Onboarding Guide

HORNETSECURITY

Content

Your first steps

This guide will help you to take your first steps in the Hornetsecurity world. We will introduce you to the Control Panel and guide you through the necessary settings.

Not all products shown in this guide will apply to your current contract, therefore feel free to use the navigation at the bottom to skip individual products or information not relevant to your individual configuration.

We and Email Laundry worked together and transferred over as much information as possible. But due to the upgrade in services and general technical restrictions not all could be transferred or needs adjustment from you in order for the service to work flawlessly. Next, you will find a short overview of the information you might need to double-check or adjust.

Transferred information

In assistance with Email Laundry, we were able to transfer the majority of your settings and information to our Control Panel. Due to technical enhancements you will find with the Hornetsecurity filter system, a one-to-one copy of the data was not possible.

Check for outdated information

This information was transferred over from Email Laundry and should only require you to double-check and update and outdated information.

- Spam & Malware Protection
  - Outbound Routes
  - Divergent settings for Alias Domains
- Spam Report Settings
- Email Disclaimer
- Black & White lists

Configuration required

The following services have been enabled, if you had them previously booked. They will require a first setup, due to the increased options with the Hornetsecurity update.

- Email Encryption: You have received additional encryption methods, which require setup, should you decide to use them.
- Advanced Threat Protection: You will need to setup URL Rewriting and the Targeted Fraud Forensic Filter
- Continuity: You will need to decide the users for whom this service should be enabled

Not transferred

The following services could not be transferred from the Email Laundry system, due to a vast difference in their setup. For example, Hornetsecurity Content Control offers more options, therefore a transfer here wasn't possible.

- Groups
- IP Restrictions
- Compliance Filter
- Content Control

This Onboarding Guide will assist you with setting up the required information per service. We also highly recommend checking our Documentation Portal for a details step-by-step description for each service.

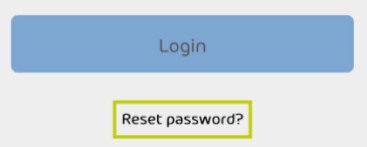
Introducing the Control Panel

The Control Panel acts as a central hub, where existing services can be managed and enabled. The main functionality of the Control Panel is to monitor and control the flow of your emails.

The Control Panel is designed for handling incoming emails and evaluating the email traffic. For example, you can mark emails as spam or release emails that have been marked as spam. You can also blacklist or whitelist senders. It provides you with an easy-to-use web interface with a responsive design. Thus, you can use it on your desktop and on your mobile device from everywhere you are.

The system was designed from the get-go as a progressive web app, to allow maximum comfort for the users, no matter from which device its being accessed.

Access to the Control Panel is handled through the website. You should have received a password reset request to the e-mail address you have previously used to login to the Email Laundry portal. If this is not the case, you can reset your password from the login page.

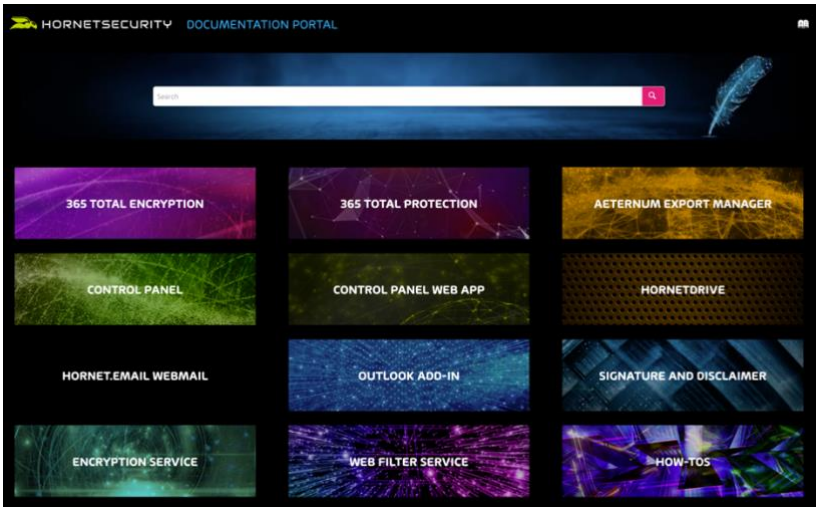


In order to be able to reset the password, you will first need to enter your username and hit continue. Once the field to enter the password appears, you will find the "Reset password?" link right under the Login button.

Documentation Portal

Linked from within the Control Panel you will find the documentation portal. From here you will be able to access the technical documentation for all our available products and services.

You can access the documentation portal either via direct link, or within the Control Panel, found at the very top of the page. Login to the documentation portal requires your Control Panel login details. Therefore, you will be required to enter your login data, even when using a direct link.



Using direct links

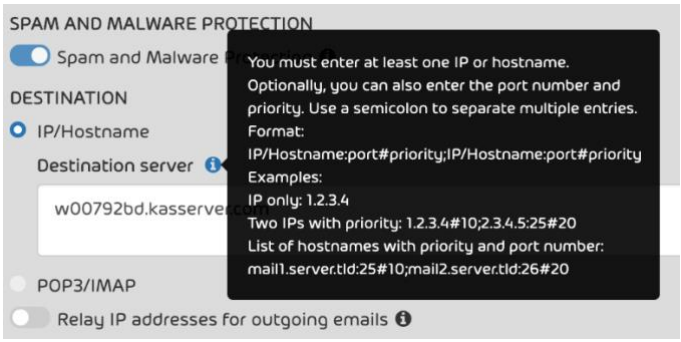
The URLs provided within this guide will forward you to the directly to the intended section of our documentation portal. In order to be forwarded correctly, you currently need to be logged into the Control Panel.

If you are not logged in, you will be prompted to log in, but you will lose the direct forwarding to the specific section and rather stop at the Documentation Portal landing page. If this is the case, you can either manually search for the correct section from the search field or return to this guide and use the link again while being logged into the Control Panel.

You can also download the Control Panel manual from our FAQ website.

Using the Control Panel

Throughout the Control Panel you will encounter information buttons, next to different menu items. Hovering over these will provide you with additional information for the menus, as well as examples on how to format data when entering it.



After making adjustments or updating information, you will need to save the information for them to take effect. To save the changes you will find this button from within the appropriate section. Make sure to confirm the changes, before switching to another tab or logging out of the Control Panel.

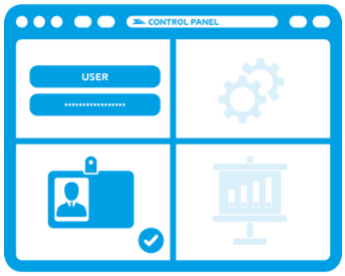
Additional items can be displayed within a sub-menu inside the Control Panel. This usually is the case, if information is provided in a table format, like the mailboxes, groups or even the individual e-mails from within Email Live Tracking.

If this is the case, you will find this icon behind each individual entry. When clicking on it, the sub-menu will expand.

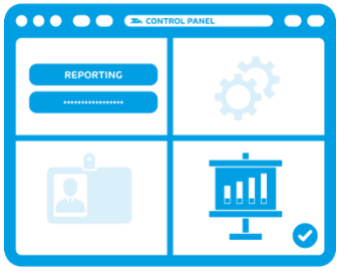
User Permissions

Your Email Laundry Login should provide you with the same administrative rights as you previously had. With those permissions you are able to perform changes to the configuration and provide permissions to other users.

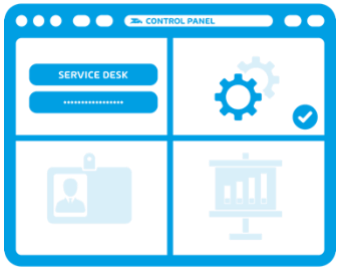
In the Control Panel, the following standard roles are defined:



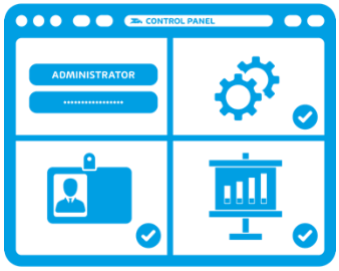
Standard User
This role is automatically assigned if no other role has been assigned. This role cannot be assigned manually.



Reporting
This role has only access to statistics.

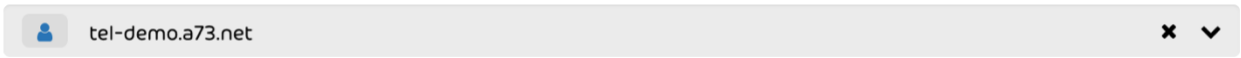


Service Desk
This role is aimed at support employees.

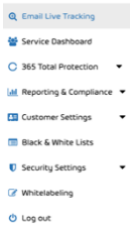


Administrator
This role has comprehensive administrative rights.

If you have been assigned a role other than the user role, the Control Panel provides an easy way to change the scope of your role. You can find the Scope selection in the upper right corner. The scope selection contains all scopes of the roles assigned to you.



To check the settings of a domain, you will first need to change to the domain level from the Scope selection. Once the domain was selected, you will find additional menu items from the left-hand side.



The number of visible menus differs based on your user privileges, your booked services, as well as the currently selected level from the Scope selection.

Contact and Support Permission

From within the Service Dashboard you can, and should, add the most important contact persons from within your organization. Persons added into the personal contact field will act as point-of-contact for our support team in case of emergencies. Our technical support team will also only accept support requests received from anyone entered in the personal contacts section.

Personal contacts

First name	Last name	Phone business	Email	
Bruce	McLeigh		admin@tel-demo.a73.net	X

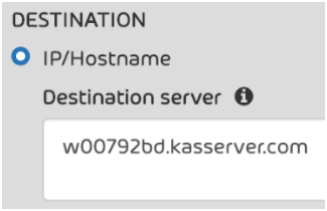
Additional information regarding permissions can be found from within our technical documentation.

Setting up Spam & Malware Protection

The Spam and Malware filter is the backbone of Hornetsecurity's services. This service is required should you wish to use any other products, such as Advanced Threat Protection or Email Encryption.

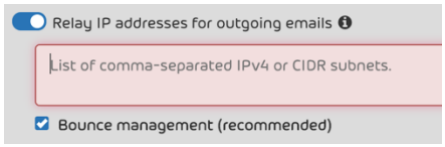
We have transferred your Email Laundry settings. Please make sure that these are correct and update any outdated information.

Confirm that the Spam and Malware Protection slider is set to active. The service is the foundation for any other services and requires to be enabled for other services to work.

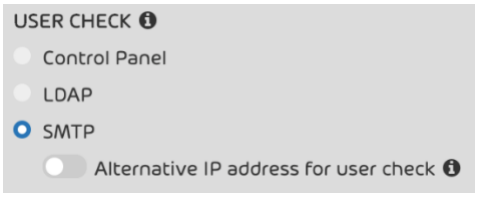


Check and confirm the destination server. Any incorrect or outdated information should be adjusted. You should also feel free to add any additional destination servers, that might have been added in the meantime.

Confirm and complement the IP addresses that will be used to send e-mails. The filter system will not accept any outgoing e-mails being delivered from IP addresses not listed within the Control Panel.



Bounce Management is a service designed to prevent delivery of Non-Delivery Reports created outside of our infrastructure. This would be the case for spoofed e-mail addressed used for sending mass spam or other malicious content. The service is optional, but we highly recommend enabling it.



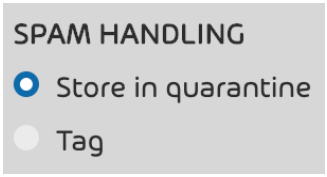
Next, select the data source for the user check. You will need to select the service, which contains the most up-to-date user list, to ensure flawless e-mail delivery.

When selecting SMTP, the system will use the server information entered in Destination. With the slider below SMTP, you can enter an alternative IP address for the user check.

Setup Mail Handling

You will need to decide whether you want to have spam e-mails delivered to the intended recipient or to quarantine them on the Hornetsecurity server.

We have transferred your Email Laundry settings from the portal as they were. Please make sure that the settings are correct and update any outdated information.



Store in quarantine: Potential spam e-mails will be moved into an isolated area where it remains accessible for 3 months.

Tag: Potential spam e-mails will be marked in the subject with a phrase or word of your choice.

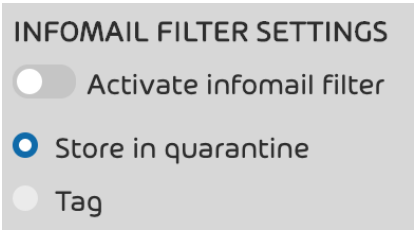
Infomail filter

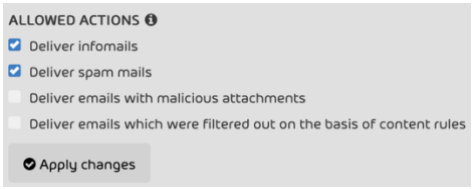
The Infomail filter is designed to identify and handle newsletters. It detects them and carries out different actions depending on the settings. Enabling the Infomail filter also allows to distinguish them from within the quarantine.

If **stored in quarantine**, Infomail will be stored along with other e-mails for 3 months.

If **tagged**, potential Infomail will be tagged with a phrase of choice in the subject and gets delivered to the intended recipient.

Our recommendation is to quarantine the e-mails, rather than tagging, as it poses a lower security risk. With the use of Email Live Tracking and spam reports, any potential delay can be kept to a minimum.





From within the User Rights tab you can choose which quarantined e-mail category the users can release from either Email Live Tracking or the Spam Report.

Domains

Under Domains, you will find an overview of all existing domains and alias domains. You can create new domains and delete existing ones. You can also export the displayed domains in CSV format and re-import them at the designated location.

Certain functions, like the Spam and Malware setup allow you to create diverging entries and setups based on individual domains. You can also create mailbox aliases.

We have transferred your Email Laundry settings from the portal as they were. Please make sure that the settings are correct and update any outdated information.

Domains can be accessed from within the Control Panel under Customer Settings. Make sure that the currently provided list is complete. If any domains are missing you can either add them manually or import them in bulk using a CSV file. When importing in bulk, you will need to make sure that the file adheres to the required formatting syntax.

Mailboxes

Under Mailboxes, all users registered under your domain are displayed. First, you should confirm that no mailboxes are missing. Your data should be the same as stored on the Email Laundry portal, but you should check nevertheless whether the information is up-to-date and complete. If the amount of your mailboxes won't allow a manual check of all users, we recommend a spot inspection of the most important mailboxes.

All available users will be visible from the list within the Control Panel. From here you can also add additional mailboxes, should you desire. If you are using a directory service via LDAP to import your mailboxes, you should perform any changes to the mailboxes from within the directory service.

The system considers the directory service as the source-of-truth, meaning any information stored within the Control Panel would be overwritten in case of conflicting information.

Additional information, such as changing users passwords or aliases can be accessed through the mailbox's sub-menu.

Groups

Under Groups, you can create, change or delete groups. You can create new groups, combine several mailboxes into one group and manage the existing groups. Lists of group members can be exported as CSV files.

Unfortunately, it was not possible to transfer your already existing groups from the Email Laundry portal into our system. It is therefore necessary to re-import or re-create the groups you require.

Groups can either be created manually or imported using a CSV file or through a database with an LDAP connection. The information stored in groups will be used for different services, such as Content Control and Signature & Disclaimer.

Each Group can be managed using its sub-menu, accessible through the list. From here you can manage the members, rename the group, customize the description and finally delete the group.

Groups synchronized via LDAP should be managed from within the directory service, as the Control Panel regards the directory service as source-of-truth, thus overwriting any changes made within the Control Panel with the next synchronization.

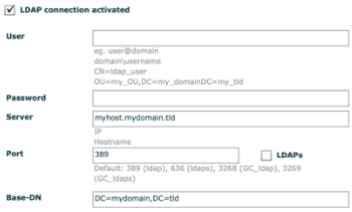
It is not possible for a mailbox to be a member in more than one group at a time.

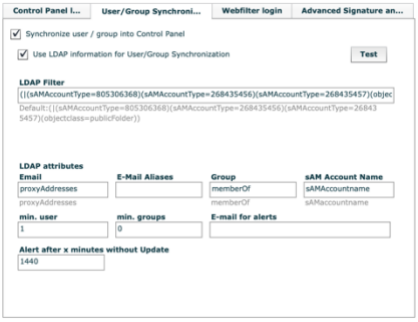
LDAP Setup

When feasible we recommend using a directory service to import your mailboxes into the Control Panel. A directory service not only provides you with the possibility to manage your users, but also to use additional Hornetsecurity services, such as the Signature & Disclaimer.

We were able to transfer most of the LDAP information that was setup within the Email Laundry portal. However, some information couldn't be transferred or might be outdated.

You can access the LDAP settings using the Dashboard from within the Control Panel. The requirements and details you need to setup your LDAP connection can be found from within the technical documentation.





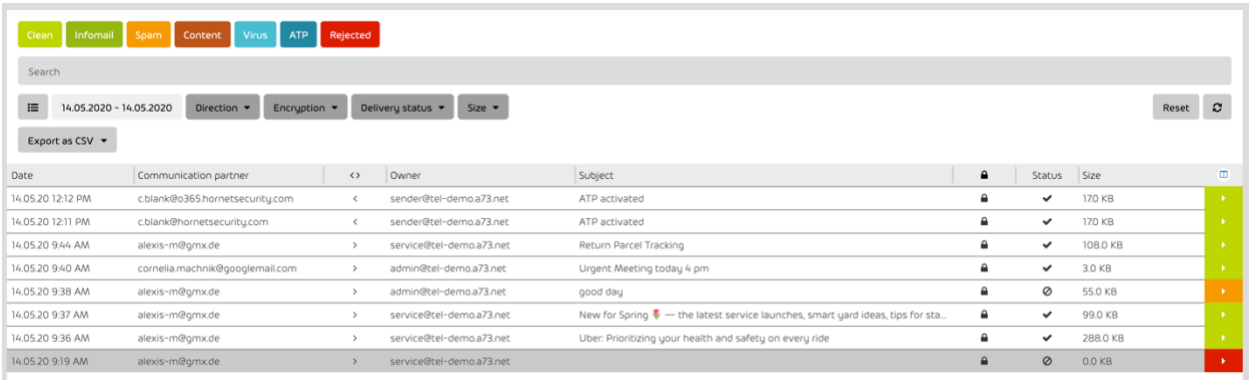
From the user and group synchronization you will find a pre-populated LDAP filter. You can either keep, adjust or completely replace this filter, as you see fit. When making any adjustments, we highly recommend testing the new filter settings using the "Test" button.

You can also use the LDAP credentials to log into the Control Panel. As with the user synchronization, there is also an LDAP filter pre-populated, which can be used, adjusted or replaced as you see fit. This section also offers the possibility to test your filter settings, which is also highly recommended.

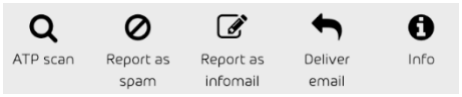
The Control Panel regards the directory service as source-of-truth, thus overwriting any changes made within the Control Panel with the next synchronization. The synchronization between the directory service and the Control Panel happens throughout the day in regular intervals.

Email Live Tracking

Email Live Tracking is a tool designed to allow you direct access to your quarantined and archived emails. The available actions depend on the user's assigned permissions and booked services. A standard user for example, will be able to see his or her complete e-mails quarantined in the past 3 months. If archiving is enabled for the domain as well, the user will not only be able to search the quarantined e-mails, but also all their archived e-mails. Every active user stored within the Control Panel has access to Email Live Tracking.

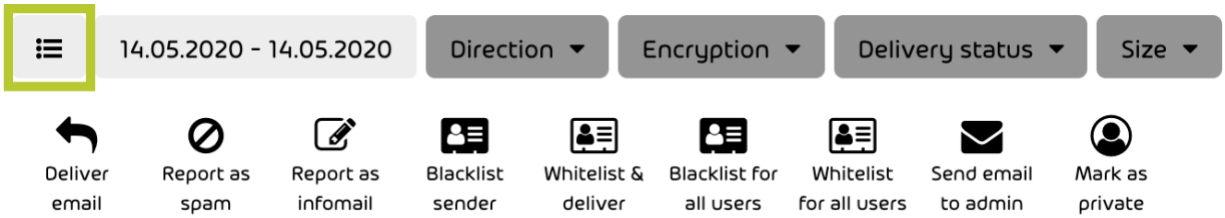


Each e-mail contains additional options through a sub-menu. Under the Info tab you will find additional helpful data, such as the e-mail-header. From here you can also release individual e-mails from both quarantine and the Email Archive.



For e-mails containing executable attachments, you can also manually trigger an ATP scan. Such e-mails will be moved to the Advanced Threat Protection Sandbox Engine and analyzed for potential threats. If you do not yet have the ATP service booked, you can manually trigger two scans per month free-of-charge. For the service to be able to scan the e-mails, they will need to be stored in quarantine.

Actions for individual e-mails will be handled through their sub-menu. If you want to perform actions for multiple e-mails, you can use the menu right next to the date.

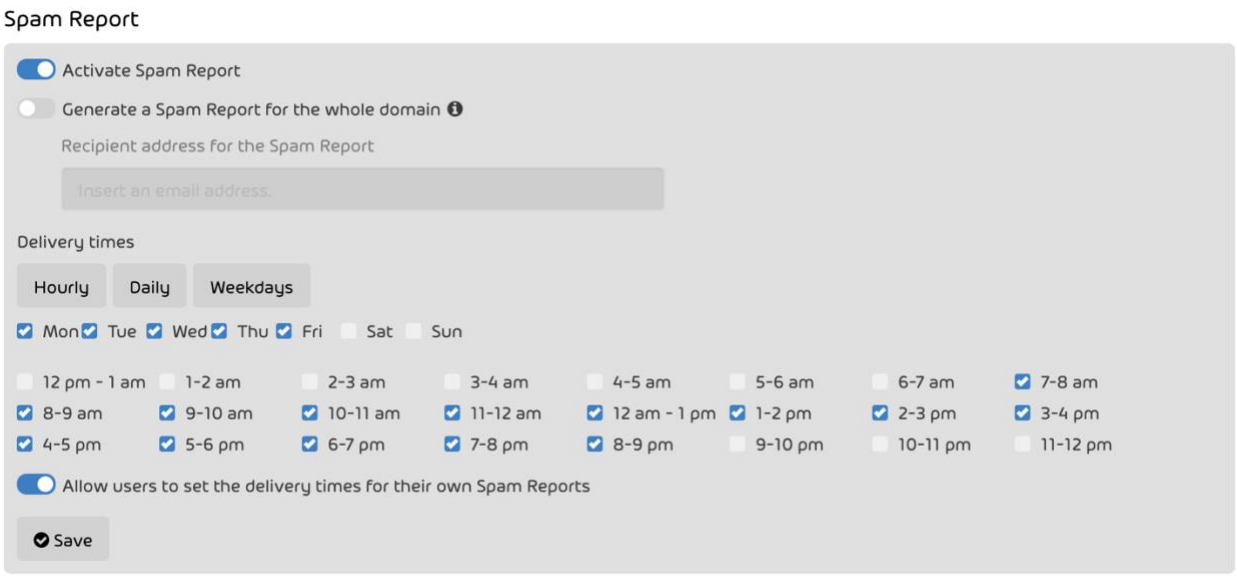


Spam Report Setup & Management

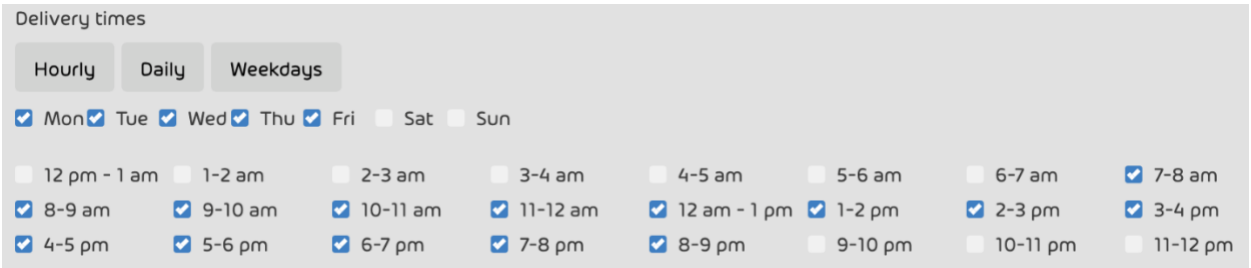
As an alternative, or in addition to, the Email Live Tracking you can also use the Spam Report to inform your users of any e-mails currently stored in quarantine.

The Spam Report is a report which is either created individually for a user, or for the whole domain and is delivered to the recipient by e-mail. It lists all e-mails which have not been delivered to the user and have been stored in quarantine. If the recipient of the Spam Report has the required authorization, they can prompt the delivery of these e-mails if desired.

We have transferred your Email Laundry settings from the portal as they were. Please make sure that the settings are correct and update any outdated information.



The delivery time can be chosen from a wide variety of pre-defined time frames, which can be combined in any combination you see fit. Should you wish, you can provide your users with a spam report 24/7.

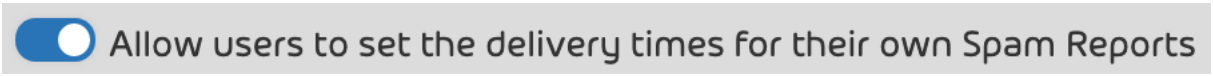


You can rest assured though, that this wouldn't result in the users receiving a spam report every hour, no matter what. The system will only send out a spam report, if the user actually has e-mails stored in their quarantine. If there are no e-mails currently stored in quarantine, the system will not generate a report.

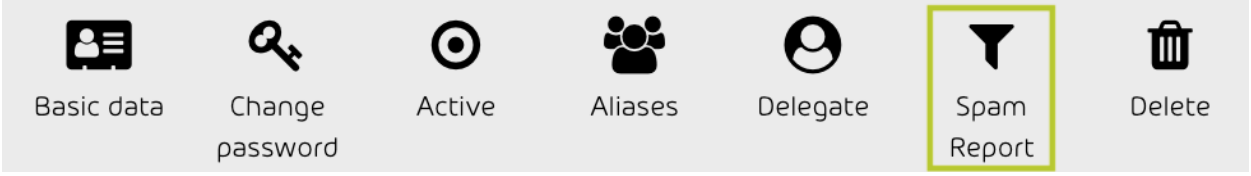
The system will also remember which e-mails where previously reported and will not include those in any future spam reports.

By default, a spam report will be delivered to every active user who has new e-mails stored in their quarantine, since the last spam report was received. Those settings are applied to all users stored within the domain or alias domains.

When allowing individual delivery times, you can set diverging delivery times per mailbox. This will also give you the option to disable the Spam Report for individual users altogether.



Individual delivery times can be set from within the Mailboxes section in the Control Panel by opening the user details.



The Spam Report will show the quarantined e-mails, grouped by their filter categories. For an easier identification of potential false positives, additional information will be provided.

Filter Category. The classification reasons the filter system assigned to the e-mail, based on the in-depths analysis.

E-mail subject. As it is shown within the e-mail.

Sender e-mail-address. This will show the e-mail's header-from. This is especially advantageous since the envelope-from can be faked or masked.

Date and time the e-mail was received by our servers. The time given here will be in relation to the time zone setup in the Control Panel by the individual user.

To release and deliver an e-mail from quarantine, the user can simply click on any of the above-mentioned details. A browser window will open and inform the user of the success or failure during the release. When trying to release an e-mail not enabled from the User Rights, an error message will be provided.

Black & White List

In the Black & White Lists module you can define that emails from specific senders or domains are always quarantined (blacklist) or delivered (whitelist). The system makes a distinction between user-specific lists and lists affecting a complete domain(s). The entries will be handled with a different priority, depending in which list they are added.

We were able to transfer your pre-existing Black and White list entries, stored in the Email Laundry portal. We do recommend though to double-check the existing entries and update any outdated information.

You can access the Black and White list from the "Black & White List" section within the Control Panel.

To add an entry, simply click the "Insert" section from either list and enter the e-mail address that should be added.

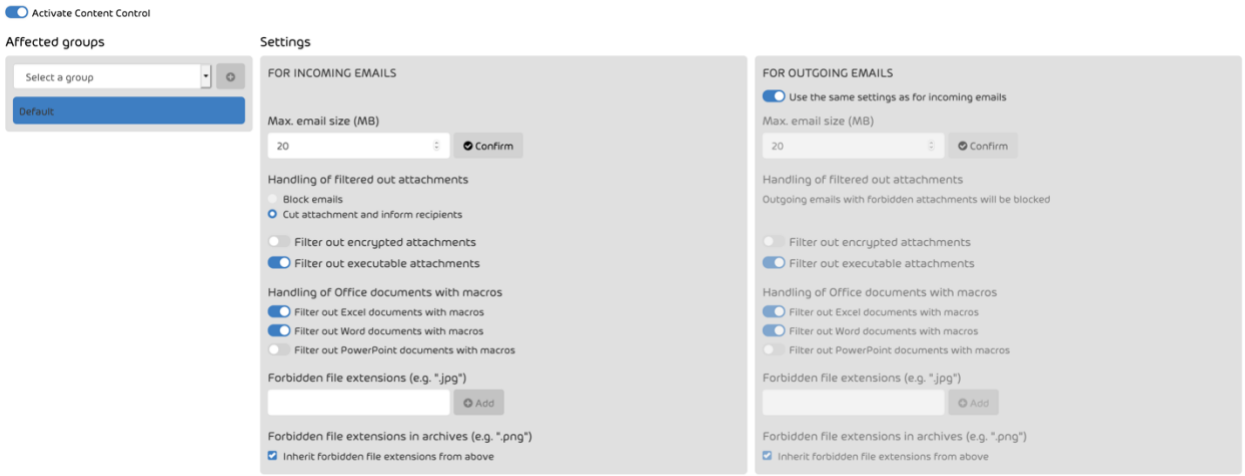
When releasing an e-mail from the Spam Report, the user can also directly add the just released recipient to their respected white list. Such a prompt is shown from the browser upon release. Some users might be surprised that an e-mail from a specific sender continues to be quarantined, even though added to the user whitelist. For such cases, please refer to the priority handling, mentioned above.

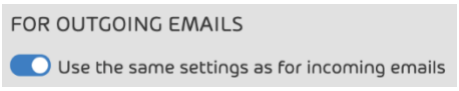
The encountered behavior after adding an Infomail sender to the white list might also cause some confusion. Infomail, such as newsletters, will usually use a different envelope-sender than in their header-from, causing the filter system to not be able to assign the whitelist entry to the e-mail when analyzing.

Content Control

Content Control offers domain administrators and partners the possibility to manage the handling of attachments of incoming and outgoing emails.

Policies are set and maintained based on existing Groups. When enabled, you can set individual policies per group. The "Default" group will apply to any users, not covered through another group setup in Content Control. It is therefore highly recommended to set rules for the "Default" group, as soon as Content Control gets enabled.





You can set different policies for incoming and outgoing e-mails, should you choose to. The available settings are congruent between incoming and outgoing e-mails, with one difference: It is not possible to quarantine outgoing e-mails, as there is no quarantine kept for sent e-mails.

Content Control allows you to prevent the delivery of specific file types, but you can also use pre-defined categories. Categories are umbrella terms, concentrating different file types for easy access, e.g. “.executable” for EXE, BAT, CMD and similar files.

Email Encryption

Email Encryption allows to communicate securely and privately. Hornetsecurity offers a wide variety of encryption methods, to either encrypt the data connection or the content itself. It is also possible to combine the two and send encrypted content using an encrypted data connection.

The encryption is handled through the Control Panel by setting up specific rules. Those rule sets are similar in their build to any mail rules you might have setup from within Microsoft Outlook. Our technical documentation provides further details on how to setup encryption rules.

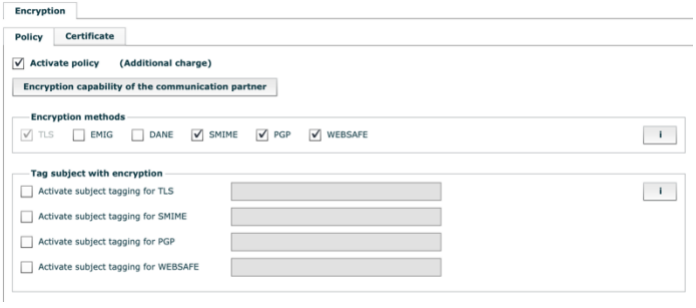
Unrelated to the services you have booked, Hornetsecurity offers every customer opportunistic TLS encryption. This means that our services will always - no matter if you have the encryption module booked or not - first try to create a connection to any other server using TLS. Only if the opposing server is not able to communicate via TLS, would it fall back to a connection not using encryption. Using the encryption module, you can overwrite that setting as well.

We are also offering you additional encryption options for you to use, if you have booked Email Encryption.

TLS
We are supporting multiple versions of TLS, including 1.2.

S/MIME & PGP
In addition to implementing your existing certificates, you can also order S/MIME certificates directly through the Control Panel.

Websafe
Our own creation. The system is designed to work with recipients, who don't have access to any other encryption method.

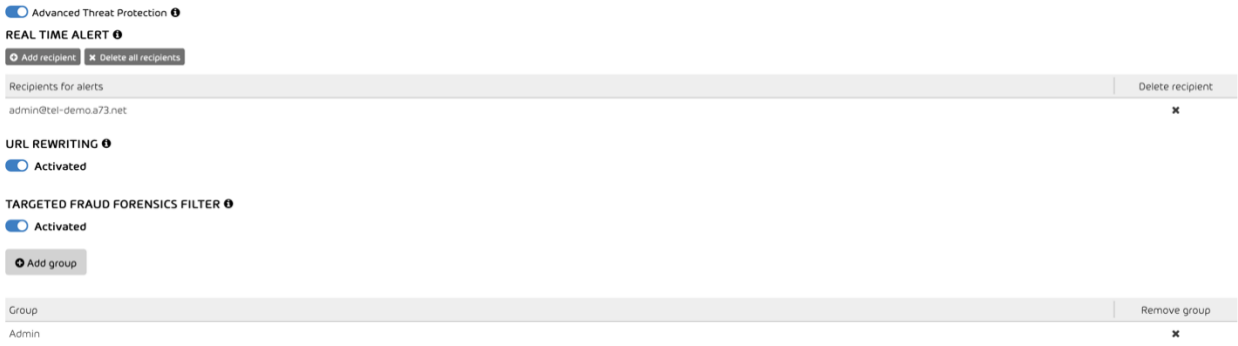


In order to use the encryption service to its fullest, you will need to create your own encryption policies, using your preferred encryption method. Additional information on Email Encryption can be found from our technical documentation.

Advanced Threat Protection

Hornetsecurity Advanced Threat Protection (ATP) protects your company against targeted, individual attacks. Innovative forensic analysis engines ensure that attacks are prevented immediately. At the same time, the solution also provides your company with detailed information about the attacks.

This service is similar to the Advanced Threat Protection you know from Email Laundry but expands the existing services.



The Advanced Threat Protection service consists of three different engines, each with their individual specialties and strength.

Sandbox Engine
Attachments are executed in a variety of system environments and their behavior is analyzed. If they turn out to be malware, you are notified. It protects against ransomware and blended attacks.

URL Rewriter
The URL Rewriting engine replaces all links in an email with our own links. As soon as the user clicks on one of those links, he is rerouted to the target website through the Web Filter service.

Targeted Fraud Forensic Filter
This engine detects targeted personalized attacks carried out without malware or links, such as Spear Phishing or Business Email Compromised.

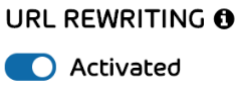
If you had ATP previously booked with Email Laundry, the Sandbox Engine will already be enabled for you. All that is left at this point is for you to setup the URL Rewriter and Targeted Fraud Forensic Filter.

You can setup the Advanced Threat Protection service from within the Control Panel under the Security Settings menu. You can enable or disable any individual engine as you see fit. To benefit from the full protection, we

recommend using all three. In order to reduce the amount of possible false positives, you might want to deactivate certain engines, as you see fit or as it meets your needs.

URL Rewriter

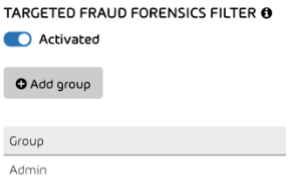
As mentioned previously, the URL Rewriter will change any links within an e-mail in order to redirect any connection established through our web filter service first. From there, the site will be checked based on multiple security characteristics and any possible downloads will be forwarded to the Sandbox Engine.



If the engine identifies any security risks within a web site, it will prevent the user from accessing the site. Instead, the user will be presented with a security warning. The scan is done - for the most part - in the background while the connection is established. For those rare occasions where the scan takes a few seconds, the user will be presented with a progress bar.

You can also whitelist certain pages. Those URL will then not be rewritten but kept as they were. To whitelist certain domains, simply provide our technical support with a list of your desired domains.

Targeted Fraud Forensic Filter



The Targeted Fraud Forensic filter is specifically designed to detect CEO Fraud, Spear Phishing, Business Email Compromised and other threats tailored to individuals or targeted departments, such as HR. You can enable the service for specific groups or users stored within the Control Panel.

The Targeted Fraud Forensic Filter examines the e-mail for its contents. Using assisted machine learning, the mechanism can detect certain expressions, peculiarities or even missing information. If inconsistencies or errors are detected here, the e-mail is moved to quarantine and the recipient can be informed via the spam report.

Due to the nature of analyzing the content of the e-mails, rather than just checking for specific outliers, recipients protected by this service can expect a slightly higher number of false positives, when the service is enabled. Therefore, this service should only be enabled for a limited audience. We recommend providing the audience with additional security awareness training, so they are able to identify potential threats from within the quarantine, before releasing any e-mails.

The Advanced Threat Protection service also offers you two alert options, informing you of potential threats.

Real Time Alerts
An e-mail being sent out for any threat identified by the Sandbox engine, containing the specific information necessary to quickly identify a potentially harmful e-mail.

Ex-Post Alerts
An e-mail containing valuable information in case a threat has been identified, after an e-mail was already delivered. This will allow administrators to act quickly and prevent any security leaks.

You can add the desired recipient(s) for both notifications from the Real Time Alert section. Any potential recipients should have the required permissions and skill set to take immediate action to counter any potential threat.

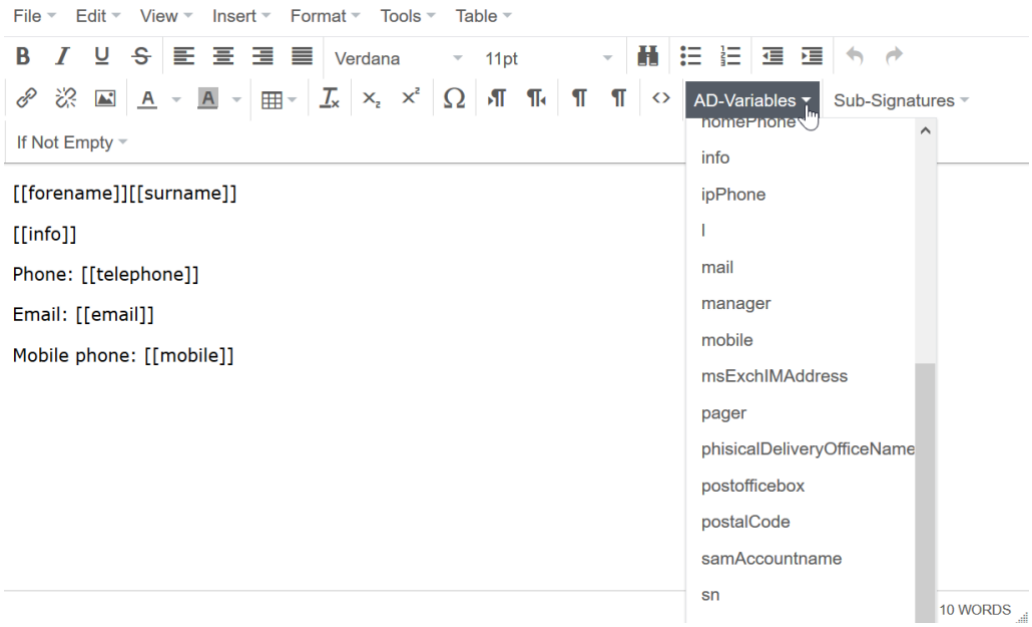
Signature & Disclaimer

Signature & Disclaimer controls the automated provision of email signatures and disclaimers on all Hornetsecurity gates. The tool dynamically generates user specific signatures, matching the Active Directory setup. The signatures are based on predefined templates and are included automatically after the body text of the email.

In order to use this service, a valid directory service needs to be setup via LDAP within the Control Panel.

The service also offers the option to use the email Disclaimer only, without the use of a directory service. If you previously had the email disclaimer enabled from Email Laundry, this is the option currently enabled for you.

The Signature & Disclaimer tool offers you an easy-to-user editor, allowing you to set multiple AD-Variables.



Continuity Service

The Continuity Service is an additional email service that guarantees continuous email functionality in the event of an email service failure. With the Continuity Service enabled, users can continue to receive and send email if their email server fails.

Your settings from the Email Laundry portal have been transferred. We do recommend double-checking them and update and outdated information.

The users setup with the service can either access their e-mails during an outage via the webmail portal, or setup POP3-Accounts from within their e-mail clients.

Final touches

Now, you are all set up!

If you haven't done so already, you will need to update your firewall, MX records and SPF record next. Once done, your traffic will be filtered through Hornetsecurity and you are free to explore your new features and services. There is a lot more to experience and even more to come in the future.

System Status Website

To stay updated on new developments, releases and the system status in general, we recommend subscribing to our System Status website. Through this service you will be informed of any service interruption, maintenances or similar situations which might impact the service in any way. You can use your e-mail address to select the services you want to subscribe to and manage your subscriptions as well.