Governance, Risk Management and Compliance (GRC) Account Role

https://campus.barracuda.com/doc/12197365/

Beyond just protection from spam and viruses, the Barracuda Email Security Gateway provides tools to protect sensitive personal, financial, medical, legal data and intellectual property transmitted via email. The **GRC** role is a tool that provides DLP (data loss prevention) for your organization by assigning one or more responsible persons with the task of viewing either message entries (Subject, From, To, etc.) or both the entries and the message contents in the outbound quarantine log. The GRC can then decide whether to deliver, reject or delete emails from this log based on the policies of the organization. **In this way, the GRC role serves to provide governance, risk management and compliance to email content.**

This account always exists on the Barracuda Email Security Gateway, but must be enabled via the **Enable GRC Account** setting on the **BASIC > Administration** page to be active. The administrator can enable or disable the GRC account at any time, but must re-create a password each time the account is re-enabled. The GRC account only has access to **Outbound Quarantine** logs, and can take the following actions with outbound quarantined messages:

- **Deliver** – GRC determines that the message is allowed, per policy, and clicks the **Deliver** button.
- **Reject** – **GRC** determines that the message is not allowed for delivery, per policy, and clicks the **Reject** button. If the **Admin** has configured it on the **ADVANCED > Bounce/NDR Settings** page, this action sends a bounce message to the sender in addition to deleting the message.
- **Delete** – **GRC** determines that the message is not allowed to be sent and clicks the **Delete** button. The message will then be removed from the Outbound Quarantine log.

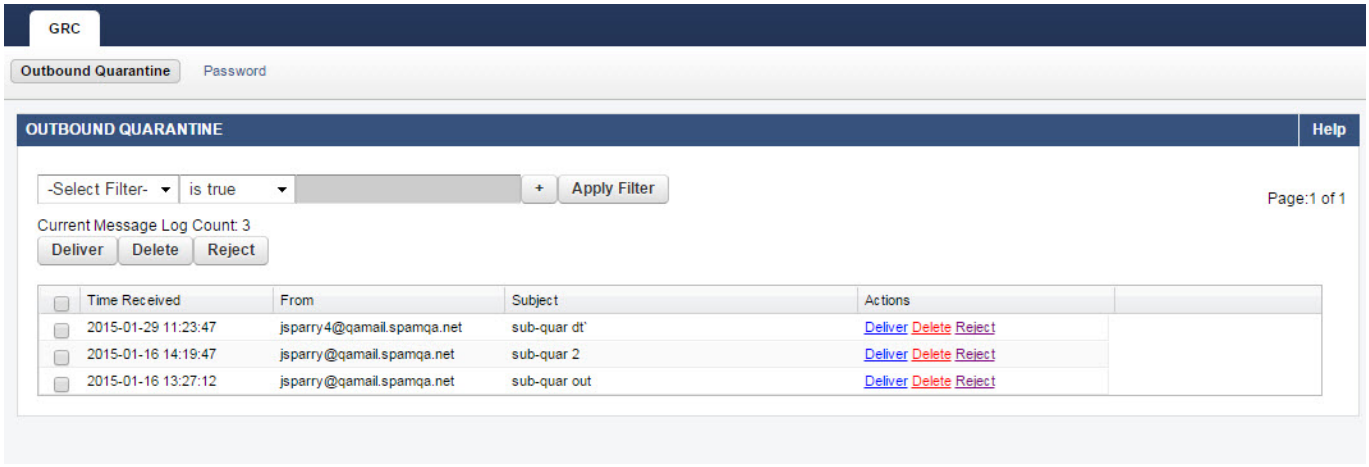
Note that you must enter a new password each time you set **Enable GRC Account** to **Yes**.

When the GRC logs in, only two pages will be visible in the web interface: the Outbound Quarantine page and a Password page as shown in Figure 1, below. From the Password page, the GRC can change the current GRC password.

Note that, to protect email privacy, the **Secondary Authorization** feature on the **BASIC > Administration** page can be configured to require a password for the GRC role to be able to see message contents when monitoring the outbound quarantine. If **Enable Secondary Authorization** is set to **Yes** and **Include Privacy for GRC Account** is also set to **Yes**, then the GRC must supply the password to see message contents in the log.

Figure 1: The GRC role can view the Outbound Quarantine and Deliver, Delete or Reject

messages.


GRC
Outbound Quarantine
Password
OUTBOUND QUARANTINE
Help
-Select Filter-
is true
+
Apply Filter
Page:1 of 1
Current Message Log Count: 3
Deliver
Delete
Reject
Time Received
From
Subject
Actions
2015-01-29 11:23:47
jsparry4@qamail.spamqa.net
sub-quar dt`
Deliver Delete Reject
2015-01-16 14:19:47
jsparry@qamail.spamqa.net
sub-quar 2
Deliver Delete Reject
2015-01-16 13:27:12
jsparry@qamail.spamqa.net
sub-quar out
Deliver Delete Reject

Figures