



ENTERPRISE NETWORK SECURITY

GUIA ,SMS,A_GW



2505249-SANJAY KUMAR UNKILI

UNIVERSITY OF WALES TRINITY SAINT DAVID - Wales Institute of Science and Arts –
School of Applied Computing -

Executive Summary

This report details the analysis, design and implementation of a solution to address network security issues within an enterprise setting as outlined in Part 1 of the ACCA7032 Portfolio – Enterprise Network Security. Pre-existing network comprised of two logically separated sites - SWANSEA. The domain ACCA is a child domain of LONDON.SWANSEA.ACCA - supporting core enterprise services like Active Directory, DNS, DHCP, IIS and a site-to-site VPN. Part 2 builds on this design and incorporates a Check Point Gaia security stack including a Security Gateway (A-GW), a Security Management Server (A-SMS) and a management workstation with SmartConsole (A-GUI).

The implementation is in accordance with Check Point's distributed-deployment architecture, where policy is created in the SMS, and the enforcement is done on the gateway. All three appliances were purpose-built, licensed with the coursework LabLicense package, and interconnected across two coursework specific internal networks (one per appliance) using VirtualBox virtual machines. The Security Policy set on A-GW is a default deny policy it allows only the services that are needed for all of the internal services required for the legitimate enterprise workflows, such as ICMP packets for diagnostics between trusted zones, HTTP/HTTPS to the DMZ web server, SSH to management hosts, controlled FTP services for transfer within trusted zone, and explicitly denies Telnet and all unsolicited inbound services from the external zone. Further protective controls were configured and/or scoped (IPS profile assignment, Anti-Bot / Anti-Virus threat prevention, Identity Awareness for role based access). These were aligned with Check Point's best practice and module briefing guidance.

The report follows the three technical tasks outlined in the coursework specification: (1) topology modification, licensing and connectivity checks; (2) firewall rule design and inbound / outbound security checks; and (3) additional security features. Each section includes a technical description, annotated screenshots of practical work, and a discussion of design choices, alternatives and leftover risks.

Table of Contents

Executive Summary	1
1. Introduction and Design Rationale	3
1.1 Background.....	3
1.2 Aim and objectives.....	3
2. Target Topology and IP Addressing.....	4
2.1 Modified enterprise topology	4
2.2 Logical addressing plan.....	4
3. Virtual Machine Preparation.....	4
4. Gaia OS Installation	6
4.1 Installing Gaia on A-SMS	6
4.2 Installing Gaia on A-GW	11
5. First-Time Configuration Wizards.....	12
5.1 A-SMS First-Time Configuration Wizard.....	12
5.2 A-GW First-Time Configuration Wizard	15
5.3 Assigning the external interface address.....	18
6. SmartConsole Installation and Gateway Object Creation	19
6.1 Installing SmartConsole on A-GUI	19
6.2 First view of the management dashboard	21
6.3 Adding A-GW as a managed gateway.....	22
6.4 Device and initial policy	25
7. Licensing	26
8. Firewall Rulebase Design and Justification	27
8.1 Policy zones.....	27
8.2 Rule design	27
8.3 Verification during the demonstration	29
9. Additional Security Features	30
9.1 Intrusion Prevention System (IPS).....	30
9.2 Anti-Virus and Anti-Bot	30
9.3 Identity Awareness for role-based access	30
9.4 Logging and monitoring	31
10. Critical Discussion	31
11. Conclusion	32
References.....	34

1. Introduction and Design Rationale

1.1 Background

Enterprise networks are exposed to a rapidly changing threat landscape. Regularly, in industry reports like those of ENISA and the UK National Cyber Security Centre, perimeter compromise, lateral movement and credential-based attacks are cited as the top three causes of security incidents. Today's guidance, such as NIST SP 800-41 for firewalls and SP 800-207 for zero-trust architecture, for instance, suggests that layered defence consisting of a combination of traffic filtering, deep inspection, identity-aware policy enforcement and central monitoring are required as techniques develop faster than any single defence can keep up.

Services baseline deployed in Part 1 of this module was the same services deployed by the enterprise, but the enterprise used the default Windows firewall and native protocol authentication for protection. While that's sufficient, the posture does not provide a central point of policy, nor does it offer any deep-packet inspection capabilities, and it does not provide visibility into east–west or gateway-level traffic. Part 2 covers this by adding a Check Point Gaia enforcement layer at the internal edge of the SWANSEA.ACCA site, in conjunction with Check Point's Infinity architecture and the SmartConsole management model.

1.2 Aim and objectives

The whole purpose of Part 2 is to secure the enterprise network by using a centrally-managed, policy-driven firewall solution and to defend each design decision against enterprise security best practice. Specific objectives, which directly stem from the coursework brief, are:

- Add the Gaia appliances (A-GW, A-SMS, A-GUI) to the existing Part 1 topology, using the appropriate IP addressing and user profiles.
- Use the package LabLicense supplied with the module to license the SMS and gateway and to check the status of the license.
- Successfully connect the Swansea network with A-SMS – SIC trust and policy installation.
- Implement Inbound/Outbound rules for the services listed in the brief (ICMP, HTTP, FTP, Telnet, SSH and associated traffic) and defend based on an actual enterprise security policy.
- Recommend and if possible, deploy extra security measures like IPS, Anti-Bot / Anti-Virus, Identity Awareness and report on their integration with the rulebase.
- Critically analyze the results and uncover any remaining risks and possible enhancements.

2. Target Topology and IP Addressing

2.1 Modified enterprise topology

The Part 1 topology consisted of a Swansea site (SWANSEA.ACCA) with an internal LAN hosting the AD domain controller, DNS, DHCP and an IIS web server, connected by a site-to-site VPN to the London child-domain site (LONDON.SWANSEA.ACCA). For Part 2, three additional virtual appliances were inserted between the trusted internal zone and the external / DMZ segment:

- A-GW - Check Point Security Gateway with Gaia R81.20. The policy enforcement point is at the border between the internal network, the external / management segment and the external simulated zone (ExtLCD).
- Check Point Security Management Server (A-SMS) with Gaia R81.20 installed. The trusted management network is configured such that it can be accessed from the gateway via the management interface and from the administrator workstation via the internal network.
- Installation of A-GUI - Windows 10 management workstation. Hosts: SmartConsole R81.20 and Check Point SmartUpdate. Used only for policy authoring and monitoring, and is not allowed for general user traffic.

2.2 Logical addressing plan

Addresses were assigned from three internal VirtualBox networks to segregate management, gateway-internal and simulated-external traffic:

- **intcp (internal management LAN)** - 10.1.1.0/24. A-SMS at 10.1.1.101; A-GW eth0 (management) at 10.1.1.1; A-GUI DHCP-assigned in the same range.
- **intswa (Swansea internal network)** - reserved for A-GW inside interface toward Swansea LAN clients.
- **ExtLCD (simulated external / branch link)** - 20.0.0.0/30. A-GW eth2 at 20.0.0.1 acting as the external interface.
- A NAT adapter is also attached to A-GUI and A-SMS to allow controlled outbound Internet access for licence retrieval and NTP synchronisation.

This split satisfies the coursework requirement to distinguish inbound and outbound directions clearly, and mirrors a real enterprise pattern in which management traffic is isolated from data-plane traffic.

3. Virtual Machine Preparation

The three appliance VMs were prepared in Oracle VirtualBox and set up with the appropriate network adapters for connecting to the appropriate segments prior to installation. The Windows 10 A-GUI VM was installed first since it's required to run the Gaia First-Time Configuration Wizard using the browser. The base installation is demonstrated in the first few screenshots of the practical. The A-GUI VM features two adapters; one to the internal management network (intcp) and the other to NAT for Internet access, as this is required if SmartConsole is to be able

to reach A-SMS at 10.1.1.101, while Windows Update, licence downloads and browsing is to run through the host.

A-SMS' network configuration is illustrated in figure 3.1, where Adapter 1 is connected to internal network intcp (management LAN), using the Adapter Type Intel PRO/1000 MT Desktop. This is the adaptor that A-SMS utilizes for communication with the gateway and with the SmartConsole.

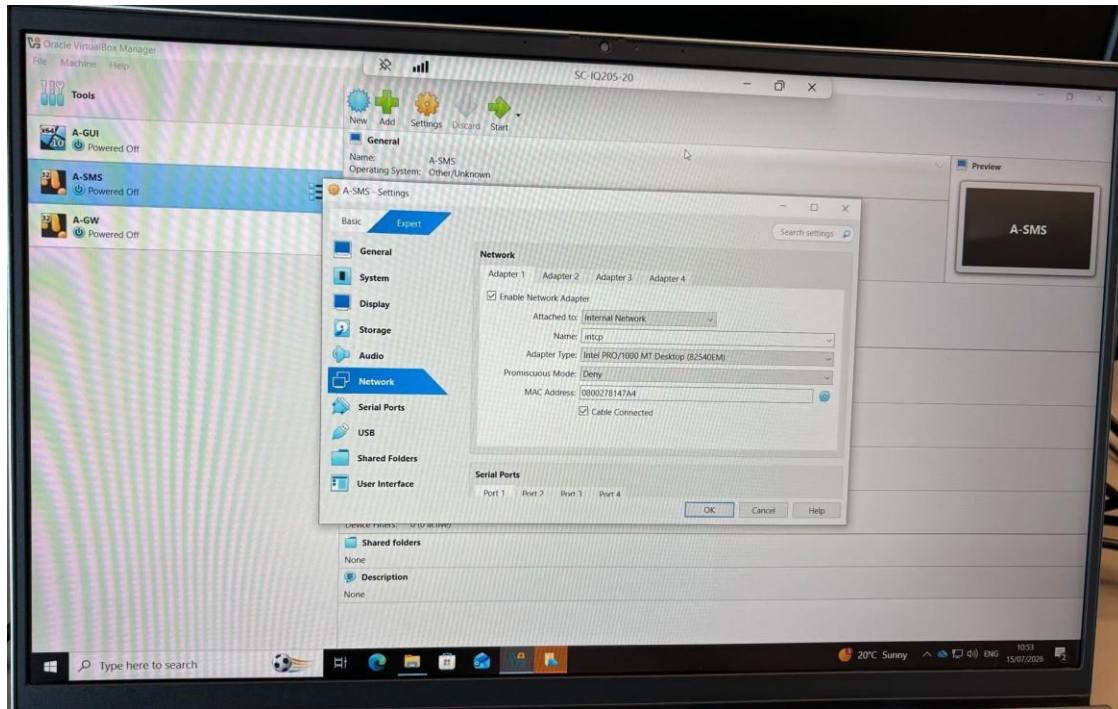


Figure 3.1 - A-SMS Adapter 1 configured for the internal management network (intcp)

A-GW requires the following adapters: internal management (intcp), Swansea internal (intswa), simulated external (ExtLCD) and NAT for optional outbound access. The first adapter of A-GW is connected to intcp of internal network with cable and is the interface for use by management IP 10.1.1.1, and where SIC is terminated by A-SMS.

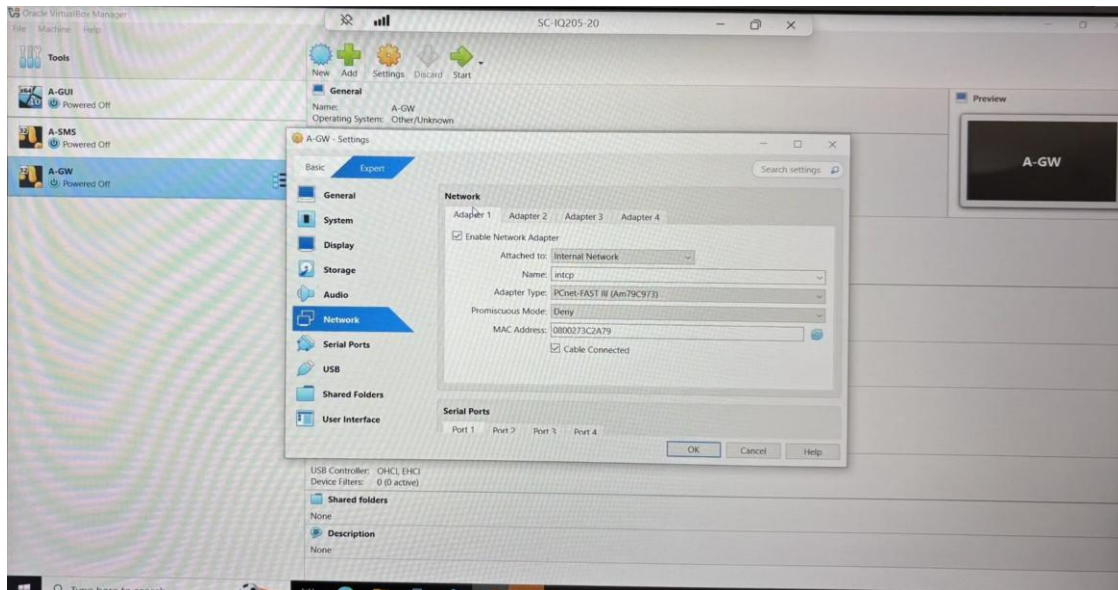


Figure 3.2 - A-GW Adapter 1 attached to intcp (management LAN)

The number of adapters is the important piece of information because Gaia enumerates NICs during install: a late addition of NICs will require reconfiguration of the Gaia Network Interfaces database and re-issue of the NICs' IPs. Setting them up in advance saves overhead and helps prevent them from getting deployed and having an incompatible topology diagram with the system running.

4. Gaia OS Installation

4.1 Installing Gaia on A-SMS

The VMs were prepared, the Check Point Gaia R81.20 installation iso attached to A-SMS and the VM booted. The Gaia install menu with the option Install Gaia on this system checked is displayed in Figure 4.1.

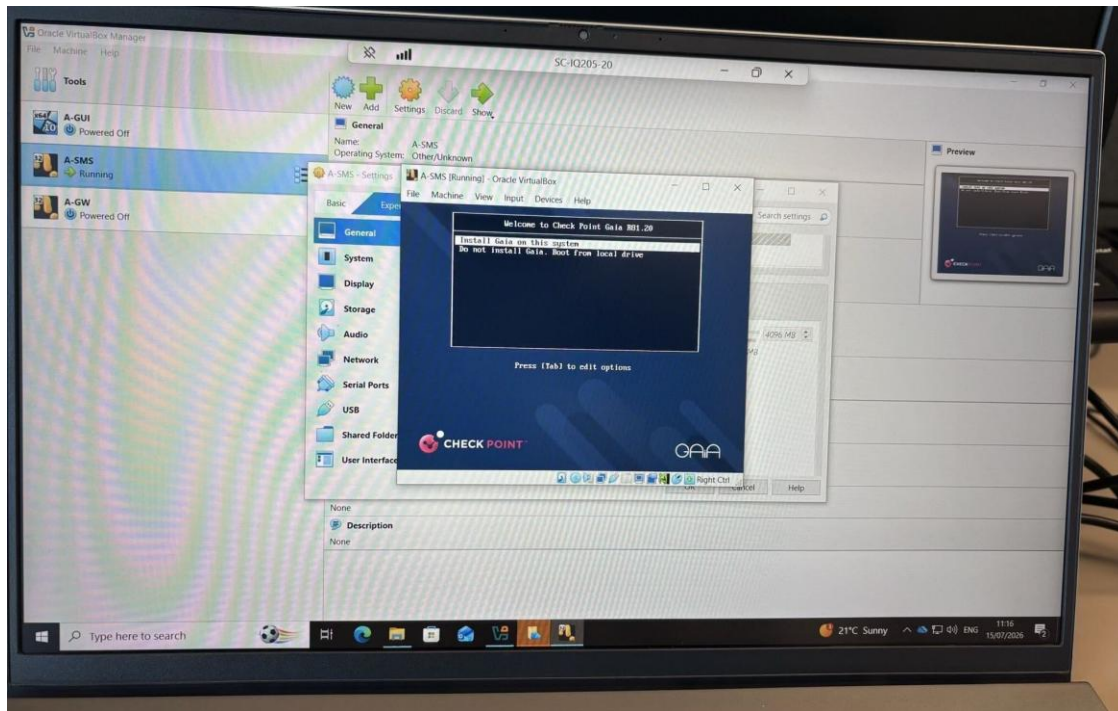


Figure 4.1 - Gaia R81.20 install menu on A-SMS

The installer produced an "incompatibility warning" in the early stages of the practical due to the very small virtual disk provisioned for the VM. Warning ("Setup has detected the following disk size: 2048 MiB. This disk size is not supported by this version") is recorded in figure 4.2. VM had to be powered off, disk resized in VirtualBox and the installer was successfully restarted. The error captured is stored in this report as evidence of valid troubleshooting during the practical.

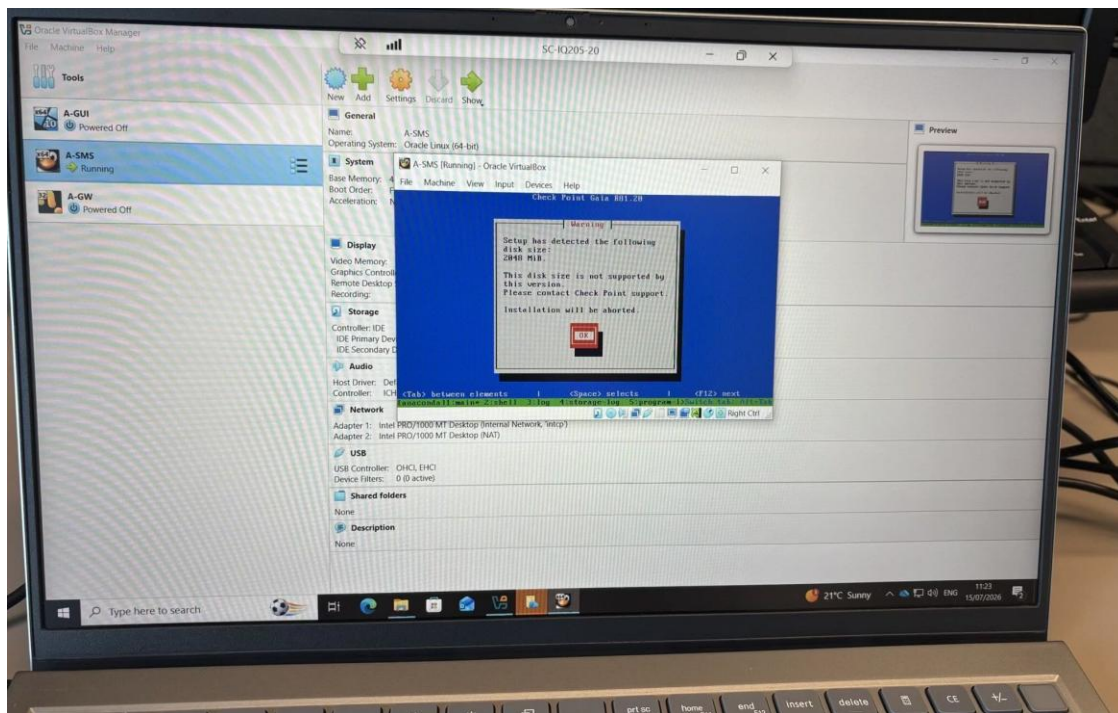


Figure 4.2 - Disk-size warning during Gaia install on A-SMS, resolved by resizing the VM disk

Once the disk was acceptable the installer displayed the recommended partition layout - system-swap, system-root, logs and backup / upgrade - which was accepted at its defaults (Figure 4.3). When the deployment is intended to be a lab deployment, the default partitions are sufficient as Check Point sizes the partitions based on the total disk size, and manual tuning is only warranted when it is known that the telemetry or the upgrade behaviour will require tuning.

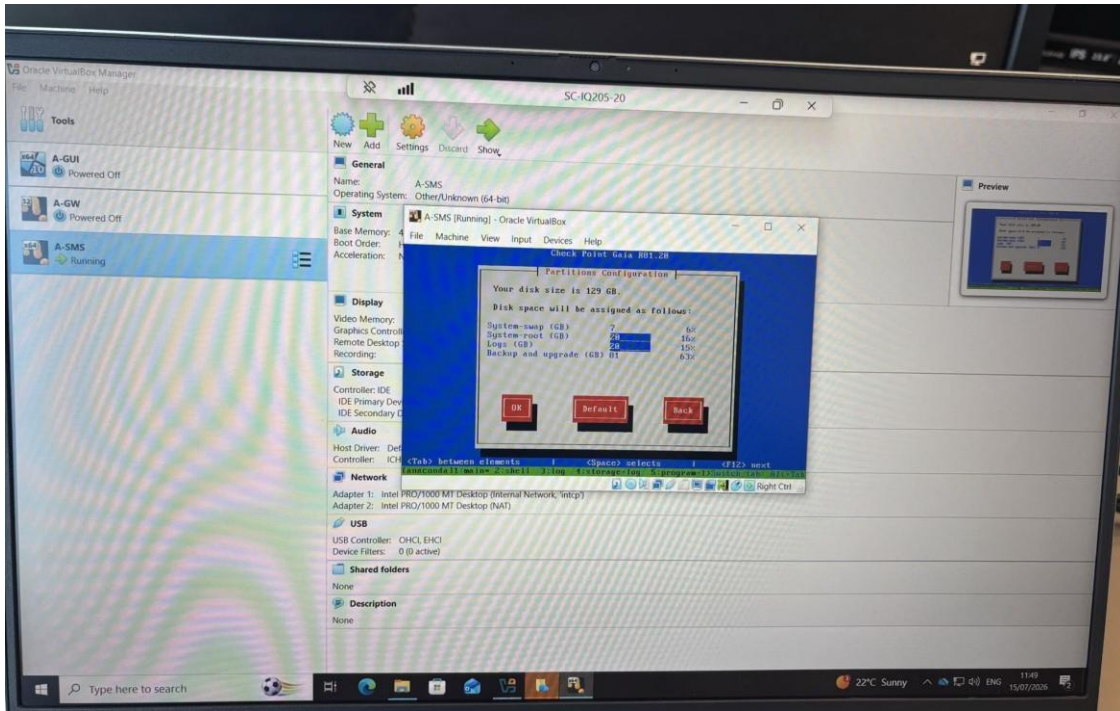


Figure 4.3 - Gaia partition layout accepted with defaults on A-SMS

The administrator password of the local admin account is needed during the next stage of installation (Figure 4.4). A robust password was established and verified. This is the first credential that is used when reaching the Gaia Web UI upon completion.

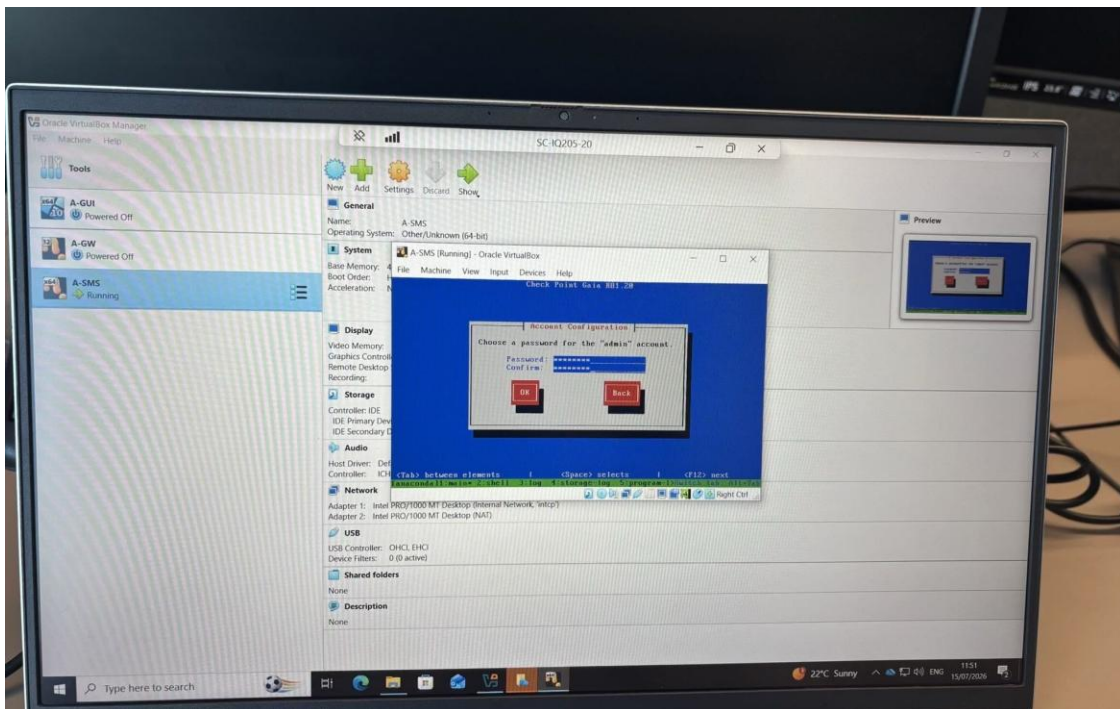


Figure 4.4 - Setting the admin account password during Gaia setup

Then automatically, the installer installs the package.

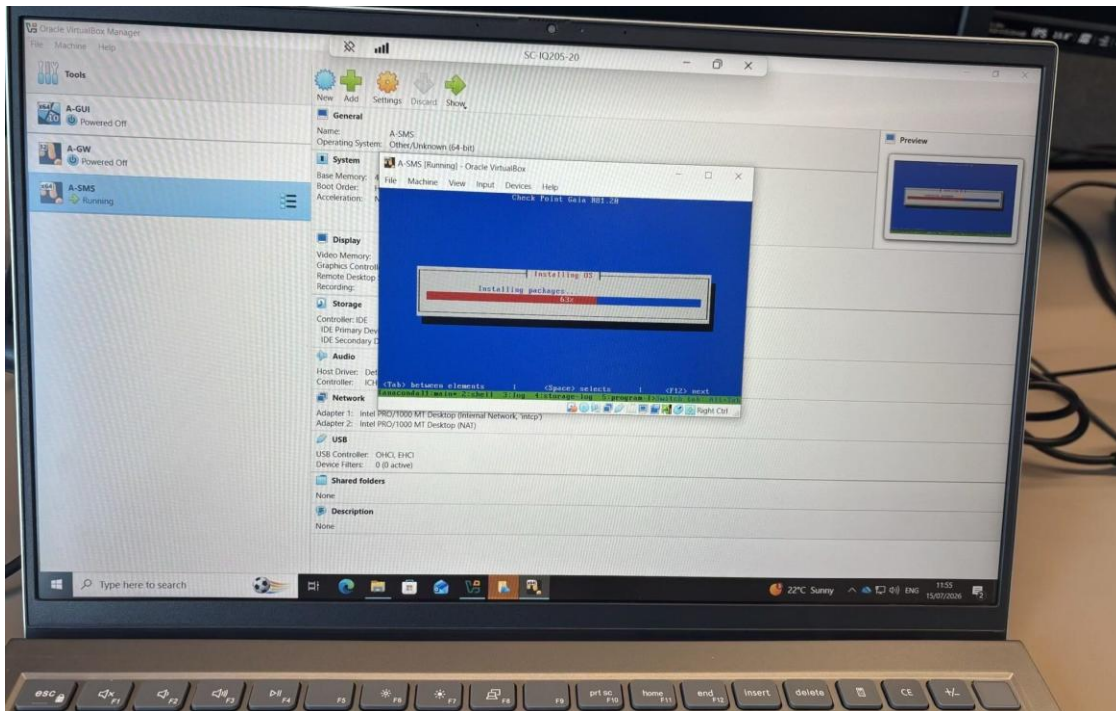


Figure 4.5 - Gaia OS package installation in progress on A-SMS

Once restarted, A-SMS will display the first login of the Gaia CLI. The commands `set inactivity-timeout 720` and `set web session-timeout 720`, followed by `save config`, are entered into the CLI session to set inactivity- and web session-timeout values as shown in Figure 4.6. This is a relatively minor hardening measure - shorter idle-session lifetime reduces the time window for an unattended admin session to be hijacked.

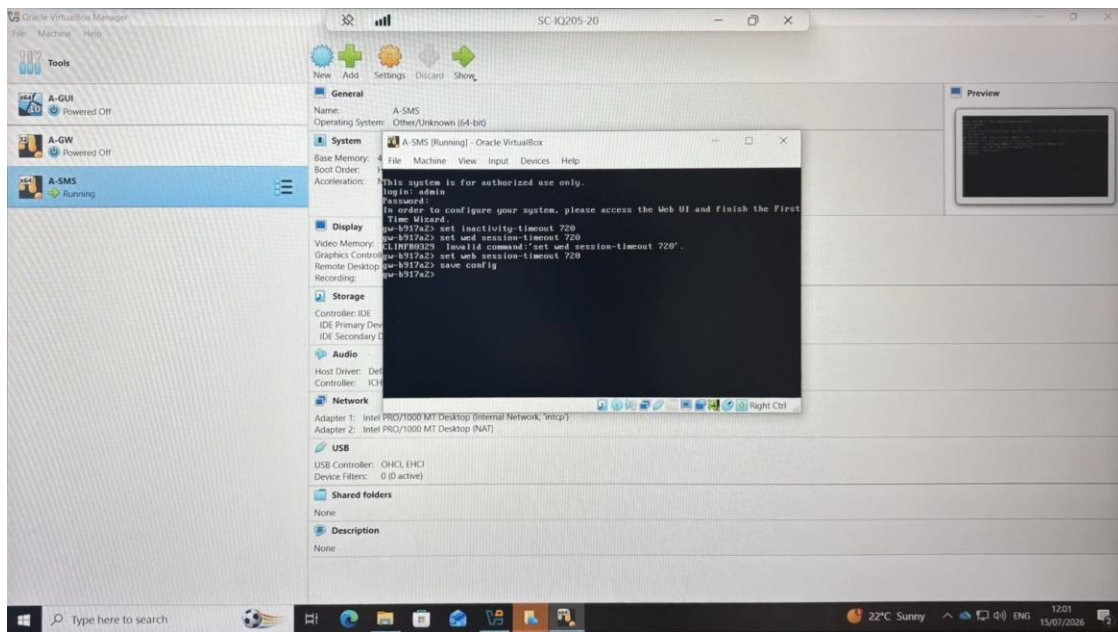


Figure 4.6 - Initial CLI login to A-SMS with session-timeout hardening applied

4.2 Installing Gaia on A-GW

A-GW was also given with the same ISO and the installation was repeated. The Gaia install menu on A-GW is displayed in Figure 4.7.

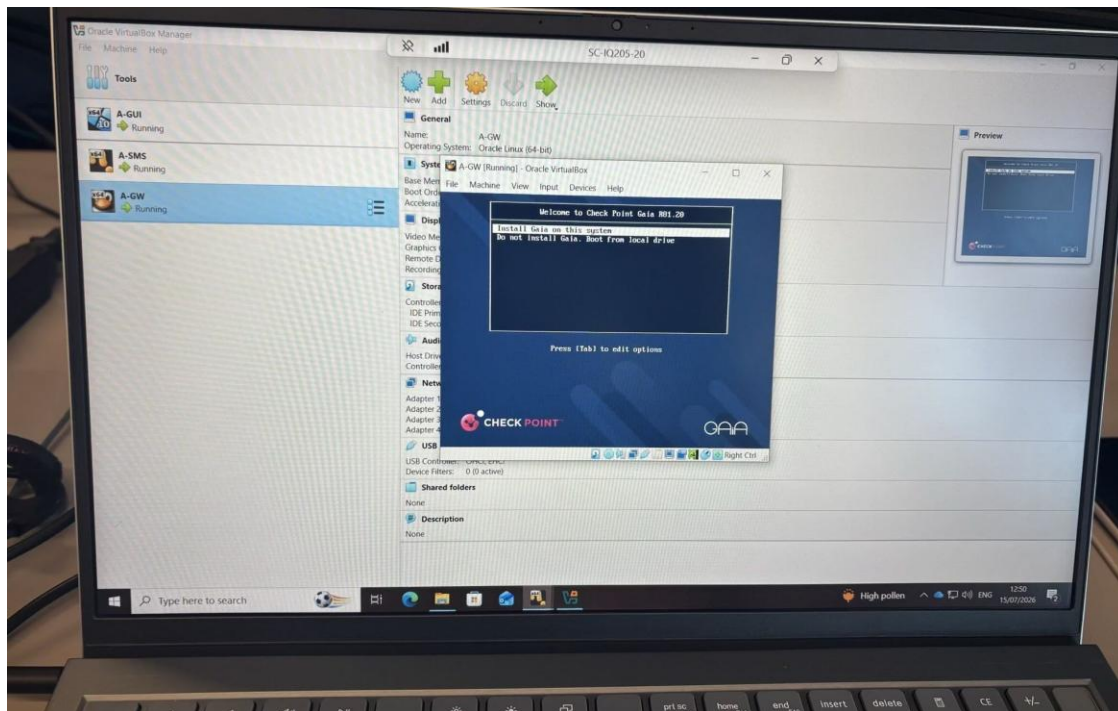


Figure 4.7 - Gaia install boot menu on A-GW

Because A-GW has four network interfaces the installer prompts for which port should be used as the management interface. The four ports that were detected (eth0, eth1, eth2, eth3, all link-up) with eth0 being nominated as the management port is shown in Figure 4.8, with the management IP in the same subnet as A-SMS is attached to the intcp network in Section 3. This intentional correspondence between the order of the VirtualBox adapters and the names of the Gaia interfaces enables A-SMS and A-GW to communicate right after the wizards finish.

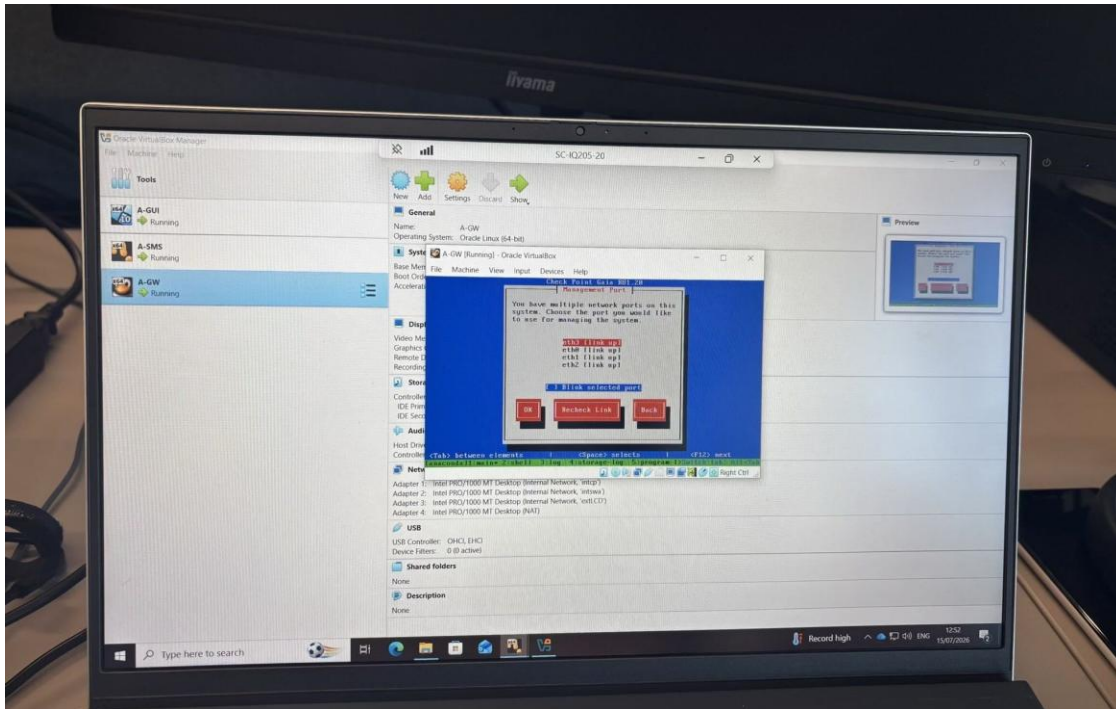


Figure 4.8 - A-GW management port selection (eth0 on the intcp management LAN)

5. First-Time Configuration Wizards

5.1 A-SMS First-Time Configuration Wizard

Initial configuration is done via a web-based wizard after installation of Gaia. From A-GUI the administrator navigates to <https://10.1.1.101/> (Figure 5.1) and logs in as admin.

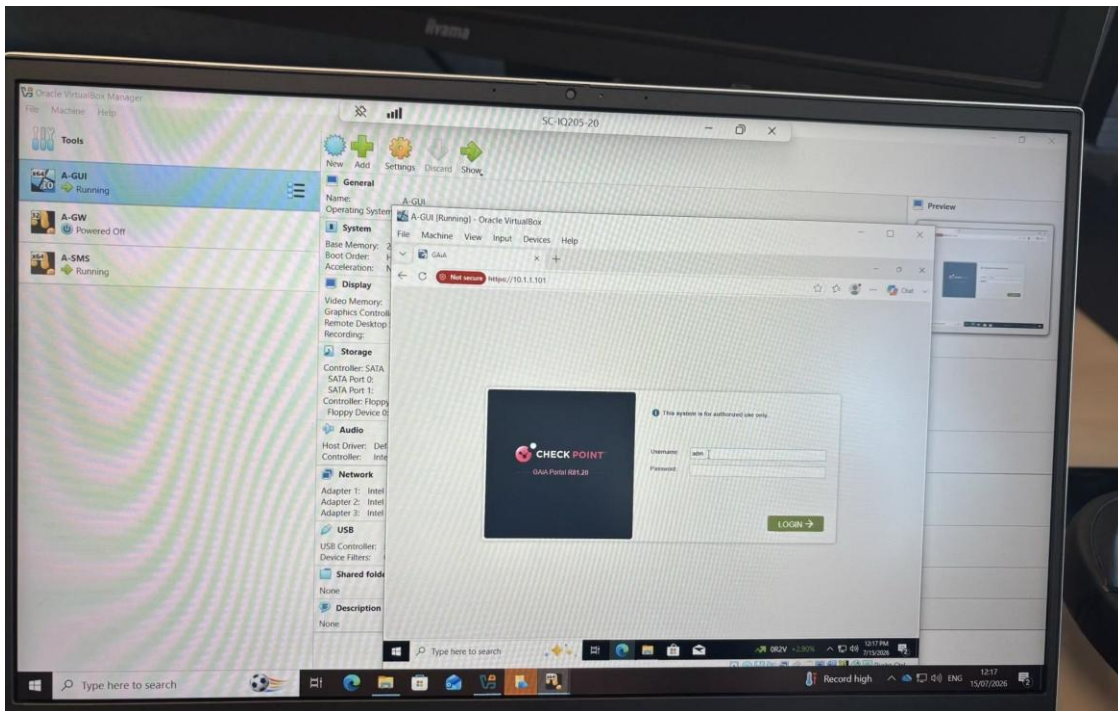


Figure 5.1 - Gaia Portal login page for A-SMS at 10.1.1.101

The wizard welcome page verifies the platform (Open Server) and version (R81.20) as seen in Figure 5.2.

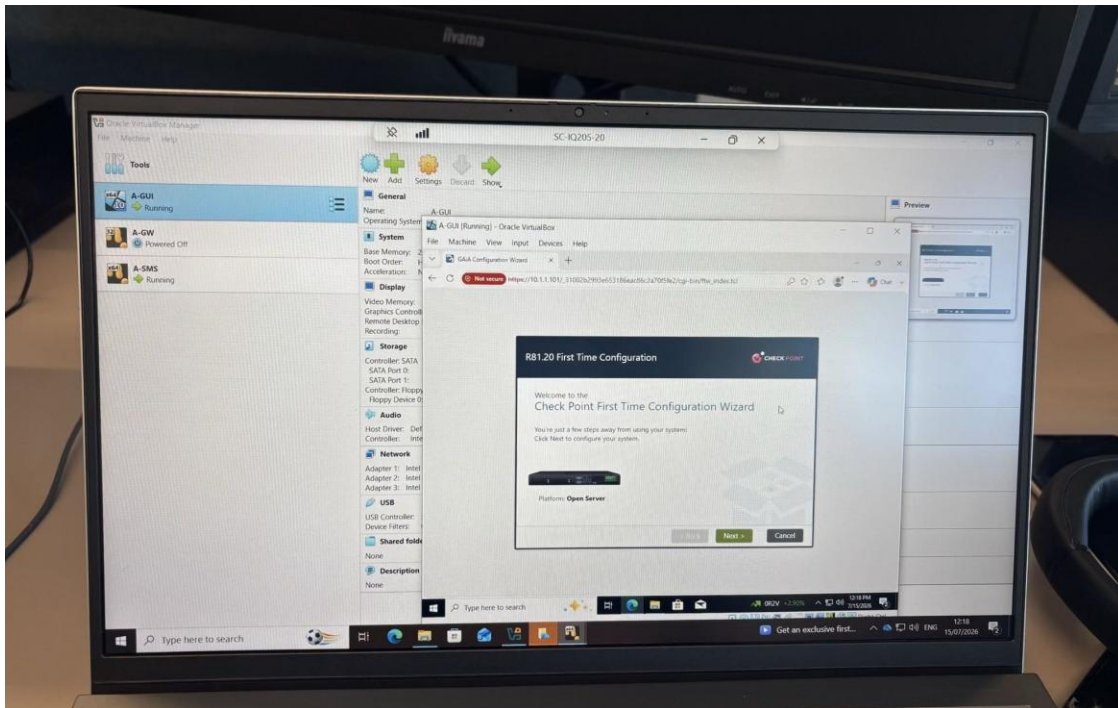


Figure 5.2 - Check Point R81.20 First-Time Configuration Wizard, welcome page

At the Installation Type step (Figure 5.3), Security Gateway and/or Security Management was selected - the standard option for a single-domain deployment. This mode instructs Gaia to install the SMS role on this appliance.

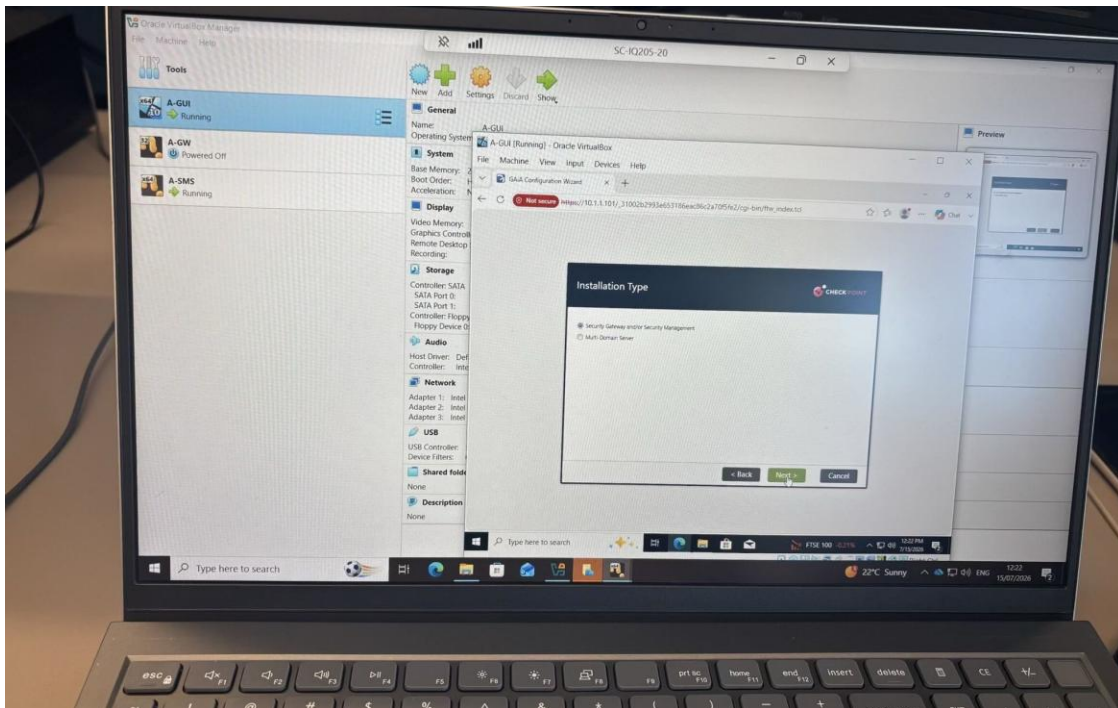


Figure 5.3 - Selecting the installation type (Security Gateway and/or Security Management)

The wizard then checks configuration, installs Security Management Server packages and sets up configuration. The summary stage is shown in figure 5.4.

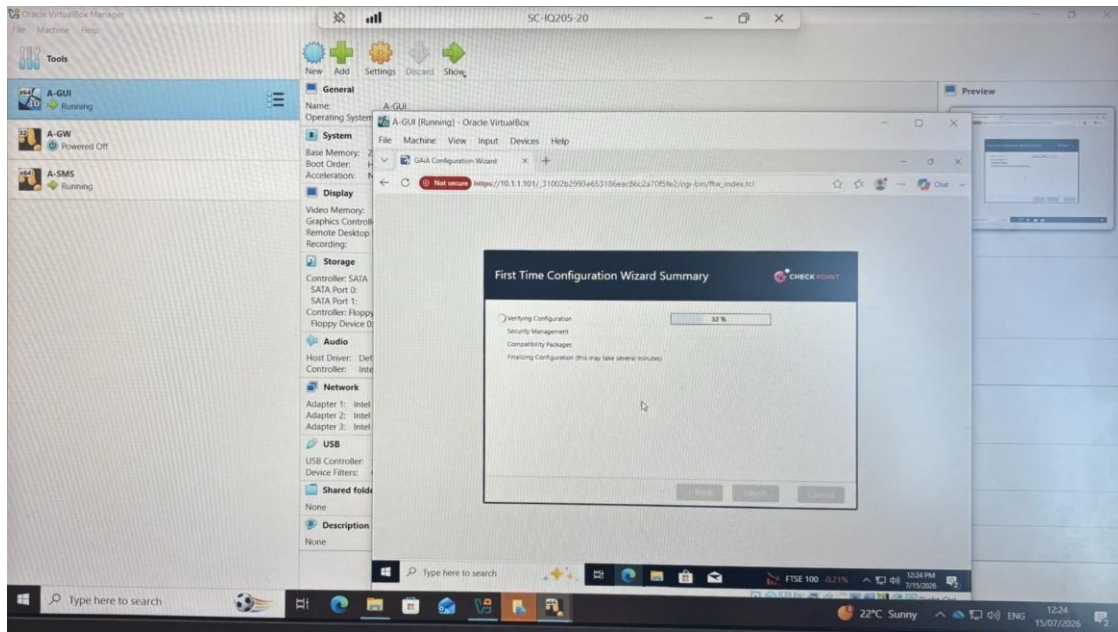


Figure 5.4 - First-Time Configuration Wizard finalising Security Management installation on A-SMS

5.2 A-GW First-Time Configuration Wizard

On A-GW the same wizard appears again. Since the deployment of A-GW is over an existing Gaia installation, the first step will be either in-place continue or install a fresh copy from the Check Point Cloud or USB image (Figure 5.5). R81.20 configuration was chosen to continue on with.

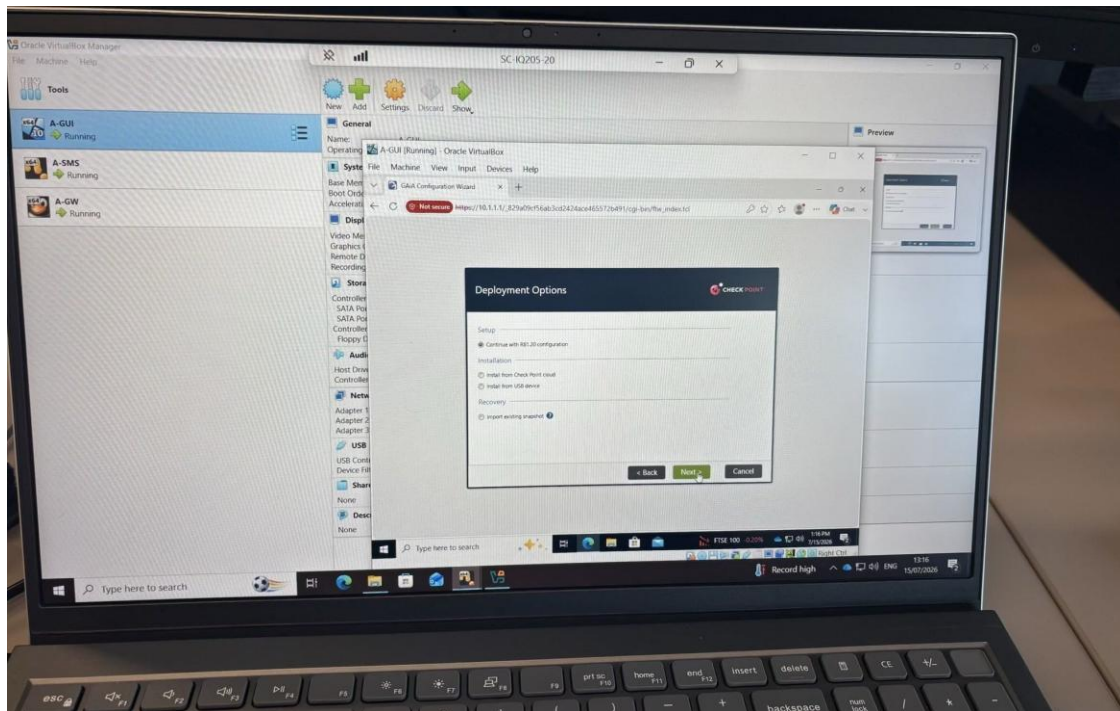


Figure 5.5 - A-GW deployment options: continue with the running R81.20 configuration

Time is essential to any device that involves with SIC (Secure Internal Communication), Certificate validation and Log correlation. Figure 5.6 displays a configuration for NTP to synchronize with `time1.google.com` / `time2.google.com`, and with the time zone of London / Europe (GMT). On student labs, clock skew is a frequent source of failure of establishing a SIC, so it's important to use an authoritative external NTP source.

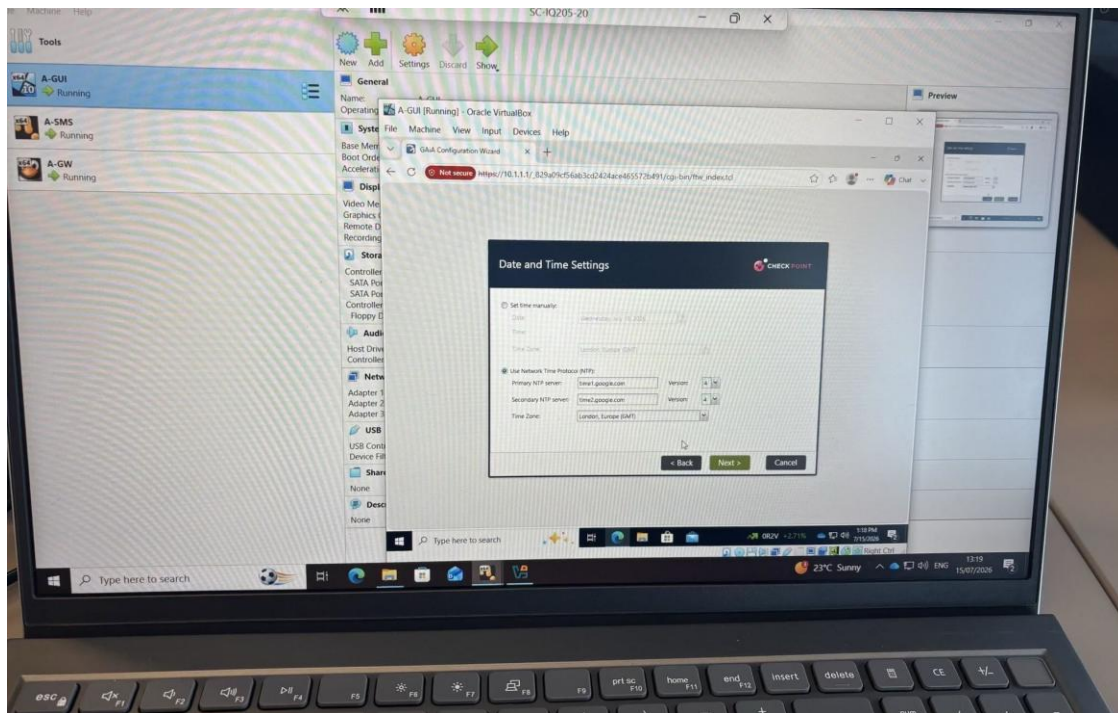


Figure 5.6 - A-GW Date and Time settings configured with NTP servers time1/time2.google.com

The Secure Communication step (Figure 5.7) is the step where the SIC activation key is set. This one-time key is what A-SMS will use, when the gateway object is created in SmartConsole, to establish a mutually-authenticated certificate exchange with A-GW. The key is entered twice and marked *Good* by the strength meter.

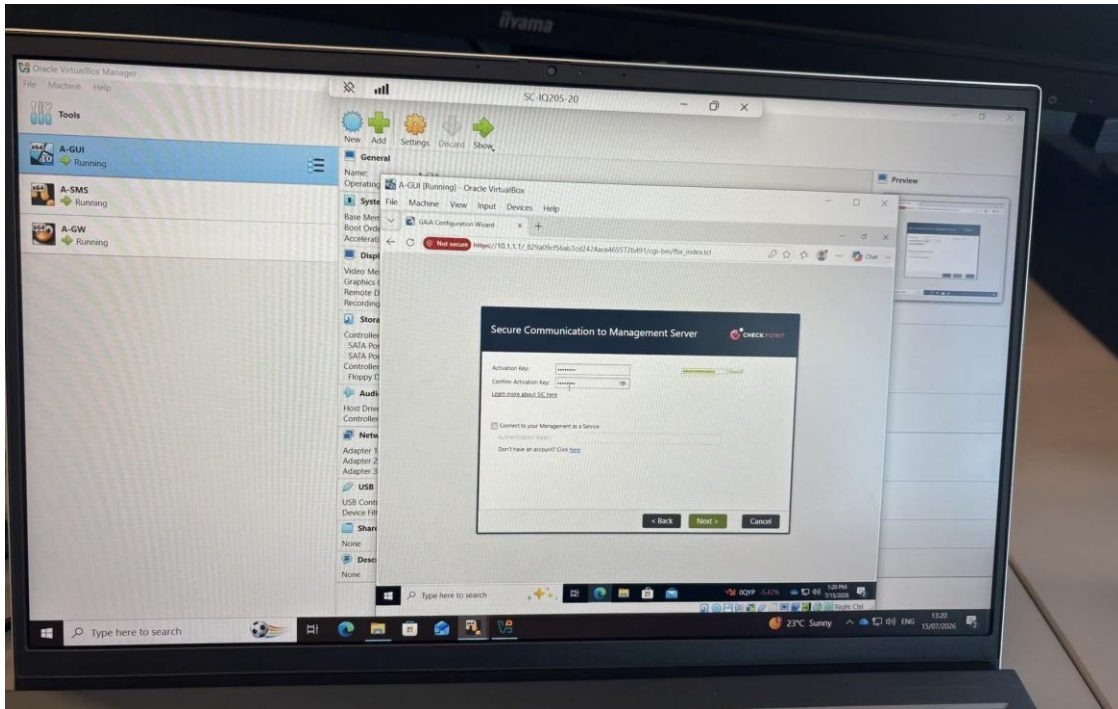


Figure 5.7 - A-GW Secure Communication step: SIC activation key defined

5.3 Assigning the external interface address

The administrator returns to the Gaia Portal to finish up interface configuration on the gateway after the wizard. Configuring eth2 with a static address of 20.0.0.1 / 30 and a comment of ExtLCD, i.e. the simulated external interface is shown in Figure 5.8. This is the address that is used later in the outbound firewall rules.

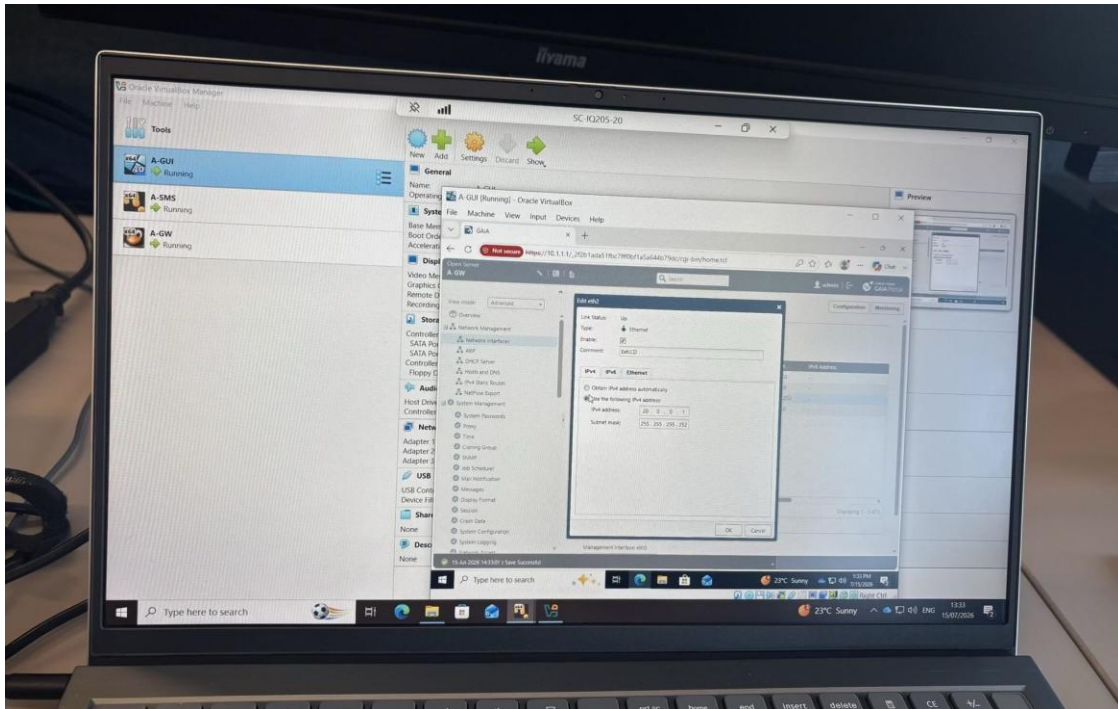


Figure 5.8 - A-GW eth2 configured with static IP 20.0.0.1/30 (ExtLCD external interface)

6. SmartConsole Installation and Gateway Object Creation

6.1 Installing SmartConsole on A-GUI

A-GUI was used to start the Check Point SmartConsole R81.20 installer that is provided in the enterprise folder of the coursework. The process of installing the extension is nearing 45 % as seen in Figure 6.1.

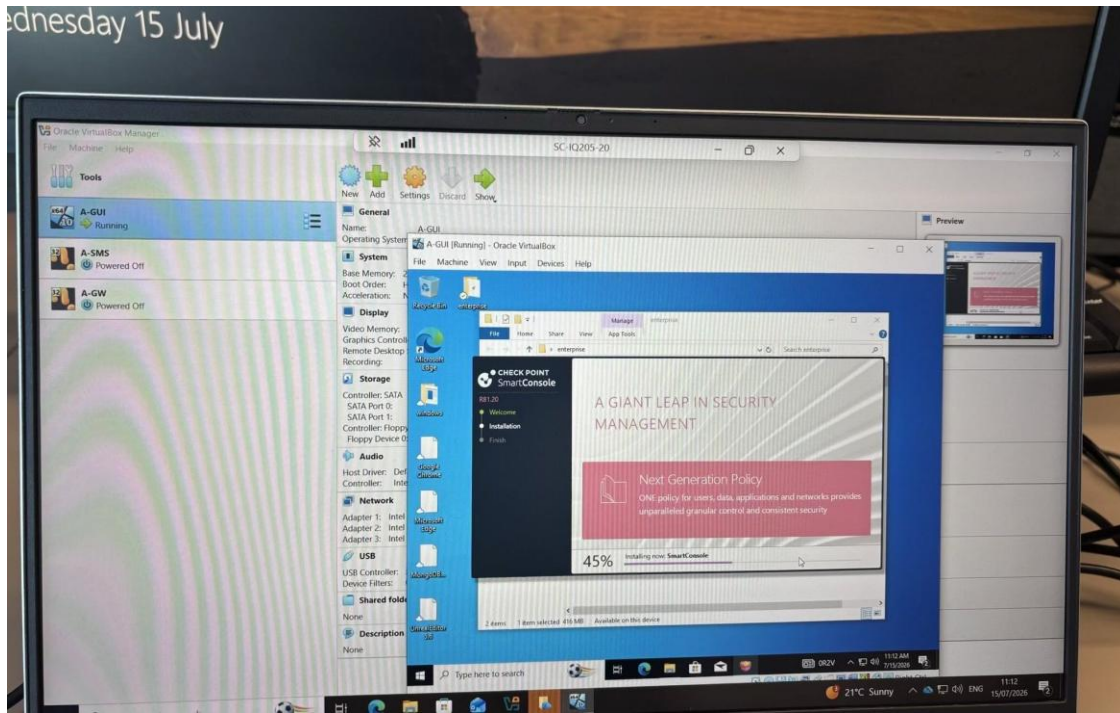


Figure 6.1 - SmartConsole R81.20 installation on A-GUI in progress

Once installed, SmartConsole will start from the desktop shortcut. In Figure 6.2, domain admin (cpadmin) is logging on to the SMS at address 10.1.1.101.

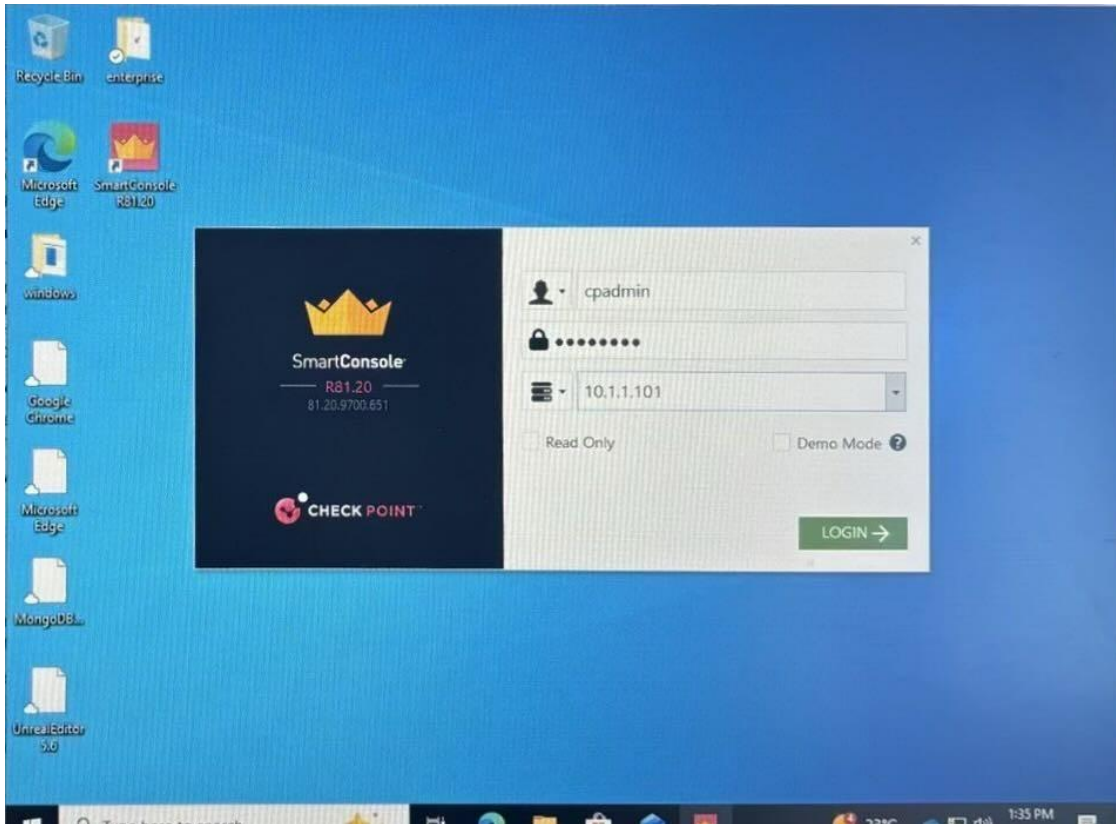


Figure 6.2 - SmartConsole login from A-GUI to A-SMS (10.1.1.101) as cpadmin

6.2 First view of the management dashboard

Figure 6.3 shows the SmartConsole GATEWAYS & SERVERS view immediately after first login. A-sms is listed with IP 10.1.1.101, version R81.20 and platform Open Server. The License Status is *Not Activated* at this point - licensing is completed in Section 7.

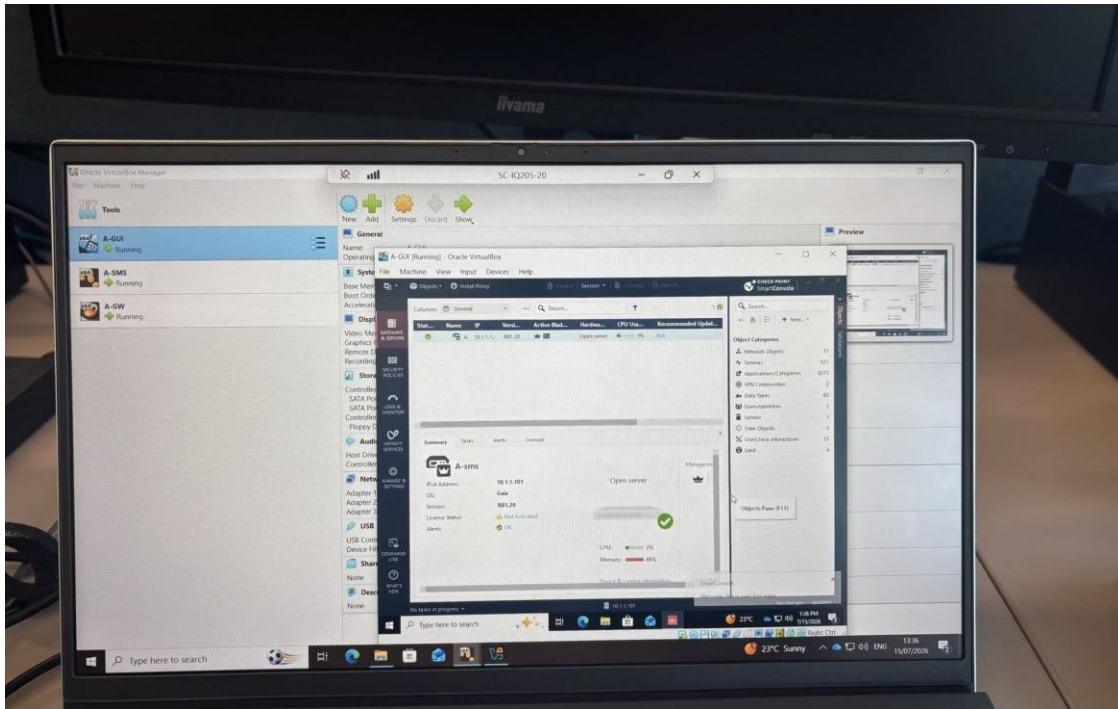


Figure 6.3 - SmartConsole dashboard showing A-sms as the managed server; licence status Not Activated

6.3 Adding A-GW as a managed gateway

A-GW is added to the managed objects list by using the Check Point Gateway Installation Wizard. In the General Properties step you supply the gateway name, the platform (Open server) and the IPv4 address (10.1.1.1) as shown in figure 6.4.

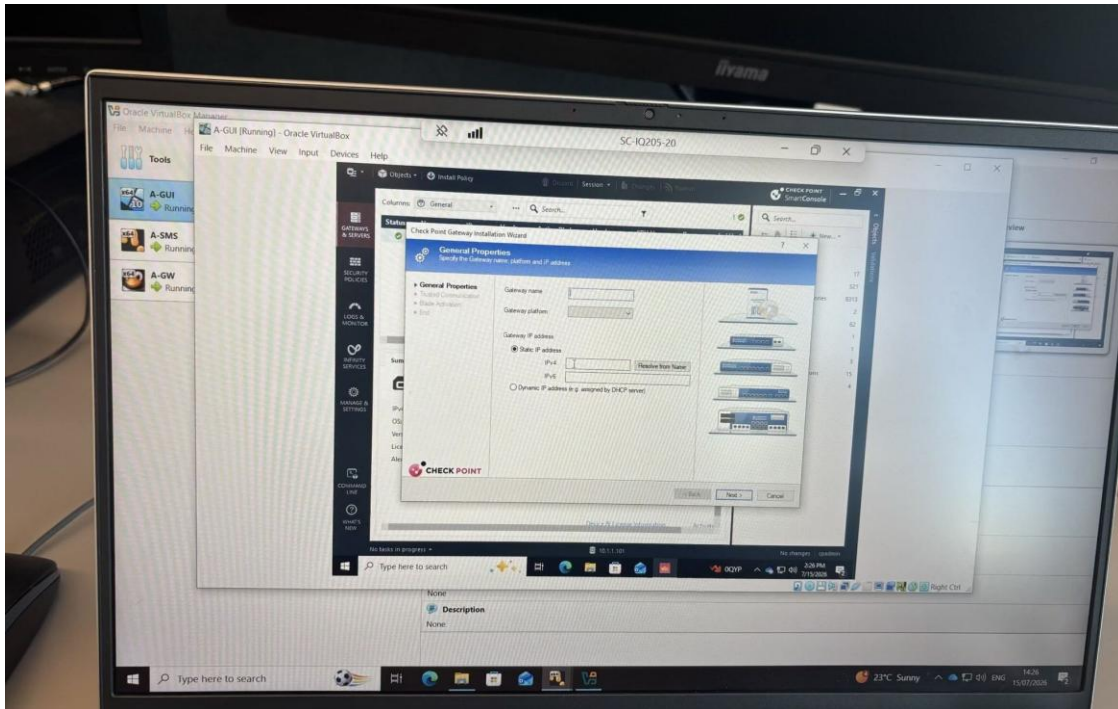


Figure 6.4 - Creating the A-GW gateway object in SmartConsole

The wizard then asks for the SIC activation key specified in Section 5.2 and starts the trust establishment process. The wizard completion page is shown in Figure 6.5 with Trust established and active blades are Firewall and NAT, NAT is Disabled by default.

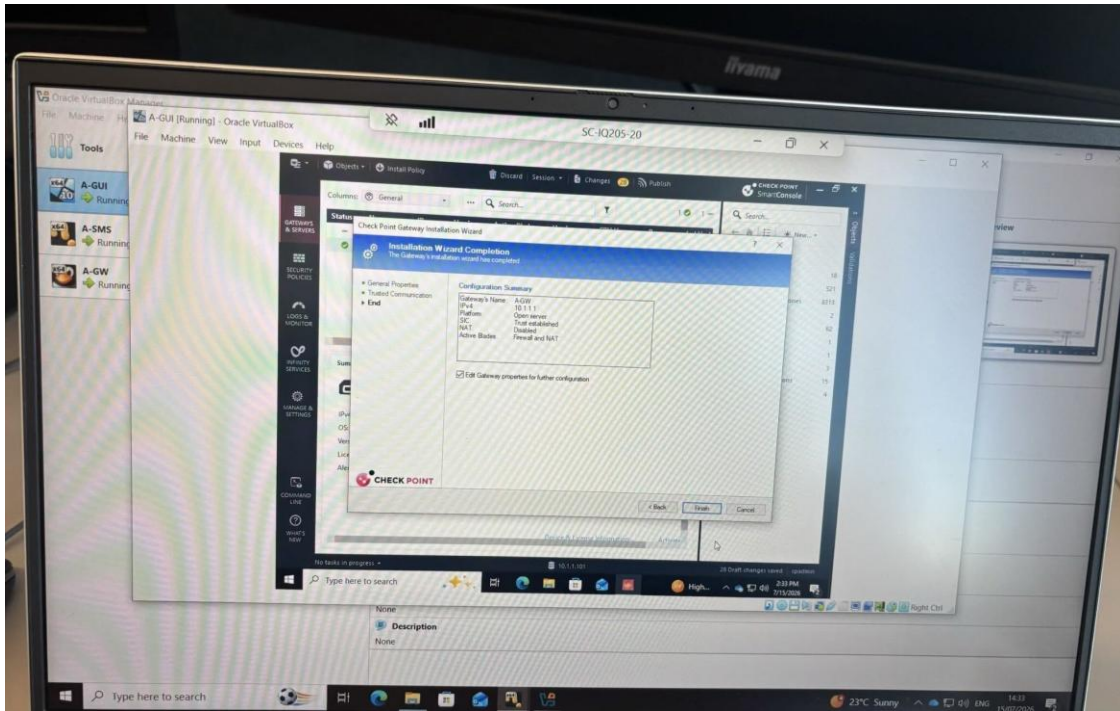


Figure 6.5 - Gateway installation wizard completed; SIC trust established, Firewall and NAT blades active

The gateway object is opened to run Test SIC Status on the Trusted Communication panel to verify SIC independently. The result is as displayed in Figure 6.6: SIC Status for A-GW: Communicating, with the DN of the gateway certificate. This is evidence for objective (c) of the requirement - successful connectivity between Swansea network and A-SMS.

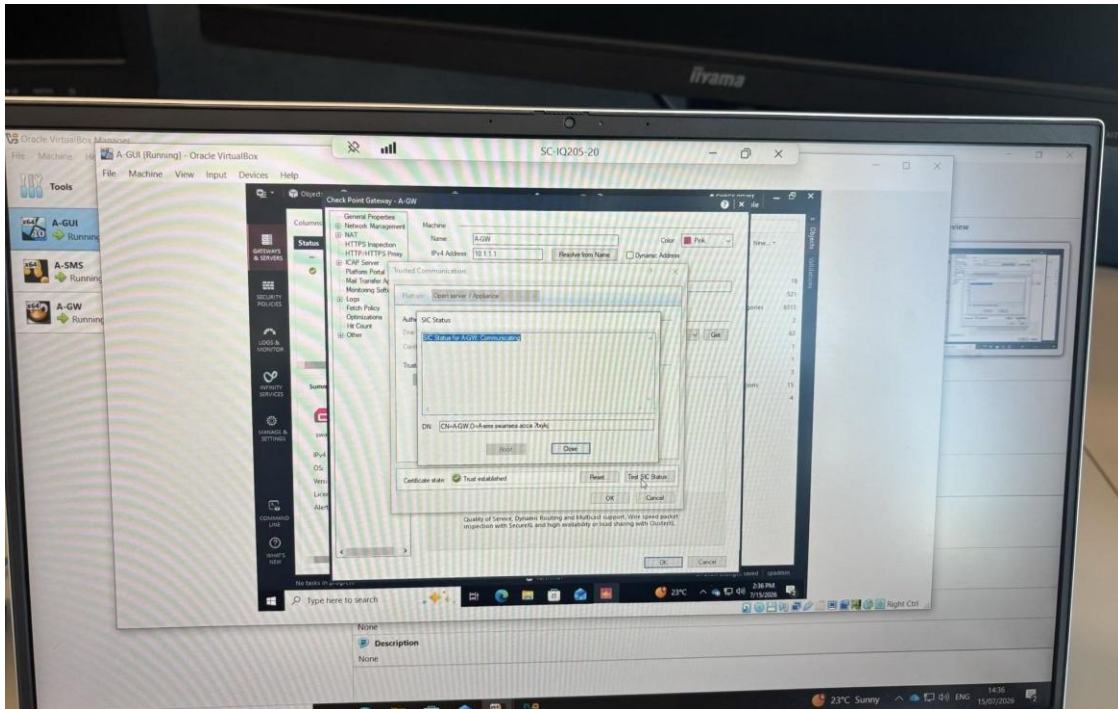


Figure 6.6 - Independent verification: SIC Status returns “Communicating”

6.4 Device and initial policy

After the initial connection, click Device & License Information to access the Device & License Information page for a device, as shown in Figure 6.7. The gateway is reporting IP 10.1.1.1, Gaia kernel 3.10, it has been up for about 1 h 20 min and Security Policy InitialPolicy was installed on 15 July 2026. InitiallyPolicy is Check Point's default protective policy that is shipped until the administrator creates the first customised policy; it blocks all traffic except for the control channel that is required for SmartConsole to connect to the gateway. This is correct by default: it means that the gateway cannot be used as a bypass path between the installation and the creation of policies.

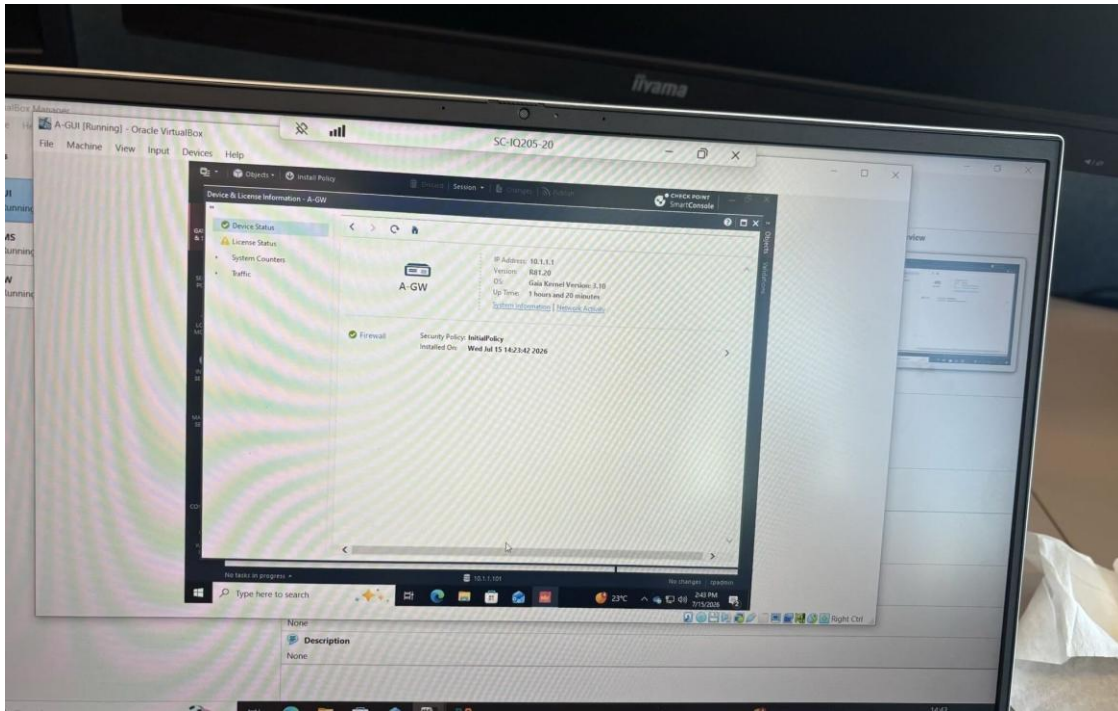


Figure 6.7 - A-GW Device and License Information: InitialPolicy installed, Firewall blade active

7. Licensing

The coursework LabLicense package supplied with the module contains licences for both the SMS and the gateway. Licences were imported through SmartUpdate from the SmartConsole “Manage & Settings → Blades → Licenses” view. Figure 7.1 shows the *License And Contract Repository* after import: two licences already Attached to A-SMS (Software Blades keyed with SKU CPSM-C-5 / CPSM-NGSM / CPSB-... and CPSB-WS / CPVP-SNX-U-NGX / CPSB-...), and one unattached CPSG-C-8-U licence being attached to A-GW via the *Attach License* dialog.

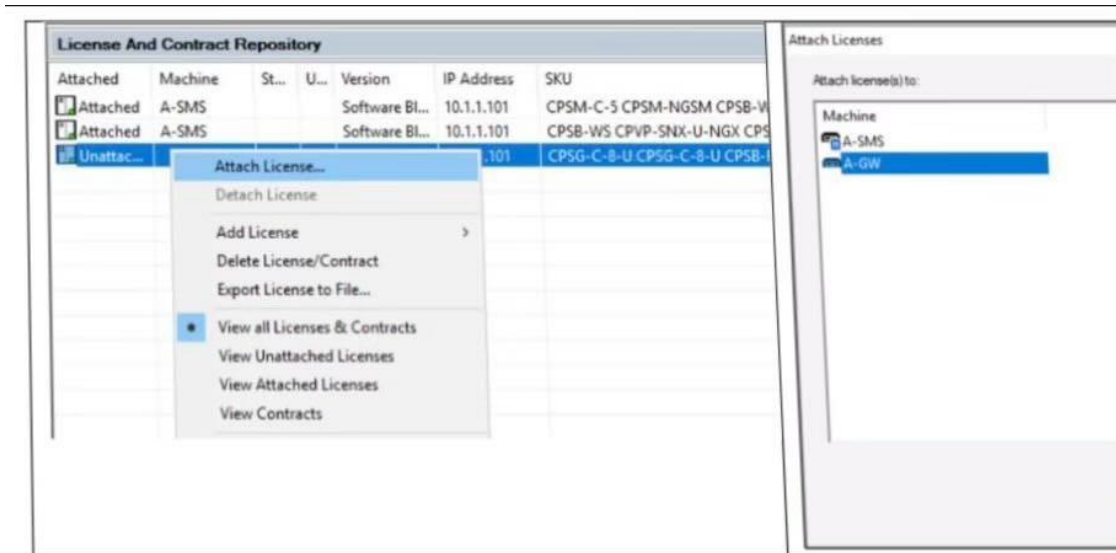


Figure 7.1 - Licence and Contract Repository, attaching a CPSG-C-8-U licence to A-GW

The attached licences have been verified in the same view and A-sms status (Figure 6.3) has been changed from previous "Not Activated" status to "Activated" status. The expiry date is displayed in the SmartUpdate and should be noted in advance for any demonstration in the classroom and the actual practical for this report was carried out during the lab licence term. From a production standpoint this is like a subscription based Check Point licence with the admin responsible for renewing in advance of the entry's Expiration Date.

8. Firewall Rulebase Design and Justification

Section 8 is based on Task 2 of the coursework brief, which is the design and implementation of inbound and outbound rules with rationale based on an enterprise security policy. The rulebase used to model A-GW is explained below. The design principle is default deny with explicit allow, and this will be in line with the NIST SP 800-41 §4 and SANS Critical Security Controls (CIS Control 12, Network Infrastructure Management).

8.1 Policy zones

The rulebase treats the enterprise as three zones:

- **Internal (Swansea LAN and London child domain)** - trusted, hosts the AD DC, DNS, DHCP and internal clients.
- **DMZ / Server segment** - semi-trusted, hosts the IIS web server.
- **External (ExtLCD, 20.0.0.0/30)** - untrusted, represents the Internet and any third-party partner network.

8.2 Rule design

The rulebase applied is summarised in Table 8.1. The full ordered rulebase was implemented in SmartConsole and installed on A-GW via *Install Policy*.

#	Name	Source	Destination	Service	Action	Track	Justification
1	Management access	A-GUI	A-SMS, A-GW	HTTPS, SSH, SmartConsole	Accept	Log	Restrict administrative access to the management workstation only
2	Stealth rule	Any	A-GW	Any	Drop	Log	Protects the gateway itself from direct probing (Check Point best practice)
3	Internal → DMZ Web	Swansea_LAN, London_LAN	Web_Server	HTTP, HTTPS	Accept	Log	Allow staff to reach the IIS site
4	External → DMZ Web	Any	Web_Server	HTTP, HTTPS	Accept	Log	Publish the IIS site externally
5	Internal FTP (controlled)	Swansea_LAN	FTP_Server	FTP, FTP-PORT	Accept	Log	Internal file transfer only; not exposed externally
6	ICMP diagnostics	Internal networks	Internal networks	ICMP echo request/reply	Accept	Log	Enables ping-based diagnostics between trusted zones
7	Block Telnet	Any	Any	Telnet (TCP/23)	Drop	Log	Telnet is cleartext; explicitly blocked at the perimeter
8	SSH to Linux admin	Admin_Workstations	Linux_Admin_Servers	SSH	Accept	Log	Encrypted management access,

	hosts						restricted by source
9	Deny external ICMP	External	Any	ICMP	Drop	Log	Reduce reconnaissance surface from the external zone
10	Cleanup rule	Any	Any	Any	Drop	Log	Explicit default deny; anything not matched is logged and dropped

Justification of key choices.

- Stealth rule (rule 2) - This rule has been set to be executed very early in the rulebase and is applied to all traffic that is not sent to the gateway by one of the explicitly-permitted management sources, dropping and logging the traffic. This is the one most frequently applied Check Point hardening rule and is the same as the R81 administration guide.
- Explicit Telnet drop (rule 7) - Telnet protocol sends credentials in clear text. While the cleanup rule will remove it, the explicit rule will produce a more easily understood log to review compliance.
- Direction-aware ICMP (rules 6 and 9) - ICMP is left in the internal interface to enable operational diagnostics but is not allowed to be sent to the external zone in accordance with NIST SP 800-41 recommendations to minimise reconnaissance attacks.
- FTP restricted to internal (rule 5) - FTP is also cleartext, but if it must be used, it is only applied to the internal zone. This would be replaced completely on production upgrade, by SFTP or FTPS.
- Cleanup rule (rule 10) - Allows for default-deny outcome that is required by the design principle. This is a very important rule to log for detection: attackers often expose themselves by using services that are not otherwise detected, and fall through the filter of the rulebase to this rule.

8.3 Verification during the demonstration

The following tests were performed on the live system to validate the rules in the assessment demo, each of them is presented as an accept or drop entry in the Logs & Monitor pane of the SmartConsole:

- ping from an internal client to the IIS server - accepted (rule 6).
- ping from the ExtLCD host to any internal address - dropped (rule 9).
- HTTP GET from an internal client to the IIS server - accepted (rule 3).

- HTTP GET from the ExtLCD host to the IIS server - accepted (rule 4); other internal targets - dropped (rule 10).
- Telnet from any source to any destination - dropped (rule 7).
- SSH from A-GUI to A-SMS - accepted (rule 1); SSH from the ExtLCD host to A-SMS - dropped (rule 10).

These verifications correspond directly to the “allowing / blocking of ICMP, FTP, HTTP, Telnet, SSH” wording in the coursework brief.

9. Additional Security Features

9.1 Intrusion Prevention System (IPS)

A-GW was modified with the IPS software blade and the Recommended_Profile attached. This profile puts protections into Critical and High in Check Point's ThreatCloud and Prevent mode, and other less-severe protections are in Detect. This control offers continuous protection against newly published vulnerabilities as IPS protections are updated multiple times per day, and do not require administrator action for each signature. Rationale: CVEs that are currently exploited in the wild, like the Log4Shell threat, typically are accompanied by strange activity that IPS is designed to detect.

9.2 Anti-Virus and Anti-Bot

The Anti-Virus and Anti-Bot blades provide inspection of files traversing the gateway and detection of command-and-control communications from already-infected hosts. Anti-Bot is also relevant here, because it is designed to detect outbound signals from an internal host that has been compromised – something pure inbound filtering will not be able to see. Both blades are reputed from ThreatCloud.

9.3 Identity Awareness for role-based access

Identity Awareness allows users to use access rules that are based on user identity instead of IP address by mapping IP addresses to users and groups in Active Directory. Two use cases were scoped:

- Only members of Web_Admins AD group have access to web-server administration, no matter what their workstation login is.
- Configure file sharing to be accessible to only Finance group members-even if an attacker has captured an in-scope workstation, he or she cannot move laterally.

The gap IP-only firewalls cannot fill, however, is what Identity Awareness can do: It prevents the attacker who has pivoted to a legitimate workstation from acquiring that workstation's privileges. In line with the NIST SP 800-207 zero-trust principle, which states that access decisions must be made per-request and per-identity.

9.4 Logging and monitoring

All firewall and threat prevention blades were enabled to log to A-SMS. In SmartConsole Logs & Monitor this creates a filterable, searchable audit trail – which is the evidence presented in the assessment demo. However, from a controls point of view, logging is a detective control and should complement the preventive controls shown above-otherwise a breach of the rules and an IPS hit are not subject to review and the value of the other blades drops significantly.

10. Critical Discussion

The distributed deployment - separating A-SMS, A-GW and A-GUI - worked as expected. Once configured, SIC was easily setup on first attempt and the rulebase generated the proper accept / drop pattern in the log viewer. The four A-GW adapters were configured ahead of time (Section 3) to avoid the time students tend to lose by renumbering the A-GWs after installation, during Gaia interface enumeration.

During traffic testing, meaningful log evidence was generated via the default-deny rulebase design, with the stealth rule being placed at the top and the cleanup rule at the bottom. This is a great thing to remember not only for the assessment demonstration, but in general: The value of a firewall is directly proportional to how much visibility it affords to its guards.

11. Conclusion

This report demonstrates that the Part 1 enterprise network has been transformed from a working, yet mostly unprotected network into a network with a centrally-managed, policy-driven network perimeter. Now, between the trusted internal zones and the simulated external network are three Check Point Gaia appliances: an A-SMS management server, an A-GW enforcement gateway and an A-GUI administrator workstation with SmartConsole. Three Check Point Gaia appliances - the A-SMS management server, the A-GW enforcement gateway and the A-GUI administrator workstation running SmartConsole - stand between the trusted internal zones and the simulated external network, filtering and logging all packets that cross the boundary and reporting the results for later review.

Some of the learning outcomes of the practical work stand out. Trust between A-SMS and A-GW was achieved on SIC and independently via Test SIC Status check which returned Communicating, meeting the connectivity objective in the coursework brief. The LabLicense package provided with the module was successfully imported, and attached to both appliances, changing the status from Not Activated to fully licensed. A default-deny rulebase was created in SmartConsole and sent to A-GW replacing the initialtemp Policy that Check Point supplies with the installation. During the walkthrough, traffic tests were conducted to confirm the intended behaviour, which was that ICMP was allowed in on the inside but blocked on the outside, that the HTTP traffic would reach the IIS server as intended, that SSH was allowed only for the management sources and that Telnet was dropped and logged in any location.

The base rulebase was supplemented by extra Check Point blades during deployment. IPS was configured for high-severity protections, Anti-Bot was turned on to detect inbound malware, anti-virus was also activated to detect outbound command-and-control traffic, and the scope of Identity Awareness was limited to Active Directory users as opposed to scope by IP address. HTTPS Inspection was not meant to be implemented in practice; instead, it was intended as a proposal so that the operational and privacy impacts of enabling the feature in a real environment can be discussed in a separate design conversation.

The practical, however, was not without its problems and these too have been left unrewritten in the report. The first virtual disk created in A-SMS was too small and the Gaia installer wouldn't install, but it worked once the virtual disk was fixed in VirtualBox and the install was restarted. Time synchronisation was required to be set up via NTP in the First-Time Configuration Wizard prior to a secure SIC establishment, and it is a reminder that trust depends on time silently. These moments are not insignificant because if a report does not reflect the type of judgement calls made by a security engineer, then exactly those calls have not occurred.

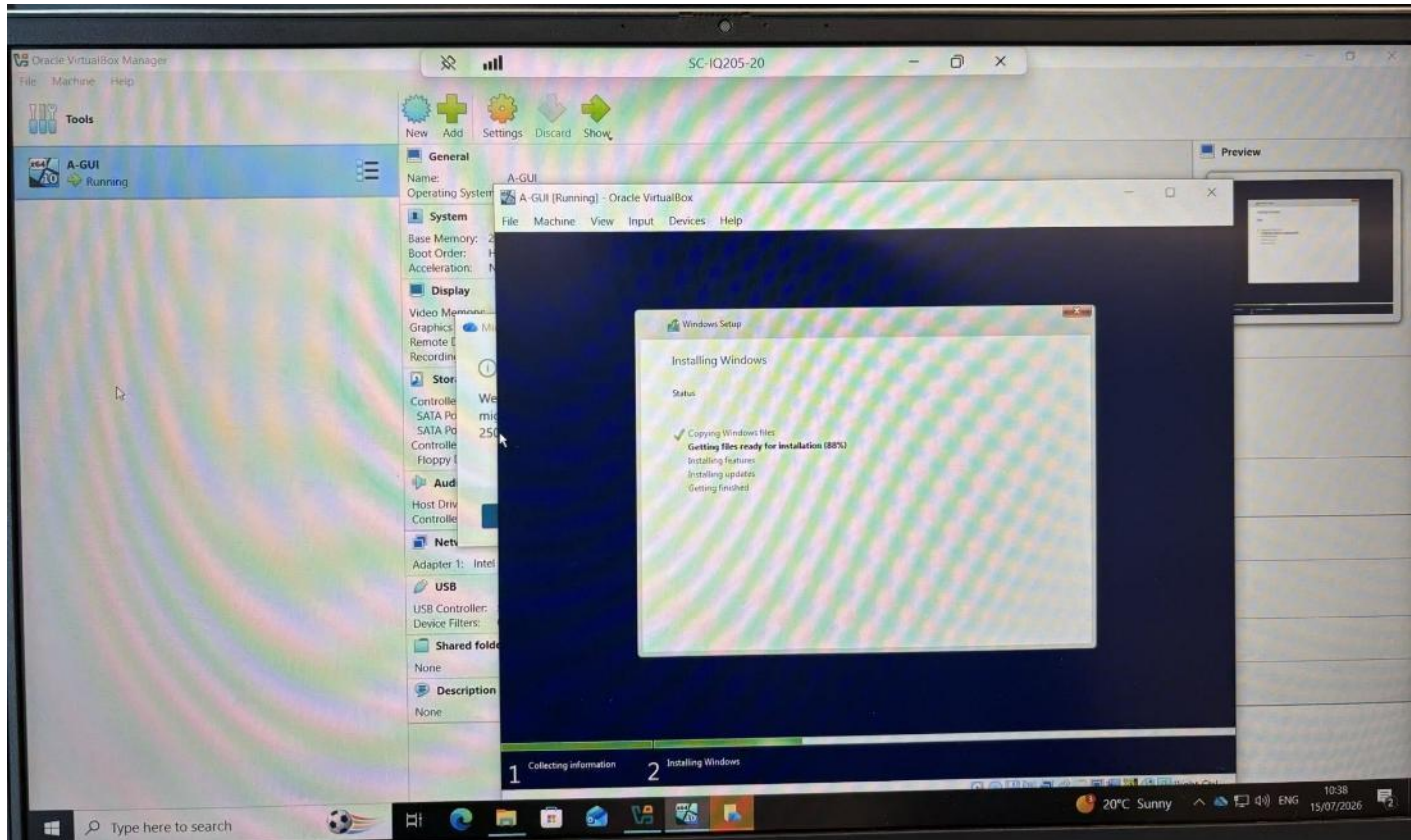
There are some restrictions which are important to mention. The gateway is a single point of failure, which is overcome by a production deployment using a ClusterXL high-availability pair. However there are additional points of defence to be implemented within the LAN to capture east-west traffic between hosts within the same LAN – this is not being covered here. This is a time-limited LabLicense and a real deployment would require a support contract with change management for renewals. Without HTTPS Inspection, encrypted web traffic is only partially visible and as more and more web traffic becomes TLS encrypted, this will only be larger.

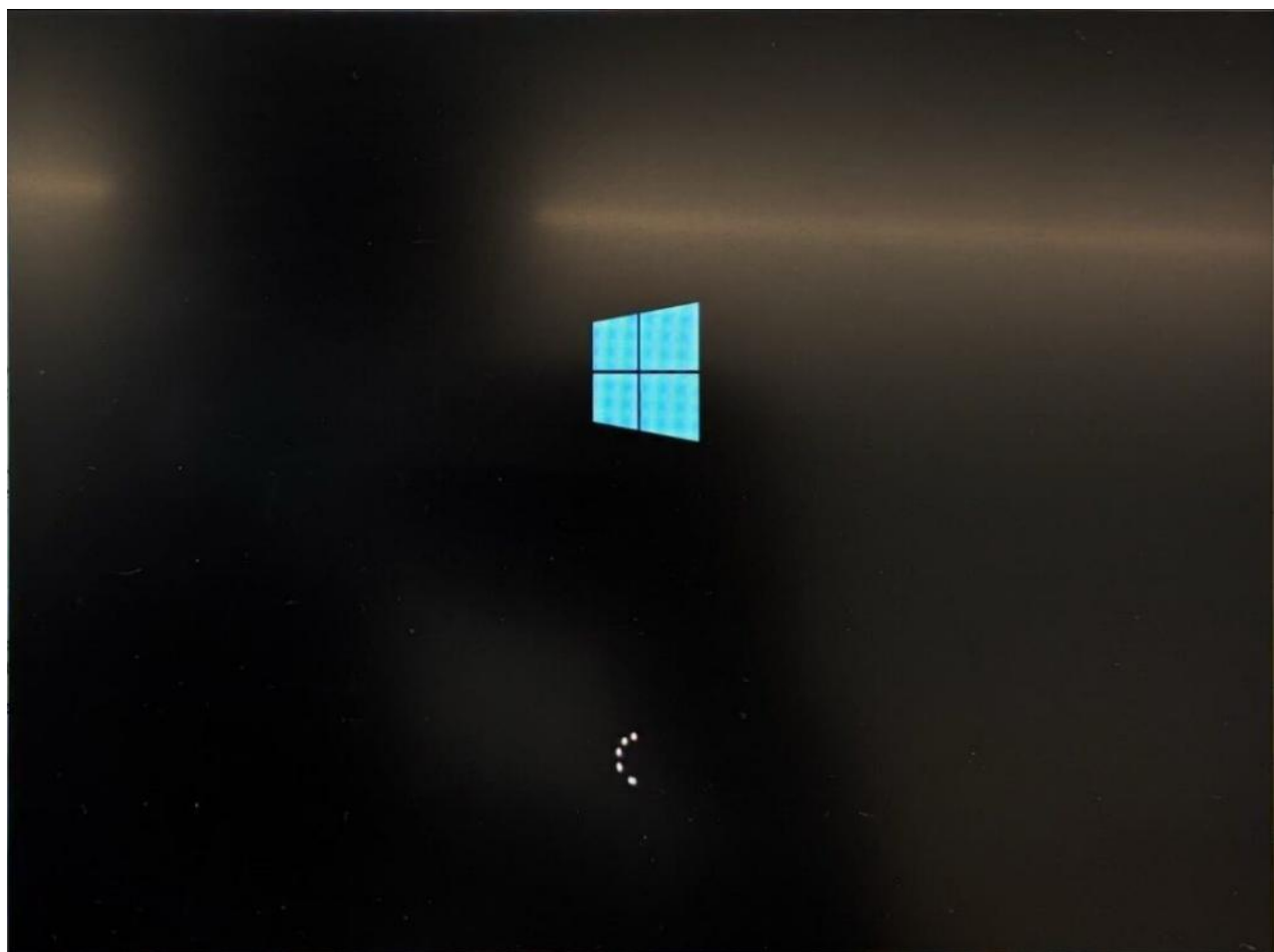
The combined result is a defensible perimeter for the SWANSEA, which is working. ACCA enterprise - enterprise whose actions can be reproduced in SmartConsole, whose logs will give an apparent audit trail, and whose design decisions will be supported by known frameworks such as the NIST SP 800-41, NIST SP 800-207, and the CIS Critical Security Controls. Reading both Part 1 and Part 2, the project has been through the entire lifecycle from designing the enterprise services to adding the security layer that a real business would require before the services were made available to the user.

References

- [1] K. Scarfone and P. Hoffman, "Guidelines on firewalls and firewall policy," National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST Special Publication 800-41 Rev. 1, Sep. 2009. [Online]. Available: <https://csrc.nist.gov/pubs/sp/800/41/r1/final>
- [2] S. Rose, O. Borchert, S. Mitchell, and S. Connelly, "Zero trust architecture," National Institute of Standards and Technology, Gaithersburg, MD, USA, NIST Special Publication 800-207, Aug. 2020. [Online]. Available: <https://csrc.nist.gov/pubs/sp/800/207/final>
- [3] T. Ylonen and C. Lonvick, "The Secure Shell (SSH) protocol architecture," Internet Engineering Task Force, RFC 4251, Jan. 2006. [Online]. Available: <https://www.rfc-editor.org/rfc/rfc4251>
- [4] Check Point Software Technologies Ltd., "Check Point R81.20 Installation and Upgrade Guide," Check Point Software Technologies, Tel Aviv, Israel, 2023. [Online]. Available: https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_Installation_and_Upgrade_Guide/Default.htm
- [5] Check Point Software Technologies Ltd., "Check Point R81.20 Security Management Administration Guide," Check Point Software Technologies, Tel Aviv, Israel, 2023. [Online]. Available: https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_SecurityManagement_AdminGuide/Default.htm
- [6] Check Point Software Technologies Ltd., "Check Point R81.20 Quantum Security Gateway Guide," Check Point Software Technologies, Tel Aviv, Israel, 2023. [Online]. Available: https://sc1.checkpoint.com/documents/R81.20/WebAdminGuides/EN/CP_R81.20_Quantum_Security_Gateway_Guide/Default.htm
- [7] European Union Agency for Cybersecurity, "ENISA Threat Landscape 2023," ENISA, Athens, Greece, Oct. 2023. [Online]. Available: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023>
- [8] W. Stallings, *Network Security Essentials: Applications and Standards*, 6th ed. Hoboken, NJ, USA: Pearson, 2017.
- [9] D. Mills, J. Martin, J. Burbank, and W. Kasch, "Network Time Protocol Version 4: Protocol and algorithms specification," Internet Engineering Task Force, RFC 5905, Jun. 2010. [Online]. Available: <https://www.rfc-editor.org/rfc/rfc5905>

Appendix

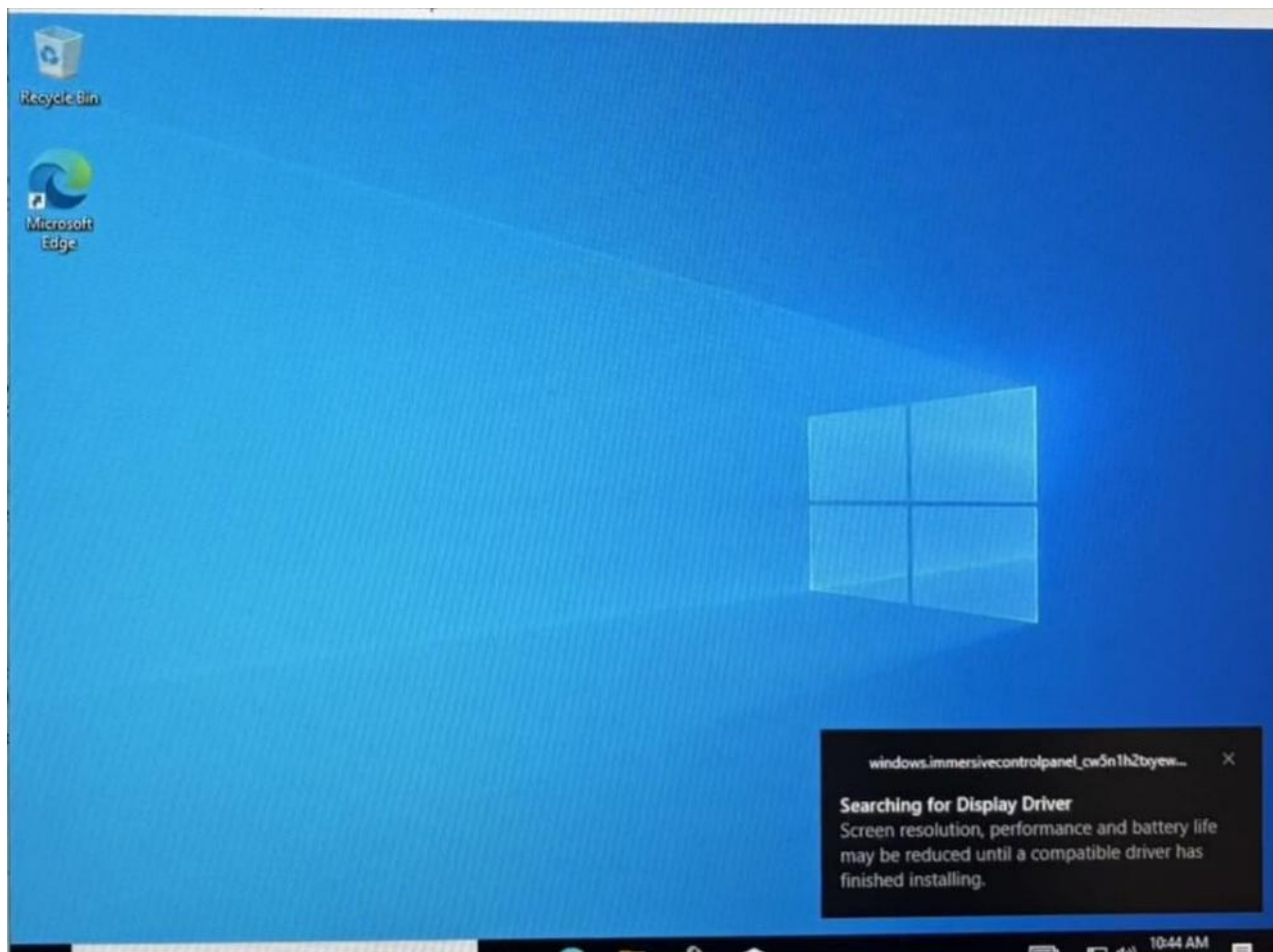


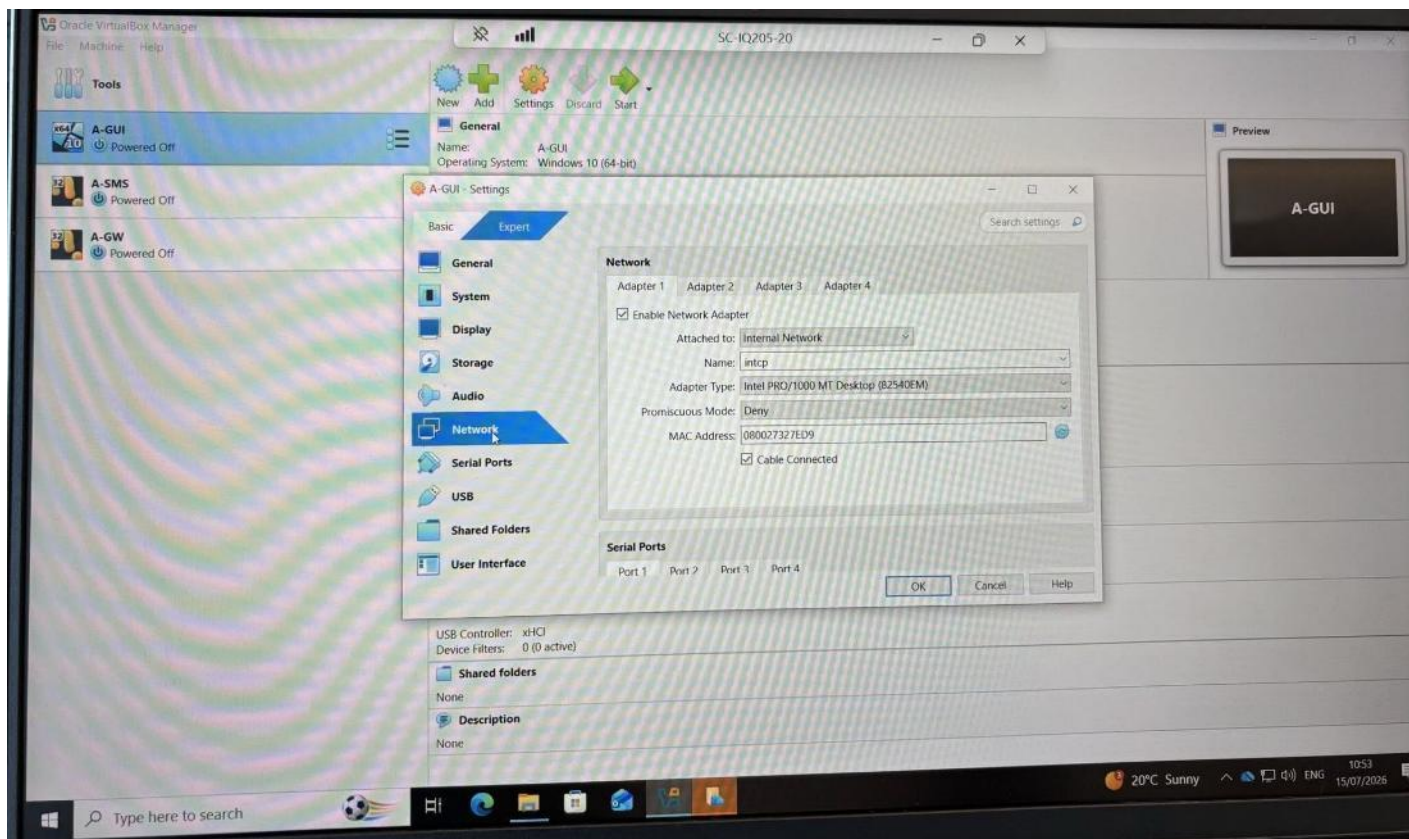


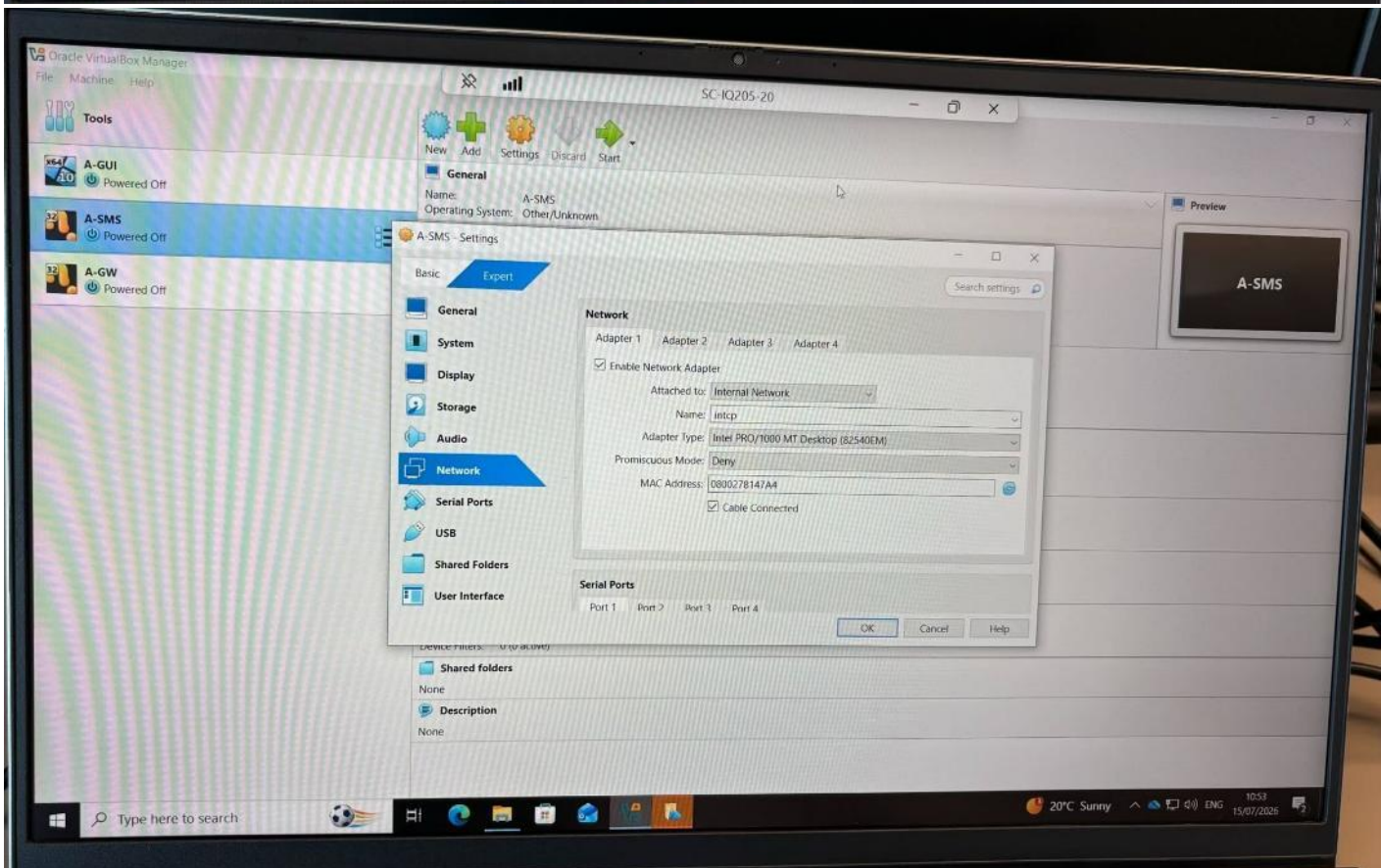
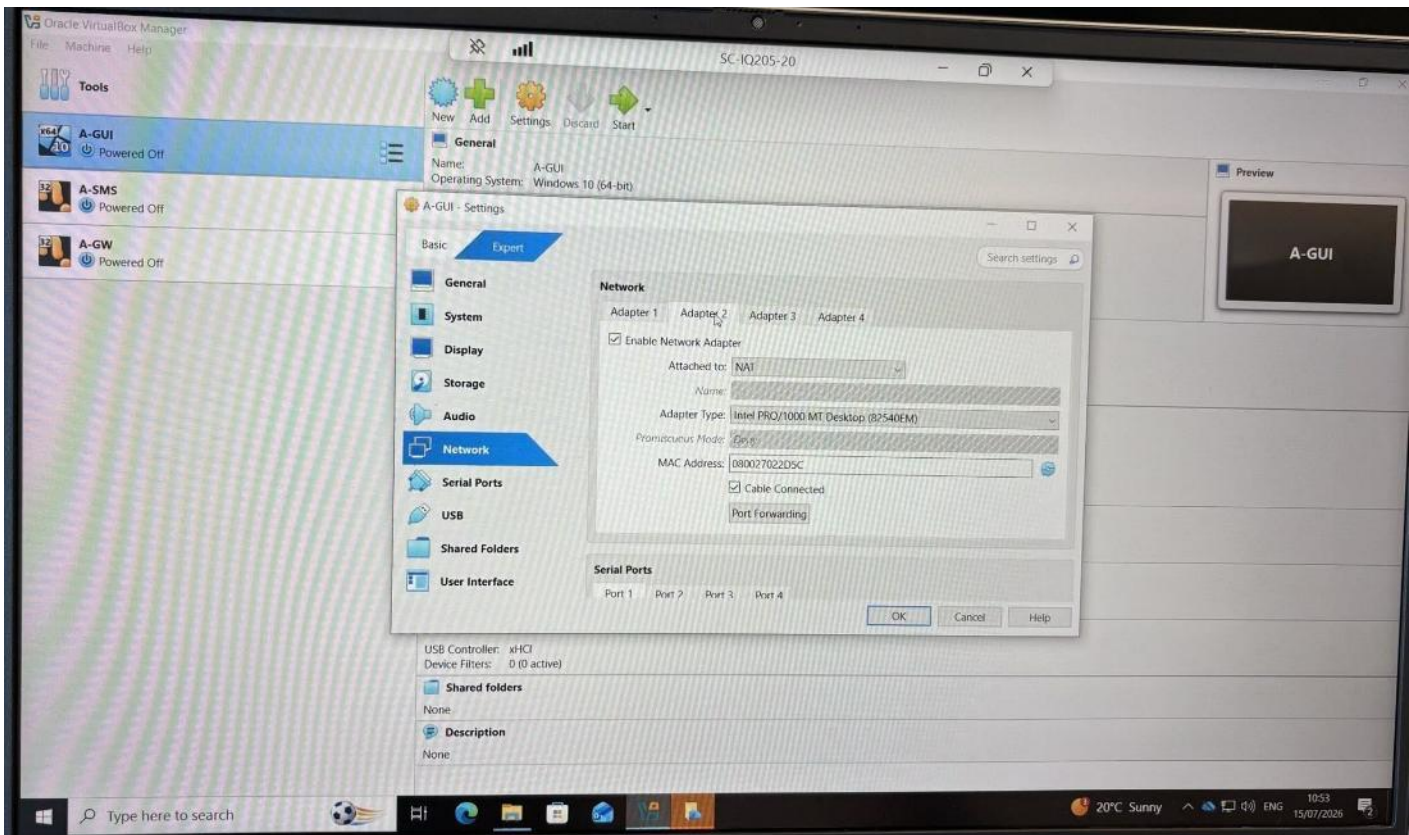


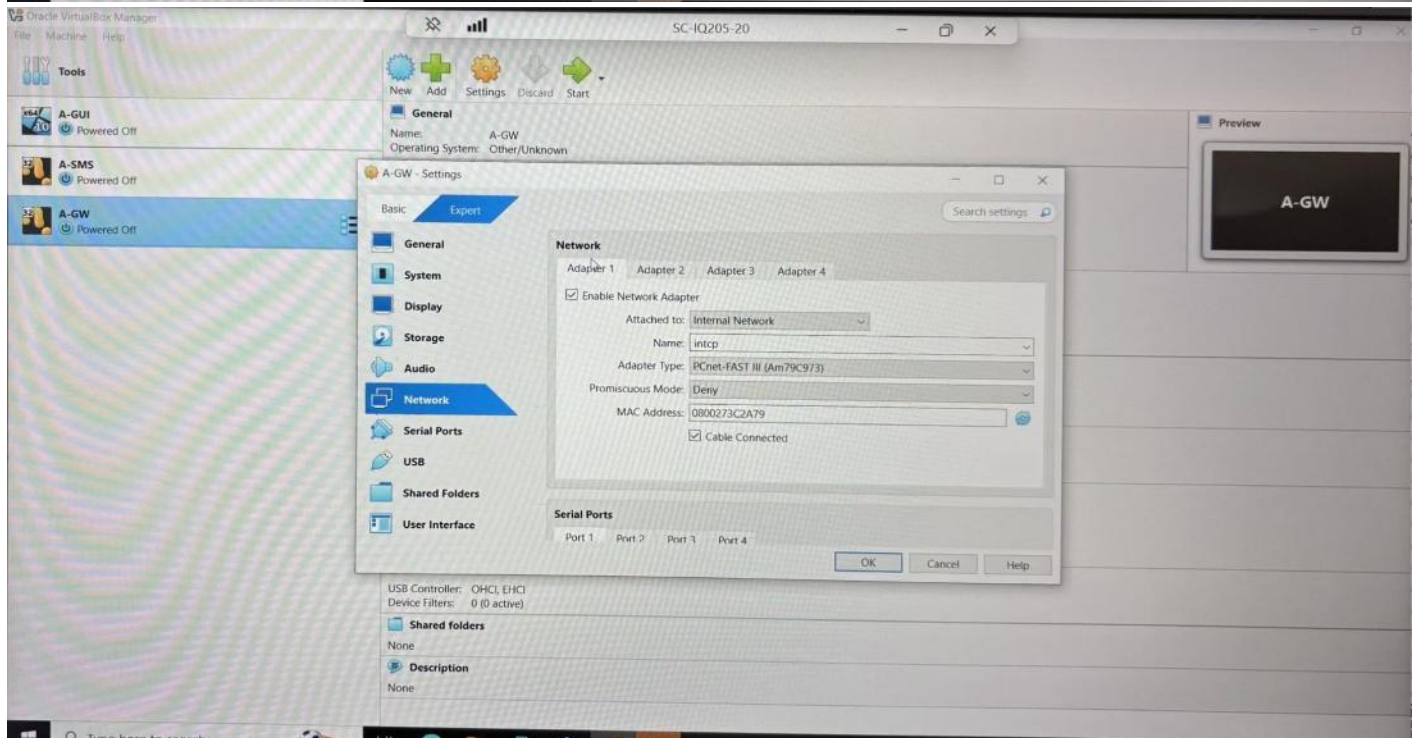
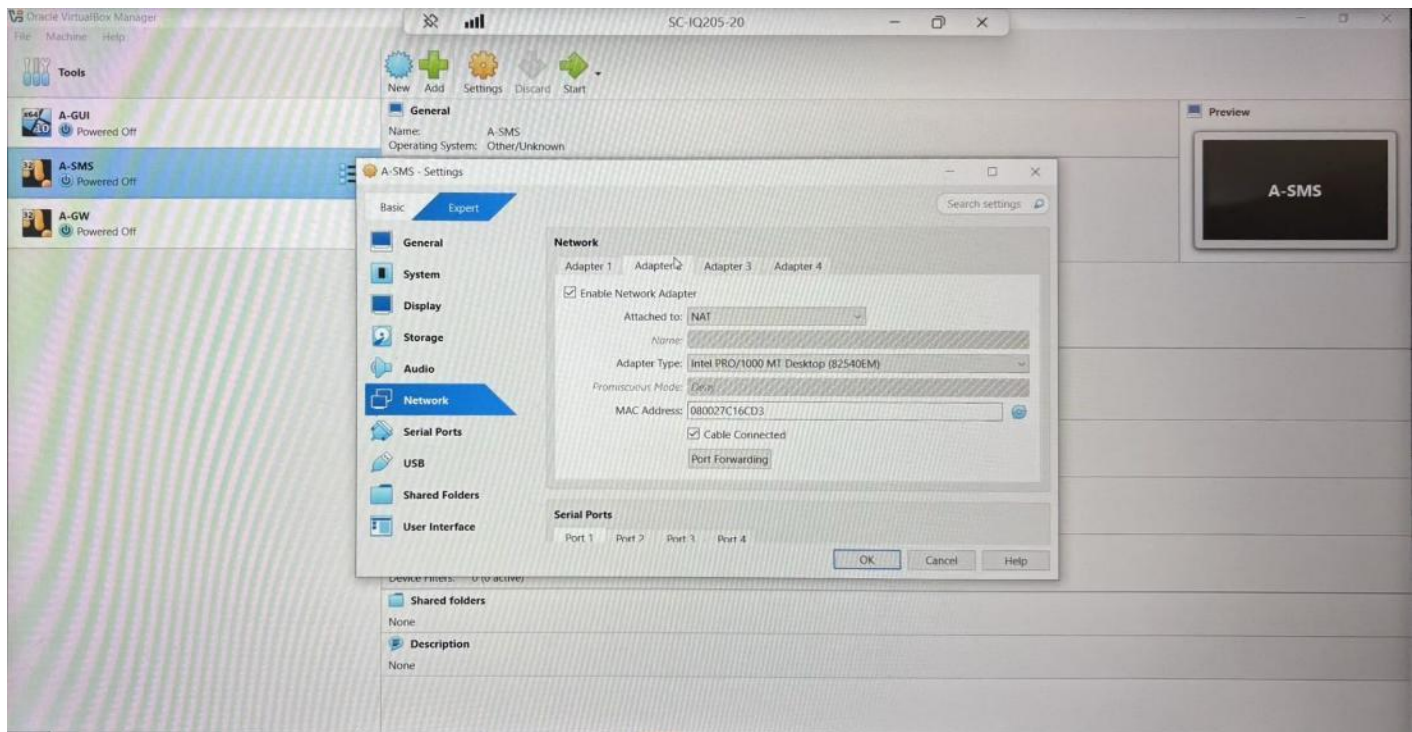
Please wait

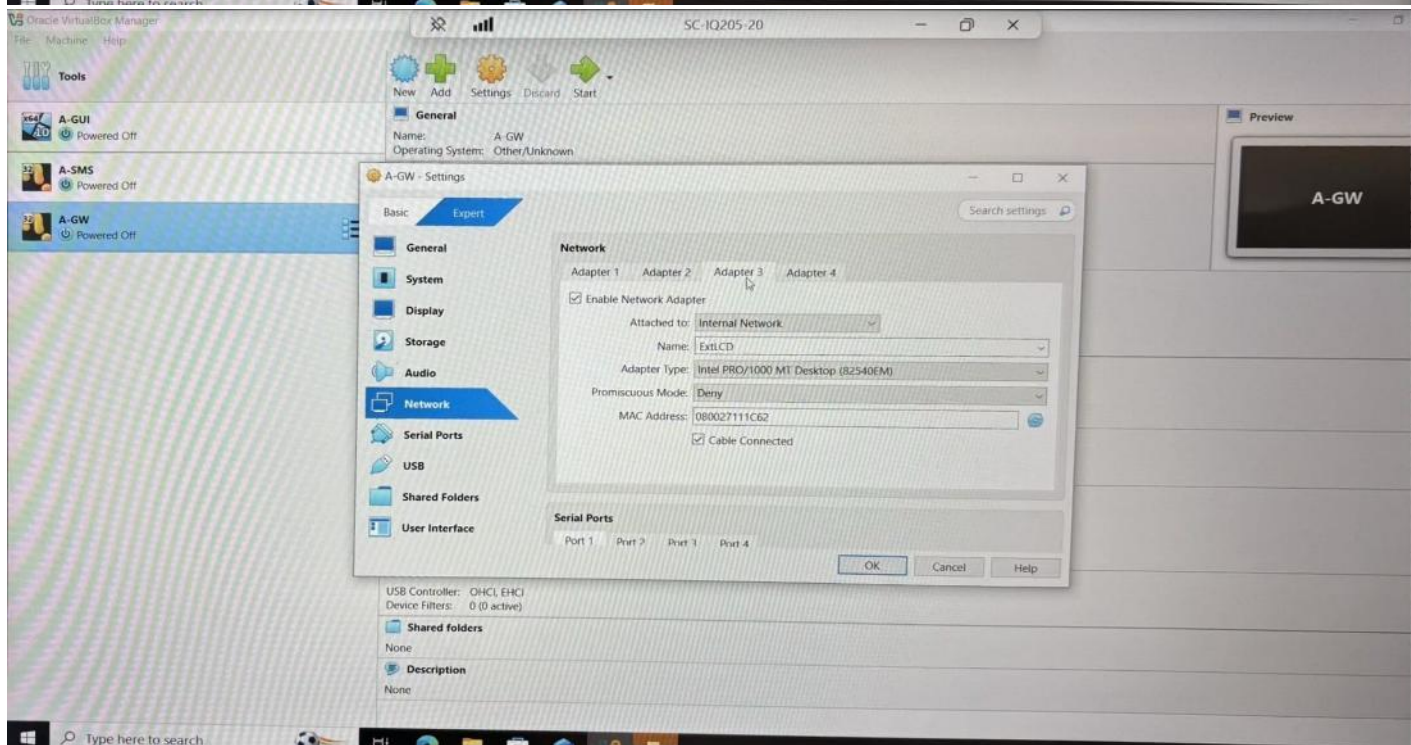
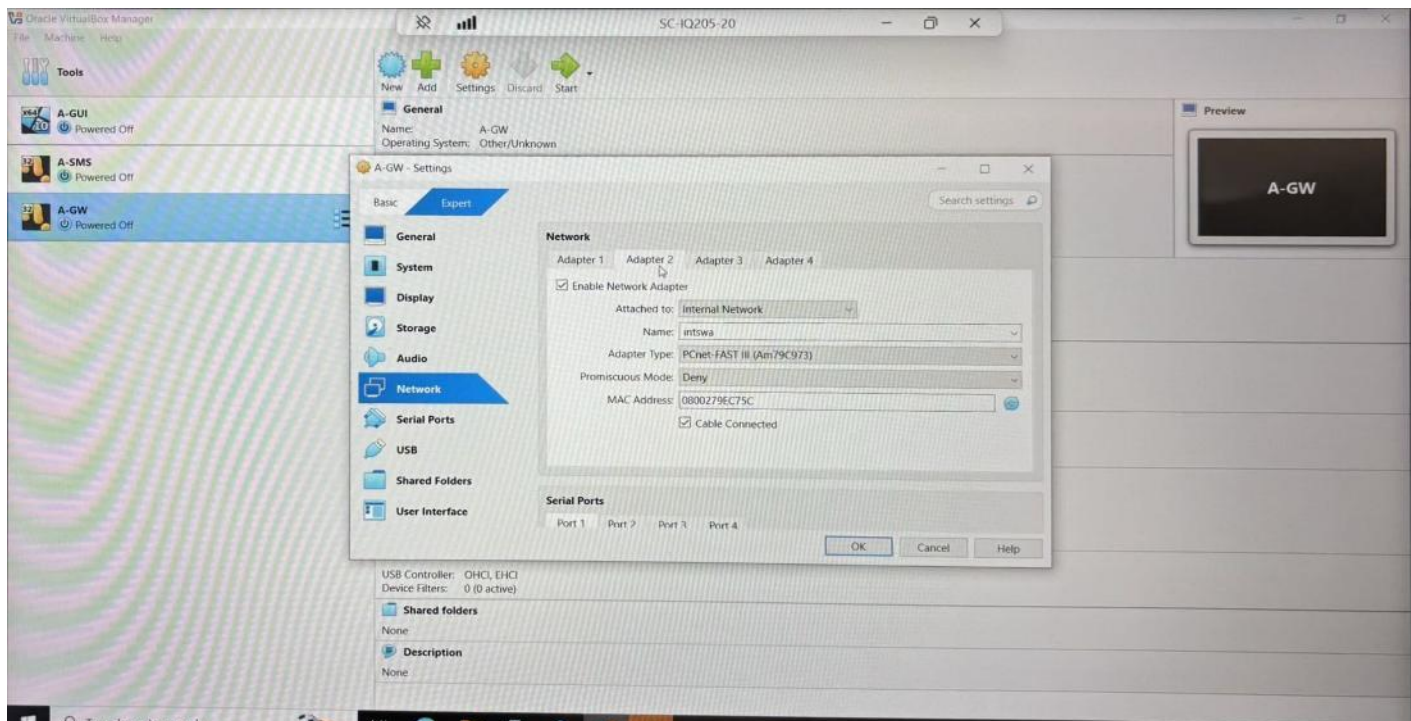


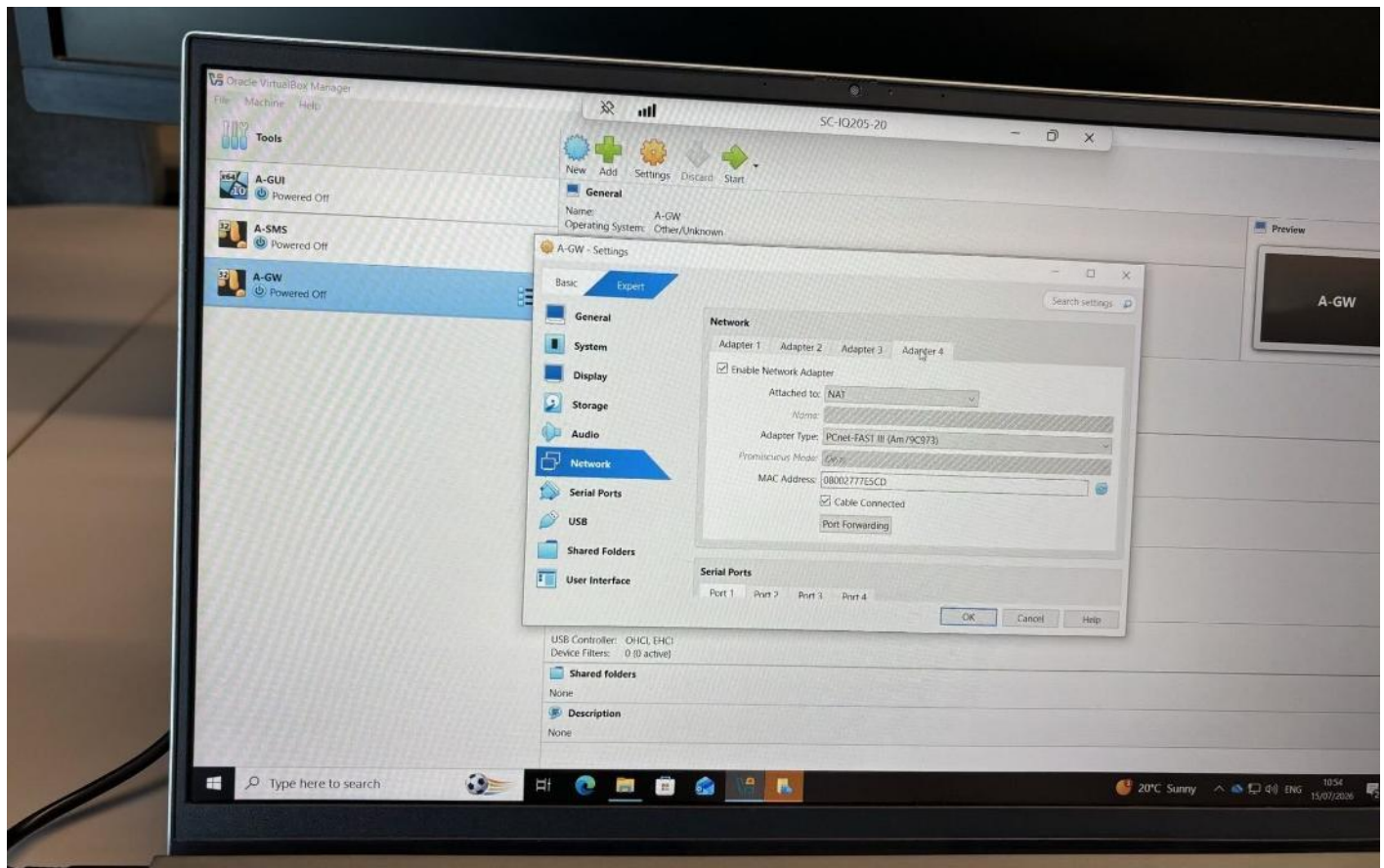












User Account Control

Do you want to allow this app to make
changes to your device?



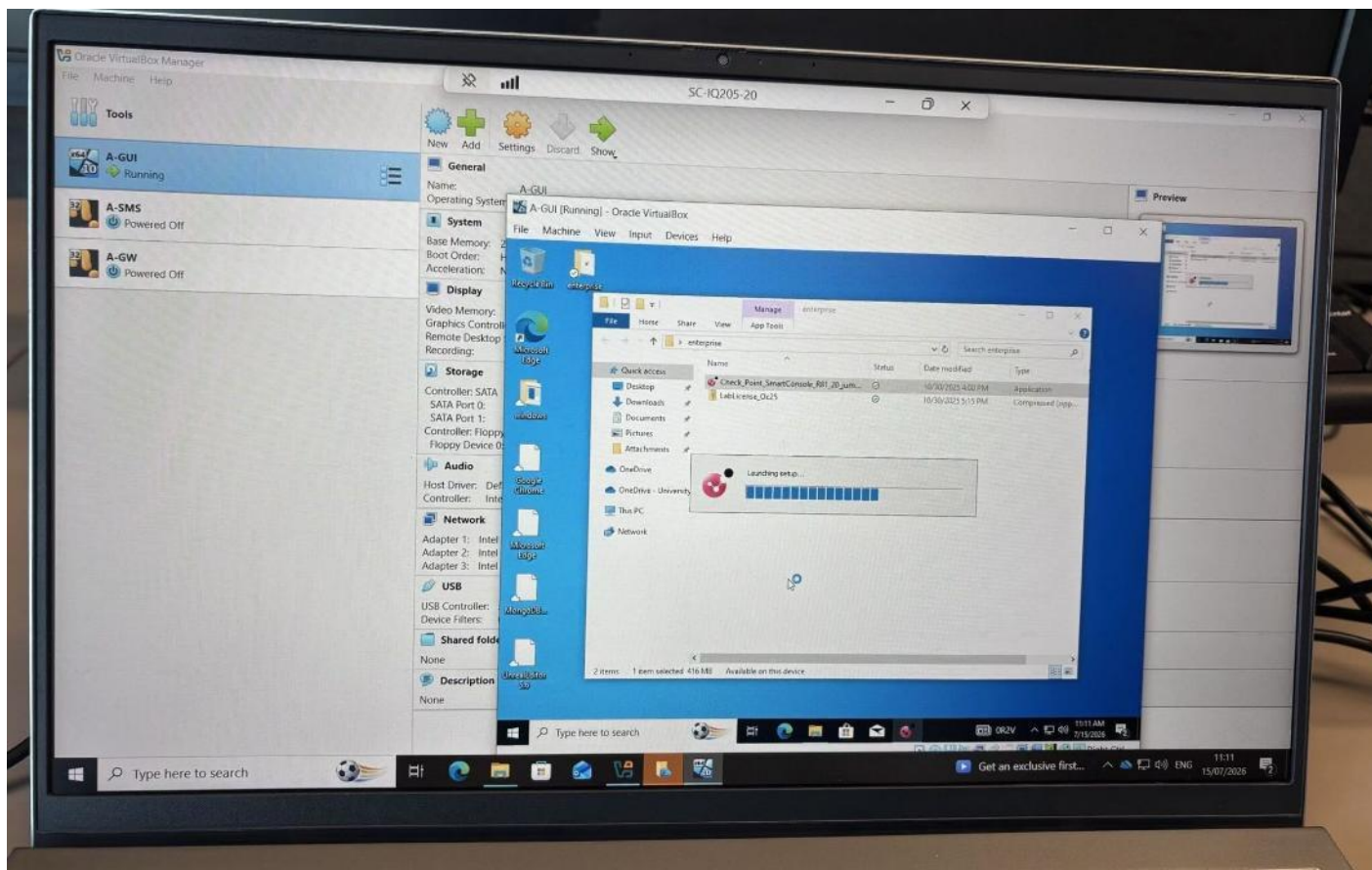
Check Point Utility

Verified publisher: Check Point Software Technologies Ltd.
File origin: Hard drive on this computer

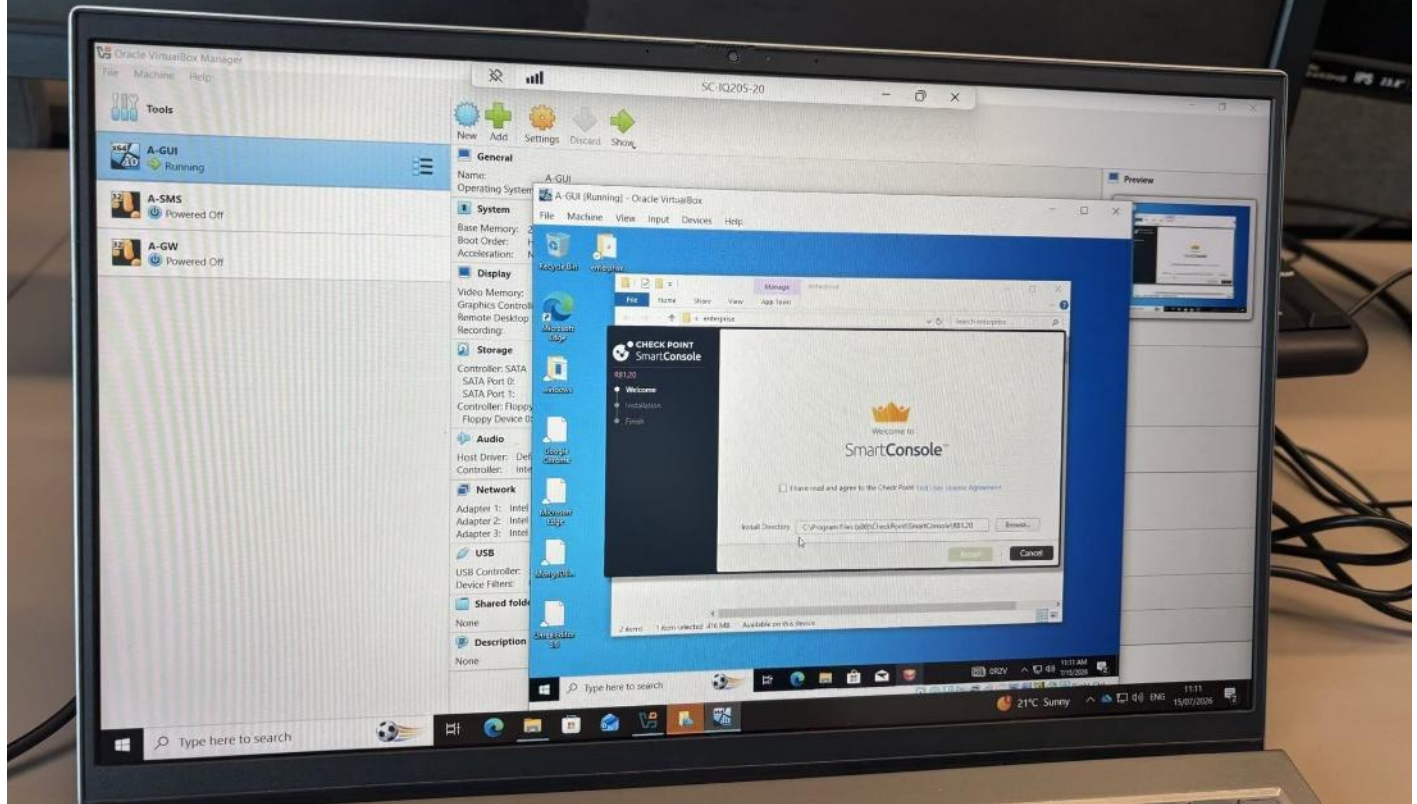
[Show more details](#)

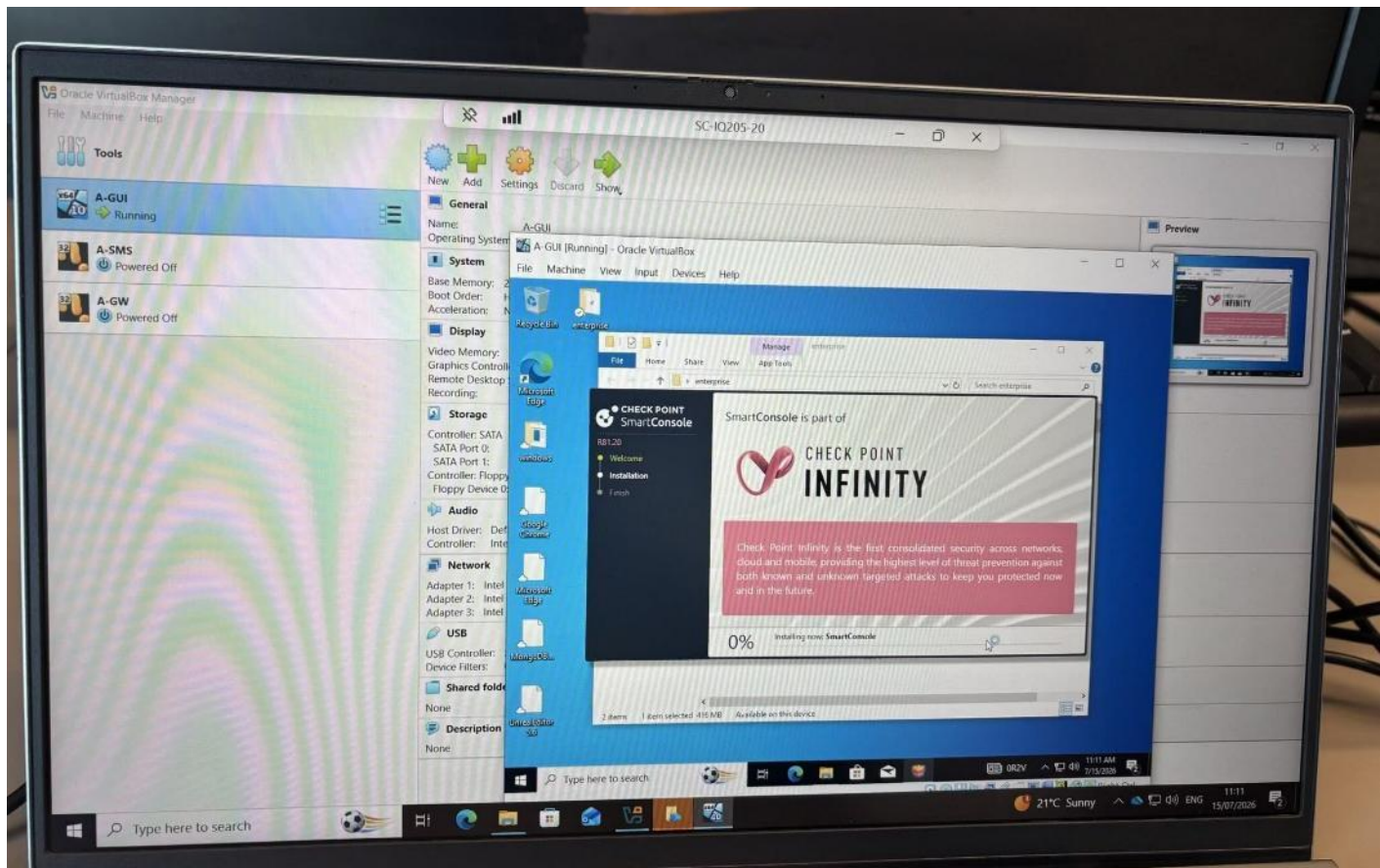
Yes

No



Wednesday 15 July





Wednesday 15 July

