

CHECK POINT

Security Administration R81.20 (CCSA) Preparation Training

Delivered from Hacky Security's own curriculum, by instructors who also work our security operations centre. Classroom, online live, or at your office.

INTERMEDIATE

At a glance

COURSE	Security Administration R81.20 (CCSA)
TRACK	Check Point
DOMAIN	Cyber Security
LEVEL	Intermediate
DURATION	On request
DELIVERY	Classroom · Online live · On-site at your office
LANGUAGE	English
CLASS SIZE	Small cohorts — everyone gets lab time

WHAT IS INCLUDED

- ✓ Instructor-led delivery by practitioners who also work our SOC
- ✓ Hands-on lab access for the duration of the course
- ✓ Course materials and lab guides
- ✓ Hacky Security certificate of completion
- ✓ Post-course support by email

Who this is for

This is an intermediate course. It suits people already working in or moving into Cyber Security who want structured, hands-on preparation rather than a video library. If you are unsure whether the level fits your team, send us the job titles and we will tell you honestly — including if a different course would serve you better.

Course outline

About this course map

R81.20 is no longer Check Point's current training release. R82 is. Check Point retired the R81.20 certification exams on 30 June 2026 and replaced them with 156-215.82 for CCSA and 156-315.82 for CCSE. This map covers R81.20 because that is what this course targets, and because a great many production estates are still sitting on R81.20 and will be for some time. If what you need is the current certification rather than the skills on the estate you actually run, you will be sitting the R82 exam — tell us when you enrol and we will put you on the R82 map instead.

The eighteen topics below are Check Point's own published course topics for Certified Security Administrator R81.20, listed in the order Check Point publishes them. That order is an index rather than a teaching sequence, so the labs run in Check Point's lab order: SmartConsole first, then the Security Management Server, then the gateway, then objects, then policy. Nothing on the published topic list is left uncovered.

CCSA is an administration course. The value is not in knowing that a Shared Inline Layer exists, it is in building one, installing policy, and then reading the logs to work out why traffic did not match the rule you thought it would. Every topic below has console time attached, on a real management server and a real gateway rather than a screenshot.

Module 01 — Security Management

The management architecture that everything else in the course plugs into.

- The three-tier model: SmartConsole, Security Management Server and Security Gateway, and what each tier is responsible for
- Why Check Point separates management from enforcement, and what that buys you when a gateway fails
- Secure Internal Communication: initialising trust, the one-time password, and re-establishing SIC when it breaks
- The management database, sessions, and how concurrent administrators avoid overwriting each other
- Publishing against installing, and why the distinction catches out every new administrator once
- Discarding a session, and recovering work that was published but not installed
- Standalone against distributed deployment, and the trade-off in each direction
- Where the management server keeps its configuration, and what that means for recovery

Module 02 — SmartConsole

The administrative interface, learned properly rather than by clicking around.

- Installing and connecting SmartConsole, including the certificate warnings you should not dismiss
- The Gateways and Servers view, and reading gateway status at a glance
- The Security Policies view and how the navigation maps to the underlying rulebase
- The Logs and Monitor view, and moving from a log entry straight to the rule that matched
- The Manage and Settings view: where sessions, permissions, blades and preferences live
- The object explorer, search, and finding every rule that references a given object
- The command line inside SmartConsole, and when it is faster than the graphical interface
- Keyboard navigation and multi-select editing, which is most of the speed difference between a fast administrator and a slow one

Module 03 — Deployment

Getting management and gateway software installed, in the right topology.

- Deployment options: standalone, distributed, and management high availability, and which suits which estate
- Appliance, open server and virtual deployments, and what changes between them
- Installing a Security Management Server from the R81.20 image
- Installing a Security Gateway and running the First Time Configuration Wizard
- Interface addressing, default route and DNS during initial configuration
- Bringing a new gateway under management: creating the object, establishing SIC, fetching the topology
- Automatic and manual topology, and the anti-spoofing consequences of getting it wrong
- Verifying a fresh deployment before you put any policy on it

Module 04 — Object Management

Objects are the vocabulary of the policy. Sloppy objects produce unreadable policy.

- Network objects: hosts, networks, address ranges and groups, and when each one is the right choice
- Gateway and server objects, and the blades enabled on them
- Service objects for TCP, UDP and ICMP, and building custom services correctly
- Object naming conventions that survive a year of change, and why this matters more than it sounds
- Groups against dynamic groups, and nesting depth that stays maintainable
- Updateable objects for cloud and service provider address space, and letting Check Point maintain the contents
- Dynamic objects and where they earn their place
- Finding unused objects, and cleaning them up without breaking a rule you forgot about

Module 05 — Licenses and Contracts

The administrative layer that quietly stops a gateway working if you ignore it.

- Central against local licensing, and why central is almost always the right answer
- Attaching and detaching licences in SmartUpdate and from the command line
- Contracts, and the difference between a licence and a support or blade contract
- Blade licensing: what a licence actually unlocks on a gateway
- Licence expiry behaviour, and the symptoms you will see before anyone tells you the contract lapsed
- Evaluation licences and how to plan around their end date
- The User Center account, and keeping licence ownership tied to the organisation rather than a departed engineer
- Verifying licence state during a health check

Module 06 — Policy Rule and Rulebase

The rulebase itself: how a packet is matched, and how to write rules that say what you mean.

- Rule anatomy: source, destination, VPN, services and applications, action, track, install on, time, comment
- Top-down matching and first-match wins, and what that implies about rule order
- The implicit cleanup rule, and why you should always write your own explicit one
- Implied rules, where they sit in the order, and viewing them before you assume traffic is being dropped by your policy
- Accept, drop and reject compared, and the diagnostic difference between the last two

- Tracking options, and the cost of logging everything against the cost of logging nothing
- Disabling a rule against deleting it, and using rule hit count to find dead rules
- Writing comments that a colleague at three in the morning can act on
- Section titles and rule organisation on a rulebase that has grown past a screen

Module 07 — Policy Packages

Grouping policy so one management server can serve gateways with different jobs.

- What a policy package contains: Access Control, Threat Prevention, Desktop Security and more
- Creating a package and selecting which policy types it holds
- Assigning a package to specific gateways rather than installing everything everywhere
- Why separate packages for perimeter, internal and data centre gateways usually beats one large package
- Package-level settings and where they override or defer to global properties
- Cloning a package to stage a change, and the discipline that keeps the clone from becoming permanent
- Package revisions and rolling back to a previous state
- Installation targets, and diagnosing the package that will not install on one gateway

Module 08 — Policy Layers

The R80-and-later structure that turns a flat rulebase into something maintainable.

- Ordered Layers: how traffic passes through each layer in turn, and what happens at the end of one
- Inline Layers: attaching a sub-rulebase to a parent rule, and the parent rule as the gate
- Shared Inline Layers reused across multiple rules and multiple packages
- Implicit cleanup action on a layer, and the drop you did not intend
- Layer-level blade enablement, so Application Control lives in its own layer rather than cluttering the network layer
- Delegating a layer to a different administrator, and the permissions that makes possible
- Reading a log entry to work out which layer and which rule matched
- Migrating a flat legacy rulebase into layers without an outage
- When layers add clarity and when they are simply more places to look

Module 09 — Traffic Inspection

What the gateway actually does to a packet, and the order it does it in.

- Stateful inspection and the connections table, and why a stateless mental model will mislead you
- The inspection order across the policy layers and the blades
- SecureXL acceleration, templates, and traffic that cannot be accelerated
- CoreXL and firewall instances, and what that means when you are reading per-instance output
- Inspection settings and protocol parsers
- HTTPS Inspection: the certificate, the trust it requires on clients, and the bypass list
- Content Awareness and inspecting what is inside the flow rather than only the header
- The performance cost of each inspection layer, and choosing what to inspect deliberately

Module 10 — Network Address Translation

Translation configured properly, and diagnosed when it is not.

- Hide NAT and Static NAT, and the situation each one exists for
- Automatic NAT configured on the object, and the rules Check Point generates for you
- Manual NAT rules, and the ordering rules that automatic NAT will not give you
- Original packet against translated packet in the NAT rulebase, and reading it correctly
- NAT and anti-spoofing together, and the topology mistake that breaks both
- Proxy ARP, and when the gateway will not answer for a translated address
- Port translation and service NAT
- NAT in the log: seeing both the original and the translated connection
- Diagnosing the connection that reaches the gateway and then vanishes

Module 11 — Application Control

Identifying traffic by what it is rather than by the port it happens to use.

- The Application Control blade, the AppWiki, and what the signature database covers
- Applications, categories and custom applications, and building a rule from each
- Application risk levels, and using risk as a policy criterion
- Putting Application Control in its own Ordered Layer rather than mixing it with network rules
- Updates to the application database, and scheduling them
- Blocking an application category while permitting named exceptions
- The limits of application identification on encrypted traffic without HTTPS Inspection
- Reading Application Control logs, and tuning a rule that is catching more than you intended

Module 12 — URL Filtering

Web access control alongside Application Control, with its own failure modes.

- The URL Filtering blade and the categorisation service it depends on
- Categories, custom sites and custom groups
- Combining URL Filtering with Application Control in a single unified rule
- UserCheck: block, inform and ask pages, and writing the text users will actually read
- Handling a miscategorised site, and submitting a recategorisation
- Safe search enforcement and the settings it relies on
- What happens when the categorisation service is unreachable, and the fail-open or fail-closed decision
- Logging and reporting on web access without collecting more than your policy allows

Module 13 — Logging

Making the gateway observable, which is most of the job after the policy is written.

- Log server architecture, and separating logging from management on a busy estate
- Log against Detailed Log against Extended Log, and the storage each one costs
- Reading a log card: rule, layer, action, blade, source, destination, NAT, and the matched object
- Search and filter syntax, and building a filter you will reuse
- Log indexing and how it affects search speed on a large log store
- Views, reports and scheduling them to arrive before the meeting rather than after

- Log retention and disk management, and what happens when the log partition fills
- Forwarding logs to an external SIEM
- Moving from a log entry to the policy change that fixes the problem

Module 14 — Snapshots

A point-in-time image of the whole system, and what it is and is not for.

- What a snapshot captures compared with a backup or a migrate export
- Taking a snapshot from Gaia Portal and from clish
- Disk space required, and why snapshots are the most common cause of a full partition
- Reverting to a snapshot, and how long the system is unavailable while it happens
- Snapshots as a pre-upgrade step, and taking one before every significant change
- Exporting a snapshot off the appliance so it survives the appliance
- Hardware and version constraints on restoring a snapshot elsewhere
- Scheduling and retention, so the snapshot set does not become its own incident

Module 15 — Backup and Restore

The recovery plan you hope never to use, tested before you need it.

- The three mechanisms — backup, snapshot and migrate export — and the right tool for each scenario
- System backup: what it contains, and restoring it to the same version
- Migrate export and import, and using it to move a management database to new hardware or a new version
- Backup scheduling, and pushing backups to an SCP or FTP target automatically
- Restoring a Security Management Server and re-establishing SIC with the gateways
- Recovering a gateway, and what the management server can push back down to it
- Verifying a backup by restoring it in the lab rather than assuming
- Documenting the recovery runbook so someone other than you can execute it

Module 16 — Gaia

The operating system underneath, and enough of it to be self-sufficient.

- Gaia Portal and clish, and the tasks that are easier in each
- The clish command structure, tab completion, and save config
- Interface configuration: physical, VLAN, bond and bridge
- Static routes, and where routing is configured against where policy is configured
- DNS, NTP, hostname and domain, and why correct time underpins every log you will read
- System users, expert mode, and the boundary between Gaia and the Check Point processes
- Software updates through CPUSE: importing, verifying and installing a package
- Proxy configuration, and system health from the command line
- cpstat, cpwd_admin and the handful of commands that tell you whether the box is well

Module 17 — Permissions

Who can do what in SmartConsole, and proving it afterwards.

- Administrator accounts on the management server, and keeping them individual rather than shared
- Permission profiles, and building one per role rather than one per person

- Read, write and none, applied per feature rather than globally
- Granting write access to a single policy layer, which is how you delegate safely
- Trusted clients, restricting where an administrator may connect from
- Authentication methods for administrators, including external directory integration
- Gaia roles, which are separate from SmartConsole permissions and are often forgotten
- Auditing administrator actions, and finding who published the change that broke it

Module 18 — Policy Installation

The step that turns a saved database into enforced behaviour.

- Publish against install, revisited now that you know what is in the database
- Choosing installation targets, and installing on a subset of gateways
- The installation process: verification, compilation, transfer and activation
- Policy verification errors, and reading them rather than retrying blindly
- Installing on a cluster, and what happens to member synchronisation during install
- Failed installation and automatic rollback to the previously installed policy
- Accelerated policy installation and what it changes
- Checking the installed policy name and timestamp on the gateway itself
- Confirming enforcement with a test connection and its log entry, every time

Who should take this

Firewall and network administrators who have inherited a Check Point estate, security engineers adding Check Point to an existing skill set, and support staff who currently raise tickets against the gateway and would rather resolve them. It also suits infrastructure generalists whose employer has standardised on Quantum and who need to stop treating the management server as someone else's problem.

Check Point's stated prerequisites are working knowledge of Unix-like and Windows operating systems and of TCP/IP networking. Take that seriously: the course spends real time at a Linux shell, and delegates who have never used one lose ground on day one. You do not need prior Check Point experience.

There is no formal certification prerequisite. CCSA is the entry point of the Check Point track and the stated prerequisite for CCSE.

The exam

The CCSA R81.20 exam is set and awarded by Check Point and delivered at Pearson VUE test centres.

- Exam code 156-215.81.20
- Delivered through Pearson VUE
- Retired by Check Point on 30 June 2026, replaced by 156-215.82 for CCSA R82
- Check Point also publishes a paid practice exam, 156-609, for the R82 version

Check Point publishes question count, time limit and passing score in its own CCSA exam prep guide. We do not restate those figures here, because we will not print numbers we cannot source directly from Check Point's current published guide — download it from Check Point before you book, and confirm the figures for the exam version you are sitting.

The exam is purchased separately from Check Point. We arrange the voucher on your behalf and send you the details, and you choose your own exam date.

How we deliver it

Three days, classroom or online live, or at your office for a private group. Every delegate gets their own pod — a management server and at least one gateway they can break and rebuild — rather than sharing a demonstration, because the difference between watching a policy install and performing one is the entire course.

Topic checkpoints at the end of each day, a policy-and-NAT troubleshooting drill every morning, and a full lab scenario on the final afternoon where you are handed a broken estate and asked to find the fault and fix it.

Mapped to Check Point's published course topics for Certified Security Administrator R81.20. Taught from Hacky Security's own curriculum and lab estate by instructors who run Check Point in production. These are our own preparation courses; they are not official Check Point courseware and we are not a Check Point Authorised Training Centre.

Sitting the official exam

Exam voucher sold separately. We buy it from the certification body on your behalf and send you the code — you book your own exam date. This course is Hacky Security's own preparation training. The certification itself is awarded by the certification body, not by us.

Investment

Priced per cohort. Tell us how many people and which delivery mode and we will send a quote the same working day.

Book this course

Tell us how many people, where, and when — we will come back with dates and a quote within one working day.

+91-8091900310 • info@hackysecurity.com

<https://hackysecurity.com/courses/checkpoint-security-administration-r81-20-ccsa/>

CHANDIGARH • SHIMLA • DELHI • DUBAI • LONDON

Independent preparation training delivered from Hacky Security's own curriculum. Hacky Security Private Limited is not affiliated with or endorsed by the certification body named in this document. Certification names and codes are the trademarks of their respective owners and are used only to describe what this course prepares you for. Prices, durations and outlines are indicative and may change; the quotation we send you is the binding one. Issued 12 September 2026.