Coro version 1.4 – Release Notes

Customizable Email notifications

Email phishing Allowlist/Blocklist management

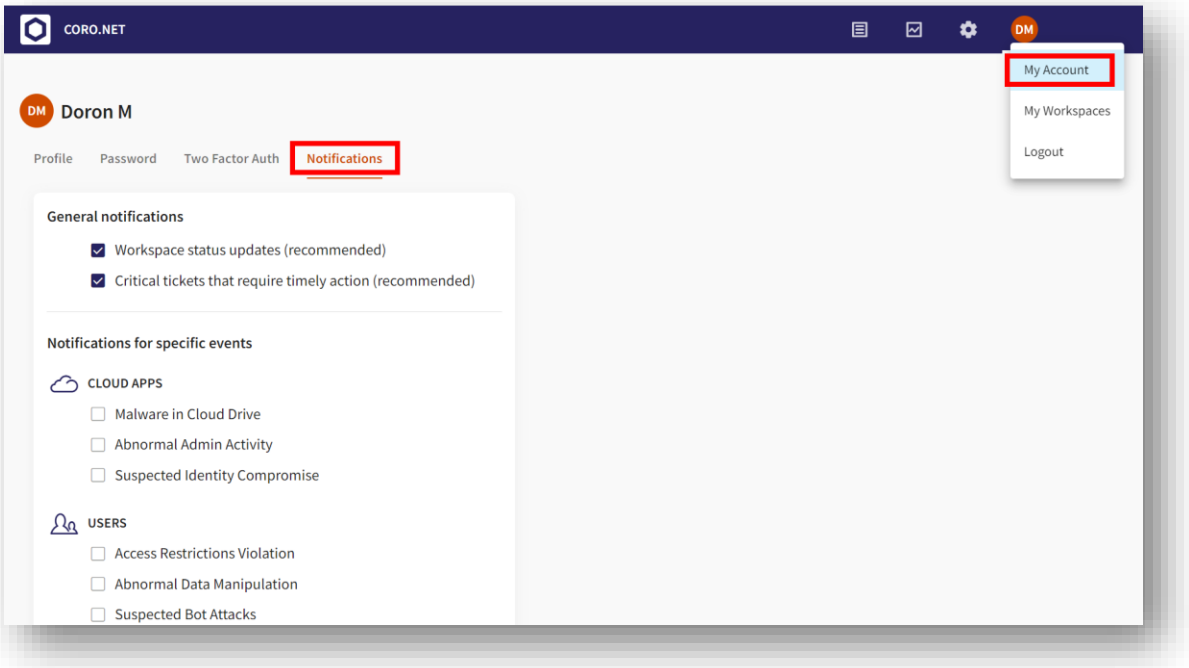
2FA access control to the Coro Console

User-less clients

Customizable Email notifications

To provide you with more granular control of the notifications you get from the Coro system to suit your specific needs, we have implemented a new mechanism which will allow each Coro console admin to select which email notifications he/she would like to receive.

To select your notification, navigate to *Control Panel/Personal menu/My account* and select the new *Notifications* tab:



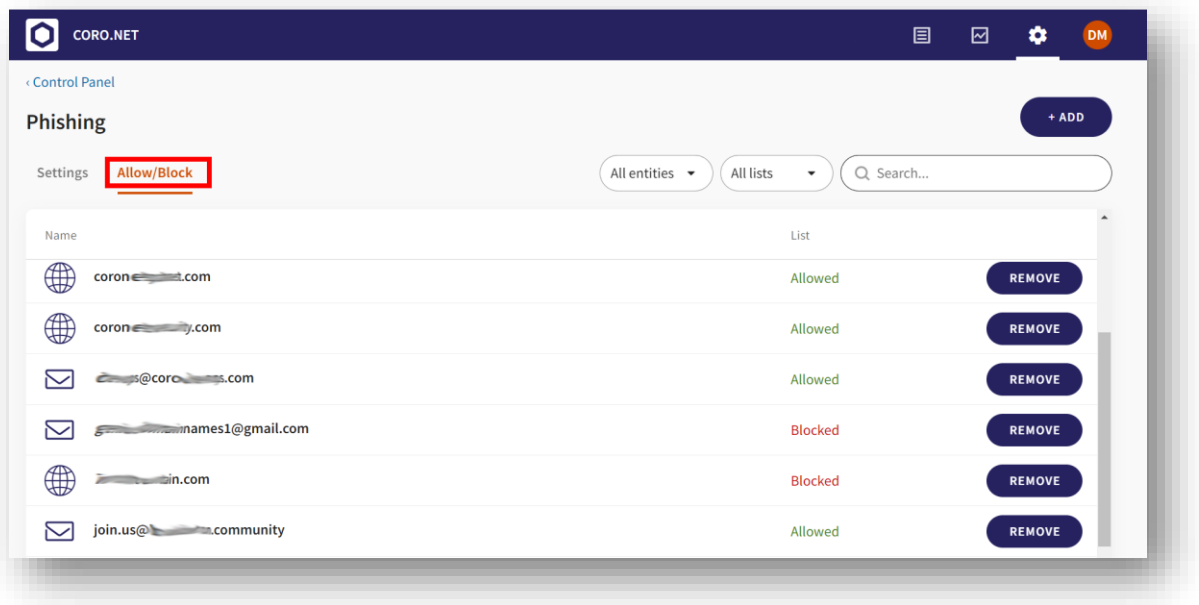
Select from several options:

- **Workspace status updates** (checked by default): Get a daily summary of open issues.
- **Critical events that require timely action** (checked by default): Get notifications for issues considered by Coro as critical that require the IT admin's timely attention.
- **Specific events** (unchecked by default): Get immediate notifications whenever a new event of this type is created.

Email phishing Allowlist/Blocklist management

Phishing is a prominent threat; its mitigation often requires either blocking or allowing messages originating from specific email addresses or domains.

The new *Allow/Block* tab, located on the *Control Panel/Phishing* settings page, allows you to easily view, search and update your email phishing Allowlist and Blocklist:

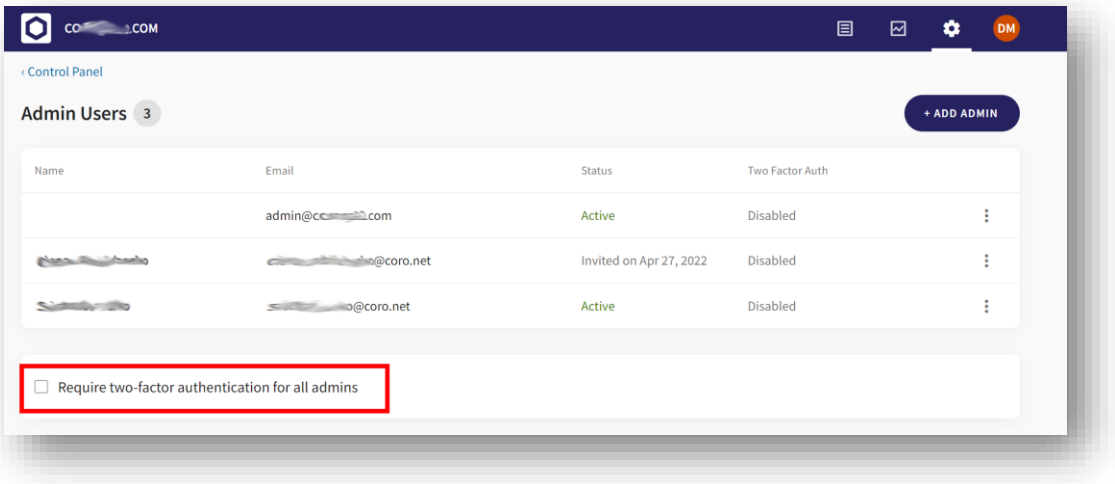


Please note that the allow and block actions will still be visible in the *Activity Logs* page.

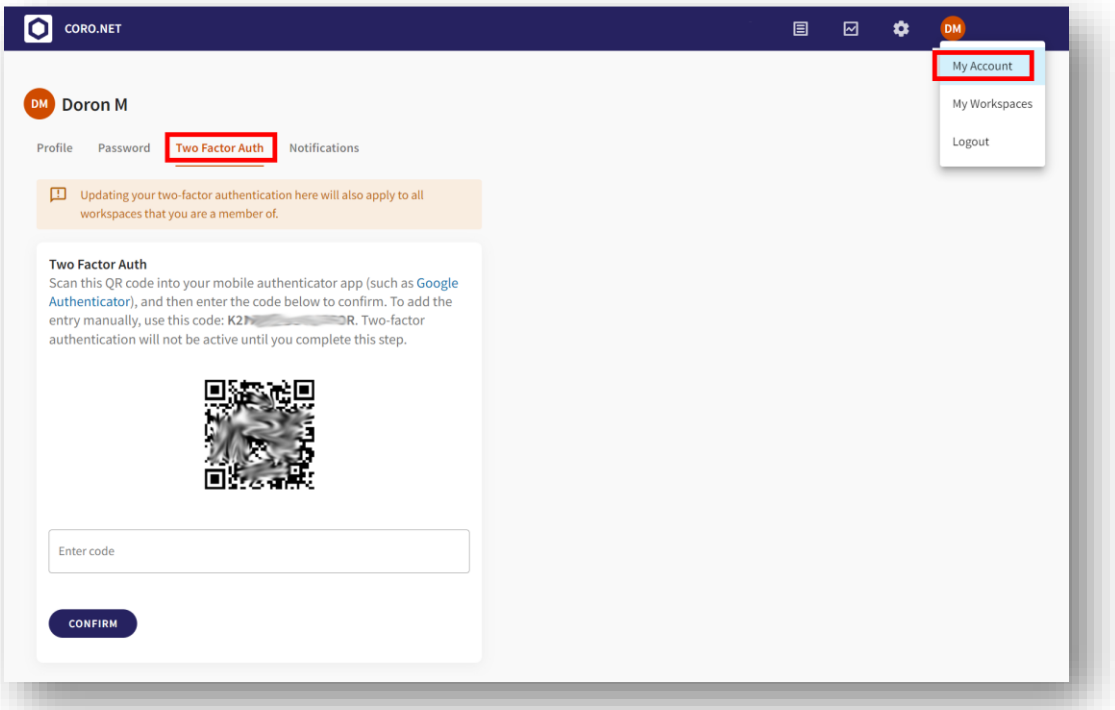
2FA access control to the Coro Console

Two-Factor Authentication (2FA) is a common method to reduce the risk of unauthorized service access.

You can now enforce 2FA for your Coro admins by checking the "*Require two-factor authentication for all admins*" on the *Control Panel/Admin Users* settings page:



To manage your own account's 2FA code, navigate to *Control Panel/Personal menu/My account* and select the new *Two Factor Auth* tab:



User-less clients

Many of our customers protect their endpoints devices with the Coro Endpoint Protection client application, greatly reducing the risks of malware, security vulnerabilities, and risky Wi-Fi networks.

Application deployment, however, can be challenging. Manual deployment that requires client activation may lack end-user knowhow or cooperation, and mass-deployment tools greatly depend on a variety of environment variables.

To help the IT team with the client deployment process and reduce friction, we have decoupled the Coro clients (the Device entity) from the end-user identity (the User entity).

No activation required

Users are no longer required to activate the client. As all installation files are unique per customer, the deployed Coro Endpoint Protection clients will be automatically associated with the customer's Coro workspace.

Simplified mass-deployment

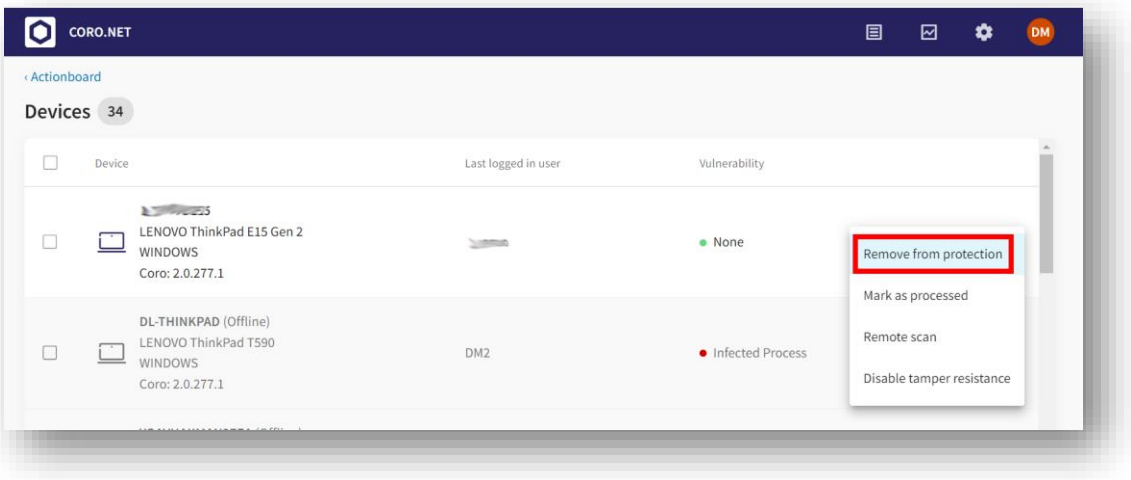
As there is no longer a requirement for an email, UPN or any other user identifier to install and activate the client, mass deployment process is much simpler and works like most other applications.

Note: Since the Coro client implements an anti-malware component, installations and driver updates will require a device reboot.

Device protection

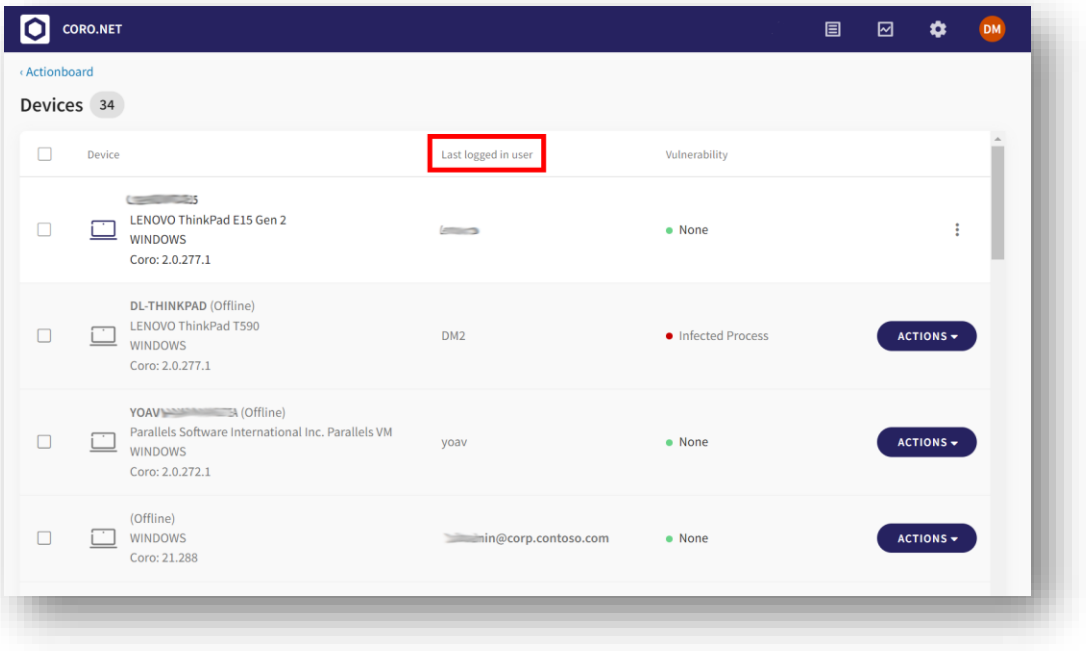
When the Coro Endpoint Protection client is installed on a device, it automatically becomes protected.

You can remove the protection from a device by navigating to the device record's menu on the Devices page:



Device list and events show available user information

The information provided in the Devices list will show information the client collected about the last logged-in user:



Device-related events will present the information of the user who was logged-in at the time of the event.

Updates do not require Admin privileges

To simplify manual updates, starting from version 1.4, updates will no longer require elevation to Admin privileges.

Please note that the update from version 1.3 to 1.4 still requires elevation.

Other Changes

Coro client information

Click on the Coro client icon in the taskbar to display the client's version number and attached domain.

Email phishing events for reported emails

Emails that users report as phishing will generate an Email Phishing event with "Reported by users" in the *Findings* field.

Updated flows for Suspected emails

If the user wishes to move an email from his Suspected folder to Inbox, he/she should mark the email as Safe using the Coro add-on (otherwise it will be returned to the Suspected folder on the next scan).

However, even if marked Safe by the user, the admin can select Discard in the console, to delete that email from the Inbox.

Emails in the Suspected folders are automatically deleted after a few days unless a user reports it as safe.