CHAPTER 4

CHECK POINT LICENSING AND CONTRACTS

YOU DESERVE THE BEST SECURITY

Learning Objectives

- Demonstrate an understanding of Check Point licenses and contracts, including purpose and structure.

- Identify the tools available to manage Check Point licenses and contracts, including their purpose and use.

License and Contracts Overview

Check Point appliances and software products must be properly licensed and activated before use.

Features	Functionality	Terms of Use
Maximum Number of Users, Devices, or IP addresses	**Signature and certification keys**	**Service entitlements**

IMPORTANT INFORMATION

Check Point software is also governed by a Download Agreement.

Before downloading Check Point software from an authorized site, you are instructed to read the agreement.

By clicking the **Download** button, you are bound by the terms and conditions of the Download Agreement.

Software Blade Packages

Offered in predefined bundles with all Software Blades included under one license.

License	Includes
Next Generation Firewall (NGFW)	Base-level protection
Next Generation Threat Prevention (NGTP)	Multi-layer threat prevention
Sandblast (SNBT)	Advanced sandboxing and Content Disarm & Reconstruction (CDR)

Software Blade Packages (Continued)

Optional Software Blades can be licensed separately. These include:

- Data Loss Prevention (DLP)

- Internet of Things (IoT) Protections

www.checkpoint.com/downloads/products/network-security-softwarebundles-at-a-glance.pdf.

IMPORTANT INFORMATION

Check Point Security Management and Security Gateway Software Blade licenses are Perpetual Blades, which means they have no expiration date.

Service blades, such as IPS, URL Filtering, and Application Control are considered Subscription Blades and their licenses can expire.

If an installed license expires, the corresponding products/features stop working. If you renew your license or install a new license, the corresponding products/features continue working again.

Software Blade Feature Summary - Security Gateway

Security Gateway	NGFW	NGTP	SNBT
Firewall	Included	Included	Included
Identity Awareness	Included	Included	Included
IPsec VPN	Included	Included	Included
Content Awareness	Included	Included	Included
Mobile Access	Included	Included	Included
IPS	Included	Included	Included
Application Control	Included	Included	Included
IoT Protection	Optional	Optional	Optional

Software Blade Feature Summary - Security Gateway (Continued)

Security Gateway	NGFW	NGTP	SNBT
DLP	Optional	Optional	Optional
URL Filtering	Not included	Included	Included
Anti-Virus/Anti-Bot	Not included	Included	Included
Anti-Spam	Not included	Included	Included
DNS Security	Not included	Included	Included
SandBlast Threat Emulation	Not included	Not included	Included
SandBlast Threat Extraction	Not included	Not included	Included
Zero-Phishing	Not included	Not included	Included

Software Blade Feature Summary - Management

Management	NGFW	NGTP	SNBT
Network Policy Management	Included	Included	Included
Logging and Status Information	Included	Included	Included

Mobile Access

- The 28000, 26000, 16000, 7000, 6000, 3000 include five users in the default package. This can be extended.

Optional Security Management Software

- SmartEvent, Compliance, SmartProvisioning, and Endpoint Policy Management are available but not listed in the table.

Standard Licenses

Central License (recommended)

- ❑ Attached to the IP address of the Security Management Server.
- ❑ Only one address needed for all licenses.

Local License

- ❑ Used for standalone devices that can manage themselves.
- ❑ For example, 6800-series devices.

PLEASE NOTE

For many solutions, Trial and Evaluation licenses are also available.

- A Trial license is generally available for 15 days.

- An Evaluation license is generally available for 30 days.

License Components

- Two primary components: Software Blade and Software Container.

Software Blade

Security feature set or module.

Examples include: Firewall, Intrusion Prevention System (IPS), and Application Control.

Each Software Blade attached to Software Container.

Software Container

Enables the Software Blade functionality and defines the Blade's purpose.

Types include: Security Management, Security Gateway, Endpoint Security.

YOU DESERVE THE BEST SECURITY
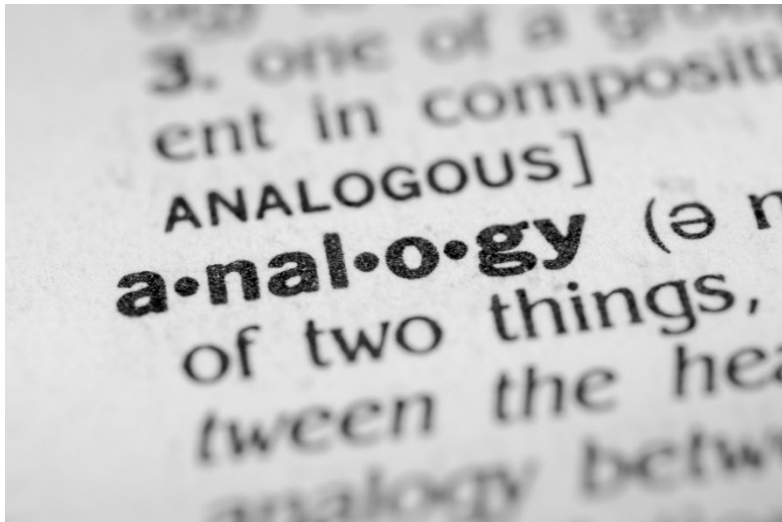
- A Software Blade is like a physical blade server.

- A Software Container is like a physical chassis.

- To enable functionality, the physical blade server must be installed in the appropriate chassis type.

First Time Activation of Licenses

Online and offline activation offered.

Online Activation

- Only available to Check Point-manufactured appliances.

- Not available to open server or virtual machines.

- Must have Internet connectivity.

- Appliance automatically pulls its own licenses.

Offline Activation

- Available to Check Point-manufactured appliances, open servers, and virtual machines.

- No Internet connectivity required.

- License files are generated from Check Point User Center and installed using SmartUpdate.

Automatic Licensing

Performs the following operations:

- Periodically verifies licenses.

- Activates new licenses added to the License & Contracts Repository.

- Automatically adds new blades to SmartConsole.

Enabled/disabled from SmartConsole Gateways & Servers view
(Application menu > Global Properties)

IMPORTANT INFORMATION

- Automatic Licensing is only supported for Check Point appliances.

- To use this feature, the Management Server must be able to connect to the Internet.

Accessing SmartUpdate

SmartUpdate is the recommended method to install licenses and contracts.

SmartConsole Gateways & Servers view:

- Application menu > Manage licenses and packages
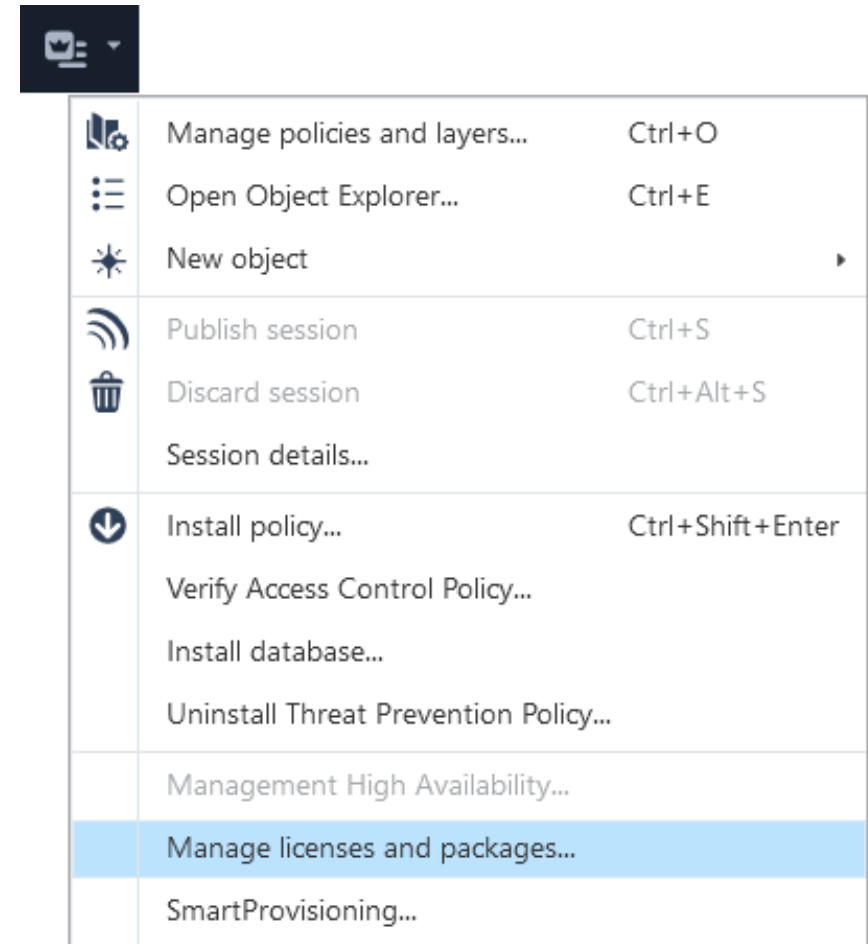
Navigate SmartUpdate - Licenses & Contracts Tab

- View license properties.

- View contracts associated to a license.

- Add a license to the License and Contract Repository.

- Attach, detach, and export a license.

Launch Menu

- Manage
  - Packages
  - Licenses & Contracts
  - Tools
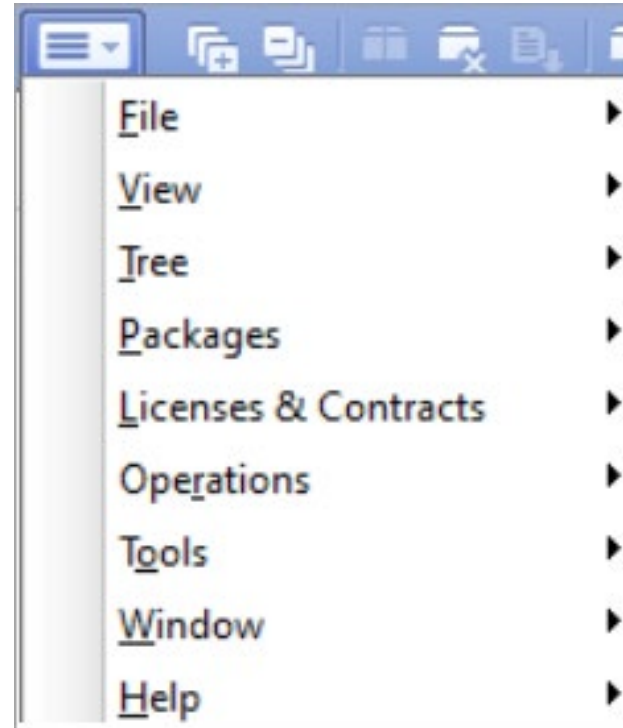
HELPFUL TIPS

You can also use icons at the top of the page. Hover over an icon to view its function.

License And Contract Repository

- Accessed from the SmartUpdate launch menu.

- Displays attached and unattached licenses.

Attached	Machine	Type	State	IP Address	Name	Description	Expiration Date
Attached	mgmt	local		1.1.1.1	CPMP-M...	Managem...	never

An attached license is associated with the Security Gateway in the License And Contract Repository.

Add and Install Licenses

From the SmartUpdate launch menu:

1. Select Licenses & Contracts → Add license.

2. Select one of these options:

   • From User Center

   • From File

   • Manually
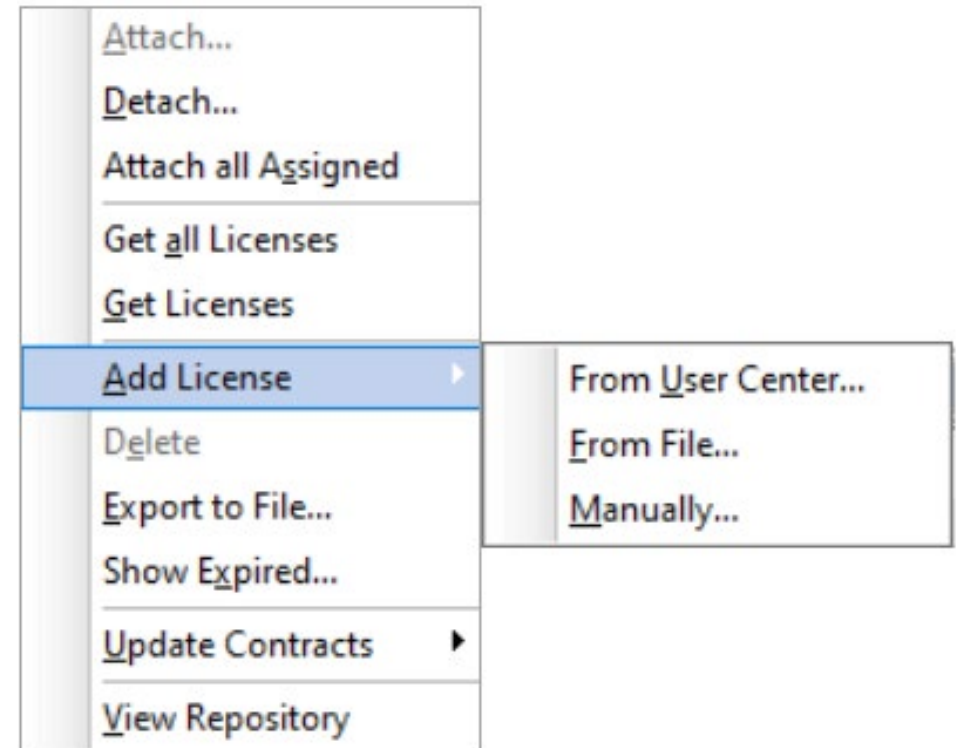
Add and Install Licenses

From User Center:

1. Use your credentials to log into User Center.

2. Take one of the following actions:

   • Generate a new license.

   • Change the IP of an existing license.

   • Change a license from Local to Central.
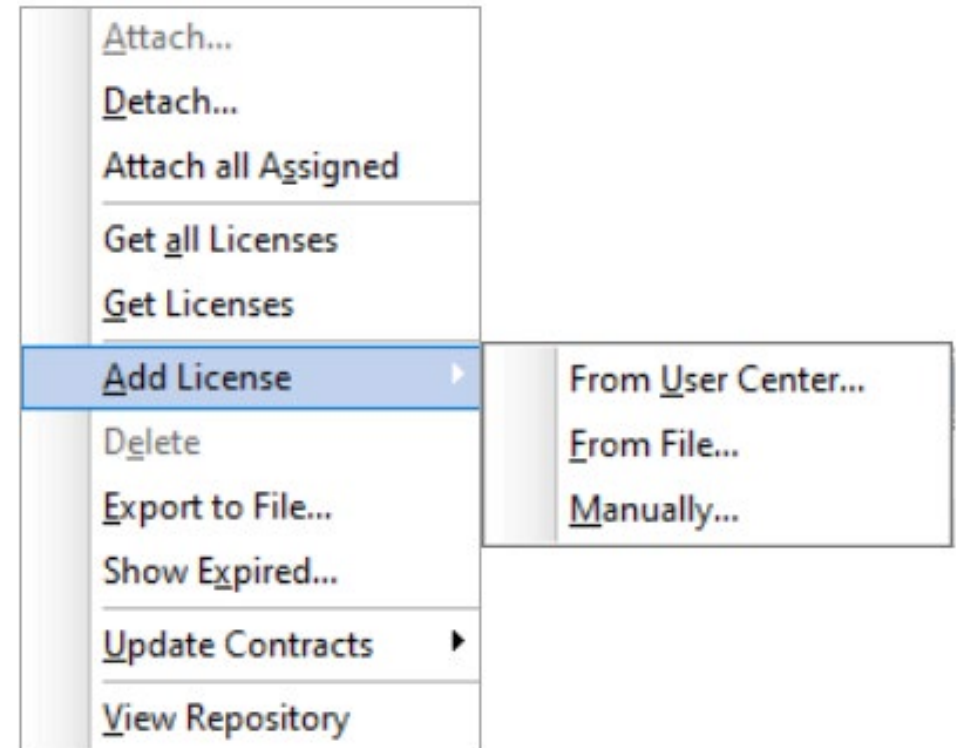
Add and Install Licenses

From File:

1. Browse to and then open **CPLicenseFile.lic**.

2. Follow the online instructions.
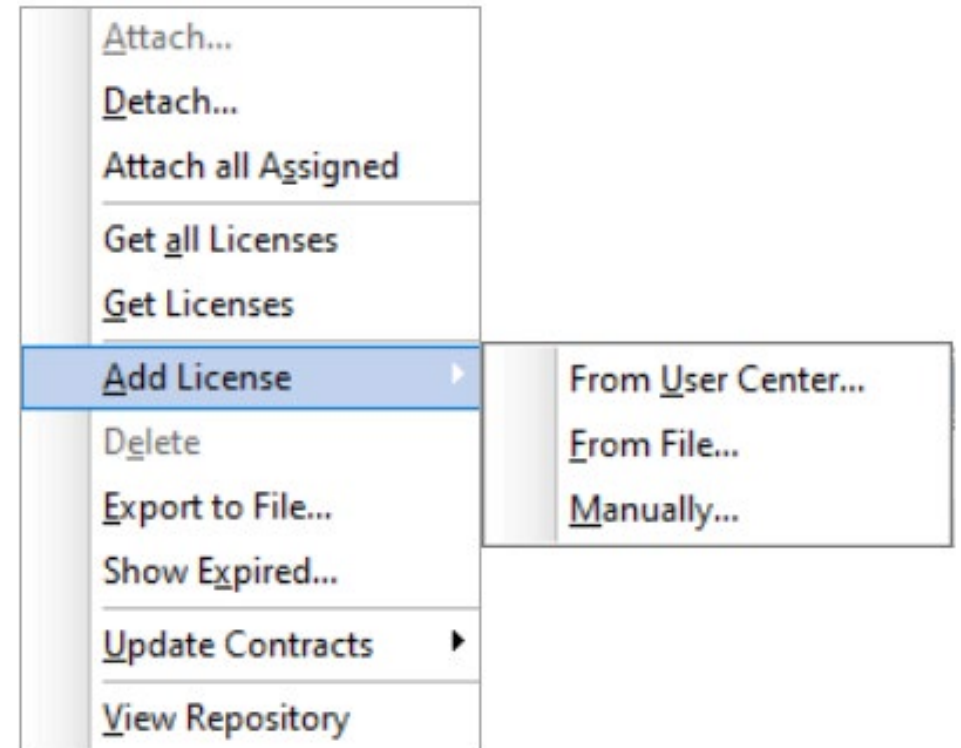
Add and Install Licenses

Manually:

1. Copy the string from the User Center email and click **Paste License**.

2. Paste the string copied from User Center.

   - If you leave the Name field empty, the license is assigned a name using this format: SKU@<*Time Date*>
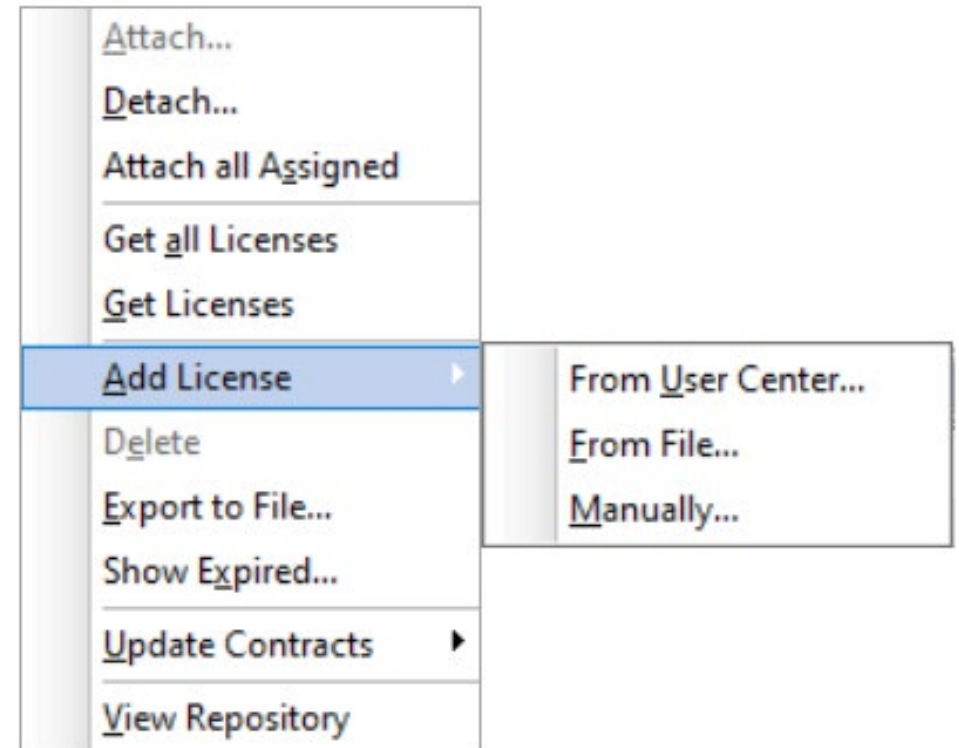
Exporting Licenses

From SmartUpdate launch menu:

1. Select **Licenses & Contracts → View Repository**.

2. Right-click a license and select **Export License to File**.

3. From the **Export license(s) to File** window:

   a) Select a destination.

   b) Type a file name.

   c) Click **Save**.
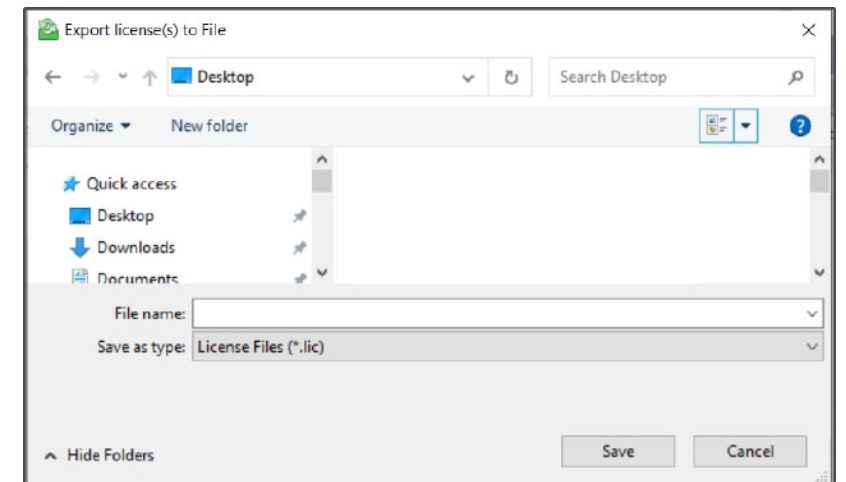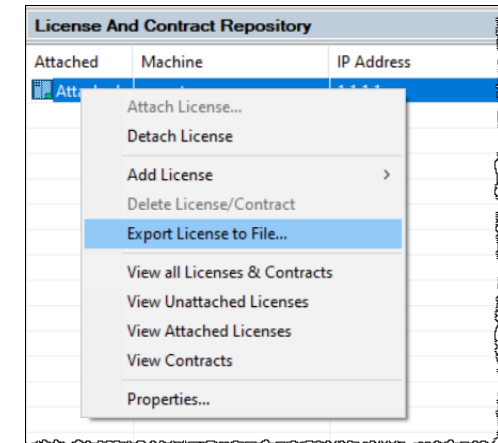
Install Service Contracts

- When a license has been activated, install a Service Contract file.

- ServiceContractFile.xml contains support data for specific devices including:

  - IPS

  - DLP

  - URL Filtering

- Install from SmartUpdate. Methods include:

  - From User Center

  - From a file

The Service Contract data is referenced whenever a Service Request (SR) is initiated or a cpinfo file needs to be forwarded to Check Point Support.

LICENSE MONITORING AND REPORTING WITH SMARTCONSOLE

License Status Indicators

✅ Green = OK (license is valid)

⚠️ Yellow = Warning
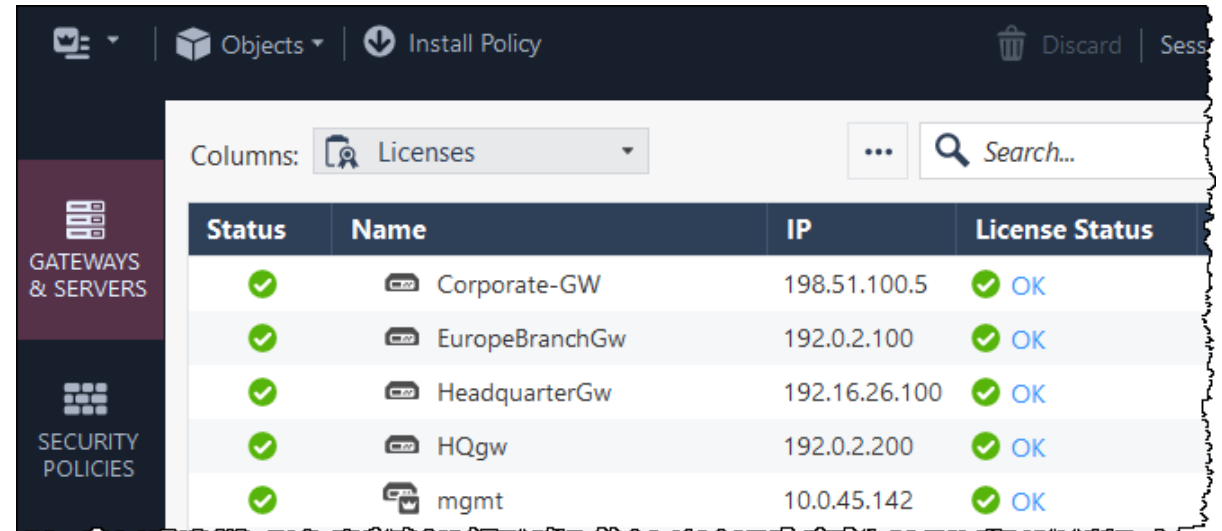
❌ Red = Critical Issue

Viewing License Status in SmartConsole

1. To see licenses for all network objects, select **Licenses** from the Columns menu.

2. View the indicators in the **License Status** column.

Viewing License Status in SmartConsole (Continued)

3. Select any network object to view additional information on the Summary tab in the bottom pane.

4. Click the **Device & License Information** link to view additional details.

Generating a License Inventory Report

From Gateways & Servers:

1. Select a network object.

2. From the top toolbar, click **Actions → License Report**.

Actions ▾

System Backup...

System Restore...

Open Shell...

Gaia Portal

Install Hotfix/Jumbo...

Version Upgrade...

License Report... ⬅

Export...

YOU DESERVE THE BEST SECURITY
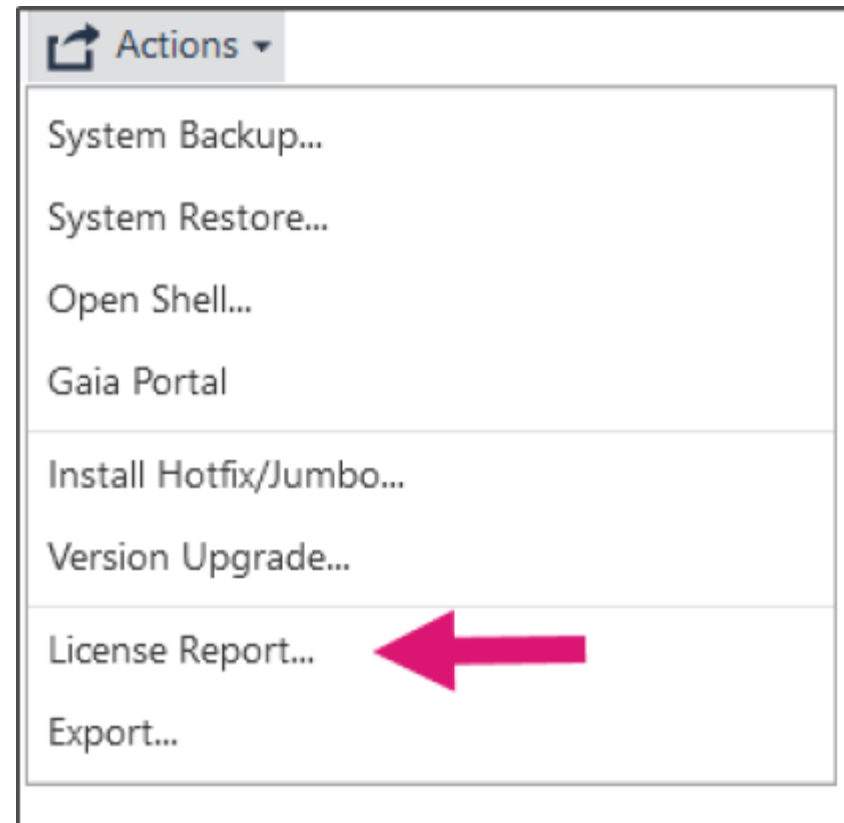
Generating a License Inventory Report (Continued)

LICENSE INVENTORY

Report

- The report includes:

  - Inventory page

  - License by Device page

- Can be exported from the Gateways & Servers view.

You can also use the SmartConsole Logs & Monitor view.

This is discussed in more detail later in this course.

Review Questions

1. Name the three types of Software Containers.

2. What are Subscription Blades?

3. Name one reason to generate and install a new license.

Lab 4A

Managing
Licenses