OpenRoaming firewall rules

OpenRoaming firewall rules

The Cisco Spaces Connector and OpenRoaming integration path require reachability to OpenRoaming, OpenRoaming services, and RadSec endpoints. For controller-based deployments, allow controller-to-connector RADIUS traffic. For connector cloud access and Meraki RadSec, allow the required outbound paths. If direct internet access is restricted, configure the required ports, FQDNs, and Meraki RadSec HAProxy IP destinations on the firewall, DNS security service, proxy, or SSL inspection device.

Note

- Apply these allowlists before enabling the Hotspot service or associating an OpenRoaming profile with a controller or Meraki network.
- Validate DNS resolution and outbound connectivity from the same network path used by the connector, controller, Meraki APs, or Meraki API integration.

Table 1: OpenRoaming Firewall Rules

Traffic / service	Requirement
Cisco Spaces or OpenRoaming cloud	Allow HTTPS or TCP 443 to the regional Cisco and OpenRoaming domains.
Controller to Connector RADIUS	For controller-based deployments, allow Cisco AireOS/Catalyst controller traffic to the OpenRoaming Connector on UDP/TCP 1812 and 1813 for OpenRoaming RADIUS messages.
RADSec	Allow TCP 2083 where RADSec-secured authentication is used.

Traffic / service	Requirement
Meraki AP RadSec	For Meraki deployments, allow Meraki AP outbound TCP 2083 to the applicable OpenRoaming RadSec HAProxy IP destination listed in the Meraki RadSec IP allowlist.
RADIUS	Allow UDP 1812 and UDP 1813 where customer RADIUS authentication/accounting flows are used.
DNS	Required FQDNs must resolve from the connector/controller/API egress network.
Proxy or SSL inspection	Bypass or explicitly trust required OpenRoaming service traffic. Proxy authentication, TLS inspection, or certificate substitution can prevent onboarding even when DNS resolution succeeds.

Meraki RadSec IP allowlist

For Meraki deployments, Meraki APs must have outbound connectivity over TCP 2083 to the applicable OpenRoaming RadSec HAProxy IP destination below. Allow the destination that corresponds to the Cisco Spaces environment used by the deployment.

Table 2: Meraki RadSec IP allowlist

Cisco Spaces environment	Meraki AP outbound HAProxy destination	Port
US or IO	184.73.46.220	TCP 2083
EU	63.33.180.45	TCP 2083
SG	54.169.186.118	TCP 2083

Domains to allowlist

Allow the FQDNs that apply to the Cisco Spaces tenant, connector, and OpenRoaming service path.

Table 3: Domains to allowlist

Domain allowlist
cisco.openroaming.org
cisco.openroaming.net
connector.dnaspaces.io
location.dnaspaces.io

Domain allowlist
idp.openroaming.net
sdk.openroaming.net
google.openroaming.net
apple.openroaming.net
samsung.openroaming.net
connect.ciscospaces.io
connector.dnaspaces.eu
location.dnaspaces.eu
eu-prod.openroaming.net
eu-sdk.openroaming.net
eu-google.openroaming.net
eu-apple.openroaming.net
connect.ciscospaces.eu
connector.ciscospaces.sg
location.ciscospaces.sg
sg-prod.openroaming.net
sg-sdk.openroaming.net
sg-google.openroaming.net
sg-apple.openroaming.net
connect.ciscospaces.sg

Carrier offload domain allowlist

Use this allowlist only when carrier offload is enabled in the OpenRoaming profile. These domains are not required for a standard OpenRoaming deployment without carrier offload.

Note Add only the carrier rows that match the enabled carrier offload providers to the firewall and DNS allowlists.

Table 4: Carrier Offload Domain Allowlist

Carrier	When to allowlist	Domains
AT&T-US	Required only when AT&T-US carrier offload is enabled.	wlan.mnc150.mcc310.3gppnetwork.org wlan.mnc280.mcc310.3gppnetwork.org wlan.mnc100.mcc313.3gppnetwork.org wlan.mnc410.mcc310.3gppnetwork.org
T-Mobile-US	Required only when T-Mobile-US carrier offload is enabled.	wlan.mnc120.mcc310.3gppnetwork.org wlan.mnc530.mcc312.3gppnetwork.org wlan.mnc490.mcc310.3gppnetwork.org wlan.mnc260.mcc310.3gppnetwork.org wlan.mnc160.mcc310.3gppnetwork.org