

RCS & MNOC FortiManager Training (UTM & SDWAN)

April 2025

Q&A

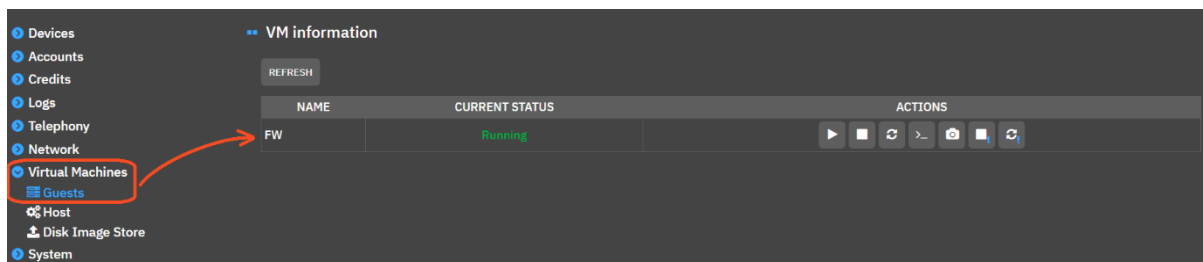
1- Question:

What are the methods to confirm that a CyberGuard UTM / SDWAN service is installed on a vessel? Is it possible to check on the XC in the Box Settings / Virtual Machine menu if the UTM has been implemented on the XC?

➤ Answer:


The Virtual Machines menu of the XChange Box is indeed a valid method as it will show if the Fortigate VM used by UTM / SDWAN services is installed or not.

If the service is installed, you will see a line named “FW” or “FW SDWAN” in the “VM information” section of the “Guests” submenu:



However, the easiest and quickest way to check if a UTM or SDWAN is installed, is to check the “Installation” section of the vessel in Merits. You will find there an installation with type “CyberGuard UTM” or “XChange SD-WAN” and status “Active”:

Services

IID	Solution	Name	Type	System	System Version	Commission Date	Installation Status
126433	▼ Anita Garibaldi - Sealink		Sealink Service	 Sealink Premium	Premium Plus Service, Contract-Bundled	2025-01-17 [1]	Active
126434	Anita Garibaldi - Ku	Customer Owned	Intellian V85NX	Newtec	MDM2510	2025-01-17	Active
126435	Anita Garibaldi - Network Device		Router	XChange	Power		Active
137215	Anita Garibaldi - Sdwan		XChange SD-WAN	Fortinet	VM01V-Premium	2025-01-21 [0]	Active
126436	Anita Garibaldi - Sealink Backup	Customer Owned	Intellian C700	Iridium Certus			Active
137214	Anita Garibaldi - Utm		CyberGuard UTM	Fortinet	VM01V-Advanced	2025-01-21 [0]	Active
145210	Anita Garibaldi - VPN		CyberGuard UTM	Fortinet		2025-03-24 [0]	Active


A last method, is to check if the FortiManger directly, and look up for a device “*Device Manager > Device & Groups*” by means of search function


Note: all installations use the following naming convention: **SIDXXXX_VesselName**

Be careful: only devices with a green or amber arrow correspond to installed devices (regardless of the colour of the arrow). If the device shows something else (a grey square) it means the device is ready on the shore side but has not yet been installed on the vessel.


Examples:

- **Installed devices:**

<input type="checkbox"/>	Device Name ⇅	Auto-link Status ⇅	Config Status ⇅	Host Name ⇅
<input type="checkbox"/>	 ID16746_Stolt Condor		✓ Synchronized	SID16746_Stolt Condor

<input type="checkbox"/>	Device Name ⇅	Config Status ⇅	Host Name ⇅
<input type="checkbox"/>	 ID7551_StenBothnia	⚠ Modified	SID7551_StenBothnia

- **Devices ready to be installed but not yet installed:**

<input type="checkbox"/>	Device Name ⇅	Auto-link Status ⇅	Config Status ⇅	Host Name ⇅
<input type="checkbox"/>	 ID19998_StoltCalluna	✓ Enabled	⚠ Modified	SID19998_StoltCalluna

2- Question:

Can we have multiple WAN1 devices on an XChange Box with SDWAN?

E.g. Customer will decide to have VSAT and MSS as backups, and will use Starlink 1, Starlink 2, OneWeb 1, OneWeb 2 and 5G as primary devices via SD-WAN?

➤ **Answer:**

The SDWAN device always comes as a replacement of the Sealink device on the WAN2 interface. This SDWAN device can be configured to use either some or all of the terminals installed on the vessel. By default, most of the installations will have a Sealink + Starlink (+ 4 or 5G) configured for usage through the SDWAN device, while the MSS Backup will remain independent and directly connected on the WAN1 of the XChange.

Therefore, it remains possible to have multiple devices connected on WAN1, but you will never see the VSAT since it's a core terminal of the SDWAN solution and always will be included in the SDWAN device.

3- Question:

What if we need to have MORE than 5 devices over the SDWAN trunk?

e.g. 4 Starlinks + 5G? It looks that there is a limitation as 1 trunk on the WAN2 and 4 trunks on vSwitch, so 5 devices only.

➤ Answer:

The current design is for 4 devices only (VSAT + 4 or 5G + Starlink 1 + Starlink 2), as Marlink wants to keep the product standard. But technically, it is possible to configure more.

4- Question:

Will Starlink always be prepared for port 8?

What if customer will not ask us for Starlink bearer? Will we have there something else then? Or is Starlink bearer mandatory for them when subscribing SD-WAN solution?

➤ Answer:

The current design of the solution has all Starlink connected to port 7 or port 8 of the XChange. This detail is checked before the installation of the SDWAN so that the VM is configured accordingly. Once the SDWAN is deployed the Starlink must not be connected to a different port.

Whether the Starlink bearer is mandatory or not, for now yes. But this is a decision of the product marketing and could change at any time.

5- Question:

Who will be in charge when the customer would like to e.g. whitelist an application or a specific web address?

Who will be then updating the file on SharePoint (note: not all MNOC/RCS members have rights to adjust files on SharePoint).

➤ Answer:

Change requests can be sent by the customer to Service Desk directly. There is no need to go through the CSE or CSM teams. These requests must be transferred to CCTS as this is the team in charge of performing such modifications.

CCTS is also in charge of keeping the files on SharePoint up to date.

6- Question:

With an SDWAN installation, what is the status of remote access to modem, ACU, HP switch when Starlink is up but VSAT down?

➤ Answer:

In the current standard configuration, the VSAT components cannot be reached remotely if the VSAT is down. The point has been raised to the engineering team, they're currently reviewing possibilities.

7- Question:

On an installation with a SDWAN, is it still possible to access the 4G device via the URA?

➤ Answer:

As the 4G device is not directly connected to the URA, there will be no IP available for this device. The point has been raised to the engineering team as well.

8- Question:

For SDWAN installations, how can we monitor in the FortiManager if only the Starlink is down?

➤ Answer:

There is no way to determine if a bearer is online or not on an SDWAN installation using the FortiManager. However, the traditional methods remain available, such as checking the Starlink status in Merits.

9- Question:

What is the failsafe procedure if Fortigate stops working?

➤ Answer:

No issue directly due to the UTM or SDWAN has been observed so far. If such an issue, linked to the UTM or SDWAN themselves, ever happened and significantly impacted the vessel, without any solution, then failsafe procedure would be to perform a complete rollback of the

XChange configuration and recover a state without the Forti VM. This procedure can only be performed by CCTS and would only happen in last resort and in very specific circumstances.

10- Question:

What time zone is used in the logs displayed in the FortiManager?

➤ Answer:

The logs are displayed in UTC.

11- Question:

Can the XChange firewall configuration, at any level (Opel LAN, Group, Device), or the device firewall configuration in Data manager affect the communication of the UTM with the outside world (internet)?

➤ Answer:

The filtering rules setup in a UTM installation and those setup in the XChange Box are independent but both are enforced when a user performs a data session. For example, if a website is allowed in the UTM but not allowed in the DNS whitelist of the XChange user group trying to access it, then the URL will be blocked. And reversely, if the website is allowed by the DNS whitelist in the XChange user group but blocked by the UTM, the access will remain impossible.

Keep in mind that the UTM traffic and the users' data traffic are totally distinct. The users' data traffic is checked by the UTM and then goes through the devices regularly. The UTM has its own machine account and user group. This is to allow the UTM to discuss with the FortiManager only, there is no other purpose. So, the UTM needs to be allowed at the device level (in XChange and Data Manager) and its dedicated user group (CyberGuard UTM) needs to have connectivity. If the UTM cannot communicate, the users' data traffic will not be affected unless the disruption lasts longer than 30 days. In case this can be anticipated (e.g. if the VSAT is out of service and the vessel uses its backup only for 30 days or more) then you should let CCTS know the soonest.

12- Question:

With SDWAN deployed is there any way to reach XC over VSAT SRA?

➤ **Answer:**

With SDWAN the XChange Box remains reachable from both URA and SRA from the VSAT Native VLAN. However, the installation of the SDWAN service causes the remote IP to change. This information is updated in the network drawing.

13- Question:

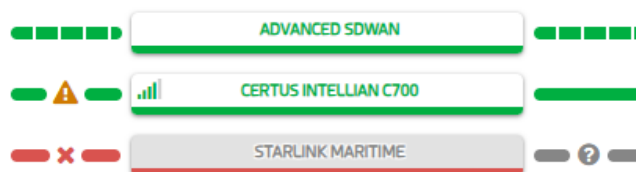
In the UTM firewall policies, there are some rules for Marlink products are mandatory, what if a customer doesn't have one of the related products (e.g. SkyFile Mail)?

➤ **Answer:**

As these rules are set in the UTM, they only apply to the traffic between the LAN and the XChange. If a customer does not have one of the related products, it has no impact. Indeed, the UTM will continue and scan the next rule. It does not create particular concern neither as these rules are behind the devices which are on the Marlink private network.

14- Question:

On a vessel with an SDWAN installation, I found on the XChange home page, the Starlink device in a red status. Is this normal? This can create confusion.



➤ **Answer:**

Yes, it is normal. In the standard design we keep the Starlink device configured on the XChange and available on the port where it used to be. This is meant as a last resort solution to have connectivity in case the SDWAN would ever have issues.

As this can create confusion indeed, we are reviewing possibilities to give more clarity.

15- Question:

How will the FortiGate firmware upgrades be managed?

➤ **Answer:**










This is transparent and it will be managed in the same way as OVP upgrades.

16- Question:

How is the application-based routing implemented (VSAT vs. Starlink) and how it can be verified?

➤ **Answer:**

This can be read in the FortiManager: *Device & Group > select the vessel > Network > SD-WAN*. Each rule (corresponding to e.g. an App) will display the connectivity used in the column Members. The devices are displayed in their relative priority order.

ID	Name	Source	Destination	Criteria	Members
7	URA_marlink_SLA_Starlink	All			 vlan216 (STARLINK_1)  vlan459 (VSAT)
1	HP_ANY_BL	All			 vlan210 (4G_210)  vlan216 (STARLINK_1)  vlan459 (VSAT)
2	SP_ANY_BL	All			 vlan210 (4G_210)  vlan216 (STARLINK_1)  vlan459 (VSAT)
3	CRW_ANY_MB_10MBPS	All		Latency	 vlan216 (STARLINK_1)

17- Question:

How frequent are the Fortinet definitions uploaded to the FortiGate and how much bandwidth does it consume?

➤ **Answer:**

We are pushing definition updates once a day to the vessels. The size of the update will vary but should be less than 100 MB (around ~50 MB in average).

18- Question:

Will RCS and MNOC have access into FortiManager?

➤ **Answer:**

The question of the access should be addressed to the management.

At the time of this document, the MNOC team already has access to the FortiManager. For the RCS, the request has been channelled through the management to the engineering team, which is estimating possibilities as there could be load issues.