Contents

Introduction

This document describes how to test Health Insurance Portability and Accountability Act (HIPAA) Data Loss Prevention (DLP) once you have enabled DLP on your outgoing mail policy on your Cisco Email Security Appliance (ESA).

Trigger a DLP Violation to Test a HIPAA Policy

This article provides some real content, which has been modified in order to protect the people, to test against the DLP Policy on your ESA. This information is designed to trigger on the HIPAA and Health Information Technology for Economic and Clinical Health (HITECH) DLP policy and also triggers other DLP policies like Social Security Number (SSN), CA AB-1298, CA SB-1386, and so on. Use the information when you send a test email through your ESA or when you use the **trace** tool.

> **Note**: You must use a valid or commonly misused SSN in the output where bolded.

> **Note**: For the HIPAA and HITECH DLP Policy, ensure that you have configured customized identification numbers as recommended. Patient Identification Numbers (customization recommended) OR US National Provider Identifier OR US Social Security Number AND Healthcare Dictionaries. You must have this configured in order to properly trigger.

```
Procedure Notes
Progress Notes
Archie M Johnson Tue Jun 30, 2009 10:31 AM Pended
June 30, 2009
Patient Name: Gina, Lucas DOB: 01/23/1945
Telephone #: (559) 221-2345
SS#: [[[PLACE SSN HERE]]]
--------------------------------------------------------------------------------
Insurance: UHC
How was the patient referred to the office: *** ({:20})
Is a family member currently being seen by the requested physician? {YES/NO:63}
If yes, what is the family members name : ***
Previous PCP / Medical Group? ***
Physician Requested: Dr. ***
REASON:
1) Get established, no current problems: {YES/NO:63}
2) Chronic Issues: {YES/NO:63}
3) Specific Problems: {YES/NO:63}
Description of specific problem and/or chronic conditions:
{OPMED SYMPTOMS:11123} the problem started {1-10:5044} {Time Units:10300}.
```

```
Any Medications that may need a refill? {YES/NO:63}
Current medications: ***
--------------------------------------------------------------------------------
Archie M Johnson
Community Health Program Assistant Chief
Family Practice & Community Medicine
(559) 221-1234
Lucas Gina Wed Jul 8, 2009 10:37 AM Pended
ELECTIVE NEUROLOGICAL SURGERY
HISTORY & PHYSICAL
CHIEF COMPLAINT: No chief complaint on file.
HISTORY OF PRESENT ILLNESS: Mary A Xxtestfbonilla is a ***
Past Medical History
Diagnosis Date
• Other Deficiency of Cell-Mediated Immunity
Def of cell-med immunity
• Erythema Multiforme
• Allergic Rhinitis, Cause Unspecified
Allergic rhinitis
• Unspecified Osteoporosis 12/8/2005
DEXA scan - 2003
• Esophageal Reflux 12/8/2005
priolosec, protonix didn't work, lost weight
• Primary Hypercoagulable State
MUTATION FACTOR V LEIDEN
• Unspecified Glaucoma 1/06
• OPIOID PAIN MANAGEMENT 1/24/2007
Patient is on opioid contract - see letter 1/24/2007
• Chickenpox with Other Specified Complications 2002
```

Verify

Your results will vary, based on the message actions you have set for your DLP policy. Configure and confirm your actions for your appliance with a review from the GUI: **Mail Policies > DLP Policy Customizations > Message Actions**.

In this example, the **Default Action** is set to quarantine DLP violations to the Policy quarantine and to also modify the message subject line with prepending "[DLP VIOLATION]".

The **mail_logs** should appear similar to this when you send the previous content through as a test email:

```
Wed Jul 30 11:07:14 2014 Info: New SMTP ICID 656 interface Management (172.16.6.165)
address 172.16.6.1 reverse dns host unknown verified no
Wed Jul 30 11:07:14 2014 Info: ICID 656 RELAY SG RELAY_SG match 172.16.6.1 SBRS
not enabled
Wed Jul 30 11:07:14 2014 Info: Start MID 212 ICID 656
Wed Jul 30 11:07:14 2014 Info: MID 212 ICID 656 From: <my_user@gmail.com>
Wed Jul 30 11:07:14 2014 Info: MID 212 ICID 656 RID 0 To: <test_person@cisco.com>
Wed Jul 30 11:07:14 2014 Info: MID 212 Message-ID
'<A85EA7D1-D02B-468D-9819-692D552A7571@gmail.com>'
Wed Jul 30 11:07:14 2014 Info: MID 212 Subject 'My DLP test'
Wed Jul 30 11:07:14 2014 Info: MID 212 ready 2398 bytes from <my_user@gmail.com>
Wed Jul 30 11:07:14 2014 Info: MID 212 matched all recipients for per-recipient
policy DEFAULT in the outbound table
Wed Jul 30 11:07:16 2014 Info: MID 212 interim verdict using engine: CASE spam
negative
Wed Jul 30 11:07:16 2014 Info: MID 212 using engine: CASE spam negative
Wed Jul 30 11:07:16 2014 Info: MID 212 interim AV verdict using Sophos CLEAN
Wed Jul 30 11:07:16 2014 Info: MID 212 antivirus negative
Wed Jul 30 11:07:16 2014 Info: MID 212 Outbreak Filters: verdict negative
```

```
Wed Jul 30 11:07:16 2014 Info: MID 212 DLP violation
Wed Jul 30 11:07:16 2014 Info: MID 212 quarantined to "Policy" (DLP violation)
Wed Jul 30 11:08:16 2014 Info: ICID 656 close
```

From the **trace** tool, you should see results listed like this image when you use previous content in the message body:

Data Loss Prevention Processing	
Result:	Matches Policy: HIPAA and HITECH Violation Severity: LOW (Risk Factor: 22)
Actions:	replace-header("Subject", "[DLP VIOLATION] $subject") quarantine("Policy")

Troubleshoot

Ensure that you have selected the needed DLP Policy from **Mail Policies > DLP Policy Manager > Add DLP Policy...** in the GUI.

Review the DLP Policy as added and ensure that you have specified your content matching classifier and that your regular expression pattern is valid. Also ensure that you have the **AND match with related words or phrases** section configured. Classifiers are the detection components of the DLP engine. They can be used in combination or individually in order to identify sensitive content.

> **Note**: Predefined classifiers are uneditable.

If you do not see the DLP trigger based on the content, also review **Mail Policies >** and ensure that you have the needed DLP Policy enabled.

Related Information

- **Cisco Email Security Appliance - End-User Guides**
- **ESA FAQ: How can I debug how a message is processed by the ESA?**
- **SSA.gov: Misused Social Security Numbers**
- **Online regex tester**
- **Technical Support & Documentation - Cisco Systems**