



# CS BBLS – EVEREST ALERTS

April 19, 2024

# Agenda

- Everest Alerts: Definition & Functionality
- Top Recommended Alerts
- Alerts in Action!



# Everest Alerts

---

*Definition & Functionality*

# Definition

- Alerts are a feature in Everest that allow users to set notifications if certain events occur. These notifications can reach users while they are not in Everest - via email, text, and a few other channels. Alerts exist across almost every feature, but their primary benefit is to **keep users informed of the information that they deem important as soon as that information is available.**
- Without alerts, users would have to log in and check multiple areas of the product to find the information. With alerts, **they are notified as soon as the information is available, and they can then log into the appropriate area within Everest and start trying to fix the problem.**
- Most alerts work by setting a threshold on a certain deliverability metric. **When that threshold is exceeded, an alert goes out.** There are a few other types of alerts that do not use numbers or thresholds, like blocklists or cert updates. More details about alerts are included in the Alert Types table on the [Product Knowledge Wiki](#).
- In general, users should determine the metrics that are most important to them, figure out what thresholds/events are cause for an alert, and who the best audience is for each of those alerts. They can set an initial batch of alerts for those events and send each one to the right person/group. **Over time, as the user becomes more acquainted with deliverability and the highest leverage metrics, they can fine tune their system of alerts.**

# Functionality

- All users have access to alerts, whether they are an admin or regular user, or if they are in a child account. **Any user can create new alerts, edit existing ones, delete alerts, and turn them on or off.** Parent accounts cannot see alerts set on child accounts from the parent account. Child accounts cannot see parent account alerts. Parent accounts may go into their child accounts and set alerts for the child account users, or for the parent users.
- **Everest Professional, Enterprise, and Partner edition have access to every alert.** Everest Elements and Essentials do not have access to: Spam Traps/Phishing, Complaints (Feedback Loops), Microsoft SNDS, Signal Spam, or Certification. For Elements Plus, where users have access to SNDS and other reputation integrations, they still do NOT have access to these alerts.
- Alerts are set in the UI, on the Alerts page (which is nested under My Everest on the sidebar). From here, the user can see all existing alerts and can create new ones. **As of now, Alerts cannot be created via API, they can only be done within Everest.**
- **Generally, the customer should be managing and creating their alerts. However, they may have a CSM do this for them.** There are also several preset alerts that the user can just switch on once they get started. Oftentimes, internal Validity employees (like CSMs or AMs) will put their own email on their customer's alerts to stay notified of significant events.



# Alert Setup

---

*Top Recommended Alerts*

# Alert Frequency

---

Daily  Don't include repetitive items in alerts [?](#)

- Daily
- Weekly
- Monthly
- Every 15 minutes
- Every 30 minutes
- Every hour
- Every 2 hours
- Every 4 hours
- Every 12 hours
- Custom

Alert frequency is how often alert checks if conditions are met:

- Alert scans immediately upon creation. It then saves the time of the scan and waits for the set interval to scan again.
  - If you edit cadence, the latest check time is still used. Ex. When switching from daily to weekly, it will not run until a week has passed from the last check.
- Timestamp on the alert is when the alert scans AND when conditions are met. If you need instant awareness of, set cadence as low as possible.
- The check will drift later in time. For example, a “Daily”, set at 10 AM one day becomes 10:02 AM the next day, and 11:00 AM in 30 days.
- Most alerts can be set to only trigger once for each event.
- Different frequency options for different alerts.

# ★ Inbox Placement Alerts

- Triggers when an inbox test hits a deliverability or authentication %.
- Default shows all tests in the last 48 hours that hit threshold. This period can be changed.
- Filters can make the alert only look for certain types of emails.
- Primarily used to notify users of concerning inbox test results.
- Multiple triggers and filters can be selected together and act as AND statements.
- Most filters allow entering multiples and operate as OR statements.
- The dropdown does not distinguish between triggers and filters. The alert can fire without a trigger - it will just show every seed test that has the filter characteristic.

The screenshot shows a configuration interface for alert triggers and filters. It consists of two rows. The first row is labeled 'If my...' and has a dropdown menu set to 'Inbox %'. Below this is a comparison operator dropdown set to '<=' and a text input field containing '90'. The second row is also labeled 'If my...' and has a dropdown menu set to 'ISP'. To the right of this dropdown is a red trash icon. Below the second row is a filter selection area with two buttons: 'x Apple' and 'x Gmail', and a red 'x' icon on the right side.

## Triggers Filters:

- Deliverability Triggers: Inbox %, Spam %, Missing %
- Authentication Triggers: DKIM % and SPF %

## Useful Filters:

- ISP – apply alert only to certain MBPs
- Region – apply alert to certain Everest regions
- IP Address – apply alert only to certain sending IPs
- Child Account – apply the alert to a child account

# Certification

---

- Certification alerts can only notify via email. You cannot select a cadence.
- There are 3 types:
  - Daily Performance Report – sent out once a day, gives full view of Certified IPs.
  - IPs suspended – notifies if a Certified IP has been suspended or unsuspended for performance or security issues.
  - Cert Placement Rate – triggers if actual inbox placement at Microsoft or Yahoo hits threshold.
- It is suggested that all Cert customers use all 3 alerts.

# ★ Blocklisting & DNS Issues

---

- Periodically checks a domain, IP, or profile for a type of blocklist activity.
- Show all IPs or domains that have had the selected blocklisted activity since the last alert scan.
- This alert is primarily used to notify the user when they **land on high-priority blocklists**, specifically Spamhaus.
- Alert can be set for IPs, Domains, or Monitoring Profiles. User can enter multiple of each option but cannot use one alert to monitor both IPs and domains. In the email it will split up results by item.
- **For “Is blocklisted on”, user can select multiple blocklists, but there is no quick way to mass-select high-priority only.**
- We check for blocklistings at different frequencies for different accounts (from 1 hour to daily), so the highest frequency for this alert is 1 hour.

## Blocklist Activity Types:

- Has any blocklist activity – shows any status change for the IP/domain
- Is blocklisted on – allows selecting one or more specific blocklists
- Is blocklisted anywhere – only notifies when the item is listed
- Blocklisting is cleared – only notifies when there is a delisting
- Has rDNS issues – for Monitoring Profile only, triggers when an rDNS issue occurs.

# Usage Alerts

---

- Triggers when a certain % of an allotment is reached for the current credit period.
- This alert is primarily used to notify users when they are getting close to hitting their credit allotments.
- This alert is not a trend (where their usage will end up if they use at the current pace), just a **snapshot of usage at the time the alert is triggered**.
- Accounts that have multiple contracts in play within Everest may have accuracy issues. Contact support if you see issues.
- Reseller accounts can also select *Child Account* after *Account Settings*, allowing them to set usage alerts across all child accounts.
- DMARC Usage option has no function.
- Cannot turn off repetition, so it is not recommended to set frequency higher than 1 day.

## Usage Alert Types:

- Inbox
- Design
- Validation
- Engagement
- Monitored IPs & Domains

# Other Alerts

---

- Spam Traps/Phishing
- Microsoft SNDS
- Integrations
- DMARC Policies
- Complaints (Feedback Loops)
- Signal Spam

Remaining alerts are not used as often, but still have value for many customers. These are more like each other than the highlighted alerts above.

Some general rules that apply to all of them:

- When triggering using  $\geq$  or  $\leq$  on a metric, they are looking at the last 24 hours of data at the time of alert scan.
- When triggering using deviates by, increases by, or decreases by, it compares the prior 24 hours to the 7, 30, or 90 day average.
- Bug with Spam Traps, Complaints, and Signal Spam – recommended to use just deviates by, increases by, or decreases by.
- SNDS, DMARC, and Integrations are percentages. Keep in mind, for deviates by, it is calculating a % change of a %. So deviating 5% from the 10% average is 10.5%, not 15%.

# Spam Traps & Phishing

---

- Triggers when the threshold number of spam traps is hit, or when spam traps deviate from an average by a certain %.
- This alert should be used to identify spikes in spam traps.
- We do not track volume, so the spam trap number is not a % - it is a raw number. There is a bug for  $\leq$  or  $\geq$  that makes the threshold a %. It is suggested to use deviates, increases, or decreases by.
- Phishing attempts is looking at suspicious mail

# Microsoft SNDS

---

- Triggers when specified threshold is hit for SNDS % (green, yellow, or red), or when there is an IP status change on SNDS.
- This alert should be used to identify when green % drops too low or when red % spikes too high.
- Deviates, increases, and decreases by is measuring a percent change of a percentage.

# Integrations

---

- Triggers when a Delivery Insight metric % reaches a certain level.
- Other conditionals can be added as filters (like with Inbox Placement).
- The %s here are based on total volume.
- There is no default time period for these alerts – user can always select the time period they are interested in.
  - This includes the deviates, increases, and decreases by option – user can select both time periods.
- Multiple options can be selected by pressing "Add Criteria", these operate as AND statements.
- Most filters allow entering multiple options – these operate like OR statements.
- If you do not select a % option, it will fire, but the alert will be blank.



# Alert Use Cases

---

*Alerts In Action*

# Use Case: Kohl's

<input type="checkbox"/>	Impactful Blocklists - Marketing IPs - SPAMCOP	If Profile Salesforce Marketing is blacklisted on 2 lists selected send SMS,EMAIL
<input type="checkbox"/>	Impactful Blocklists - Marketing IPs - SPAMHAUS! LOOK!	If Profile Salesforce Marketing is blacklisted on 22 lists selected send SMS,EMAIL
<input type="checkbox"/>	Impactful Blocklists - Transactional IPs	If Profile Salesforce Transactional is blacklisted on 24 lists selected send SMS,EMAIL

Email

Text Message

Webhook

Slack

PagerDuty

Microsoft Teams

kristina.ek@validity.com,julie.stuck@validity.com,kendall.x.mccoy@kohls.com,therealmccoy@gvtc.com,  
Comma-separated email addresses

2102898669,7607127558,7278041321  
Comma-separated phone numbers

Would NOT recommend adding your # to all, but just Spamhaus.

**Use Case:** Spamhaus Blocks in Advance of Holiday Sending Period  
Notification came in over the weekend when less likely to be in email or checking email  
Having alert clearly labeled and sent to us via text was huge in us being able to help Kohl's remediate quickly and take steps to prevent it from happening again.  
(Note: Their ESP basically said they couldn't do anything to support them until Monday!)

# Use Case: Wayfair

<input type="checkbox"/>	P1 - Spamhaus Listing (SBL / DBL / XBL) for AllModern Batch	If Profile All Modern is blacklisted on 7 lists selected send SMS,EMAIL,PAGERDUTY
<input type="checkbox"/>	P1 - Spamhaus Listing (SBL / DBL / XBL) for Birch Lane Batch	If Profile Birch Lane is blacklisted on 7 lists selected send SMS,EMAIL,PAGERDUTY
<input type="checkbox"/>	P1 - Spamhaus Listing (SBL / DBL / XBL) for Joss&Main Batch	If Profile Joss & Main is blacklisted on 7 lists selected send SMS,EMAIL,PAGERDUTY
<input type="checkbox"/>	P1 - Spamhaus Listing (SBL / DBL / XBL) for Perigold Batch	If Profile Perigold is blacklisted on 7 lists selected send SMS,EMAIL,PAGERDUTY
<input type="checkbox"/>	P1 - Spamhaus Listing (SBL / DBL / XBL) for Triggered IP(s)	If Profile Triggered IPs is blacklisted on 7 lists selected send SMS,EMAIL,PAGERDUTY
<input type="checkbox"/>	P1 - Spamhaus Listing (SBL / DBL / XBL) for Wayfair CA Batch	If Profile Wayfair CA is blacklisted on 7 lists selected send SMS,EMAIL,PAGERDUTY
<input type="checkbox"/>	P1 - Spamhaus Listing (SBL / DBL / XBL) for Wayfair DE Batch	If Profile Wayfair DE is blacklisted on 7 lists selected send SMS,EMAIL,PAGERDUTY
<input type="checkbox"/>	P1 - Spamhaus Listing (SBL / DBL / XBL) for Wayfair UK Batch	If Profile Wayfair UK is blacklisted on 7 lists selected send SMS,EMAIL,PAGERDUTY
<input type="checkbox"/>	P1 - Spamhaus Listing (SBL / DBL / XBL) for Wayfair US Batch	If Profile Wayfair US is blacklisted on 7 lists selected send SMS,EMAIL,PAGERDUTY
<input type="checkbox"/>	P1 - Spamhaus Listing (SBL / DBL / XBL): Transactional IPs	If Profile Transactional IPs is blacklisted on 7 lists selected send SMS,EMAIL,PAGERDUTY

**Use Case:** Similar to Kohl's real concern about receiving Spamhaus Notifications outside of Business Hours and having it go to the people who can respond. Labeled the alert to align with Customers own SLA tiers and had it go to their PagerDuty Notification, as well as text and email!



# Report

---

<https://metabase.everest.validity.com/question/548-alerts-report-active-everest-customers>

