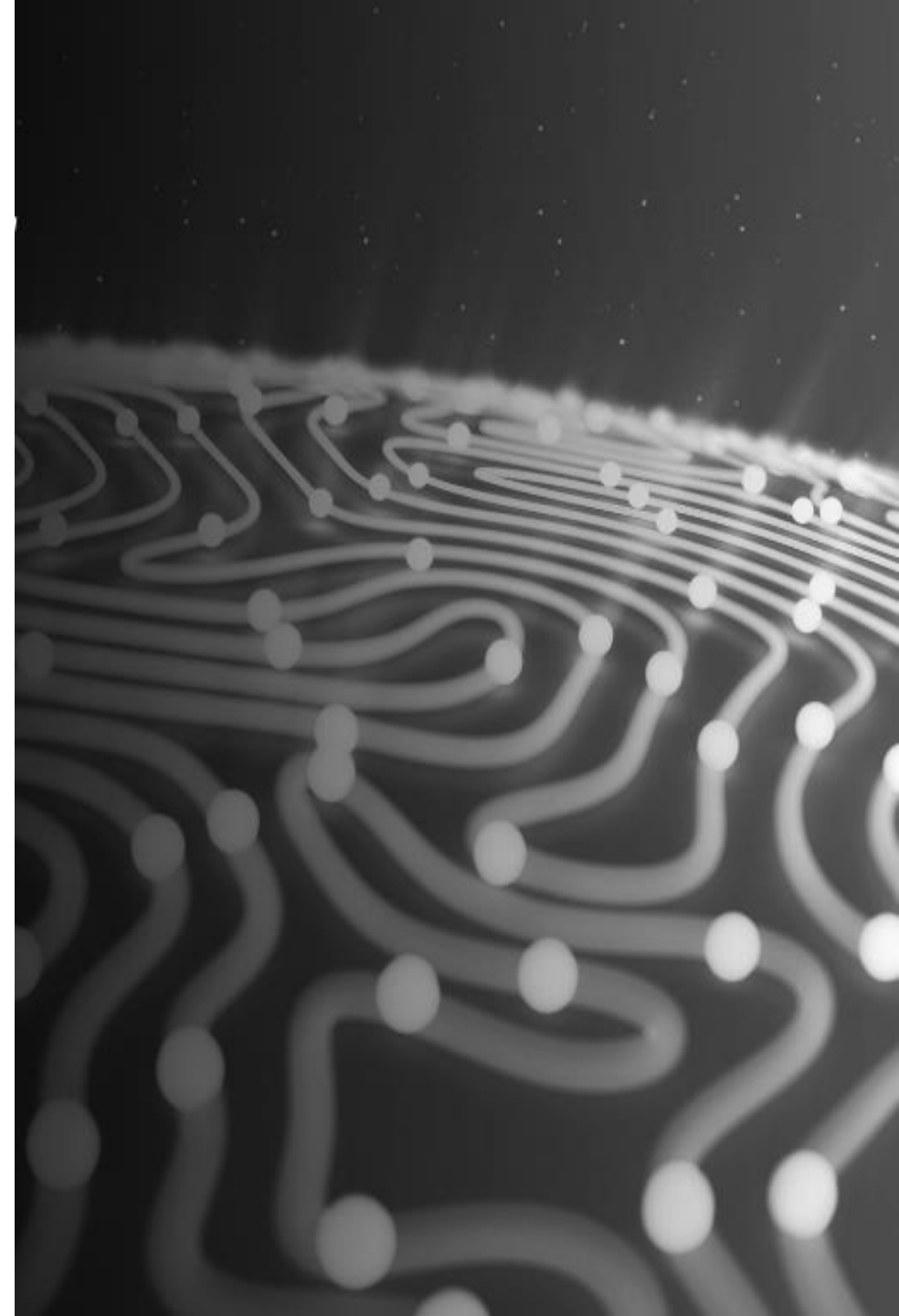


Portfolio 2: Securing the Enterprise Network

- Subtitle:** Deployment, Verification, and Contract Licensing of Check Point Infrastructure
- Presenter Name:** Hridoy Majumder
- Module Code:** ACCA7032 Enterprise Network Security
- Evaluation Date:** July 20, 2026



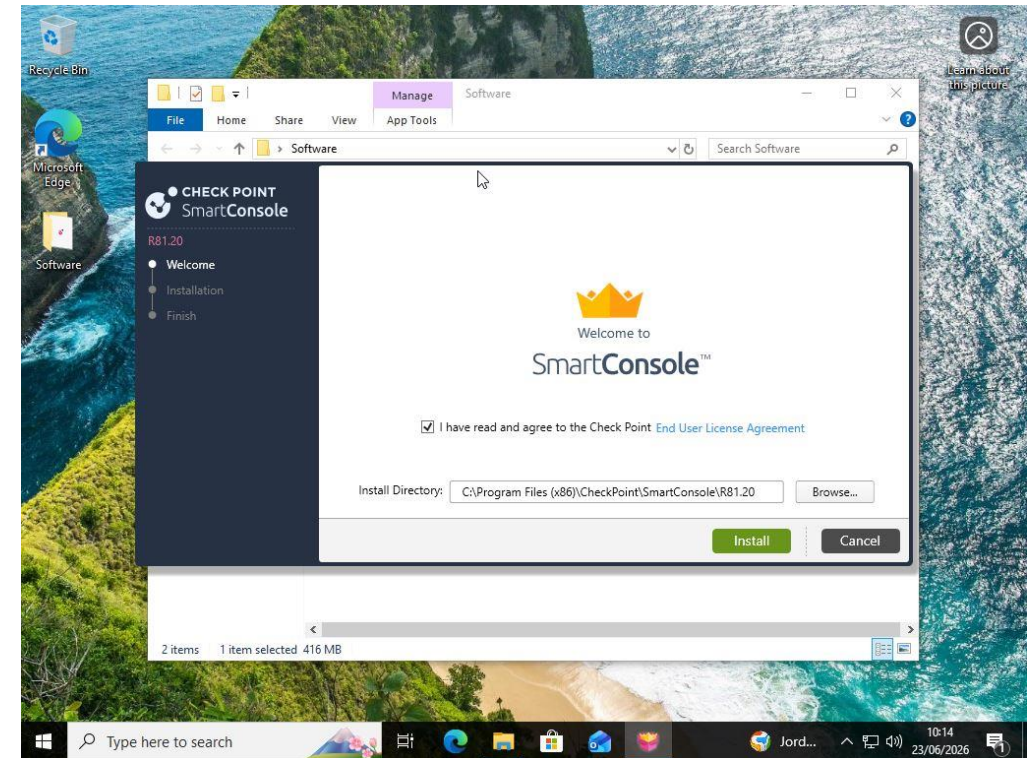
Deployment Scope & Phase Milestones

- **Prerequisite Baseline:** Builds directly on Part 1 domain configurations (SWANSEA.ACCA).
- **Phase 1 Execution:** Multi-component deployment of GAIa R81.20 appliances (A-SMS & A-GW).
- **Phase 2 Execution:** Establish cryptographic Secure Internal Communication (SIC).
- **Phase 3 Execution:** Production license injection via SmartUpdate utility platforms.



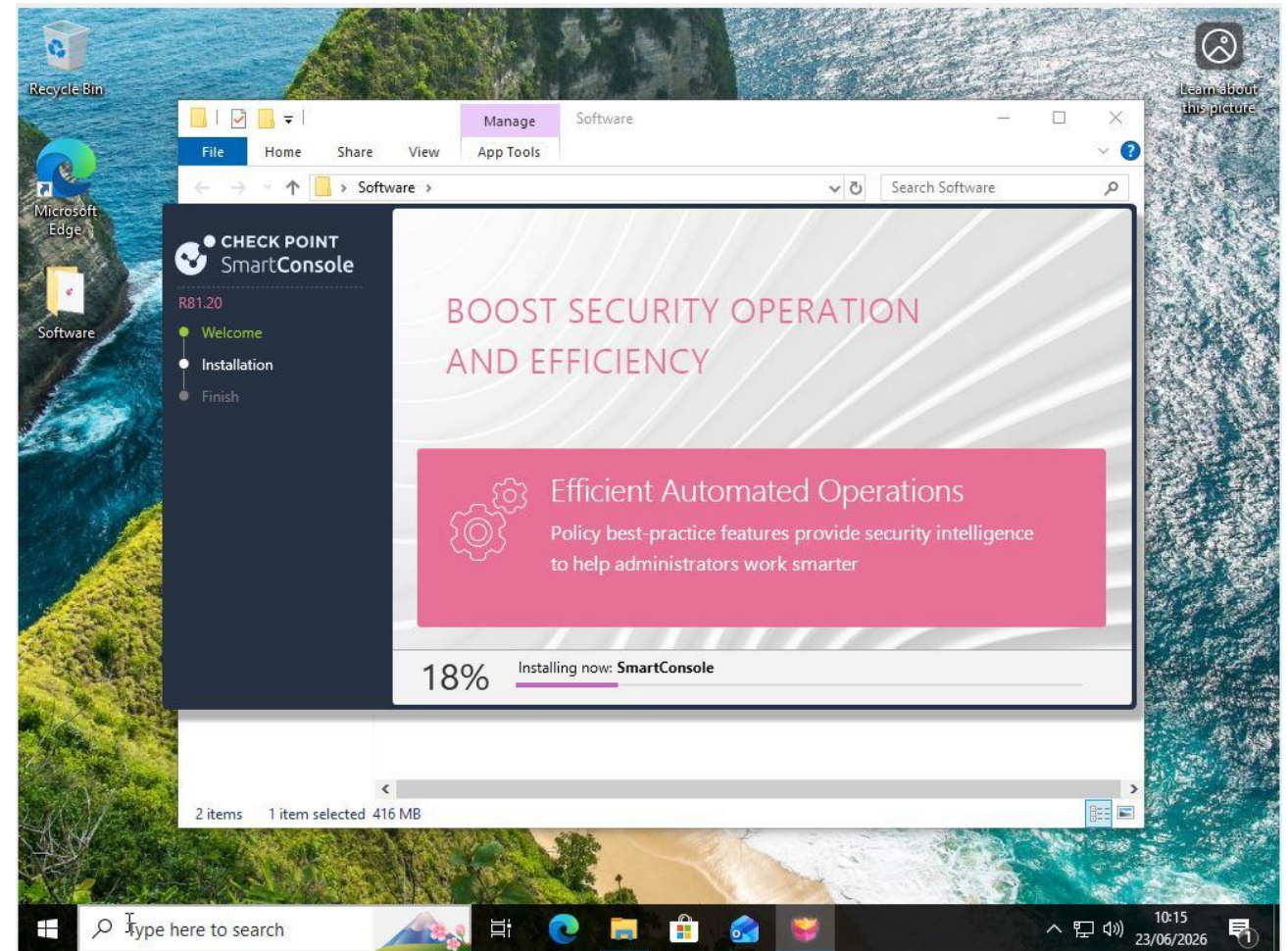
SmartConsole Setup Wizard Initialization

- **Package Origin:** Native R81.20 deployment assets retrieved from local network domain storage shares.
- **Target Workspace:** Windows 10 enterprise administrative endpoint client framework.
- **Compliance Protocol:** Explicit review and execution of the Check Point End User License Agreement.



Installer Tracking & Binary Package Extraction

- **Extraction Mechanics:** Unpacking core binary management files onto local disk storage tracks.
- **System Integrity:** Validation checks run concurrently to prevent runtime library corruption.
- **Progress Tracking:** Verifying steady deployment tracking past initial setup phases.

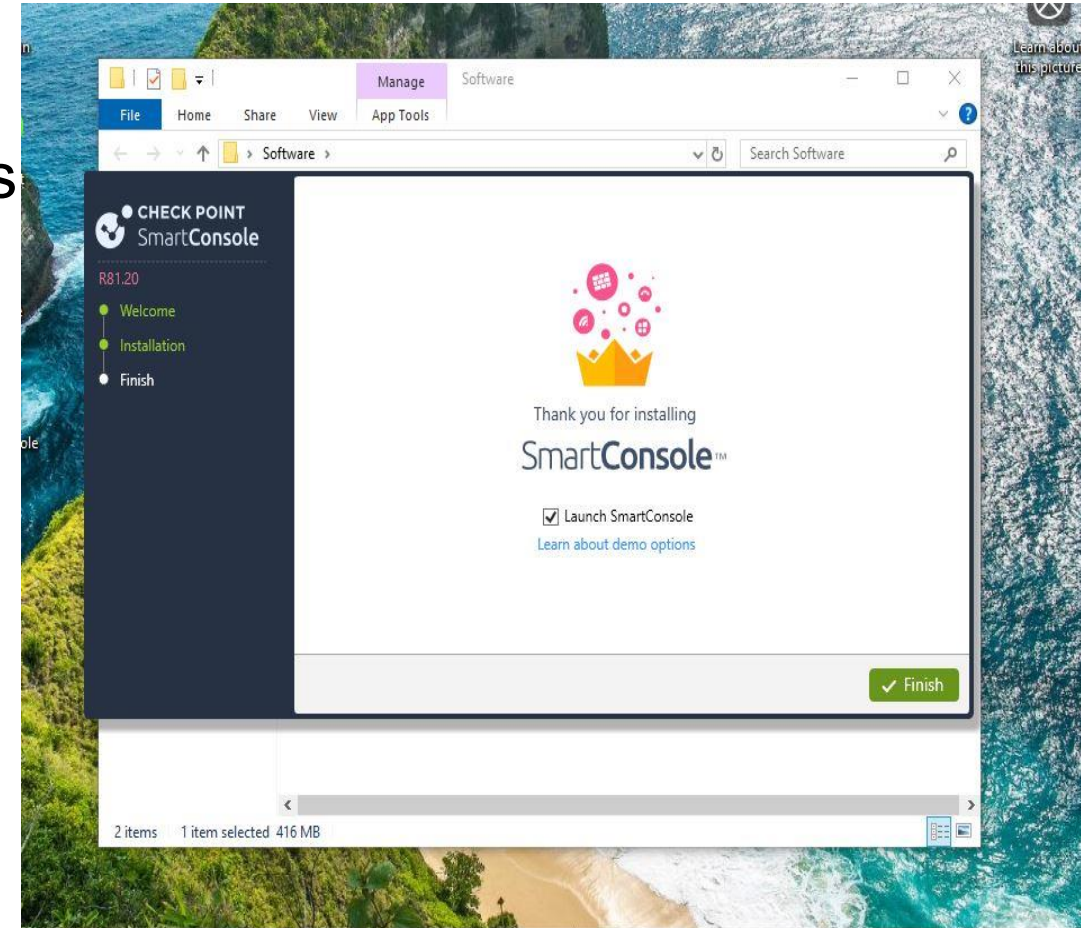


•SmartConsole Management Client Completion

•**Wizard Termination:** Setup program terminates successfully following block copy completions.

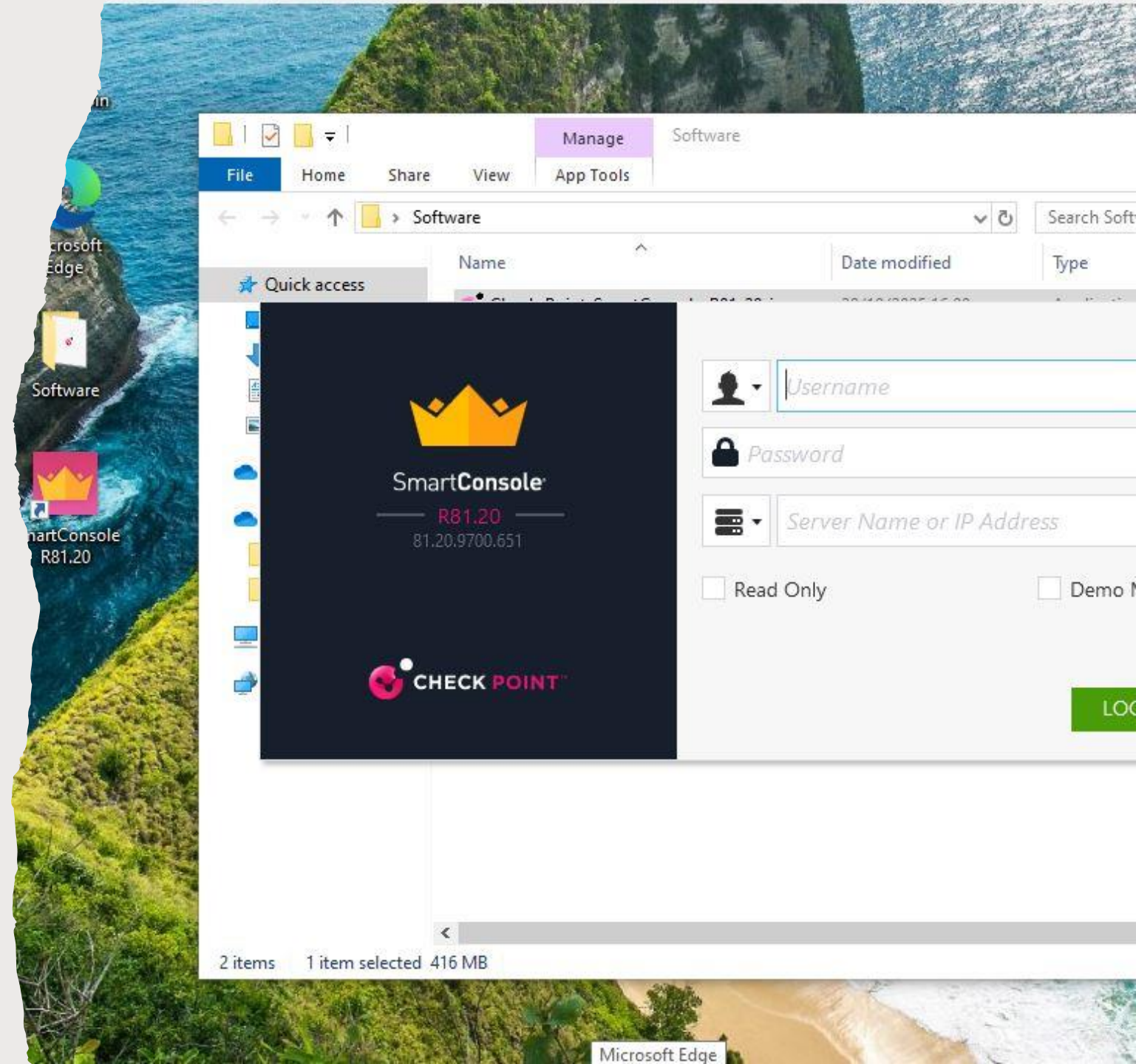
•**Application Shortcutting:** Local paths register interface links directly on the A-GUI desktop space.

•**Launch Readiness:** Preparing the endpoint to access local management environments over the wire.



SmartConsole Management Authentication Window

- **Secure Administration:** Desktop access window launched to handle daily infrastructure modifications.
- **Dynamic Variable Form:** Fields enforce entry of distinct Usernames, Passwords, and target Server IPs.
- **Target Destination:** Pointed to location 10.1.1.101 to access the Security Management Server.

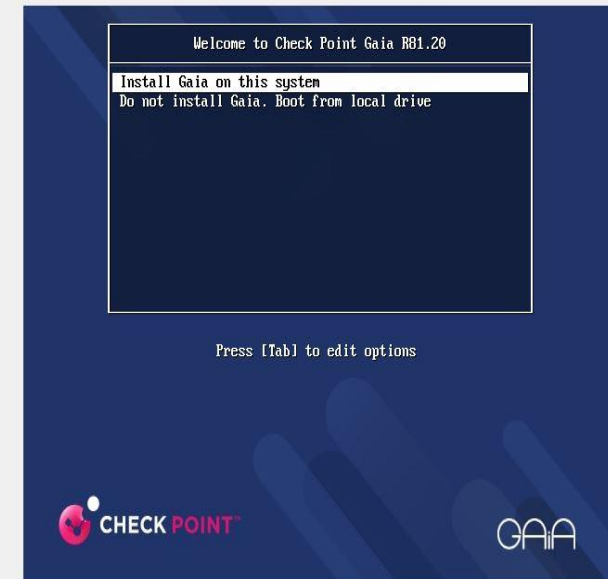


•Gaia Operating System Base Boot Initialization

•**Boot Media Payload:** Initiating virtual system installations via the native Gaia R81.20 ISO image file.

•**Boot Sequencing:** Diverting system focus from internal virtual disk tracks to load installation kernels.

•**Initial Selection:** Executing the primary text menu instruction string: **"Install Gaia on this system"**.



Virtual Machine System Memory Assignment

- Allocated Memory:** Assigning **10,166 MB** of system

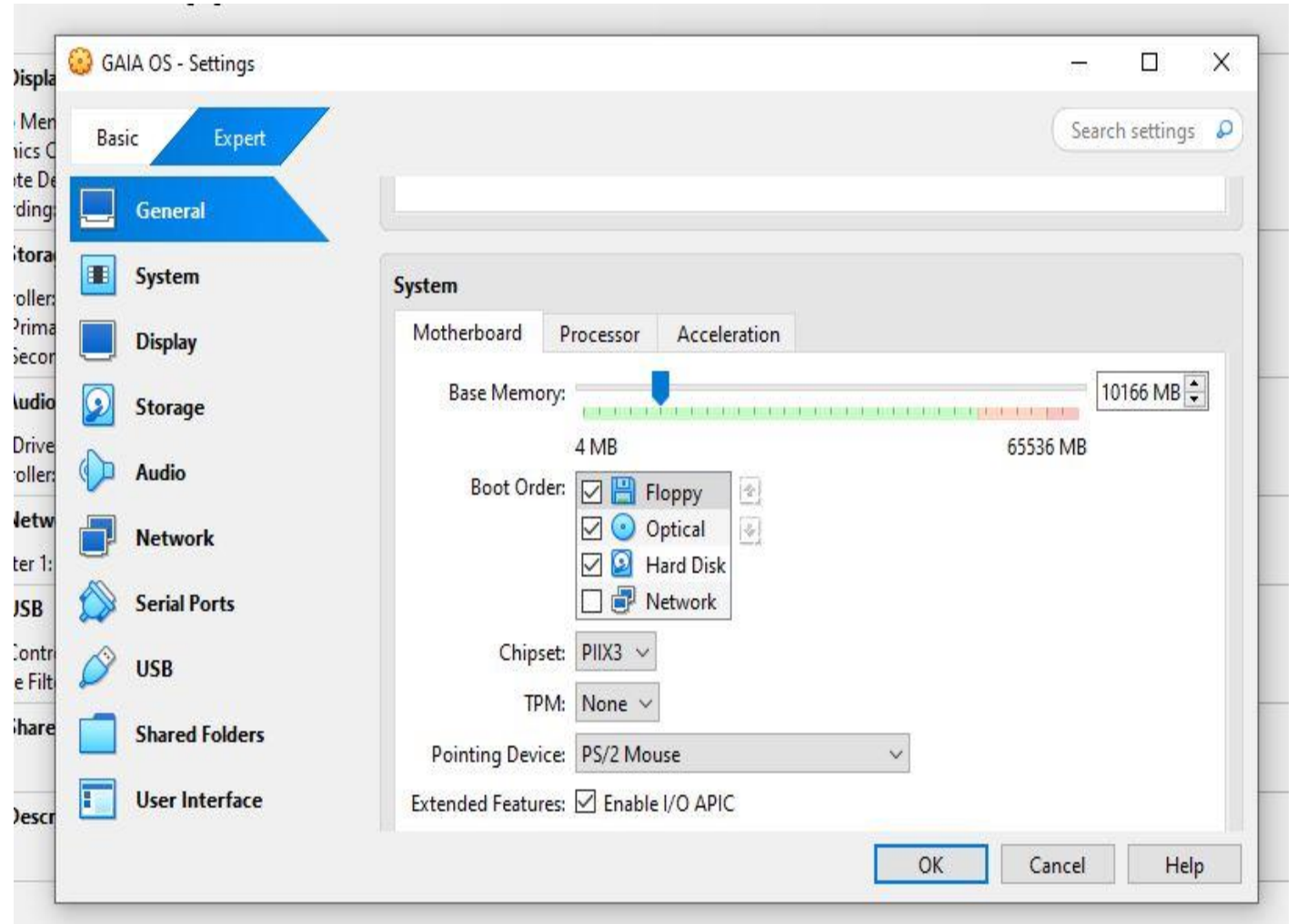
Base Memory within Oracle VirtualBox parameters.

- Performance Stability:** Provisioning hardware resource

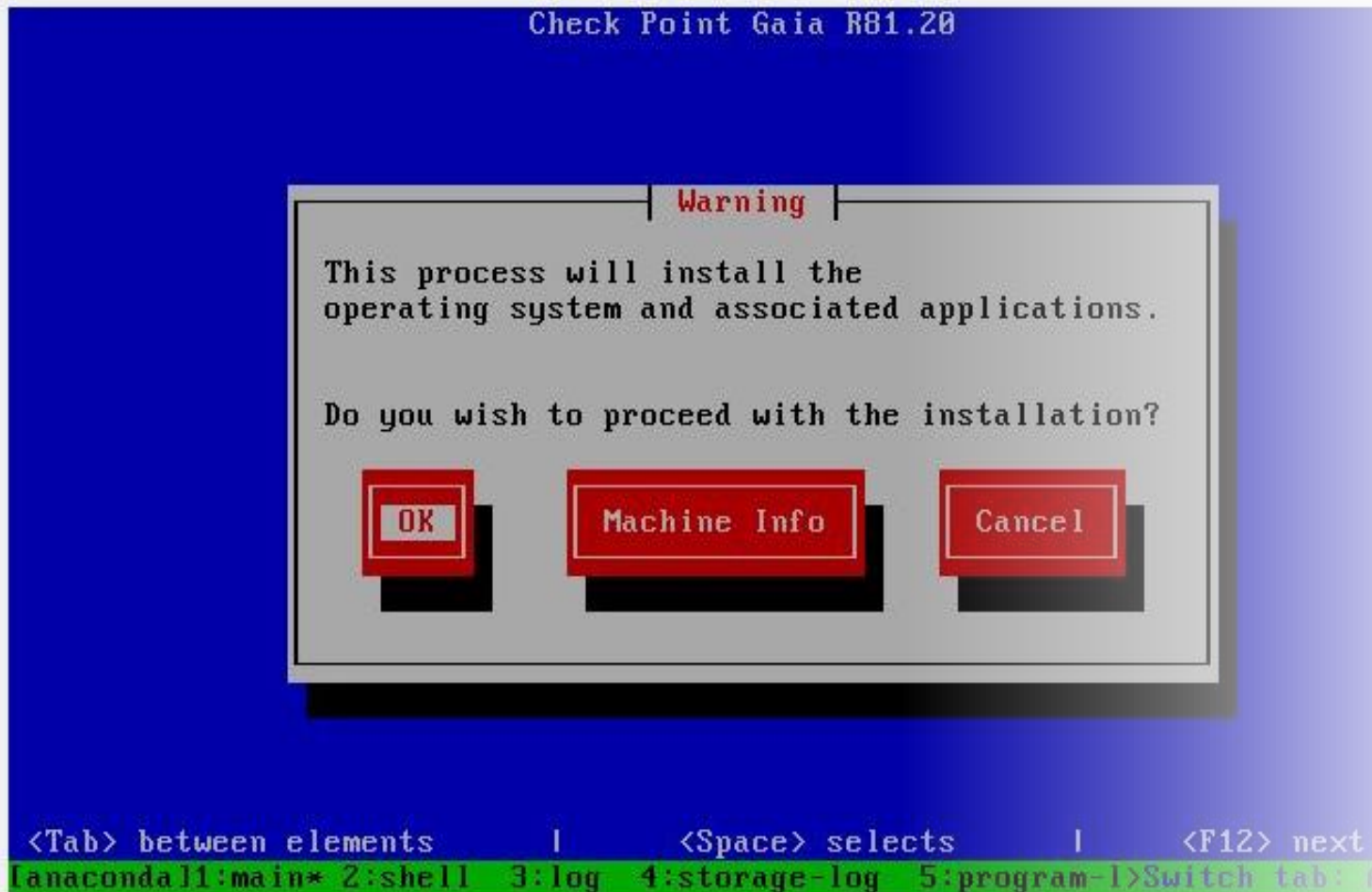
pools to run underlying firewall engine routines smoothly.

- Boot Order Setup:** Defining clean optical device boot

mapping choices under expert properties tabs.



Hardware Disk Formatting Warning Confirmation



- **Formatting Boundary:** System forces manual safety prompts before running disk partition writing tasks.

- **Safety Interlocking:** Prevents accidental data overwrites on active virtual storage allocations.

- **User Intent Check:** Manual selection of "OK" to allow deep formatting routines to start.



Regional Profile: Great Britain Keyboard Selection

- **Input Alignment:** Swapping standard default layouts to accommodate local input styles.
- **Target Choice:** Explicit configuration selection of the "Great Britain" keyboard map format.
- **Character Translation:** Prevents symbol layout errors during raw command-line administration sessions.

Check Point Gaia R81.20

Account Configuration

Choose a password for the "admin" account.

Password: *****

Confirm: *****

OK **Back**

> between elements | <Space> selects | <F12>
ondall:main* 2:shell 3:log 4:storage-log 5:program-1>Switch

Primary Admin Account Password Assignment

- **Default Root Account:** Establishing core passwords for the native system admin user profile.
- **Hardening Threshold:** Enforcing strict string validation matching requirements across input characters.
- **Verification Field:** Dual identical confirmation entries protect baseline configuration security access paths.

Maintenance Password Configuration

Check Point Gaia R81.20

Maintenance password

Create a password for Maintenance mode ("admin" user).

Password: *****

Confirm: *****

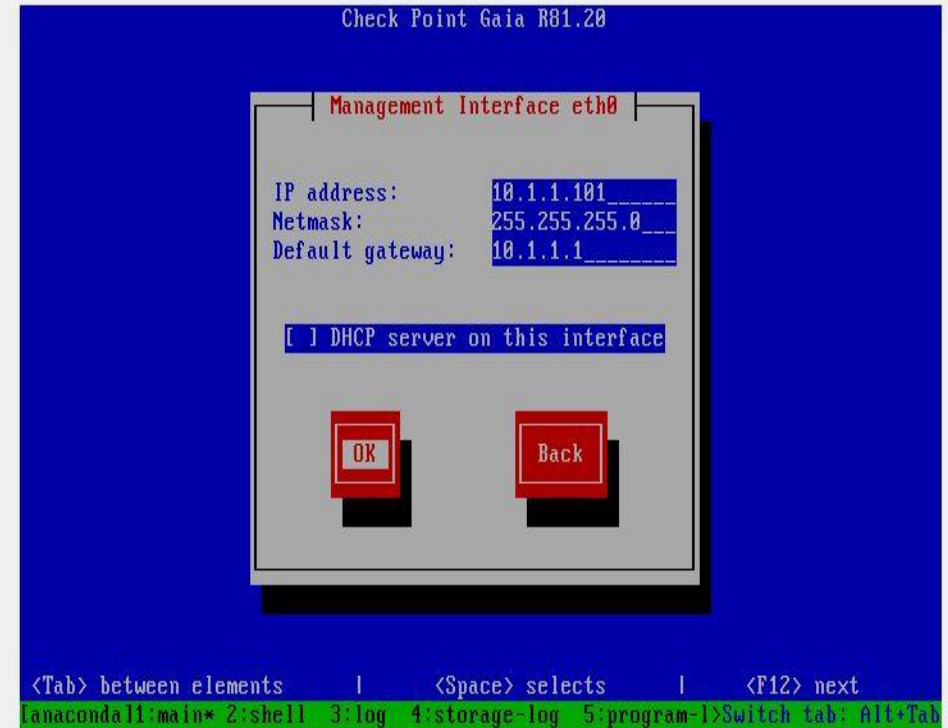
OK **Back**

- **Isolated Fail-safe:** Setting up passwords for low-level recovery interface access modes.
- **Separation of Scope:** Keeps everyday management tasks isolated from emergency recovery access paths.
- **Access Restriction:** Restricts low-level boot modification rights to verified senior network infrastructure engineers.

<Tab> between elements | <Space> selects | <F1>
[anaconda]1:main* 2:shell 3:log 4:storage-log 5:program-1>Switch

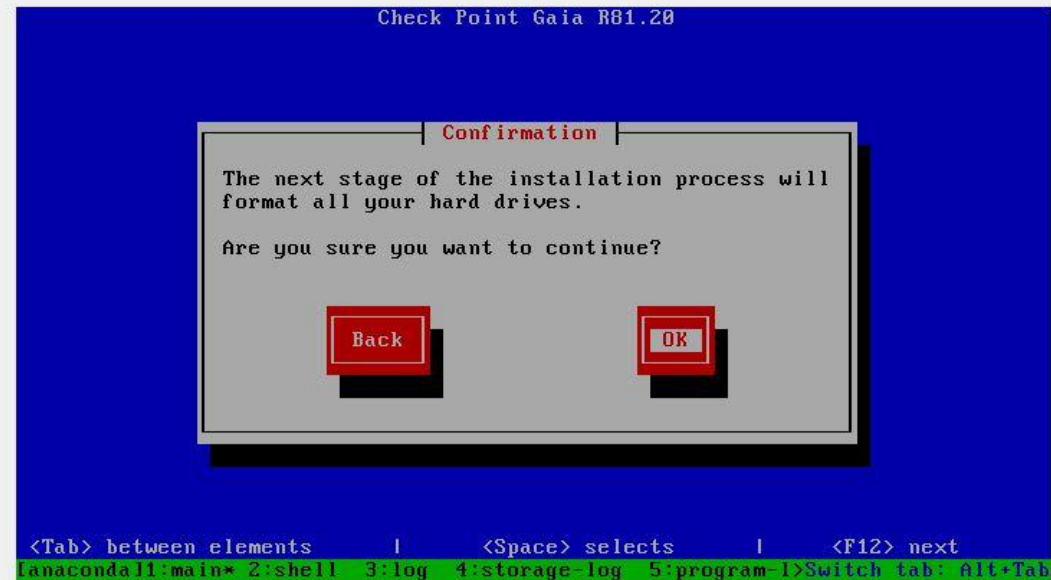
Management Interface eth0 Network Configuration

- **Interface Base Address:** Assigning static addressing details directly to interface eth0:
- **IP Address:** 10.1.1.101
- **Subnet Mask:** 255.255.255.0
- **Default Gateway Route:** 10.1.1.1
- **Permanence Control:** Keeping DHCP disabled to ensure management destination IPs do not change.



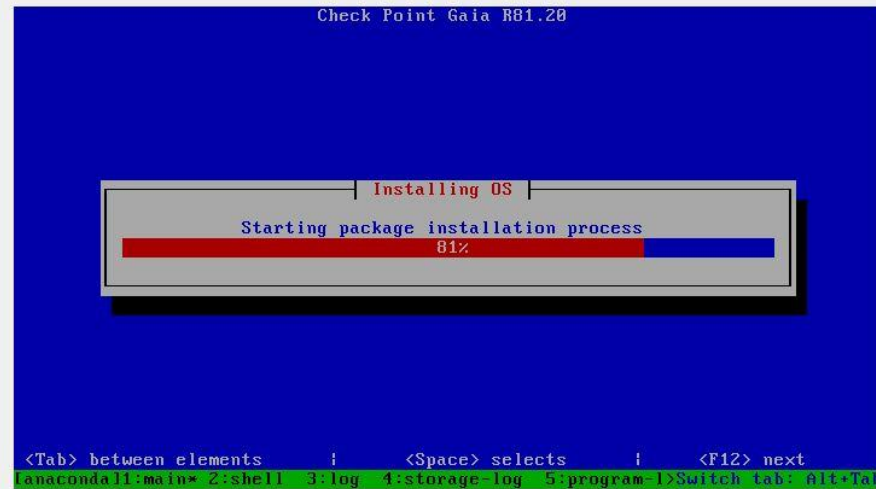
Disk Surface Partition Formatting Confirmation

- **Execution Step:** Final validation window alerting the operator that storage drives will be wiped clean.
- **Destructive Step:** Confirms deletion of unmanaged partition tracks on the virtual drive asset.
- **Write Commitment:** Selecting yes flags the host engine to begin deep system image transfers.



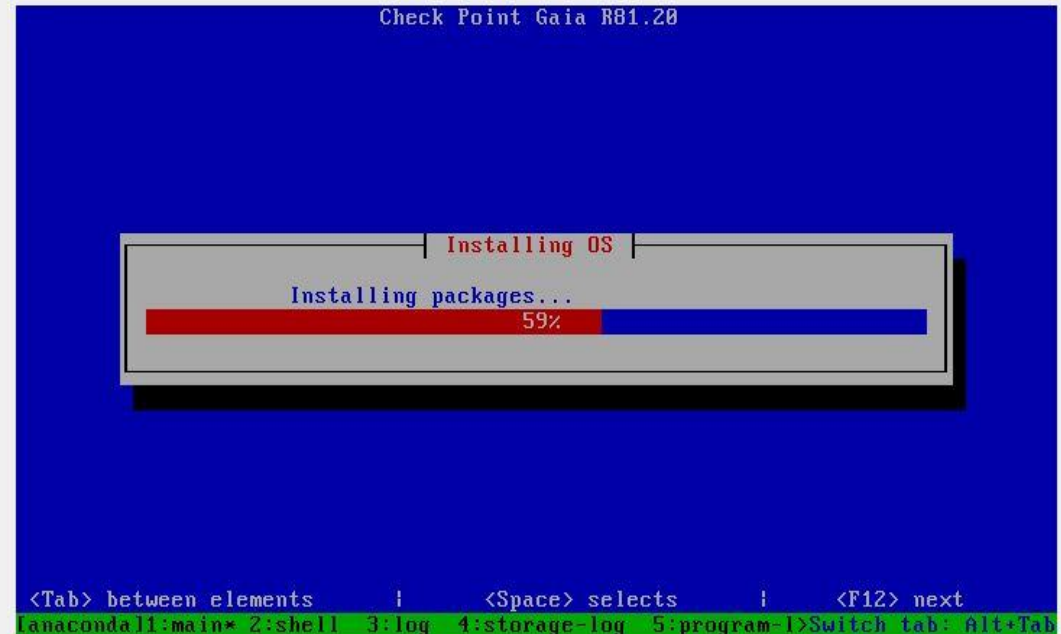
Gaia OS Block Copy & Installation Tracking (Part A)

- **Image Deployment:** Writing core firewall system file trees out to storage partitions.
- **File Transfer Status:** Monitoring data transfers during installation script operations.
- **Landmark Checkpoint:** Verifying steady deployment tracking as operations approach conclusion.



Gaia OS Block Copy & Installation Tracking (Part B)

- **System Tracking:** Processing secondary database file trees and application binary segments.
- **Library Validations:** Ensuring background dependencies register correctly across kernel modules.
- **Reboot Preparation:** System completes script runs, preparing hardware blocks for clean restarts.



Base Installer Termination & Ejection Notification

- **Successful Termination:** Local automated image writes conclude successfully across storage surfaces.
- **Media Ejection Protocol:** Explicit terminal reminders warning users to drop raw ISO maps before booting.
- **Interactive Directive:** Demands pressing return keys to safely flush cash structures to clear system reboots.

```
Starting installer, one moment...
anaconda 21.48.22.156-1 for anaconda bluesky started.
* installation log files are stored in /tmp during the installation
* shell is available on TTY2
* when reporting a bug add logs from /tmp as separate text/plain attachments

Installation complete.      Press return to quit

Please do not remove the installation media until the system reboots.

[anaconda11:main* 2:shell 3:log 4:storage-log 5:program-1]Switch tab: Alt+Tab
```

Local CLI Shell Hardening & Timeout Extensions

- **Operational Shell Access:** Opening terminal routes to manage platform settings using the root admin profile.
- **Inactivity Hardening:** Setting higher active session window lifetimes to prevent drops during laboratory tasks.
- **Applied Command Rules:**
 - set inactivity-timeout 720
 - set web session-timeout 720
 - save config

```
This system is for authorized use only.
login: admin
Password:
Last login: Tue Jun 23 08:47:20 on tty1
In order to configure your system, please access the Web UI and finish the First
Time Wizard.
gw-180e66> set inactivity-timeout 720
gw-180e66> set web session-timeout 720
gw-180e66> save config
gw-180e66> _
```

Multi-User Access Banner Notice Verification

A terminal window with a black background and white text. The text reads: "This system is for authorized use only." followed by "login:" on the next line.

```
This system is for authorized use only.  
login:
```

- **Compliance Notification:** Activating clear access policy banner strings: *"This system is for authorized use only."*
- **Security Control Layer:** Confirms shell access
paths demand complete login
reviews prior to granting control.
- **Isolation Integrity:** Ensures unauthenticated sessions drop automatically at the terminal border.

Web Wizard: Hostname & Local DNS Registration

- **Device Context:** Setting the device naming string explicitly to A-SMS via the web console.
- **Domain Registration:** Binding the system structure inside local reference domain parameter swansea-acca.
- **Upstream Reference Entries:** Programmatic mapping across primary, secondary, and tertiary DNS routes.

tion Wizard x +

Not secure https://10.1.1.101/_d5ca2f6ab9edd7a8f4903bd5a8a222cf/cgi-bin/ftw_index.tcl

Device Information

CHECK POINT

Host Name:	A-SMS
Domain Name:	swansea-acca
Primary DNS Server:	192.168.1.1
Secondary DNS Server:	8.8.8.8
Tertiary DNS Server:	4.2.2.2

Proxy Settings

☐ Use a Proxy server

Address:	
Port:	8080

< Back Next > Cancel

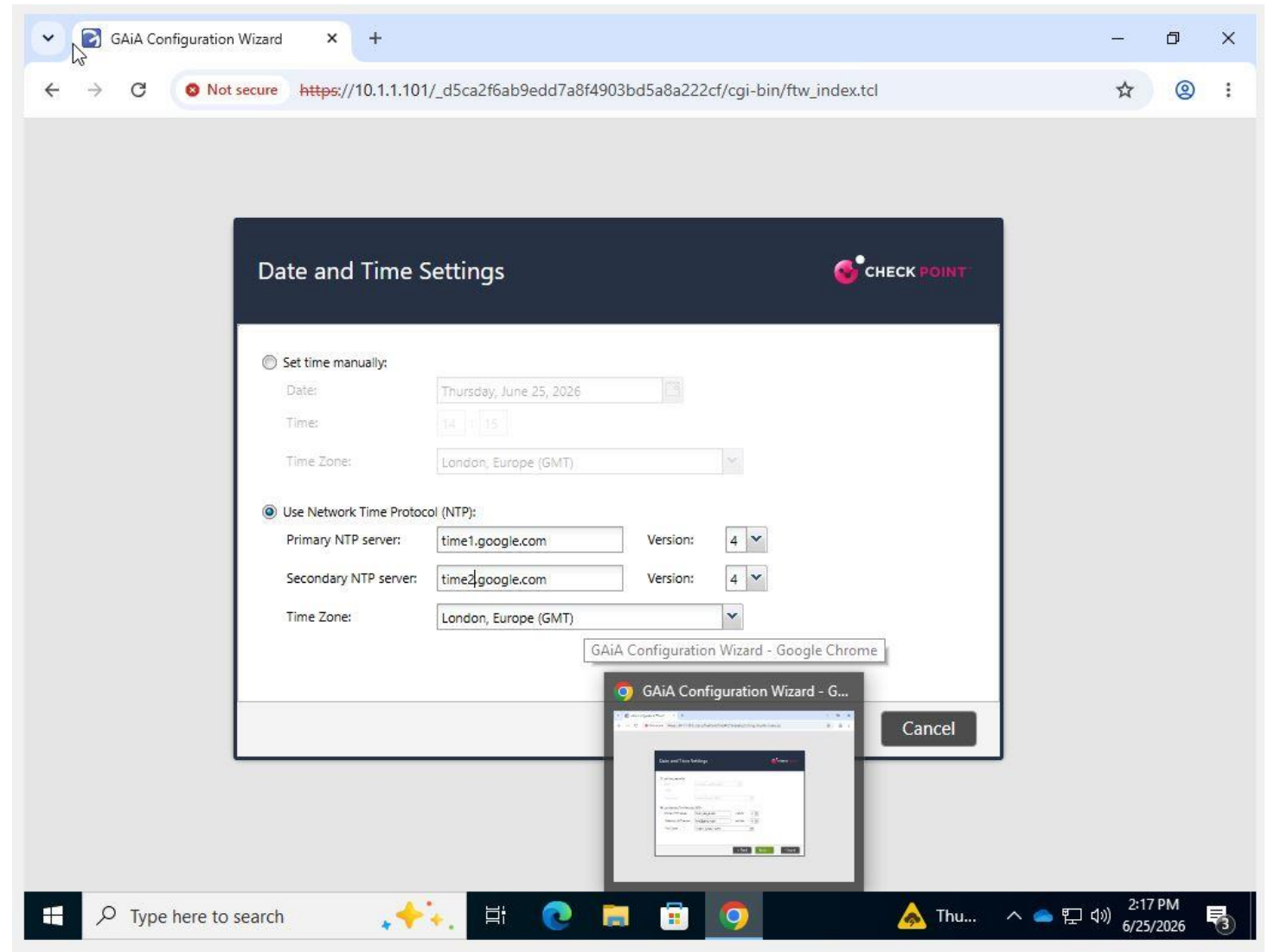
Microsoft Edge

Type here to search

Cura...

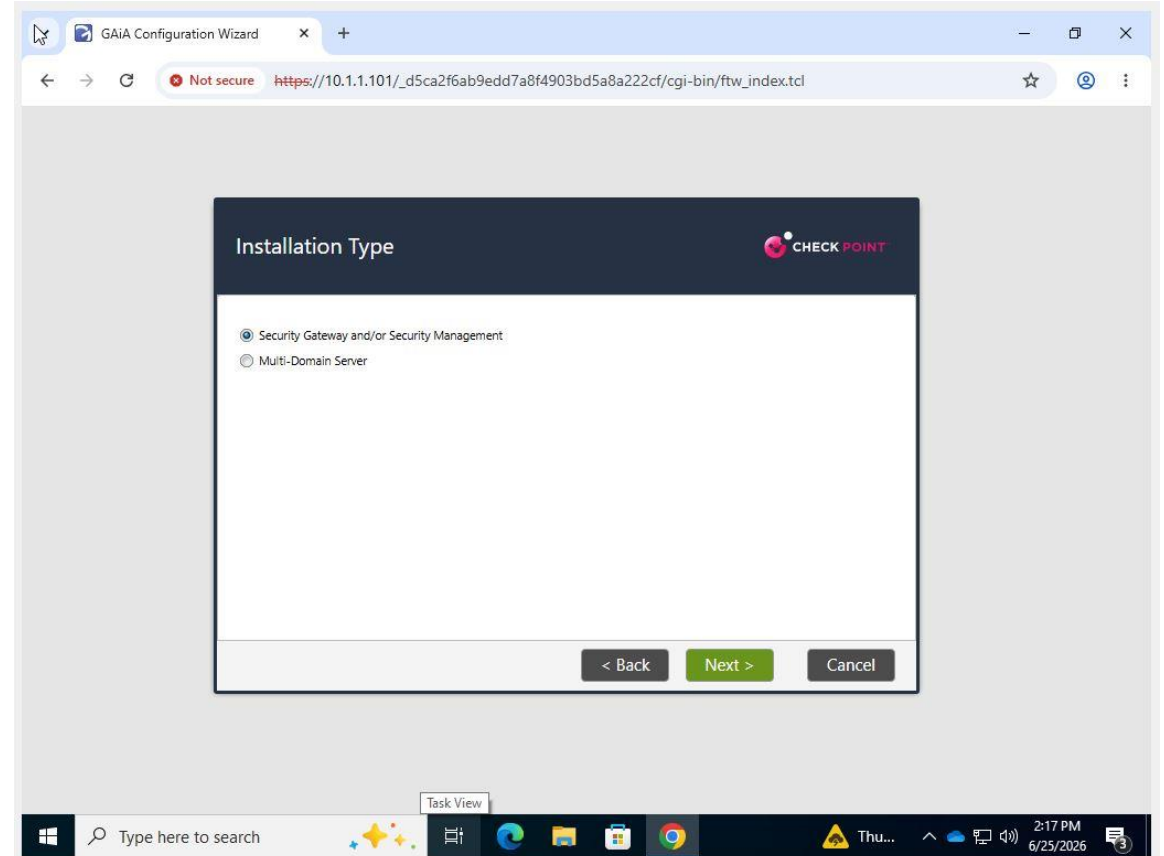
Web Wizard: Network Time Protocol Synchronization

- **Timeline Validation:** Synchronizing clock structures via Network Time Protocol (NTP) to enable accurate log auditing.
- **External Reference Sources:** Linking server clocks to upstream timing points (://google.com / ://google.com).
- **Time Zone Localization:** Setting localization fields to match London, Europe (GMT) regional tracking rows.



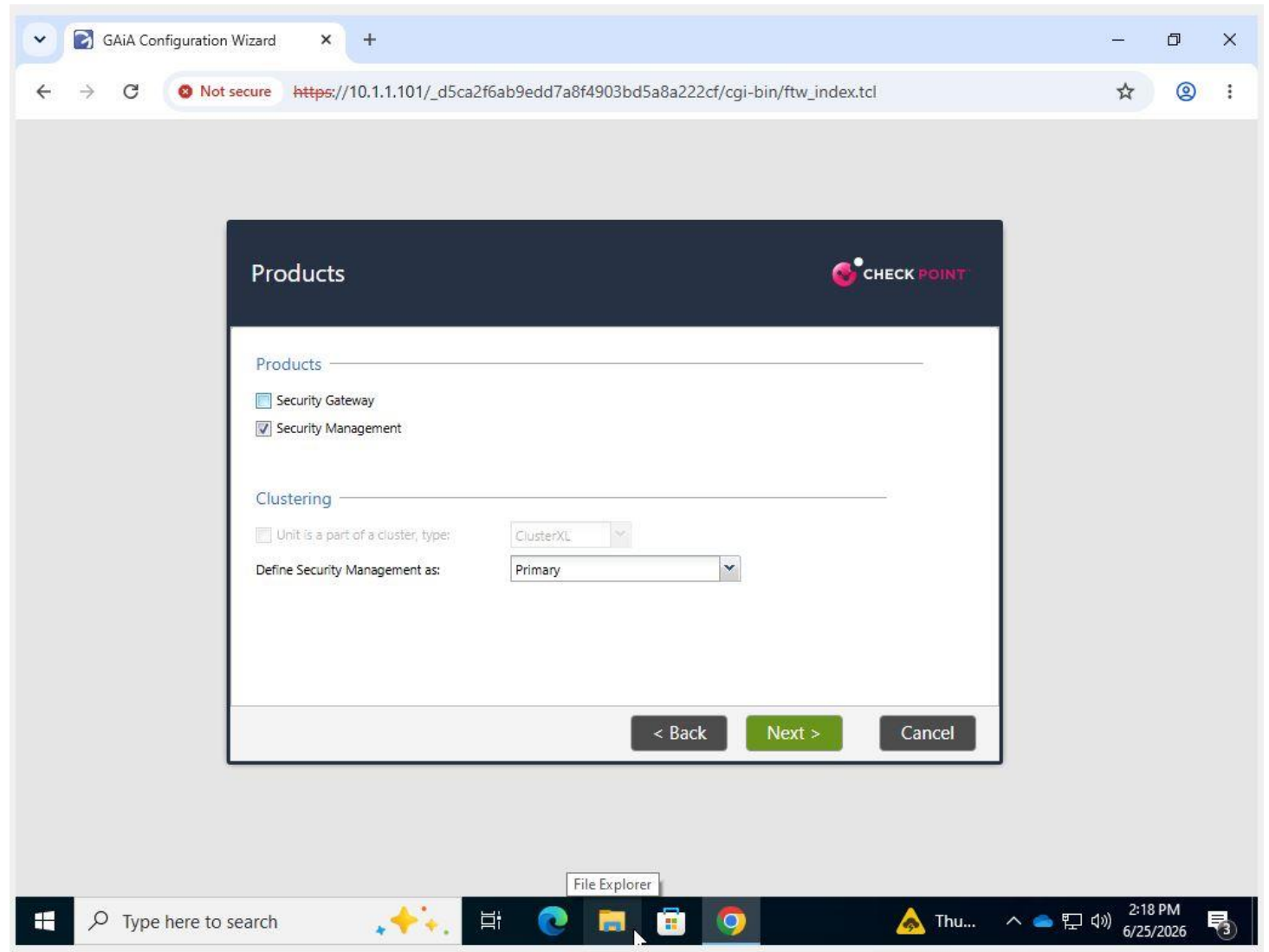
Web Wizard: System Deployment Strategy Choices

- **Role Mapping:** Defining specific software tasks using the deployment setup checklists.
- **Functional Core Setup:** Selecting options for "Security Gateway and/or Security Management".
- **Blade Framework Engine:** Prepares core systems to load modern security inspection software blades.



Web Wizard: Activating the Security Management Blade

- **Architecture Isolation:** Turning off gateway components on this node to prioritize management server functions.
- **Software Blade Selection:** Activating "Security Management" exclusively and setting its type to Primary.
- **Task Optimization:** Ensures the system functions solely as a central repository for firewall rulesets.

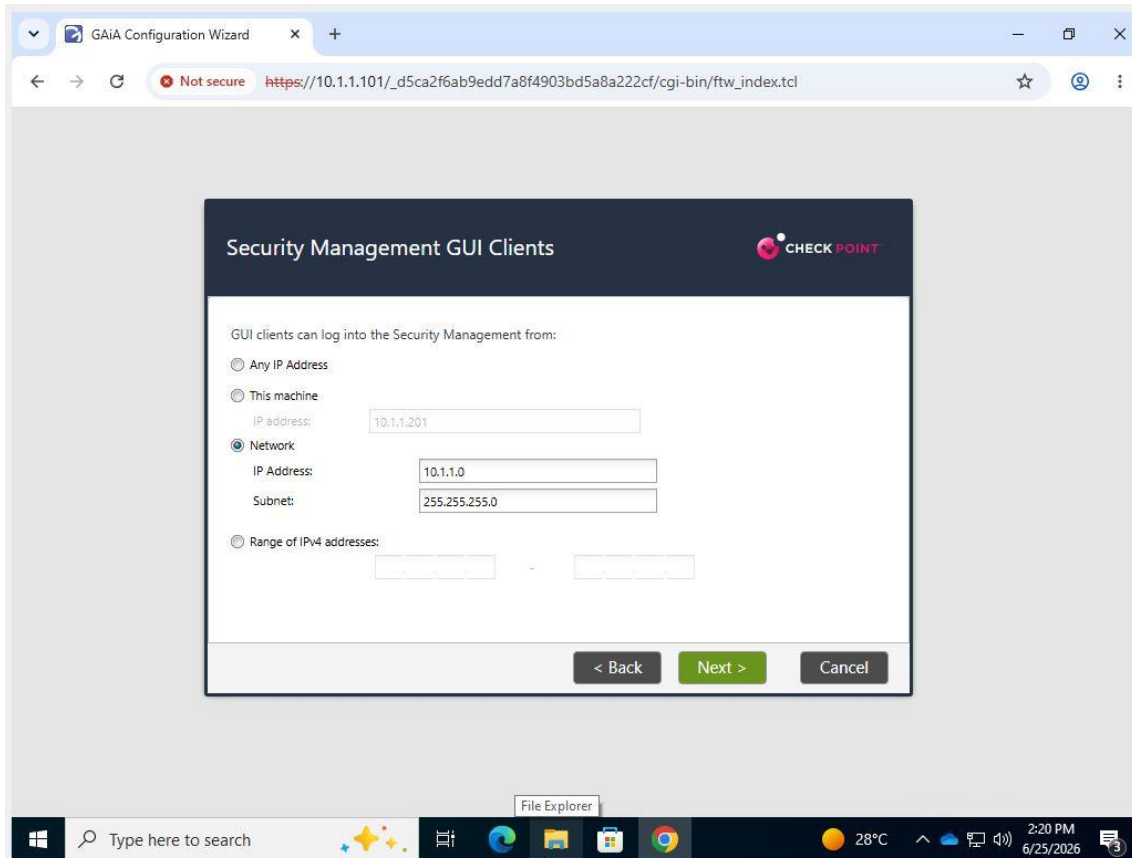


Web Wizard: SmartConsole Admin Profile Creation

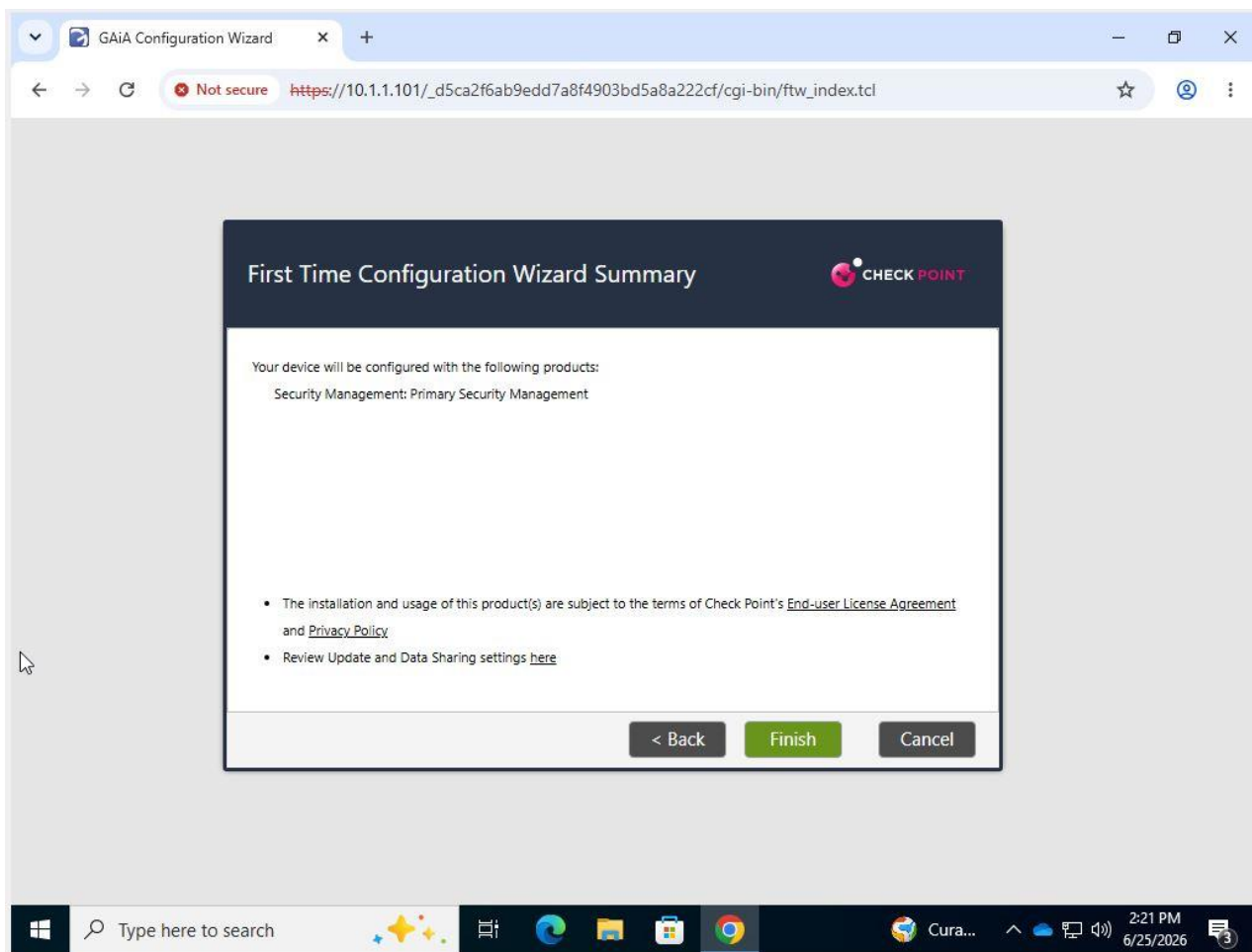
- **Decoupled Profile Identity:** Creating a new system administrator identity decoupled from root credentials.
- **Defined Username Key:** Explicitly setting the administrative identifier account string to cadmin.
- **Strength Assurance:** Automatic evaluation gauges confirm password strings meet robust safety rules.

The screenshot shows a web browser window titled "GAiA Configuration Wizard" with the address bar displaying "https://10.1.1.101/_d5ca2f6ab9edd7a8f4903bd5a8a222cf/cgi-bin/ftw_index.tcl". The main content area displays the "Security Management Administrator" configuration screen, which includes the Check Point logo and two radio button options: "Use Gaia administrator: admin" and "Define a new administrator". The "Define a new administrator" option is selected. Below this, there are three input fields: "Administrator Name" (containing "cadmin"), "New Password" (containing masked characters), and "Confirm Password" (containing masked characters). To the right of the password fields is a green progress bar and the word "Good". At the bottom of the form are three buttons: "< Back", "Next >", and "Cancel". The Windows taskbar at the bottom shows the search bar, task view button, and several application icons, including the Microsoft Store, with a system tray showing the time as 2:19 PM on 6/25/2026.

Web Wizard: GUI Management Workstation Client Subnet Locking



- **Access Control Logic:** Bypassing global connection options to restrict client traffic paths.
- **Subnet Level Entry:** Restricting interface control access to the explicit management network block: 10.1.1.0/24.
- **Network Security Shield:** Discards unauthorized connections before processing authentication challenges.

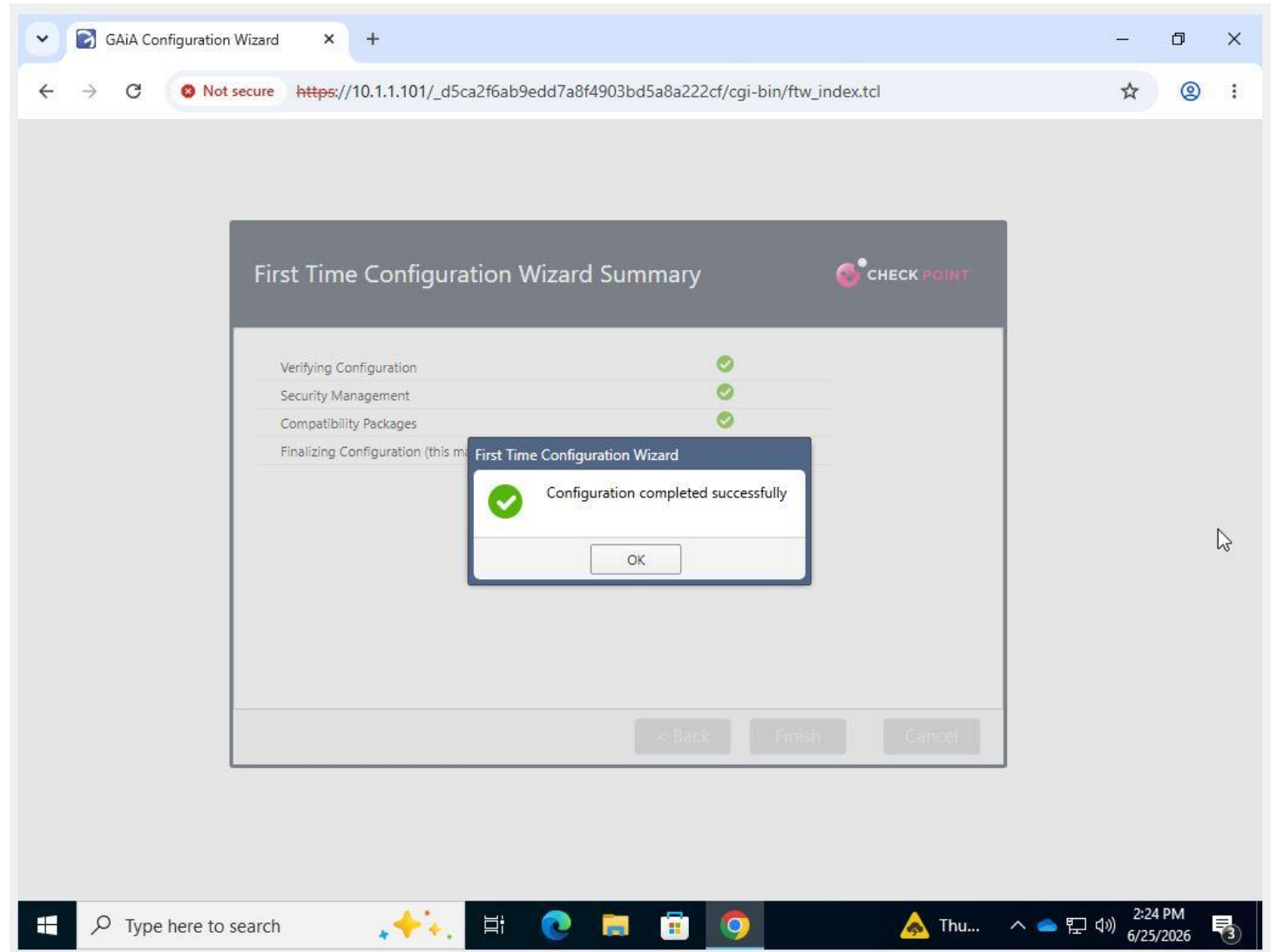


Web Wizard: Final Configuration Review

- **Audit Step:** Final validation review before committing local system files to active settings profiles.
- **Target Verification:** Confirming the appliance role matches the target role: Primary Security Management.
- **Commit Trigger:** Selecting "Finish" to write wizard selections directly to disk.

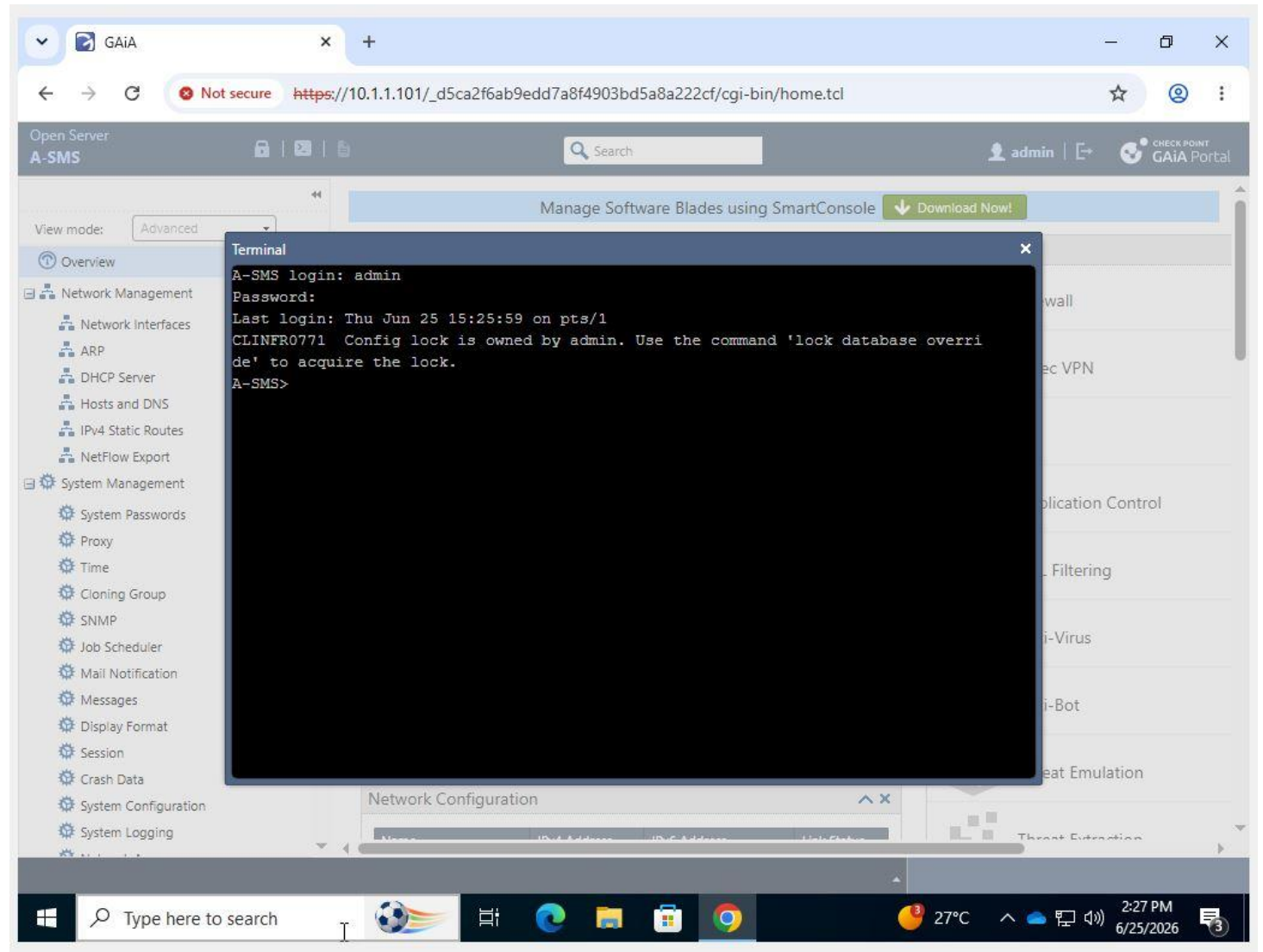
Post-Wizard Execution Success Validation

- **Execution Verification:** Monitoring automatic setting applications across core system folders.
- **Graphical Status Success:** System displays a clear confirmation message indicating successful completion.
- **Operational Readiness:** Enables internal system engines, allowing remote management clients to connect.



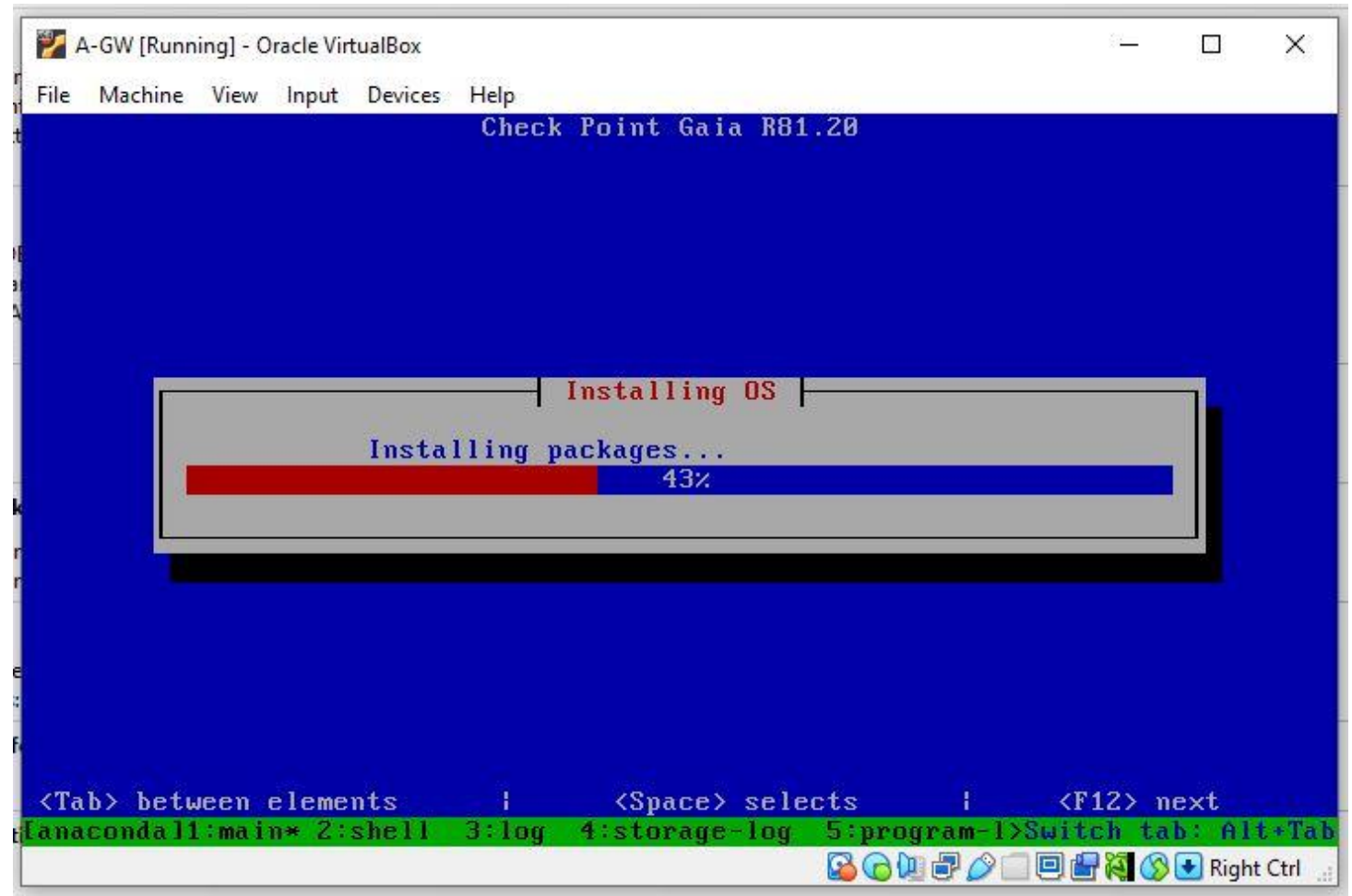
Gaia Portal Embedded CLI Management Authentication

- **Portal Authentication Access:** Logging in to web configuration dashboards for server A-SMS (10.1.1.101).
- **Integrated Console Engine:** Running terminal shells directly within browser windows using embedded portal web apps.
- **Lock Verification Checks:** Evaluating status strings to confirm configuration locks are held correctly by the admin profile.



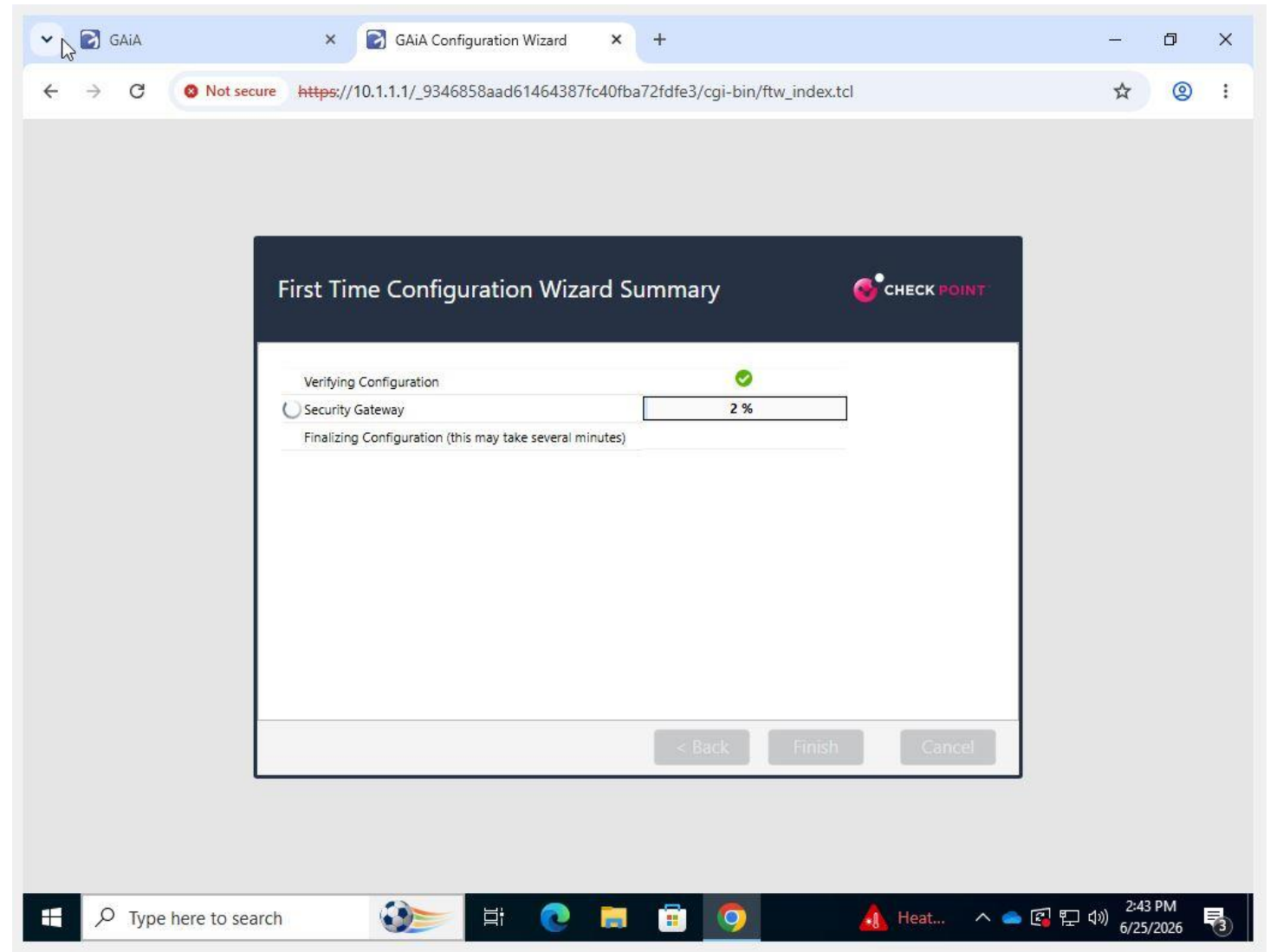
Security Gateway Operating System Installation Progress

- **Boundary Node Deployment:** Building the discrete Security Gateway hardware profile (A-GW) within VirtualBox.
- **Resource Tracking:** Monitoring extraction runs as the gateway operating system engine processes setup scripts.
- **Progress Tracking:** Tracking installation status levels to ensure clean data transitions to storage.



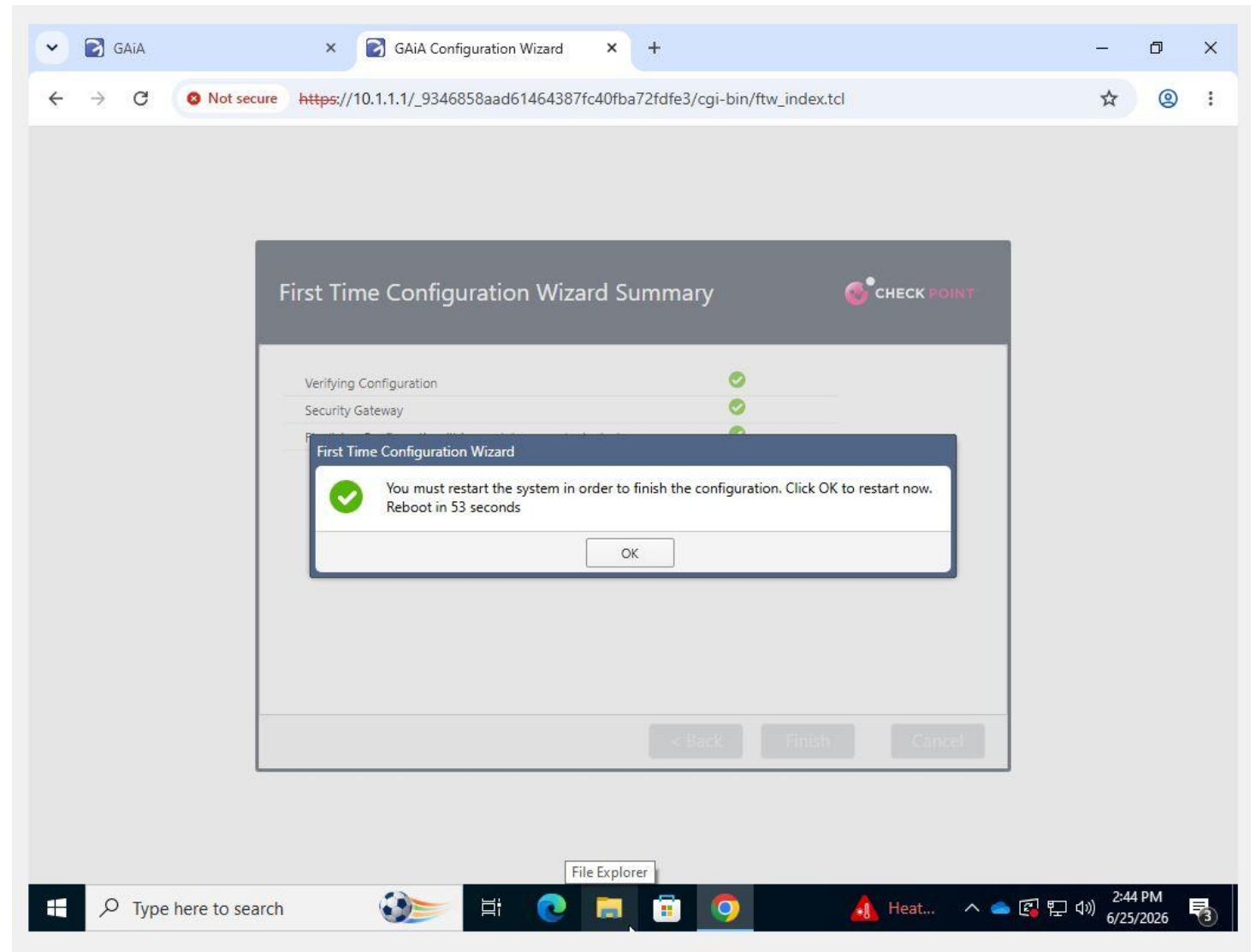
Security Gateway Web Wizard Initial Operations Pacing

- **Initial Gateway Setup:** Opening remote web connection paths to link with the gateway at address 10.1.1.1.
- **Wizard Execution Tracking:** Monitoring progress during first-time database script adjustments.
- **Underlying Tracking Layer:** Tracking low-level processes as they build core gateway components.

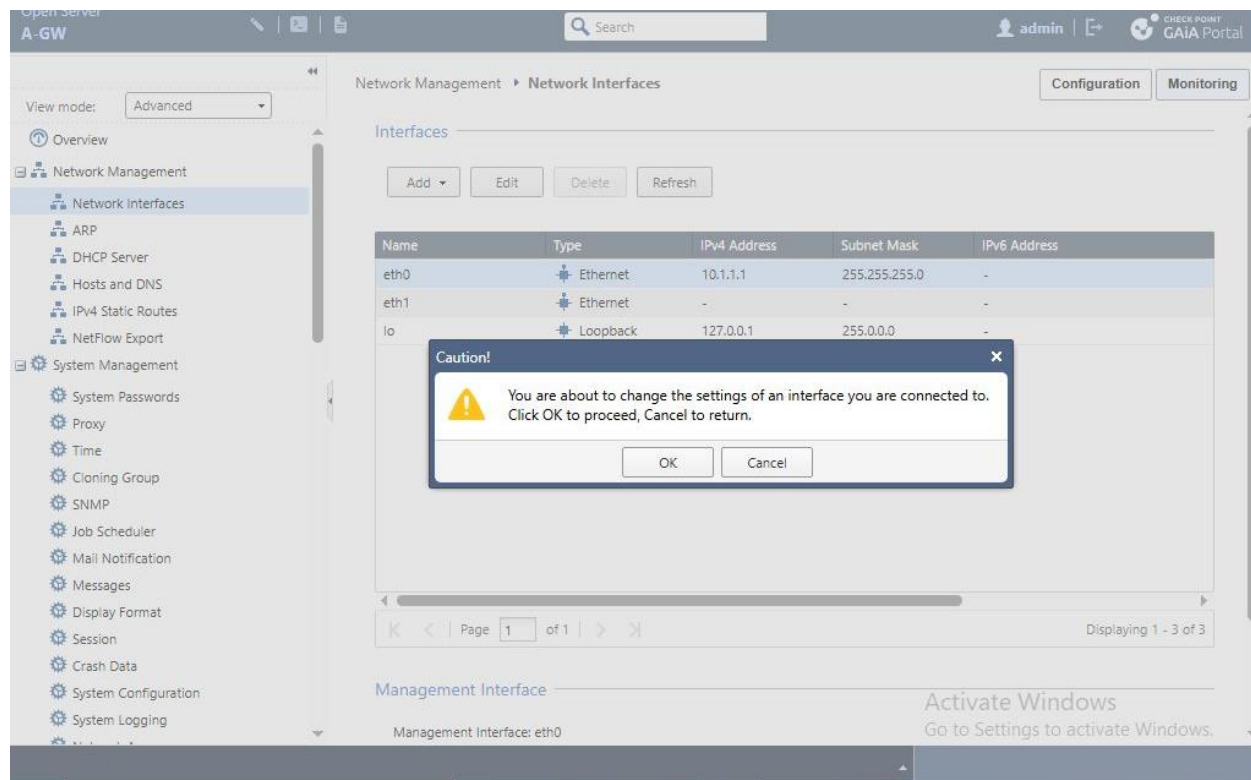


Gateway Post-Wizard Soft Restart Enforcement

- **Wizard Completion State:** First-time setup tasks conclude successfully across the boundary appliance framework.
- **System Action Call:** Triggers system notifications indicating a full machine reboot is mandatory.
- **State Alignment Step:** Soft restarts load configurations into memory, activating the gateway network stack.



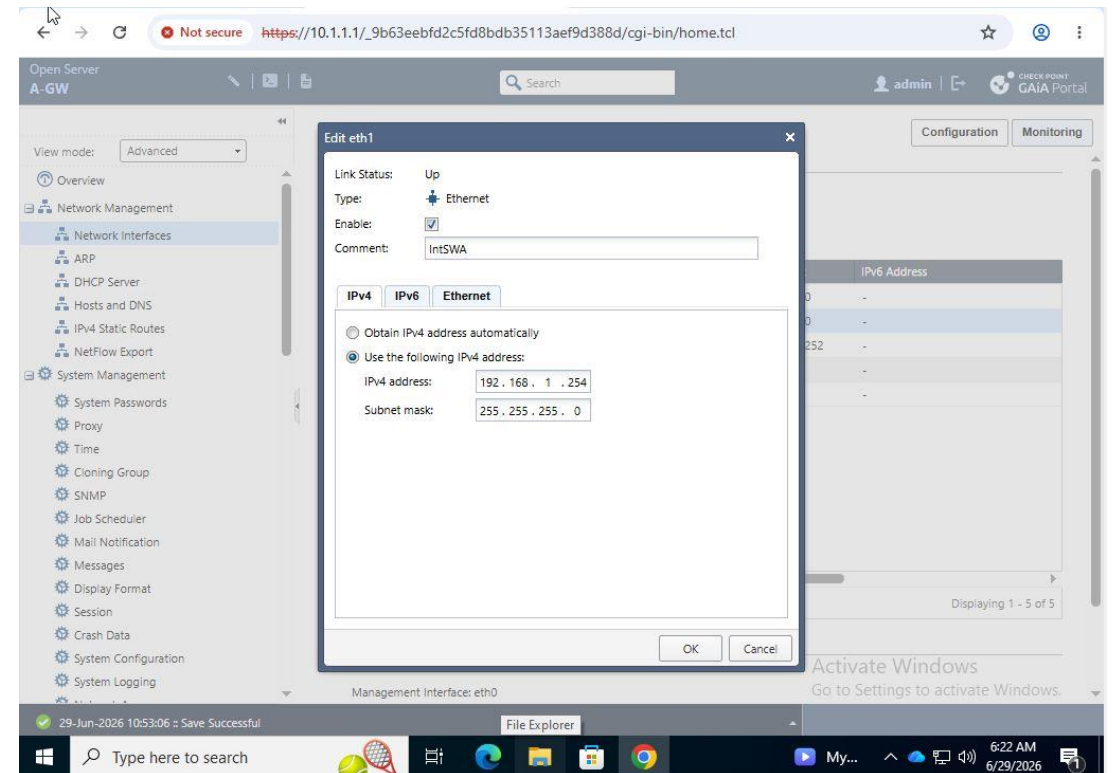
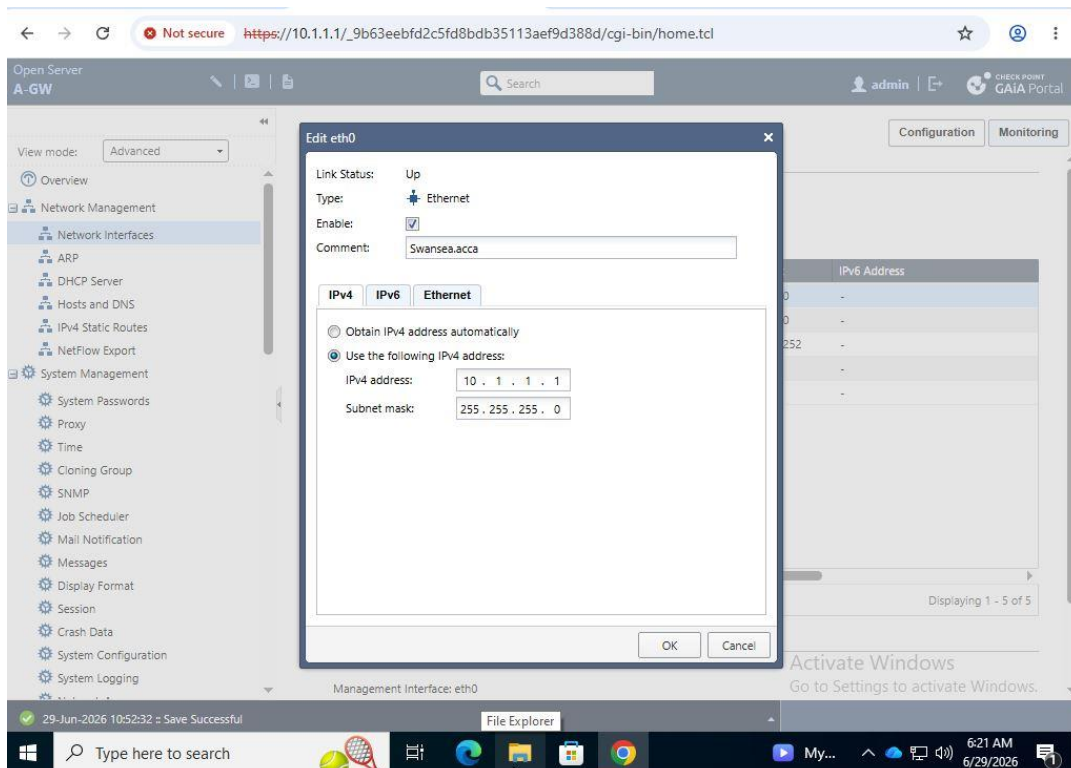
Live Interface Parameter Change Caution Alerts



- **Live Connection Monitoring:** Opening interface panels via the browser to adjust physical interface paths.
- **Safety Warning Notice:** System displays caution warnings before allowing modifications to active, connected interfaces.
- **Architect Decision Point:** Selecting OK confirms full knowledge of potential remote connection disconnects.

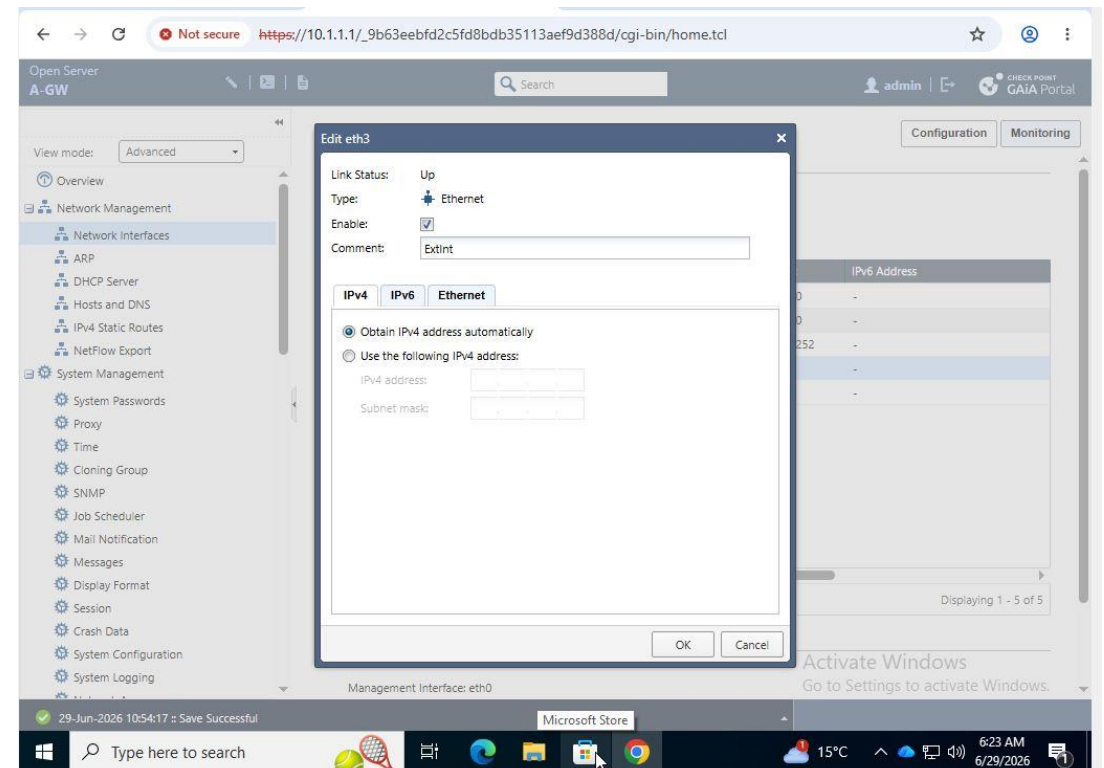
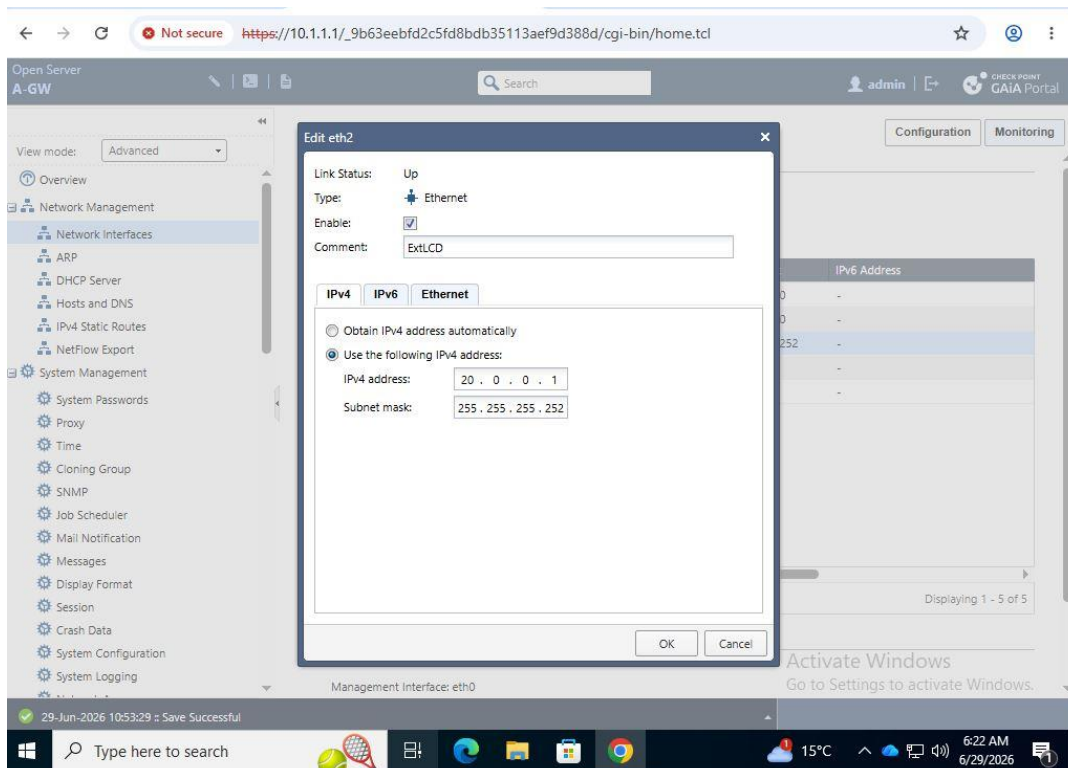
Properties Customization for Management & Internal Interfaces

- **eth0 (Mgmt Zone):** Statically assigned 10.1.1.1/24 with description Swansea.acca.
- **eth1 (Secure S-DC LAN):** Statically assigned 192.168.1.254/24 with description IntSWA.
- **Isolation Protocol:** Separates administrative system control paths from everyday corporate network user traffic.



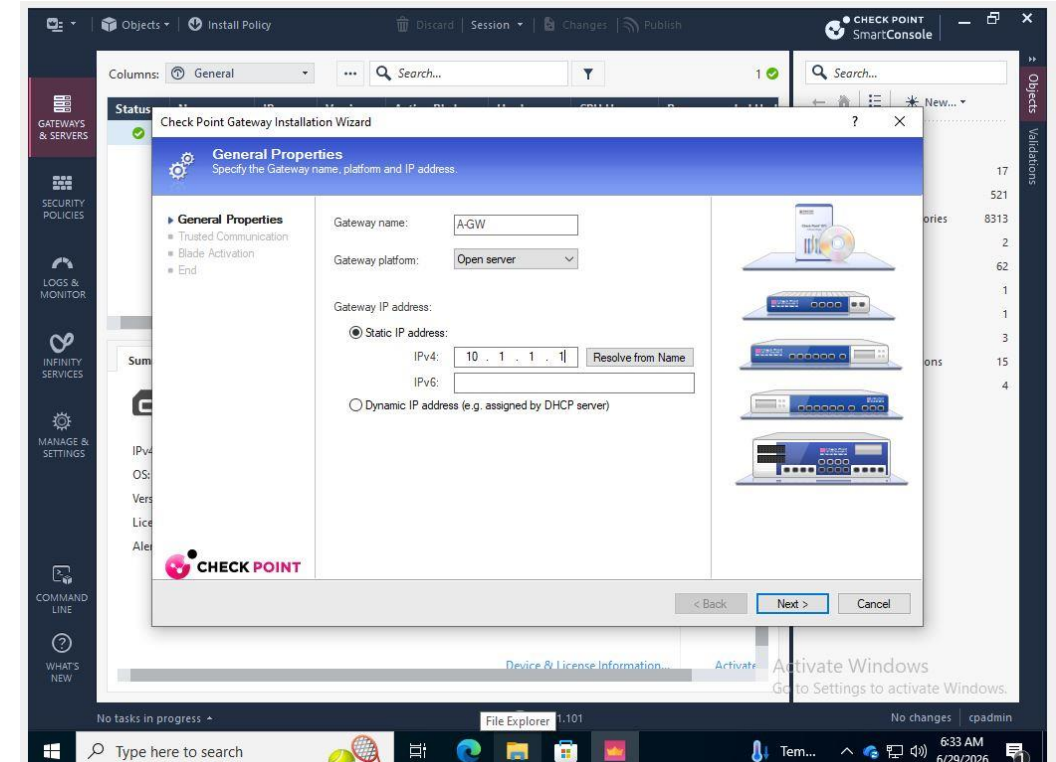
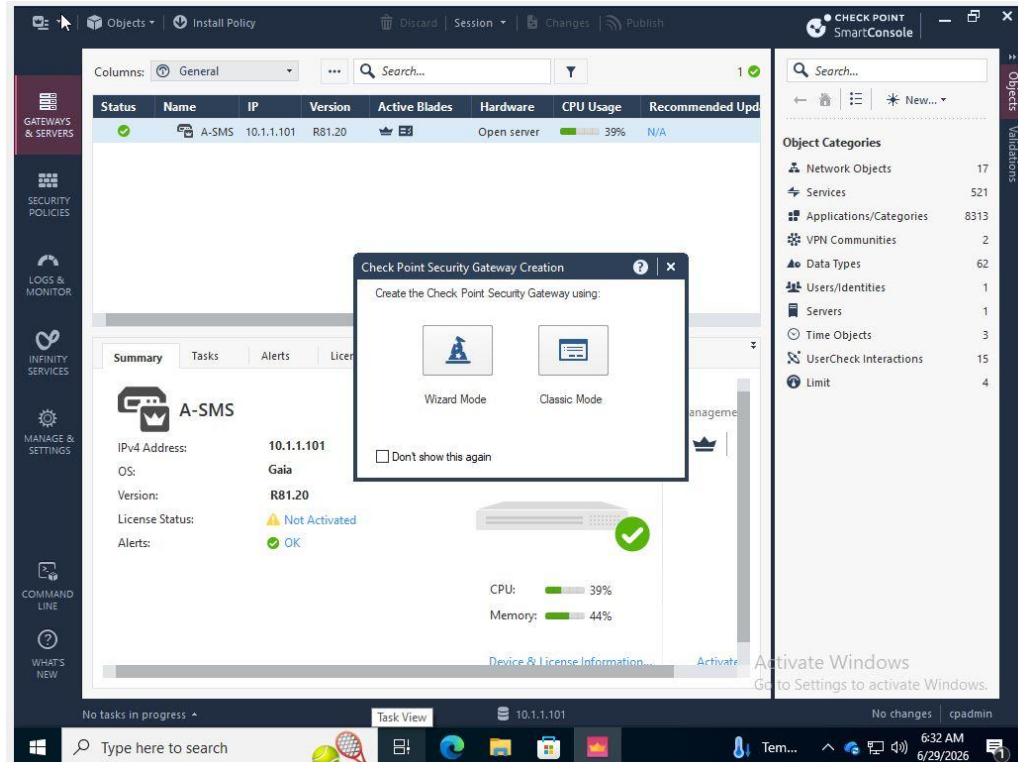
Properties Customization for Inter-Site & Public Interfaces

- **eth2 (Inter-site DMZ Link):** Statically assigned 20.0.0.1/30 with description ExtLCD.
- **eth3 (Public WAN Edge):** Set to dynamic assignment mode via DHCP with description Extint.
- **Border Controls Scope:** Provides multi-homed connectivity to link internal resources with
- outside communication targets.



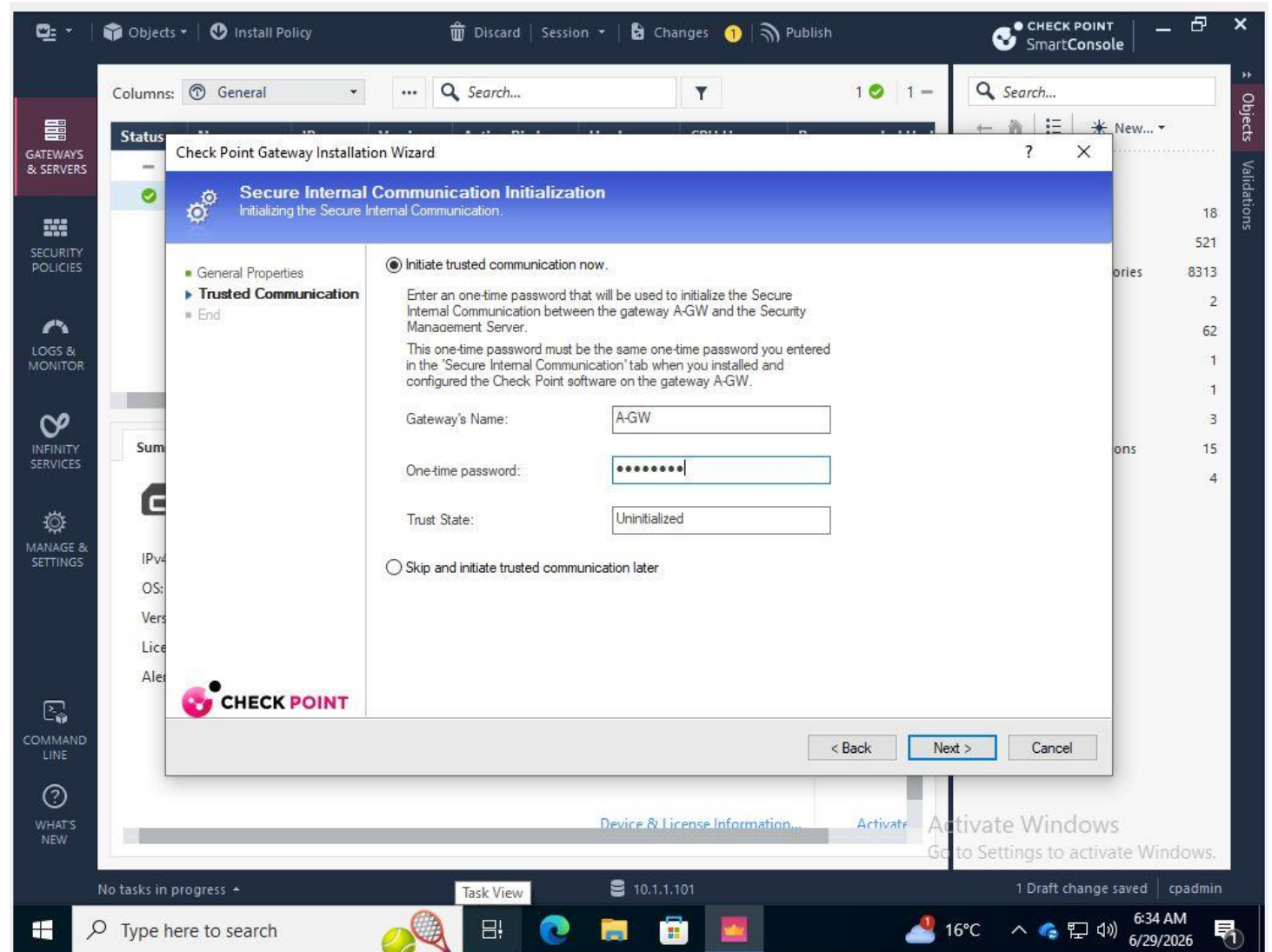
Security Gateway Object Modelling & Connection Pairing

- **Object Modeling:** Creating the primary Security Gateway object identity inside the SmartConsole network configuration map layout (A-GW).
- **IP Binding Configuration:** Binding the target framework node directly to static management location address 10.1.1.1.
- **One-Time Password Exchange:** Initializing cryptographic handshakes using matching trust authorization keys.



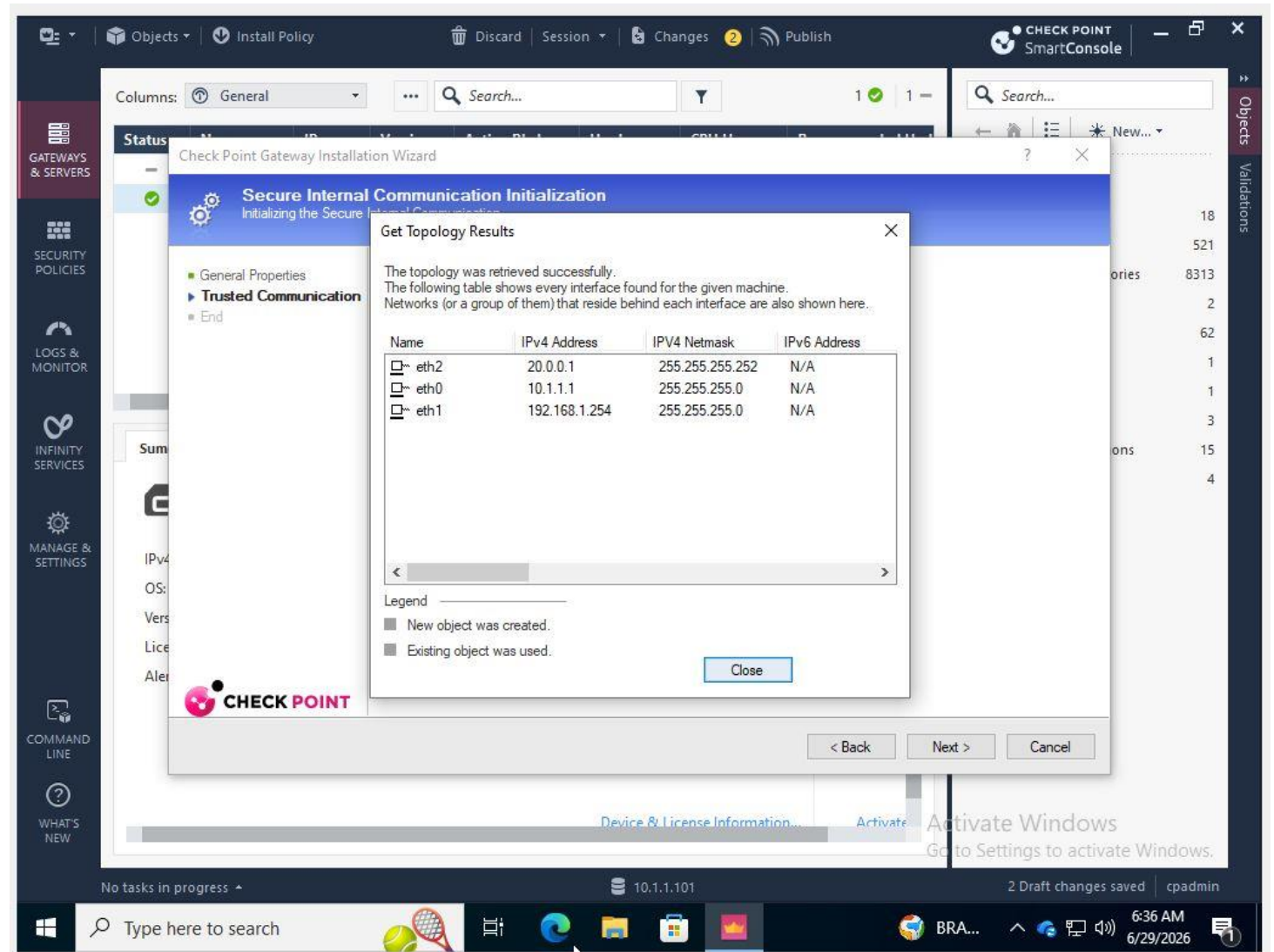
Remote Gateway Inter-Component Key Pairing Setup

- **Trust Relationship Pairing:** Establishing secure, encrypted tracking paths over network links.
- **Cryptographic Key Pairing:** Exchanging one-time security passkeys to securely link the components.
- **Policy Path Shield:** Encrypts policy distribution paths using mutual certificate verification keys.



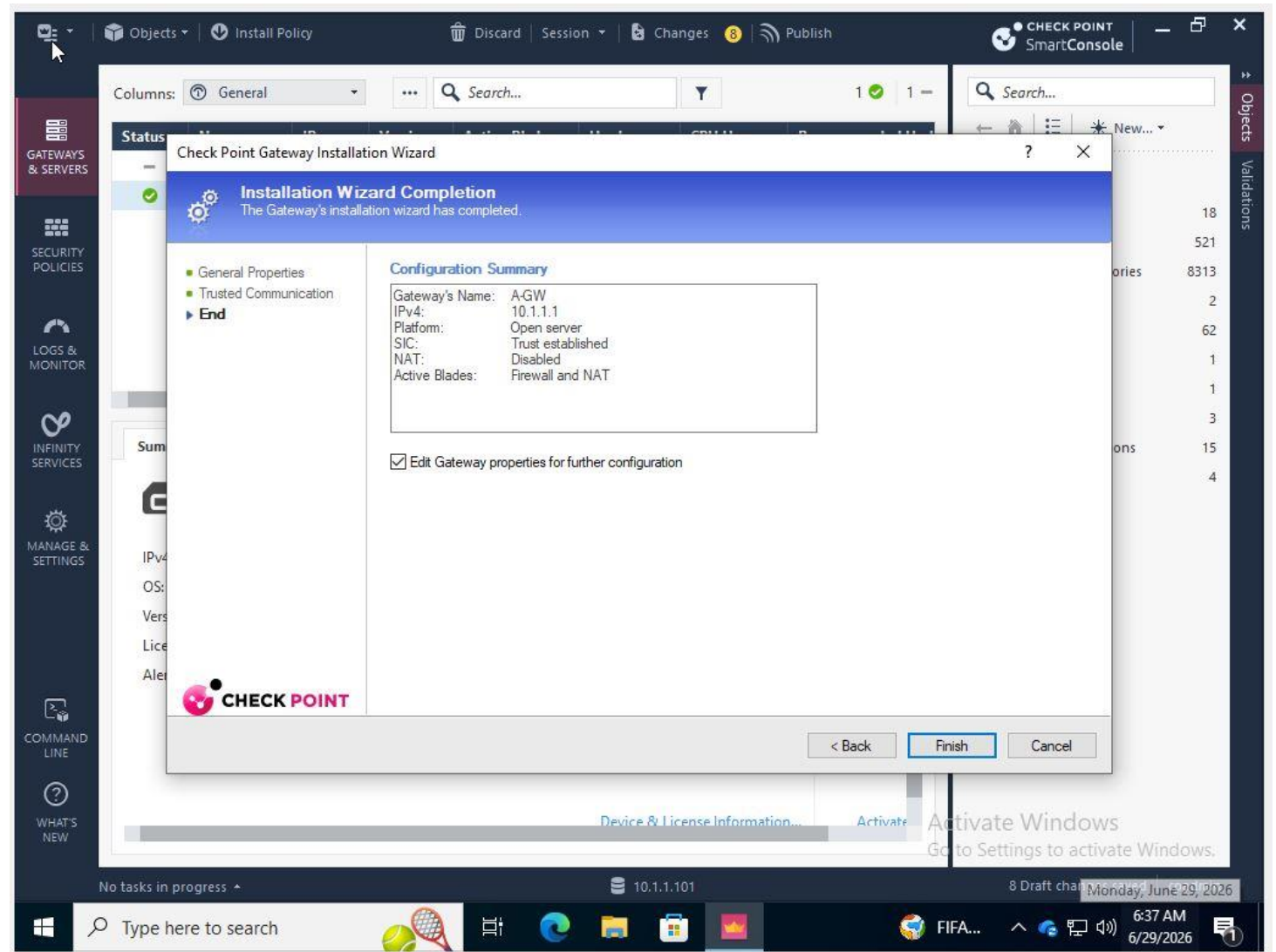
Programmatic Interface Topology Extraction

- **Automated Interface Query:** Management systems successfully pull topology properties across the cryptographic link.
- **Discovered Assets List:** Automatically maps interface lines including eth0, eth1, and eth2 subnets.
- **Verification Check:** Confirms addressing schemas discovered match target infrastructure topology profiles.



Gateway Installation Pipeline Success Completion

- **Configuration Log Summary:** Reviewing final operational definitions prior to completing the deployment pipeline.
- **Trust State Confirmed:** Structural logs explicitly confirm: "**SIC: Trust established**".
- **Default Engines Profile:** Activates core Firewall and Network Address Translation engines by default.



The screenshot displays the Check Point SmartConsole interface. On the left, a table lists active blades for the gateway A-GW:

Status	Name	IP	Version	Active Blades	Hardware	CPU Usage	Recommended Upd
—	A-GW	10.1.1.1	R81.20	—	Open server		
✓	A-SMS	10.1.1.101	R81.20	—	Open server	18%	N/A

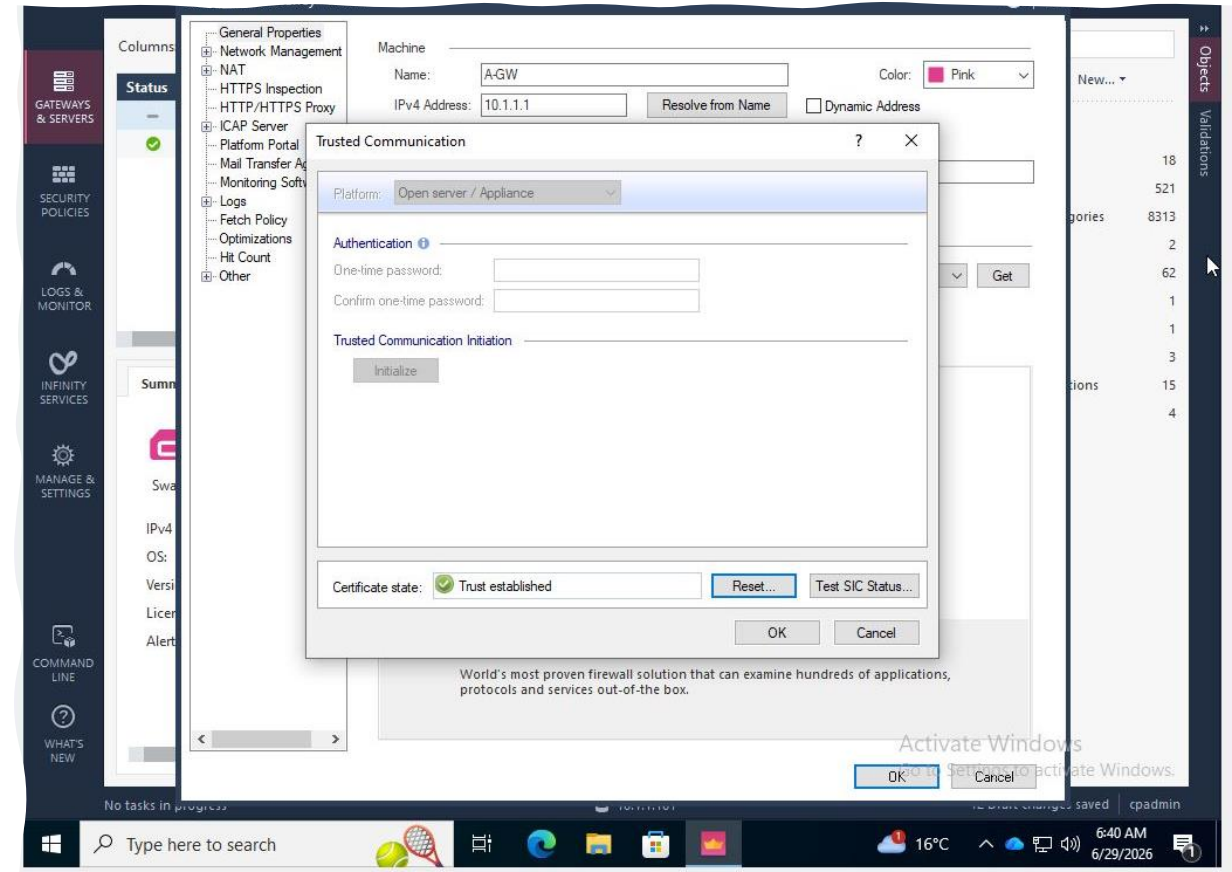
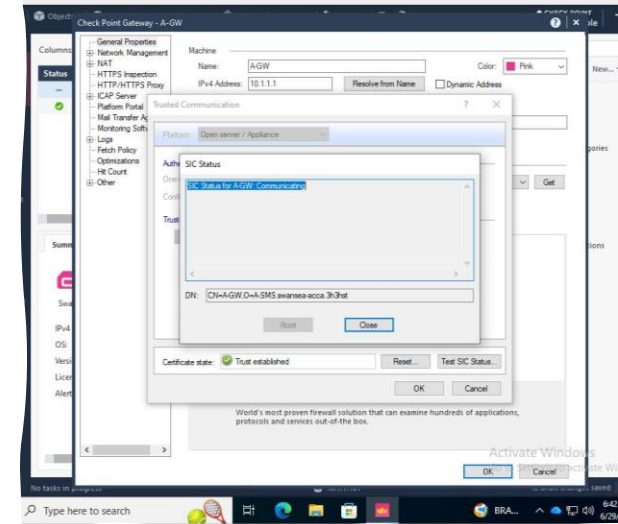
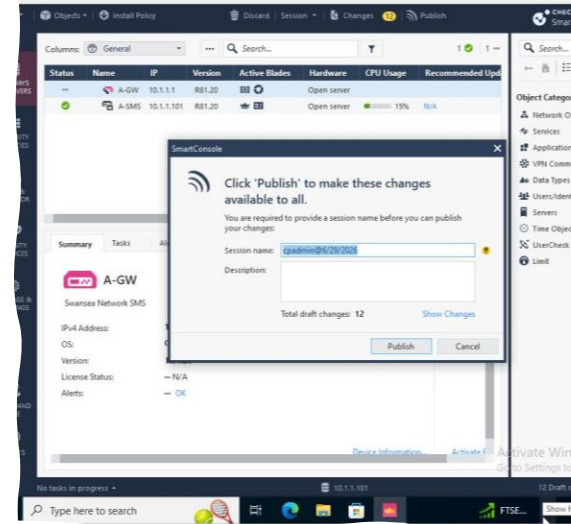
The main panel shows the configuration for the A-GW blade, including its name (Swansea Network SMS), IP address (10.1.1.1), OS (Gaia), and version (R81.20). The 'Open server' button is visible. On the right, the 'General Properties' tab is active, showing the machine name (A-GW), IP address (10.1.1.1), and various security settings. The 'Network Security (2)' tab is selected, showing the 'Access Control' section with 'Firewall' and 'IPSec VPN' options. The 'Advanced Networking' section includes 'Dynamic Routing' and 'SecureXL'. The 'Infinity Services' section includes 'IoT Protect' and 'SD-WAN'. The 'Content Awareness' section is also visible, stating: 'Content Awareness software blade provides data visibility and enforcement in unified access policy.'

Software Blade Optimizations & Global Dashboard Auditing

- **Core Blade Activation:** Checking individual feature items to activate Firewall and Monitoring services.
- **Unified Monitoring Map:** Central view tracking management engine A-SMS alongside firewall gateway asset A-GW.
- **Health Status Assurance:** Overall system indicators report clear "OK" health marks across components.

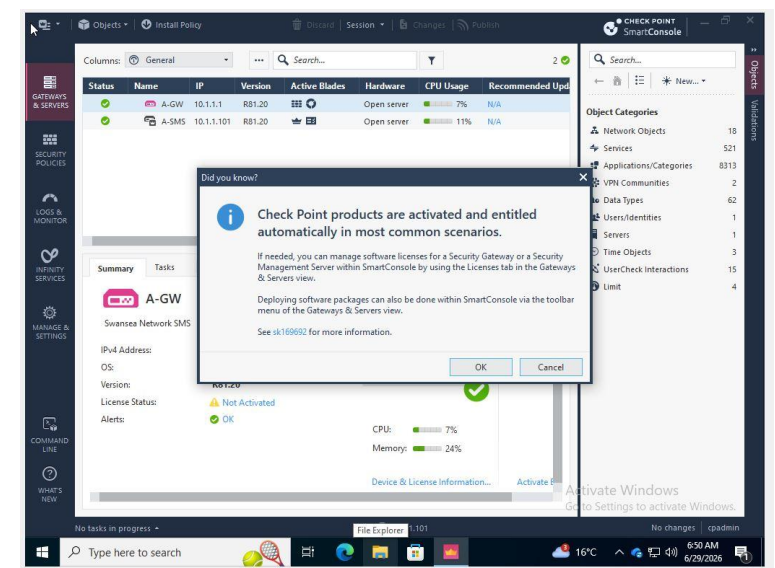
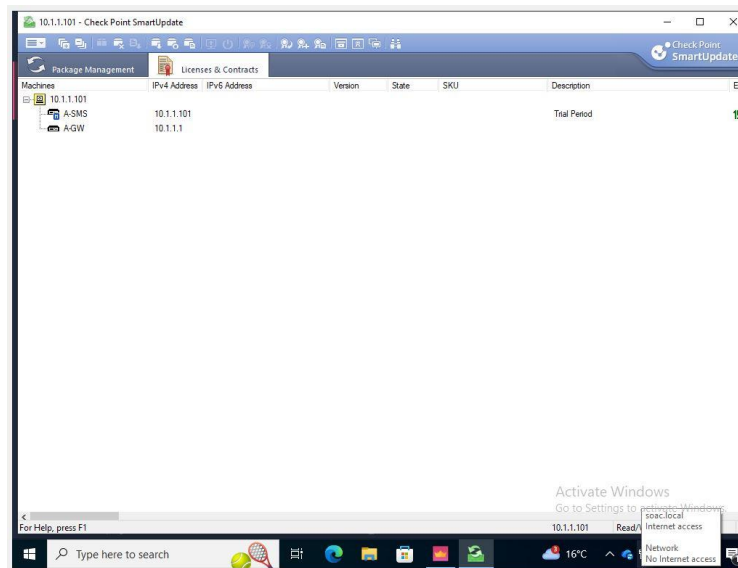
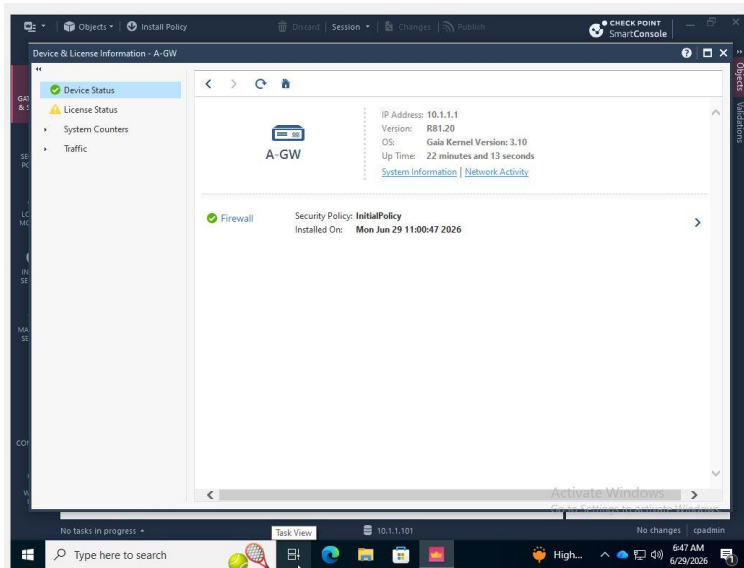
Advanced Operational Certificate State Verifications

- **Visual Status Assurance:** Green confirmation mark checks confirm a valid operational state.
- **Target Output Text:** Test window confirms clear communication paths:
"SIC Status for A-GW: Communicating".
- **Session Management Commit:** Pushing 12 pending infrastructure changes to the primary system database repository location via session publishing controls.



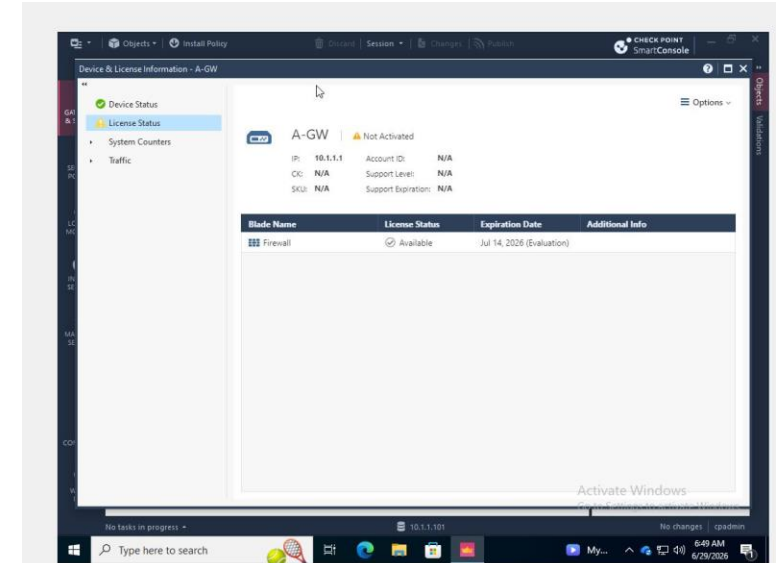
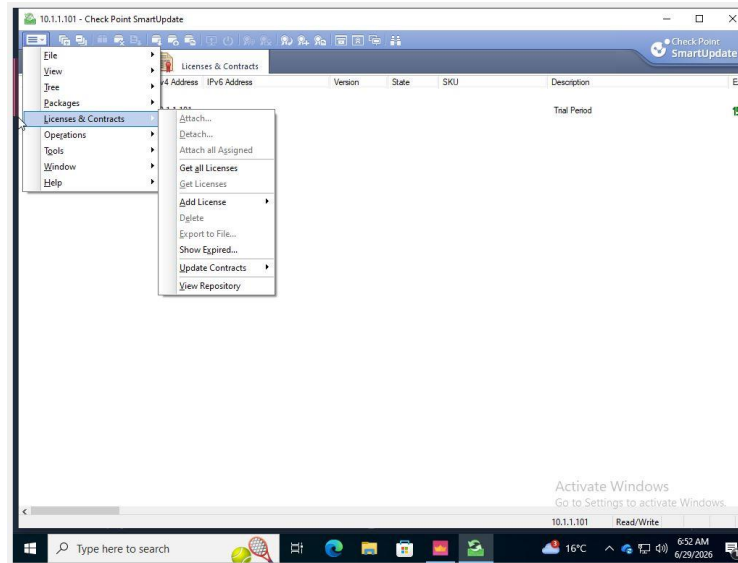
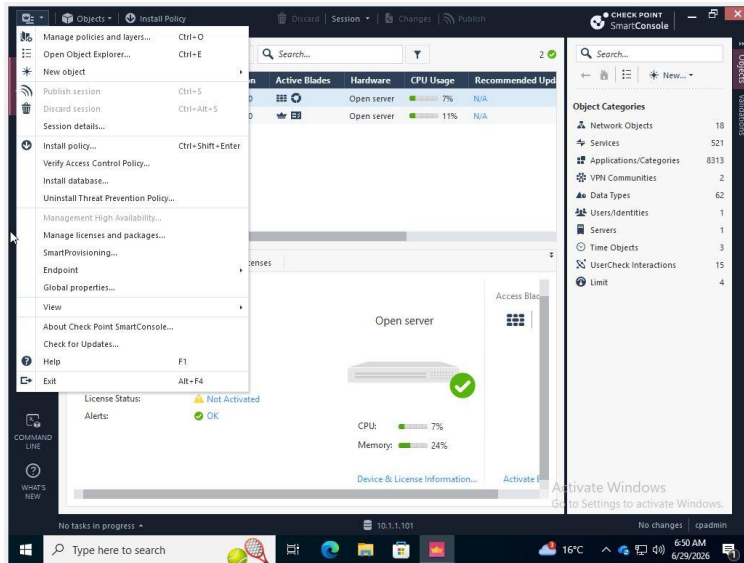
Base Firewall Rule Tables & Audit Log Engines

- **Implicit Catch-All Rule:** Evaluating the system-defined "Cleanup rule" configured to catch unmatched traffic.
- **Default Action Profile:** Set to drop traffic explicitly, ensuring a secure default perimeter posture.
- **Auditing Dashboard Access:** Launching monitor interfaces to track configuration changes for total administrative accountability.

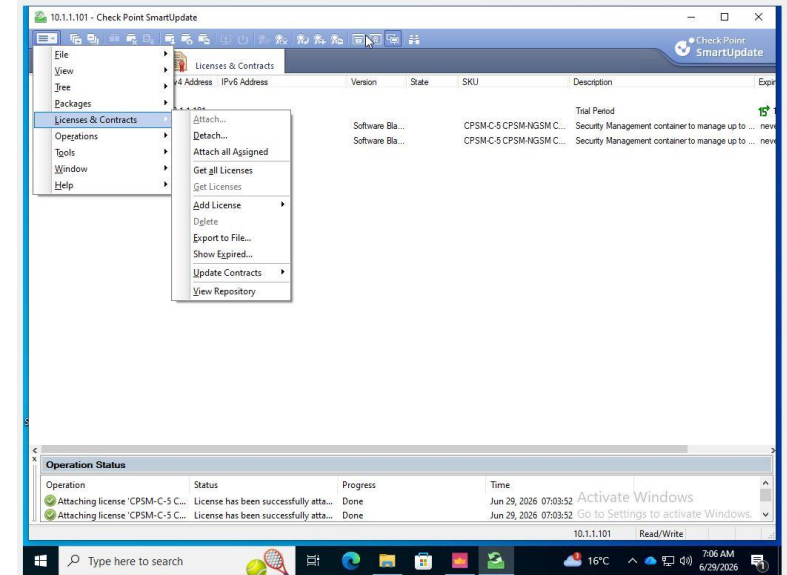
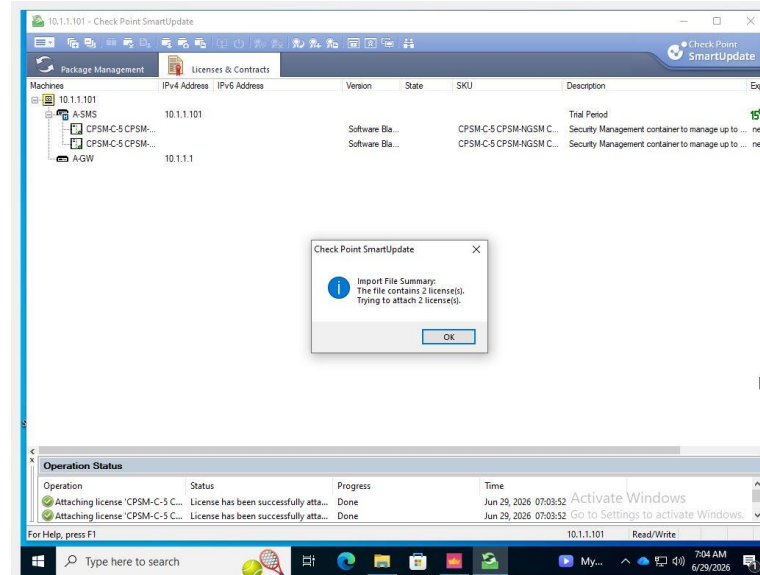
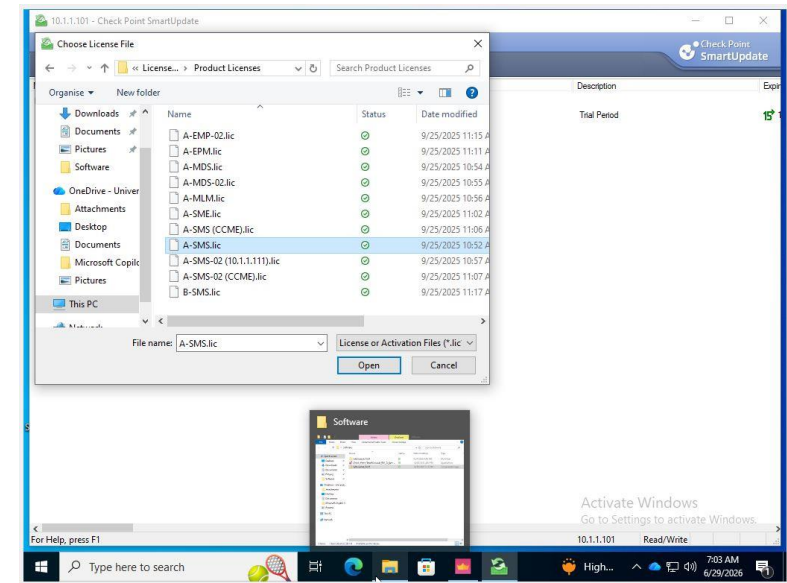
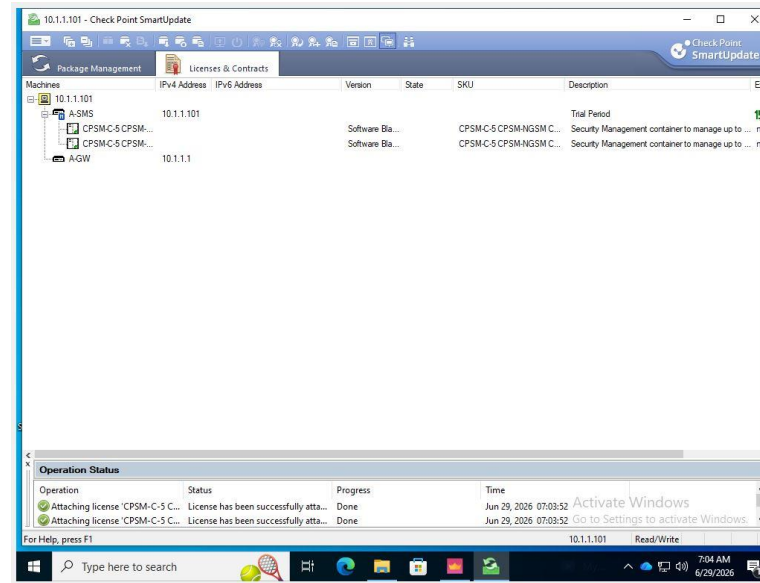


Administrative Identity Matrix (RBAC) & Command-Line Attestations

- **Identity Separation:** Creating a separate super-user account under personal name records (Hriday Majumder).
- **Principle of Least Privilege:** Testing system access limits by logging in under read-only auditor profiles ("No changes | Read Only | auditor").
- **Terminal Diagnostics Command:** Remotely accessing the core engine terminal interface over PuTTY SSH to run standard check commands (cplic print -x).



Administrative Identity Matrix (RBAC) & Command-Line Attestations



Thank You All