OneLayer & Check Point Integration Guide

Identity Awareness Configuration for Private Cellular Networks

Document Version	1.0
Date	April 2026
Classification	Customer Confidential

Overview

OneLayer and Check Point integrate to deliver identity-aware security for LTE and 5G private cellular networks. OneLayer provides real-time device visibility, identification, and context enrichment. Check Point's Identity Awareness blade consumes this enrichment data and makes device identity context available to the Access Control policy engine, enabling identity-based enforcement.

OneLayer Bridge integrates with the cellular packet core to identify and fingerprint every device on the private cellular network. Device context—including IMEI, IMSI, IP address, device type, and group membership—is pushed to Check Point Security Gateways via the Identity Awareness Web API. The Check Point firewall team then uses this enriched device context to build and enforce identity-based access control policies tied to the actual device, not just its IP address.

> *Responsibility model: OneLayer is responsible for device discovery, fingerprinting, and identity enrichment. All policy creation, enforcement, and firewall rule management is the responsibility of the customer's networking and security team using Check Point SmartConsole.*

This integration addresses the unique security challenges of private cellular networks and IoT devices. OneLayer surfaces device identity and context that would otherwise be invisible to the firewall, enabling the customer's security team to make informed enforcement decisions.

Architecture Overview

The OneLayer Bridge integrates with the cellular packet core, on both the control and data planes. OneLayer OneID identifies and fingerprints devices, correlating their cellular identifiers (IMEI, IMSI) to their IT network identifiers (IP address, MAC address). This enrichment provides full device context for all devices on the private cellular network—including devices behind cellular routers.

Device context and identity information is shared with Check Point Security Gateways via the Identity Awareness Web API. OneLayer pushes identity-to-IP mappings and device metadata, providing the Check Point firewall with the enriched context needed to support identity-based access control. The customer's security team is responsible for creating and managing the firewall rules and policies that leverage this data.

> *Note: The Identity Awareness Web API uses the REST protocol over HTTPS. OneLayer pushes device context data directly to the Check Point Security Gateway—no additional agents or collectors are required. OneLayer provides the enrichment layer; all enforcement decisions and policy management remain under the customer's control.*

Integration Data Flow

The integration operates in the following sequence:

1. OneLayer Bridge discovers and fingerprints devices on the private cellular network.
2. Device identity data (user/device name, IP address, device type, group membership) is mapped by OneLayer OneID.
3. OneLayer pushes identity-to-IP mappings to the Check Point Security Gateway via the Identity Awareness Web API (HTTPS POST to the gateway's /_IA_API endpoint).
4. Check Point Security Gateway associates the identity data with the corresponding IP addresses. The customer's security team can then leverage this context in access control policies.
5. When device properties change (IP reassignment, SIM swap, device removal), OneLayer automatically updates or removes the identity mapping on the Check Point gateway.

Prerequisites

Before configuring the integration, verify the following requirements are met:

Requirement	Details
Check Point Gateway	Security Gateway running Gaia OS R81 or later with a valid license for the Identity Awareness blade.
SmartConsole	SmartConsole installed and connected to the Security Management Server managing the target gateway.
OneLayer Bridge	OneLayer Bridge deployed and connected to the private cellular packet core, with devices discovered and fingerprinted.
Network Connectivity	HTTPS (TCP port 443) connectivity from the OneLayer Bridge to the Check Point Security Gateway management interface.
Credentials	Administrative access to both SmartConsole and the OneLayer dashboard.

Check Point Configuration

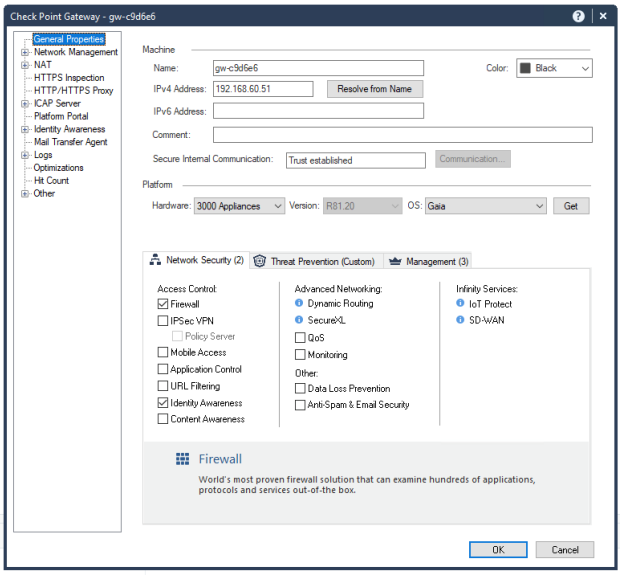
The Check Point configuration consists of three steps: enabling the Identity Awareness blade, configuring the Identity Web API as an identity source, and installing the access control policy. Both SmartConsole (GUI) and CLI methods are provided.

Step 1 — Enable the Identity Awareness Blade

The Identity Awareness blade must be enabled on the Security Gateway that will receive device identity data from OneLayer.

SmartConsole (GUI):

1. Open SmartConsole and log in to the Security Management Server.
2. In the left navigation panel, click Gateways & Servers.
3. Double-click the Security Gateway object to open its properties.
4. In the General Properties pane, locate the Network Security tab.
5. Check the box next to Identity Awareness to enable the blade.



6. The Identity Awareness First Time Configuration Wizard opens.
7. On the Methods For Acquiring Identity page, you may optionally configure an Active Directory domain if AD integration is required for your environment. For the OneLayer integration, the primary identity source is the Identity Web API (configured in Step 2).
8. Click Finish to close the wizard.
9. Click OK to save the gateway object.

> *Note: You do not need to configure Active Directory integration for the OneLayer integration to work. The Identity Web API is the sole identity source used by OneLayer. However, if your environment already uses AD-based identity sources, they will coexist with the Web API source.*

CLI Alternative (Expert Mode):

To verify the Identity Awareness blade status from the gateway CLI:

```
cpstat identityServer
```

This command returns the current status and statistics for the Identity Awareness daemon on the gateway.

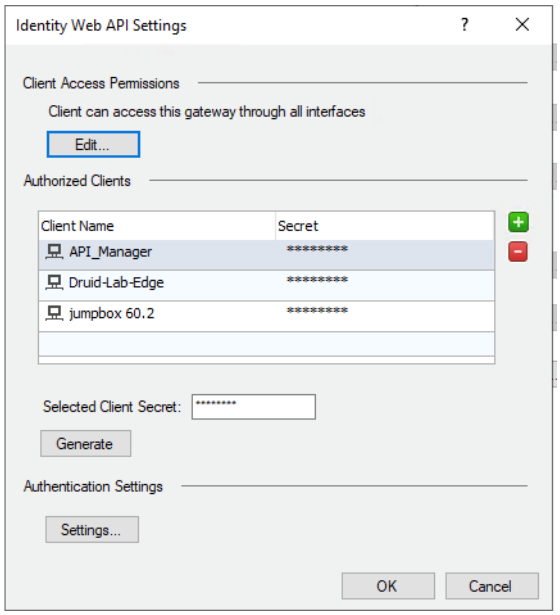
Step 2 — Configure the Identity Web API

The Identity Web API is the identity source that allows OneLayer to push device-to-IP mappings directly to the Check Point Security Gateway via HTTPS REST calls.

SmartConsole (GUI):

1. In SmartConsole, double-click the Security Gateway object to open its properties.
2. In the left pane, click Identity Awareness.
3. In the Identity Sources section, check the box next to Identity Web API.
4. Click Settings next to the Identity Web API option.

The Identity Web API Settings window opens.



Configure Client Access Permissions:

5. In the Client Access Permissions section, click Edit.
6. Select the Security Gateway interfaces that should accept connections from the OneLayer Bridge. Choose the interface(s) connected to the network where OneLayer Bridge resides.
7. Click OK to save the interface selection.

Configure Authorized Clients:

8. In the Authorized Clients section, click the + (Add) icon.
9. Add the OneLayer Bridge host object. If the object does not exist, create a new host object with the OneLayer Edge's IP address.
10. Select the OneLayer Bridge entry in the Authorized Clients list.

11. Click Generate to create a shared secret, or enter a shared secret manually. Record this shared secret—it is required for the OneLayer configuration in Step 2 of the OneLayer Configuration section.

> *Important: The shared secret is displayed only once when generated. Copy and store it securely. This secret will be entered in the OneLayer dashboard to authenticate API calls to the Check Point gateway.*

12. Click OK to close the Identity Web API Settings window.
13. Click OK to save the gateway object.

CLI Alternative (Expert Mode):

To verify the Identity Web API is listening on the gateway:

```
netstat -tlnp | grep 443
```

You can also test the API endpoint from the OneLayer Bridge server using curl:

```
curl -k -X POST https://<GATEWAY_IP>/_IA_API/v1.0/show-identity \
  -H "Content-Type: application/json" \
  -d '{"shared-secret":"<YOUR_SHARED_SECRET>","ip-address":"<TEST_IP>"}'
```

> *Note: The -k flag disables certificate verification for testing. In production, use a valid certificate or configure the OneLayer Bridge to trust the gateway's certificate.*

Step 3 — Publish and Install Policy

After enabling Identity Awareness and configuring the Identity Web API, publish the SmartConsole session and install the Access Control policy on the gateway.

SmartConsole (GUI):

1. In SmartConsole, click Publish (top toolbar) to save the session.
2. Click Install Policy.
3. Select the Access Control policy and the target Security Gateway.
4. Click Install.

CLI Alternative (mgmt_cli):

From the Security Management Server CLI:

```
mgmt_cli publish -s <session-id>
mgmt_cli install-policy policy-package "Standard" access true \
  threat-prevention false targets "<gateway-name>"
```

> *Important: The Identity Web API becomes active only after the Access Control policy is installed on the gateway. Any configuration changes to Identity Awareness settings require a policy reinstall.*

Step 4 (Optional) — Create Identity-Based Access Rules

Once the integration is active, the customer's security team can create firewall rules that reference the device context and identity data provided by OneLayer. This step is the customer's responsibility and can be configured at any time based on the organization's security requirements.

> *Note: Policy creation and enforcement are entirely under the customer's control. OneLayer provides the device identity context; the customer's networking and security team defines what actions to take based on that context.*

SmartConsole (GUI):

1. Navigate to Security Policies > Access Control > Policy.
2. Add a new rule or edit an existing rule.
3. In the Source or Destination column, click the + icon.
4. Select Access Role from the object type list.
5. Create or select an Access Role object that references the identity users or groups pushed by OneLayer.
6. Define the desired Action (Accept, Drop, etc.) and other rule parameters.
7. Publish and install the policy.

Identity-based rules allow the Check Point gateway to enforce policies based on device identity rather than IP address. When OneLayer updates the device-to-IP mapping (for example, after an IP reassignment), the customer's firewall rules automatically apply to the new IP—without requiring manual policy changes.

OneLayer Configuration

After completing the Check Point gateway configuration, configure the OneLayer Bridge to push identity data to the Check Point Security Gateway.

Step 1 — Navigate to Integrations

1. Log in to the OneLayer dashboard.
2. In the left navigation menu, go to the Integrations page.
3. Locate Check Point in the Security integrations section and click on it.

Step 2 — Configure the Check Point Integration

On the Check Point integration page, configure the following fields:

Field	Description
Gateway IP / FQDN	The IP address or fully qualified domain name of the Check Point Security Gateway. This is the gateway where the Identity Awareness Web API is enabled.
Shared Secret	The shared secret generated or configured in Step 2 of the Check Point Configuration (Authorized Clients section). This authenticates OneLayer API calls to the gateway.

1. Enter the Gateway IP / FQDN of the Check Point Security Gateway.
2. Enter the Shared Secret obtained from the Check Point Identity Web API configuration.
3. Click Test to verify connectivity and authentication to the Check Point gateway.
4. Click Activate to enable the integration.

Verification

After activating the integration, verify that device identity data is flowing from OneLayer to Check Point.

Verify in SmartConsole

1. In SmartConsole, open the Logs & Monitor view.
2. In the Logs & Monitor view, filter by the Identity Awareness blade to query identity events.
3. Confirm that device identities pushed by OneLayer appear with the correct IP-to-identity mappings.

Verify from the Gateway CLI

From the Security Gateway Expert Mode shell, run the following command to display current identity mappings:

```
pep show user all
```

This command lists all identity-to-IP associations currently held by the gateway. Verify that devices discovered by OneLayer appear with their expected identifiers.

To view Identity Awareness daemon status and statistics:

```
cpstat identityServer
```

Verify in OneLayer Dashboard

1. In the OneLayer dashboard, navigate to the Integrations page.
2. Confirm that the Check Point integration shows an Active status.
3. Verify the Last Change timestamp reflects recent synchronization activity.

Troubleshooting

Issue	Resolution
OneLayer Test button fails	Verify HTTPS (port 443) connectivity from the OneLayer Bridge to the Check Point gateway. Confirm the gateway IP/FQDN is correct. Ensure the Identity Awareness blade is enabled and the Access Control policy has been installed.
Authentication error (shared secret rejected)	Confirm the shared secret entered in OneLayer matches the secret configured in the Check Point Identity Web API Authorized Clients section. Regenerate the secret if necessary and update both sides.
Identity mappings not appearing on the gateway	Verify the Identity Web API is enabled in the gateway object's Identity Awareness settings. Check that the correct gateway interface is selected in Client Access Permissions. Reinstall the Access Control policy after any configuration changes.
Policies not matching identity-based rules	Confirm that Access Role objects in the firewall rules reference the correct identity users/groups. Verify that the OneLayer integration is active and pushing current device data. Use "pep show user all" on the gateway CLI to confirm identity associations.
Certificate warnings during API calls	The Check Point gateway uses a self-signed certificate by default. Configure the OneLayer Bridge to trust the gateway's CA certificate, or replace the gateway certificate with one signed by a trusted CA.

Important Notes

Responsibility Model

OneLayer Responsibility	Customer Responsibility
Device discovery and fingerprinting on the private cellular network	Firewall policy creation, management, and enforcement using Check Point SmartConsole
Identity enrichment: correlating IMEI, IMSI, IP, device type, and group membership	Defining access control rules and Access Role objects that leverage OneLayer-provided context
Pushing device-to-IP identity mappings to the Check Point gateway via the Identity Awareness Web API	Publishing and installing firewall policies on the Security Gateway
Automatic updates when device properties change (IP reassignment, SIM swap, device removal)	Monitoring enforcement outcomes and adjusting policies as needed
Device group management in the OneLayer dashboard	Network connectivity and firewall infrastructure maintenance

Additional Notes

OneLayer provides context and enrichment—not enforcement. OneLayer discovers, fingerprints, and maps device identities to IP addresses. This context is delivered to the Check Point gateway. All decisions about what to allow, block, or restrict based on this context are made by the customer's security team through Check Point firewall policies.

OneLayer is the authoritative source for device identity data. Device identity mappings are managed exclusively by OneLayer Bridge. Manual changes to identity data on the Check Point gateway may be overwritten during the next synchronization cycle.

Identity updates are automatic. When a device's IP address changes (for example, due to DHCP renewal or roaming), OneLayer automatically updates the identity-to-IP mapping on the Check Point gateway. The customer's firewall rules referencing the device identity continue to apply to the updated IP without manual intervention.

Session timeout behavior. Identity mappings pushed via the Web API include a session timeout. OneLayer refreshes these mappings periodically to ensure they remain active. If the OneLayer Bridge loses connectivity to the gateway, existing mappings will expire after the configured timeout period.

Coexistence with other identity sources. The Identity Awareness blade can operate multiple identity sources simultaneously (AD Query, Identity Collector, Web API, etc.). OneLayer's Web API identity source coexists with any other configured identity sources on the same gateway.