CyberGuard EDR Support Process

Date: 12 December 2024

Version: V1.23

1) Table of contents

Version 1.23 - 12/12/2024

2) Context

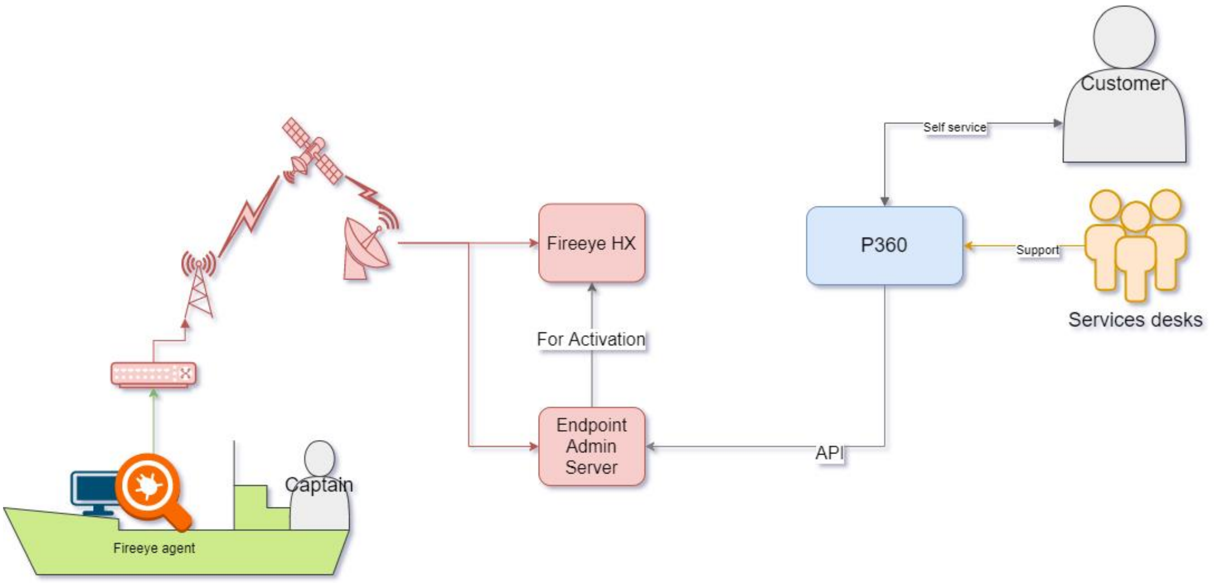
CyberGuard EDR is Marlink’s end point protection solution (similar, but superior to an Anti Virus software).

Objectives of the new solution

- Advanced EDR Protection (signature+behaviour-based, USB devices)
- Enhanced Detection (processes, machine learning, 3rd party IOC, …)
- Additional services provided by SOC: Remote Investigation (forensic acquisition), Advanced Countermeasures …
- Integration with CyberGuard Poral (Alerts, Isolation, Exclusions …)
- Satellite-optimised architecture (IT Link Master server/Clients)

	CyberGuard EDR	ESET / SkyFile AV
Technology	EPP (signature) + EDR (behavior)	Anti-virus (signature) + behaviour (Premium)
Satellite-optimised architecture	Master/Client PC architecture to distribute signature updates	Master / Client PC architecture to distribute signature updates
Device/quarantine logs	• Triage summary on demand • Forensics acquisition	N/A
CyberGuard	Correlation with CyberGuard Threat Detection / Countermeasures	N/A
Remote Management	• Device Quarantine • Remote Host remediation	N/A
USB devices	USB device policy (monitor / restrict access)	N/A

The overall architecture of the CyberGuard EDR Service is shown below.



2.1) Technical Compatibility

Supported Operating Systems and Environments	
Windows	Windows 8, 8.1, 10, 11 Server 2008R2, 2012R2, 2016, 2019, 2022

Please note: Windows 7 is no longer supported!

2.1) Onboarding Process

The CyberGuard EDR Onboarding Process is shown in Figure 1 below. After Sales has agreed on the EDR service’s contractual details, new installations are activated using the CPQ, while for existing installations CyberGuard EDR may be added through a COF. All Order Forms include CyberGuard EDR with a selection of the licence package (“5-12 PCs”, “13-20 PCs” ...).

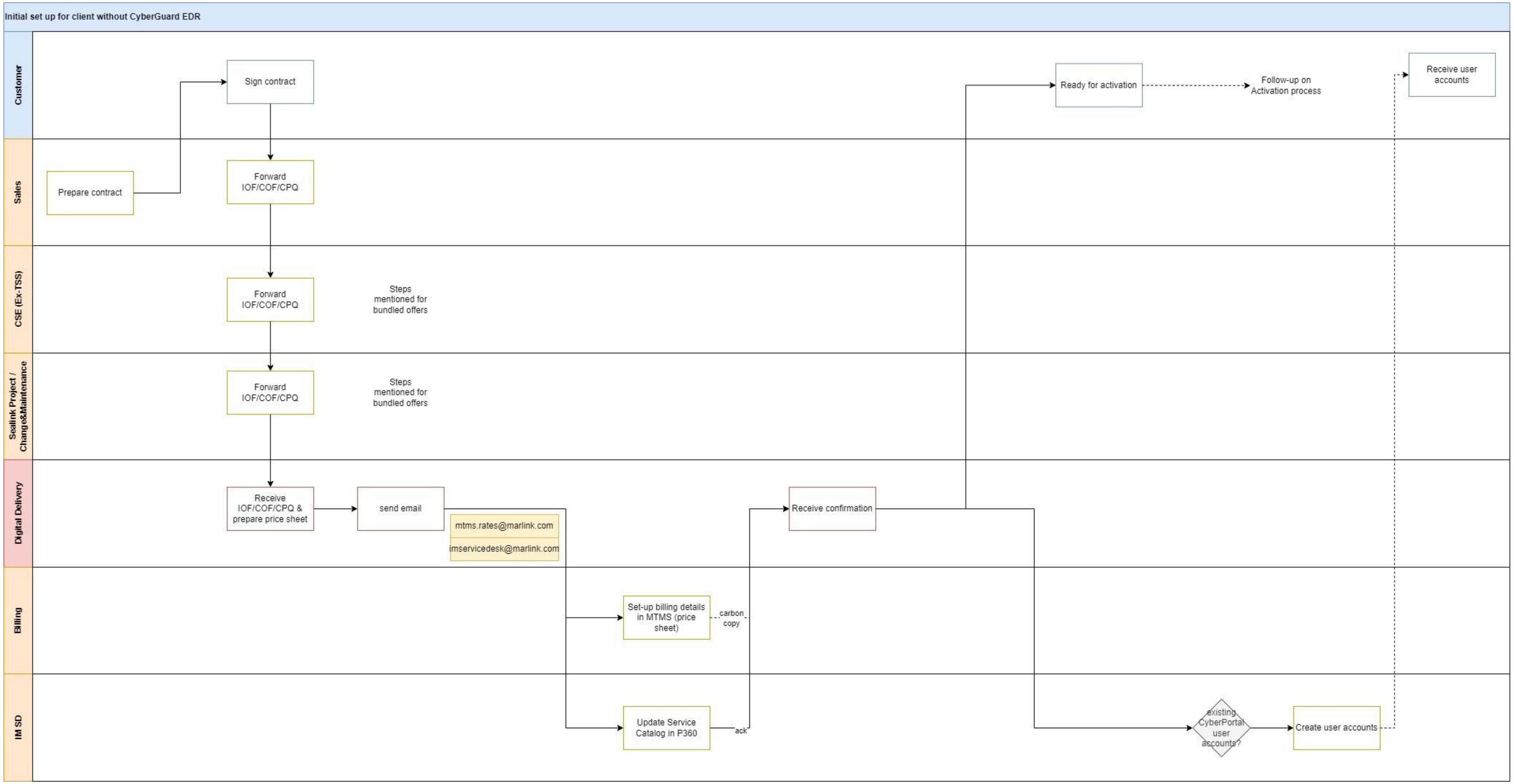

Initial set up for client without CyberGuard EDR
Customer
Sales
CSE (Ex-TSS)
Sealink Project / Change&Maintenance
Digital Delivery
Billing
IM SD
Sign contract
Ready for activation
Follow-up on Activation process
Receive user accounts
Prepare contract
Forward IOF/COF/CPQ
Forward IOF/COF/CPQ
Steps mentioned for bundled offers
Forward IOF/COF/CPQ
Steps mentioned for bundled offers
Receive IOF/COF/CPQ & prepare price sheet
send email
mtms.rates@marlink.com
imservicedesk@marlink.com
Receive confirmation
Set-up billing details in MTMS (price sheet)
carbon copy
Update Service Catalog in P360
ack
existing CyberPortal user accounts?
Create user accounts

Figure 1 – Set-up

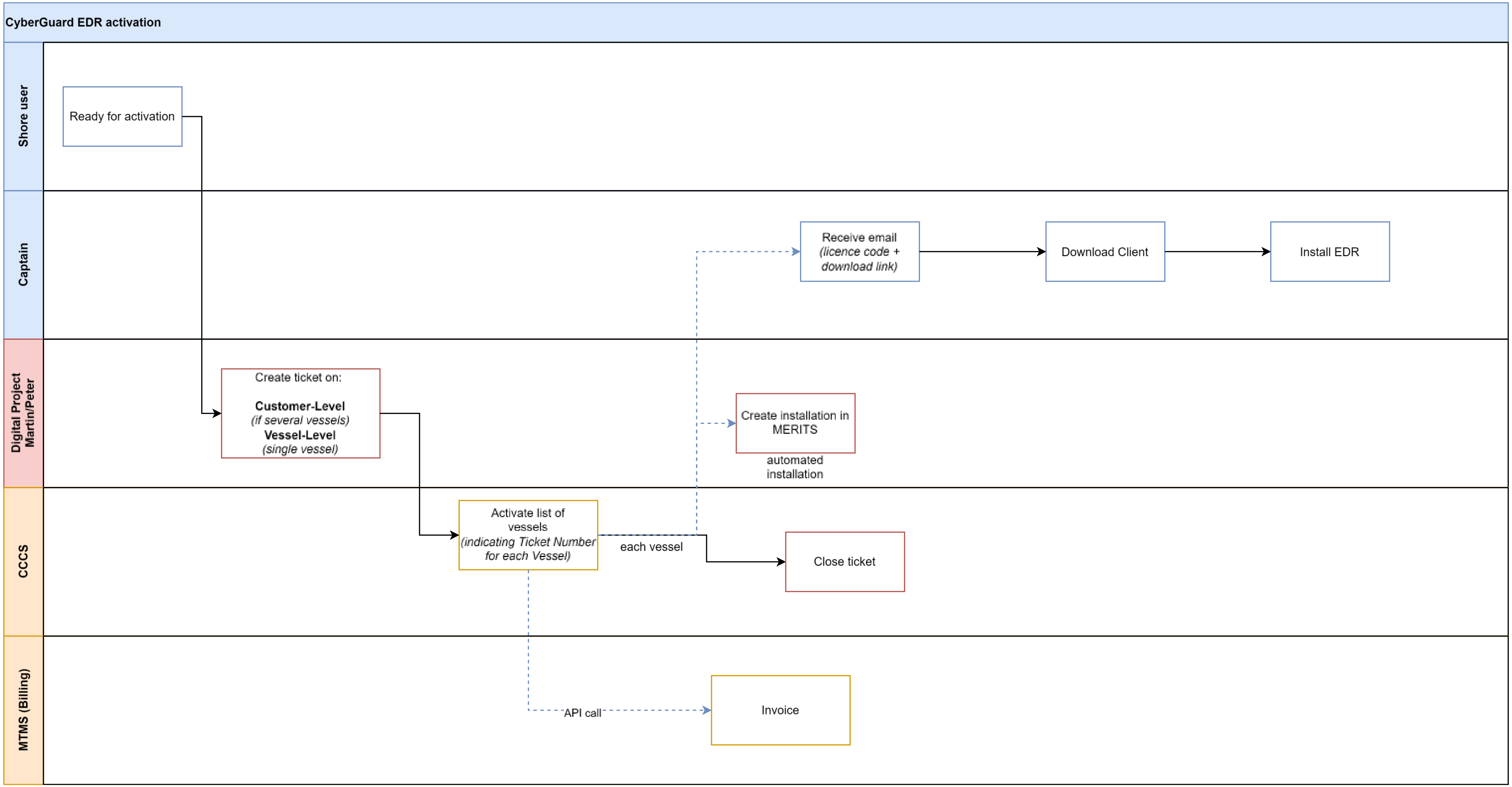

CyberGuard EDR activation
Shore user
Captain
Digital Project Martin/Peter
CCCS
MTMS (Billing)
Ready for activation
Receive email (licence code + download link)
Download Client
Install EDR
Create ticket on:
Customer-Level (if several vessels)
Vessel-Level (single vessel)
Create installation in MERITS
automated installation
Activate list of vessels (indicating Ticket Number for each Vessel)
each vessel
Close ticket
API call
Invoice

Figure 2 – Activation

2.2) Portal360 Backoffice configuration

Backoffice tasks are performed in Portal360:

Section in Portal360	Tasks
CyberGuard / EDR Services	- Service Activation / Deactivation

2.3) Outages

CyberGuard EDR uses an external provider (Trellix/FireEye) for the agent and the console, the console is hosted by Marlink.

It is Engineering task to detect any outages and Service Desk’s task to inform customers (see 8.1).

3) General Support Process

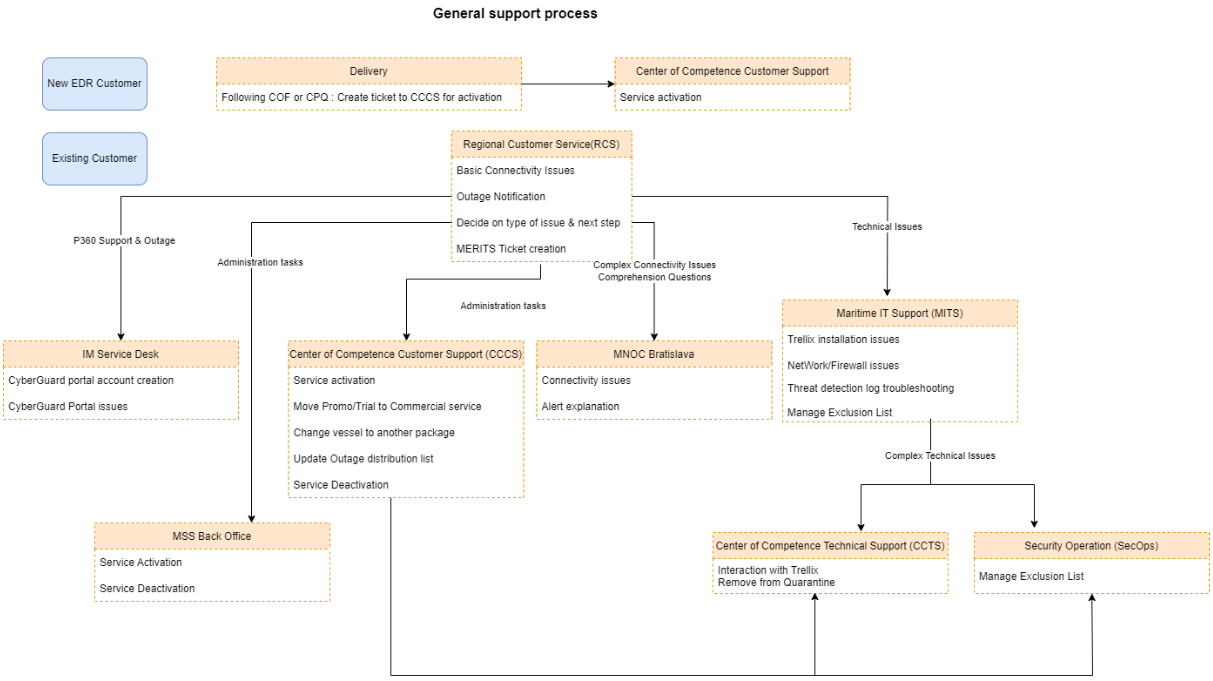

General support process
New EDR Customer
Existing Customer
Delivery
Following COF or CPQ : Create ticket to CCCS for activation
Center of Competence Customer Support
Service activation
Regional Customer Service(RCS)
Basic Connectivity Issues
Outage Notification
Decide on type of issue & next step
MERITS Ticket creation
P360 Support & Outage
Administration tasks
Administration tasks
Complex Connectivity Issues
Comprehension Questions
Technical Issues
IM Service Desk
CyberGuard portal account creation
CyberGuard Portal issues
Center of Competence Customer Support (CCCS)
Service activation
Move Promo/Trial to Commercial service
Change vessel to another package
Update Outage distribution list
Service Deactivation
MNOC Bratislava
Connectivity issues
Alert explanation
Maritime IT Support (MITS)
Trellix installation issues
NetWork/Firewall issues
Threat detection log troubleshooting
Manage Exclusion List
Complex Technical Issues
MSS Back Office
Service Activation
Service Deactivation
Center of Competence Technical Support (CCTS)
Interaction with Trellix
Remove from Quarantine
Security Operation (SecOps)
Manage Exclusion List

Figure 3 - general support process

3.1) Order process lifecycle

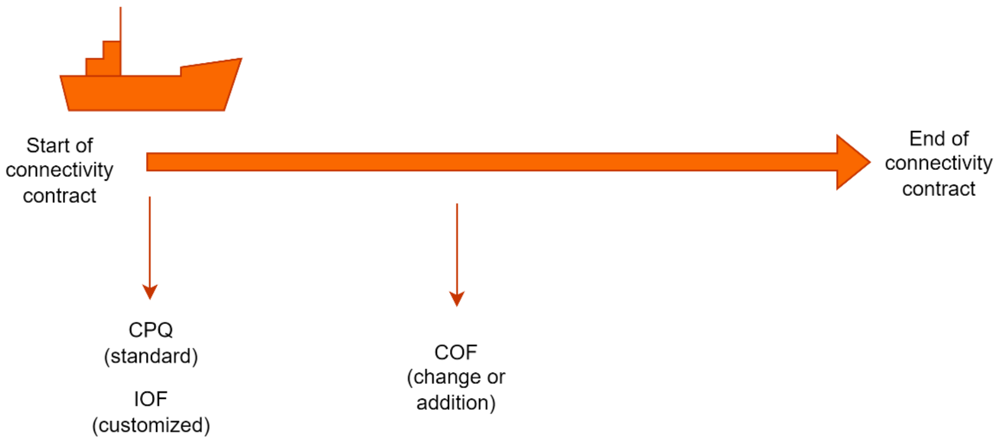


Figure 4 - different kind of orders

CPQ: Configuration Price Quote, for standard connectivity, may include CyberGuard EDR

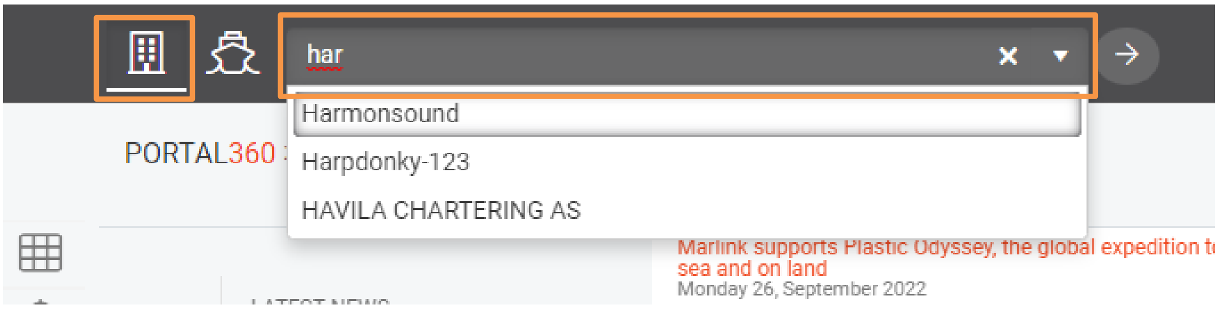
IOF: Installation Order Form, for customized connectivity solution, may include CyberGuard EDR

COF: Change Order Form, for change and additional services, like CyberGuard EDR, after the initial contract

3.2) Check subscription status

In case a customer ticket for CyberGuard EDR is raised, it may be required for several Marlink Customer Support teams to check the current customer subscription status.

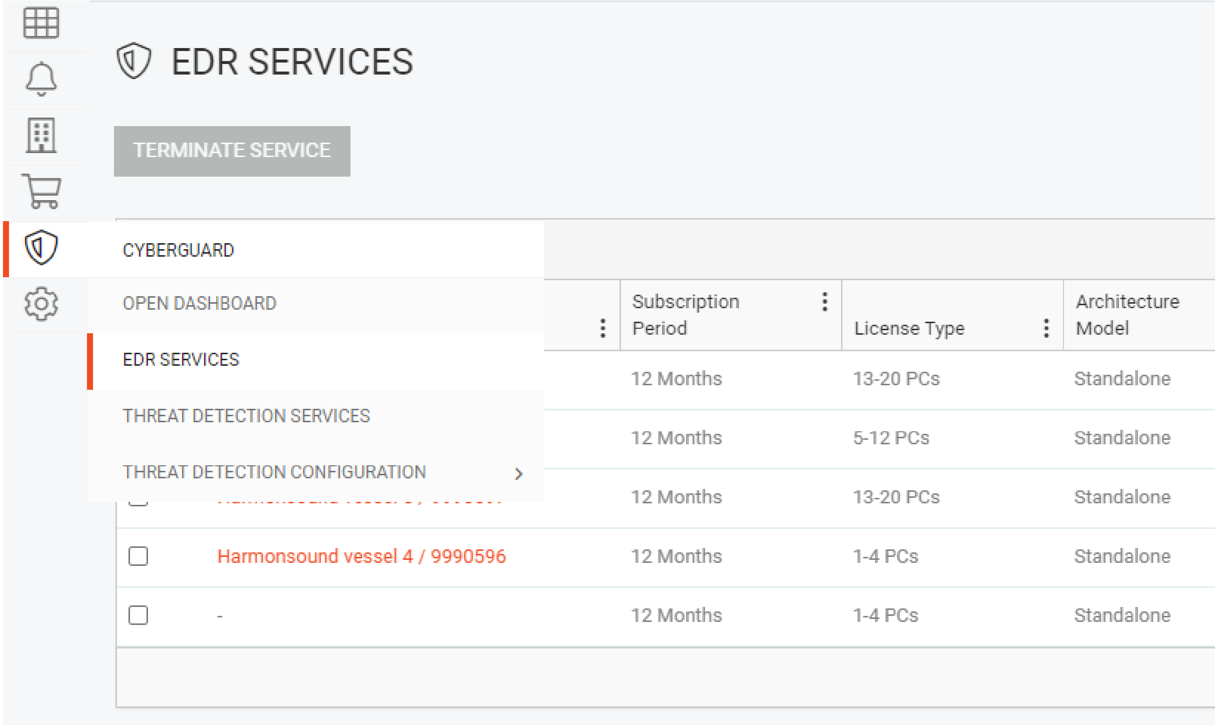
Navigate to the relevant subcompany on Portal360 by selecting the “headquarter” icon and using the search field:



Marlink supports Plastic Odyssey, the global expedition t
sea and on land
Monday 26, September 2022

Figure 5: Subcompany search in Portal360

In the **“CyberGuard”** submenu, select **“EDR Services”**. In the table, you will see all active subscriptions.



		Subscription Period	License Type	Architecture Model
		12 Months	13-20 PCs	Standalone
		12 Months	5-12 PCs	Standalone
		12 Months	13-20 PCs	Standalone
☐	Harmonsound vessel 4 / 9990596	12 Months	1-4 PCs	Standalone
☐	-	12 Months	1-4 PCs	Standalone

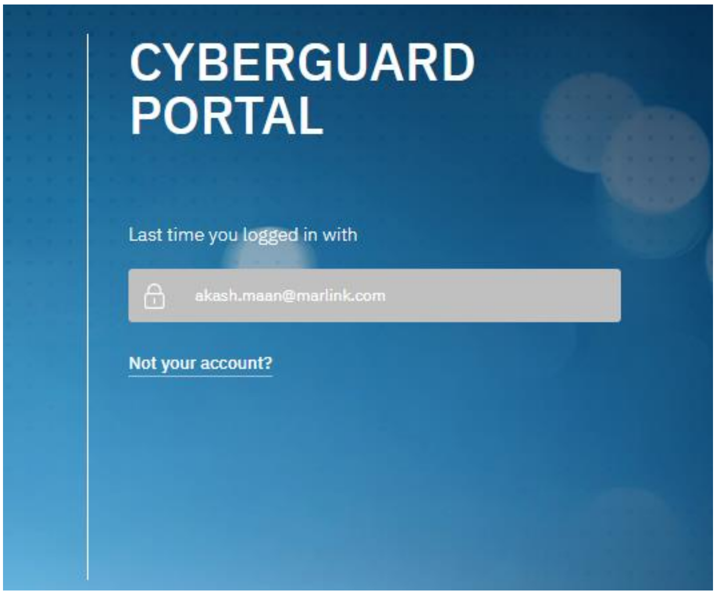
Figure 6: EDR Services subscriptions overview

3.3) Check installation status

It may be required for several Marlink Customer Support teams to check the installation status of CyberGuard EDR on the ship stations.

Change to the relevant company on the CyberGuard Portal by clicking on the current company name in the upper right corner:

Switch Company | Marlink CyberGuard

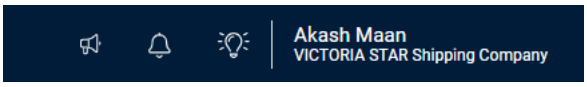


CYBERGUARD PORTAL

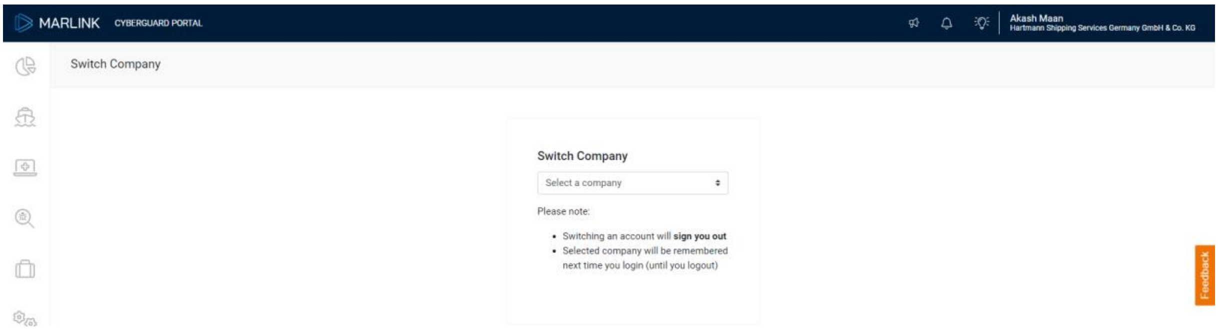
Last time you logged in with

akash.maan@marlink.com

Not your account?



Akash Maan
VICTORIA STAR Shipping Company



MARLINK CYBERGUARD PORTAL

Akash Maan
Hartmann Shipping Services Germany GmbH & Co. KG

Switch Company

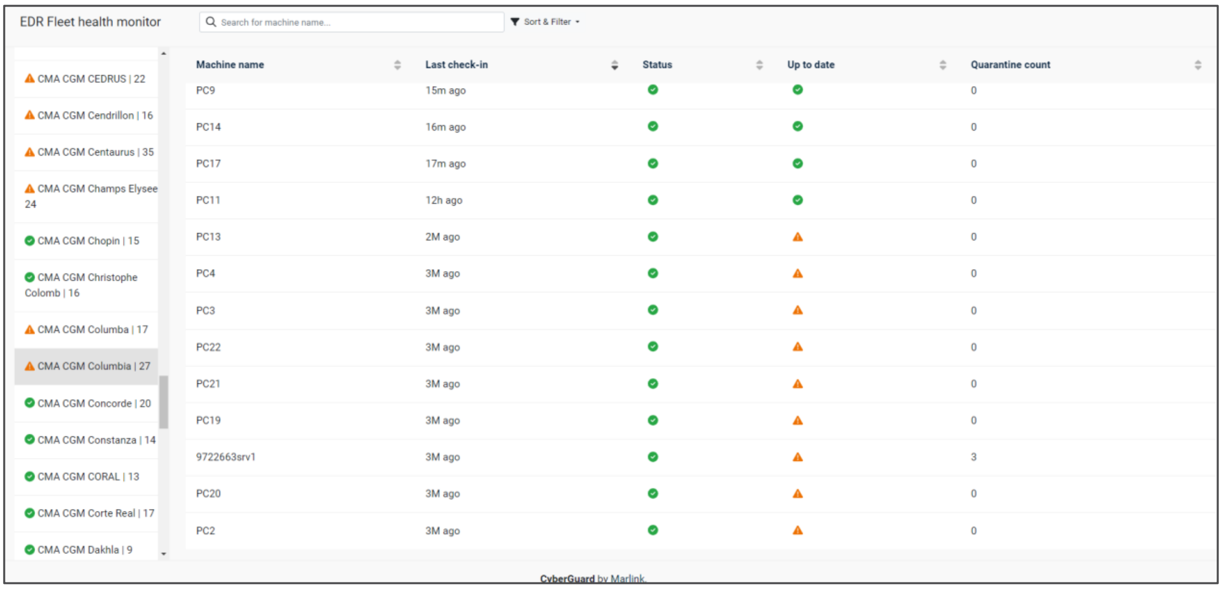
Switch Company

Select a company

Please note:

- Switching an account will **sign you out**
- Selected company will be remembered next time you login (until you logout)

You can now check the status of the installation for each computer, in the status column. You can filter the computer per vessel by using the column on the left.



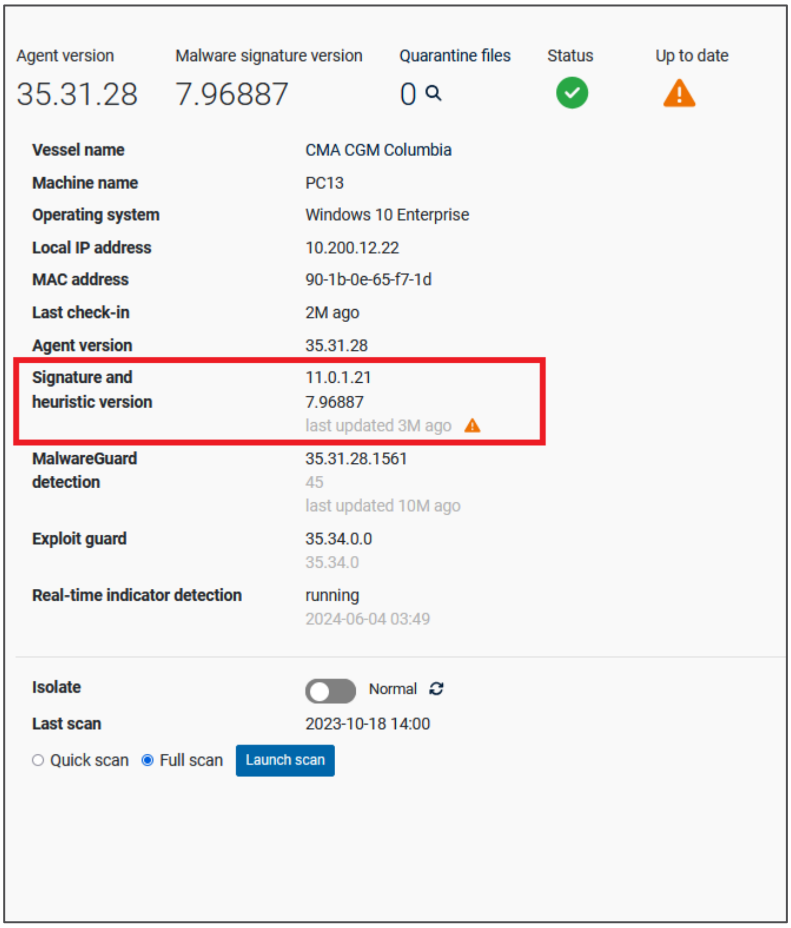
EDR Fleet health monitor

- ⚠ CMA CGM CEDRUS | 22
- ⚠ CMA CGM Cendrillon | 16
- ⚠ CMA CGM Centaurus | 35
- ⚠ CMA CGM Champs Elysee 24
- ✓ CMA CGM Chopin | 15
- ✓ CMA CGM Christophe Colomb | 16
- ⚠ CMA CGM Columba | 17
- ⚠ CMA CGM Columbia | 27
- ✓ CMA CGM Concorde | 20
- ✓ CMA CGM Constanza | 14
- ✓ CMA CGM CORAL | 13
- ✓ CMA CGM Corte Real | 17
- ✓ CMA CGM Dakhla | 9

Machine name	Last check-in	Status	Up to date	Quarantine count
PC9	15m ago	✓	✓	0
PC14	16m ago	✓	✓	0
PC17	17m ago	✓	✓	0
PC11	12h ago	✓	✓	0
PC13	2M ago	✓	⚠	0
PC4	3M ago	✓	⚠	0
PC3	3M ago	✓	⚠	0
PC22	3M ago	✓	⚠	0
PC21	3M ago	✓	⚠	0
PC19	3M ago	✓	⚠	0
9722663srv1	3M ago	✓	⚠	3
PC20	3M ago	✓	⚠	0
PC2	3M ago	✓	⚠	0

CyberGuard by Marlink

By clicking on the vessel, a sidebar will open which shows additional information on the exact modules which are outdated:



Agent version	Malware signature version	Quarantine files	Status	Up to date
35.31.28	7.96887	0	✓	⚠

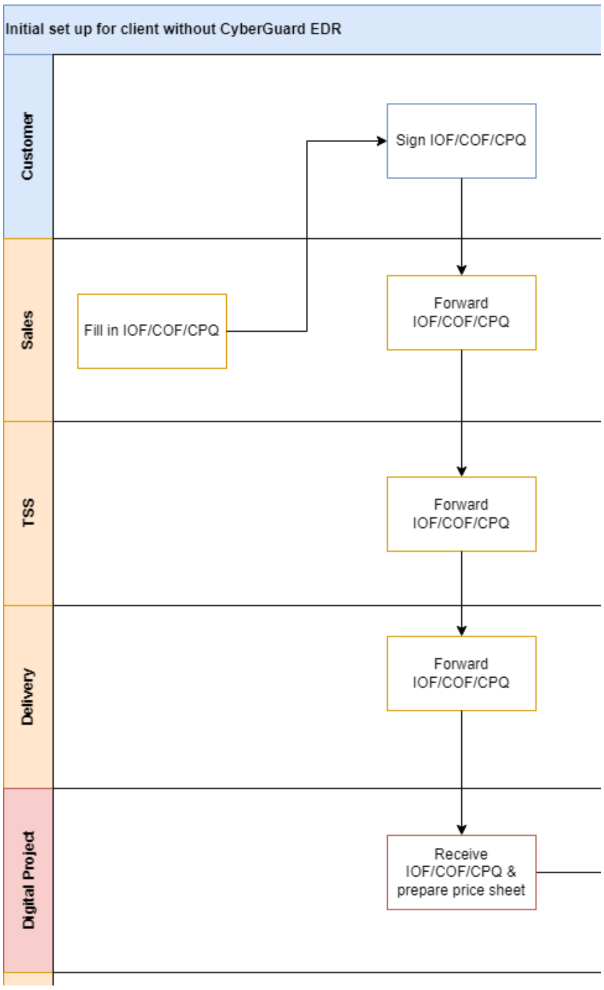
Vessel name	CMA CGM Columbia
Machine name	PC13
Operating system	Windows 10 Enterprise
Local IP address	10.200.12.22
MAC address	90-1b-0e-65-f7-1d
Last check-in	2M ago
Agent version	35.31.28
Signature and heuristic version	11.0.1.21 7.96887 last updated 3M ago ⚠
MalwareGuard detection	35.31.28.1561 45 last updated 10M ago
Exploit guard	35.34.0.0 35.34.0
Real-time indicator detection	running 2024-06-04 03:49

Isolate	Normal
Last scan	2023-10-18 14:00

○ Quick scan ● Full scan

4) Maritime Project

Following the validation of the Order Form (CPQ for Sealink Standardized, IOF for Sealink Customized or COF for both existing installations), Maritime Project Delivery will forward the information to Digital Delivery at digital.delivery@marlink.com.

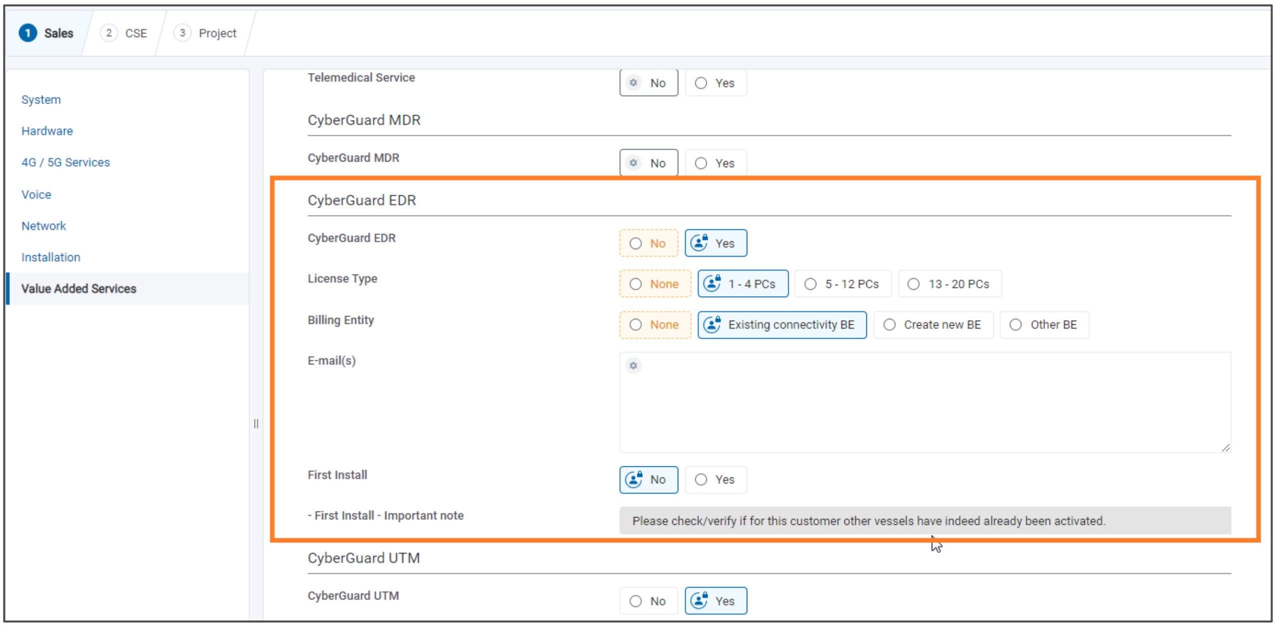


5) Digital Delivery

5.1) Digital Delivery Tasks

Following the validation of the Order Form (CPQ for Sealink Standardized, IOF for Sealink Customized or COF for both existing installations), Maritime Project Delivery will forward the information to Digital Delivery. Digital Delivery will get the information from the order forms, prepare the service catalogue and send them to Billing and IM, and upon confirmation create a ticket for activation to CCCS.

Alongside the service catalogue sent to IM, Digital Delivery will ask IM Service Desk to create CyberGuard Portal user accounts as per 6.3)



Telemedical Service: ● No ○ Yes

CyberGuard MDR

CyberGuard MDR: ● No ○ Yes

CyberGuard EDR

CyberGuard EDR: ○ No ● Yes

License Type: ○ None ● 1 - 4 PCs ○ 5 - 12 PCs ○ 13 - 20 PCs

Billing Entity: ○ None ● Existing connectivity BE ○ Create new BE ○ Other BE

E-mail(s):

First Install: ● No ○ Yes

- First Install - Important note: Please check/verify if for this customer other vessels have indeed already been activated.

CyberGuard UTM

CyberGuard UTM: ○ No ● Yes

Figure 7: CyberGuard EDR Option in the CPQ

Please create a ticket to CCCS to activate CyberGuard EDR on the fleet, stating:

- Vessel Name
- Package: 1-4 PCs, 5-12 PCs, 13+ PCs
- Billing Entity ID
- Email address
  - To receive the licence (On Shore or On Vessel)
  - Customer IT Dept. (On Shore)
    - To be informed in case of an outage
    - To access CyberGuard Portal
- Company under which CyberGuard EDR is to be activated under

Please Note: Please sent the above information to Digital Delivery **via Email** and update the information in the merits ticket. Please allow a minimum processing time of **24hrs** for issuing a EDR licence by the Digital Delivery team.

5.2) Service Catalogue missing

A customer service catalogue may be missing in two scenarios:

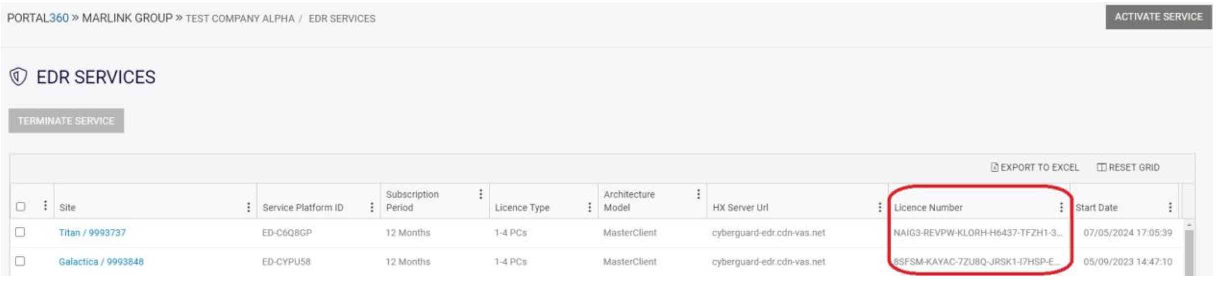
1. The checkbox “First installation of CyberGuard EDR for this customer” has been ticked in the order form. Therefore, it is normal that the service catalogue has not yet been set up.
2. You are contacted with a message with subject: “[CyberGuard] service catalogue missing for client <fill in the name>”
   - ➢ This might occur if the checkbox listed above was not ticked in the Order Form and CCCS is therefore unable to activate the vessel

In both cases, please forward the message to IM Service Desk with the subject: “[CyberGuard service catalogue missing for client <fill in the name>” and add the missing service catalogue as an attachment.

5.3) EDR Licence Details

CyberGuard EDR licence details can be retrieved when you navigate to Portal 360 > select a company > CyberGuard > EDR Services

Here you will find the EDR licence key for the vessel.



PORTAL360 » MARLINK GROUP » TEST COMPANY ALPHA / EDR SERVICES

□	Site	Service Platform ID	Subscription Period	Licence Type	Architecture Model	HX Server Url	Licence Number	Start Date
□	Titan / 9993737	ED-C6Q8GP	12 Months	1-4 PCs	MasterClient	cyberguard-edr.cdn-vas.net	NAIG3-REVPW-KLORH-H6437-TFZH1-3...	07/05/2024 17:05:39
□	Galactica / 9993848	ED-CYPU58	12 Months	1-4 PCs	MasterClient	cyberguard-edr.cdn-vas.net	8SFSM-KAYAC-7ZU8Q-JRSK1-I7HSP-E...	05/09/2023 14:47:10

6) IM Service Desk Tasks

6.1) Portal360 Support

As explained in chapter 7.7), Portal360 issues may concern either the customer-facing CyberGuard Portal (https://cyber.apps.marlink.io) or the backoffice administration in Portal360.

Please try to troubleshoot any tickets you receive for obvious root-causes (*e.g. Is the customer actually subscribed? Is an Outage ongoing? etc*). If you believe there is a deeper technical issue, you may contact the following IM colleagues as Third Line:

Portal	Third Line Contact
CyberGuard EDR Backoffice Administration in Portal360	Enzo Metroz Enzo.Metroz@marlink.com

6.2) Data Quality

IM Service desk can coordinate the actions to correct outdated information (vessels attached to the wrong company), but the KAM should always be informed as he/she is the owner of the customer data.

6.3) CyberGuard Portal User Account Creation

Please ensure that the request clearly states:

- Requested User Account mail address
- Companies the new user should have access to

If either is missing, please reach out to the requester for clarification.

IM Service Desk may create / modify accounts in the **Users & Role** section in the **Auth0 Portal**: https://manage.auth0.com/dashboard/eu/marlink/ . See separate user management document.

In case of any issue, please reach out to:

Portal	Third Line Contact
CyberGuard Portal *(customer-facing)* ➢ Incl: user account creation	Juliën Hanssens Julien.Hanssens@marlink.com

7) CCCS Tasks

7.1) Update Outage distribution list

Please request a generic email address from the shipping company on shore side and reach out to **Katrin Lerchenmüller** (KATRIN.LERCHENMUELLER@MARLINK.COM) and **Martina Benkert** (MARTINA.BENKERT@MARLINK.COM) with a request to add it to the CyberGuard EDR outage distribution list.

7.2) Service Activation

In most cases, CCCS will receive a MERITS ticket from Delivery / Project to activate a vessel because it has been selected in the Order Form (CPQ / IOF / COF), see chapter 5)

You need to switched to the relevant subcompany

Activation on Marlink Group is <u>not</u> possible

In the Portal360 CyberGuard section, select **“EDR Services”** and click the **“Activate Service”** button.

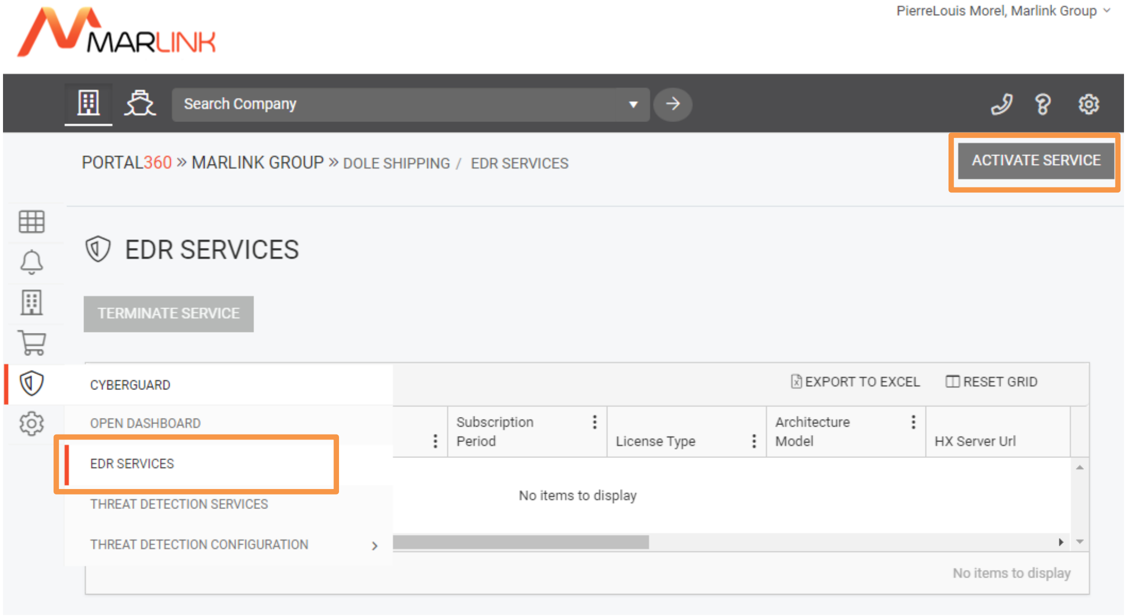
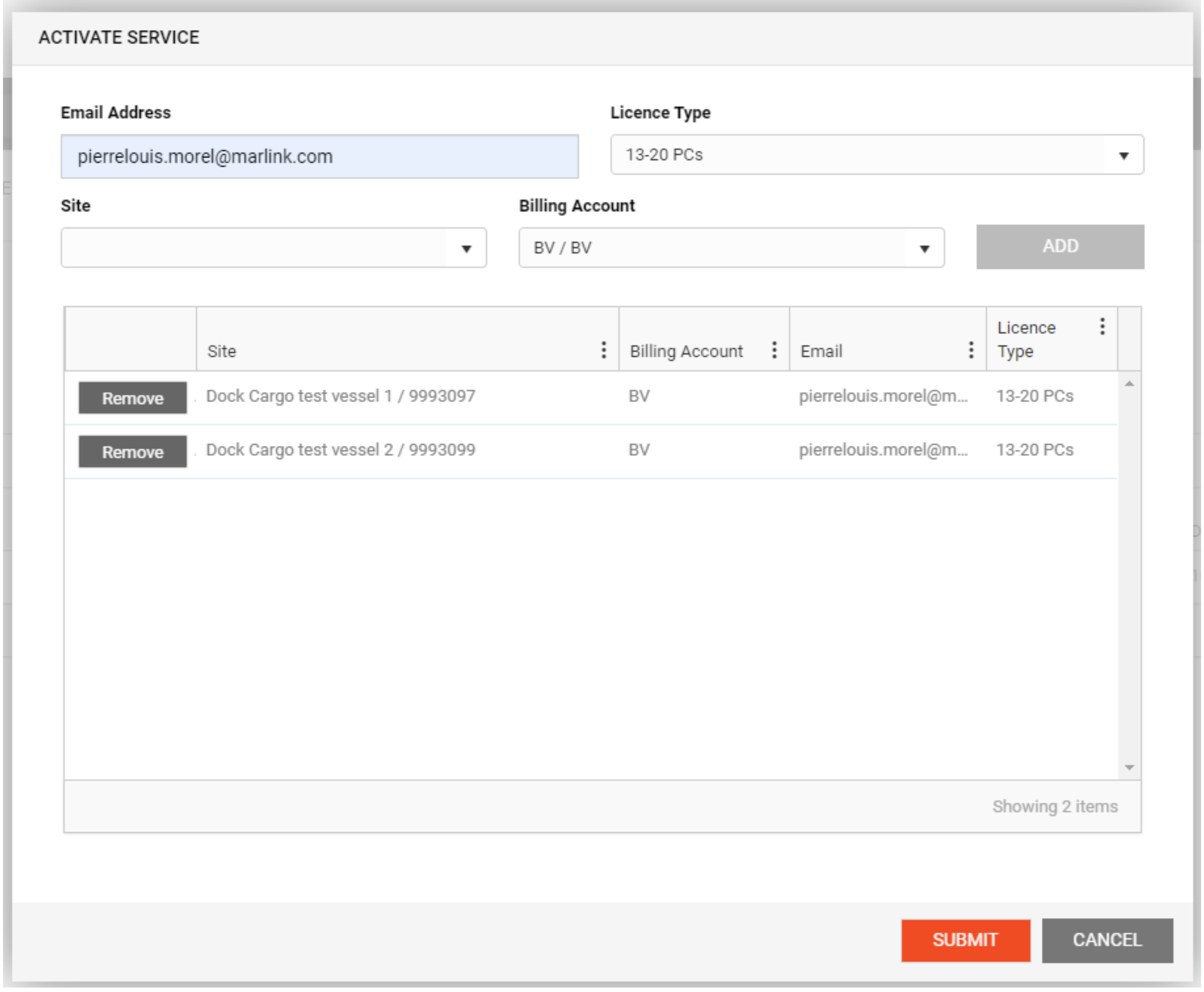


Figure 8: EDR Service Activation in Portal360

The following pop-up will appear:



ACTIVATE SERVICE

Email Address: pierrelouis.morel@marlink.com

Licence Type: 13-20 PCs

Site:

Billing Account: BV / BV

	Site	Billing Account	Email	Licence Type
Remove	Dock Cargo test vessel 1 / 9993097	BV	pierrelouis.morel@m...	13-20 PCs
Remove	Dock Cargo test vessel 2 / 9993099	BV	pierrelouis.morel@m...	13-20 PCs

Showing 2 items

Figure 9: EDR Activation Pop-Up

Please select:

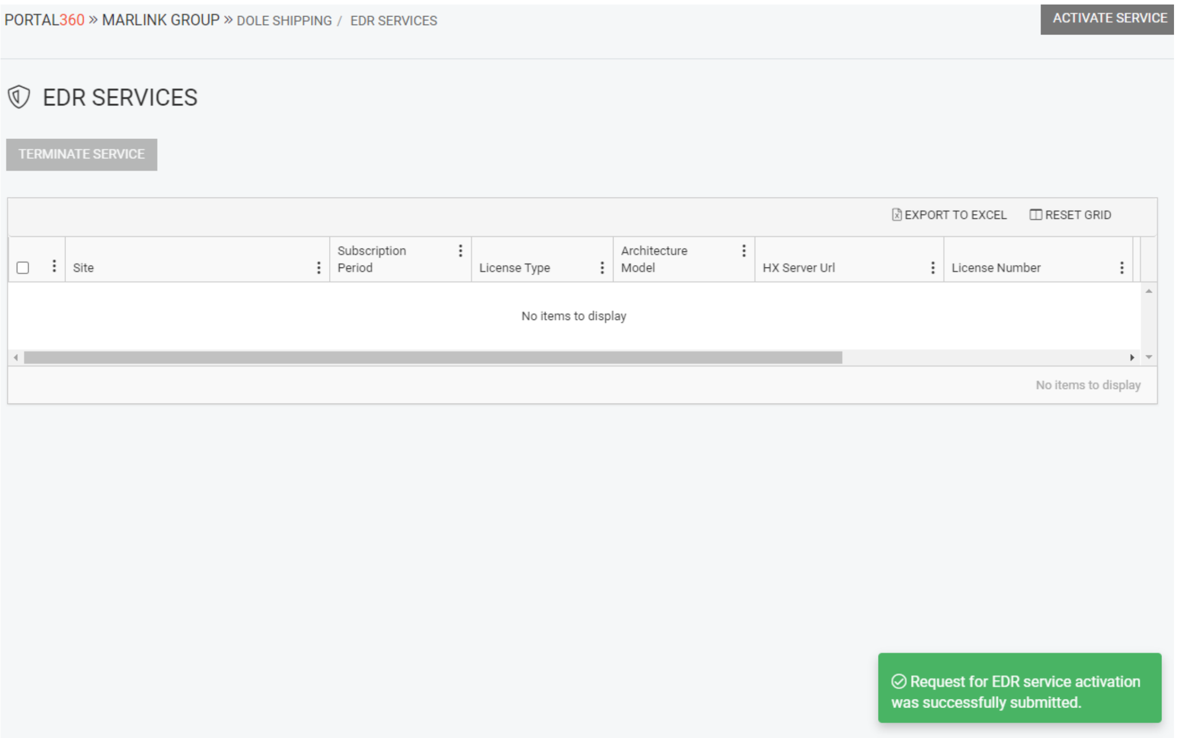
- Vessel: Select the vessel indicated in your MERITS ticket
- Billing Account: Select the billing account indicated in your MERITS ticket
  - ➢ Billing account should have been created during setup
- Email Address: Select the email address of the vessel that can be found in MERITS, multiple email address can be filled, separated by a ; (semicolon). Up to 5 email addresses can be filled.
- Licence type: Select the licence type indicated in your MERITS ticket

7.2.1) Vessel missing in the drop down list

If a vessel is missing in the drop down list, it may be due to outdated data, with the vessel not yet linked to the company.

IM Service Desk can help with the coordination of effort to ensure that the data is up to date in all systems, see 6.2)

After activation, you should see a confirmation message on the bottom right screen:



□	Site	Subscription Period	License Type	Architecture Model	HX Server Url	License Number

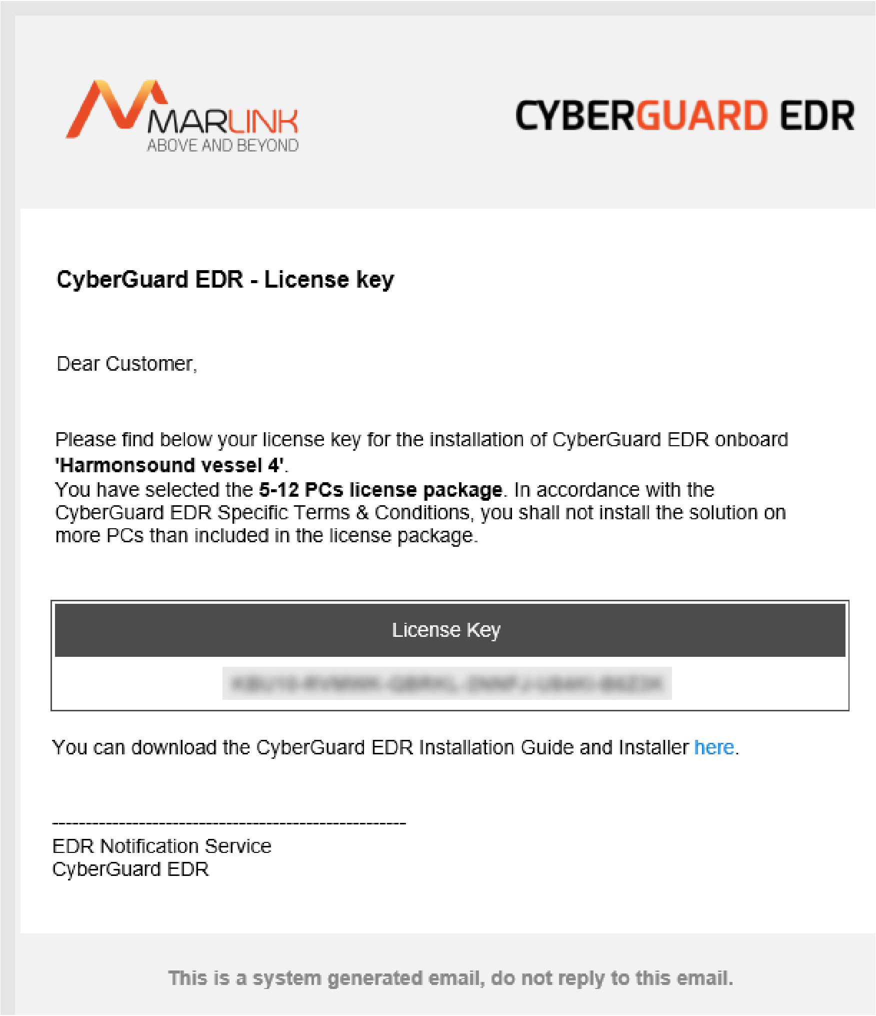
No items to display

No items to display

Request for EDR service activation was successfully submitted.

Figure 10: Service Activation confirmation message

The client will receive a mail with a link to the installation documentation and the installer (see Figure 11 - Activation mail & Figure 12 - https://marlink.com/cyberguard-edr/).



CyberGuard EDR - License key

Dear Customer,

Please find below your license key for the installation of CyberGuard EDR onboard **'Harmonsound vessel 4'**.
You have selected the **5-12 PCs license package**. In accordance with the CyberGuard EDR Specific Terms & Conditions, you shall not install the solution on more PCs than included in the license package.

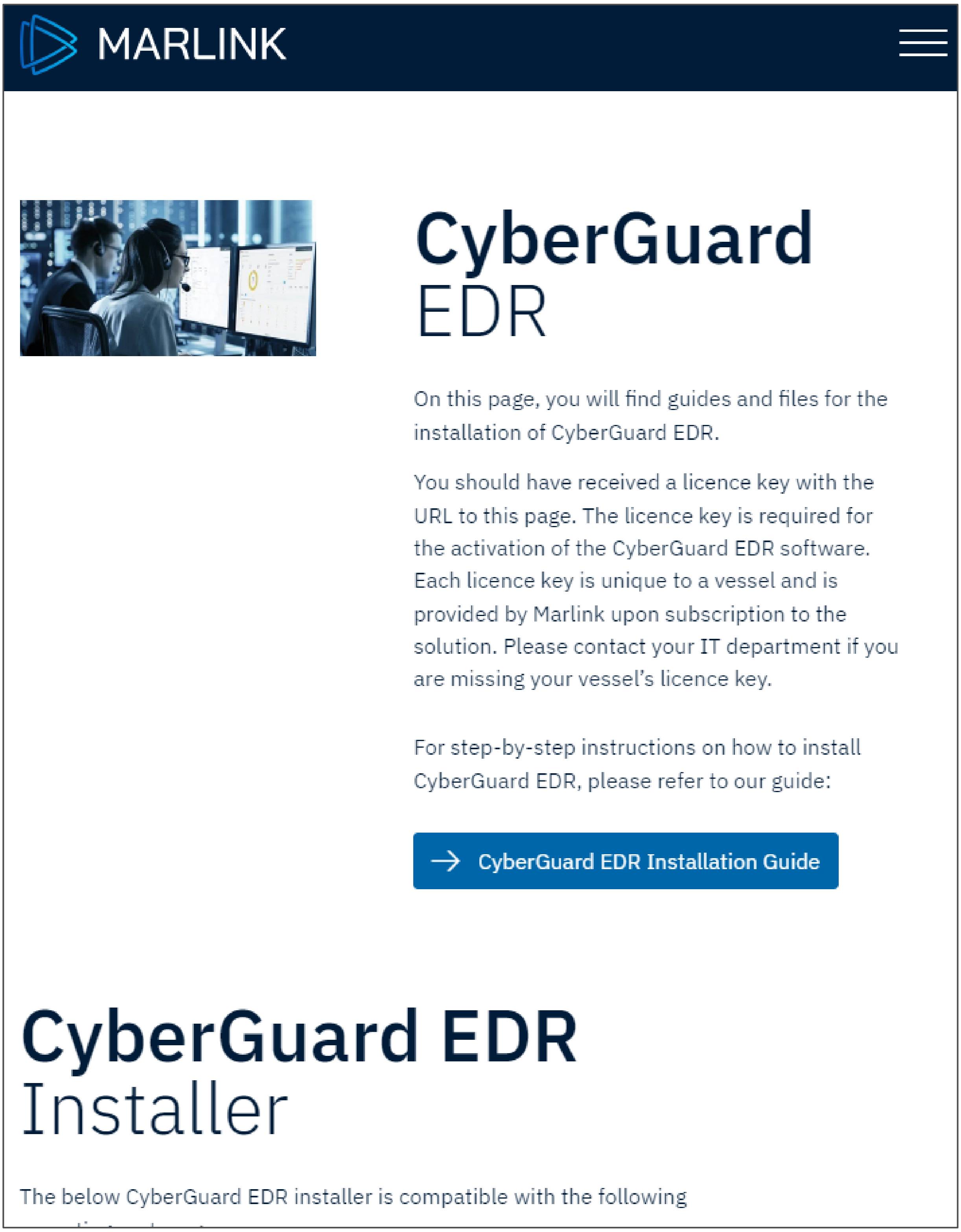
License Key
[redacted]

You can download the CyberGuard EDR Installation Guide and Installer here.

EDR Notification Service
CyberGuard EDR

This is a system generated email, do not reply to this email.

Figure 11 - Activation mail



CyberGuard EDR

On this page, you will find guides and files for the installation of CyberGuard EDR.

You should have received a licence key with the URL to this page. The licence key is required for the activation of the CyberGuard EDR software. Each licence key is unique to a vessel and is provided by Marlink upon subscription to the solution. Please contact your IT department if you are missing your vessel's licence key.

For step-by-step instructions on how to install CyberGuard EDR, please refer to our guide:

CyberGuard EDR Installer

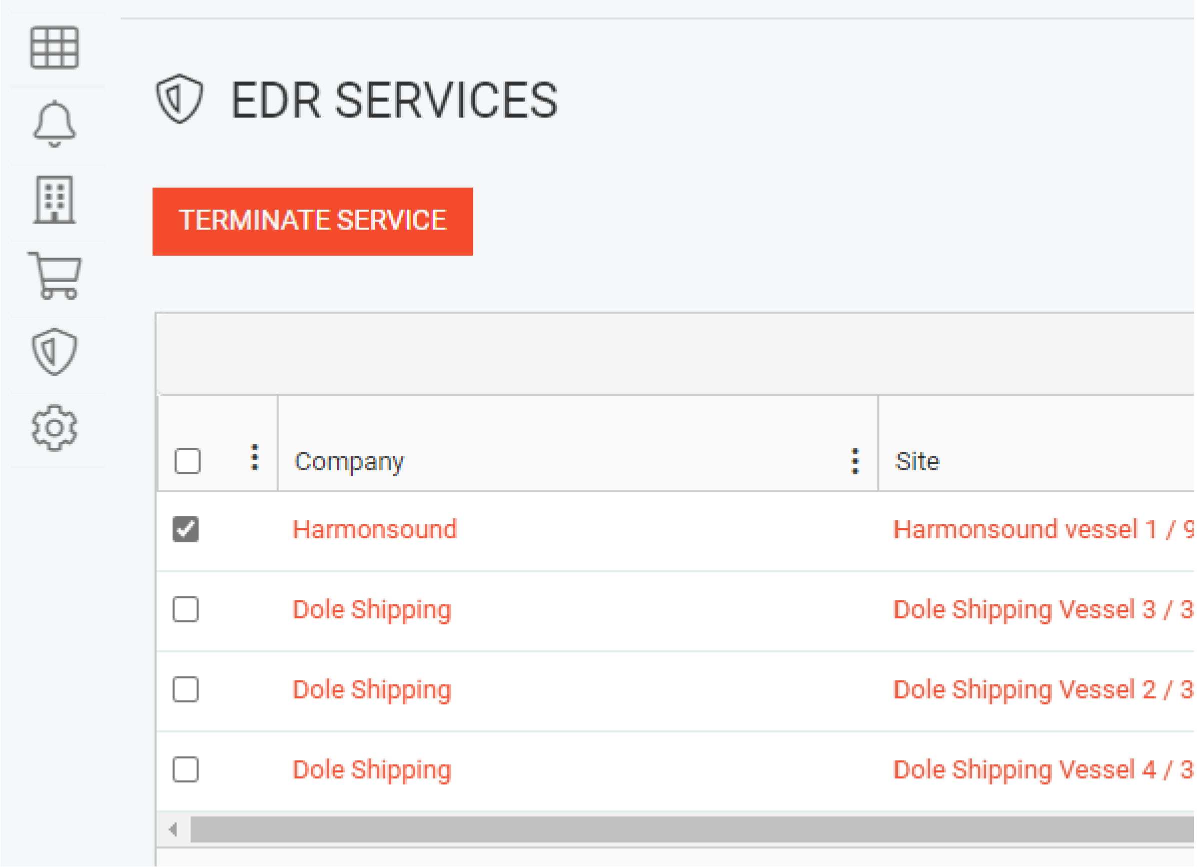
The below CyberGuard EDR installer is compatible with the following

Figure 12 - https://marlink.com/cyberguard-edr/

See chapter 8.2.1) on how to check the implementation status.

7.3) Service Termination

In the Portal360 CyberGuard section, select **"EDR Services"**, **tick the checkbox for the affected vessel** and click the **"Terminate Service"** button:

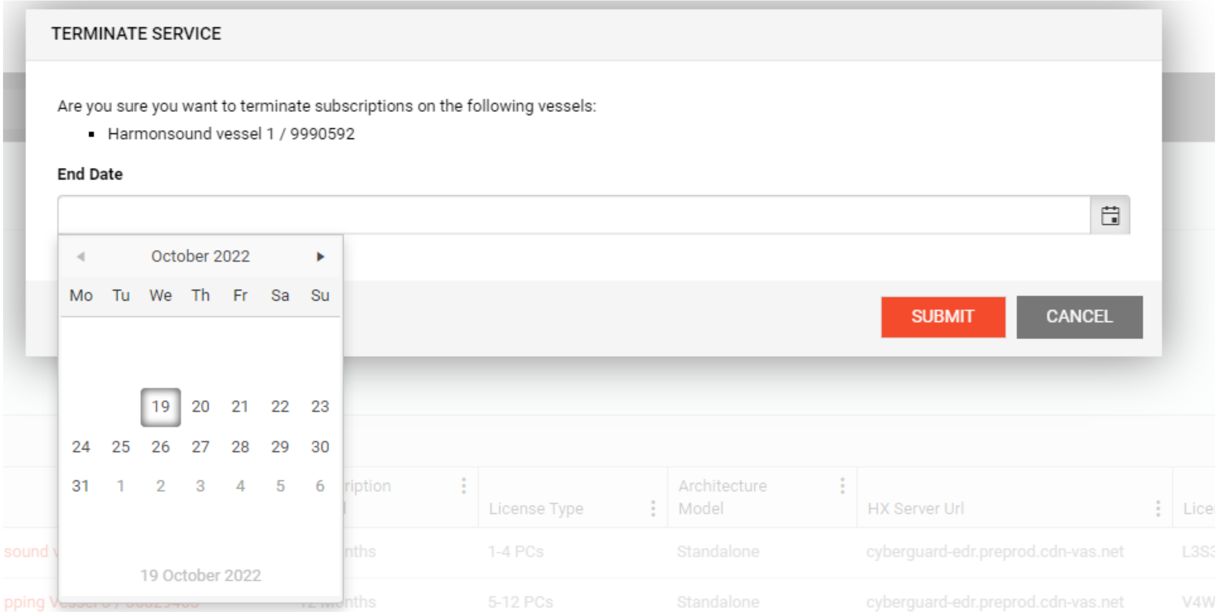


EDR SERVICES

TERMINATE SERVICE

□	Company	Site
☑	Harmonsound	Harmonsound vessel 1 / 9
□	Dole Shipping	Dole Shipping Vessel 3 / 3
□	Dole Shipping	Dole Shipping Vessel 2 / 3
□	Dole Shipping	Dole Shipping Vessel 4 / 3

Select the requested service **End Date** and **click "Submit"**:



TERMINATE SERVICE

Are you sure you want to terminate subscriptions on the following vessels:

- Harmonsound vessel 1 / 9990592

End Date

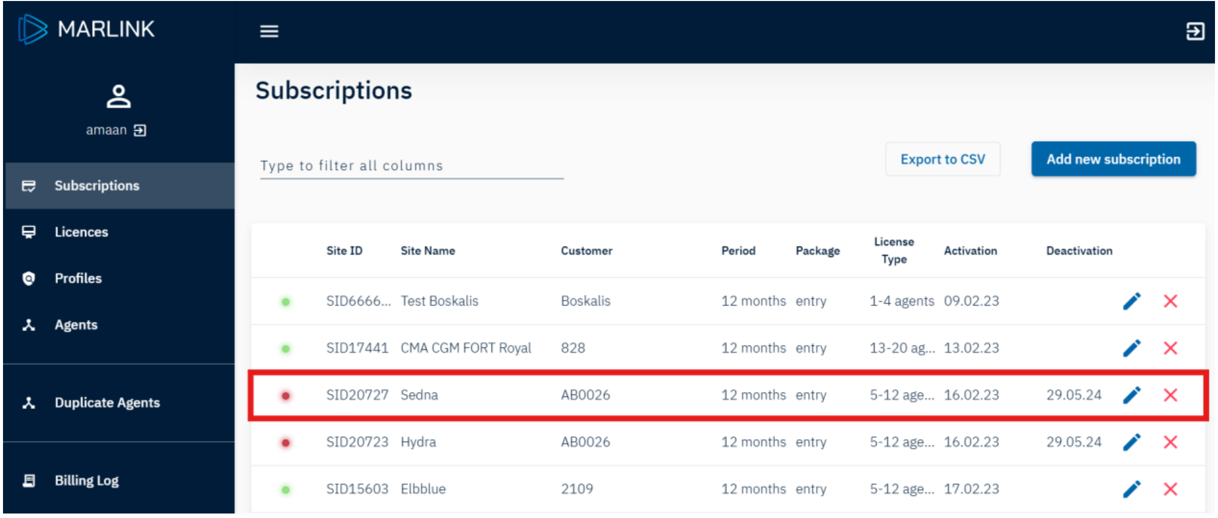
7.4) Vessel owner change

When a vessel is requested for an owner change, it is required to deactivate the EDR subscription under the former owner and reactivate it under the new owner, which will generate a new EDR licence code.

Please make the vessel aware that the EDR onboard will have to be uninstalled and reinstalled with the new licence code.

The following steps should be followed:

1. Deactivate the EDR subscription of the vessel in Portal360
2. Connect to EAS and navigate to the "Subscriptions" page
3. Find the concerned vessel and check if the subscription is indeed "inactive" (shown by the red dot left of it)
4. **Only if it is indeed inactive:** Delete the vessel entry from subscriptions on EAS by simply clicking on 'X' for the concerned vessel.



Subscriptions

	Site ID	Site Name	Customer	Period	Package	License Type	Activation	Deactivation		
🟢	SID6666...	Test Boskalis	Boskalis	12 months	entry	1-4 agents	09.02.23		✎	✕
🟢	SID17441	CMA CGM FORT Royal	828	12 months	entry	13-20 ag...	13.02.23		✎	✕
🔴	SID20727	Sedna	AB0026	12 months	entry	5-12 age...	16.02.23	29.05.24	✎	✕
🔴	SID20723	Hydra	AB0026	12 months	entry	5-12 age...	16.02.23	29.05.24	✎	✕
🟢	SID15603	Elbblue	2109	12 months	entry	5-12 age...	17.02.23		✎	✕

5. Reactivate the vessel in Portal360 under the new vessel owner.

Please Note: The feature to modify change ownership of a vessel in case of error is not available in Portal360 yet. *(While the back-office work has been done, it still needs to be implemented in the front-end and tested)*

7.5) Package upgrade / downgrade (not available yet)

The feature to upgrade an existing subscription to a higher package (e.g. from “1-4 PCs” to “5-12 PCs” is not available in Portal360 yet. *(While the back-office work has been done, it still needs to be implemented in the front-end and tested)*

The only way to way to upgrade or downgrade a vessel to a different package, is to terminate a subscription and reactivate it under another package.

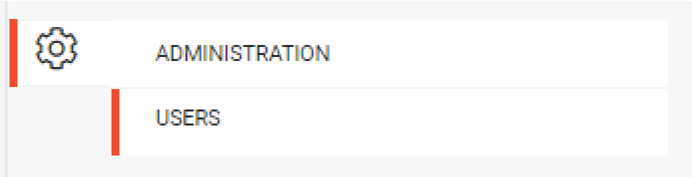
⚠

In this case a new licence code is generated which requires an uninstallation of the previous instance and reinstallation with the new licence code.

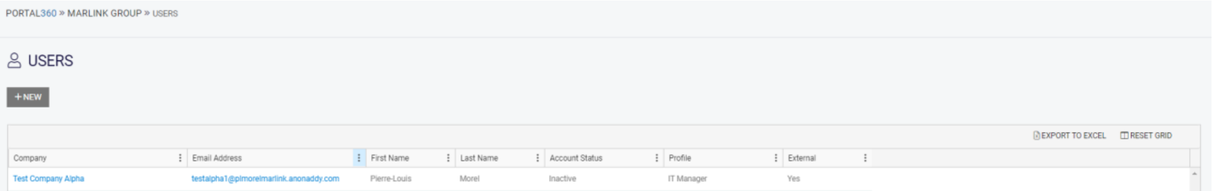
Please inform the vessel of this consequence as their existing installation will stop functioning after the termination

7.6) User Rights

If you are activating the first vessel for a customer who has just subscribed to CyberGuard, please check in Portal360 Administration > Users



You will see if user rights have been assigned enabling the customer to check and modify their configuration themselves later.

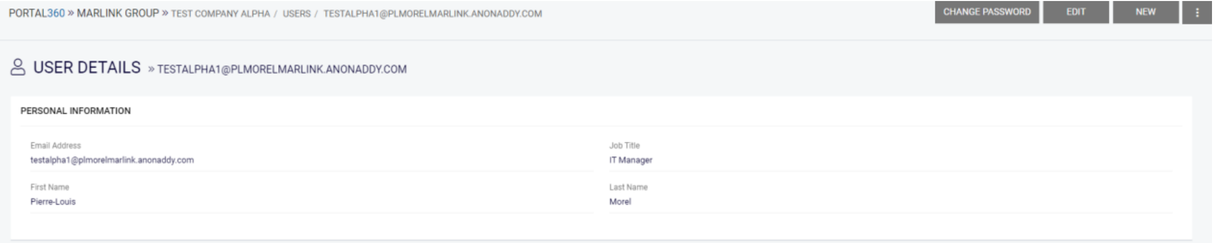


Company	Email Address	First Name	Last Name	Account Status	Profile	External
Test Company Alpha	testalpha1@plmorelmarlink.anonaddy.com	Pierre-Louis	Morel	Inactive	IT Manager	Yes

Operational Manager have view only rights
IT Manager can manage all subscribed services
Admin can manage user and all subscribed services

If you are not sure which user rights should be assigned to which customer account, please contact the Key Account Manager.

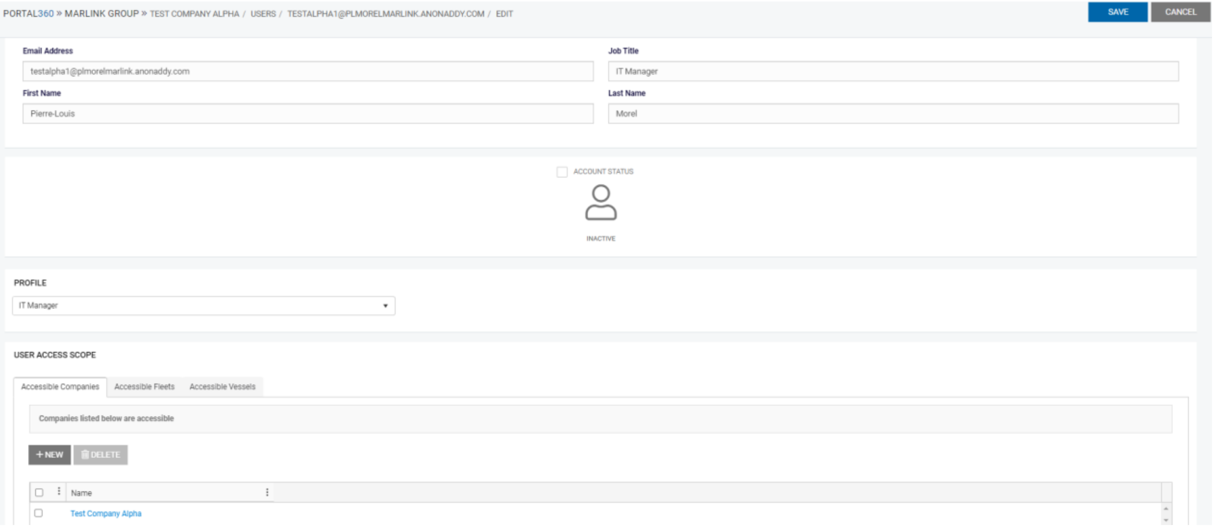
To change a profile, click on the user email address,


PORTAL360 » MARLINK GROUP » TEST COMPANY ALPHA / USERS / TESTALPHA1@PLMORELMARLINK.ANONADDY.COM
CHANGE PASSWORD
EDIT
NEW
USER DETAILS » TESTALPHA1@PLMORELMARLINK.ANONADDY.COM

PERSONAL INFORMATION

Email Address: testalpha1@plmorelmarlink.anonaddy.com
Job Title: IT Manager
First Name: Pierre-Louis
Last Name: Morel

then in the user detail on the Edit button in the upper right corner


PORTAL360 » MARLINK GROUP » TEST COMPANY ALPHA / USERS / TESTALPHA1@PLMORELMARLINK.ANONADDY.COM / EDIT
SAVE
CANCEL
Accessible Companies
Accessible Fleets
Accessible Vessels
+NEW
DELETE

Email Address: testalpha1@plmorelmarlink.anonaddy.com
Job Title: IT Manager
First Name: Pierre-Louis
Last Name: Morel

□ ACCOUNT STATUS
INACTIVE

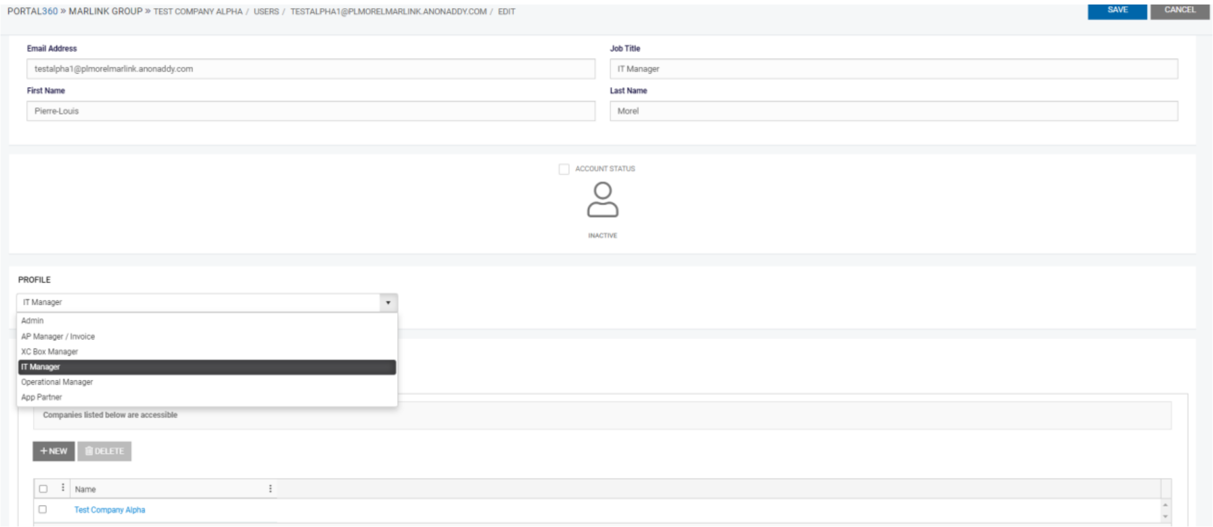
PROFILE
IT Manager ▾

USER ACCESS SCOPE

Companies listed below are accessible

□	Name
□	Test Company Alpha

Select the appropriate profile in the middle-left side, then click on Save in the upper left corner



PORTAL360 » MARLINK GROUP » TEST COMPANY ALPHA / USERS / TESTALPHA1@PLMORELMARLINK.ANONADDY.COM / EDIT

Email Address: testalpha1@plmorelmarlink.anonaddy.com

Job Title: IT Manager

First Name: Pierre-Louis

Last Name: Morel

□ ACCOUNT STATUS

INACTIVE

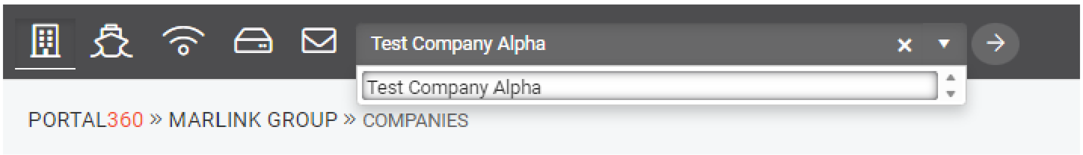
PROFILE: IT Manager

Companies listed below are accessible

□	Name
□	Test Company Alpha

7.6.1) To create a new user

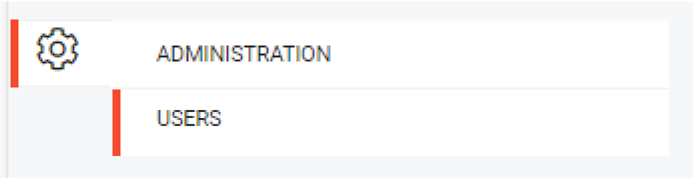
Switch to the company (you need to do this to select end-user profiles, otherwise you would be creating a Marlink user with Marlink user profile)



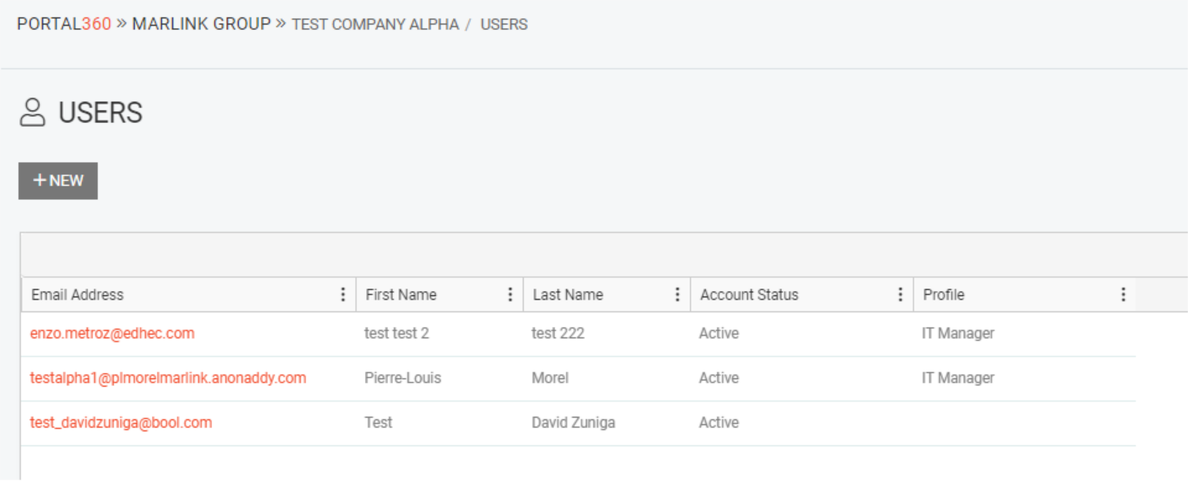
Test Company Alpha

Test Company Alpha

Administration > Users

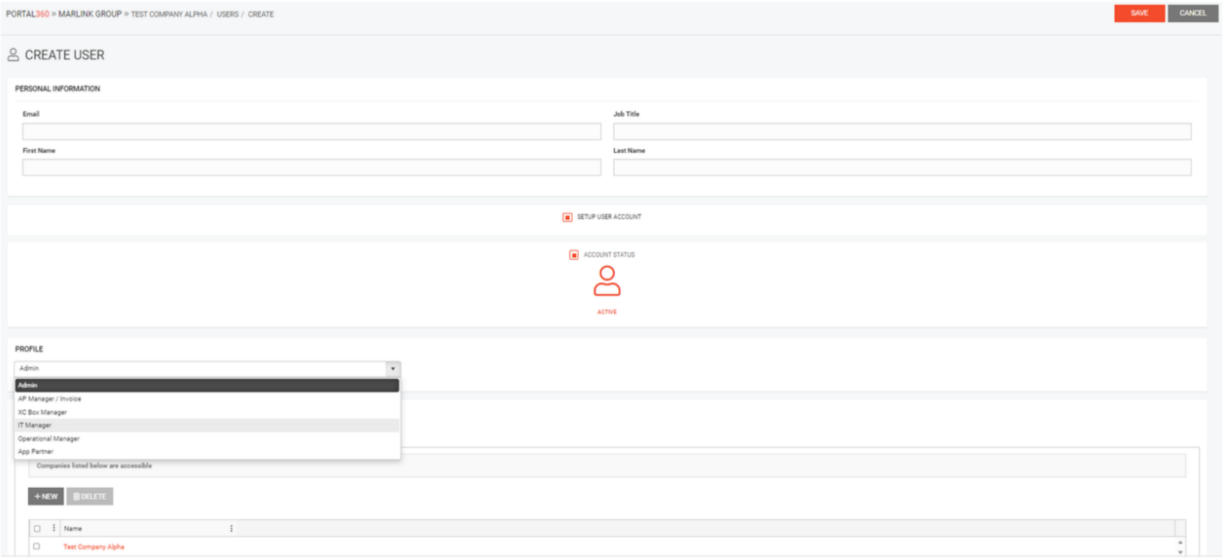


Click on the +New button in the upper left side



Email Address	First Name	Last Name	Account Status	Profile
enzo.metroz@edhec.com	test test 2	test 222	Active	IT Manager
testalpha1@plmorelmarlink.anonaddy.com	Pierre-Louis	Morel	Active	IT Manager
test_davidzuniga@bool.com	Test	David Zuniga	Active	

Fill in the information for email, Job Title, First Name, Last name and select a profile, then click on Save in the upper left corner.
Note that email address cannot contain some special characters such as "+"



Operational Manager have view only rights
IT Manager can manage all subscribed services
Admin can manage user and all subscribed services

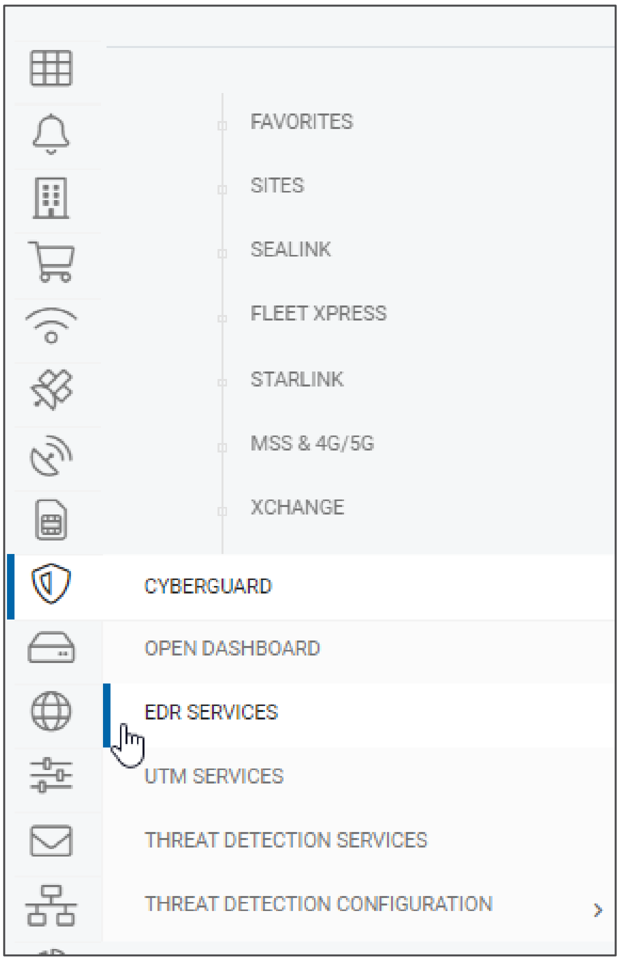
7.7) Portal360 Issues

7.7.1) Portal360 Backoffice

In case of any issue with the steps described previously, please describe your issue and create a ticket in https://imservicedesk.marlink.com/ under the *category “Business Application - Administrative Tasks / Functional / Technical Support”* and *“CyberGuard”* or send a mail to imservicedesk@marlink.com

7.7.1.1) Cyber Icon missing

If the CyberGuard section (represented by the “shield” icon) is missing from your sidebar in Portal360, please send a message to IM Service Desk with subject: [CyberGuard] user rights EDR Services View & Manage



7.7.1.2) EDR icon missing in sidebar (service catalogue missing)

If your account can see the CyberGuard section in the sidebar but “EDR Services” is not listed, this means that service catalogue is missing for this customer. Please do the following:

Contact Digital Delivery (digital.delivery@marlink.com) with subject: “[CyberGuard] service catalogue missing for client <fill in the name>”

8) RCS Tasks

8.1) Outage Notifications

In outage situation, VAS will send notification to service desk, the notification shall contain the outage mail distribution list that service desk will use.

8.1.1) Outage for dedicated customers consoles

8.1.1.1) CMA

VAS will send Outage Notifications to Service Desk who will create a priority ticket in Marlink.

RCS should inform CMA using Mailgun and the “CyberGuard EDR CMA” Outage mail distribution list, which can be found, as for all other Outage notifications, on the “Outage Distribution List” Excel sheet accessible through the Knowledge Base Quick Links”.

8.1.1.1) Boskalis

VAS will send Outage Notifications to Service Desk who will create a priority ticket in Marlink.

RCS should inform Boskalis using Mailgun and the “CyberGuard EDR Boskalis” Outage mail distribution list, which can be found, as for all other Outage notifications, on the “Outage Distribution List” Excel sheet accessible through the Knowledge Base Quick Links”.

8.1.1.1) Hoegh Autoliners

VAS will send Outage Notifications to Service Desk who will create a priority ticket in Marlink.

RCS should inform Hoegh Autoliners using Mailgun and the “CyberGuard EDR Hoegh Autoliners” Outage mail distribution list, which can be found, as for all other Outage notifications, on the “Outage Distribution List” Excel sheet accessible through the Knowledge Base Quick Links”.

8.1.2) Outage Notification (general case)

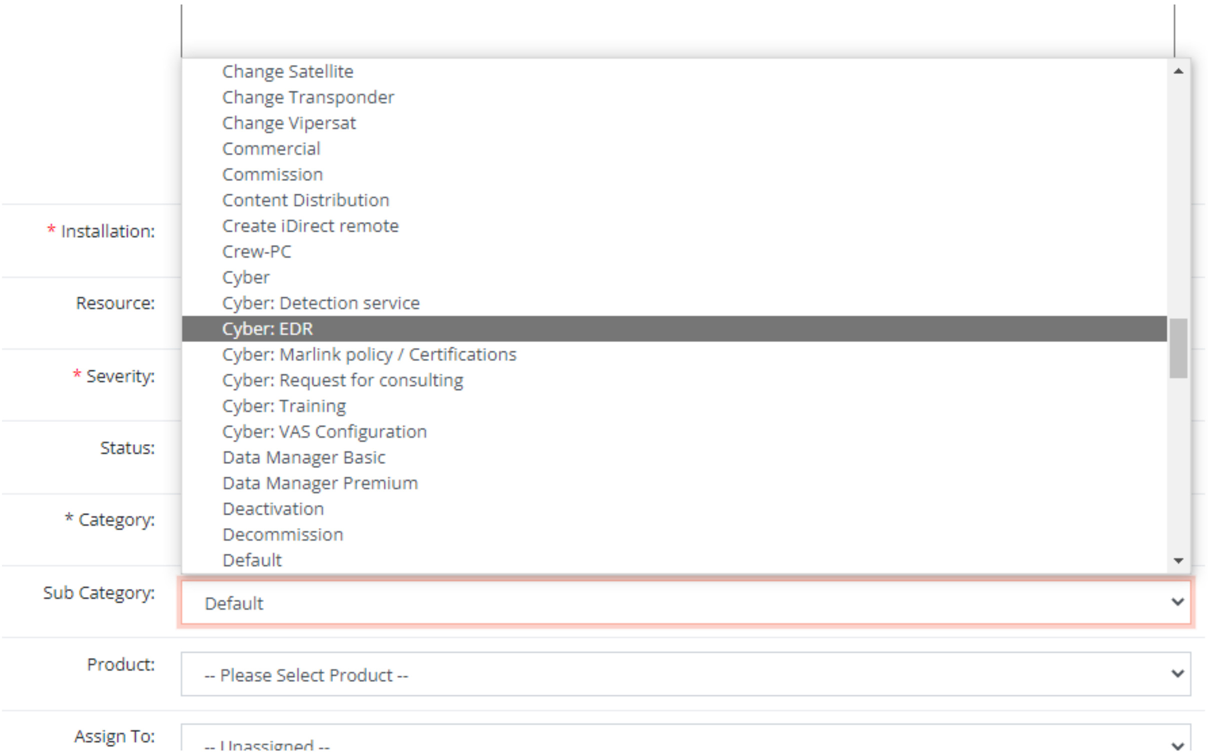
VAS will send Outage Notifications to Service Desk who will create a priority ticket in Marlink Postman.

RCS should inform CyberGuard EDR subscribed customers using Mailgun and the "CyberGuard EDR" Outage mail distribution list, which can be found, as for all other Outage notifications, on the "Outage Distribution List" Excel sheet accessible through the Knowledge Base Quick Links".

8.2) Assign EDR tickets to right department

Before continuing to handle a ticket, please check first whether the Customer is actually subscribed to CyberGuard EDR using the procedure described in 3.2)

For all customer support requests concerning EDR, please open a ticket in MERITS in “Cyber: EDR” sub-category.



* Installation:

Resource:

* Severity:

Status:

* Category:

Sub Category: Default

Product: -- Please Select Product --

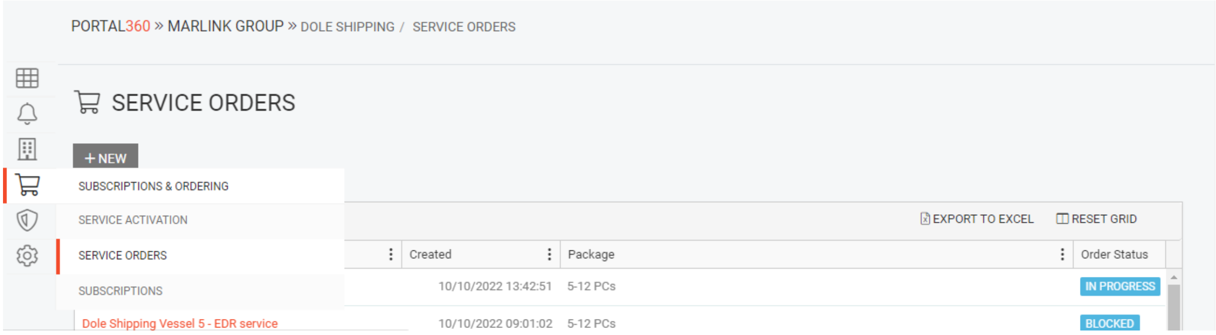
Assign To: -- Unassigned --

Figure 13: Cyber ticket sub-categories in MERITS

Assign the ticket to the relevant support department according to the schema in Chapter 3).

8.2.1) Check implementation status

Note that you can check the status of any activations you have submitted in the **“Service Orders”** section in **“Subscriptions & Ordering”**:



PORTAL360 » MARLINK GROUP » DOLE SHIPPING / SERVICE ORDERS

SERVICE ORDERS

+ NEW

SUBSCRIPTIONS & ORDERING

SERVICE ACTIVATION

SERVICE ORDERS

SUBSCRIPTIONS

EXPORT TO EXCEL

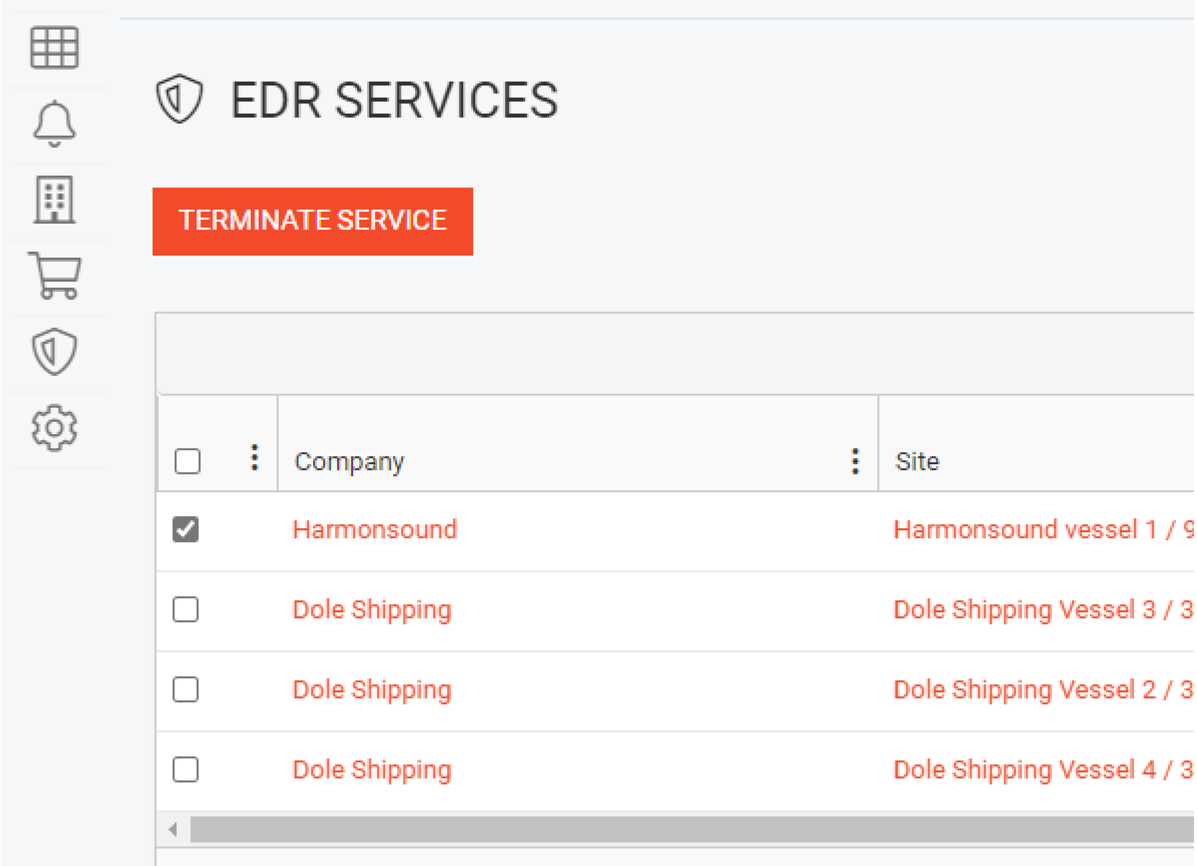
RESET GRID

	Created	Package	Order Status
	10/10/2022 13:42:51	5-12 PCs	IN PROGRESS
Dole Shipping Vessel 5 - EDR service	10/10/2022 09:01:02	5-12 PCs	BLOCKED

Figure 14: EDR Service Order Status

8.3) Service Termination

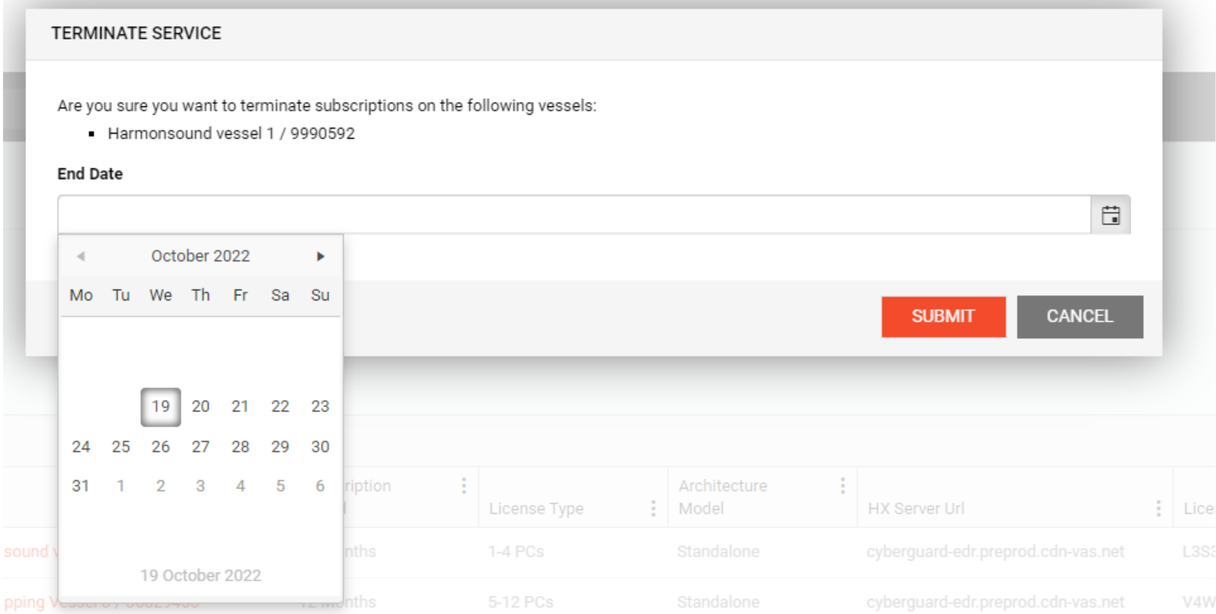
In the Portal360 CyberGuard section, select **“EDR Services”**, **tick the checkbox for the affected vessel** and click the **“Terminate Service”** button:



EDR SERVICES

□	Company	Site
☑	Harmonsound	Harmonsound vessel 1 / 9
□	Dole Shipping	Dole Shipping Vessel 3 / 3
□	Dole Shipping	Dole Shipping Vessel 2 / 3
□	Dole Shipping	Dole Shipping Vessel 4 / 3

Select the requested service **End Date** and **click “Submit”**:



TERMINATE SERVICE

Are you sure you want to terminate subscriptions on the following vessels:

- Harmonsound vessel 1 / 9990592

End Date

9) MSS BO

9.1) Service Activation

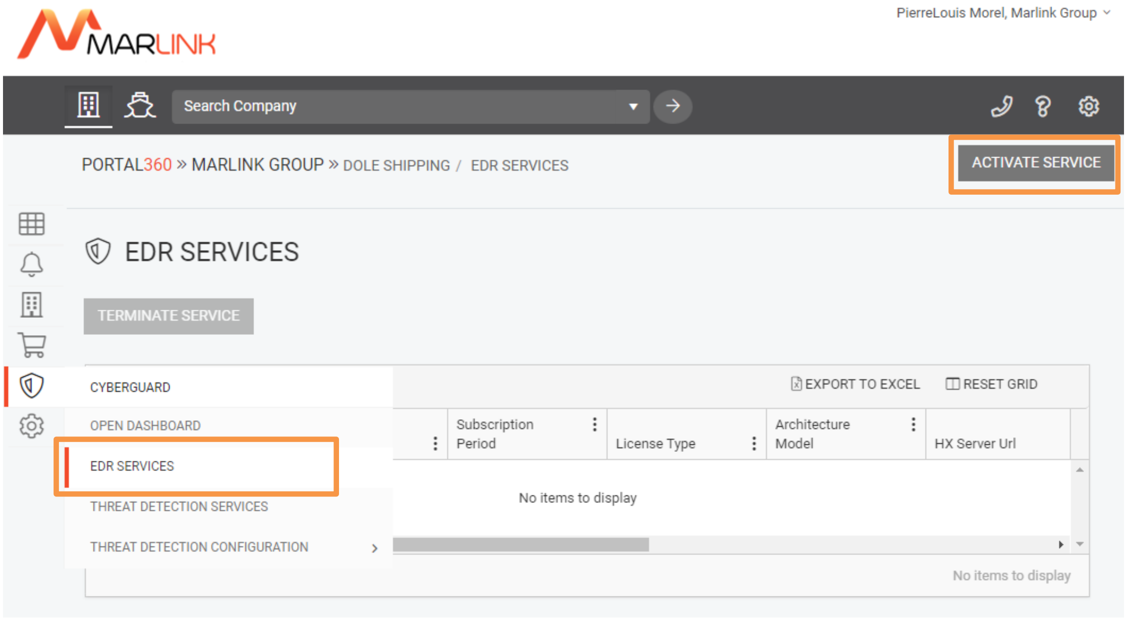
While CyberGuard EDR will be activated by CCCS if it has been selected on one of the order forms (CPQ, COF, IOF), in some cases an activation might be done by MSS Back Office.

In particular, if KAMs or Delivery / Project have contacted Service Desk directly without completing an order form, then MSS Back Office will receive a MERITS ticket from to activate a vessel.

You need to switched to the relevant subcompany

Activation on Marlink Group is not possible

In the Portal360 CyberGuard section, select **"EDR Services"** and click the **"Activate Service"** button.

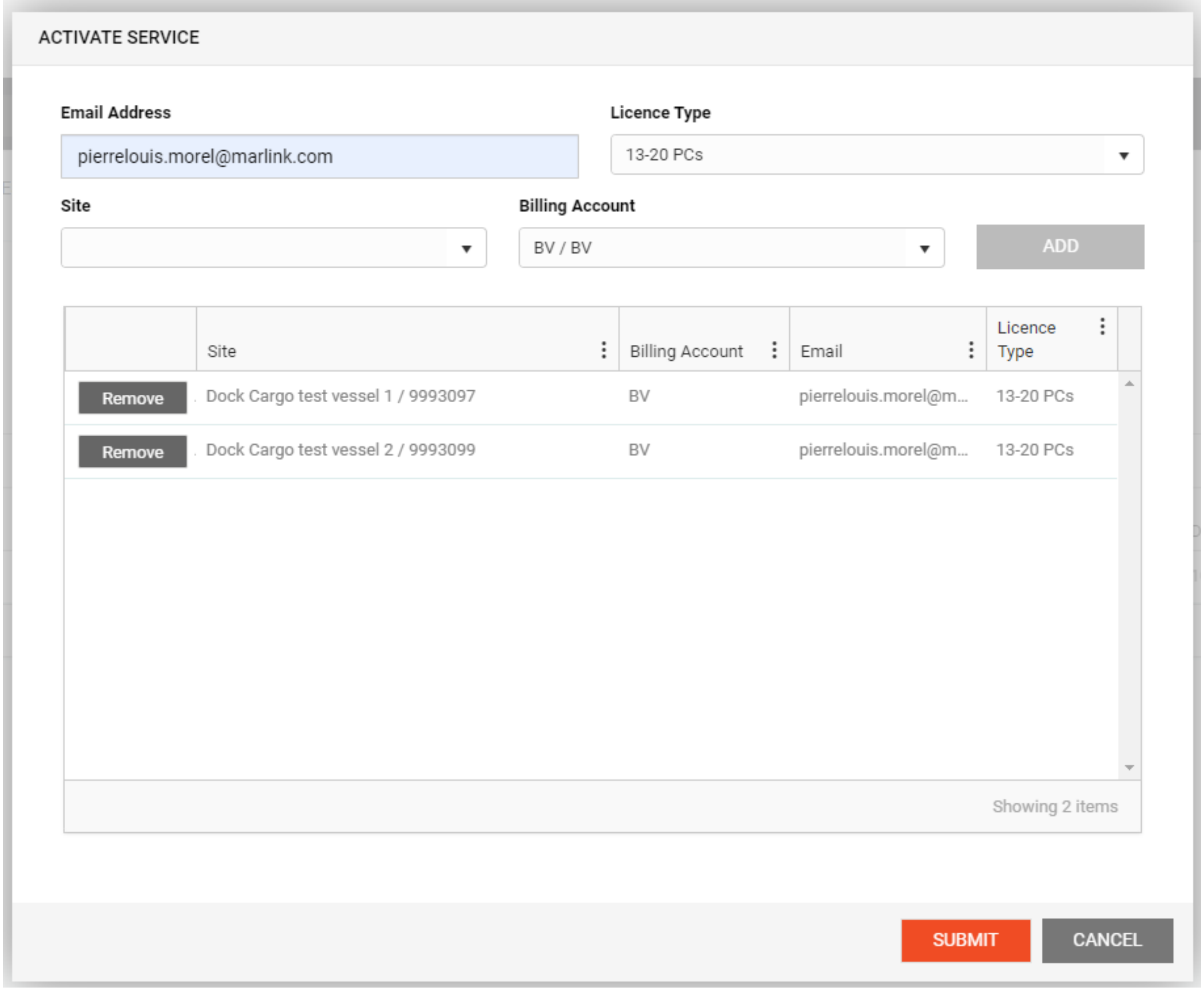


No items to display

No items to display

Figure 15: EDR Service Activation in Portal360

The following pop-up will appear:



ACTIVATE SERVICE

Email Address: pierrelouis.morel@marlink.com

Licence Type: 13-20 PCs

Site:

Billing Account: BV / BV

	Site	Billing Account	Email	Licence Type
Remove	Dock Cargo test vessel 1 / 9993097	BV	pierrelouis.morel@m...	13-20 PCs
Remove	Dock Cargo test vessel 2 / 9993099	BV	pierrelouis.morel@m...	13-20 PCs

Showing 2 items

Figure 16: EDR Activation Pop-Up

Please select:

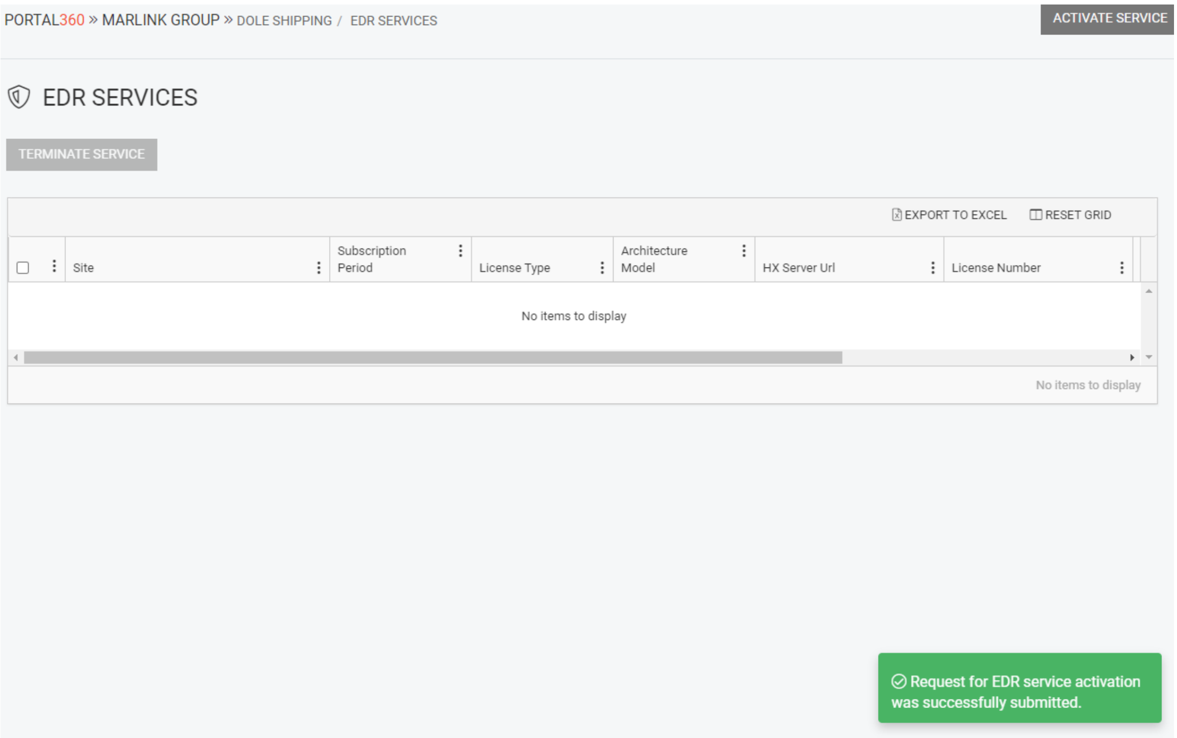
- Vessel: Select the vessel indicated in your MERITS ticket
- Billing Account: Select the billing account indicated in your MERITS ticket
  - ➢ Billing account should have been created during setup
- Email Address: Select the email address of the vessel that can be found in MERITS, multiple email address can be filled, separated by a ; (semicolon). Up to 5 email addresses can be filled.
- Licence type: Select the licence type indicated in your MERITS ticket

9.1.1) Vessel missing in the drop down list

If a vessel is missing in the drop down list, it may be due to outdated data, with the vessel not yet linked to the company.

IM Service Desk can help with the coordination of effort to ensure that the data is up to date in all systems, see 6.2)

After activation, you should see a confirmation message on the bottom right screen:



PORTAL360 » MARLINK GROUP » DOLE SHIPPING / EDR SERVICES

ACTIVATE SERVICE

EDR SERVICES

TERMINATE SERVICE

EXPORT TO EXCEL RESET GRID

□	Site	Subscription Period	License Type	Architecture Model	HX Server Url	License Number

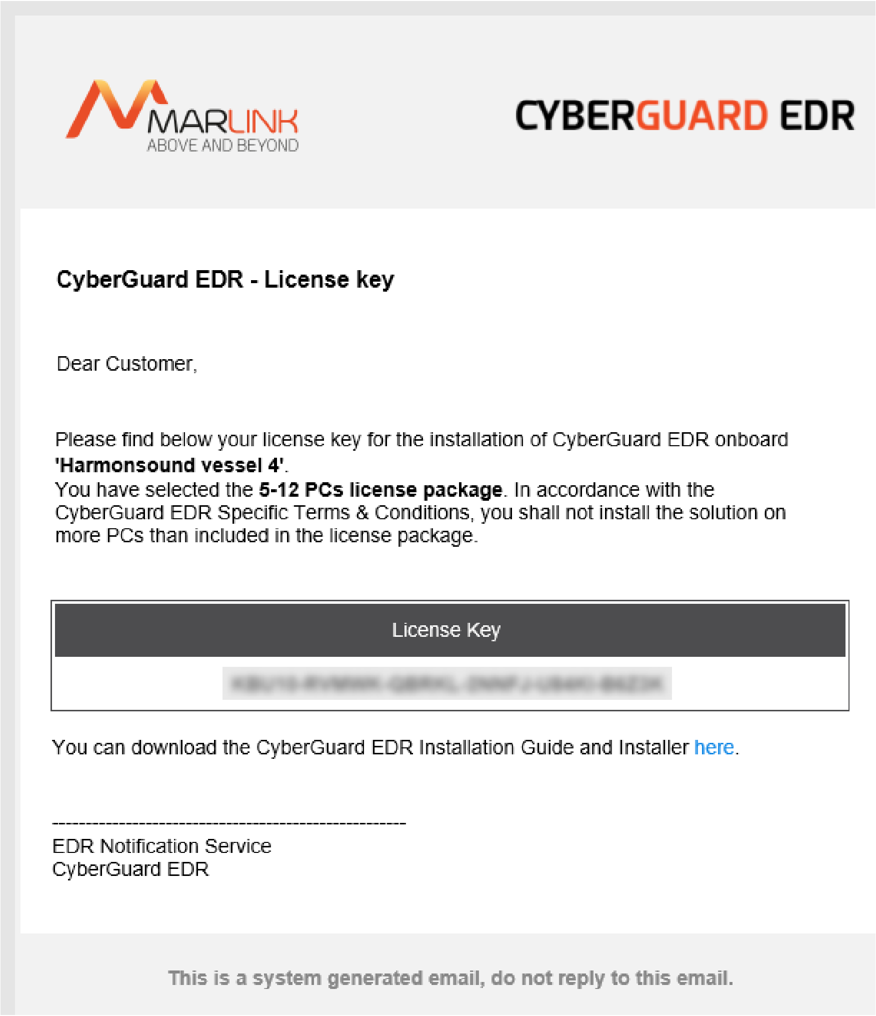
No items to display

No items to display

Request for EDR service activation was successfully submitted.

Figure 15: Service Activation confirmation message

The client will receive a mail with a link to the installation documentation and the installer (see Figure 11 - Activation mail & Figure 12 - https://marlink.com/cyberguard-edr/).



CyberGuard EDR - License key

Dear Customer,

Please find below your license key for the installation of CyberGuard EDR onboard **'Harmonsound vessel 4'**.
You have selected the **5-12 PCs license package**. In accordance with the CyberGuard EDR Specific Terms & Conditions, you shall not install the solution on more PCs than included in the license package.

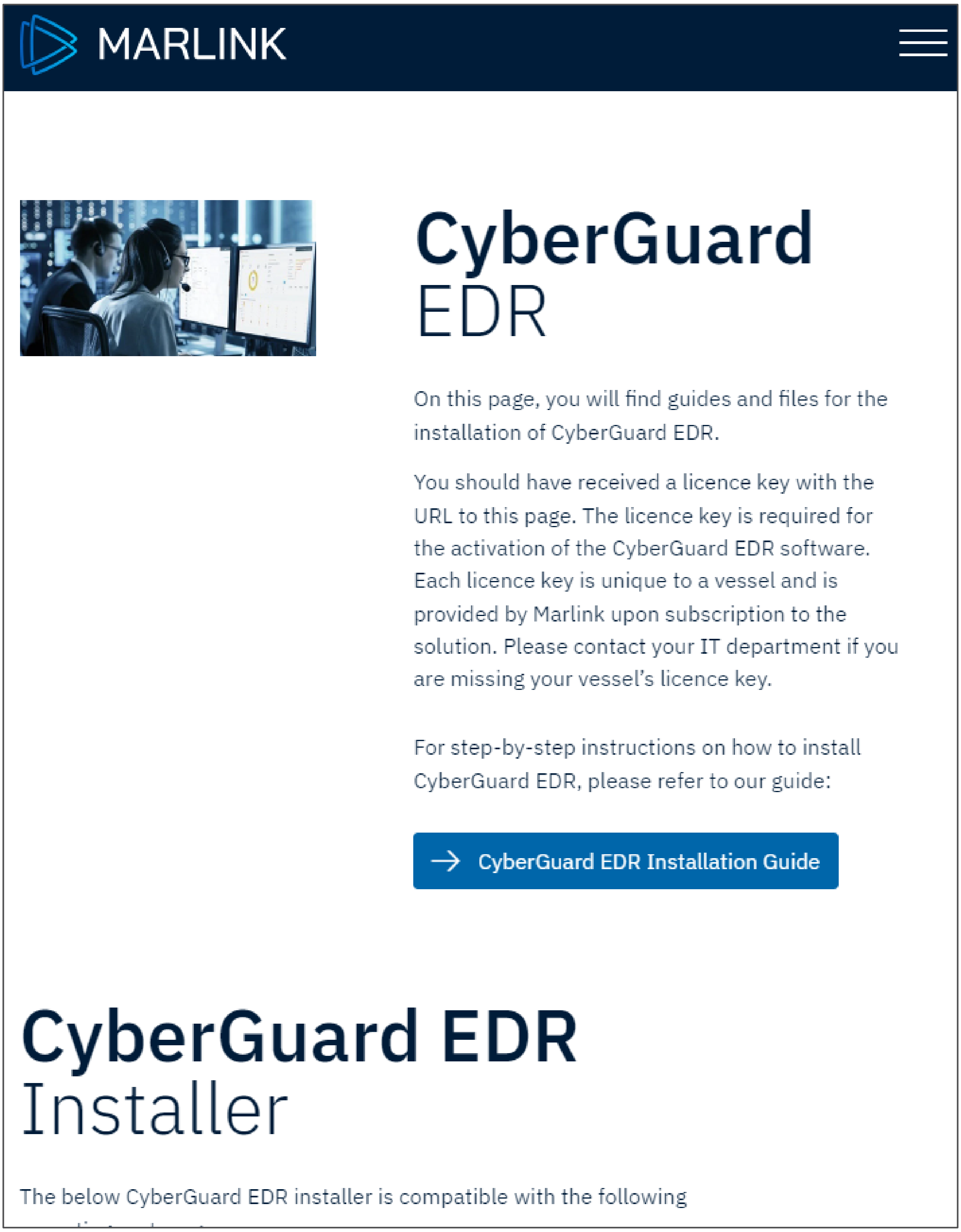
License Key
[redacted]

You can download the CyberGuard EDR Installation Guide and Installer here.

EDR Notification Service
CyberGuard EDR

This is a system generated email, do not reply to this email.

Figure 18 - Activation mail



MARLINK

CyberGuard EDR

On this page, you will find guides and files for the installation of CyberGuard EDR.

You should have received a licence key with the URL to this page. The licence key is required for the activation of the CyberGuard EDR software. Each licence key is unique to a vessel and is provided by Marlink upon subscription to the solution. Please contact your IT department if you are missing your vessel's licence key.

For step-by-step instructions on how to install CyberGuard EDR, please refer to our guide:

→ CyberGuard EDR Installation Guide

CyberGuard EDR Installer

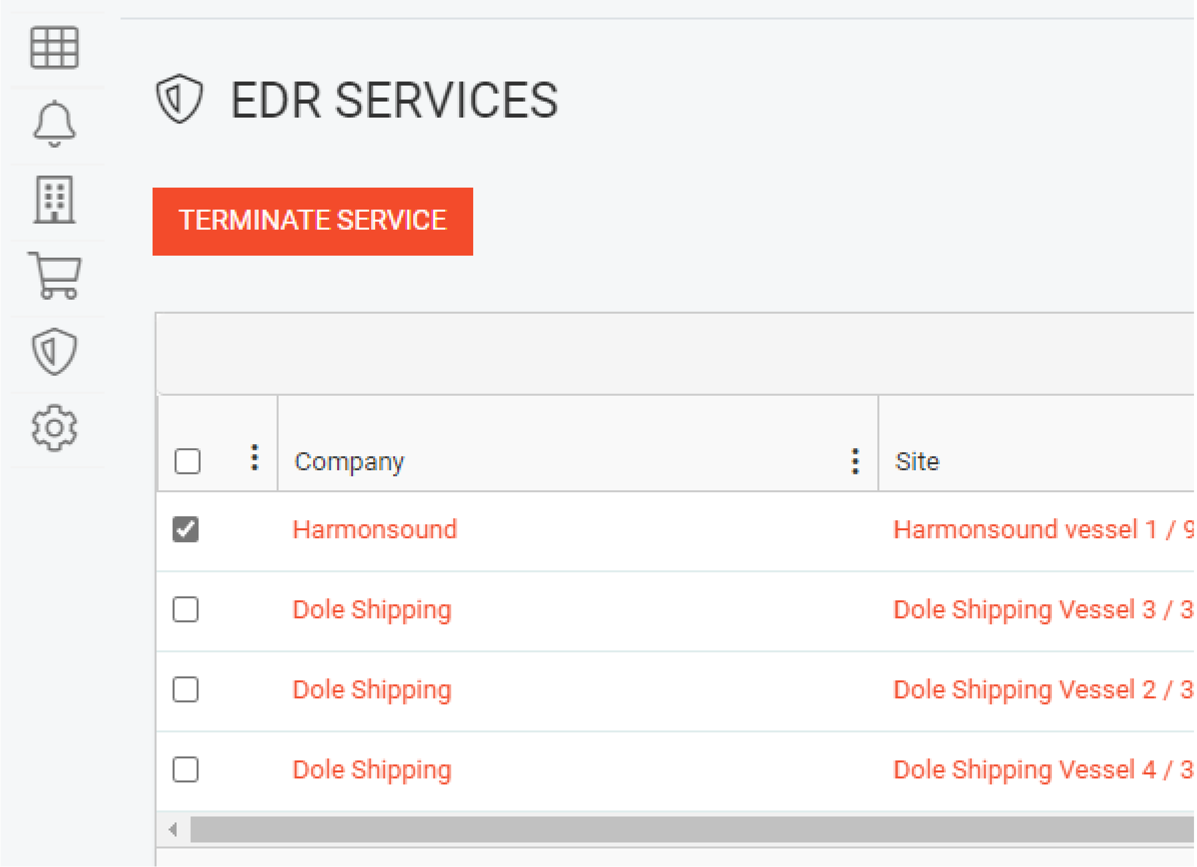
The below CyberGuard EDR installer is compatible with the following

Figure 19 - https://marlink.com/cyberguard-edr/

See chapter 8.2.1) on how to check the implementation status.

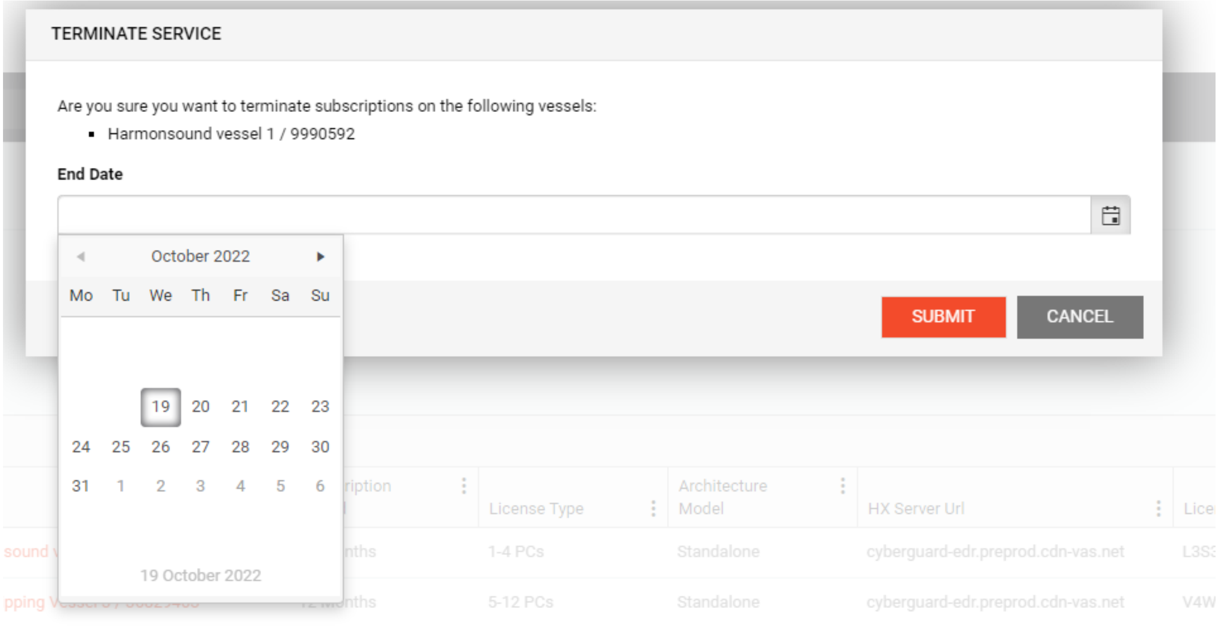
9.2 Service Termination

In the Portal360 CyberGuard section, select **"EDR Services"**, **tick the checkbox for the affected vessel** and click the **"Terminate Service"** button:



□	Company	Site
☑	Harmonsound	Harmonsound vessel 1 / 9
□	Dole Shipping	Dole Shipping Vessel 3 / 3
□	Dole Shipping	Dole Shipping Vessel 2 / 3
□	Dole Shipping	Dole Shipping Vessel 4 / 3

Select the requested service **End Date** and **click "Submit"**:



TERMINATE SERVICE

Are you sure you want to terminate subscriptions on the following vessels:

- Harmonsound vessel 1 / 9990592

End Date

10) MNOC Bratislava Tasks

10.1)Connectivity issue

MNOC Bratislava will assist customers with connectivity issues.

10.2)Data usage

The application uses data to keep up to date with new threats.

	CyberGuard EDR (Trellix)
Initial installation	**30 MB** installer + **250 MB** initial signatures **Per computer**
Daily signature updates (average)	**2 MB / computer / day**
Engine updates (average)	**30 MB** (every 2-3 months) **/ computer**

11) MITS Tasks

MITS will investigate any technical issue which does not appear to be related to an Administrative Task (see section 11.1).

11.1)CyberGuard installation issues

Common causes for customer complaints might be:

Root cause	Check	If not resolved, reach out to
Has CyberGuard EDR been properly installed	• Check installation status in the CyberGuard Portal see §3.3)	
CyberGuard EDR installation failed because Trellix/FireEye is already present	• Uninstall the Trellix/FireEye agent and relaunch the Cyberguard EDR installer	CCTS

CyberGuard EDR admin server cannot be reached	• If CMA o Check that the url https://rdb-api.cdn-vas.net/api and IP 77.70.254.120 are reachable on port 443 (used by the installer) ▪ If not, check the computer firewall ▪ If not, contact CCTS o Check that http://cyberguard-edr.cmacgm.cdn-vas.net and 77.70.254.121 are reachable on port:80 & port:443 are reachable (you should get 404 error) ▪ If not, check the computer firewall ▪ If not, contact CCTS • Else (general case) o Check that the url https://rdb-api.cdn-vas.net/api and IP 77.70.254.120 are reachable on port 443 (used by the installer) ▪ If not, contact CCTS o Check that the URL http://cyberguard-edr.cdn-vas.net and IP 77.70.254.86 are reachable on port 80 & port 443 are reachable (you should get 404 error) ▪ If not, contact CCTS ▪ else continue • Check if the computer is running Windows 7 o As Microsoft no longer supports Windows 7, the HTTPS certificates may be outdated and therefore no longer support connection to the EAS	CCTS
Licence number rejected	• Check that the subscription has been not deactivated • Check the format of the licence number	CCTS

Ports used for the Master service and the web server already used by another application	- Check that the port 8084 is not used by another application: this port is required for the Master service - Check that at least one port from 81 to 91 is available for the web server	CCTS
Network share cannot be reached to download the client installer	- Check if the client can use http://cyberguard-edr.local:81 (81 to 91 depending on the available port) to download the client installer	CCTS
Unforeseen Installation failure	- Retrieve the install log cg_setup.log in C:\Marlink\Cyberguard-EDR of the installer and share it with CCTS	CCTS

If IT Link app deployer is used:

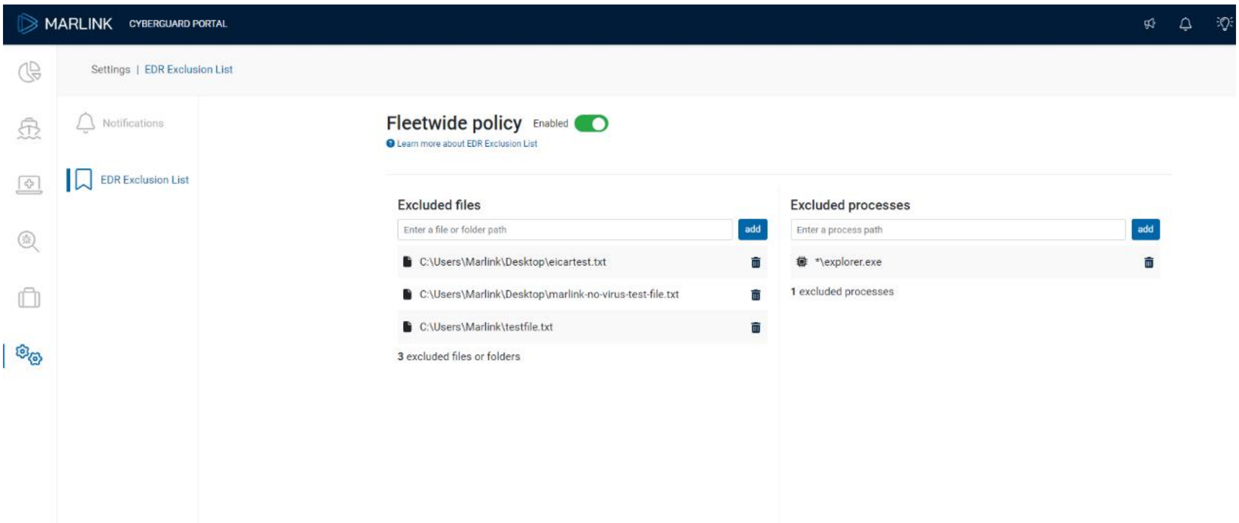
Root cause	Check	If not resolved, reach out to
CyberGuard EDR installation through IT Link App deployer failed	- Check that the app deployer agent is present on the computer	MITS technical

11.2) EDR Exclusion List

MITS shall manage the EDR Exclusion list directly from the CyberGuard Portal for all the customer and if you encounter any issues you can contact SecOps.

When we have a customer who requests to exclude their file from getting quarantined it can directly be done via CyberGuard Portal > Settings > EDR Exclusion List and then add the files/processes that customer is considering as trusted.

Root cause	Connect to	Resolution
Managing EDR Exclusion List	Connect to CyberGuard Portal for the customer. Add the file and process exclusions that the customer is requesting.	- Connect to CyberGuard Portal - Go to Settings > EDR Exclusion List - Add the exclusion file or process


MARLINK CYBERGUARD PORTAL
Settings | EDR Exclusion List
Notifications
EDR Exclusion List
Learn more about EDR Exclusion List
add
add

Fleetwide policy Enabled

Excluded files

Enter a file or folder path

C:\Users\Marlink\Desktop\eicartest.txt

C:\Users\Marlink\Desktop\marlink-no-virus-test-file.txt

C:\Users\Marlink\testfile.txt

3 excluded files or folders

Excluded processes

Enter a process path

*\explorer.exe

1 excluded processes

This is how the EDR Exclusion List looks like in the CyberGuard Portal. This is a self-managed service.

If a request is raised by the customer for restoring the customer files/processes from getting quarantined, Marlink Service Desk can connect to the CyberGuard Portal on the customer's behalf and set the requested file/process exclusions. However, please explain to the customer how he/she could perform this themselves next time.

12) SecOps Tasks

SecOps will manage the EDR exclusion list when it cannot be resolved by MITS. A detailed explanation for EDR Exclusion list is shown in chapter 10.2.

13) CCTS Tasks

CCTS will investigate any complex technical issue when it cannot be resolved by MITS

13.1)CyberGuard installation issues

Before the ticket reaches CCTS, MITS will have done a number of checks.
It is possible to check agent's installation status on the CyberGuard Portal see §3.3)
Common causes for customer complaints during installation might be:

Root cause	Reach out to	MITS Checks
CyberGuard EDR installation failed because an SkyFile antivirus is still present	Customer IT and/or Shamrock info@shamrock.de With guilhem.more-causse@marlink.com in copy	Cf 11.1)

CyberGuard EDR installation freeze after inputting the licence key	Shamrock info@shamrock.de With guilhem.more-causse@marlink.com in copy	- Have you used the paste button ? (if the input is done through Ctrl+V the installer can freeze, in this case the application need to be killed and the installation restarted)
CyberGuard EDR admin server cannot be reached	VAS/Engineering VAS.Operations@marlink.com	Cf 11.1)
Unforeseen Installation failure	Shamrock info@shamrock.de Engineering VAS.Operations@marlink.com Cc Guilhem.more-causse@marlink.com	Cf 11.1)
Ports used for the Master service and the web server already used by another application	Customer IT and/or Shamrock info@shamrock.de Cc Guilhem.more-causse@marlink.com	Cf 11.1)

13.1.1) Ports used for the Master service and the web server already used by another application

The installer check if a port is currently in use, in situation where EDR was installed and took the port from another application (if that other application was not yet installed for example), it is possible to change the port used by changing some configuration files:

- httpd.conf,
- cyberguardedr.ini

and to restart the services.

Just search in both files for "81" and replace it by for example 82.

13.2)CyberGuard EDR Agent issues

Marlink has a Platinum support plan that give access to 15 identified people to Trellix/FireEye support

CHANNEL	
Web	https://thrive.trellix.com/s/ Alternatively, see direct link to create a New Case via web: https://thrive.trellix.com/s/supportnewcase
Phone	https://kcm.trellix.com/corporate/index?page=content&id=KB95597 Also, refer to Trellix Thrive Support Contact Numbers for local telephone numbers.

TEMPLATE FOR SUPPORT REQUESTS	
Customer Details • Company name • Contact details: Name, Contact Number and Email • Severity (this should reflect the impact of the issue on the business: High, Medium, or Low)	System Details • Product: Endpoint Security Agent HX • System: Windows o State the version

France	0805543959	Other countries	+1 408 324 9400

13.2.1) Collecting Agent Diagnostic Information

If you experience problems with Endpoint Security on your host endpoint, collect diagnostic information to help troubleshoot the problem. This section describes the types of data you should collect.

13.2.1.1) Export a Copy of Your Log File

Exporting a copy of your log file might help you diagnose the problem. To export a copy of the host log file, enter the following command on the command line:

```
xagt --log-export <filename>
```

The log file is exported using the specified file name from the agent database and decrypted.

13.2.1.2) Export a Copy of Your Configuration File

Exporting a copy of your configuration file might help you diagnose the problem. To export a copy of the host configuration file, enter the following command on the command line:

```
xagt --cfg-export <filename>
```

The configuration file is exported using the specified file name and decrypted.

13.2.1.3) Acquire Agent Diagnostics Data from the Endpoint Security Server

If you decide to contact Trellix/FireEye Technical Support with your problem, you should acquire agent diagnostics data from the Endpoint Security server. This report will help your Trellix/FireEye technician help you diagnose problems.

To acquire agent diagnostics data from the Endpoint Security server:

1. Log in to the Web UI as an administrator.

2. Select Hosts at the top of the Web UI to access the Hosts page.

3. Select the All Hosts tab and locate the host for which you want diagnostics.

4. Select the checkbox to the left of the host line.

5. In the Actions menu above the host list, select Acquire: Agent Diagnostics to request the agent diagnostics.

6. Select Acquisitions at the top of the Web UI.

7. Locate and select your acquisition on the Acquisitions page. Details about the acquisition appear in the Acquisition Detail pane.

8. When the acquisition status has changed to Acquired, click Download in the Acquisition Detail pane. The acquisition .zip file is downloaded to your computer.

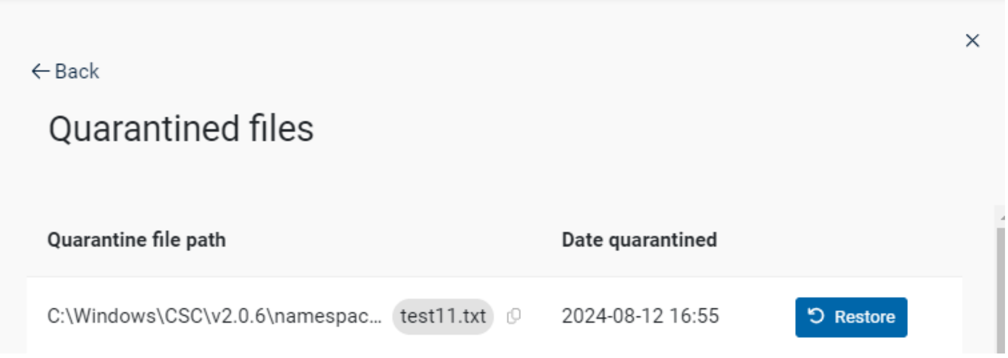
13.2.2) EDR Remove/Restore from quarantine

When we have a customer who requests to exclude their file from getting quarantined it can directly be done via CyberGuard Portal > EDR Fleet health Monitor page > Quarantine List and then restore the files/processes that customer is requesting to restore.

Root cause	Connect to	Resolution
Restore Quarantine Files	Connect to CyberGuard Portal for the customer. Restore the file customer is requesting to restore from quarantine.	• Connect to CyberGuard Portal • EDR Fleet Health Monitor > Machine Name > quarantine list • Restore the quarantined file

While these exclusions will prevent files and processes from being quarantined in future, these do not release any previously quarantined files. To restore a file from quarantine there are 2 possible ways:

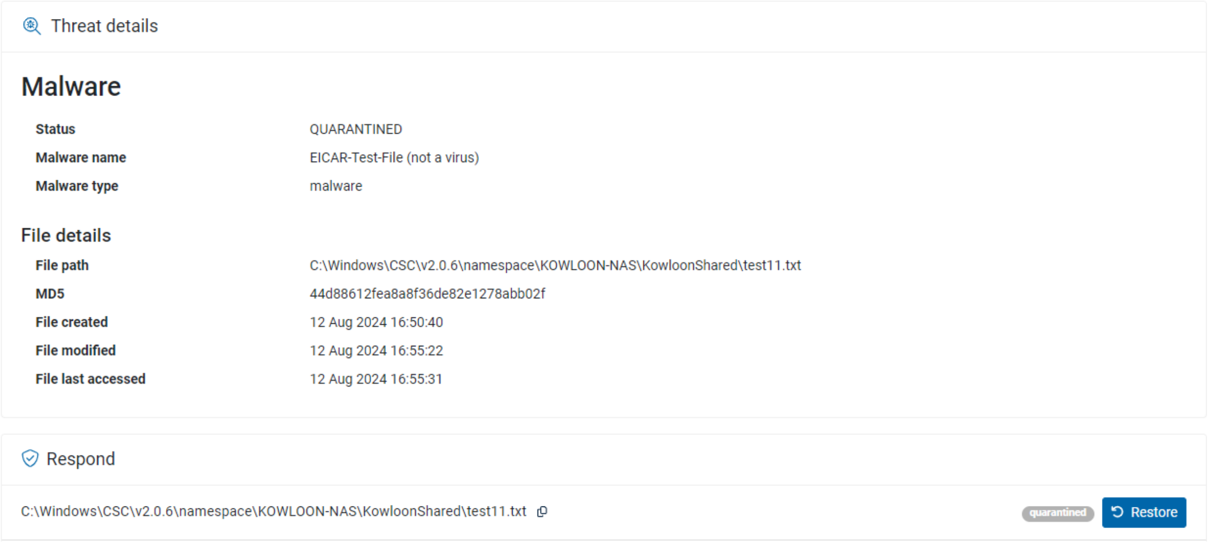
1. Navigate to the machine name from EDR fleet health monitor page and go to quarantine files.



Quarantined files

Quarantine file path	Date quarantined	
C:\Windows\CSC\v2.0.6\namespac... test11.txt	2024-08-12 16:55	Restore

2. Navigate to the relevant detected threat(s) and Restore the file from the respond section.



Threat details

Malware

Status	QUARANTINED
Malware name	EICAR-Test-File (not a virus)
Malware type	malware

File details

File path	C:\Windows\CSC\v2.0.6\namespace\KOWLOON-NAS\KowloonShared\test11.txt
MD5	44d88612fea8a8f36de82e1278abb02f
File created	12 Aug 2024 16:50:40
File modified	12 Aug 2024 16:55:22
File last accessed	12 Aug 2024 16:55:31

Respond

C:\Windows\CSC\v2.0.6\namespace\KOWLOON-NAS\KowloonShared\test11.txt

Please Note: It’s highly recommended to wait 30min after performing the Restore action from CyberGuard Portal as the EDR Exclusions are not updated on the Endpoint device in Real time. If the endpoint device is online, within 30min. the exclusion list is updated and now you need to perform the Restore action again.

Please check after some time that the quarantine file is removed from the quarantine file list to assure the successful restore.

13.2.2.1) EDR Alert Status

Following below are the alert statuses which can be seen in the CyberGuard Portal when an EDR alert is raised on the endpoint device:

1. **Alert**: An EDR alert where the threat is still alive and the user is required to perform countermeasures.
   - ‘Alerts’ are displayed in the **“Active Threats”** section of the CyberGuard Portal

2. **Quarantine**: When a file is found with malicious content and is quarantined by the EDR.
   - ‘Quarantine’ status alerts are displayed in the **“Handled Threats”** section

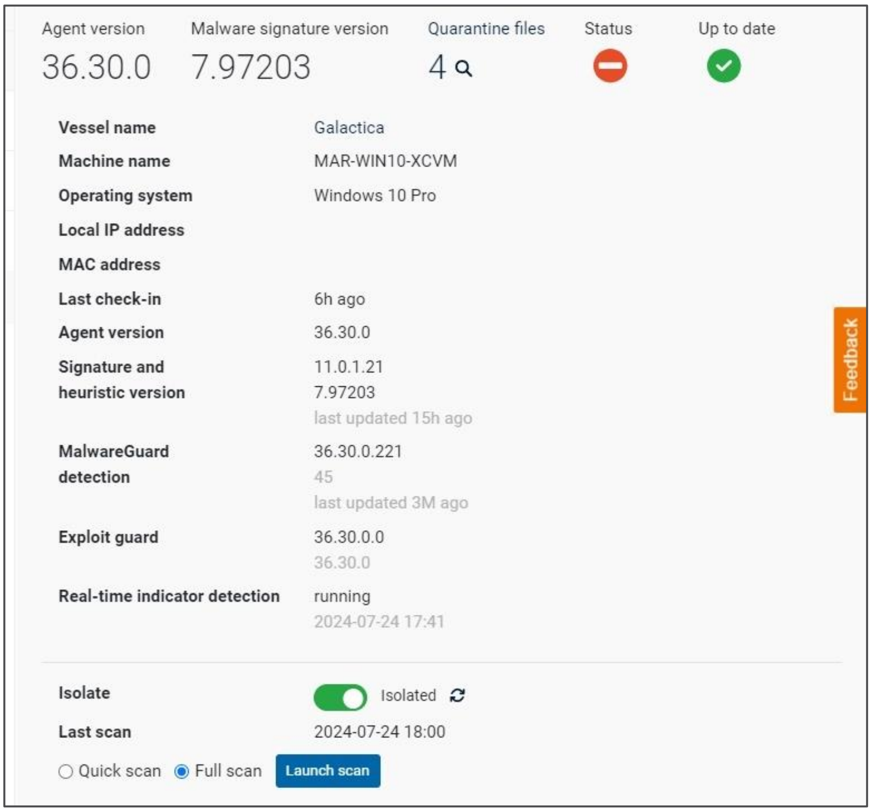
3. **Cleaned**: When a part of a file is found malicious and is cleaned by the EDR. The cleaned file will be accessible as before and not moved to quarantine.
   - ‘Cleaned’ status alerts are displayed in the **“Handled Threats”** section

13.2.3) EDR Isolate a Device/PC

Root cause	Connect to	Resolution
Isolating an infected device /PC	Connect to CyberGuard Portal for the customer. Isolate the device/PC which is highly infected.	• Connect to CyberGuard Portal • Go to EDR fleet health monitor page • Isolate the device/PC after selecting the machine.

When we have a customer who requests to isolate a device/PC when the PC is found highly infected and there's a risk of spread of infection through the LAN/VLAN on board then this device/PC can be isolated via CyberGuard Portal > EDR fleet health monitor page > select an infected machine you want to isolate.

In the sidebar, you will find the isolate button as shown below



Agent version	Malware signature version	Quarantine files	Status	Up to date
36.30.0	7.97203	4	⛔	✓

Vessel name	Galactica
Machine name	MAR-WIN10-XCVM
Operating system	Windows 10 Pro
Local IP address	
MAC address	
Last check-in	6h ago
Agent version	36.30.0
Signature and heuristic version	11.0.1.21 7.97203 last updated 15h ago
MalwareGuard detection	36.30.0.221 45 last updated 3M ago
Exploit guard	36.30.0.0 36.30.0
Real-time indicator detection	running 2024-07-24 17:41
Isolate	Isolated
Last scan	2024-07-24 18:00

○ Quick scan ● Full scan Launch scan

<u>Please note</u>: When you isolate a device, you may observe a wait time of 5-7min for both isolation and release from isolation of a device.

This is a self-managed feature. Upon a customer request to Marlink Service Desk, the customer can be guided by using the above steps to perform the actions him/herself.

13.2.3.1) EDR Machine Status

Following below are the statuses which can be seen while isolating a machine/PC:

1. **Normal**: state when the endpoint device is not isolated.
2. **Isolating** (**Containing**): In process of isolating the endpoint device.
3. **Isolated** (**Contained**): Successful isolation of the endpoint device.