

How to Use Content Filters to Allow Salesforce Emails

<https://campus.barracuda.com/doc/110560570/>

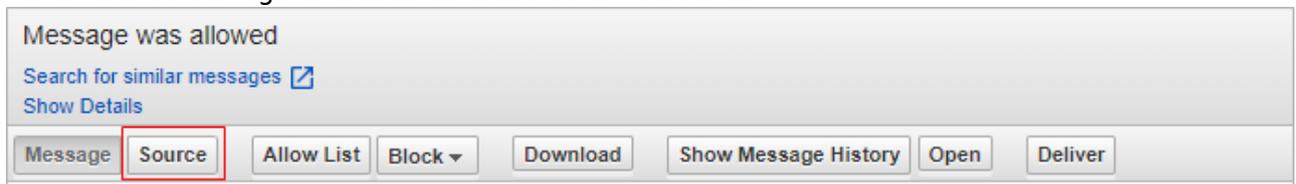
Salesforce is commonly used by organizations as their customer relationship management (CRM) system. Emails sent to your employees are generated externally, and therefore subject to inbound filtering policies within Email Gateway Defense. This could result in legitimate Salesforce emails being blocked or quarantined. Creating policies to exempt the Salesforce domain or IP would also apply to all other emails being sent from Salesforce, including unwanted emails. For that reason, it is not recommended to create such a policy.

You can avoid creating too broad a policy by using the Salesforce header that contains your account ID. For more information, see the Salesforce article

<https://help.salesforce.com/s/articleView?id=000386477&type=1>.

Locate Your Salesforce Organization ID

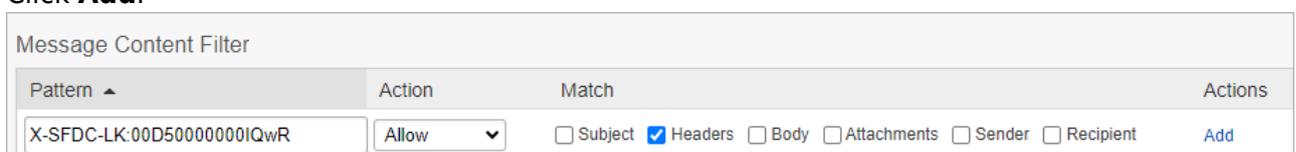
1. From your Email Gateway Defense [Message Log](#), locate an email sent from your Salesforce account.
2. Click on the message and then click the **Source** button.



3. Locate the "X-SFDC-LK" header value in the message. For example, X-SFDC-LK:00D50000000IQwR.
4. Copy the entire string as this will be used in the next step to create the content policy.

Create Message Content Filter Policy

1. In Email Gateway Defense, navigate to **Inbound Settings > Content Policies**.
2. In the **Message Content Filter** section, under **Pattern**, paste in the string you copied above.
3. Under **Action**, select **Allow**.
4. Under **Match**, click **Headers**.
5. Click **Add**.



All emails originating from this specific Salesforce account will now be exempted from all filtering.

Review your existing sender and IP policies and remove any Salesforce entries as they will no longer be needed.

Figures

1. messageLogSource.png
2. salesforceContentFilter.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.