Software

Exchange 2013 Data Loss Prevention (DLP)

Abstract

Ensuring that sensitive data does not leave an organization has always been one of the most challenging tasks for Exchange administrators. The new data loss prevention feature in Exchange 2013 and Exchange Online in Office 365 enables administrators to control the flow of sensitive information within, inbound to and outbound from the organization. This paper explains the DLP feature and explains how to get the DLP reporting you need, whether you're using Exchange Online or on-premises Exchange 2013.

Introduction

Ensuring that sensitive data does not leave an organization has always been one of the most challenging tasks for Exchange administrators. Exchange 2007 introduced transport rules, a mechanism to control the internal and external flow of messages in an Exchange organization. Administrators define rules (consisting of conditions, actions and optional exceptions) that they use to define policies, such as adding a disclaimer to outbound messages, dropping messages between users or groups of users either with or without a non-delivery report, or creating a copy of a message for auditing or archiving purposes. Additional conditions and actions were added in Exchange 2010.

In Exchange 2013 and Exchange Online in Office 365, the feature set has been extended to data loss prevention (DLP). In this paper we'll explore the DLP feature and explain how to get the DLP reporting you need, whether you're using Exchange Online or on-premises Exchange 2013.

Exchange data loss prevention (DLP)

Data loss prevention is a premium feature in both Exchange 2013 and Office 365. It is based on transport rules and consists of DLP policies—packages that contain rules consisting of conditions, actions and exceptions that you create in the Exchange Administration Center (EAC) or Exchange Management Shell cmdlets and then activate to filter email messages. Policies can be tested before they are activated and affect mail flow.

The new DLP feature can perform deep content analysis—through keyword matches, dictionary matches, regular expression evaluation, and other content examination—to detect content that violates organizational DLP policies, and can then apply an appropriate action. DLP also includes policy tips, a notification in the Outlook 2013 client that warns email users that the content of a mail message infringes on your DLP policy, before the email is sent.

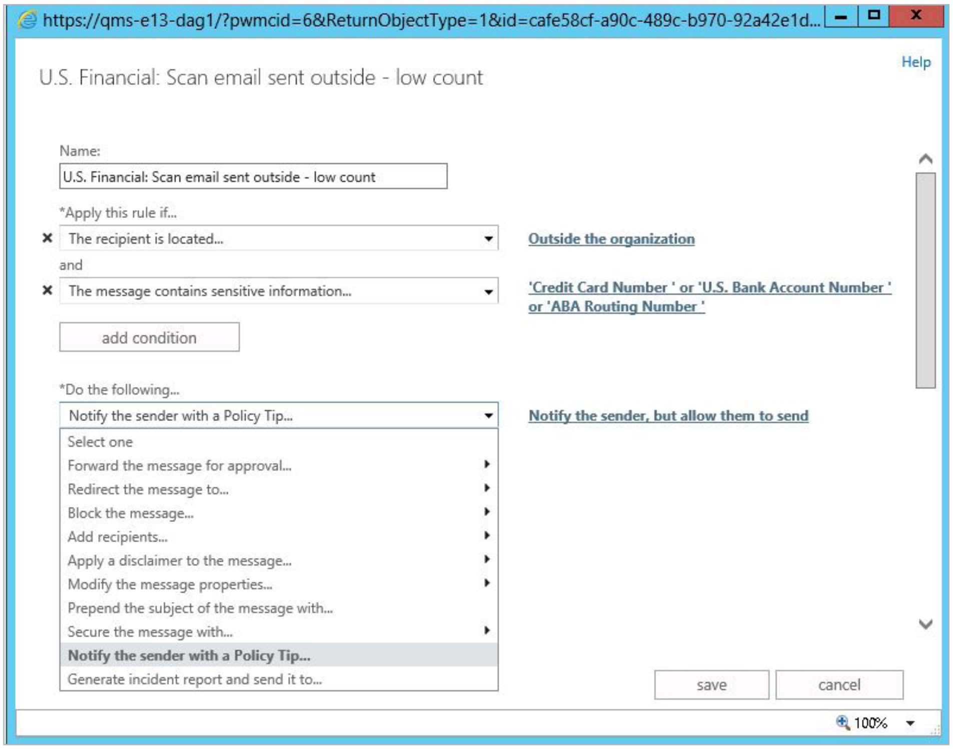
> DLP policies contain rules consisting of conditions, actions and exceptions that you create in the Exchange Administration Center or Exchange Management Shell cmdlets and then activate to filter email messages.

DLP policies

DLP policies can be created from scratch or based on a template. Pre-defined templates are provided in Exchange 2013 and Office 365 and can also be supplied by Microsoft partners. The pre-defined templates include policies covering different sensitive information types (finance, health, personally identifiable information and so on), such as:

- ABA routing number (United States)
- Australian passport number (Australia)
- Canada bank account number (Canada)
- Credit card number
- German driver's license number (Germany)
- IP address
- Spain national ID (Spain)
- U.S. Social Security number (United States)

The full list of sensitive information types can be found on Technet at http://technet.microsoft.com/en-us/library/jj150541(v=exchg.150).aspx.



https://qms-e13-dag1/?pwmcid=6&ReturnObjectType=1&id=cafe58cf-a90c-489c-b970-92a42e1d...

U.S. Financial: Scan email sent outside - low count

Name: U.S. Financial: Scan email sent outside - low count

*Apply this rule if...

The recipient is located... — Outside the organization

and

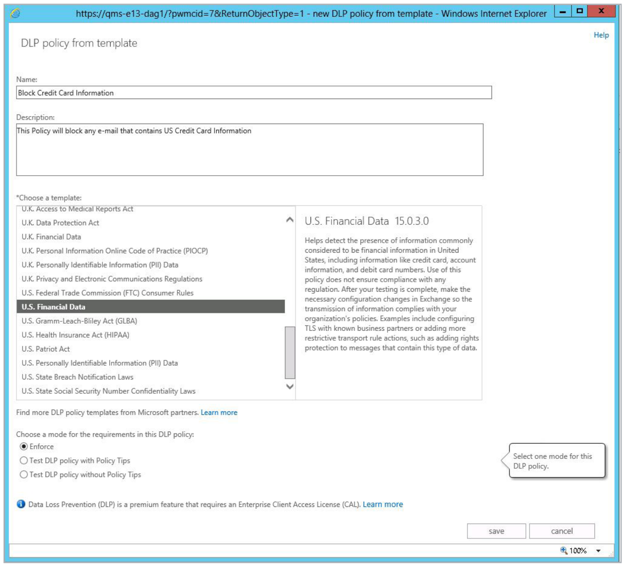
The message contains sensitive information... — 'Credit Card Number ' or 'U.S. Bank Account Number ' or 'ABA Routing Number '

*Do the following...

Notify the sender with a Policy Tip... — Notify the sender, but allow them to send

Help
add condition
Select one
Forward the message for approval...
Redirect the message to...
Block the message...
Add recipients...
Apply a disclaimer to the message...
Modify the message properties...
Prepend the subject of the message with...
Secure the message with...
Notify the sender with a Policy Tip...
Generate incident report and send it to...
save
cancel
100%

Figure 1. Conditions options for DLP rules



https://qms-e13-dag1/?pwmcid=7&ReturnObjectType=1 - new DLP policy from template - Windows Internet Explorer

Help

DLP policy from template

Name:
Block Credit Card Information

Description:
This Policy will block any e-mail that contains US Credit Card Information

*Choose a template:

- U.K. Access to Medical Reports Act
- U.K. Data Protection Act
- U.K. Financial Data
- U.K. Personal Information Online Code of Practice (PIOCP)
- U.K. Personally Identifiable Information (PII) Data
- U.K. Privacy and Electronic Communications Regulations
- U.S. Federal Trade Commission (FTC) Consumer Rules
- **U.S. Financial Data**
- U.S. Gramm-Leach-Bliley Act (GLBA)
- U.S. Health Insurance Act (HIPAA)
- U.S. Patriot Act
- U.S. Personally Identifiable Information (PII) Data
- U.S. State Breach Notification Laws
- U.S. State Social Security Number Confidentiality Laws

U.S. Financial Data 15.0.3.0

Helps detect the presence of information commonly considered to be financial information in United States, including information like credit card, account information, and debit card numbers. Use of this policy does not ensure compliance with any regulation. After your testing is complete, make the necessary configuration changes in Exchange so the transmission of information complies with your organization's policies. Examples include configuring TLS with known business partners or adding more restrictive transport rule actions, such as adding rights protection to messages that contain this type of data.

Find more DLP policy templates from Microsoft partners. Learn more

Choose a mode for the requirements in this DLP policy:
● Enforce
○ Test DLP policy with Policy Tips
○ Test DLP policy without Policy Tips

Select one mode for this DLP policy.

Data Loss Prevention (DLP) is a premium feature that requires an Enterprise Client Access License (CAL). Learn more

Figure 2. Creating a DLP policy from a template

DLP policy templates

Out-of-the-box DLP policy templates are provided as a starting point for building DLP policies that help you meet your specific regulatory and business policy needs. You can modify the templates to meet the specific needs of your organization. Out-of-the box templates include policies for:

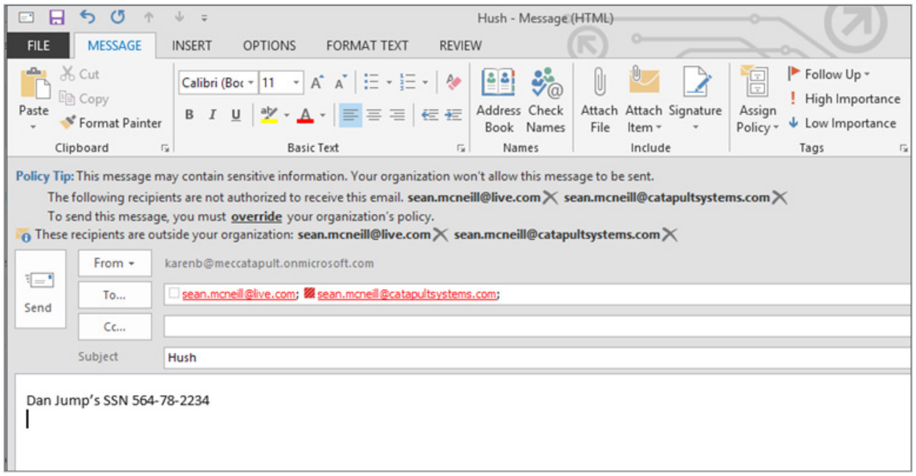
- HRIP Act (Australia)
- HIA & PHIPA (Canada)
- PCI DSS
- PIOCP (UK)
- FTC (United States)
- GLBA (United States)
- HIPAA (United States)
- Patriot Act (United States)
- Personally identifiable information (PII)

A complete list of DLP templates can be found on Technet at http://technet.microsoft.com/en-us/library/jj150530(v=exchg.150).aspx.

Policy tips

A DLP policy can contain a "Notify the sender with a policy tip" rule, which notifies users when the contents in the subject, body or attachment of a message violates your organization's

Policy tips ensure users are notified when their messages contain sensitive data that may violate your DLP policies.



Policy Tip: This message may contain sensitive information. Your organization won't allow this message to be sent.
The following recipients are not authorized to receive this email. **sean.mcneill@live.com** ✕ **sean.mcneill@catapultsystems.com** ✕
To send this message, you must **override** your organization's policy.
These recipients are outside your organization: **sean.mcneill@live.com** ✕ **sean.mcneill@catapultsystems.com** ✕

Send

From: karenb@meccatapult.onmicrosoft.com

To...: sean.mcneill@live.com; sean.mcneill@catapultsystems.com;

Cc...:

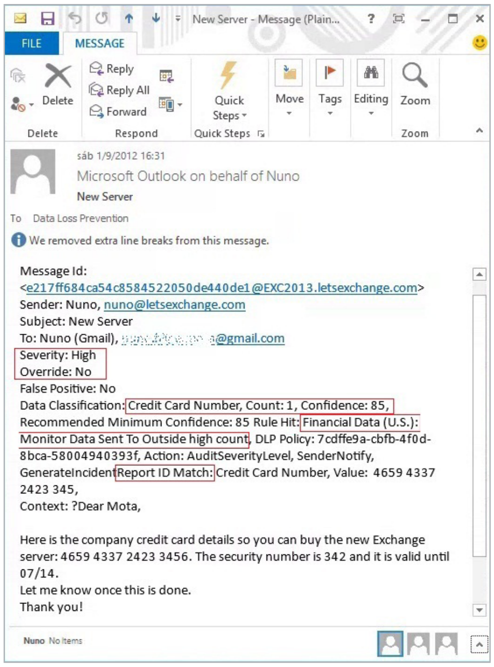
Subject: Hush

Dan Jump's SSN 564-78-2234

Figure 3. A policy tip in Outlook 2013

Share:

Natively, reporting is available only for Exchange Online. For organizations using on-premises Exchange 2013, DLP reporting is available using MessageStats Business Insights from Dell.



sáb 1/9/2012 16:31

Microsoft Outlook on behalf of Nuno

New Server

To Data Loss Prevention

We removed extra line breaks from this message.

Message Id:
<e217ff684ca54c8584522050de440de1@EXC2013.letsexchange.com>
Sender: Nuno, nuno@letsexchange.com
Subject: New Server
To: Nuno (Gmail), [redacted]a@gmail.com
Severity: High
Override: No
False Positive: No
Data Classification: Credit Card Number, Count: 1, Confidence: 85, Recommended Minimum Confidence: 85 Rule Hit: Financial Data (U.S.): Monitor Data Sent To Outside high count, DLP Policy: 7cdffe9a-cbfb-4f0d-8bca-58004940393f, Action: AuditSeverityLevel, SenderNotify, GenerateIncidentReport ID Match: Credit Card Number, Value: 4659 4337 2423 345,
Context: ?Dear Mota,

Here is the company credit card details so you can buy the new Exchange server: 4659 4337 2423 3456. The security number is 342 and it is valid until 07/14.
Let me know once this is done.
Thank you!

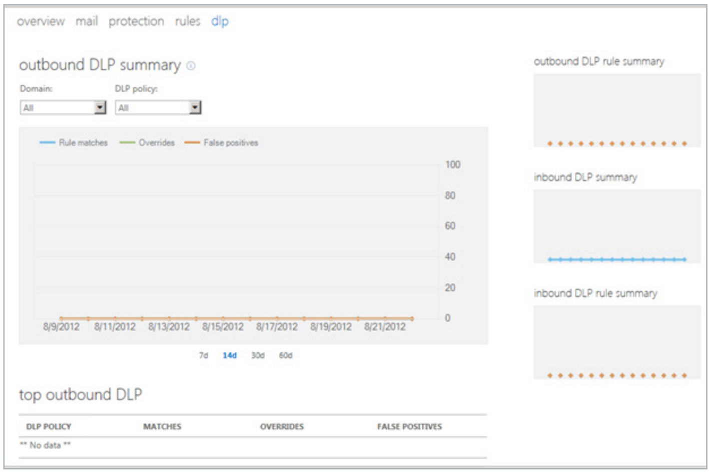
Figure 4. A DLP incident report

DLP policy. This tip can just be a notification, or it can block the message from being sent, either with or without an override option. Policy tips ensure users are notified when their messages contain sensitive data that may violate your DLP policies.

Auditing and reporting on DLP policy violations

One of the possible actions of a DLP policy is to send an incident report to up to 10 SMTP recipients (see Figure 4).

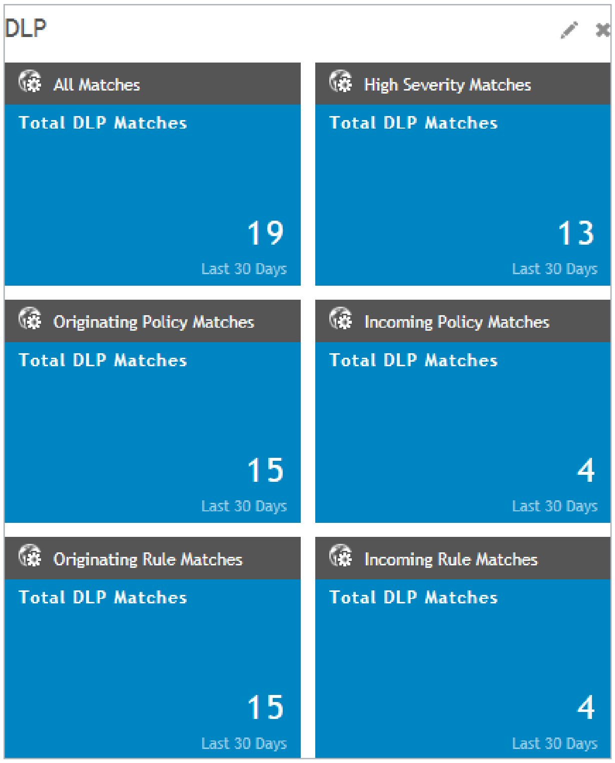
For additional auditing purposes, data related to DLP is written to the message tracking logs. Natively, reporting is available only for Exchange Online (see Figure 5). For organizations using on-premises Exchange 2013, DLP reporting is available using MessageStats Business Insights from Dell (see Figure 6 and Figure 7).



top outbound DLP

DLP POLICY	MATCHES	OVERRIDES	FALSE POSITIVES
** No data **			

Figure 5. A sample DLP report summary for Exchange Online



DLP

All Matches
Total DLP Matches
19
Last 30 Days

High Severity Matches
Total DLP Matches
13
Last 30 Days

Originating Policy Matches
Total DLP Matches
15
Last 30 Days

Incoming Policy Matches
Total DLP Matches
4
Last 30 Days

Originating Rule Matches
Total DLP Matches
15
Last 30 Days

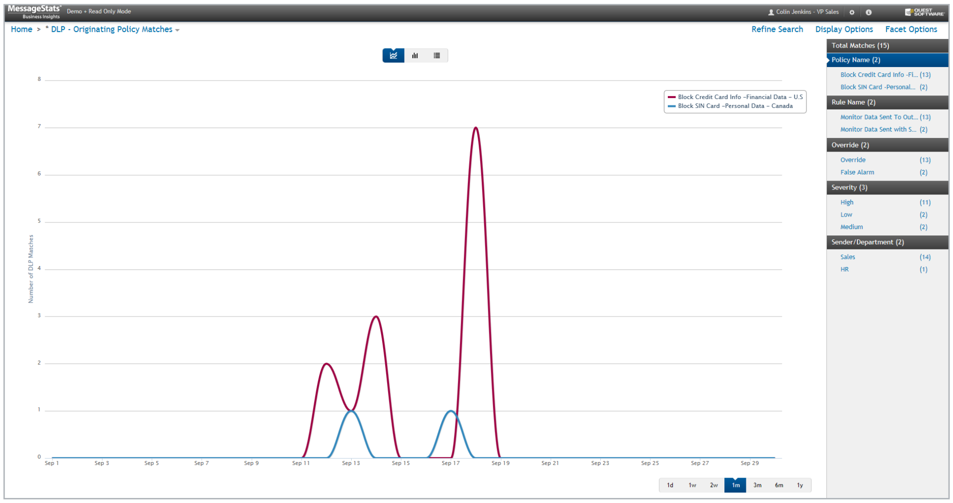
Incoming Rule Matches
Total DLP Matches
4
Last 30 Days

Figure 6. The default DLP insights in MessageStats Business Insights

MessageStats Business Insights gathers DLP data from the Exchange 2013 message tracking logs and reports on policy violations.

DLP reporting for Exchange Online
For Exchange Online, you can access DLP reports via the Admin Center. Here all your DLP policies will be listed with information on whether they are enabled and enforced or in testing, and the number of matches, false positives and overrides. Further details can be downloaded as an Excel workbook.

DLP reporting for on-premises Exchange 2013 using MessageStats Business Insights
MessageStats Business Insights gathers DLP data from the Exchange 2013 message tracking logs and reports on policy violations. The default insights (Figure 6) provide details on the rules, policies and matches in your



Total Matches (15)
Policy Name (2)
Block Credit Card Info -Fi... (13)
Block SIN Card -Personal... (2)
Rule Name (2)
Monitor Data Sent To Out... (13)
Monitor Data Sent with S... (2)
Override (2)
Override (13)
False Alarm (2)
Severity (3)
High (11)
Low (2)
Medium (2)
Sender/Department (2)
Sales (14)
HR (1)

Figure 7. The trending of the outbound DLP policy matches over the last month in MessageStats Business Insights

Share:

organization, and you can filter and group on any property of the DLP policy or rule, sender or receiver to customize the insight to best fits your requirements. For example, Figure 7 shows the trending of the outbound DLP policy matches over the last month.

Summary

The data loss prevention feature in Exchange 2013 and Exchange Online enables administrators to control the flow of sensitive information within, inbound to and outbound from the organization. DLP policies can be created from templates provided out of the box or from Microsoft partners, or created from scratch. Policy tips in Outlook 2013 can warn mail senders of potential DLP violations when they attempt to mail sensitive information.

Native DLP reporting is available only for Exchange Online. MessageStats Business Insights uses data gathered from the message tracking logs to deliver comprehensive DLP reporting for on-premise Exchange.

> The data loss prevention feature in Exchange 2013 and Exchange Online enables administrators to control the flow of sensitive information within, inbound to and outbound from the organization.

For More Information

The information in this document is provided in connection with Dell products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell products. EXCEPT AS SET FORTH IN DELL'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, DELL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

About Dell

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.dell.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software

5 Polaris Way
Aliso Viejo, CA 92656
www.dell.com
Refer to our Web site for regional and international office information.