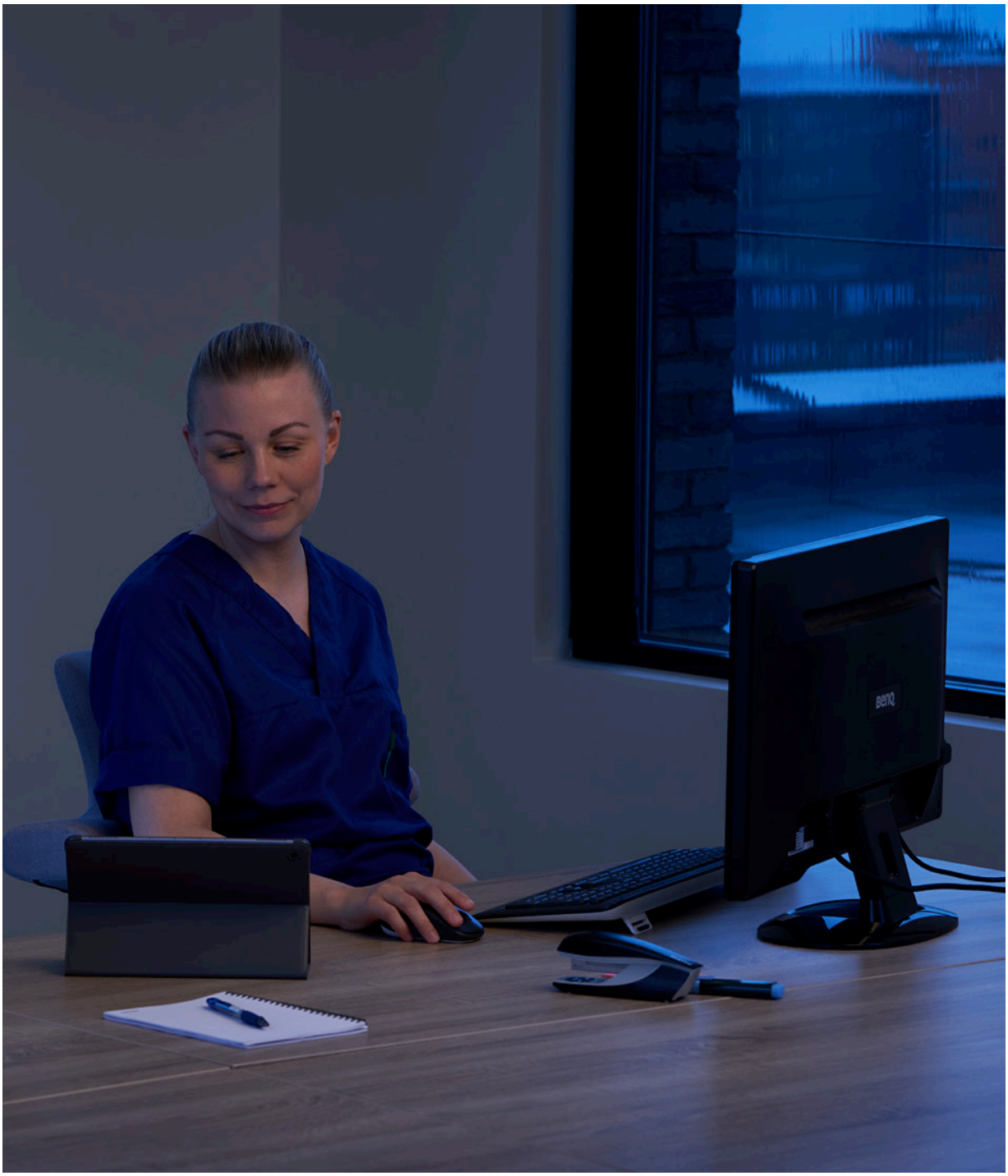
Night Owl Firewall and Network Settings



Contents

Backend communication and supervisory connection

IP	Gate	Features
nest.nattugla.no <your endpoint>.nattugla.no	TCP: 443	Nest Service
stun-turn.nattugla.no	TCP: 443 TCP/UDP: 3478	STUN/TURN

Other Services

NTP Time Server

IP	Gate	Features
2.android.poolntp.org	UDP/123	Server for clock synchronisation

Google FCM

Taken from Google's documentation:
Traffic to these endpoints should also bypass SSL inspection. SSL intercepted traffic to Google services are often interpreted to be person-in-the-middle attacks and are blocked.

For Supervisory Control:

FQDN	Ports
mtalk.google.com mtalk4.google.com mtalk-staging.google.com mtalk-dev.google.com alt1-mtalk.google.com alt2-mtalk.google.com alt3-mtalk.google.com alt4-mtalk.google.com alt5-mtalk.google.com alt6-mtalk.google.com alt7-mtalk.google.com alt8-mtalk.google.com android.apis.google.com device-provisioning.googleapis.com firebaseinstallations.googleapis.com fcm.googleapis.com fcm-xmpp.googleapis.com	TCP: 5228-5230, 443

ESPER (MDM Systems)

Esper is our management system for Night Owl.
If the firewall does not support wildcards, or you need static addresses, please refer to: Firewall: Esper Static rules.
The list below reflects recent changes made by Esper to rule designs and descriptions.

FQDNs	Wildcard	Ports	Features
*.amazonaws.com	*.amazonaws.com	TCP: 443 (HTTPS), TCP: 8883 (MQTT)	For provisioning, app management and device management
mqtt.shoonyacloud.com	*.shoonyacloud.com	TCP: 1883 (MQTT)	For MQTT communication with devices
services.shoonyacloud.com		TCP: 443 (HTTPS)	For Provisioning services and Remote Viewer APK
turn.shoonyacloud.com		TCP/UDP: 3478 (SCTP) TCP/UDP: 5349 (SCTP) UDP: 49152 -65535	For Remote Viewer and Remote Control services
authn2.esper.cloud	*.esper.cloud	TCP: 443 (HTTPS)	For Single Sign-on (SSO).
id.esper.cloud	*.esper.cloud	TCP: 443 (HTTPS)	For Single Sign-on (SSO).
ping.esper.cloud	*.esper.cloud	TCP: 443 (HTTPS)	Checks device's internet connectivity.
qhavr.esper.cloud	*.esper.cloud	TCP: 443 (HTTPS)	Grants access to the Esper Console when operating under a network with a restricted outbound firewall.
qhavr-api.esper.cloud	*.esper.cloud	TCP: 443 (HTTPS)	For communicating from the device to the Esper tenant. (example: device status events and command success/ failure messages).
mqtt.esper.cloud	*.esper.cloud	TCP: 443 (HTTPS)	For MQTT communication to devices for commands (with TLS).
downloads.esper.io	*.esper.cloud	TCP: 443 (HTTPS)	Need for standalone Esper Agent updates.
statserv.esper.cloud	*.esper.cloud	TCP: 443 (HTTPS)	Sends deployment stats and provisioning failures to Esper monitoring systems.
eea-sentry.esper.cloud	*.esper.cloud	TCP: 443	Sends telemetry data to Sentry.
dpcdownloads.esper.cloud	*.esper.cloud	TCP: 443 (HTTPS)	For the Remote Viewer APK

13.52.132.230	N/A	TCP: 40000-50000	For allowing secure remote ADB access to your devices and the Esper CLI.
shoonya-firebase.firebaseio.com, *.crashlytics.com, crashlyticsreports-pa.googleapis.com, firebasecrashlyticssymbols.googleapis.com https://8.8.8.8/generate_204	*.firebaseio.com *.crashlytics.com *.googleapis.com 8.8.8.8	TCP: 443 (HTTPS) TCP: 5228 (HTTPS) TCP: 5229 (HTTPS) TCP: 5230 (HTTPS)	Firebase/Crashlytics. Used to send crash reports.
		TCP: 443 (HTTPS)	Checks device's internet connectivity.
mqtt-telemetry-prod.esper.cloud	*.esper.cloud	TCP: 1883	MQTT communication to devices for commands (with TLS).
clients3.google.com/generate_204	N/A	Port: 443 (HTTPS)	Checks device's internet connectivity. Note: Only required for devices running Esper Agent Version 7.8.7060 and below.
firebaseinstallations.googleapis.com, fcm.googleapis.com	*.googleapis.com	TCP: 443 (HTTPS) TCP: 5228 (HTTPS) TCP: 5229 (HTTPS) TCP: 5230 (HTTPS)	Used to send commands and pings to wake up devices.

Static rule changes

If you're unable to use wildcards in the firewall *.amazonaws can be used instead.

FQDN	Port	Notes
mqtt.esper.cloud	TCP:8883 (MQTT over ssl)	This is an additional port on the existing entry
streamer.esper.io	TCP: 443	

Terminology

FQDN	Ports
Communication Channels	Customers interact with their devices by sending commands using the Esper Console or APIs. In either case, all communication to their devices are routed via one of four communication channels that a device can use. These channels are: • AWS IOT Core • FCM (Google Managed) • MQTT • HTTP
FQDN (Fully Qualified Domain Name)	A complete domain name that specifies the exact location of a resource in a hierarchical DNS (Domain Name System) structure.
HTTP (Hypertext Transfer Protocol)	A protocol used for transmitting and receiving hypertext documents on the World Wide Web. HTTP is the foundation of data communication on the internet and defines how web browsers and servers interact.
HTTPS	Hypertext Transfer Protocol Secure. A secure version of HTTP that uses encryption to protect the data transmitted between a web browser and a web server.
MQTT	Message Queuing Telemetry Transport. A lightweight publish-subscribe messaging protocol designed for low-bandwidth, high-latency, or unreliable networks. MQTT is commonly used in IoT (Internet of Things).
NTP	Network Time Protocol. A protocol used to synchronize theclocks of systems on a network. NTP ensures that all systemshave accurate and synchronized time.
SCTP	Stream Control Transmission Protocol. A transport layerprotocol that combines some of the features of both TCP and UDP. SCTP offers reliable, ordered, and multiplexed data transmission with congestion control and error detection

FQDN	Ports
SNTP	Simple Network Time Protocol. A simplified version of NTP that provides basic time synchronization capabilities. SNTP is often used in situations where high accuracy is not critical.
SSL	Secure Sockets Layer. A cryptographic protocol that is used to establish secure and encrypted connections between a client and a server.
Stack	A stack is a physically isolated infrastructure which can be used to create multiple customer Tenants. All customer Tenants in a stack share the same compute and storage resources.
TCP	Transmission Control Protocol. A connection-oriented communication protocol that provides reliable and ordered data delivery between two systems over a network.
UDP	An FQDN that can stand in for other FQDNs. It allows all variations of the subdomain. For example, the FQDN wildcard *.esper.cloud would allow dpc downloads.esper.cloud, ping.esper.cloud, mqtt.esper.cloud, etc.

Installation

Please see our in-depth guides to assist you with installation:

Installation

Link goes here

Alarm settings

Link goes here

Anonymisation

Link goes here

Furniture scanning

Link goes here

Firewall and network

Link goes here

Alarm testing

Link goes here