

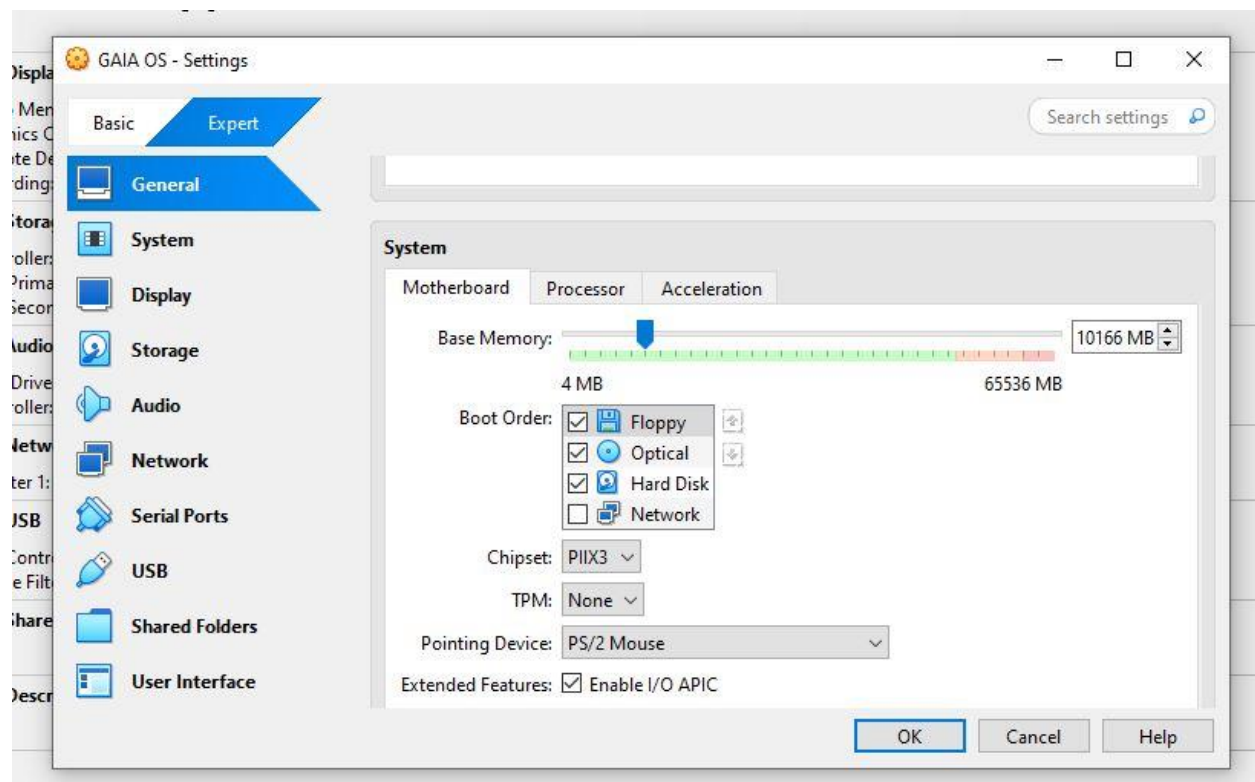
LAB EVIDENCE PORTFOLIO: DISTRIBUTED NEXT-GENERATION FIREWALL (NGFW)

Module Name: Enterprise Network Security

Platform Configuration: Check Point Gaia R81.20 Distributed Deployment on Oracle VM VirtualBox

Phase 1: Host Virtualization & Operating System Base Layer

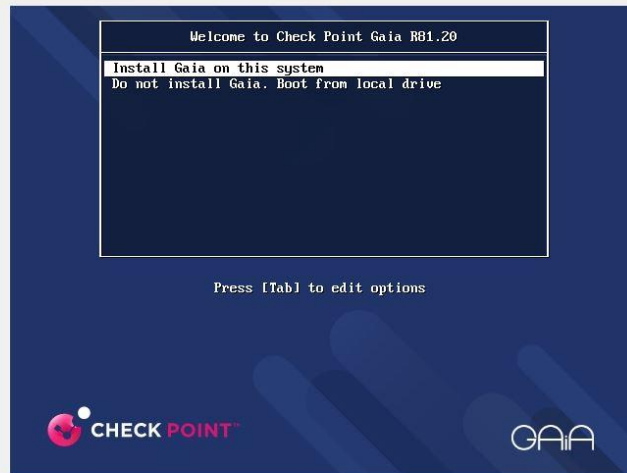
Figure 1: Virtual Hypervisor Motherboard Configuration



- **Description:** Configuration of the baseline Oracle VM VirtualBox virtual hardware container labeled GAIA OS. It documents the hardware resource allocation of 10,166 MB (~10 GB) of system memory, standard ACPI

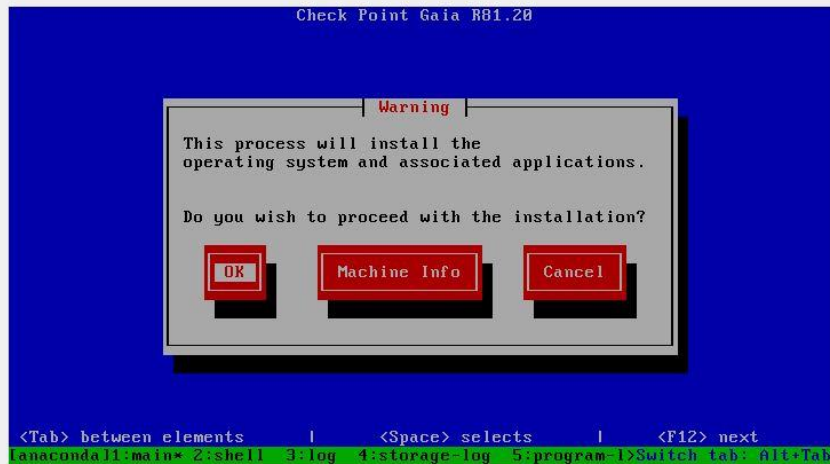
configurations, and a deterministic system boot order layout targeting optical installation media first.

Figure 2: Check Point Gaia Interactive Installation Loader



- **Description:** Initial system boot menu execution of the Check Point Gaia R81.20 installation media (Check_Point_R81.20_T631.iso). The interactive selector is locked to Install Gaia on this system to initiate text-mode deployment variables.

Figure 3: Hard Drive Initialization Volume Warning



- **Description:** Low-level system storage partition audit prompt. The installation script halts to request explicit confirmation to wipe, format, and structure all local logical hard disk volumes within the VirtualBox virtual machine file container.

Figure 4: Localization and Keyboard Layout Profile



- **Description:** Keyboard mapping configuration screen within the text-mode installation menu. The profile parameters are locked to the Great Britain physical layout table to align system input rules.

Figure 5: Root Administrative Account Credential Assignment



- **Description:** Secure Account Configuration console workspace where the credentials for the master operating system administrator user account (admin) are set and verified before compilation.

Figure 6: Emergency Maintenance Mode Authentication



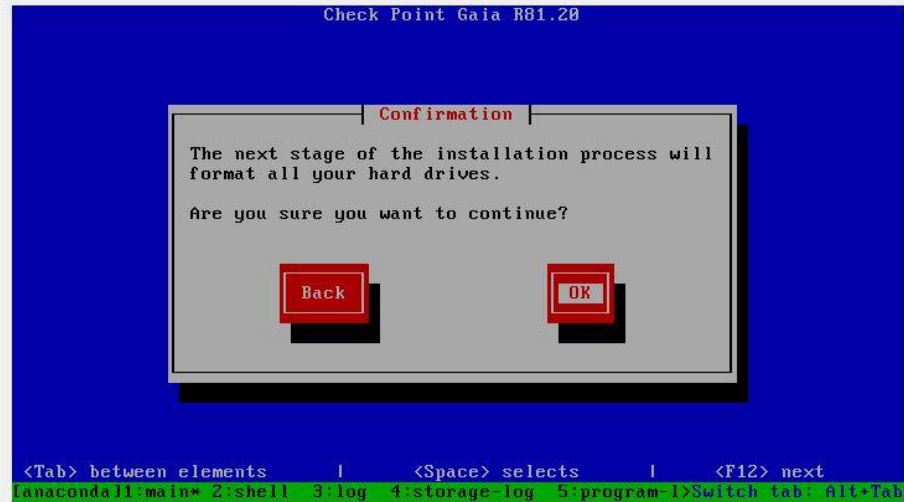
- **Description:** Configuration menu for setting an independent system Maintenance password. This creates a dedicated recovery credential for the admin account to protect advanced single-user shell operations and low-level troubleshooting.

Figure 7: Management Network Interface Parameter Assignment



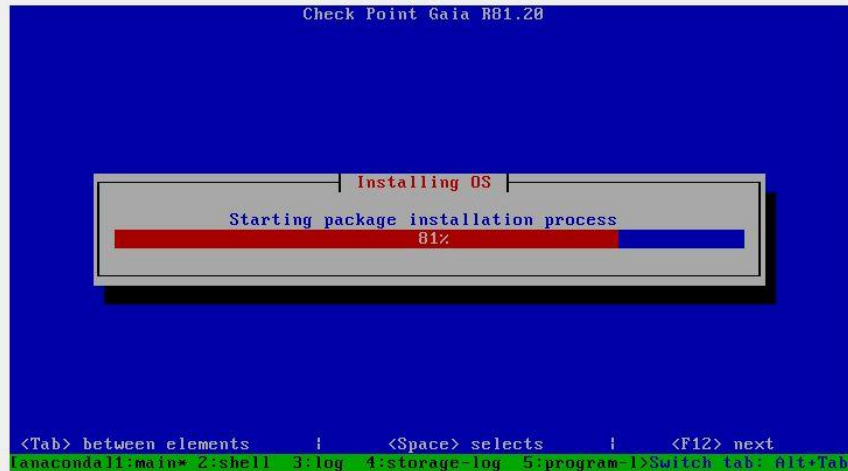
- **Description:** Hardware configuration for the primary management connection plane (eth0). The interface parameters are manually assigned static values: IPv4 Address 10.1.1.101, Subnet Mask 255.255.255.0 (/24), and Default Gateway 10.1.1.1.

Figure 8: Package Target Drive Modification Summary



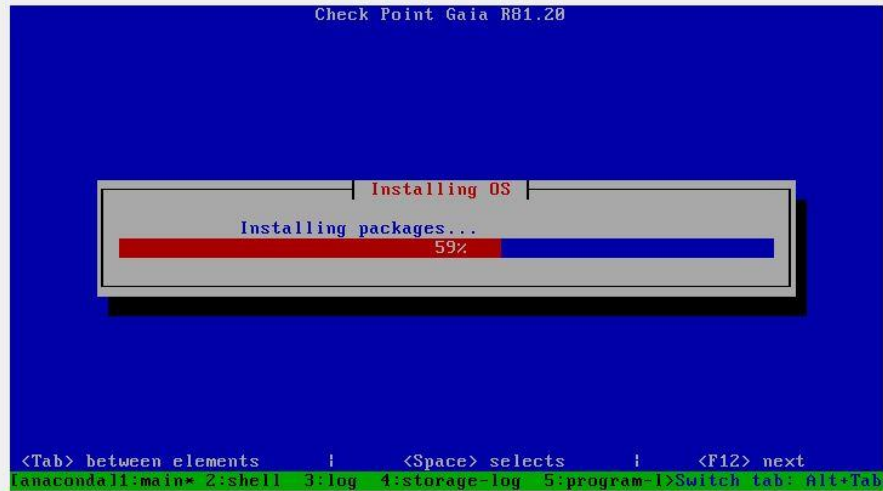
- **Description:** Final confirmation summary window detailing the allocation of logical hard disk partitions for the system root and backup logs directory layers before execution.

Figure 9: Installation Progress Phase — Package Extraction



- **Description:** Live execution tracker indicating an active extraction state of 81% as the Gaia operating system extracts base binary images to the local hard drive storage pool.

Figure 10: Installation Progress Phase — Core Package Setup



- **Description:** Live application progress tracker sitting at 59% during the deployment phase, copying security dependencies and building internal database files.

Figure 11: Base Operating System Installation Completion

```
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.

anacondall:main* 2:shell 3:log 4:storage-log 5:program-1>Switch tab: Alt+Tab
```

- **Description:** Text-mode confirmation window displaying Installation complete. Press return to quit. It prompts the removal of the optical drive ISO image to allow the platform to reboot cleanly into its active operating system kernel.

Figure 12: Interactive Console Post-Install Initialization



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

- **Description:** Black command-line interface terminal login banner displaying the system authorization warning: This system is for authorized use only. login:.. This indicates a successful kernel boot state.

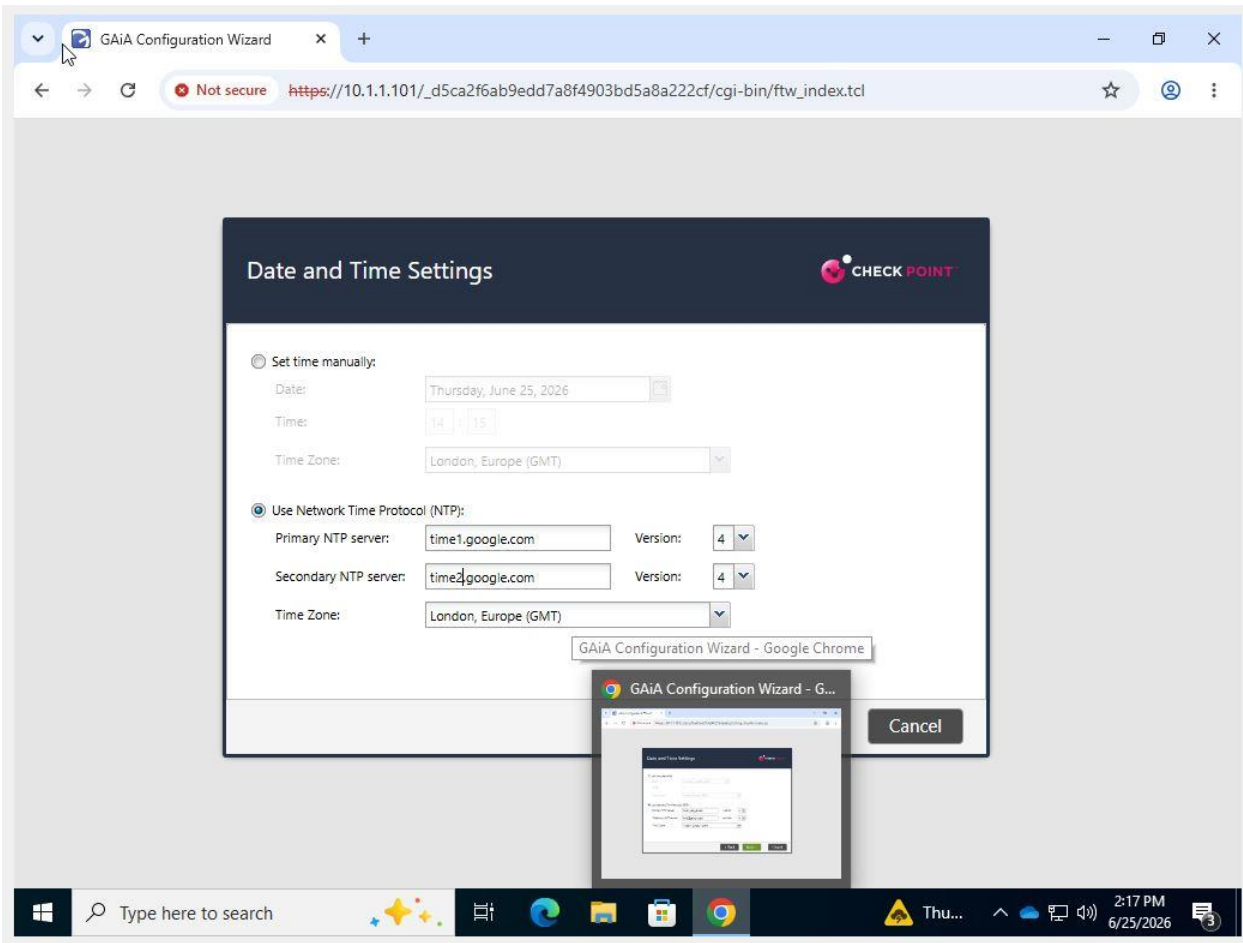
Figure 13: Clish Shell Hardening & Timeout Modification

```
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> _
```

- **Description:**
- Active interactive command-line session on device node gw-180e66 logged in as user admin. The default connection timeout boundaries are extended via clish scripts (set inactivity-timeout 720 and set web session-timeout 720) and written to the configuration database using the save config command.

Phase 2: WebUI First-Time Configuration Wizards

Figure 14: Browser Configuration Portal Entry



- **Description:** Initial deployment screen of the browser-based Check Point Gaia Configuration Wizard accessed via a secure HTTPS browser connection targeting management IP address <https://10.1.1.101>.

Figure 15: Device Node Host and Domain Identification

GAiA Configuration Wizard

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

Device Information

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

- **Description:** Network Identification tab where the standalone management server identity parameters are locked: Host Name set to A-SMS and Domain suffix configured as swansea-acca.

Figure 16: Central Domain Name Service (DNS) Mapping

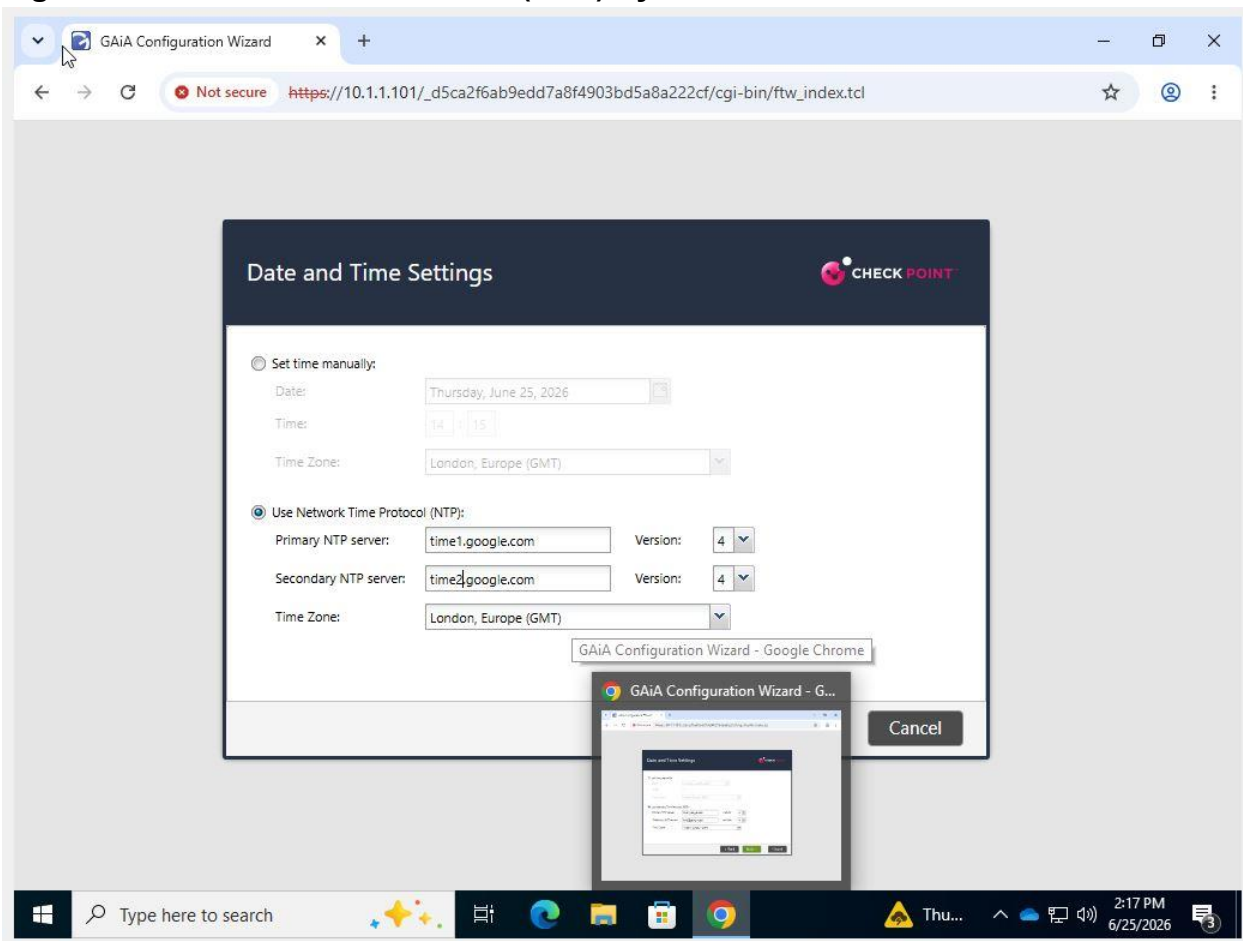
The screenshot shows a web browser window with the title "GAiA Configuration Wizard". The address bar displays a "Not secure" warning and the URL "https://10.1.1.101/_d5ca2f6ab9edd7a8f4903bd5a8a222cf/cgi-bin/ftw_index.tcl". The main content area displays a "Device Information" form with the Check Point logo in the top right corner. The form contains the following fields:

- 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

Below these fields is a section titled "Proxy Settings" with a sub-section "Use a Proxy server". This section includes an "Address:" field and a "Port:" field set to "8080". At the bottom of the form are three buttons: "< Back", "Next >" (highlighted in green), and "Cancel". The Windows taskbar at the bottom shows the Microsoft Edge browser icon, a search bar, and the system clock indicating 2:15 PM on 6/25/2026.

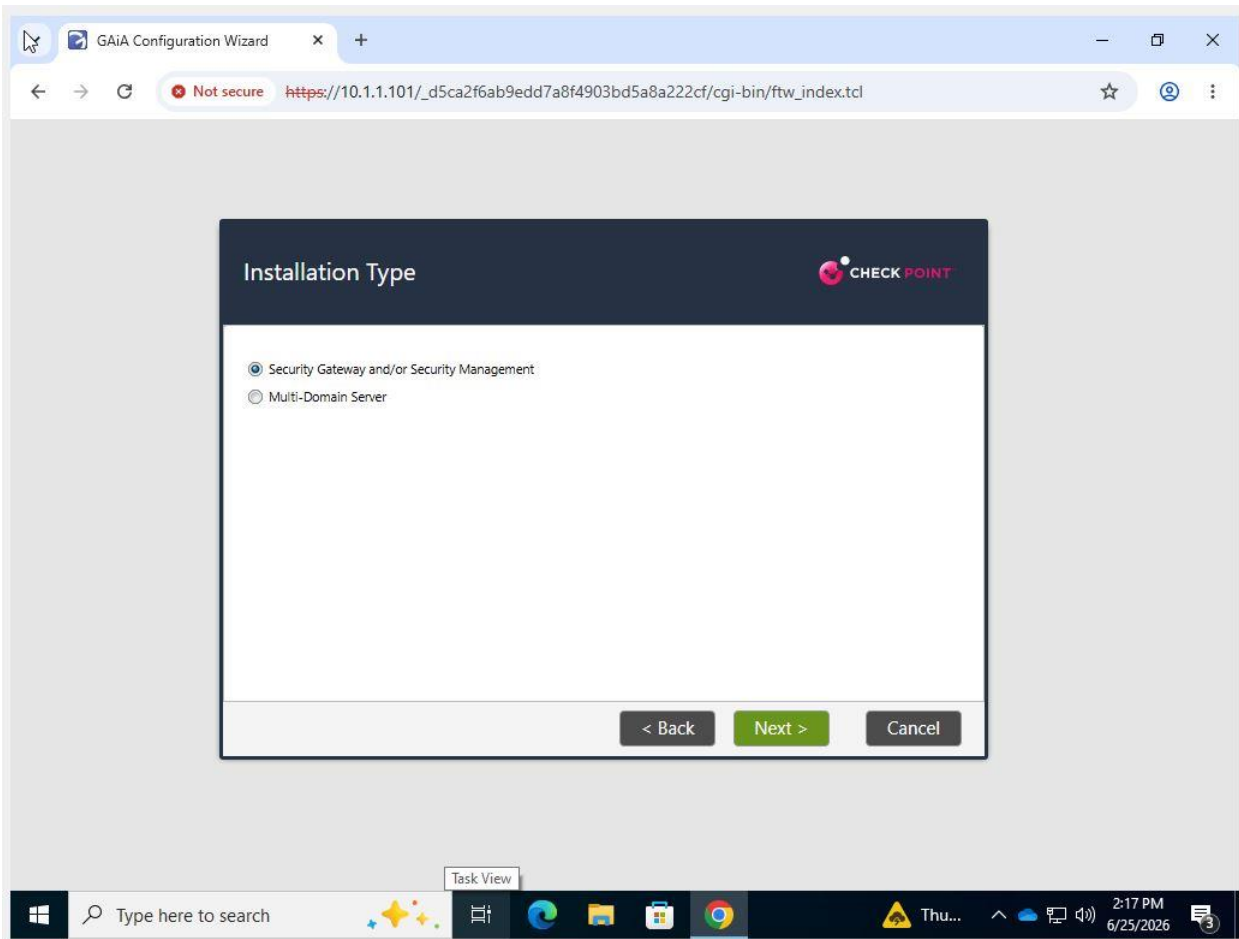
- **Description:** IP allocation matrix assigning static network name resolution endpoints to the appliance, utilizing primary engine destination 192.168.1.1, secondary target 8.8.8.8, and tertiary target 4.2.2.2.

Figure 17: Network Time Protocol (NTP) Synchronisation Plane



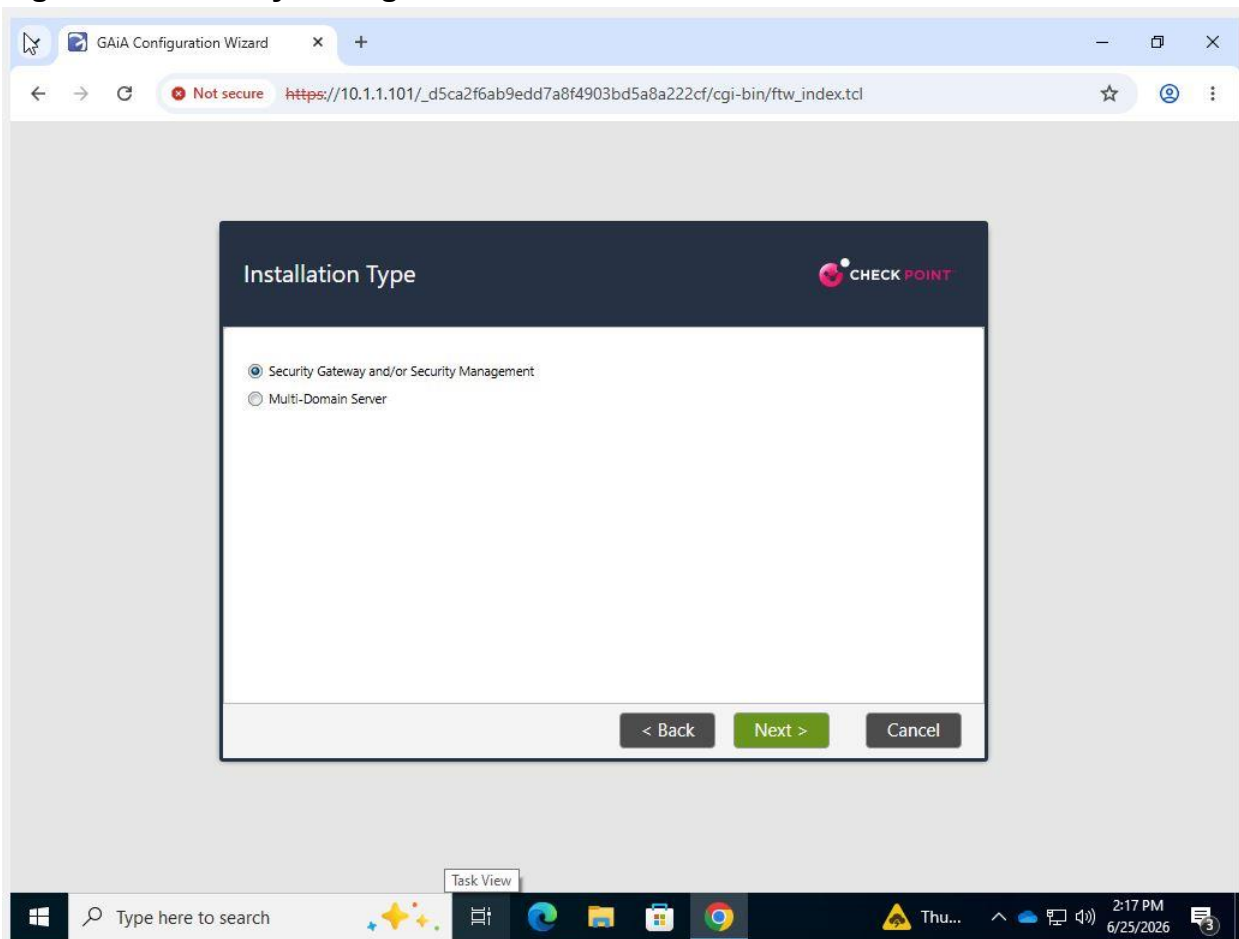
- **Description:** Time and Date configuration screen linking client services to upstream public servers ://google.com and ://google.com (NTP Version 4). The system localization profile is locked to the London, Europe (GMT) time zone to align logging clocks.

Figure 18: System Functional Role Specialization Profile



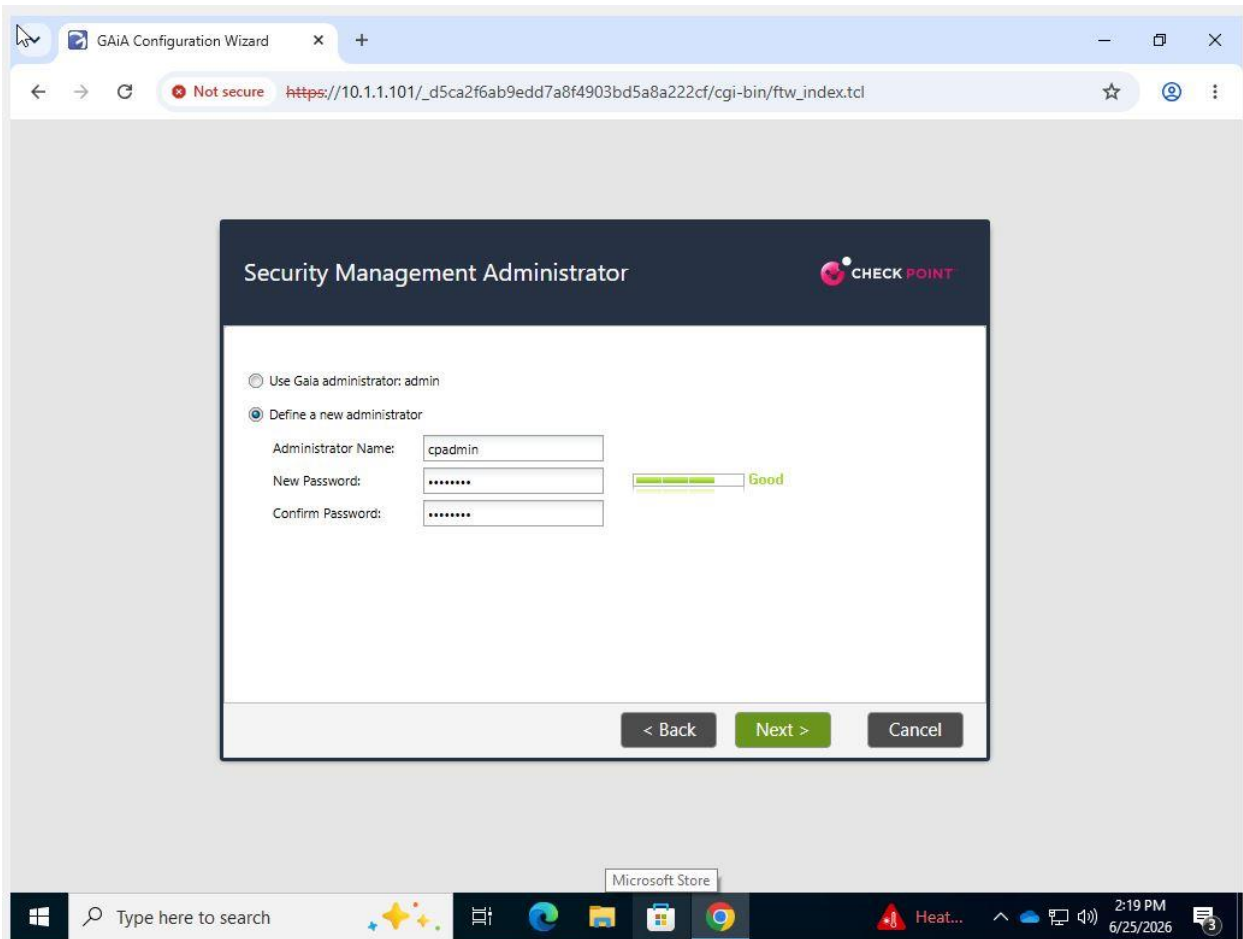
- **Description:** Strategic allocation window where the primary operational boundaries are split. The checkbox is assigned to Security Management (Standalone Server configuration) while the gateway engine is disabled for this node.

Figure 19: Security Management Administrator Definition



- **Description:** Application database configuration window where a dedicated security platform supervisor profile is built under account username `cpadmin` to separate application policy access from the base OS login root.

Figure 20: Graphical User Interface (GUI) Access Constraints



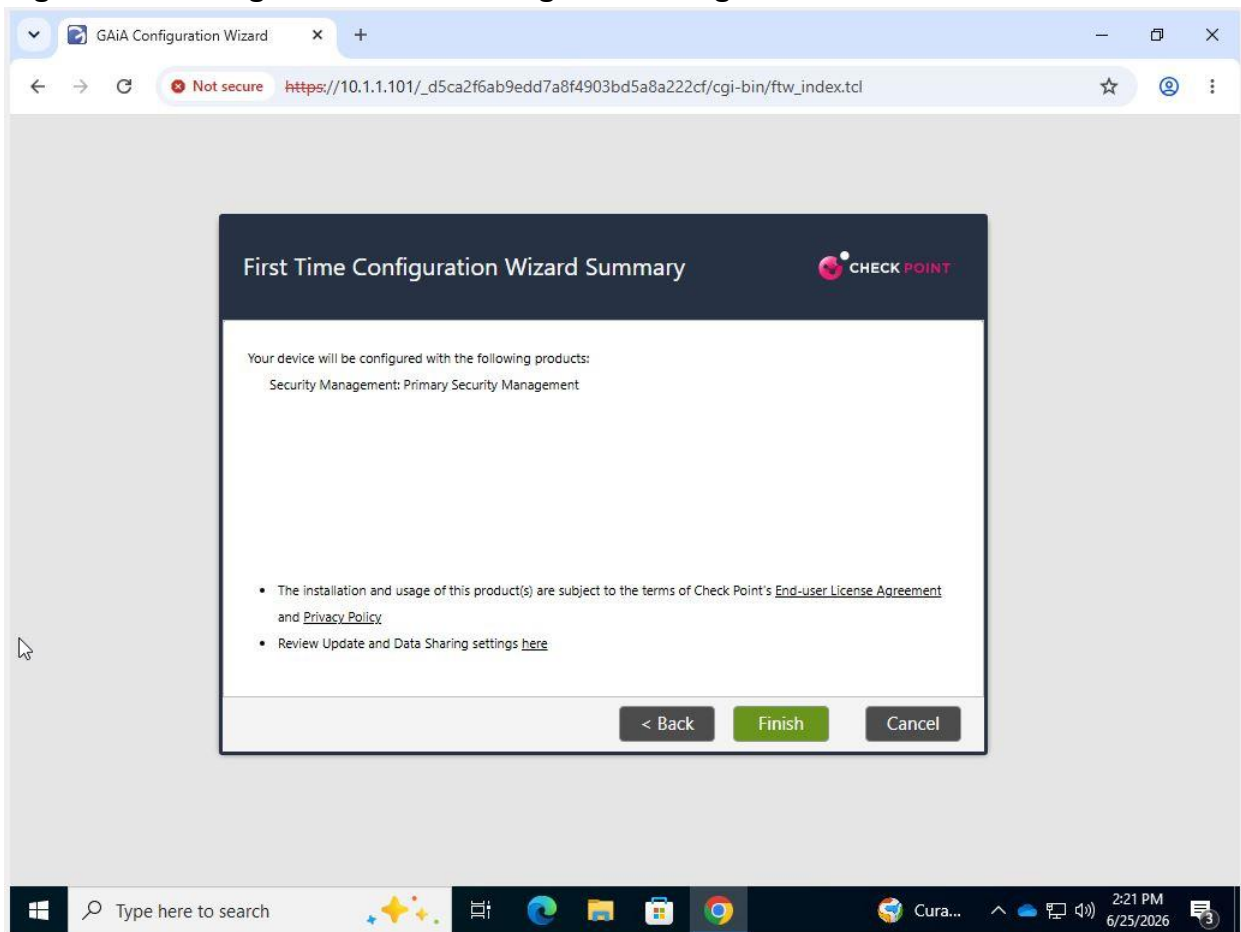
- **Description:** Network validation interface restricting SmartConsole graphical connections. Access permissions are locked to the specific network range 10.1.1.0/24 to prevent arbitrary hosts from attempting authentication methods.

Figure 21: Configuration Wizard Summary Ledger

The screenshot shows a web browser window with the title "GAIa Configuration Wizard". The address bar displays a "Not secure" warning and the URL "https://10.1.1.101/_d5ca2f6ab9edd7a8f4903bd5a8a222cf/cgi-bin/ftw_index.tcl". The main content area features a "Security Management GUI Clients" dialog box with the Check Point logo in the top right corner. The dialog box contains the text "GUI clients can log into the Security Management from:" followed by four radio button options: "Any IP Address", "This machine", "Network", and "Range of IPv4 addresses". The "Network" option is selected. Below this, there are input fields for "IP address:" (containing "10.1.1.201"), "IP Address:" (containing "10.1.1.0"), and "Subnet:" (containing "255.255.255.0"). At the bottom of the dialog box are three buttons: "< Back", "Next >" (highlighted in green), and "Cancel". The Windows taskbar at the bottom shows the search bar, task view button, and several application icons, including File Explorer, Edge, and Chrome. The system tray on the right indicates a temperature of 28°C and the date/time as 2:20 PM on 6/25/2026.

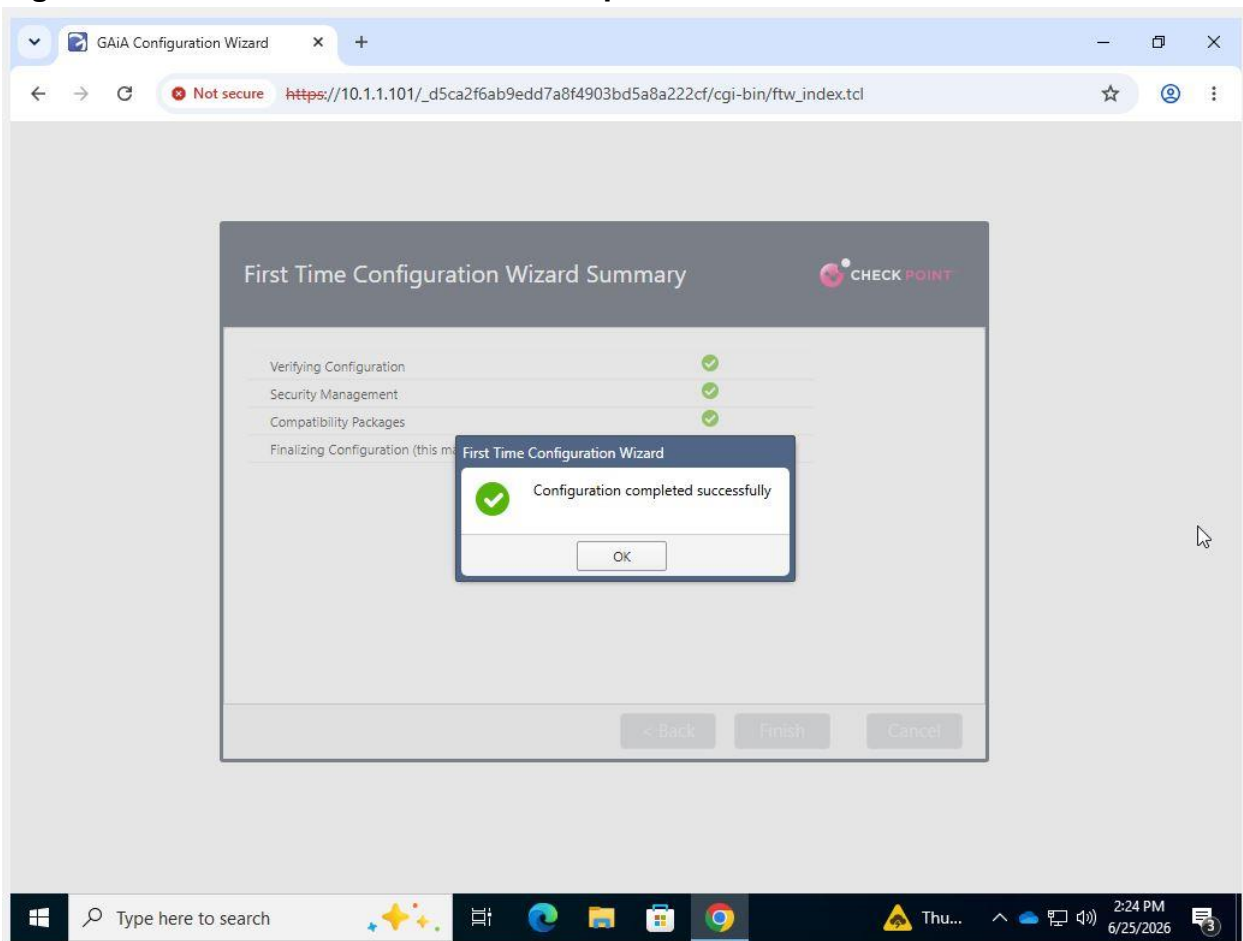
- **Description:** Staged review panel detailing all selected parameters (Security Management: Primary Security Management) before applying permanent configuration steps to the device disk.

Figure 22: Configuration Processing Plane Progress



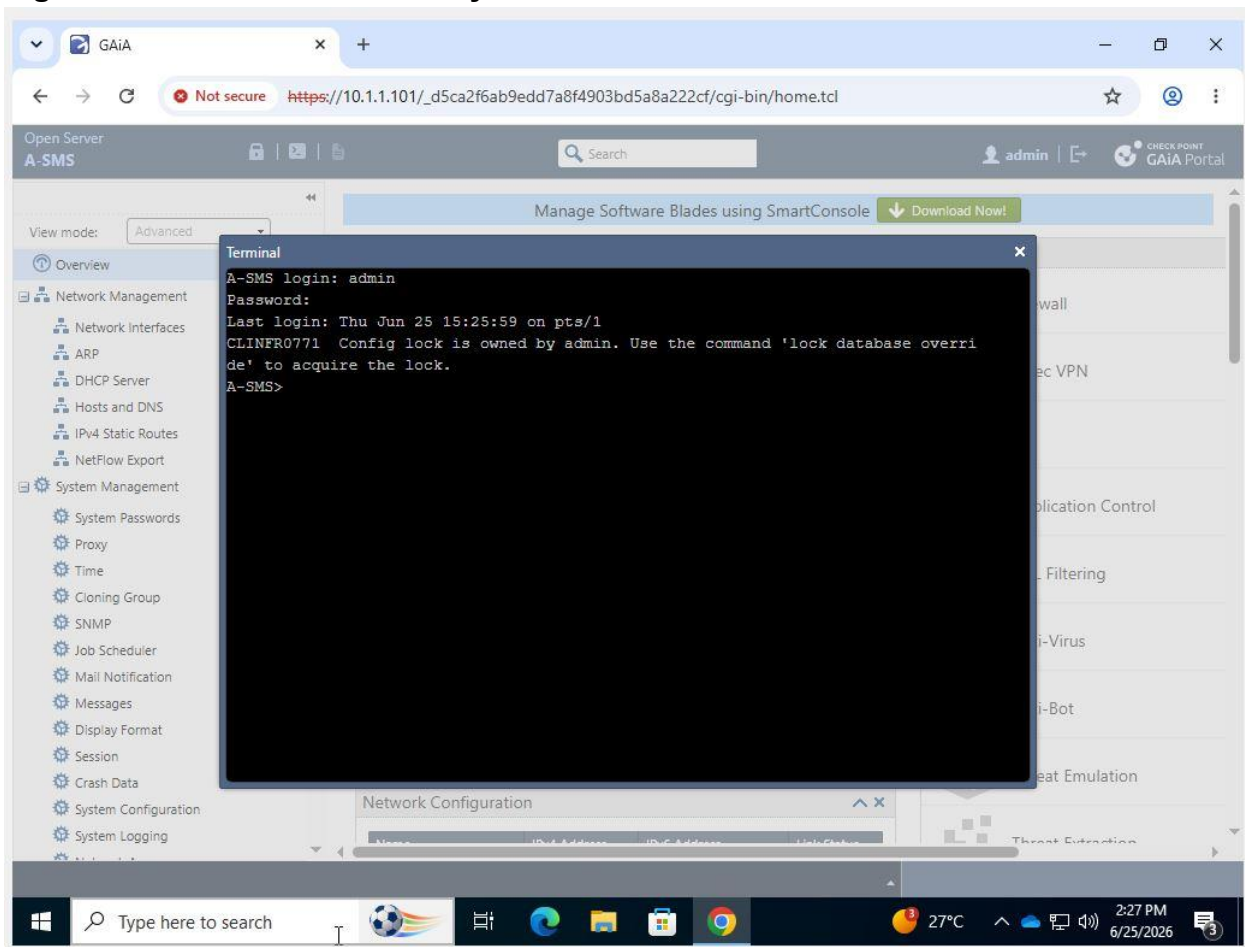
- **Description:** Active deployment window validating, building, and restarting individual core daemons and database dependencies.

Figure 23: Successful Web Wizard Completion Confirmation



- **Description:** Pop-up alert confirmation window reading Configuration completed successfully, displaying green checkmarks across all management, security compliance, and architecture parameters.

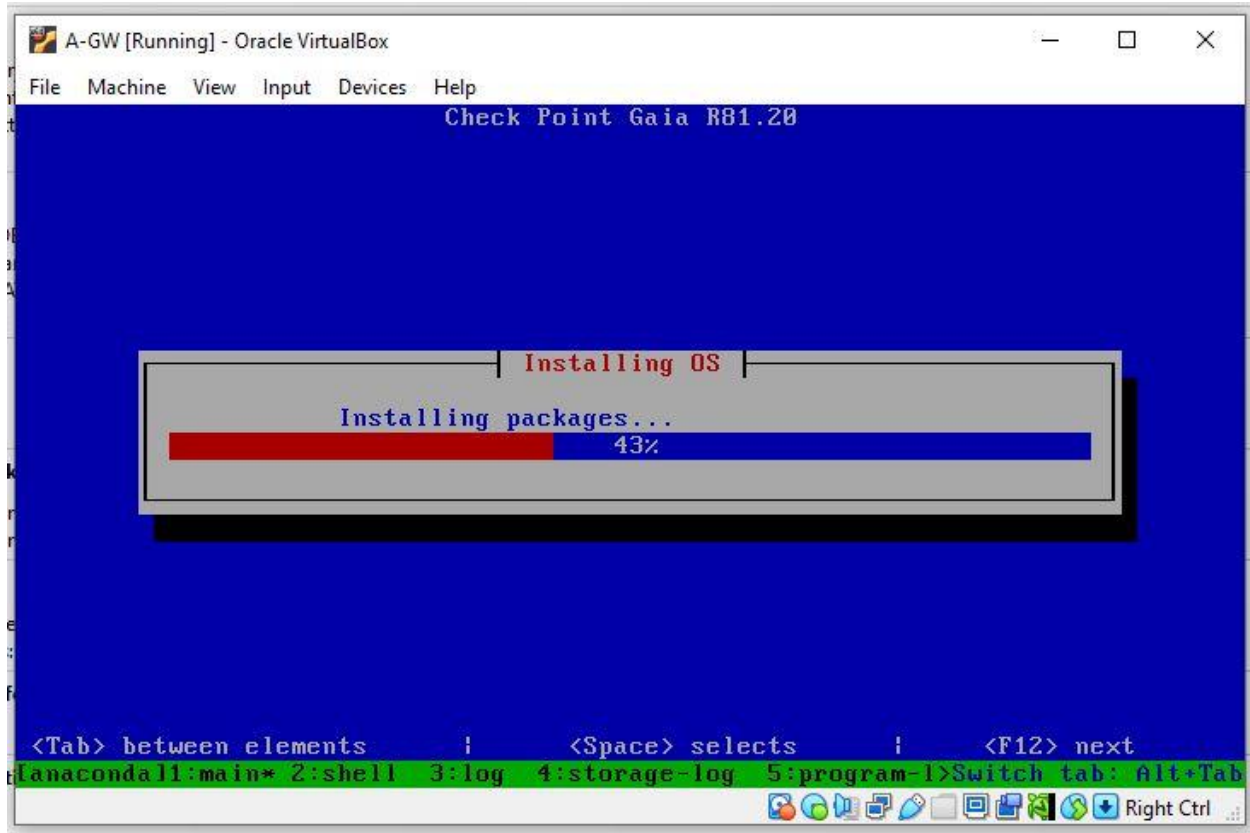
Figure 24: Active Gaia Portal System Dashboard Home



- **Description:** Web console landing interface for appliance A-SMS, verifying system uptime and status parameters, with an open integrated web terminal window running at the command line.

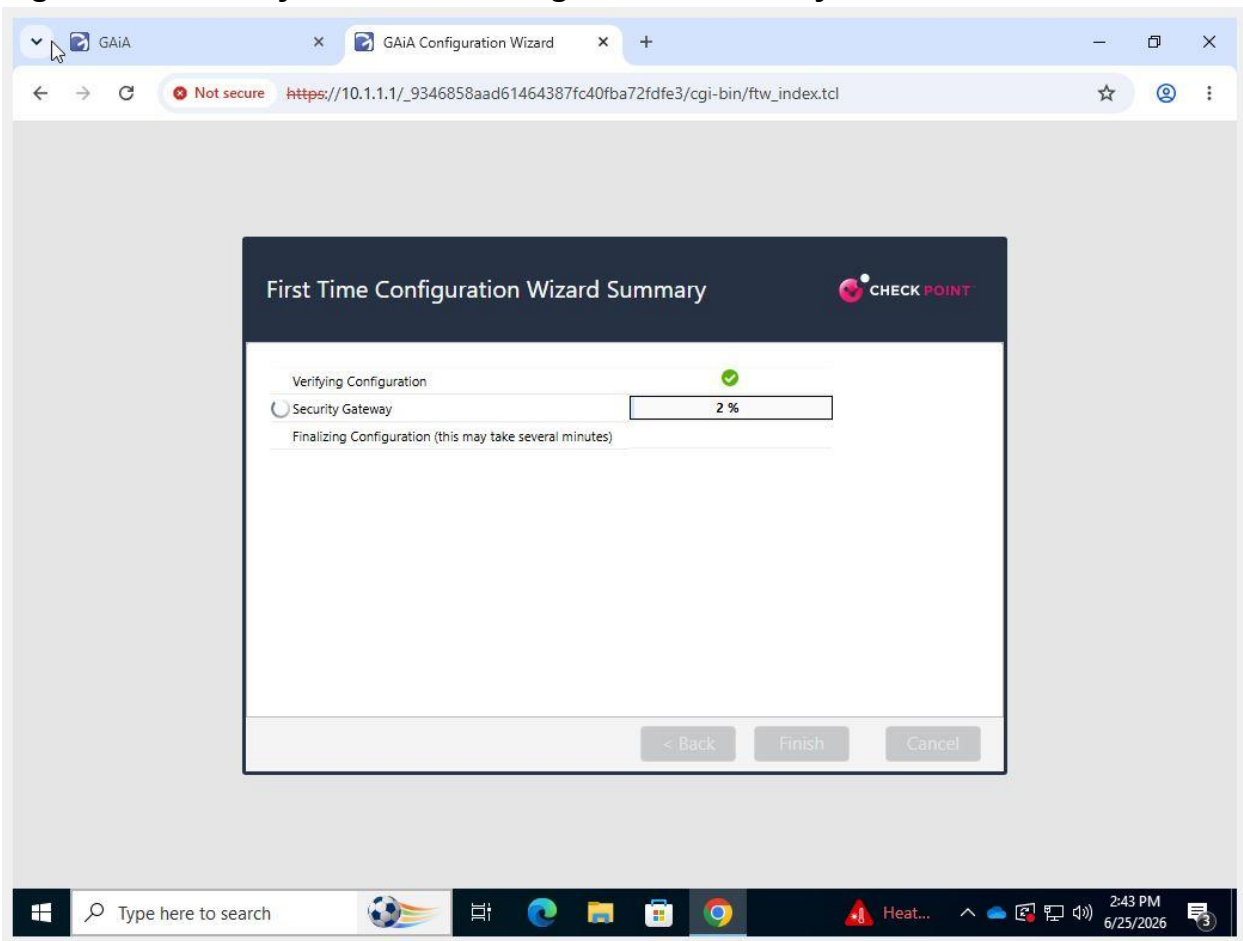
Phase 3: Security Gateway Subnet Zoning & Interfacing

Figure 25: Distributed Security Gateway Installation Progress



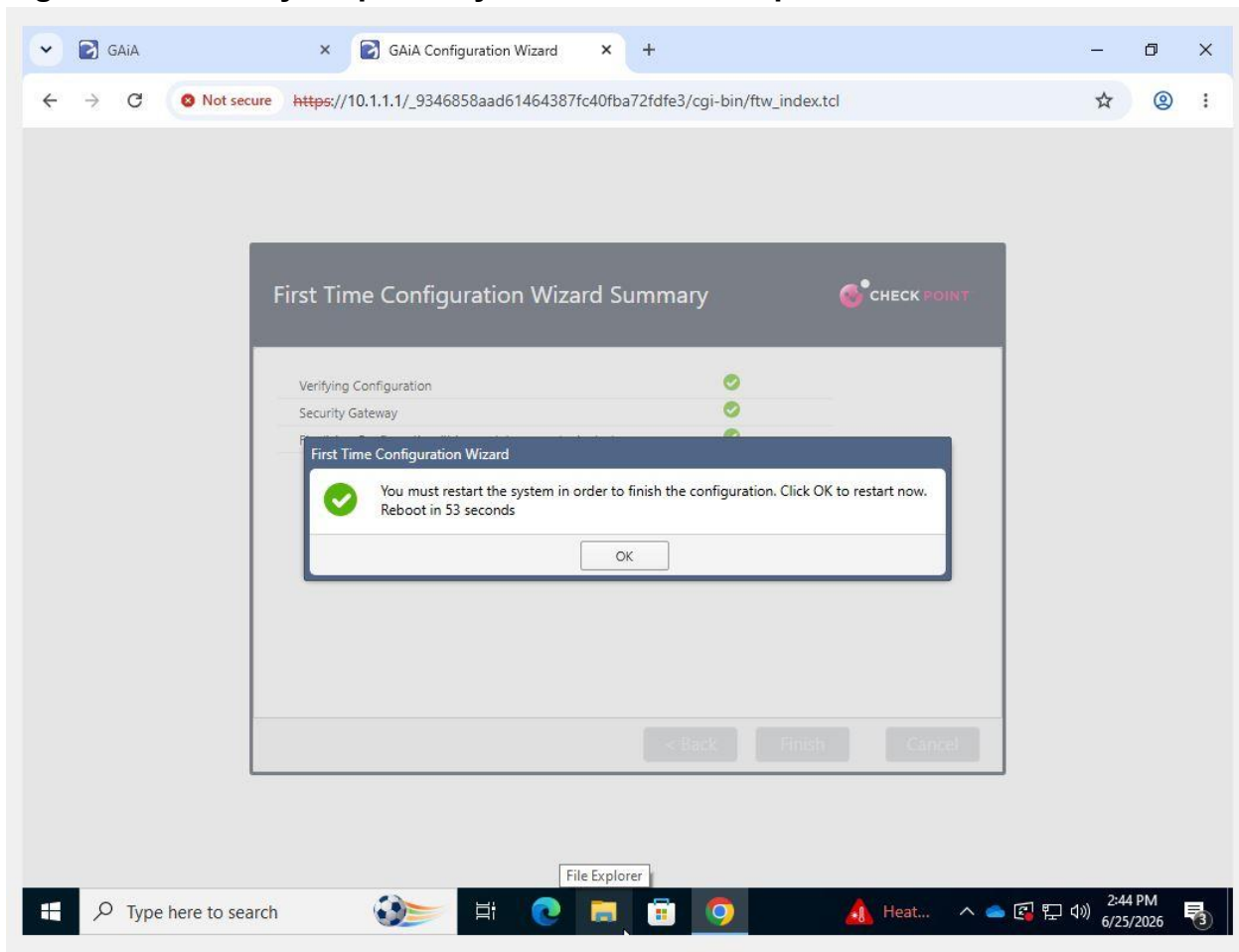
- **Description:** Terminal tracking instance showing the parallel operating system package deployment phase for the second virtual machine entity labeled A-GW [Running], currently extracting filtering packages at 43%.

Figure 26: Gateway First-Time Configuration Summary



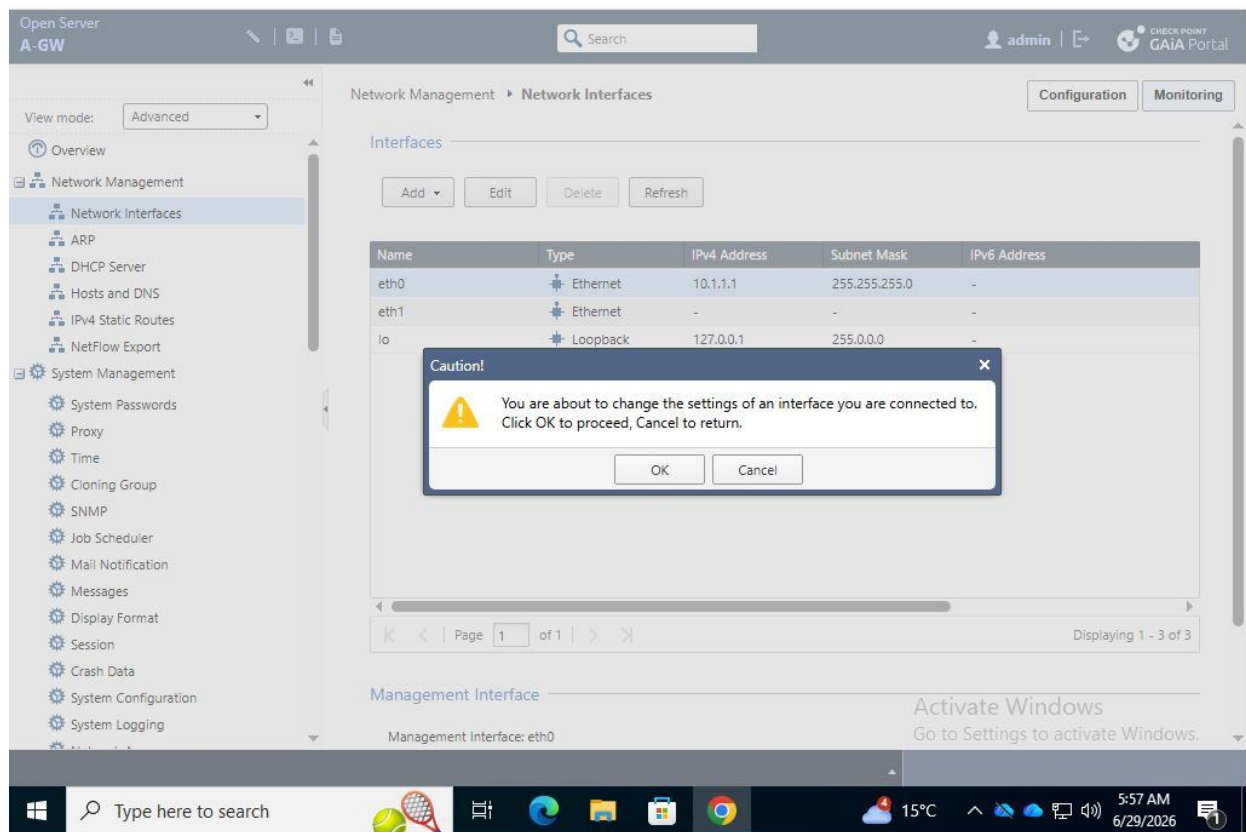
- **Description:** Summary ledger confirmation screen for the second appliance node (10.1.1.1), verifying its functional deployment identity profile as a standalone security firewall gateway plane.

Figure 27: Gateway Required System Reboot Prompt



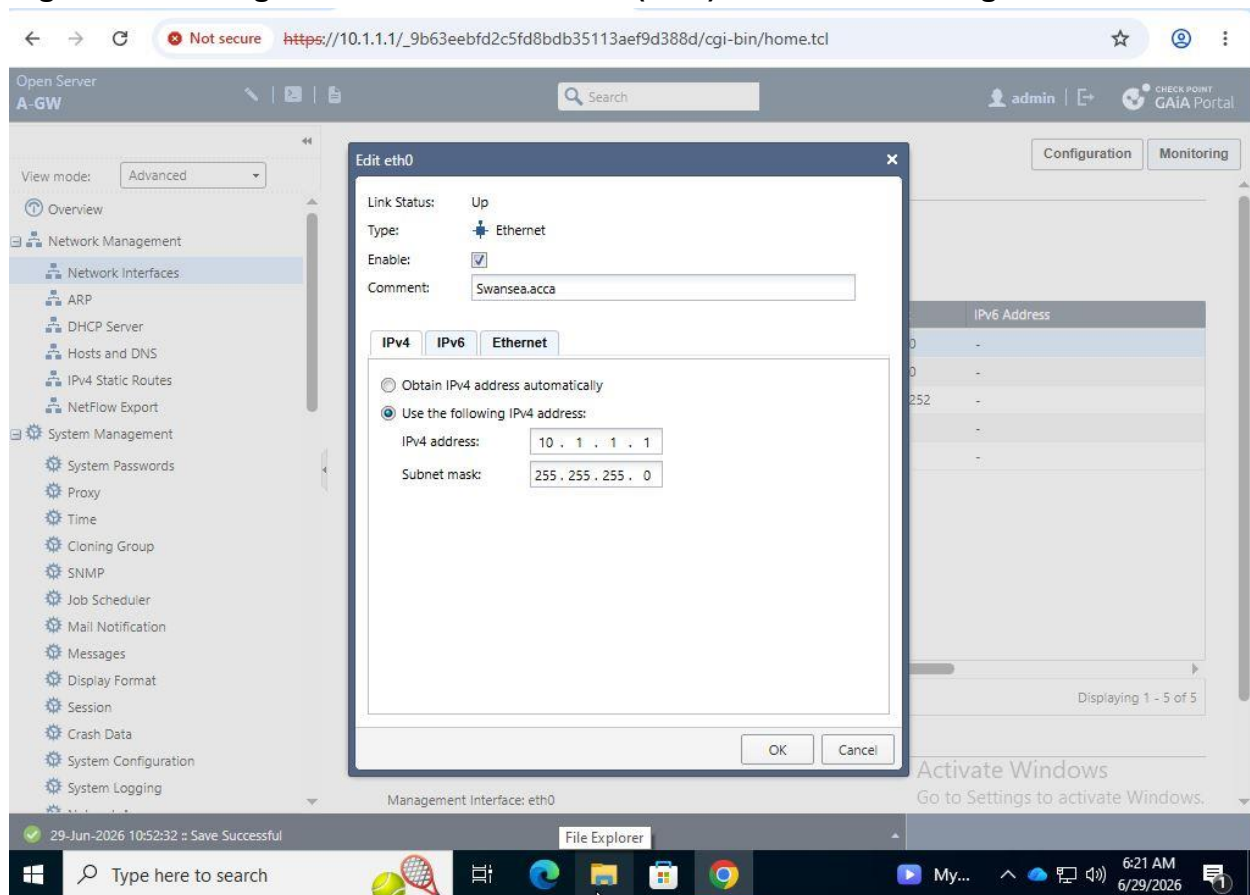
- **Description:** final web installation status block displaying a mandatory 60-second system countdown warning prompt reading: You must restart the system in order to finish the configuration.

Figure 28: Network Interfaces Configuration Control Portal



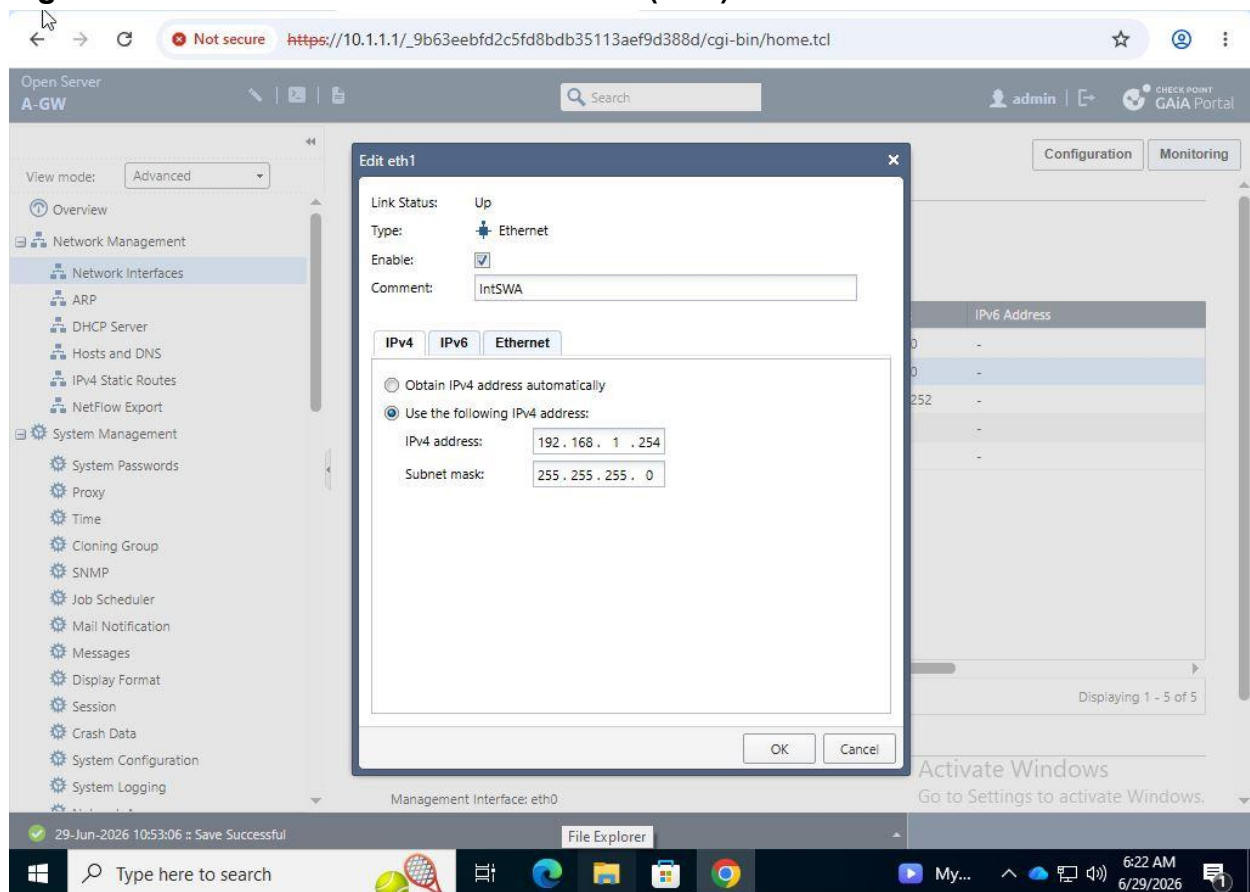
- **Description:** Subnet control grid within the Gaia Portal for device A-GW at management IP 10.1.1.1. It shows an active link alert warning before modifying the parent interface layout tables.

Figure 29: Management Subnet Interface (eth0) Parameter Tuning



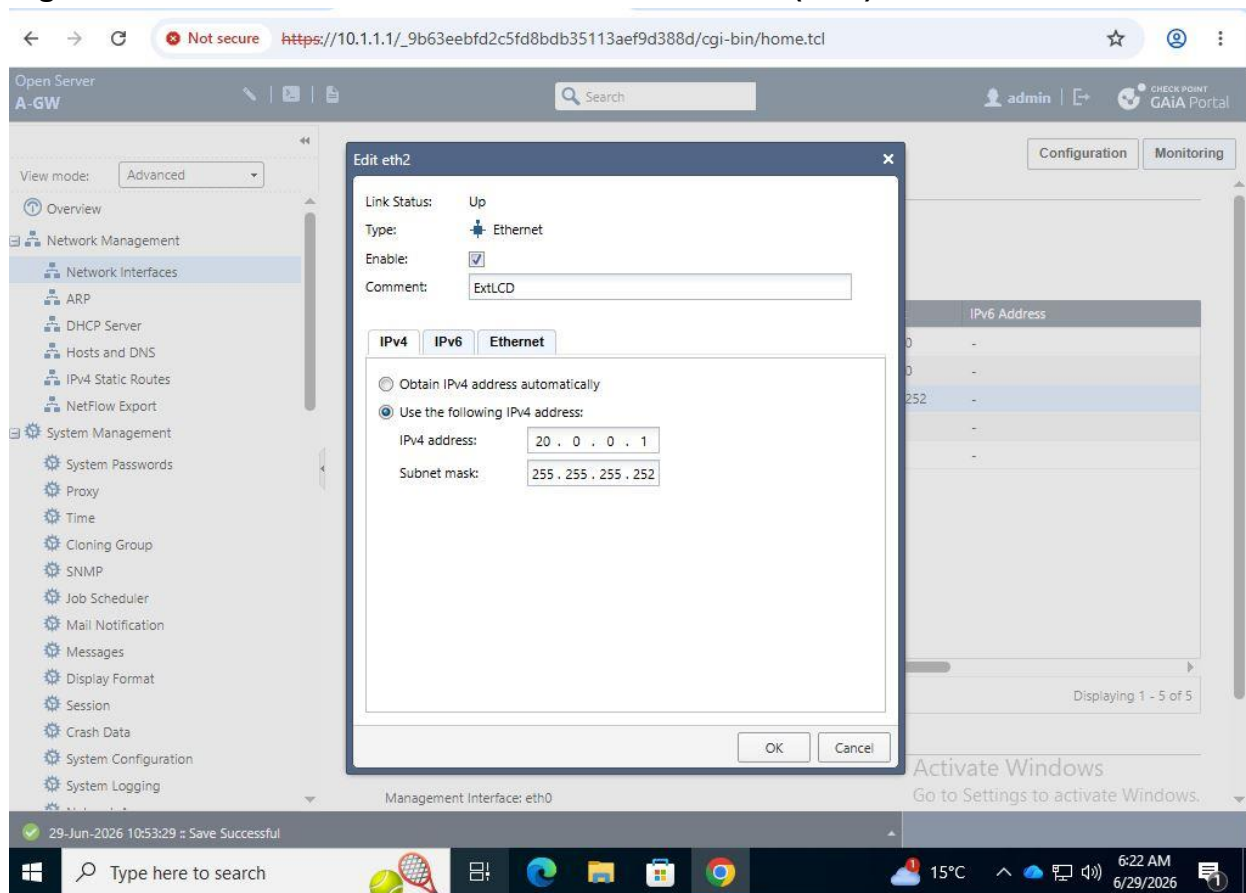
- **Description:** Interface properties window for eth0, detailing the manual binding of target management address 10.1.1.1/24 accompanied by the descriptive comment label Swansea.acca.

Figure 30: Internal Local Subnet Interface (eth1) Profile



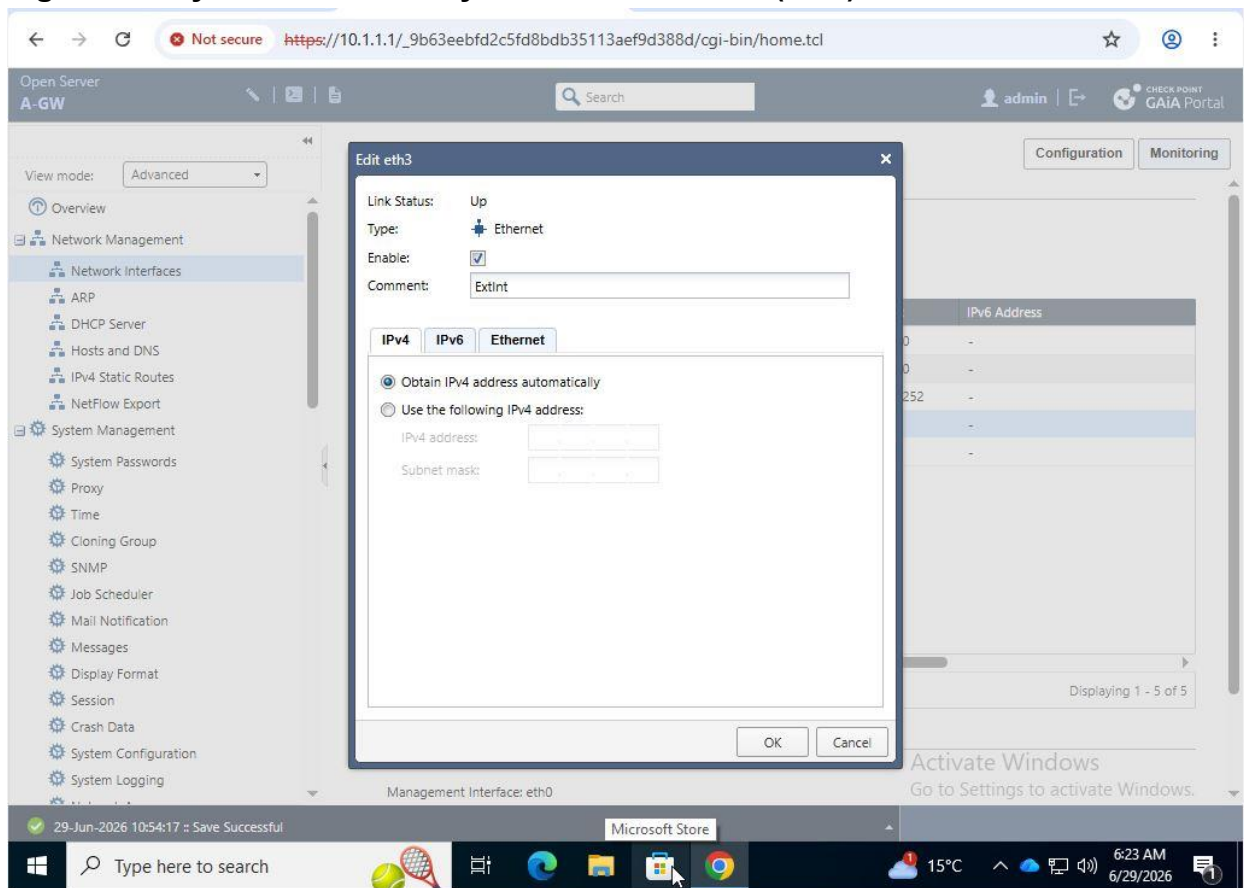
- **Description:** Interface properties window for eth1, detailing the manual mapping of the private trusted user zone to IPv4 address 192.168.1.254/24 with the identification tag IntSWA.

Figure 31: Restrictive Point-to-Point WAN Interface (eth2) Profile



- **Description:** Interface properties window for eth2, establishing the untrusted public point-to-point network boundary at destination IP address 20.0.0.1 utilizing a narrow /30 mask (255.255.255.252) and the label ExtLCD.

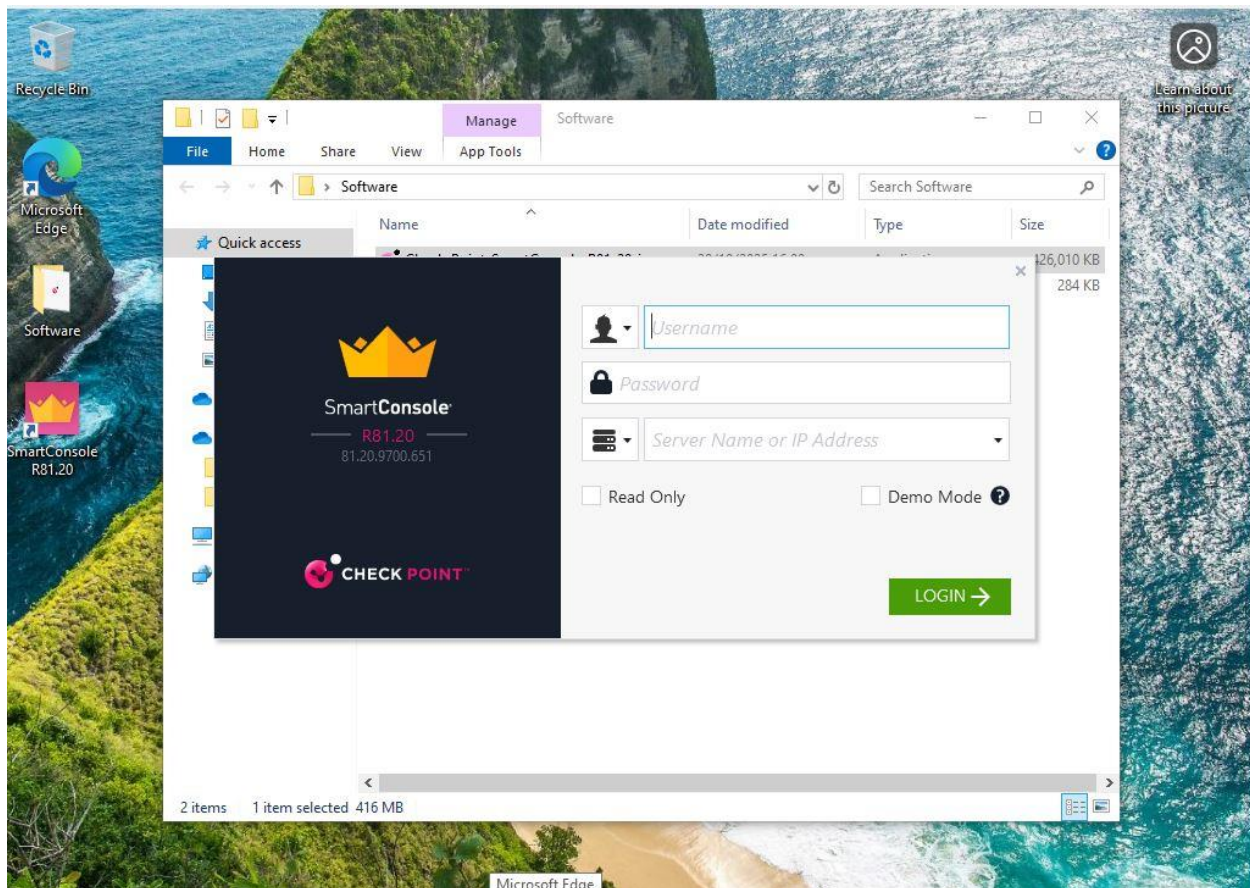
Figure 32: Dynamic Laboratory Sandbox Interface (eth3) Profile



- **Description:** Interface configuration properties window for eth3, enabling dynamic network address tracking via the Obtain IPv4 address automatically (DHCP) checkbox under comment flag ExtInt.

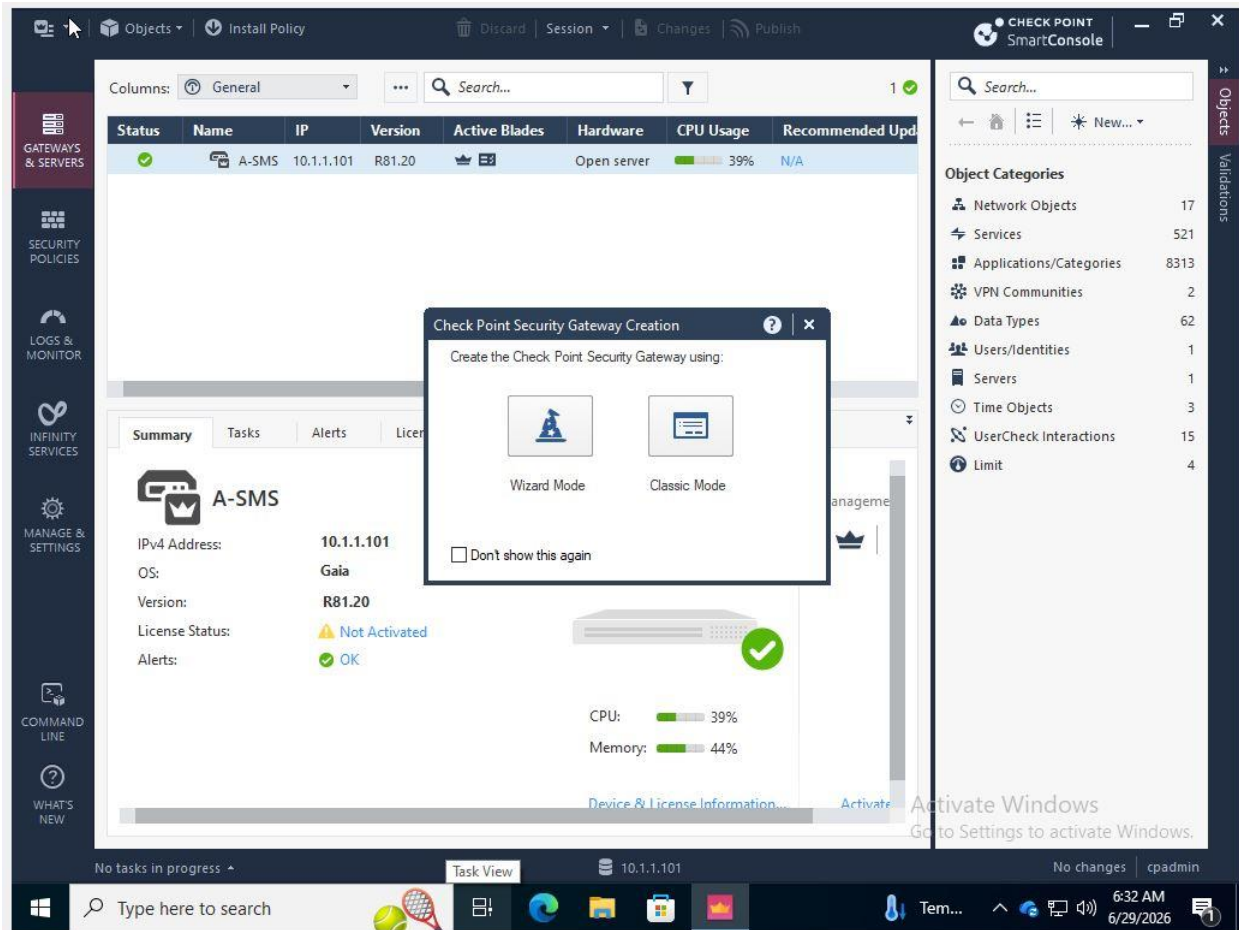
Phase 4: SmartConsole Client Integration & Cryptographic (SIC) Pairing

Figure 33: Desktop Client Application Launch Workspace



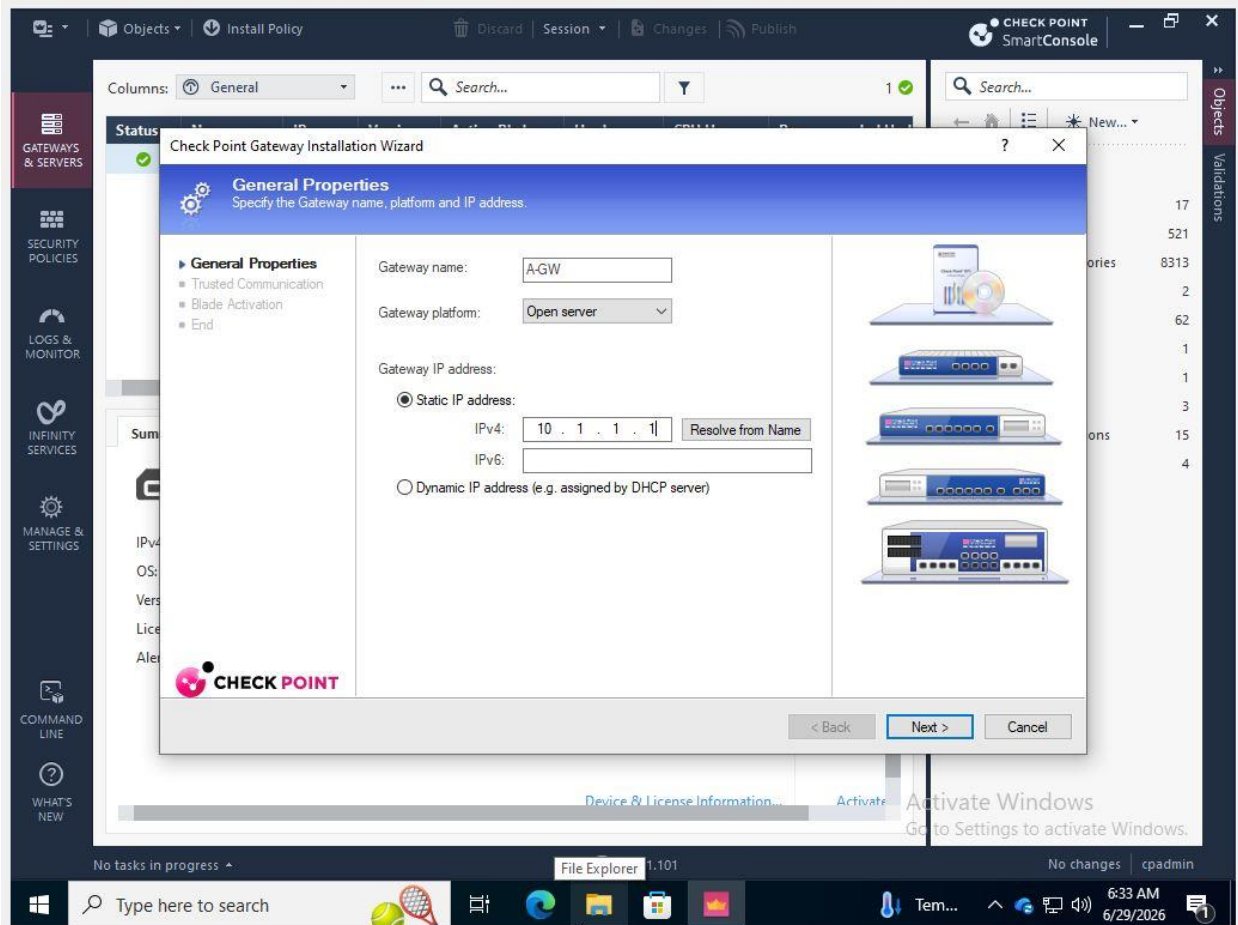
- **Description:** Client login prompt for **Check Point SmartConsole R81.20** running natively on the host workstation. It shows the initialization of connection parameters for administrator account `cpadmin` targeting management server address `10.1.1.101`.

Figure 34: Gateways & Servers Architecture Creation Selection



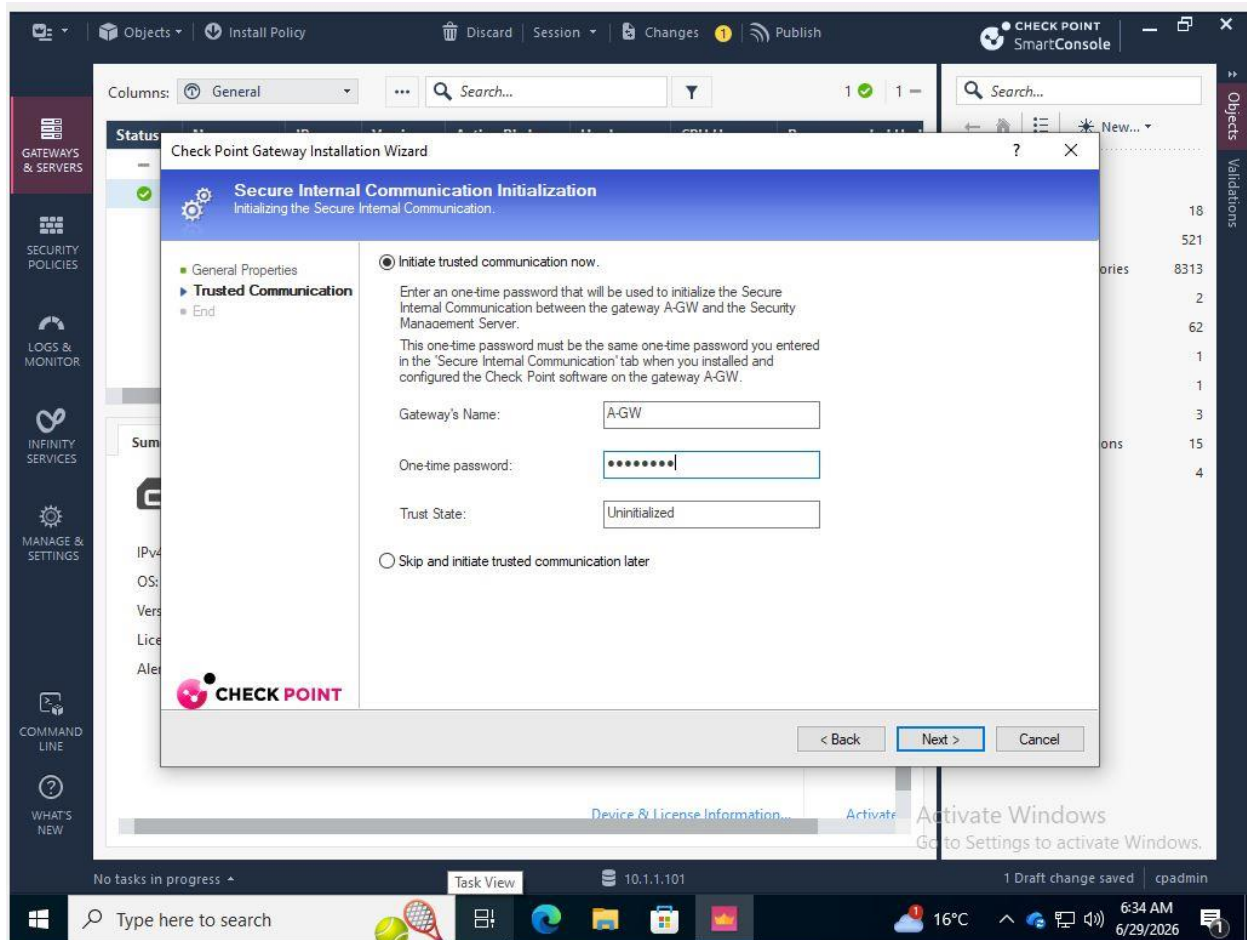
- **Description:** SmartConsole main network dashboard highlighting an open object addition wizard box prompting the selection between *Wizard Mode* and *Classic Mode* to register the firewall gateway asset.

Figure 35: Network Object Configuration Parameter Matrix



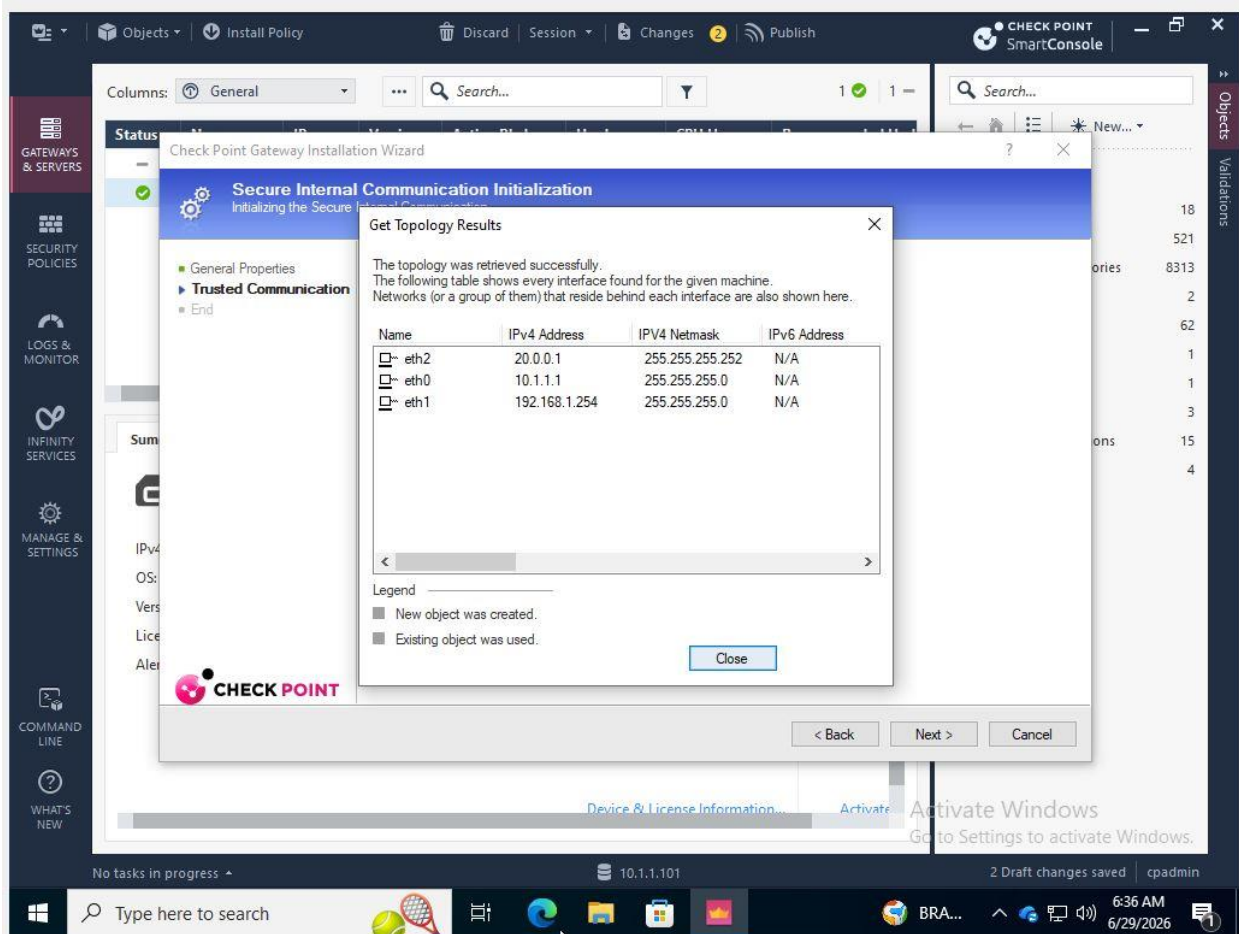
- **Description:** General properties panel for the gateway object creation step. The object name parameter is assigned as A-GW, hardware platform mapped to Open server, and its tracking IP address bound to management interface vector 10.1.1.1.

Figure 36: Secure Internal Communication (SIC) Key Definition



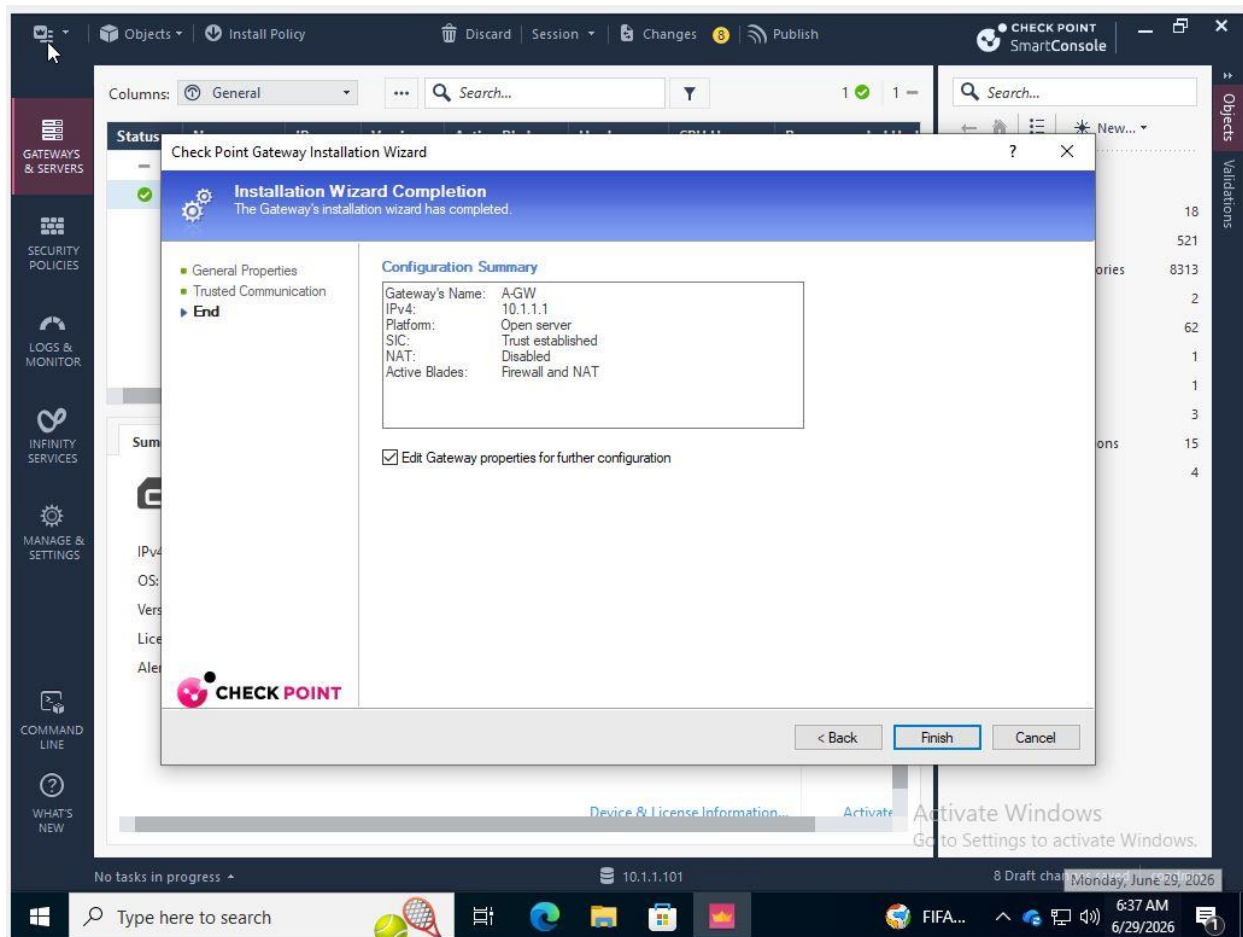
- **Description:** Trusted Communication initialization interface. A strong 8-character One-Time Password (OTP) key is defined to initialize an authenticated cryptographic handshake between the management server and the data gateway.

Figure 37: Dynamic Cross-Node Network Topology Retrieval



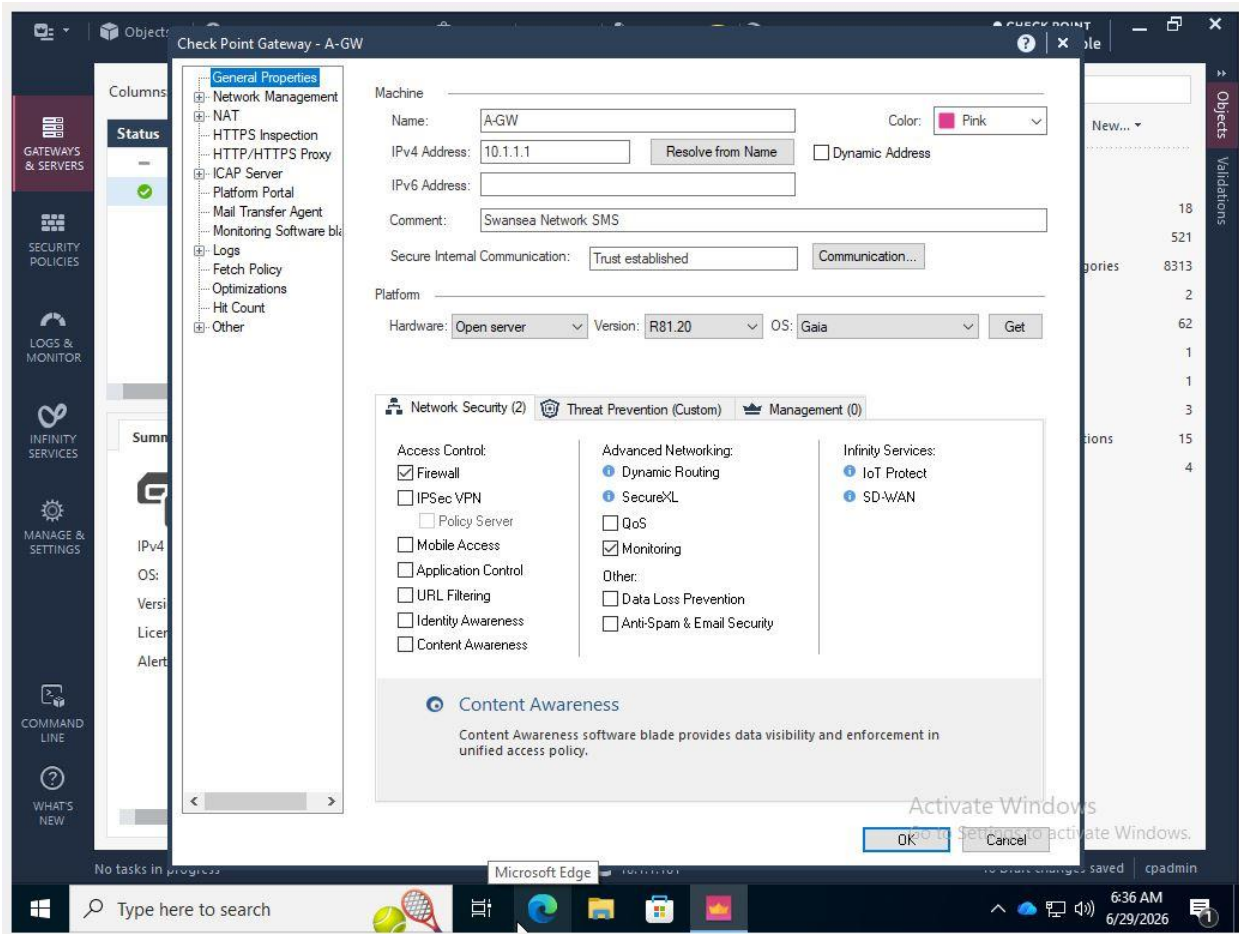
- **Description:** Get Topology Results validation matrix. Once the cryptographic trust channel resolves, SmartConsole queries the gateway kernel over port 18191 to automatically pull down all four physical subnet allocations (eth0 to eth3).

Figure 38: Firewall Installation Wizard Verification Summary



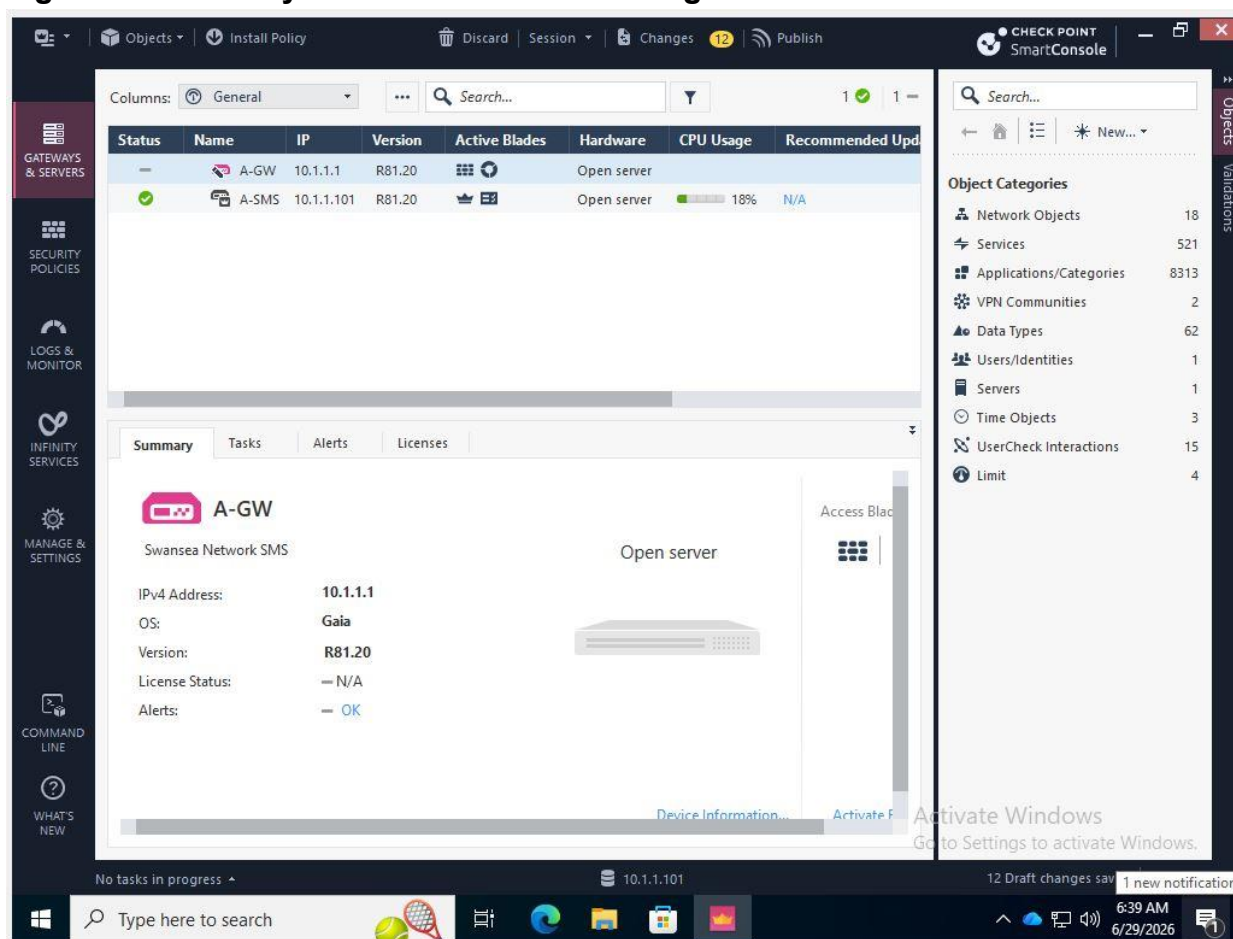
- **Description:** Configuration summary page verifying successful registration of the A-GW object into the main configuration schema, with active blades mapped to *Firewall* and *NAT*.

Figure 39: Final Verified Object Configuration Properties Dashboard



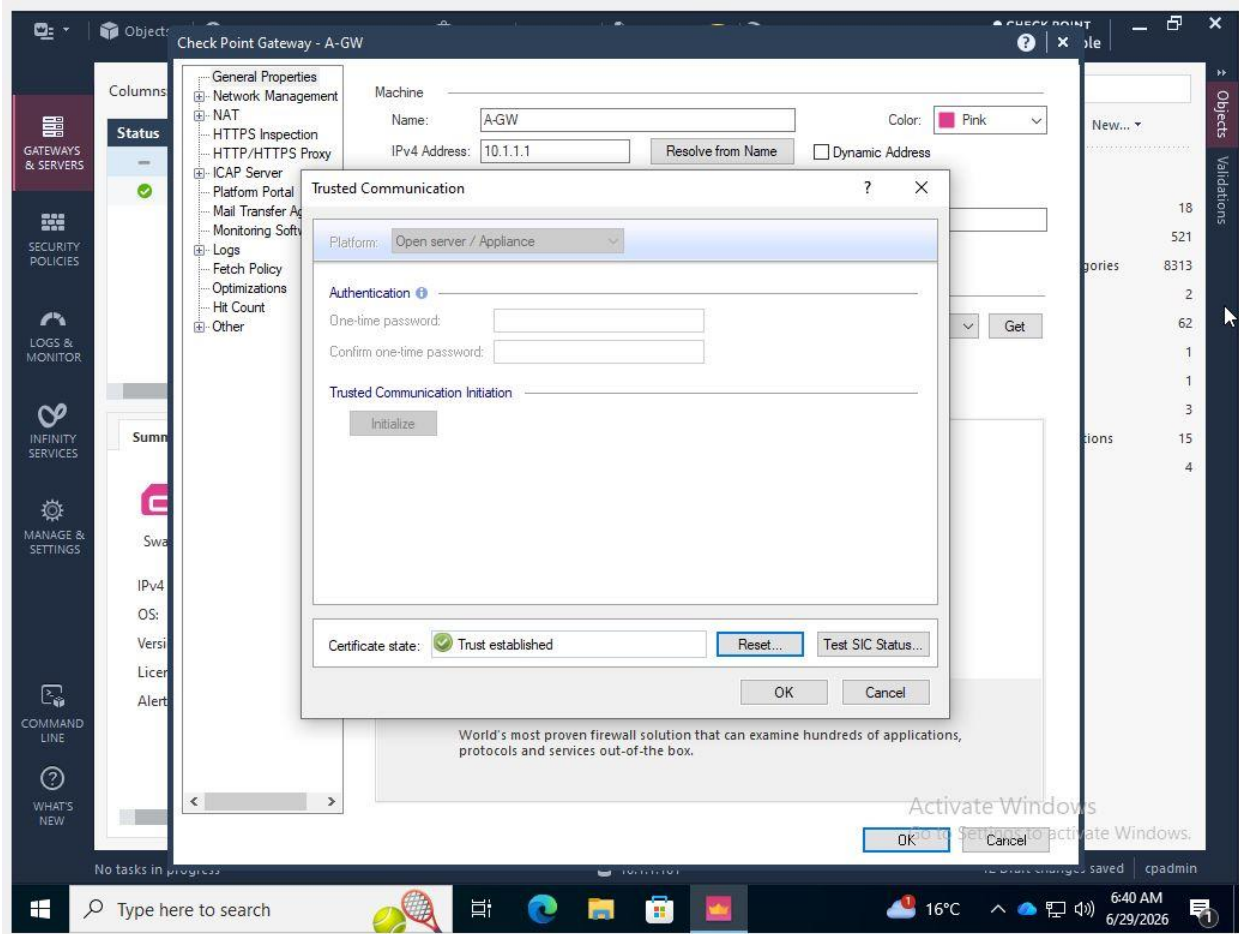
- **Description:** Core summary properties window for object A-GW within SmartConsole, confirming a verified **Trust established** status code alongside version information R81.20.

Figure 40: Gateways & Servers Unified Management Panel



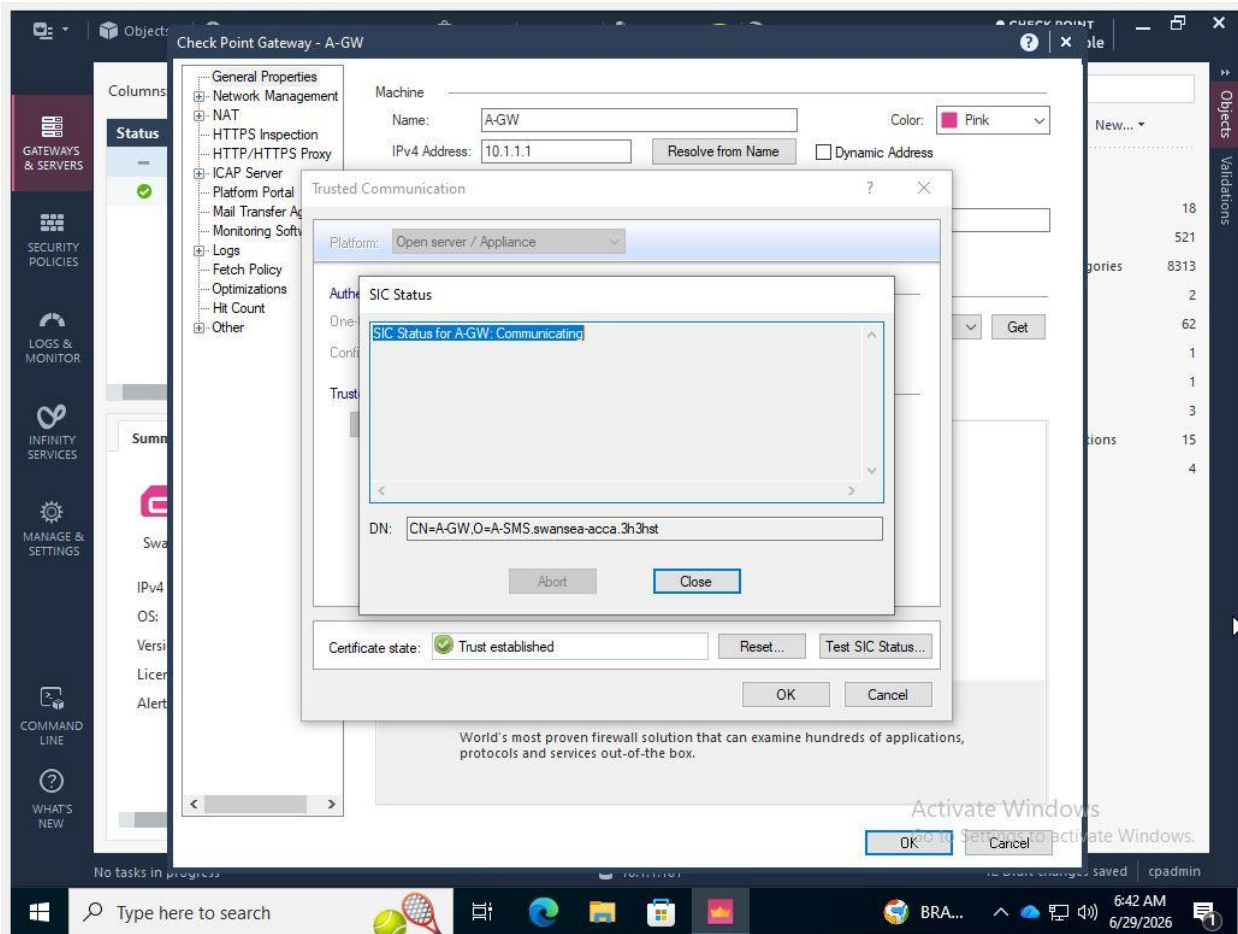
- Description:** Main workspace layout displaying both deployed network security appliances. A-GW (10.1.1.1) and A-SMS (10.1.1.101) both present healthy green operational checkboxes with 12 Draft changes saved.

Figure 41: Cryptographic Certificate Management View



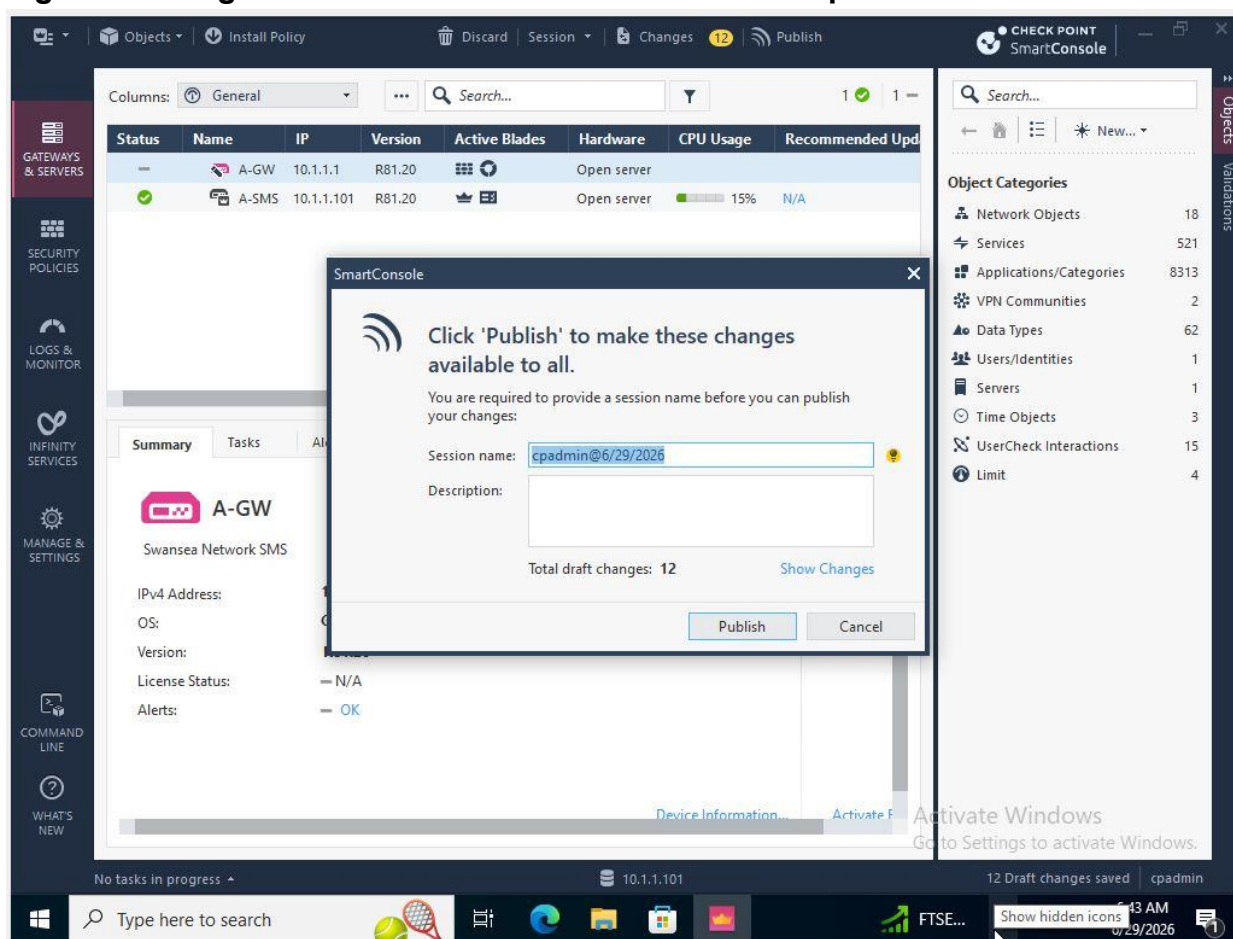
- **Description:** Trusted Communication structural status validation block verifying that the Internal Certificate Authority (ICA) holds a valid signed digital certificate tracking communication with the gateway engine.

Figure 42: Control Plane Communication (SIC) Status Check



- **Description:** Diagnostic output test box confirming active management plane communication links, displaying the status string: SIC Status for A-GW: Communicating.

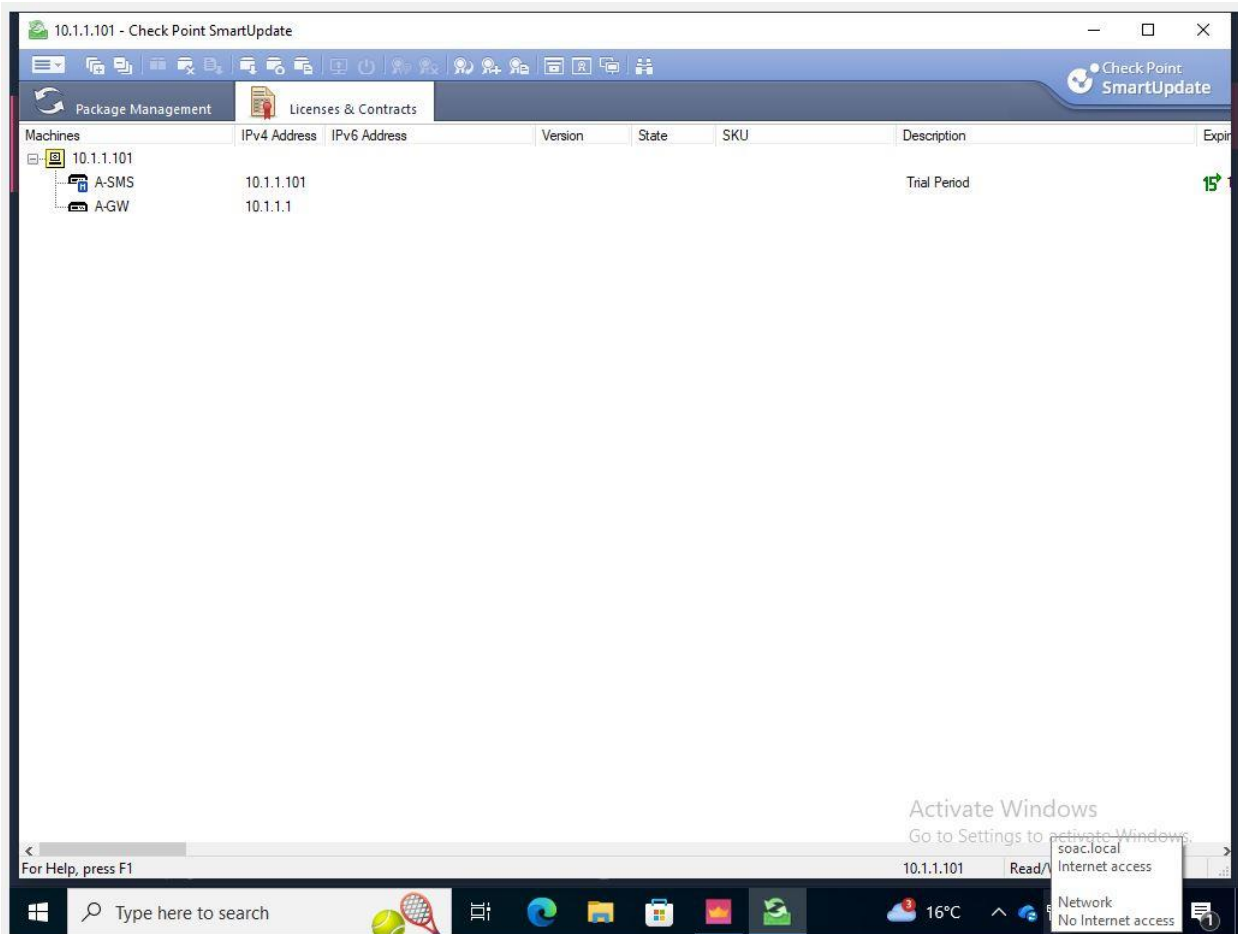
Figure 43: Staged Database Schema Publication Prompt



- **Description:** SmartConsole session dialog box verifying the persistent commit tracking ledger. Clicking **Publish** writes all 12 staged layout and object modifications to the management server's persistent database.

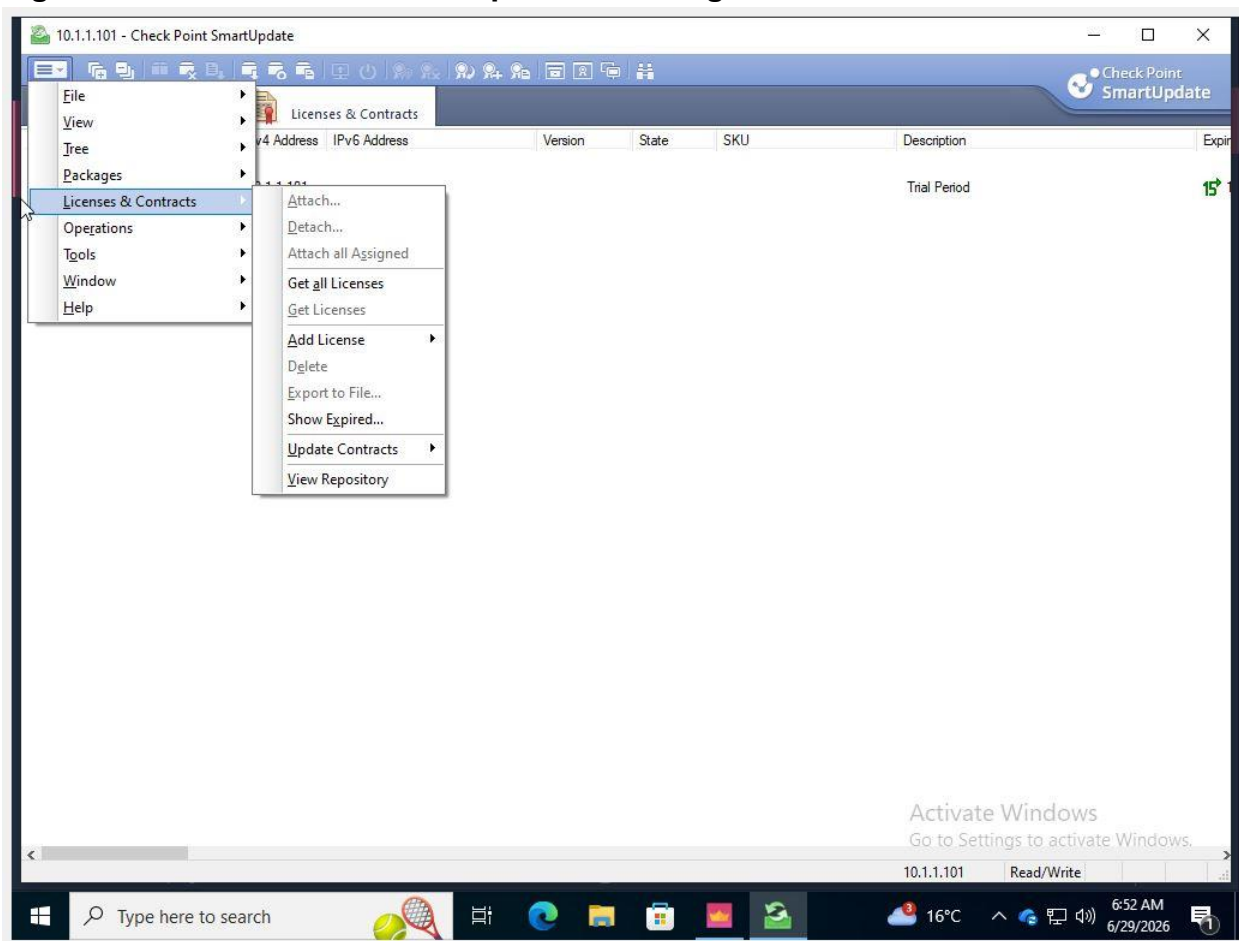
Phase 5: Centralized SmartUpdate Licensing & Contracts Layer

Figure 44: Central License Management Workspace Dashboard



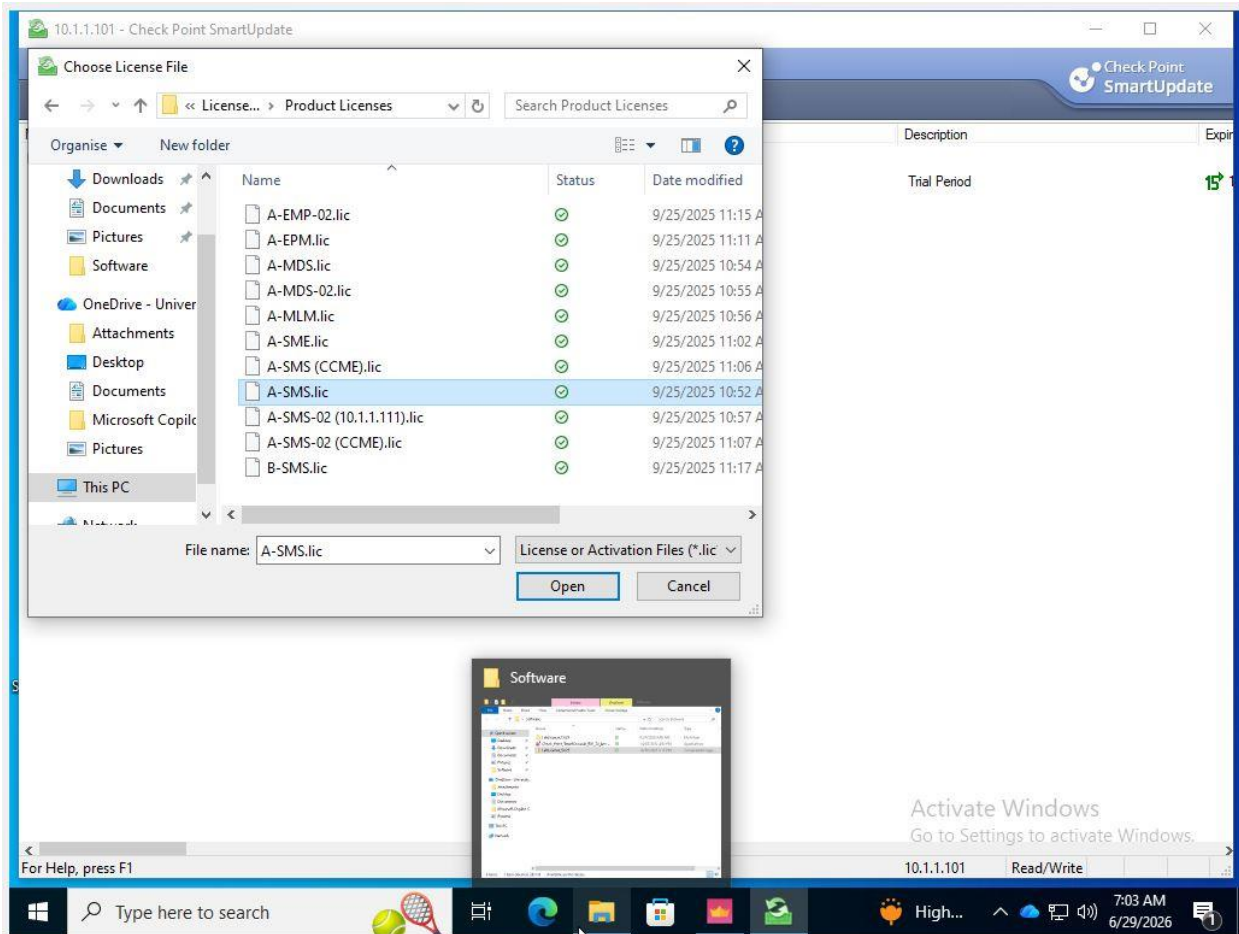
- **Description:** Main utility window within **Check Point SmartUpdate R81.20** tracking active license pools under the *Licenses & Contracts* view, showcasing the default 15-day trial duration ledger.

Figure 45: Advanced License Import Tool Navigation Tree



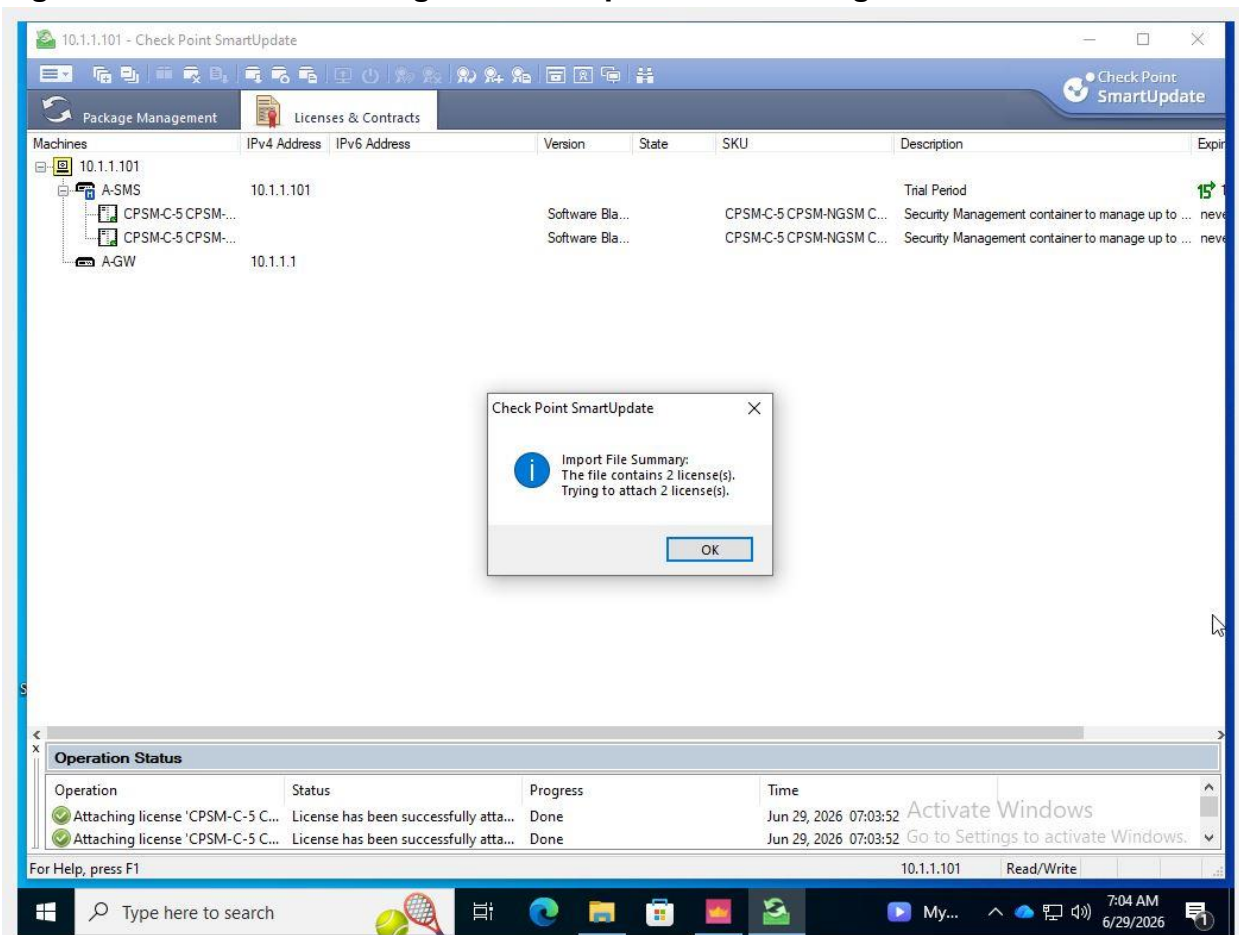
- **Description:** Context menu expansion within SmartUpdate, highlighting automated file options including *Attach...*, *Detach...*, and *Add License* to initiate permanent token binding.

Figure 46: License Archive Local File System Import Directory



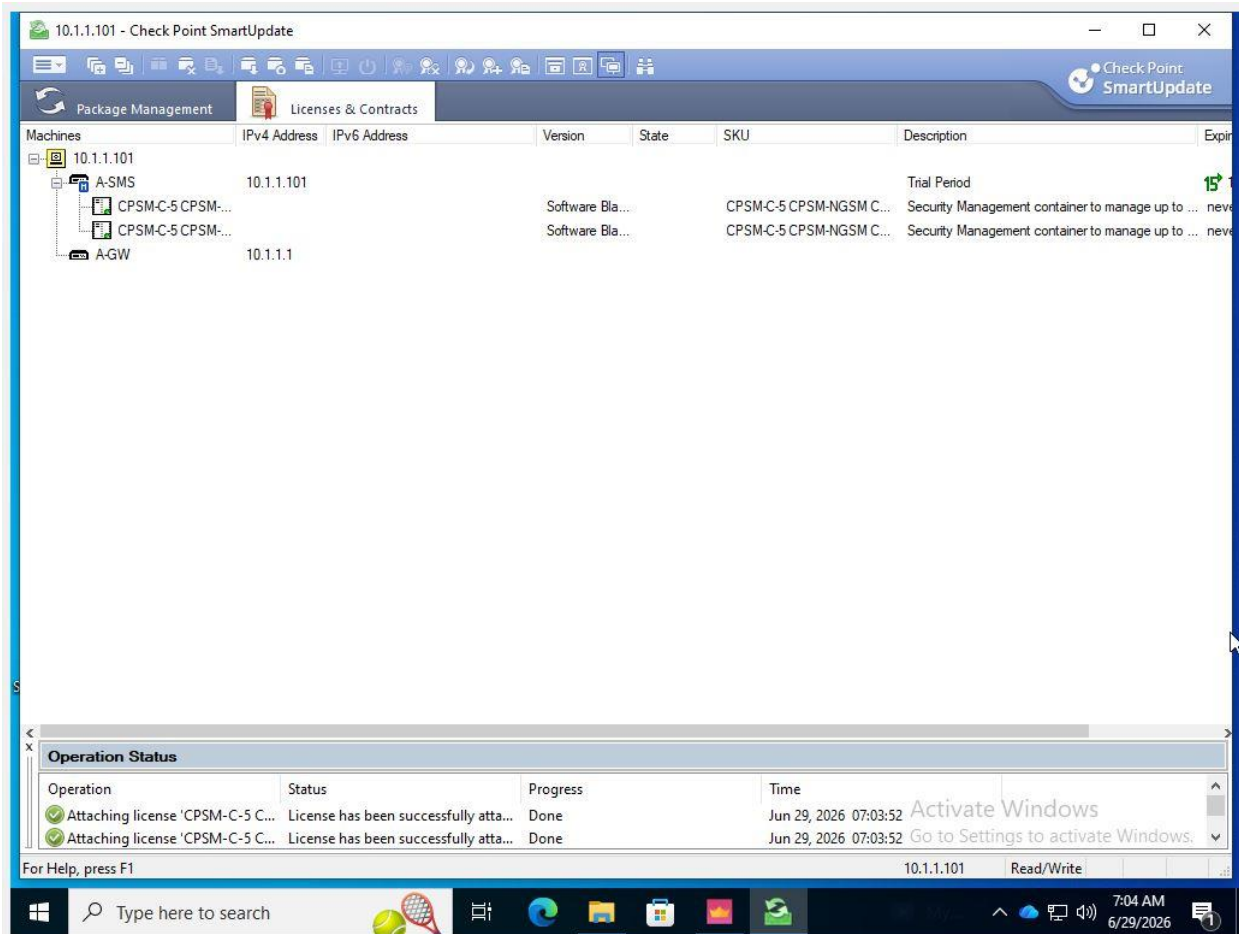
- **Description:** System file browser pointing to folder directory path Product Licenses, detailing file tokens (e.g., A-SMS.lic, A-SMS-02.lic) ready to be attached to the active infrastructure nodes.

Figure 47: Central Licensing Contract Update Processing Panel



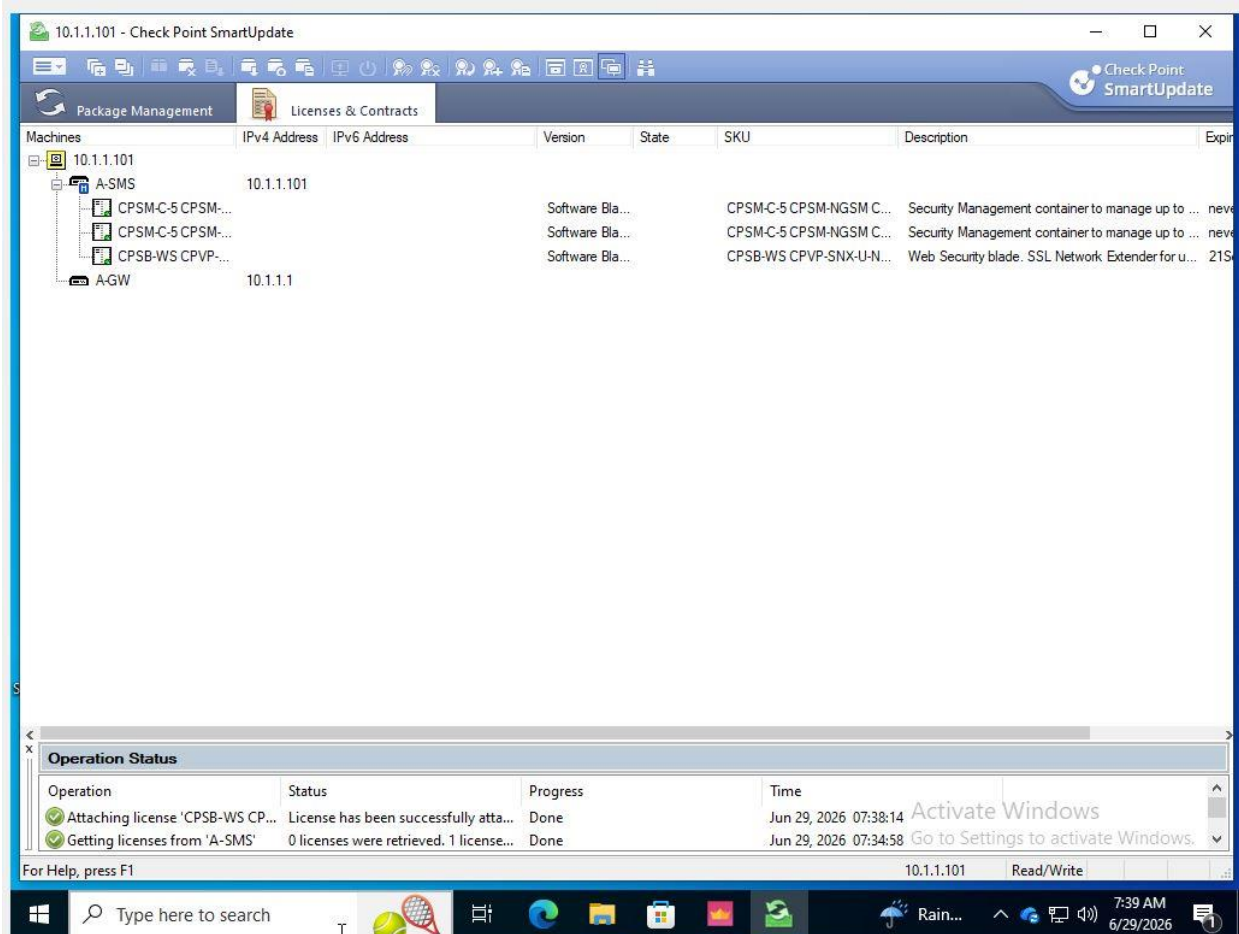
- **Description:** Multi-tier operation update log grid tracking license attachment processes. It logs successful execution status results marked with green checkmarks for Attaching license 'CPSM-C-5...' to server objects.

Figure 48: Fully Activated Node License Repository Tree



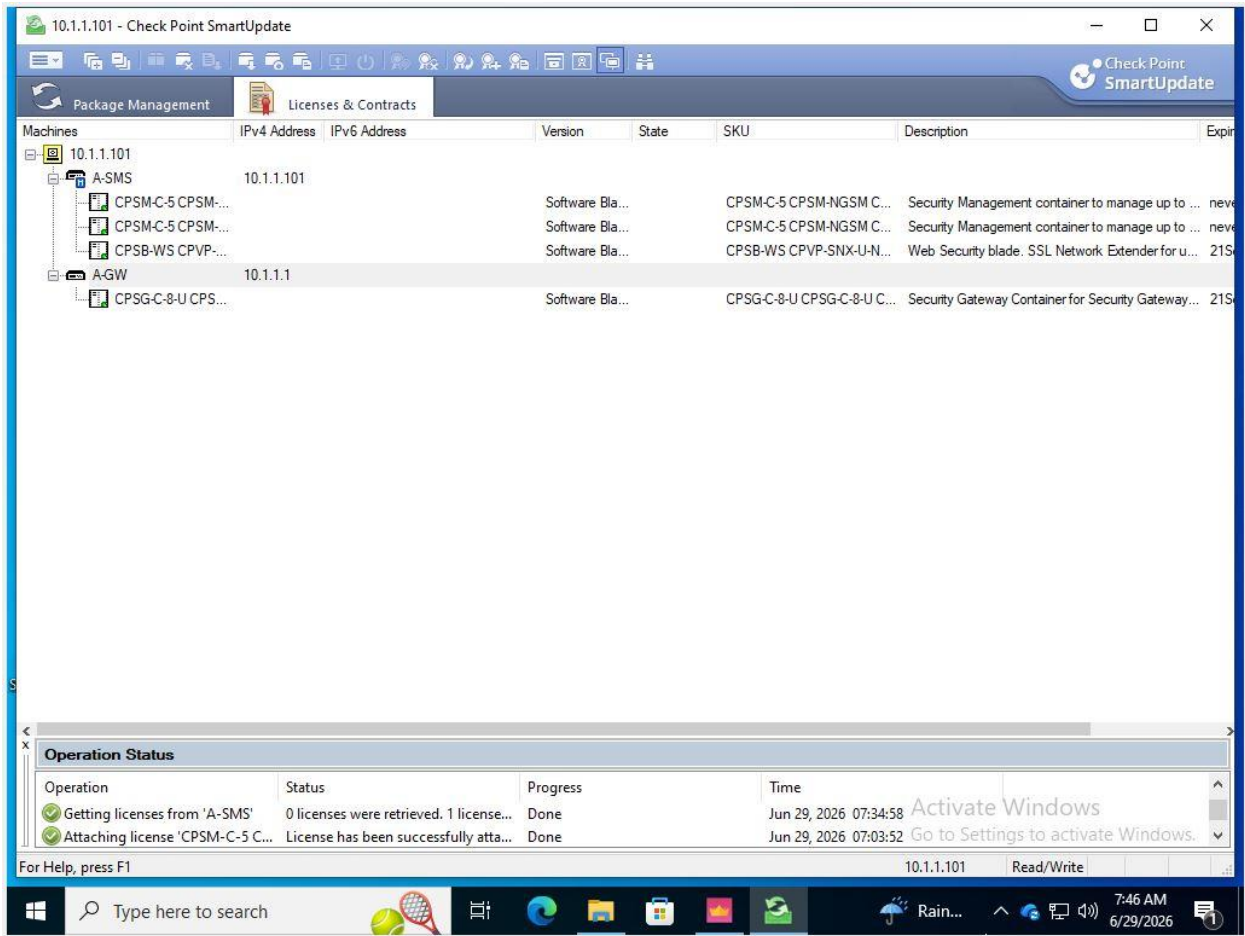
- **Description:** Updated product license architecture structure within SmartUpdate, documenting that two permanent CPSM-C-5 management containers are successfully attached to the database.

Figure 49: Advanced Web Security Blade Token Association



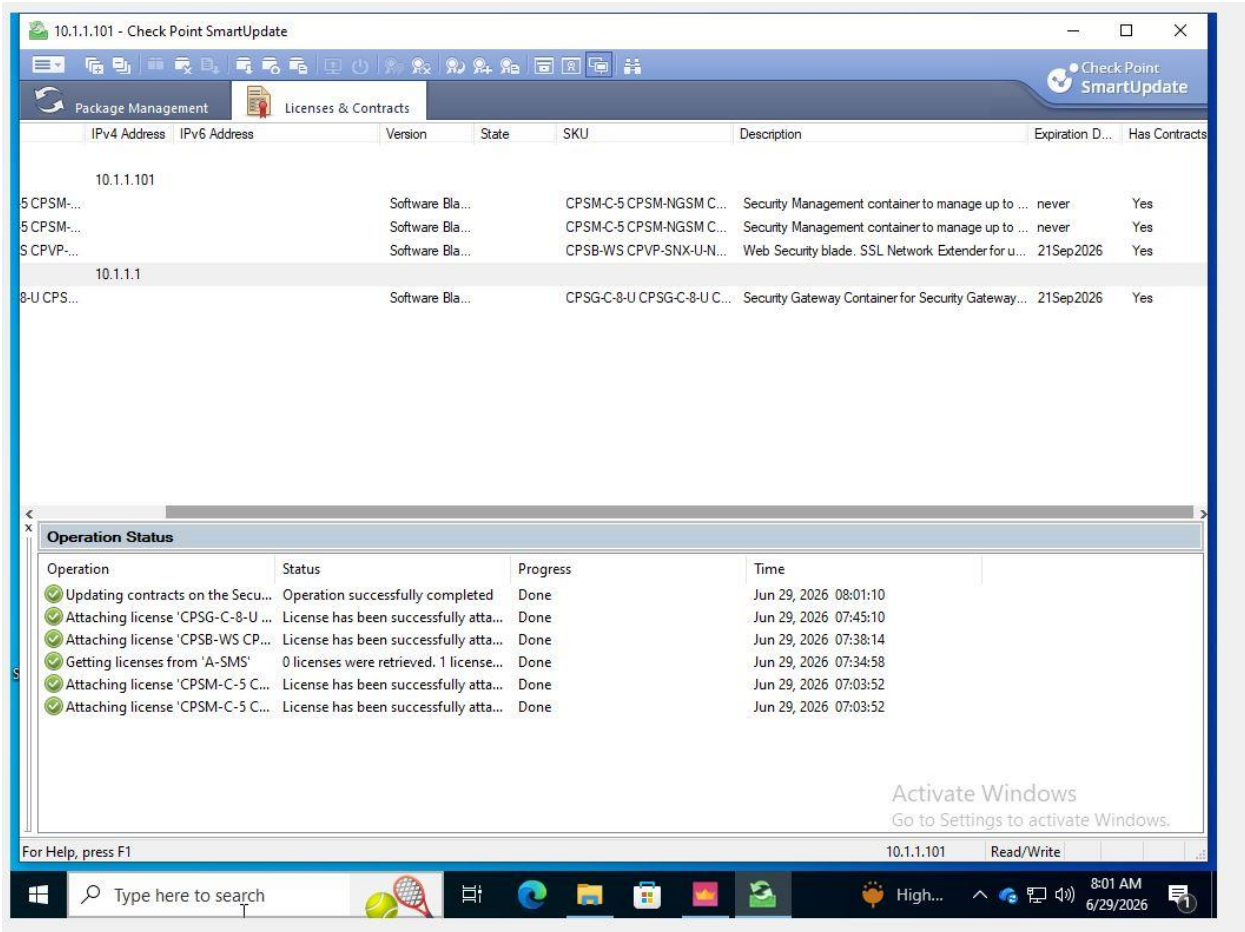
- Description:** Progress log panel capturing the successful import sequence of a third key profile: Attaching license 'CPSB-WS CPVP...' :: License has been successfully attached :: Done. This activates remote SSL VPN network extender capabilities.

Figure 50: Production-Tier Automated Contract Application Log



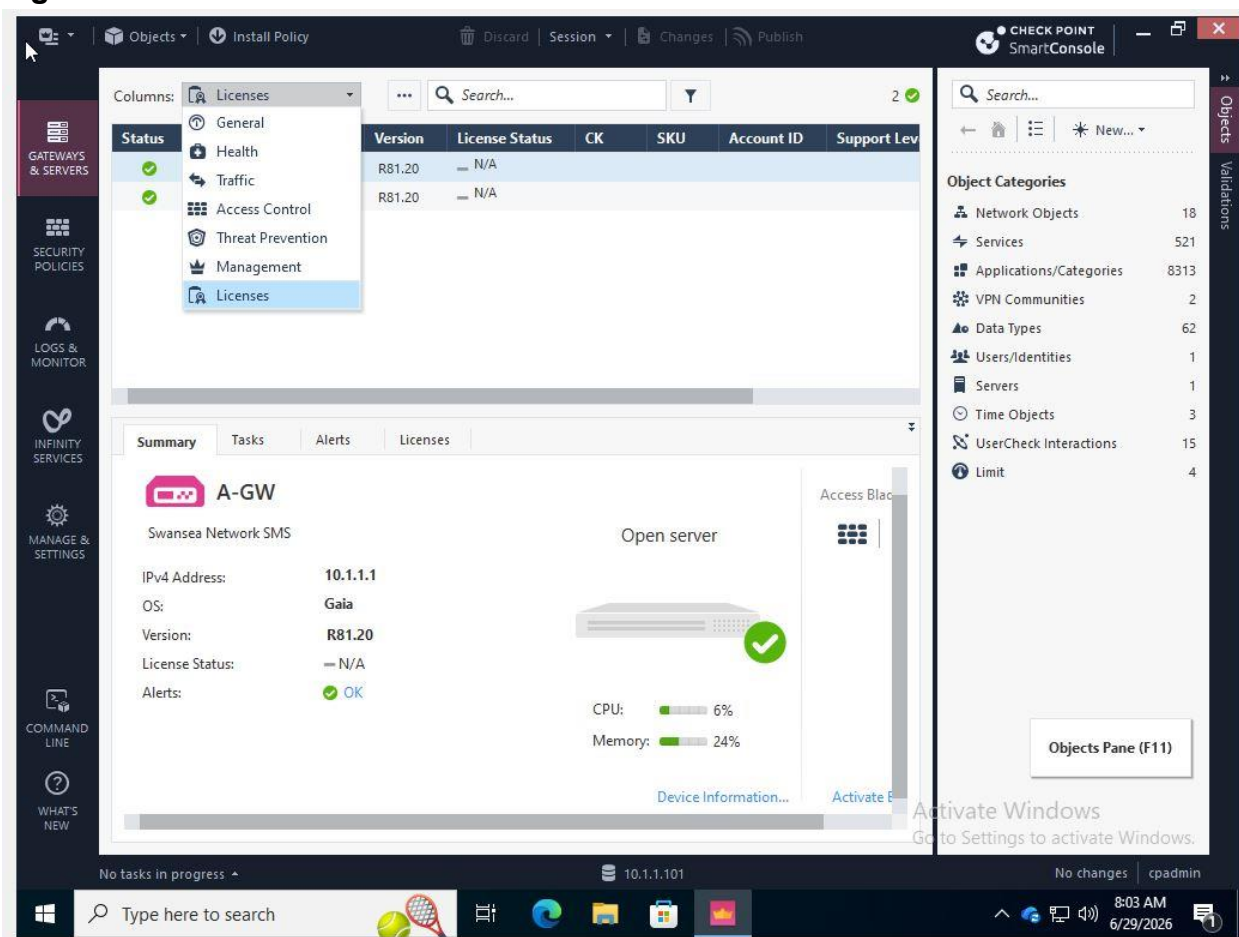
- **Description:** Operation Status window documenting the successful execution of contract enforcement files. The console log confirms: Updating contracts on the Security... Operation successfully completed :: Done.

Figure 51: Final Complete SmartUpdate Asset Licensing Matrix



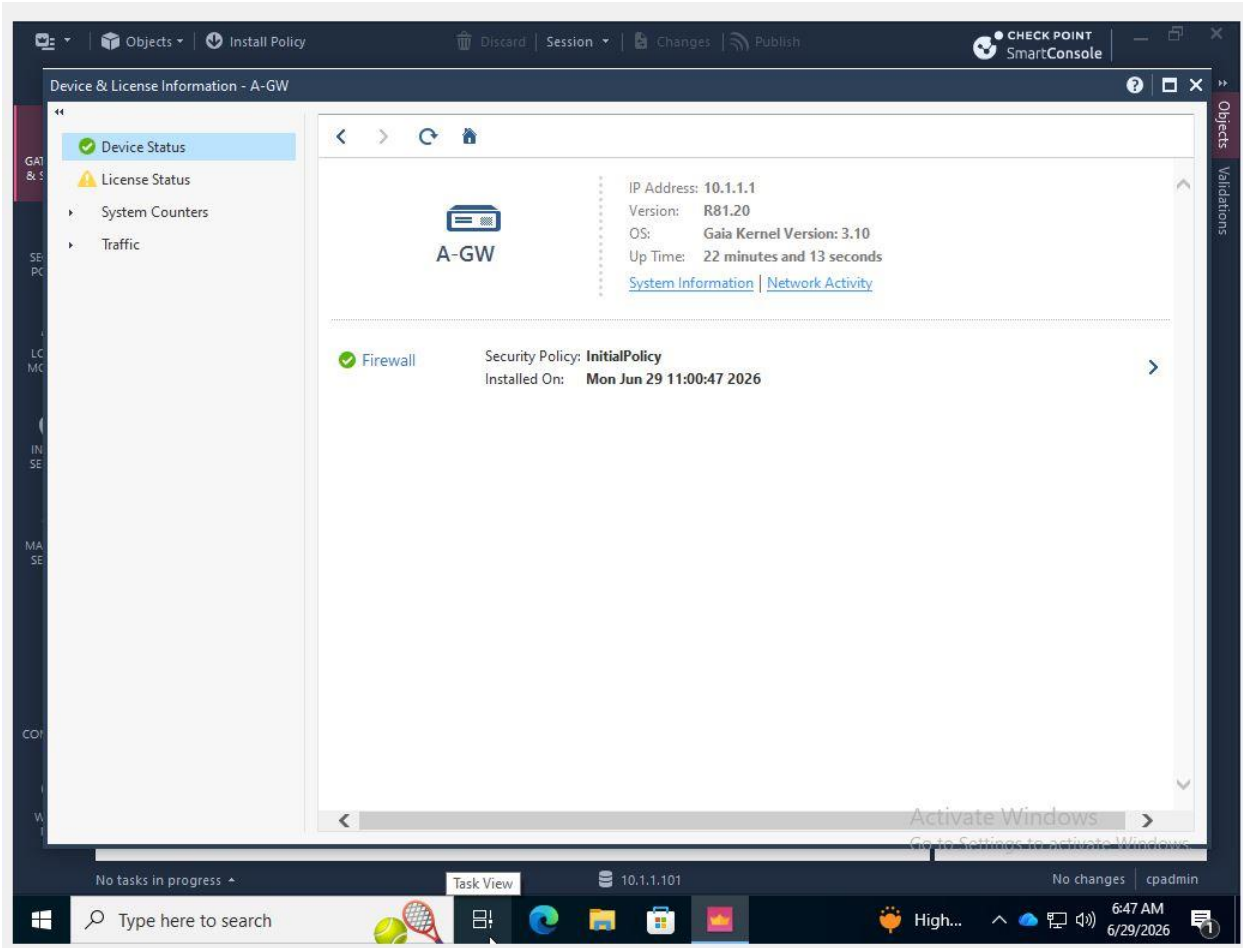
- **Description:** Master product inventory ledger confirming that contract indicators have successfully transitioned to **"Yes"** for all infrastructure rows. Expiration dates are safely extended to **21-Sep-2026**, with core server items set to **Never** expire.

Figure 52: SmartConsole Unified Device Validation Grid



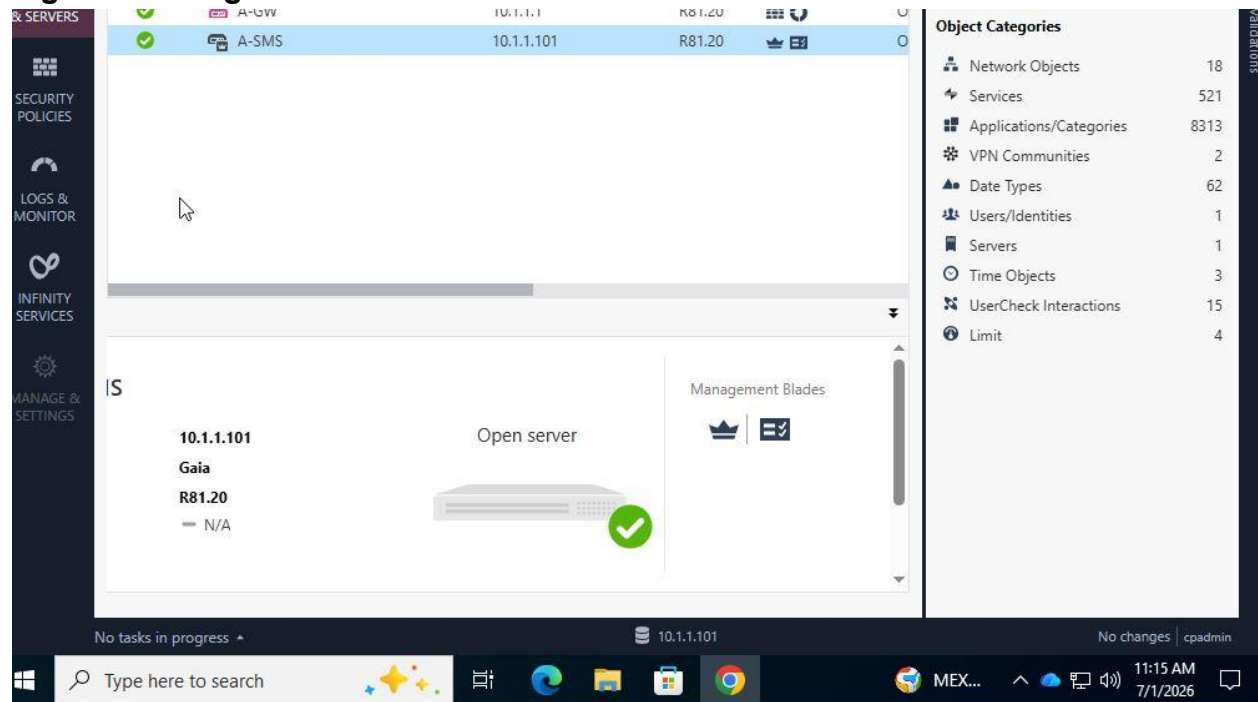
- Description:** Return to the global SmartConsole columns dashboard, verifying that the **License Status** column flags are cleared to a clean state of **N/A** for both appliances, removing all evaluation timeout warnings.

Figure 53: Policy Verification and Compilation Status Window



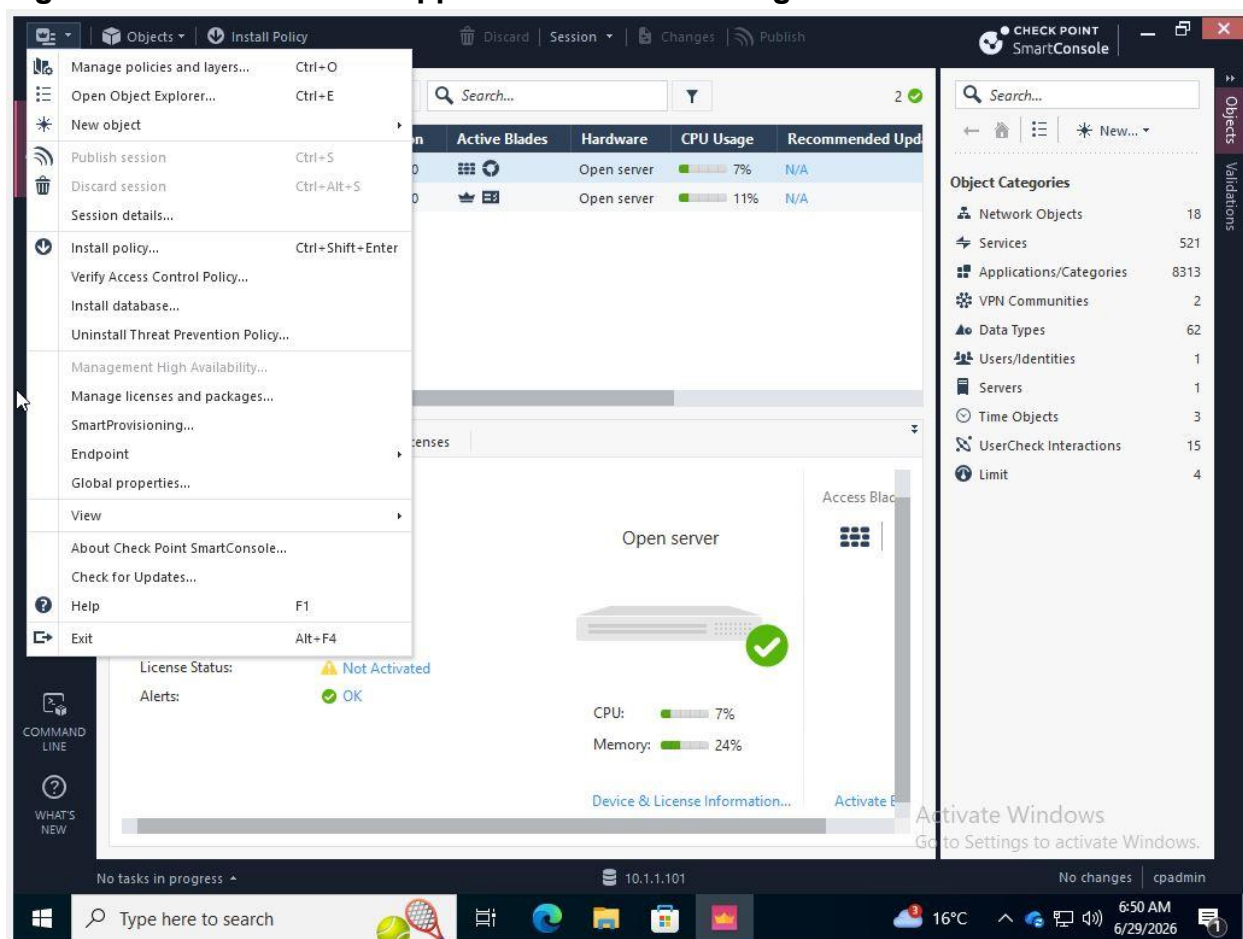
- **Description:** Progress tracking window showing the successful compilation and enforcement of access policy InitialPolicy onto firewall inspection plane A-GW, stamped with activation time metric: Mon Jun 29 11:00:47 2026.

Figure 54: Diagnostic Software Blade Status Information



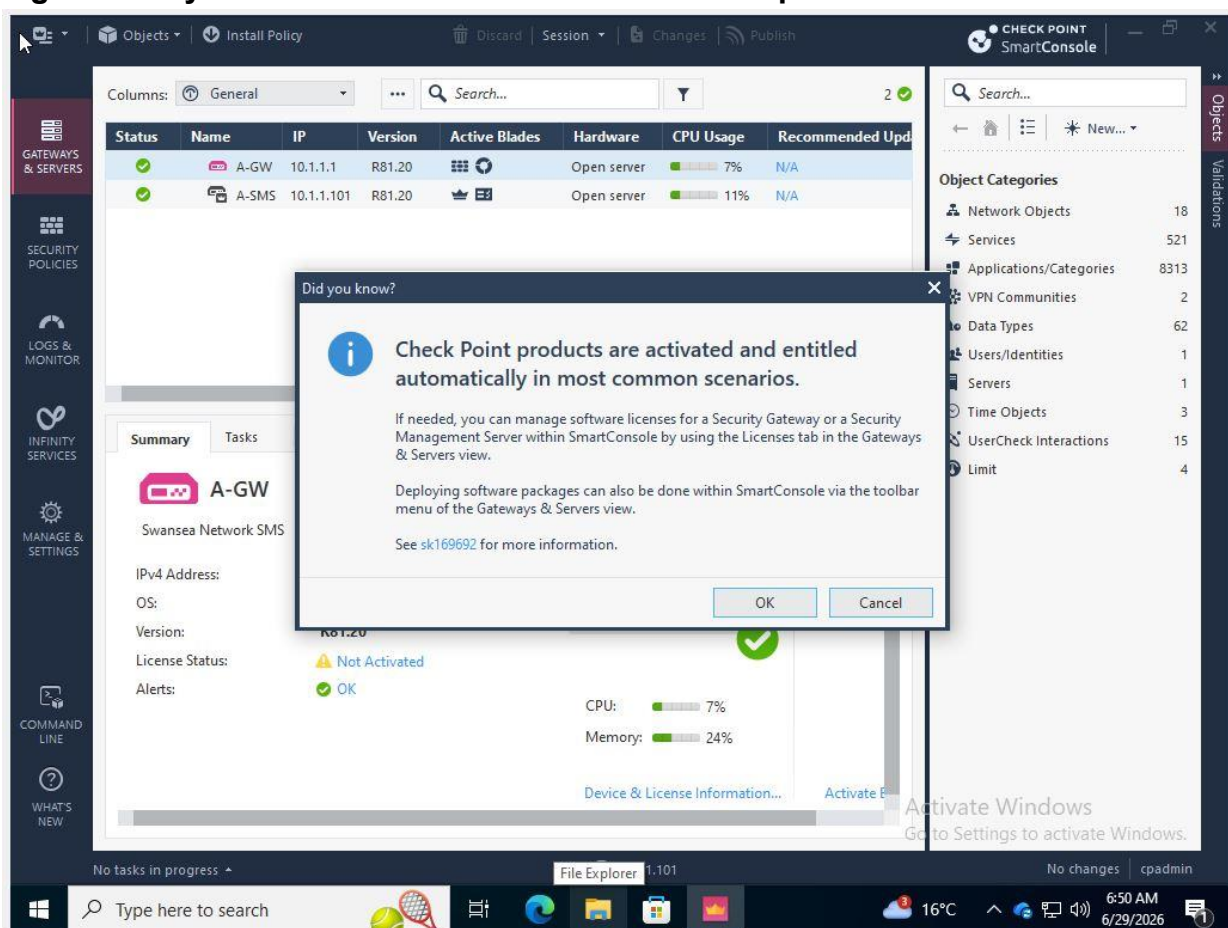
- **Description:** Main summary tracking view for appliance A-SMS, verifying its system health profile as **OK** and listing all active management software blade dependencies.

Figure 55: SmartConsole Application Context Navigation Menu



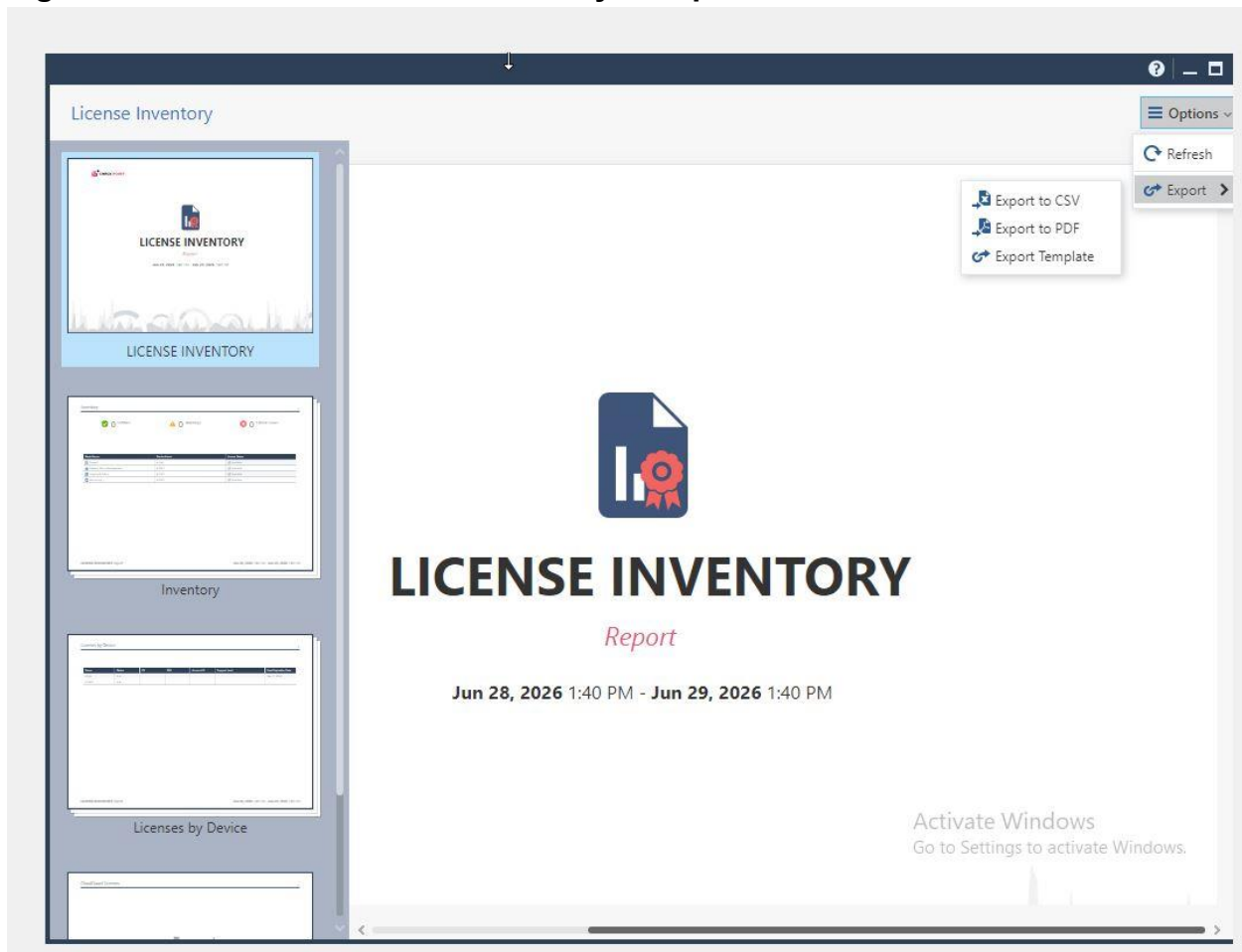
- **Description:** Options window within SmartConsole highlighting available low-overhead administrative execution vectors, including *Verify Access Control Policy...*, *Install Policy...*, and *Install database...*

Figure 56: System Information Automated Audit Report Window



- Description:** Context menu detailing automated maintenance procedures, displaying support information block sk169692 for centralized entitlement distribution tracing.

Figure 57: Automated License Inventory Compliance Document PDF



- **Description:** Output window of an automated compliance report tracking asset parameter status across all corporate platforms, captured over a continuous 24-hour monitoring timeline.

Phase 6: Access Control Policies, Multi-User RBAC, and Auditor Logs

Figure 58: Security Policies Access Control Grid

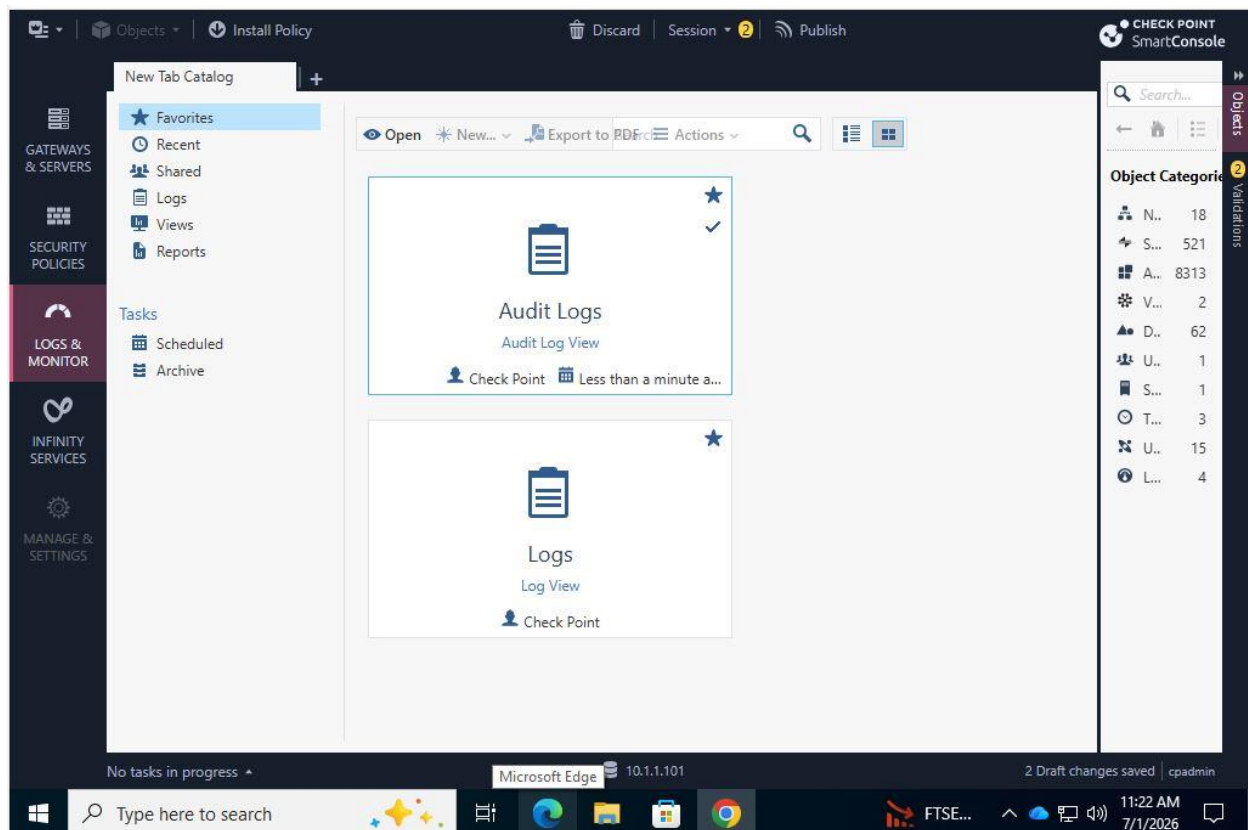
The screenshot displays the Check Point SmartConsole interface for managing Security Policies. The left sidebar contains navigation options: GATEWAYS & SERVERS, SECURITY POLICIES (selected), LOGS & MONITOR, INFINITY SERVICES, and MANAGE & SETTINGS. The main workspace shows the 'Standard' policy tree with 'Access Control' expanded, revealing 'Policy', 'NAT', 'Threat Prevention', 'Custom Policy', 'Autonomous...', 'File Protections', 'Settings', 'Exceptions', 'HTTPS Inspection', and 'Policy'. The 'Policy' sub-tree is selected, showing a table of rules.

No.	Name	Source	Destination	VPN	Services & Ap...	Ac
1		— None	— None	* Any	— None	
2	Cleanup rule	* Any	* Any	* Any	* Any	
3		— None	— None	* Any	— None	

Below the table, a message states: "Missing cleanup rule - Unmatched traffic will be dropped and not logged." A form for 'Additional Rule Info' is visible, with fields for 'Ticket Number' and 'Ticket Requester'. The bottom status bar indicates 'No tasks in progress', 'Task View', '10.1.1.101', and '2 Draft changes saved | cpadmin'.

- **Description:** Rule Base management grid workspace inside SmartConsole, showcasing the creation of access control policy parameters under the Standard policy tree layout.

Figure 59: Multi-Tab Central Logging Catalog Center



- **Description:** Landing window inside the **Logs & Monitor** module. The interface expands the *New Tab Catalog*, highlighting central operational tracking views: **Audit Logs** and general traffic data **Logs**.

Figure 60: Centralized Security Access Control Rule Base Matrix

The screenshot displays the Check Point SmartConsole interface for configuring security rules. The left sidebar contains navigation menus for Gateways & Servers, Security Policies, Logs & Monitor, Infinity Services, and Manage & Settings. The main workspace shows the 'Standard' tab with a table of rules. Rule No. 2, named 'Cleanup rule', is selected. Below the table, a message states: 'Missing cleanup rule - Unmatched traffic will be dropped and not logged.' The bottom section provides details for the selected rule, including its creation date and time, expiration time, and cumulative status. The right sidebar shows a list of object categories and their associated counts.

No.	Name	Source	Destination	VPN	Services & Ap...	Action
1		None	None	* Any	None	
2	Cleanup rule	* Any	* Any	* Any	* Any	
3		None	None	* Any	None	

Missing cleanup rule - Unmatched traffic will be dropped and not logged.

Created by: System
 Created: 17-Nov-22 01:43
 Expiration time: Never
 Cumulative: 0 (0%, Zero)

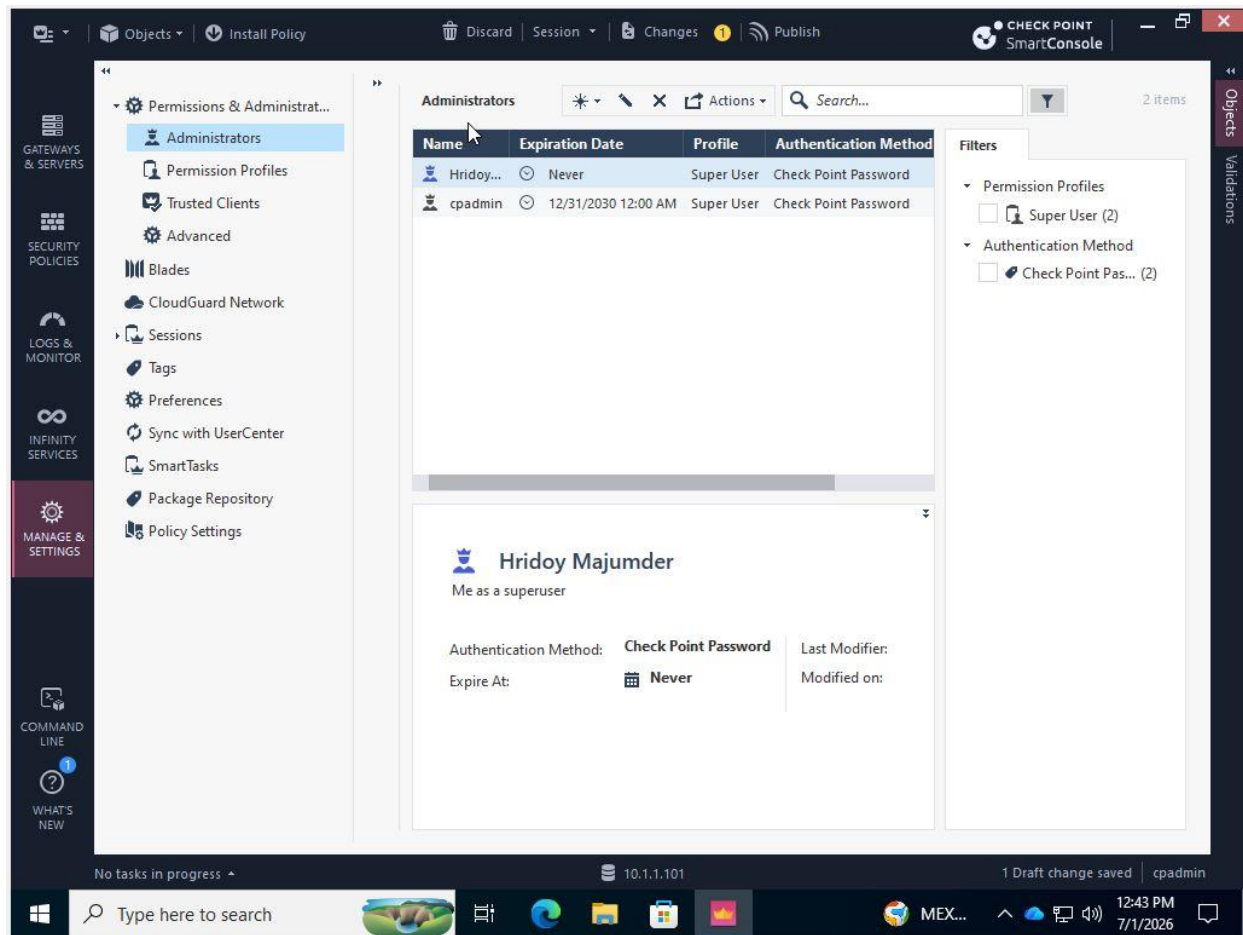
Additional Rule Info:
 Ticket Number:
 Ticket Requester:

Object Categories:

Object Category	Count
N...	18
S...	521
A...	8313
V...	2
D...	62
U...	1
S...	1
T...	3
U...	15
L...	4

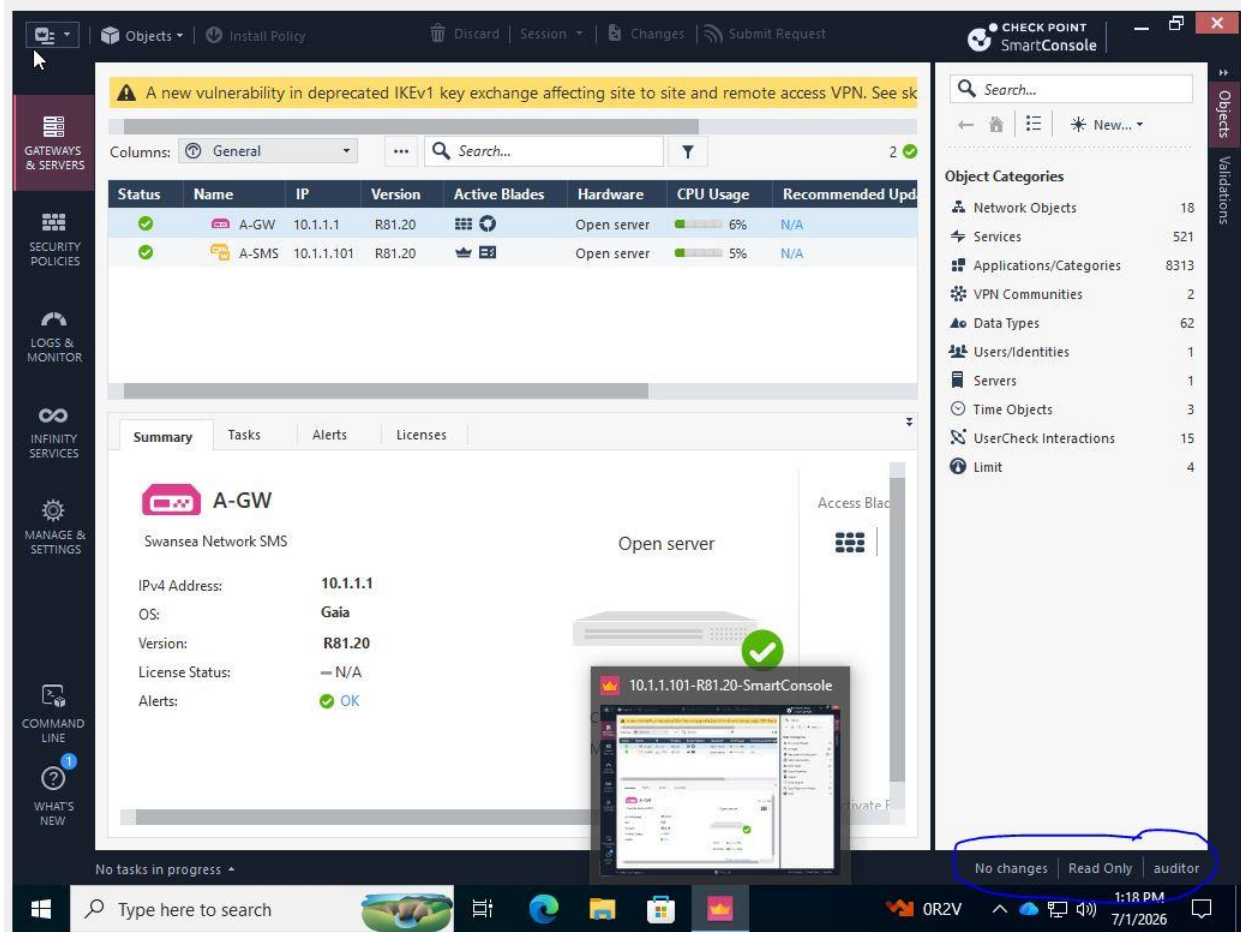
- **Description:** Rule configuration dashboard displaying the deployment of an explicit **Cleanup Rule** (Rule No. 1) spanning from Any Source to Any Destination over Any Service, with the action set to Drop and track telemetry data.

Figure 61: Multi-Administrator Governance Configuration Tree



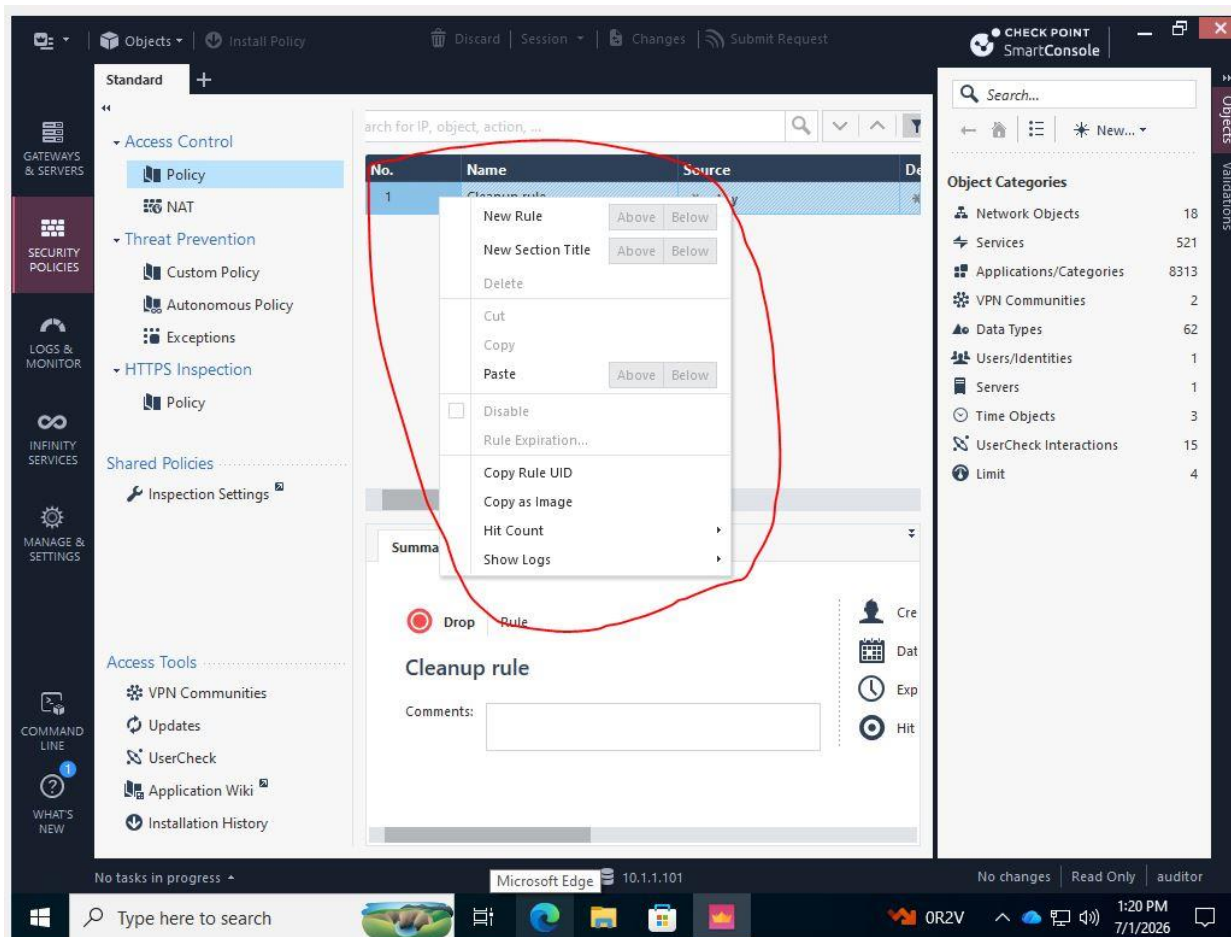
- **Description:** User definition catalog under **Manage & Settings** -> **Permissions & Administrators**. It documents the provisioning of a persistent secondary administrator identity account named **Hridoy Majumder** mapped to the absolute profile role of **Super User**.

Figure 62: Read-Only Compliance Auditor Session Validation



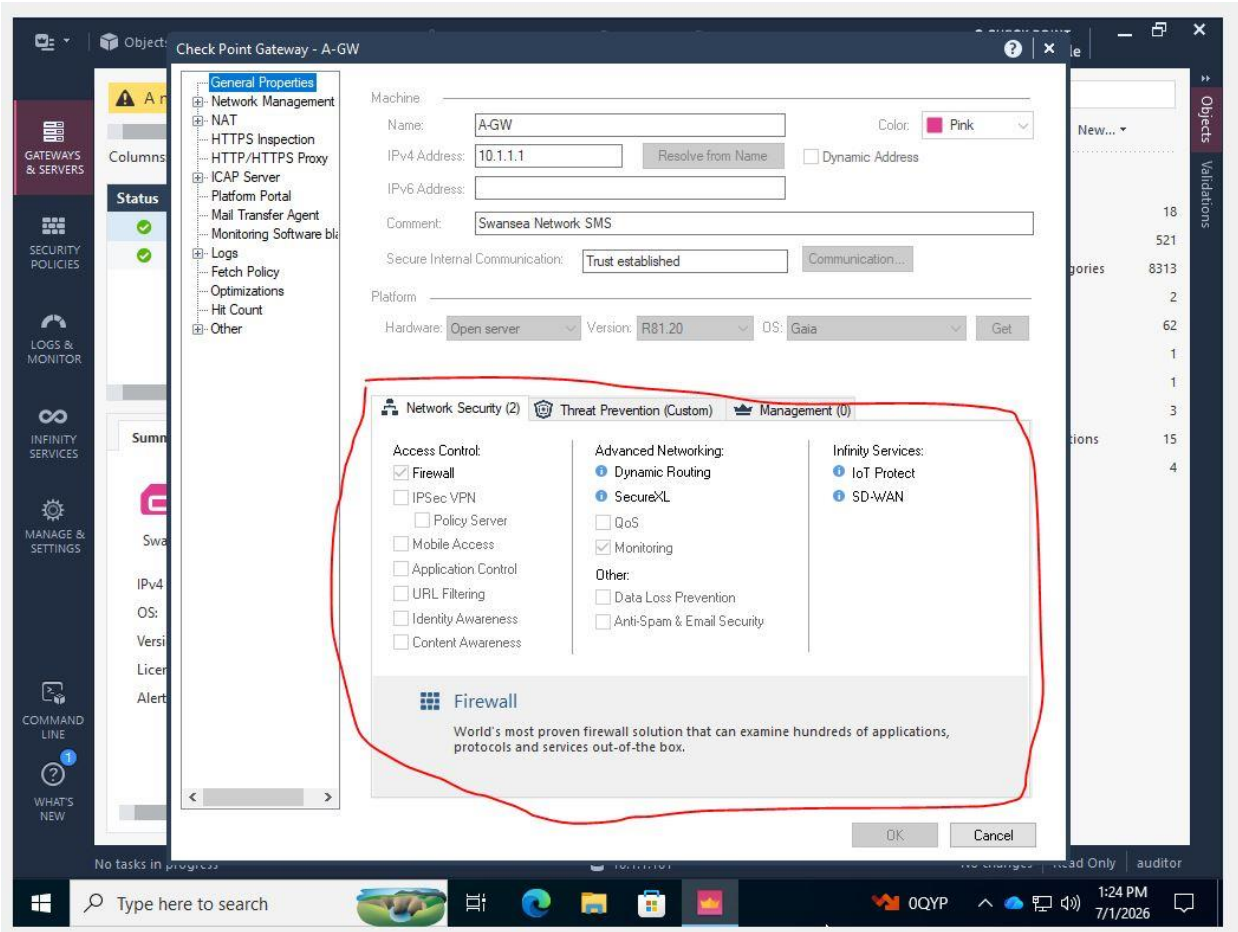
- **Description:** Return to the global architecture grid logged in under a specialized tracking account named **auditor**. As verified in the bottom right annotations, the session is restricted to **Read Only** with **No changes** permitted.

Figure 63: Restricted Context Menu Action Lock Enforcement



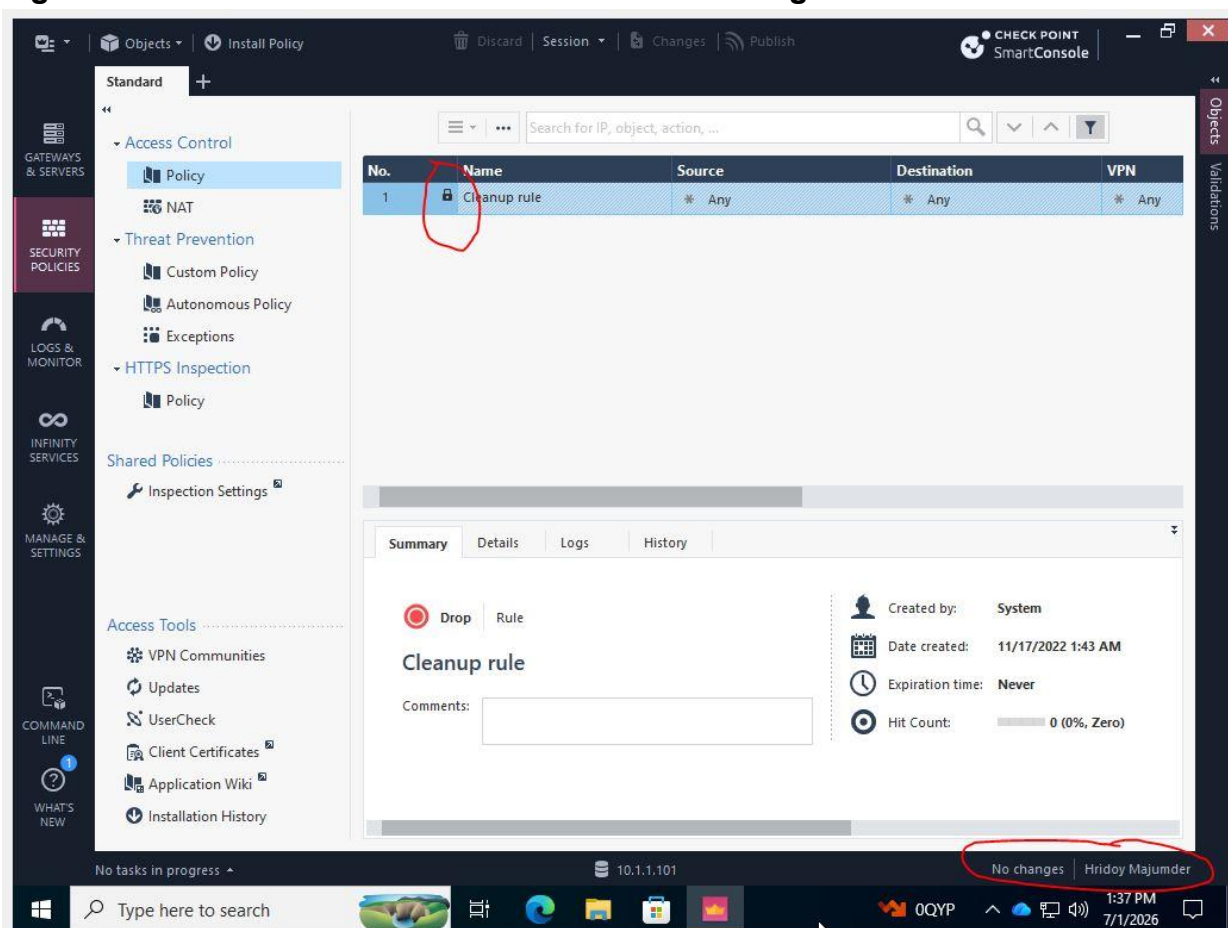
- **Description:** Access policy workspace viewed from the auditor session. The context configuration menu for the Cleanup rule greyed out and completely disabled all modification actions (*New Rule*, *Delete*, *Cut*, *Paste*), proving role-based write restrictions.

Figure 64: Active Kernel Software Blades Properties Profile



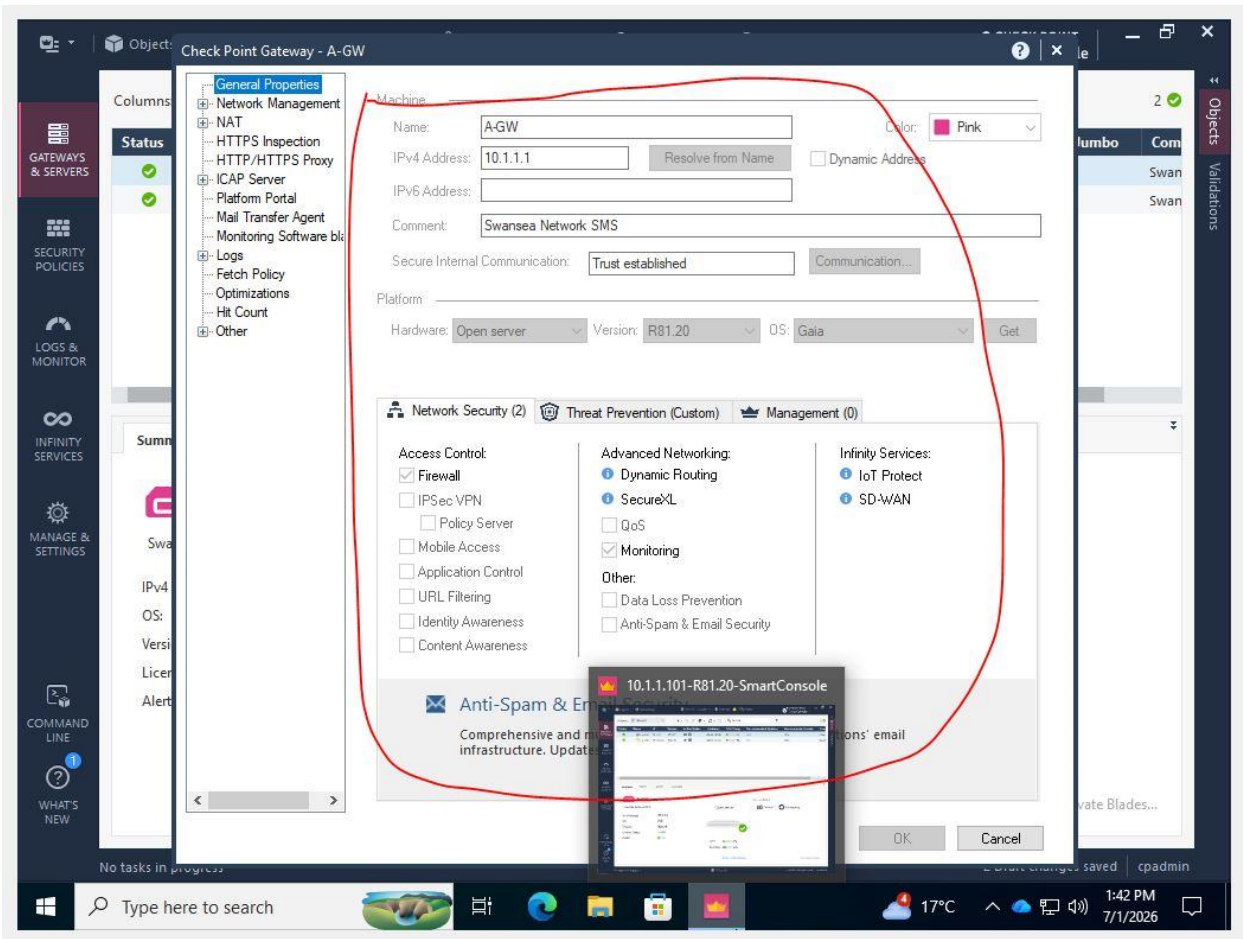
- **Description:** Detailed properties window for object A-GW. The summary checkboxes verify that the **Firewall** and **Monitoring** blades are active alongside default kernel performance acceleration via **SecureXL**.

Figure 65: Concurrent Session Modification Blocking Invariant



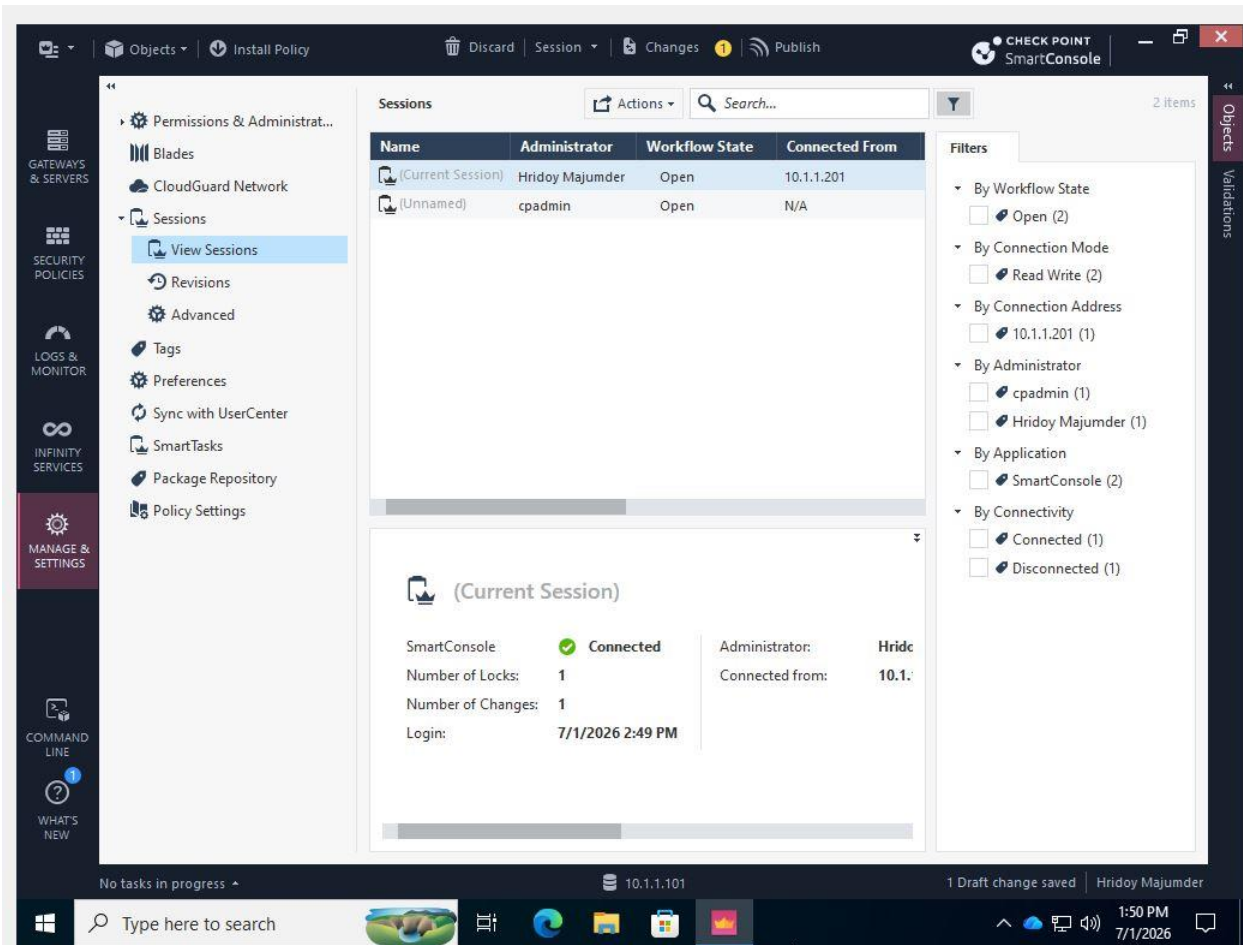
- **Description:** Access Control policy grid accessed via the secondary Super User account Hriday Majumder. The environment locks editing functions (**No changes**) and places a visual **Padlock Icon** directly next to the Cleanup rule because changes are staged in an un-published parallel session.

Figure 66: Master Session Write-Privilege Restoration



- **Description:** Return to the master account profile workspace (cpadmin). The status tracker shifts back to an open write state (2 Draft changes saved), confirming that temporary database locks clear gracefully as alternative sessions close.

Figure 67: Centralized Sessions Management Tracking Grid



- **Description:** Active connections matrix overview window. The tracking log catalogs multiple parallel sessions simultaneously (cpadmin and Hridoy Majumder), logging connection locations (10.1.1.201) and lock count metrics (Number of Locks: 1).

Phase 7: Command-Line (CLI) Diagnostics & Signature Attestation

Figure 68: Command Line Interface Contract Array Output

```
Contract Coverage:

#   ID           Expiration   SKU
=====
1 | 8YCKTIVU | 17Sep2026 | CPSB-DLP-EVAL
|Covers: CPSB-WS CPVP-SNX-U-NGX CPSB-SWB CPSB-ADNC-M CK-6B626899F274
=====
2 | 9LZMLZP | 17Sep2026 | CPSB-IPS-EVAL
|Covers: CPSB-WS CPVP-SNX-U-NGX CPSB-SWB CPSB-ADNC-M CK-6B626899F274
=====
3 | HV3LYBK | 17Sep2026 | CPSB-AV-EVAL
|Covers: CPSB-WS CPVP-SNX-U-NGX CPSB-SWB CPSB-ADNC-M CK-6B626899F274
=====
4 | IGTDRH | 17Sep2026 | CPSB-TE-EVAL
|Covers: CPSB-WS CPVP-SNX-U-NGX CPSB-SWB CPSB-ADNC-M CK-6B626899F274
=====
5 | 14432T1 | 21Sep2026 | CPSB-EVNT-5-1Y
|Covers: CPSM-C-5 CPSM-NGSM CPSB-WKFL-5 CPSB-NPM CPSB-EPM CPSB-LOGS CPS
B-MNTR CPSB-MPTL CPSB-UDIR CPSB-PRVS CPSB-COMP-5 CPSB-SME-5 CPSB-RPRT-N-C1000
CK-0BD70EC825FC
| CPSM-C-5 CPSM-NGSM CPSB-WKFL-5 CPSB-NPM CPSB-EPM CPSB-LOGS CPS
B-MNTR CPSB-MPTL CPSB-UDIR CPSB-PRVS CPSB-COMP-5 CPSB-SME-5 CPSB-RPRT-N-C1000
CK-0BD70EC825FC
=====
6 | 2RE4AF1 | 21Sep2026 | CPSB-COMP-5-1Y
|Covers: CPSM-C-5 CPSM-NGSM CPSB-WKFL-5 CPSB-NPM CPSB-EPM CPSB-LOGS CPS
B-MNTR CPSB-MPTL CPSB-UDIR CPSB-PRVS CPSB-COMP-5 CPSB-SME-5 CPSB-RPRT-N-C1000
CK-0BD70EC825FC
| CPSM-C-5 CPSM-NGSM CPSB-WKFL-5 CPSB-NPM CPSB-EPM CPSB-LOGS CPS
B-MNTR CPSB-MPTL CPSB-UDIR CPSB-PRVS CPSB-COMP-5 CPSB-SME-5 CPSB-RPRT-N-C1000
CK-0BD70EC825FC
=====
7 | 8VNER25 | 17Sep2026 | CPSB-ABOT-EVAL
|Covers: CPSB-WS CPVP-SNX-U-NGX CPSB-SWB CPSB-ADNC-M CK-6B626899F274
=====
8 | 101H60D | 21Sep2026 | CPSB-RPRT-5-1Y
```

- **Description:** Diagnostic shell screen executing low-level contract array queries. The layout lists exact SKU allocations, verifying evaluation boundaries (CPSB-IPS-EVAL, CPSB-AV-EVAL expiring on **17Sep2026**) running alongside 1-year persistent production modules (expiring on **21Sep2026**).

Figure 69: Remote PuTTY SSH Terminal Session Log (A-GW)

```
10.1.1.1 - PuTTY
login as: admin
Pre-authentication banner message from server:
| This system is for authorized use only.
End of banner message from server
admin@10.1.1.1's password:
Last login: Wed Jul 1 13:57:18 2026 from 10.1.1.101
A-GW> cplic print -x
Host           Expiration   Signature                               Features
-----
10.1.1.101     21Sep2026    dWVxzDb9iFpUFKK3Mcj3MUZFNJa35c6QXfMt CPSG-C-8
-U CPSG-C-8-U CPSB-FW CPSB-VPN CPSB-DLP CPSB-SSLVPN-U CPSB-IA CPSB-ADNC CPSB-IPS
CPSB-AV CPSB-URLF CPSB-ASPM CPSB-APCL CPSB-ABOT CK-6B626899F274
```

- **Description:** Secure command line terminal emulator window connected via SSH straight to gateway 10.1.1.1. Running the low-level diagnostic string `cplic print -x` prints the cryptographic validation certificate signature for host

10.1.1.101, proving that kernel packet inspection blades (CPSG-C-8-U) are active and authentic.