Integration with Other Barracuda Networks Features

https://campus.barracuda.com/doc/85494108/

Both Automatic Remediation and Incident Response integrate seamlessly with other Barracuda Networks features, including:

- Email Gateway Defense
- Impersonation Protection
- DNS Filtering (part of Barracuda Cloud Security)

Shared Account
To fully enable integration, you must use a common account for Incident Response and other Barracuda Networks features. When you initially sign up for Incident Response, be sure to select the same account that you are using for your other Barracuda Networks features. If your user is associated with more than one Barracuda Networks account, these accounts are displayed in a menu on the upper right corner of the Incident Response screen where you can choose the correct account.

Email Gateway Defense

There are multiple points of integration with Email Gateway Defense. For more information, refer to Email Gateway Defense.

Important. To take advantage of these integration points, you must make the configurations in Email Gateway Defense, at the end of this section.

Reporting Suspicious Emails

There are two methods by which users and administrators can send suspicious messages to Incident Response:

- In the Email Gateway Defense Message Log, you can mark an email as incorrectly delivered.
- In the Outlook plugin, you can report an email as suspicious.

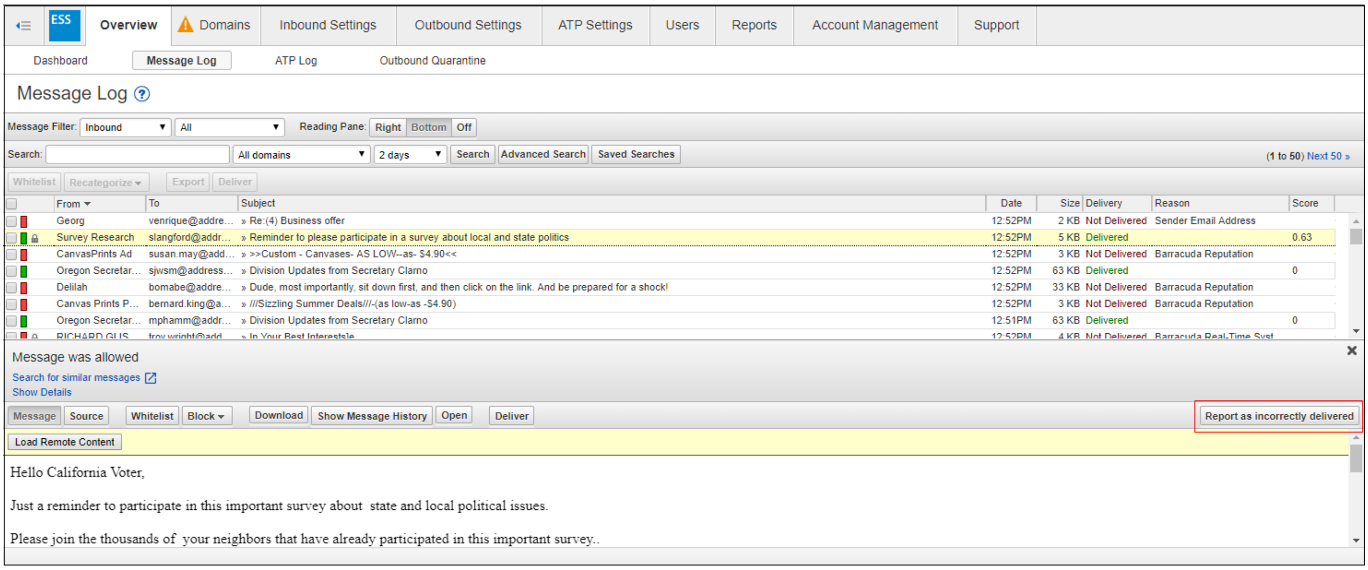
This information is displayed in the User-Reported Emails page and is described in User-Reported Emails.

Reporting a Message as Incorrectly Delivered

In the Message Log

Administrators reviewing message logs within Email Gateway Defense might notice that there is suspicious email. Messages marked as Incorrectly Delivered are reported both to Barracuda Central and to Incident Response, where they can be investigated.

To report email as incorrectly delivered, select a message in the Message Log and click **Report as Incorrectly Delivered** above the message preview.



Message Filter: Inbound ▼ All ▼ Reading Pane: Bottom

Search: All domains ▼ 2 days ▼ (1 to 50) Next 50 »

☐		From	To	Subject	Date	Size	Delivery	Reason	Score
☐	🟥	Georg	venrique@addre...	» Re:(4) Business offer	12:52PM	2 KB	Not Delivered	Sender Email Address	
☐	🟩	Survey Research	slangford@addr...	» Reminder to please participate in a survey about local and state politics	12:52PM	5 KB	Delivered		0.63
☐	🟥	CanvasPrints Ad	susan.may@add...	» >>Custom - Canvases- AS LOW--as- $4.90<<	12:52PM	3 KB	Not Delivered	Barracuda Reputation	
☐	🟩	Oregon Secretar...	sjwsm@address...	» Division Updates from Secretary Clarno	12:52PM	63 KB	Delivered		0
☐	🟥	Delilah	bomabe@addre...	» Dude, most importantly, sit down first, and then click on the link. And be prepared for a shock!	12:52PM	33 KB	Not Delivered	Barracuda Reputation	
☐	🟥	Canvas Prints P...	bernard.king@a...	» ///Sizzling Summer Deals///-(as low-as -$4.90)	12:52PM	3 KB	Not Delivered	Barracuda Reputation	
☐	🟩	Oregon Secretar...	mphamm@addr...	» Division Updates from Secretary Clarno	12:51PM	63 KB	Delivered		0
☐	🟥	RICHARD GUS	troy.wright@add	» In Your Best Interests!e	12:52PM	4 KB	Not Delivered	Barracuda Real-Time Syst	

Message was allowed

Hello California Voter,

Just a reminder to participate in this important survey about state and local political issues.

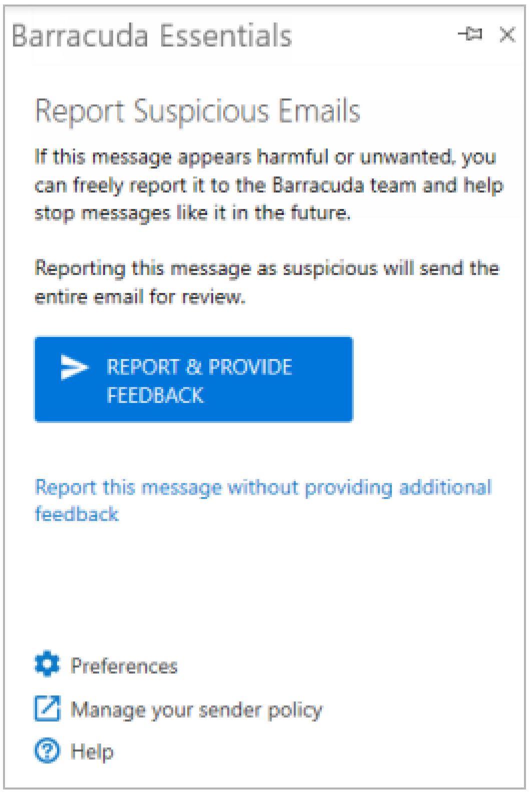
Please join the thousands of your neighbors that have already participated in this important survey..

For more information, refer to Understanding the Message Log in the Email Gateway Defense documentation.

Reporting a Message as Suspicious

Using the Reporting Button in the Outlook Plugin

Within the Barracuda Outlook Add-In, users can report suspicious emails, as shown below. This allows end users to be active participants in reporting phishing and spear phishing emails. These reports go to Barracuda Central and Incident Response. Administrators of Incident Response can investigate these end-user reported emails, create incidents, and take corrective action.



Barracuda Essentials

Report Suspicious Emails

If this message appears harmful or unwanted, you can freely report it to the Barracuda team and help stop messages like it in the future.

Reporting this message as suspicious will send the entire email for review.

REPORT & PROVIDE FEEDBACK
Report this message without providing additional feedback
Preferences
Manage your sender policy
Help

For more information, refer to Barracuda Outlook Add-In User Guide.

Finding Similar Suspicious Messages

If you find a questionable email in the Email Gateway Defense message log, you can move seamlessly from Email Gateway Defense to Incident Response to investigate it.

To find messages similar to the questionable email:

1. Log into Email Gateway Defense as an administrator.
2. In the Message Log, find the questionable email and click it to view its details.
3. Click **Search** for similar messages. The Incident Response wizard opens in a new browser tab.
4. Continue with the wizard, as described in Creating an Incident. Note that the fields in the wizard are pre-populated with the information from the email in the message log.

For more information, refer to Understanding the Message Log in the Email Gateway Defense documentation.

Creating Sender Policies

As a remediation action, you can choose to quarantine or block future emails *from one or more specific senders or from an entire domain*. This action creates a policy in Email Gateway Defense, marked as originating from Incident Response.

This remediation action is described as part of the wizard instructions in Creating an Incident.

Users Involved / Link Protection

The Link Protection feature in Email Gateway Defense is required for the functionality of the Users Involved feature. When viewing an incident, click the **Users** tab to see the users that might be affected by the incident.

Ensure that the Link Protection feature is turned ON for the appropriate accounts and domains.

Configuring Email Gateway Defense for Integration

The following settings are required if you are using Incident Response with Email Gateway Defense to take advantage of the functionality described above.

Verified Domains

Verifying domains is essential for mail to flow through Email Gateway Defense and, in turn, for Incident Response to work with the emails. As described in Understanding the Domains Page, each of the domains where you want to filter email must be verified by Email Gateway Defense for proof of ownership; Email Gateway Defense does not process email for a domain until the verification process is complete. See Understanding the Domains Page and the deployment process for your specific platform for more details.

Link Protection Feature

As described above, the Link Protection feature in Email Gateway Defense is required for the functionality of the Users Involved feature.

Ensure that the Link Protection feature is turned ON for the appropriate accounts and domains.

If Link Protection is turned OFF when a suspicious email is received, users that are potentially affected by that incident might not be listed as Users Involved and might not receive the proper remediation and attention.

Link Protection must be turned ON when emails are received to provide complete results for Users Involved for a specific incident. Turning Link Protect ON after a suspicious email has already been received will not change the Users Involved results for an incident involving that email.

Web Traffic Filtering (part of Barracuda CloudGen Access)

Blocking Web Traffic

As a remediation action, you can choose to block traffic *from an entire domain*. This action automatically creates a policy in **Web Security** (part of Barracuda CloudGen Access), marked as originating from Incident Response.

This remediation action is described as part of the wizard instructions in Creating an Incident.

After you configure Web Security within Barracuda CloudGen Access, it will also shield your organization from emails sent from entire domains or categories of domains, resulting in your having to create fewer incidents. For more information, see Incident Response and Creating Policies With Barracuda CloudGen Access, part of the Barracuda CloudGen Access documentation.

Impersonation Protection

Impersonation Protection calls Incident Response for the following activity:

Searching for Similar Issues

When viewing the details of an attack, you can click **Search for Similar Issues** to find issues similar to the attack you are currently viewing.

Security Awareness Training

Incident Response can create a group of users involved in an incident and send it to Barracuda Security Awareness Training (SAT). SAT can use this list to:

- Train users to recognize malicious emails.
- Provide follow up testing.
- Analyze results with advanced metrics and reporting.

Figures