



CISCO EMAIL SECURITY APPLIANCE

DATA LOSS PREVENTION

September 2015
Version 1.0

David Newell
Cisco Sales Engineer

THE MOST RECENT VERSION OF THIS DOCUMENT CAN BE FOUND HERE:

<https://cisco.com/go/emailsecurity-customer>

Data Loss Prevention - Best Practices

PURPOSE OF THIS DOCUMENT	3
OVERVIEW OF STEPS	3
STEP 1: ENABLING DLP	3
STEP 2: CREATING DLP MESSAGE ACTIONS	4
STEP 3: CREATING DLP POLICIES	9
STEP 4: APPLYING DLP POLICIES TO OUTGOING MAIL POLICY	11
NEXT STEPS AND SUMMARY	11

PURPOSE OF THIS DOCUMENT

This document will step you through a Cisco ESA Data Loss Prevention (DLP) deployment, suitable for POVs and testing.

OVERVIEW OF STEPS

This document will provide the steps necessary for you to implement some Best Practices around Cisco's DLP solution for the Email Security Appliance. The steps are:

1. Enabling DLP
2. Creating DLP Message Actions
3. Creating DLP policies
4. Applying DLP Policies to Outgoing Email Policy

STEP 1: ENABLING DLP

On the ESA appliance, Navigate to: *Security Services>RSA Email DLP*

Data Loss Prevention Settings

RSA Email Data Loss Prevention Settings	
Data Loss Prevention:	Enabled
Matched Content Logging:	Enabled
Automatic Updates:	Enabled

[Edit Settings...](#)

Enable Data Loss Prevention, Matched Content Logging and Automatic Updates.

Updates for the RSA DLP engine and predefined content matching classifiers on your appliance are independent of updates for other security services. The 3-5 minute regular Talos/SIO signature updates is different and does not include updating RSA DLP policies and dictionaries. RSA updates must be enabled here.

When "Matched Content Logging" is Enabled, it allows Message Tracking to show the content of the email that caused the violation. Here is an example of Message Tracking showing the email content that caused the DLP violation. In this way an admin can know exactly which data triggered a specific DLP policy.

Data Loss Prevention - Best Practices

Message Details	
Envelope and Header Summary	
Received Time:	20 Aug 2009 00:53:37 (GMT)
MID:	153
Message Size:	4.88 (KB)
Subject:	example message
Envelope Sender:	user@example.com
Envelope Recipients:	example@recipient.com
Message ID Header:	<40ee3344p@example.com>
SMTP Auth User ID:	N/A
Sending Host Summary	
Reverse DNS Hostname:	example.com (verified)
IP Address:	127.0.0.1
SBRs Score:	not enabled

Message Details	
Summary	DLP Matched Content
	MESSAGE ID "153" MATCHED DLP POLICY: custom_policy
Violation Severity:	MEDIUM (Risk Factor: 50)
attachment.xls:	Credit Cards <ul style="list-style-type: none">• Carolyn Anderson 4886, Lynn Avenue Eau Claire WI 54701 US 715-491-2806 MasterCard 5337767638591724 938 4/2008• Albert Bearer 1141, Johnny Lane Milwaukee WI 53202 US 414-283-3835 MasterCard 5350705902658342 849 4/2010• Jordan Lape 2551, Browning Lane Madison WI 53703 US 608-227-8939 MasterCard 5386923042900742 513 12/2009• Barbara Scott 1678, Abner Road Edgar WI 54426 US 715-352-9535 MasterCard 5404108958654883 110 8/2009

When you click Submit it will start the DLP Assessment Wizard. Click Cancel on this Wizard and we will manually configure the DLP settings.

STEP 2: CREATING DLP MESSAGE ACTIONS


Create DLP Quarantines

If you'd like to keep a copy of messages violating DLP policies you can create individual Policy quarantines for each type of policy violation. This is especially useful when running a 'transparent' POV, where Outbound messages violating DLP policies are logged and delivered but no action is taken on the messages.

On the SMA, navigate to: *Email Tab > Message Quarantine > PVO Quarantines*

This is what the Quarantines table should look like before we start. Note that if you don't have an SMA deployed, the PVO Quarantines are located on the individual ESA at: *Monitor > Policy, Virus and Outbreak*

Data Loss Prevention - Best Practices

Quarantines						
Add Policy Quarantine...		Search Across Quarantines				
Quarantine Name	Type	Messages	Default Action	Last Message Quarantined On	Size	Delete
File Analysis	Advanced Malware Protection	0	Retain 1 hour then Release	--	0	
Outbreak [Manage by Rule Summary]	Outbreak	0	Retention Varies Action: Release	--	0	
Policy	Centralized Policy	0	Retain 10 days then Delete	--	0	
Unclassified	Unclassified	0	Retain 30 days then Release	--	0	
Virus	Antivirus	0	Retain 30 days then Delete	--	0	

Available space for Policy, Virus & Outbreak quarantines is 33G.

All quarantines are default.

Click the “Add Policy Quarantine” button and Create the below Quarantines to be used by the DLP policies.

PVO Quarantines - used by DLP Policies	
HIPAA: Name: DLP HIPAA Retention Period: 14 Days Default Action: Delete Free up space: Enable	SSN: Name: DLP SSN Retention Period: 14 Days DefaultAction: Delete Free up space: Enable
PCI : Name: DLP PCI Retention Period: 14 Days DefaultAction: Delete Free up space: Enable	US Drivers License: Name: DLP US Drivers License Retention Period: 14 Days DefaultAction: Delete Free up space: Enable
Sarbanes-Oxley: Name: DLP SOX Retention Period: 14 Days DefaultAction: Delete Free up space: Enable	

About DLP Message Actions

DLP message actions describe what actions that the ESA will take when it detects a DLP violation in an outgoing email. You can specify primary and secondary DLP Actions and different actions can be assigned for different violation types and severities.

Primary actions include:

- Deliver
- Drop
- Quarantine

For a “transparent POV” where DLP violations are logged and reported but the messages are not stopped/quarantined or encrypted, the Deliver action is most often used.

Secondary actions include:

- Sending a copy to any custom quarantine or the ‘Policy’ quarantine.
- **Encrypt the message.** The appliance only encrypts the message body. It does not encrypt the message headers.
- Altering the Subject header.
- Adding disclaimer text/html to the message.
- Sending the message to an alternate destination mailhost.
- Sending bcc copies of the message.
- Sending DLP violation notification to sender and/or other contacts.

These actions are not mutually exclusive — you can combine some of them within different DLP policies for various processing needs for different user groups.

We are going to implement the following DLP Actions:

Quarantine:

When we configured our custom policy quarantines earlier we did so with the intention of them being used by the DLP Actions:

- DLP HIPAA
- DLP PCI
- DLP SOX
- DLP SSN Encrypt:

Encrypt:

These actions assume that Encryption is licensed and configured on the ESA and three profiles have been created for High, Medium and Low security.

- EncryptHigh
- EncryptMedium
- EncryptLow

Create the DLP Message Actions

Go to *Mail Policies > DLP Message Customizations* .

Click the “Add Message Action” button and add the following DLP Actions.

DLP Message Actions
Name: EncryptHigh Deliver and Copy to DLP HIPAA MessageAction: Deliver Enable Encryption: Enabled (Checked) Encryption Rule: Always use message encryption Encryption Profile: EncryptHigh Send a copy of message to: DLP HIPAA Advanced: No setting in Advanced for this Action
Name: EncryptMedium Deliver and Copy to DLP HIPAA MessageAction: Deliver Enable Encryption: Enabled (Checked) Encryption Rule: Always use message encryption Encryption Profile: EncryptMedium Send a copy of message to: DLP HIPAA Advanced: No setting in Advanced for this Action
Name: EncryptLow Deliver and Copy to DLP HIPAA MessageAction: Deliver Enable Encryption: Enabled (Checked) Encryption Rule: Always use message encryption Encryption Profile: EncryptLow Send a copy of message to: DLP HIPAA Advanced: No setting in Advanced for this Action

Name: EncryptMedium Deliver and Copy to DLP PCI

MessageAction: Deliver

Enable Encryption: Enabled (Checked)Encryption Rule: Always use message encryption

Encryption Profile: EncryptMedium

Send a copy of message to: DLP PCI

Advanced: No setting in Advanced for this Action

Name: EncryptMedium Deliver and Copy to DLP SOX

Message Action: Deliver

Enable Encryption: Enabled (Checked)Encryption Rule: Always use message encryption

Encryption Profile: EncryptMedium

Send a copy of message to: DLP SOX

Advanced: No setting in Advanced for this Action

Name: Copy to DLP HIPAA

MessageAction: Deliver

Enable Encryption: Disabled (Not Checked)

Send a copy of message to: DLP HIPAA

Advanced: No setting in Advanced for this Action

Name: Copy to DLP PCI

Message Action: Deliver

Enable Encryption: Disabled (Not Checked)

Send a copy of message to: DLP PCI

Advanced: No setting in Advanced for this Action

Name: Copy to DLP SOX

Message Action: Deliver

Enable Encryption: Disabled (Not Checked)

Send a copy of message to: DLP SOX

Advanced: No setting in Advanced for this Action

Name: Copy to DLP SSN

Message Action: Deliver

Enable Encryption: Disabled (Not Checked)

Send a copy of message to: DLP SSN

Advanced: No setting in Advanced for this Action

Commit the changes.

STEP 3: CREATE DLP POLICIES

A DLP policy includes:

- A set of conditions that determine whether an outgoing message contains sensitive data
- The actions to be taken when a message contains such data.

Navigate to:

Mail Policies > DLP Policy Manager

Click ‘Add DLP Policy’

Open the “Regulatory Compliance” disclosure triangle.

Add DLP Policy from Templates	
Display Settings: Expand All Categories Display Policy Descriptions	
▽ Regulatory Compliance	
Add	FERPA (Family Educational Rights and Privacy Act) <i>Customization recommended.</i>
Add	GLBA (Gramm-Leach Bliley Act) <i>Customization recommended.</i>
Add	HIPAA and HITECH <i>Customization recommended.</i>
Add	HIPAA and HITECH Low Threshold <i>Customization recommended.</i>
Add	PCI-DSS (Payment Card Industry Data Security Standard)
Add	PIPEDA (Personal Information Protection and Electronic Documents Act)
Add	Puerto Rico DACO 7207, 7336 and 7376 <i>Customization recommended.</i>
Add	SOX (Sarbanes-Oxley)
▷ US State Regulatory Compliance	
▷ Acceptable Use	
▷ Privacy Protection	
▷ Intellectual Property Protection	
▷ Company Confidential	
▷ Custom Policy	

For the “Low Severity Incidents” try using the “Copy to <quarantine name>” instead of Encrypt Deliver and Copy to Quarantine. This allows you to monitor the Quarantine for a week to check for false-positives on those messages that barely breached the Severity scale.

HIPAA Policy: Click the “Add” button to the left of “HIPAA and HIGHTECH”

Name: HIPAA and HITECH Severity Settings:

Critical Severity Incident: EncryptHigh Deliver and Copy to DLP HIPAA

High Severity Incident: Inherit Action from Critical Severity Incident

Medium Severity Incident: EncryptMedium Deliver and Copy to DLP HIPAA

Low Severity Incident: Copy to DLP HIPAA

PCI Policy: Click the “Add” button to the left of “PCI-DSS”

Name: PCI-DSS (Payment Card Industry Data Security Standard) Severity Settings:

Critical Severity Incident: EncryptMedium Deliver and Copy to DLP PCI

High Severity Incident: Inherit Action from Critical Severity Incident

Medium Severity Incident: Inherit Action from High Severity Incident

Low Severity Incident: Copy to DLP PCI

SOX Policy: Click the “Add” button to the left of “SOX”

Name: SOX (Sarbanes-Oxley) Severity Settings:

Critical Severity Incident: EncryptMedium Deliver and Copy to DLP SOX

High Severity Incident: Inherit Action from Critical Severity Incident

Medium Severity Incident: Inherit Action from High Severity Incident

Low Severity Incident: Copy to DLP SOX

SSN Policy: Close the Regulatory disclosure triangle and open the “Privacy Protection” disclosure triangle. Click the “Add” button to the left of “US Social Security Numbers” — the very last row.

Name: US Social Security Numbers Severity Settings:

Critical Severity Incident: Copy to DLP SSN

High Severity Incident: Inherit Action from Critical Severity Incident

Medium Severity Incident: Inherit Action from High Severity Incident

Low Severity Incident: Inherit Action from Medium Severity Incident

US Drivers License Policy: Open the “Privacy Protection” disclosure triangle. Click the “Add” button to the left of “US Drivers License Numbers” — the 5th row from the bottom.

Name: US Drivers License Numbers Severity Settings:

Critical Severity Incident: Copy to DLP US Drivers License

High Severity Incident: Inherit Action from Critical Severity Incident

Medium Severity Incident: Inherit Action from High Severity Incident

Low Severity Incident: Inherit Action from Medium Severity Incident

STEP 4: APPLY DLP POLICIES TO OUTGOING MAIL POLICY

Navigate to:

Mail Policies > Outgoing Mail Policies

Click on the control cell for DLP for the Default Policy. It will read “Disabled” if you have not enabled it yet.

Change the pulldown button from Disable DLP to Enable DLP and you will immediately be presented with all the DLP Policies you just created.

Click the “Enable All” checkbox. Submit and then Commit the changes.

CONCLUSION

The best way to test the efficacy of Cisco’s DLP solution for email is to enable it and run for a week or two in Deliver and Copy mode. You’ll have access to the DLP Incidents report which will outline any DLP hits for that time period. Using the DLP Incidents report, you can answer these kinds of questions:

- What type of sensitive data is being sent by your users?
- How severe are these DLP incidents?
- How many of these messages are being delivered?
- How many of these messages are being dropped?
- Who is sending these messages?

The DLP Incidents page is comprised of two main sections:

- The DLP incident trend graphs summarizing the top DLP incidents by severity (Low, Medium, High, Critical) and policy matches

DLP Incident Summary

[Printable \(PDF\)](#)

Time Range: 90 days
 27 Jan 2013 00:00 to 27 Apr 2013 06:12 (GMT) Data in time range: 94.01 % complete

Top Incidents by Severity

Export...

Incident Summary

Severity	%	Messages
Critical	0.0%	0
High	66.7%	276
Medium	1.7%	7
Low	31.6%	131
Total		414

Export...

Top DLP Policy Matches

Export...

- The DLP Incidents Details listing. Clicking on the blue highlighted incident numbers will launch Message Tracking for those incidents.

DLP Policy	Low	Medium	High	Critical	Total	Delivered (encrypted)	Delivered (clear)	Dropped
Restricted Files	0	0	265	0	265	0	0	0
Payment Card Industry Data Security Standard (PCI-DSS)	76	0	11	0	87	0	0	0
HIPAA (Health Insurance Portability and Accountability Act)	55	7	0	0	62	0	0	62

Columns... | Export...

In summary, we have shown the three steps necessary to prepare a Cisco Email Security Appliance for scanning outbound mail for data loss using Cisco DLP for ESA.

5. Enabling DLP
6. Creating DLP Message Actions
7. Creating DLP policies
8. Applying DLP Policies to Outgoing Email Policy

Additional detail is available in the ESA User Guide corresponding to your ESA software release. User guides are available at the following link:

<http://www.cisco.com/c/en/us/support/security/email-security-appliance/products-user-guide-list.html>