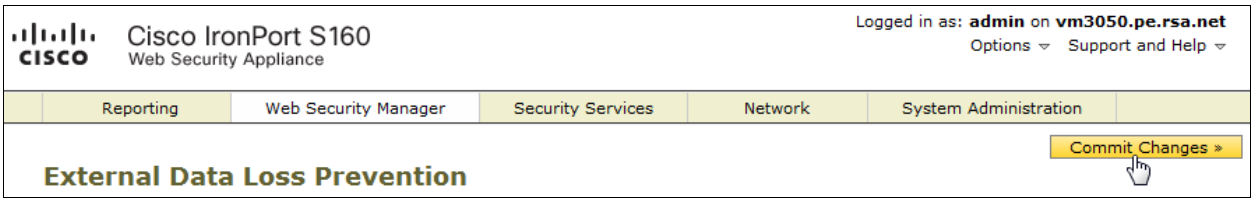
3. Under the **Edit Destination Settings** section, choose **Define Destinations Scanning Custom Settings** from the drop down menu if it is not selected already.



4. In the **Destinations to scan** section, choose one of the following options:

   - **Do not scan any uploads**. No upload requests are sent to the configured DLP system(s) for scanning. All upload requests are evaluated against the Access Policies.
   - **Scan all uploads**. All upload requests are sent to the configured DLP system(s) for scanning. The upload request is blocked or evaluated against the Access Policies depending on the DLP system scanning verdict.
   - **Scan uploads to specified custom URL categories only**. Upload requests that fall in specific custom URL categories are sent to the configured DLP system for scanning. The upload request is blocked or evaluated against the Access Policies depending on the DLP system scanning verdict. Click Edit custom categories list to select the URL categories to scan.

5. **Submit** then **Commit Changes**. The Cisco IronPort device is now configured to forward upload traffic to the RSA DLP ICAP Server for processing.



Configuring RSA Data Loss Prevention Suite

Note: Before you can start utilizing Cisco Ironport, an RSA DLP Network ICAP Server must be deployed and properly configured. For instructions, see the RSA DLP Network Deployment Guide.

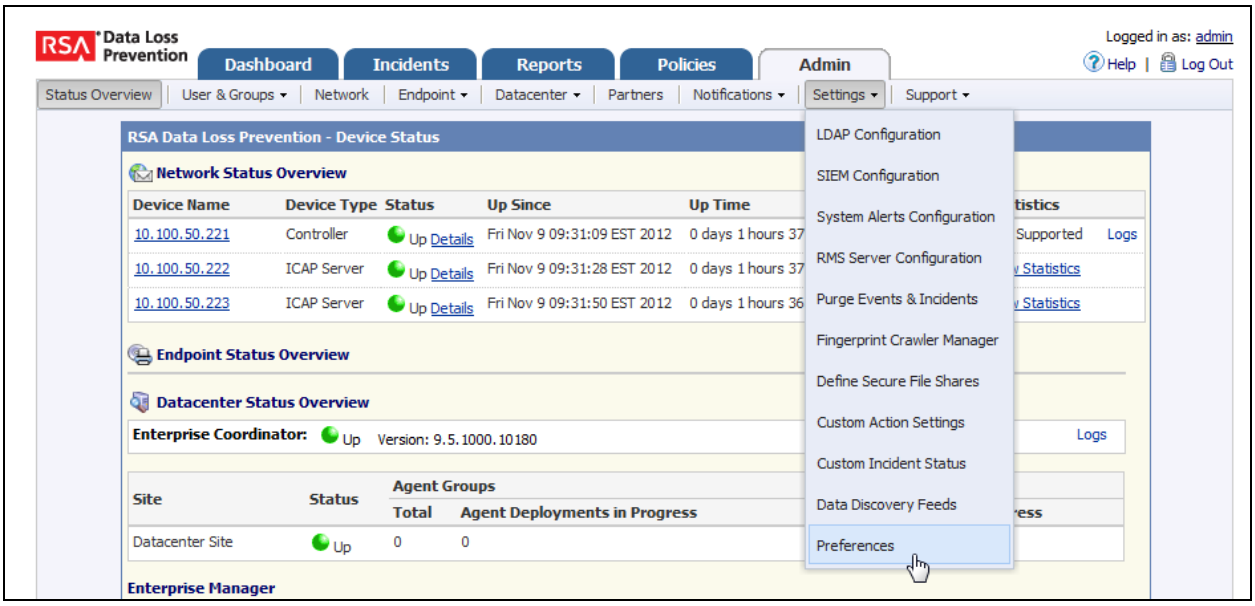
Once you have deployed the RSA DLP ICAP server, there are a number of steps required to configure the ICAP Server for proper inspection of HTTP/HTTPS content:

- Enabling Detection of Content in URLs
- Configuring Content Blades to Detect Content in URLs and HTTP Forms
- Configuring HTTPS Encrypt Policy Actions

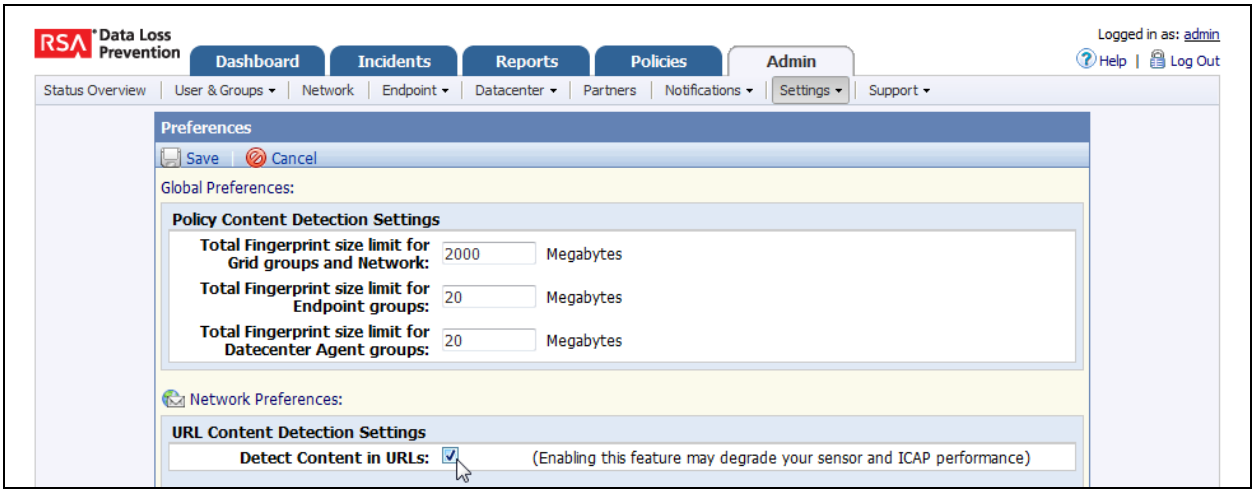
Enabling Detection of Content in URLs

The steps to enable content detection in URLS are as follows:

1. From the RSA DLP Enterprise Manager, select the **Admin…** tab → **Preferences**.



2. Under Network Preferences, select the **Detect Content in URLs** checkbox.



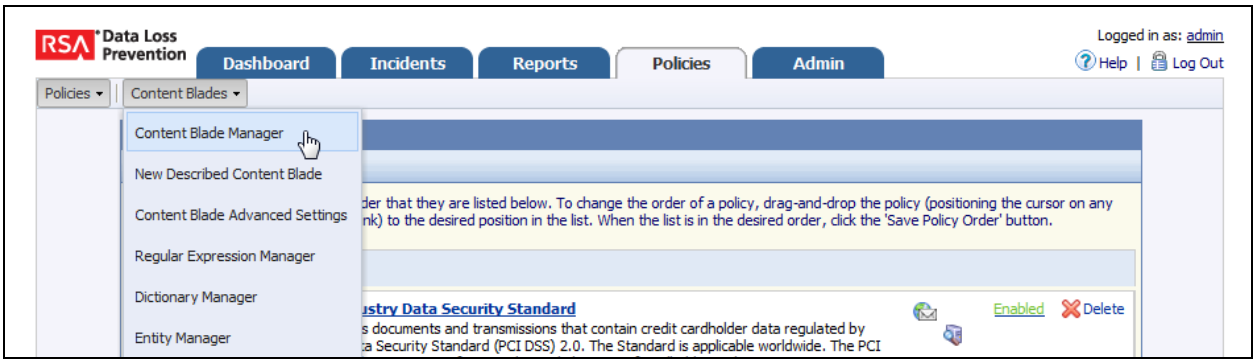
3. Click **Save** to preserve your changes.

Configuring Content Blades to Detect Content in URLs and HTTP Forms

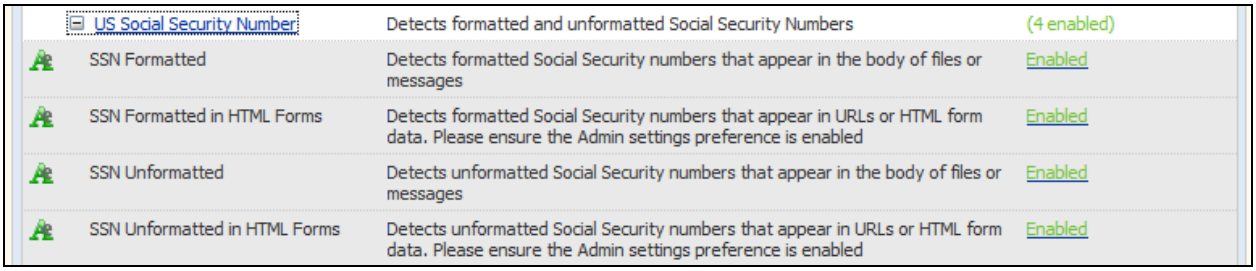
The second step for ICAP configuration is to ensure that for any given policy, the associated content blades are configured to detect content in URLs and HTTP forms. To do this, perform the following steps via the DLP Enterprise Manager.

> **! Important: Detecting content in URLs and HTTP forms can degrade the performance of the ICAP server. For more information, please see Consequences of Enabling HTML Form-Specific Content Blades in the RSA DLP Network User Guide.**

1. Select the **Policies…**tab → **Content Blades…** → **Content Blade Manager**.



2. Ensure that (as in the US Social Security Number example provided below) the option to detect content in URLs or HTML forms is **Enabled** for the given content blade.

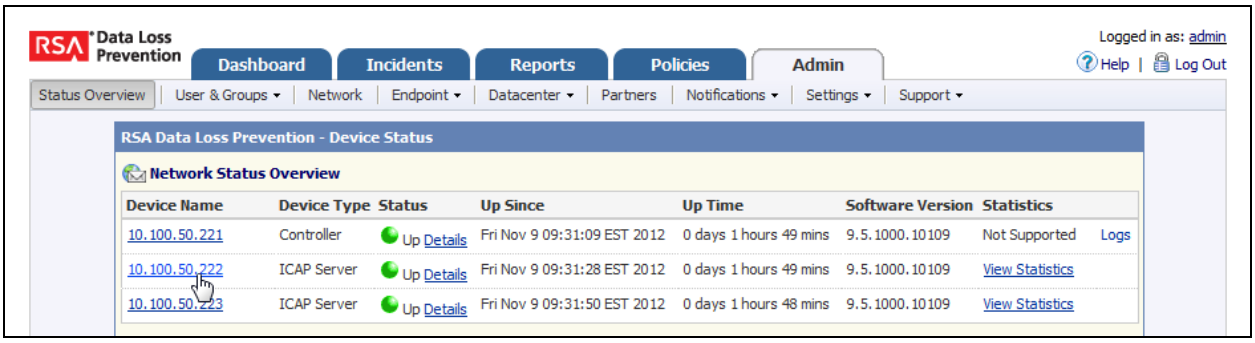


3. Save your changes and verify that this option is enabled for any other relevant content blades.

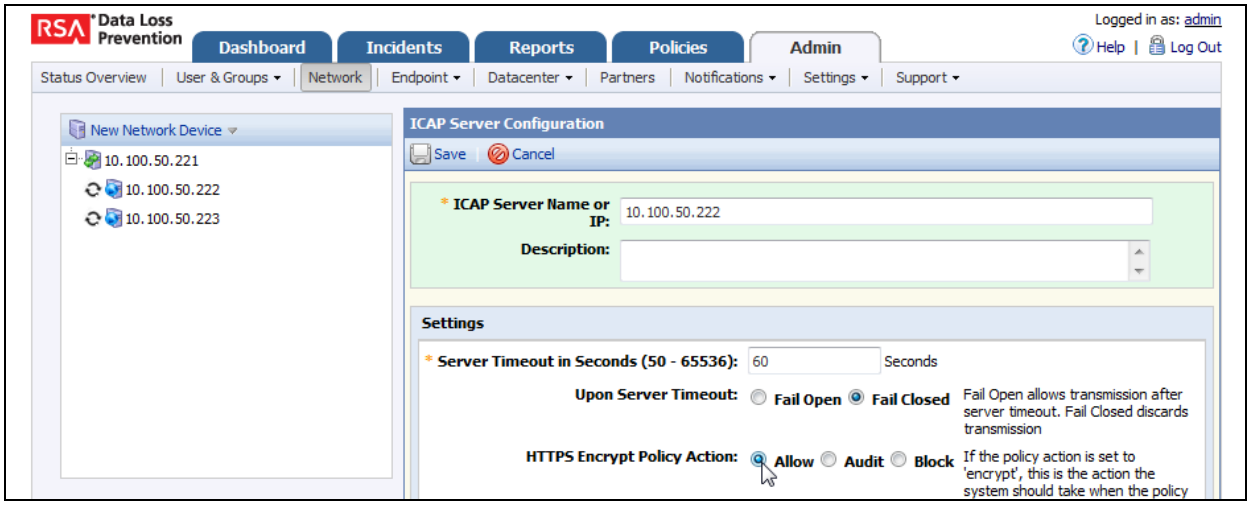
Configuring HTTPS Encrypt Policy Actions

You may also optionally configure the default behavior of the ICAP Server if the **Encrypt & Audit** policy is being used in conjunction with HTTPS traffic. To change this, perform the following steps:

1. Select the **ICAP Server** device on the **Admin** tab.



2. Select your ICAP Server in the left-hand pane. Click **Edit** and select the appropriate HTTPS policy action. Consult the Enterprise Manager online help for more information on the behavior of each option presented.



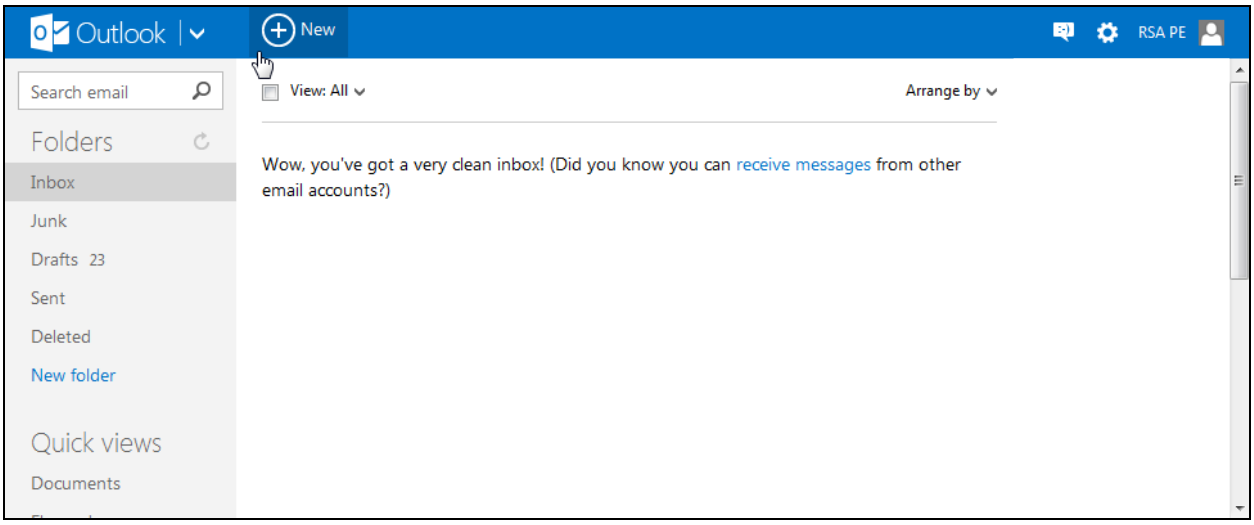
3. Click **Save** to preserve your changes.

End User Experience

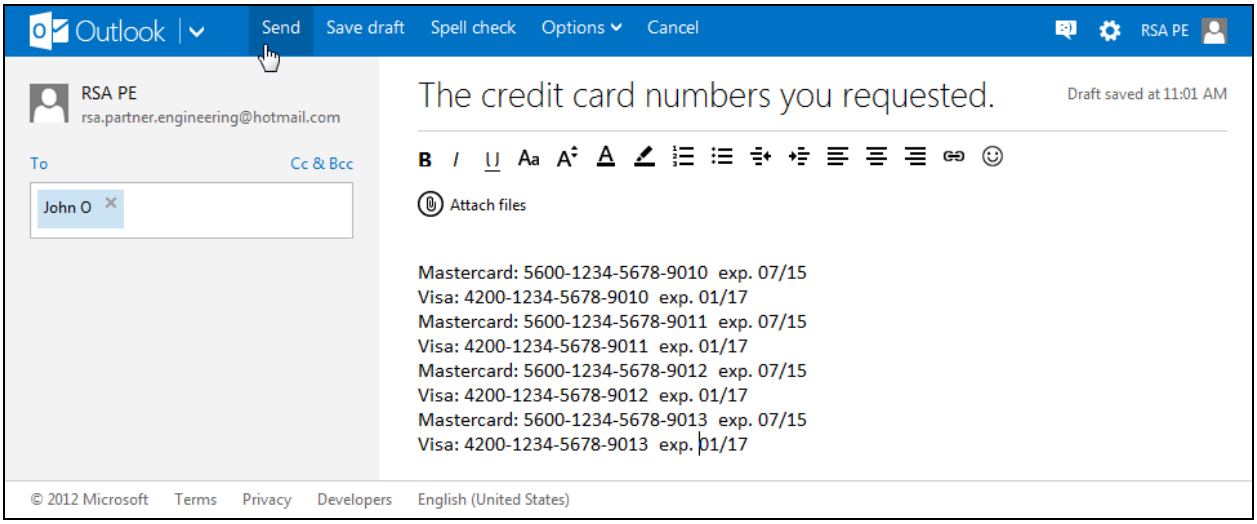
Depending on the way you have configured your policies, a user may or may not be notified when a DLP violation occurs. The following screenshots demonstrate what a user would see when attempting to send an email with sensitive content via Outlook (Hotmail).

> **Note: The screenshots provided below are for example purposes only. Individual Webmail clients may behave slightly differently in the way they process blocked messages or attachments.**

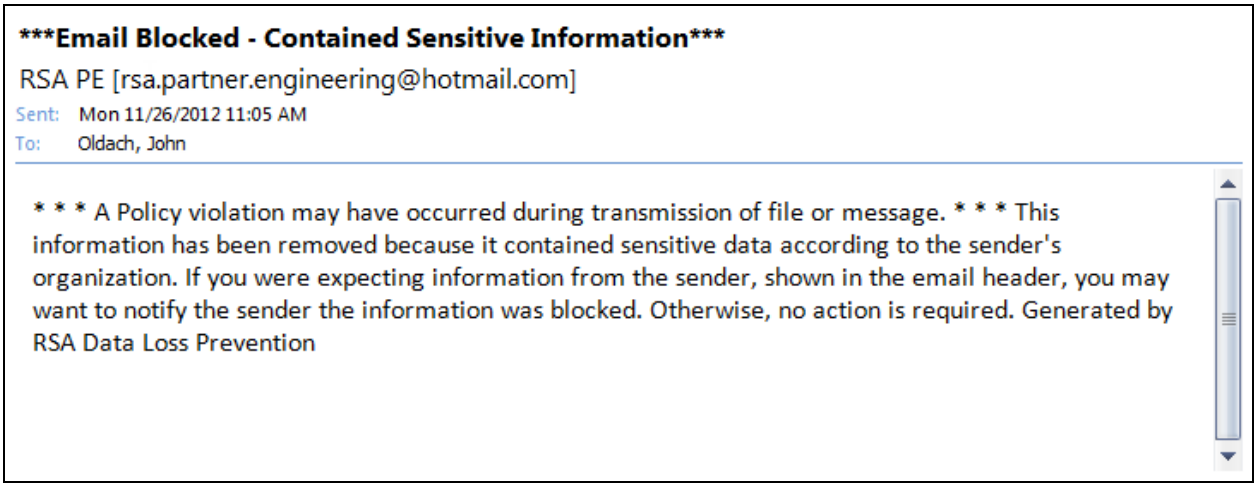
1. The user browses to Outlook (Hotmail) and composes a new message.



2. The user enters credit card data in the body of the email which violates corporate policy.



3. Upon sending the email, the **Block** policy is invoked but transparent to the sender. When the recipient receives the email, the original email will be replaced by the DLP policy violation message.



Certification Checklist for RSA Data Loss Prevention Suite

Date Tested: December 5th, 2012

Certification Environment		
Product Name	**Version Information**	**Operating System**
RSA DLP Enterprise Manager	9.5.1000.10226	Microsoft Windows Server 2003
RSA DLP Network ICAP Server	9.5.1000.10109	Appliance
Cisco IronPort S160	7.5.0-833	AsyncOS

Protocol – HTTP (GET)

Policy	Content	Result
Allow	URL encoded with sensitive content	N/A**
Audit	URL encoded with sensitive content	N/A**
Block	URL encoded with sensitive content	N/A**

** See Known Issues Section

Protocol – HTTP (POST)

Policy	Content	Result
Allow	Binary file with sensitive content	✓
Allow	Plaintext file with sensitive content	✓
Allow	Plaintext form with sensitive content	✓
Allow	URL encoded with sensitive content	✓
Allow	Multipart POST with sensitive content	✓
Audit	Binary file with sensitive content	✓
Audit	Plaintext file with sensitive content	✓
Audit	Plaintext form with sensitive content	✓
Audit	URL encoded with sensitive content	✓
Audit	Multipart POST with sensitive content	✓
Block	Binary file with sensitive content	✓
Block	Plaintext file with sensitive content	✓
Block	Plaintext form with sensitive content	✓
Block	URL encoded with sensitive content	✓
Block	Multipart POST with sensitive content	✓

Protocol – HTTP (PUT)

Policy	Content	Result
Allow	Plaintext form with sensitive content	✓
Audit	Plaintext form with sensitive content	✓
Block	Plaintext form with sensitive content	✓

Protocol – HTTPS (GET)		
Policy	**Content**	**Result**
Allow	URL encoded with sensitive content	N/A**
Audit	URL encoded with sensitive content	N/A**
Block	URL encoded with sensitive content	N/A**

****See Known Issues Section**

Protocol – HTTPS (POST)		
Policy	**Content**	**Result**
Allow	Binary file with sensitive content	✓
Allow	Plaintext file with sensitive content	✓
Allow	Plaintext form with sensitive content	✓
Allow	URL encoded with sensitive content	✓
Allow	Multipart POST with sensitive content	✓
Audit	Binary file with sensitive content	✓
Audit	Plaintext file with sensitive content	✓
Audit	Plaintext form with sensitive content	✓
Audit	URL encoded with sensitive content	✓
Audit	Multipart POST with sensitive content	✓
Block	Binary file with sensitive content	✓
Block	Plaintext file with sensitive content	✓
Block	Plaintext form with sensitive content	✓
Block	URL encoded with sensitive content	✓
Block	Multipart POST with sensitive content	✓
Encrypt	ICAP Settings -- HTTPS encrypt policy action “Allow”	✓
Encrypt	ICAP Settings -- HTTPS encrypt policy action “Audit”	✓
Encrypt	ICAP Settings -- HTTPS encrypt policy action “Block”	✓

Protocol – HTTPS (PUT)		
Policy	**Content**	**Result**
Allow	Plaintext form with sensitive content	✓
Audit	Plaintext form with sensitive content	✓
Block	Plaintext form with sensitive content	✓

Protocol – FTP (Passive Mode)

Policy	Content	Result
Allow	Binary file with sensitive content	✓
Allow	Plaintext file with sensitive content	✓
Audit	Binary file with sensitive content	✓
Audit	Plaintext file with sensitive content	✓
Block	Binary file with sensitive content	✓
Block	Plaintext file with sensitive content	✓

Protocol – FTP (Active Mode)

Policy	Content	Result
Allow	Binary file with sensitive content	✓
Allow	Plaintext file with sensitive content	✓
Audit	Binary file with sensitive content	✓
Audit	Plaintext file with sensitive content	✓
Block	Binary file with sensitive content	✓
Block	Plaintext file with sensitive content	✓

Webmail – Yahoo! Mail

Policy	Content	Result
Allow	Submit sensitive content as email attachment	✓
Allow	Submit sensitive content in email body	✓
Allow	Submit sensitive content in email subject line	✓
Audit	Submit sensitive content as email attachment	✓
Audit	Submit sensitive content in email body	✓
Audit	Submit sensitive content in email subject line	✓
Block	Submit sensitive content as email attachment	✓
Block	Submit sensitive content in email body	✓
Block	Submit sensitive content in email subject line	✓

Webmail – Microsoft Outlook (Hotmail)

Policy	Content	Result
Allow	Submit sensitive content as email attachment	✓
Allow	Submit sensitive content in email body	✓
Allow	Submit sensitive content in email subject line	✓
Audit	Submit sensitive content as email attachment	✓
Audit	Submit sensitive content in email body	✓
Audit	Submit sensitive content in email subject line	✓
Block	Submit sensitive content as email attachment	✓
Block	Submit sensitive content in email body	✓
Block	Submit sensitive content in email subject line	✓

Webmail – Gmail

Policy	Content	Result
Allow	Submit sensitive content as email attachment	✓
Allow	Submit sensitive content in email body	✓
Allow	Submit sensitive content in email subject line	✓
Audit	Submit sensitive content as email attachment	✓
Audit	Submit sensitive content in email body	✓
Audit	Submit sensitive content in email subject line	✓
Block	Submit sensitive content as email attachment	✓
Block	Submit sensitive content in email body	✓
Block	Submit sensitive content in email subject line	✓

JJO

✓ = Pass ✗ = Fail N/A = Non-Available Function

Known Issues

- Cisco IronPort has a minimum request body size, below which upload requests are not scanned by the external DLP server. The minimum size for this is 4K. For more information on this, please consult the *Bypassing Upload Requests Below a Minimum Size* section of the Cisco IronPort online help or user guide.
- For the reason stated above, it is not feasible to have an HTTP GET that is greater than 1K in size that is inspected by RSA DLP.