Gateway User Manual
Model GW3

Contents

Introduction .................................................. 2
About the Gateway ........................................ 2
Safety Information ......................................... 2
Installation .................................................... 3
    Preparation ............................................. 3
    Assembling the Gateway ......................... 3
Powering On the Gateway ............................. 3
    Connect the Gateway to Your Network ....... 4
    Positioning the Gateway .......................... 4
Additional Information .................................. 6
    Network Priority ................................... 6
    Maintenance and Post-Installation .......... 6
Specifications .............................................. 6
Certifications .............................................. 6
Appendix 1: Declarations of Conformity ........... 8
Appendix 2: Platform Network Summary ....... 10
Introduction

This manual provides instructions for installing the Elemental Gateway-3, GW3, referred to as “The Gateway”, as part of the Elemental Machines System. It includes additional supplementary information regarding security, specifications, and certifications.

About the Gateway

The Elemental Gateway receives data from Elemental Machines “Elements” and communicates to the Elemental Machines Cloud via Ethernet, Wi-Fi, and Cellular data connections. The Gateway is primarily powered using an AC wall adapter, but contains a battery backup which can maintain data connections during power outages.

The Gateway contains an LED Status panel, two antennas, an ethernet port, and magnetic feet for secure placement.

Safety Information

Batteries

WARNING: The Gateway contains a rechargeable lithium battery pack as an alternative power source if primary power is lost. This battery can explode or leak and cause burns if disassembled or exposed to fire, high temperature or rapid warming from extremely cold temperatures.

The environment in which the Gateway is installed must not exceed the environmental operating limits of 0 to 40° Celsius and 0% to 95% Relative Humidity (non-condensing).

Non-ionizing Radiation exposure

The Gateway regularly communicates over Wi-Fi and Cellular LTE networks and transmits at a maximum power of 23 dBm (200 mW). This level is not recognized as hazardous, but several nations (e.g. Canada, Australia) advise not to use such a device within 20cm of your body i.e. as a personal electronic device without further precautionary testing.

This equipment has been tested and found to comply with the USA’s (FCC) limits for a Class B digital device, which are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial or residential environment. If not installed and used in accordance with this User Manual, the Gateway may possibly cause harmful interference to other radio communications. Possible remedies for any such interference include reorienting the receiving antennae, increasing the separation between affected equipment and Gateway or connecting the affected equipment into an outlet on a circuit different from that to which the Gateway is connected.

Mounting the Gateway

To minimize harm from a falling Gateway, do not rely on magnets for mounting higher than 2m (6’6”). Further mounting recommendations can be found in the “Mounting and Positioning” section.

Protecting the Environment

The Gateway is designed with consideration for the environment and complies with EU’s RoHS regulations and Batteries Directive, as well as the USA’s EPA initiative to ‘Reduce, Reuse, Recycle’. Elemental Gateways are provided to customers to support the service Elemental Machines provides, but they remain the property of Elemental Machines and should be returned to Elemental Machines at the end of their life for reuse, recycling, or disposal as appropriate. Elemental Machines relies on customers to play their role in the process of disposing of Elemental Gateways correctly, to help Elemental Machines in protecting the environment.

The Gateway qualifies as Electrical or Electronic Equipment that the EU requires not to be added to unsorted municipal waste when it has reached the end of its life. The correct disposal, which includes when the battery pack has reached its maximum lifecycle use, is to return the Gateway to Elemental Machines, or their agent, where:

- Lithium battery packs that have reached the end of their life can be removed from the Gateway for disposal according to local regulations (EU and UK Non-hazardous Waste code: 16 06 04).
- The Gateway can have a new battery pack installed or, if it has reached the end of life, will have its battery pack removed for disposal as above and treated as Waste Electronic and Electrical Equipment (WEEE) (EU and UK Non-hazardous Waste code 16 02 14).
Installation

This is the recommended setup procedure for most customers. Your unique setup may require modifications. If you have any questions, please reach out to your account representative or email help@elementalmachines.com for assistance.

Preparation

Verification Email

Prior to receiving the devices, you will receive an email for your account verification. Refer to this email to enable the system.

When devices are shipped they will be added to your Elemental Machines Insights Dashboard™ with default names. When you first log in you will see all of your devices with a ‘disconnected’ status.

Components

Prior to installation, ensure you have all necessary components. When Elemental Gateways and Elements are shipped, they are automatically added to your Elemental Insights Dashboard™ with default names. Upon first log-in, these devices will be shown with a ‘disconnected’ status.

Additional Elements and equipment may be included in your installation kit. Please refer to the guides for each device for installation instructions.

Assembling the Gateway

Before powering on the Gateway, if the device does not have the antennas installed, screw the two provided antennas in the antenna ports by rotating them clockwise.

Powering On the Gateway

Plug in the provided wall adapter into an AC outlet, plug the round (barrel) connector into the Gateway, and flip the switch as indicated.

When the switch is turned on, the power indicator light glows white. The Cellular, Wi-Fi, and Battery indicators will also glow to indicate their status.

Important Note: Antennas should be finger-tightened. Do not use pliers or other tools to tighten.
Battery Indicator

The battery will charge when the device is plugged into the wall. When the device power switch is on, the battery indicator color shows the battery charge status.

<table>
<thead>
<tr>
<th>Battery Indicator Colors</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Solid Blue</strong></td>
</tr>
<tr>
<td><strong>Blue Flashing / Green</strong></td>
</tr>
<tr>
<td><strong>Blue Flashing / Red</strong></td>
</tr>
<tr>
<td><strong>Green</strong></td>
</tr>
<tr>
<td><strong>Red</strong></td>
</tr>
</tbody>
</table>

Connect the Gateway to Your Network

The Gateway requires either an Ethernet or Wi-Fi connection to begin collecting data.

Connecting to Ethernet

To connect the Gateway to the internet via an ethernet cord, insert an ethernet cord directly into the exposed RJ-45 jack on the Gateway. Make sure that the cord’s locking mechanism has engaged fully after installation by gently tugging on the cord, which should remain firmly in the ethernet jack.

Connecting to Wi-Fi

To connect the Gateway to Wi-Fi, first ensure that no ethernet cable is plugged in. When the Gateway is plugged into power and fully booted without an ethernet connection, it will begin to broadcast an access-point Wi-Fi network with the name “EM Setup xxxxxxx”, where xxxxxxx is the 7-character serial number located on the bottom of the Gateway. Connect to this Wi-Fi network on any iPhone or Android device, or on a Macintosh or Windows PC.

After a connection is established, your device will bring up a “captive portal”-style window which will prompt you to select the SSID of the network to which you would like to connect the Gateway, and to enter the Passphrase of your selected Wi-Fi network.

After pressing the connect button, the “captive portal” window will minimize, and the connection process will begin on the Gateway.

If the Passphrase you entered was incorrect, then the network “EM Setup xxxxxxx” will be available again in ~30 seconds, and you can re-enter the Passphrase.

Note: If the captive portal window doesn’t appear automatically, you may need to launch a web browser window manually.
Mounting and Positioning

The following 4 factors will contribute to a well-positioned and properly functioning gateway.

1: Proximity to Wi-Fi and Cellular Networks

To prevent data loss or delay, make sure that the Wi-Fi and Cellular indicator LEDs are both green at the location you have chosen before you finalize your installation.

The strengths of the Wi-Fi and Cellular connections are displayed by the Wi-Fi indicator LED and the Cellular indicator LED.

2: Proximity to Elemental Machines Elements

All battery-powered Elements like Element-T and Element-A have prescribed maximum ranges from the Gateway of 30 to 90 feet, depending on device and layout/concentration of equipment in your lab. Signal strength for individual Elements can be checked on the Dashboard by navigating to the Machine Overview of the Element in question. The signal icon will have 1 to 4 bars of strength (4 bars indicates the best signal strength). 2 or more bars indicate sufficient signal strength between an Element and the Gateway.

3: Heat

Because the Gateway is installed in environments containing equipment which might rise significantly above the ambient temperature of the room, it is important to position the Gateway away from any equipment which might vent significant amounts of heat. For more information on handling the effects of heat, see the Post-Installation Guide below on responding to heat-related alert tones.

4: Orientation, Location, and Safety

The Gateway can be installed in both vertical and horizontal orientations. Integrated magnets make it convenient to attach to the side of many types of lab equipment and metal surfaces. Adhesive metal plates are available, which can be used to mount the Gateway to non-magnetic surfaces while still allowing the Gateway to be moved to a new position.

In many laboratory situations, the side of a lab bench shelf is the optimum location for the Gateway.

To avoid any physical disturbance which might knock the Gateway out of its position or unplug the device, ensure the Gateway is kept away from any equipment which experiences a high volume of door opens/closes, or which might be frequently moved or shifted. Keep cables (ethernet and power) tidy and away from commonly used pathways; cables present trip hazards that can not only disturb the Gateway but also lead to larger accidents.

For mounting applications higher than 2m (6’6”), to minimize harm in case of a falling Gateway, the keyhole slot on the rear of the device should be utilized instead of the magnetic connection. See the Safety section above for more information.
Additional Information

Network Priority
1: Ethernet
2: Wi-Fi
3: Cellular Connection

⚠️ Cellular Connection is intended as a temporary data transfer backup only. If a default WiFi network has never been set for the Gateway, and ethernet connection is not available, data will be collected but not uploaded until a WiFi or ethernet connection is available.

Maintenance and Post-Installation

Overheat Alert Tone
The Gateway produces a 2-second monotone when the device is overheated. In this state, the Gateway should be moved to a cooler location immediately.

Powering Off the Gateway
In the case where a Gateway needs to be decommissioned and stored or shipped, it will need to be powered off. To power off the Gateway, first unplug it from the wall adapter, then flip the power switch to the off position.

Specifications

<table>
<thead>
<tr>
<th>GATEWAY SPECIFICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Model Number</td>
</tr>
<tr>
<td>Unit Dimensions Without Antenna</td>
</tr>
<tr>
<td>Antenna Dimensions</td>
</tr>
<tr>
<td>Operating Temperature Range</td>
</tr>
<tr>
<td>Operating Humidity Range</td>
</tr>
<tr>
<td>Battery Life</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>COMMUNICATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wi-Fi 2.4GHz Max. TX Power</td>
</tr>
<tr>
<td>Wi-Fi 5GHz Max. TX Power</td>
</tr>
<tr>
<td>Cellular LTE Max. TX Power</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>COMPLIANCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contains FCC ID (Part 15.247)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Contains IC ID (RSS 247)</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Battery</td>
</tr>
</tbody>
</table>
Certifications

United States FCC:

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

• Reorient or relocate the receiving antenna.
• Increase the separation between the equipment and receiver.
• Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
• Consult the dealer or an experienced radio/TV technician for help.

WARNING: Changes or modifications not expressly approved by Elemental Machines, Inc. could void the user's authority to operate the equipment.

Canada IC:

This equipment complies with Canada radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

This device complies with Industry Canada licence exempt RSS standard(s). Operation is subject to the following two conditions: (1) this device may not cause interference, and (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Cet équipement est conforme Canada limites d’exposition aux radiations dans un environnement non contrôlé. Cet équipement doit être installé et utilisé à distance minimum de 20cm entre le radiateur et votre corps.

Le présent appareil est conforme aux CNR d’Industrie Canada applicables aux appareils radio exempts de licence. L’exploitation est autorisée aux deux conditions suivantes : (1) l’appareil ne doit pas produire de brouillage, et (2) l’appareil doit accepter tout brouillage radioélectrique subi, même si le brouillage est susceptible d’en compromettre le fonctionnement.
Appendix 1: Declarations of Conformity

EU DECLARATION OF CONFORMITY

1. Radio equipment: Gateway, GW3
2. Name and address of the manufacturer or his authorised representative:
   Elemental Machines
   185 Alewife Brook Parkway, Suite 401
   Cambridge, MA 02138 USA
3. This declaration of conformity is issued under the sole responsibility of the manufacturer.
4. Object of the declaration:

5. The object of the declaration described above is in conformity with the relevant European Union harmonisation legislation:
   Directive 2014/53/EU (RED), including:
   a. essential EMC requirements under Directive 2014/30/EU (EMC)
   b. safety under 2014/35/EU (LVD)
   Directive 2011/65/EU and amendment 2015/863 (RoHS)
   Directive 2006/66/EC and amendment 2013/56/EU (Batteries Directive)
   Directive 2012/19/EU (WEEE)
6. Relevant harmonised standards used:

   | EN 50419:2006   | EN 62311:2008   |
   | EN 61000-4-2:2009 | ETSI EN 300 328 V2.2.2 (2019-07) |
   | EN 61000-4-3:2006+A2:2010 | ETSI EN 301 893 V2.1.1 (2017-05) |
   | EN 61000-4-4:2012 | ETSI EN 301 511 V12.5.1 (2017-03) |
   | EN 61000-4-5:2014 | ETSI EN 301 908-1 V15.1.1 (2021-09) |
   | EN 61000-4-6:2014 | ETSI EN 301 489-1 V2.2.3 (2011-09) |
   | EN 61000-4-8:2010 | ETSI EN 301 489-17 V3.2.4 (2020-09) |
   | EN 61000-4-11:2004 | ETSI EN 301 489-52 V1.2.1 (2021-11) |
   | EN 62368-1:2018 |

Signed for and on behalf of: Elemental Machines [2023 Apr 13]

(signature):

Sridhar Iyengar, CEO
UK DECLARATION OF CONFORMITY

1. Radio equipment: Gateway, GW3
2. Name and address of the manufacturer or his authorised representative:
   Elemental Machines
   185 Alewife Brook Parkway, Suite 401
   Cambridge, MA 02138 USA
3. This declaration of conformity is issued under the sole responsibility of the manufacturer.
4. Object of the declaration:

5. The object of the declaration described above is in conformity with the relevant statutory requirements:
   Radio Equipment Regulations 2017(S.I. 2017/1206) including:
   a. EMC under Electromagnetic Compatibility Regulations 2016(S.I. 2016/1091)
   b. safety under Electrical Equipment (Safety) Regulations 2016(S.I. 2016/110)
   Restriction of the Use of Certain Hazardous Substances in Electrical and Electronic Equipment Regulations 2012(S.I. 2012/3032)
   The Batteries and Accumulators (Placing on Market) Regulations 2008(S.I. 2008/2164)
   The Waste and Electrical and Electronic Equipment Regulations 2013(S.I. 2013/3113)

6. Relevant harmonised standards used:
   EN 50419:2006
   EN 55035:2017 + A11:2020
   EN 61000-4-2:2009
   EN 61000-4-3:2006+A2:2010
   EN 61000-4-2012
   EN 61000-4-5:2014
   EN 61000-4-6:2014
   EN 61000-4-8:2010
   EN 61000-4-11:2004
   EN 62368-1:2018
   EN 62311:2008
   EN 63000:2018
   ETSI EN 303 367 V1.1.1 (2016-06)
   ETSI EN 300 328 V2.2.2 (2019-07)
   ETSI EN 301 893 V2.1.1 (2017-05)
   ETSI EN 301 511 V12.5.1 (2017-03)
   ETSI EN 301 908-1 V15.1.1 (2021-09)
   ETSI EN 301 489-1 V2.2.3 (2011-09)
   ETSI EN 301 489-17 V3.2.4 (2020-09)
   ETSI EN 301 489-52 V1.2.1 (2021-11)

Signed for and on behalf of: Elemental Machines [2023 Apr 13]

(signature):

Sridhar Iyengar, CEO
Appendix 2: Platform Network Summary

Elemental Machines’ platform delivers actionable intel to operators that will help improve operations and speed discovery. Elemental Machines devices are designed to operate securely on our customers’ networks. The entire platform includes:

- Devices called **Elements** that monitor critical equipment and/or the ambient environment
- **Elemental Gateway** that gathers data from the non-cloud connected Elements
- **Elemental Insights** dashboard

The full scope of Elemental Machines’ Data Services is shown below:

Local Communication

Wireless sensors (**Element-T**, **Element-A**, **Element-U Model EU2**, and **Element-B**) communicate individually to a local **Elemental Gateway** (either an Elemental Tablet Gateway, Elemental Gateway models GW2 or GW3) via a low-powered 2.4 GHz wireless communication protocol. These devices do not connect to the corporate network. Each **Elemental Gateway** will only process data from **Elements** that are on a pre-defined list that is unique to each installation. This list is created prior to shipping the **Gateway** and is updated whenever new **Elements** are added to the network.

**Element-C**, **Element-D**, and **Element-U model EU1** devices do not require an **Elemental Gateway** and transmit data directly from a piece of equipment to the **Elemental Insights** dashboard via customer Wi-Fi or ethernet.
Communication through Customer Ethernet or Wi-Fi

Elemental Gateway Models GW2/GW3 and Element-C, Element-D, and Element-U Model EU1 will always connect to Ethernet first, if available. If there is no Ethernet then the device will connect to Wi-Fi. The system uses HTTPS to protect data transmitted between Elemental Gateways, Element-C, Element-D, and Element-U Model EU1 devices and necessary API and data ingest endpoints, such as Elemental Insights. HTTPS is the established communication and security standard for protecting sensitive data transmitted across the web, with applications that include usernames, passwords, credit card, and banking information.

Elemental Machines devices use socket connections through port 80, 123, and 443 of a customer’s firewall, opening only outbound connections.

Elemental Tablet Gateway require the following outbound TCP/UDP connections to be open in a customer’s firewall for the system to work:

<table>
<thead>
<tr>
<th>ENDPOINT</th>
<th>PORT</th>
<th>PROTOCOL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>*.elementalmachines.io</td>
<td>443</td>
<td>TCP</td>
<td>sending data to the dashboard</td>
</tr>
<tr>
<td><a href="http://api.elementalmachines.io">http://api.elementalmachines.io</a></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ingest.elementalmachines.io</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s3.amazonaws.com</td>
<td>80,443</td>
<td>TCP</td>
<td>configuration files</td>
</tr>
<tr>
<td>*.awmdm.com</td>
<td>443</td>
<td>TCP</td>
<td>mobile device management</td>
</tr>
<tr>
<td>appwrapandroid.awmdm.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>discovery.awmdm.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>signing.awmdm.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>gem.awmdm.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><a href="http://play.google.com">http://play.google.com</a></td>
<td>443</td>
<td>TCP</td>
<td>provisioning</td>
</tr>
<tr>
<td>android.clients.google.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>android.googleapis.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>time.elementalmachines.io</td>
<td>123</td>
<td>UDP</td>
<td>time synchronization</td>
</tr>
<tr>
<td>*.pubnub.com</td>
<td>443</td>
<td>TCP</td>
<td>secure IoT device messaging</td>
</tr>
<tr>
<td>*.pubnub.net</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*.pndsn.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*.papertrailapp.com</td>
<td>443</td>
<td>TCP</td>
<td>log management</td>
</tr>
</tbody>
</table>
Elemental Gateway Model GW3 requires the following outbound TCP/UDP connections to be open:

<table>
<thead>
<tr>
<th>ENDPOINT</th>
<th>PORT</th>
<th>PROTOCOL</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>*.elementalmachines.io</td>
<td>443</td>
<td>TCP</td>
<td>sending data to the dashboard</td>
</tr>
<tr>
<td>api.elementalmachines.io</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ingest.elementalmachines.io</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s3.amazonaws.com</td>
<td>80,443</td>
<td>TCP</td>
<td>configuration files</td>
</tr>
<tr>
<td>time.elementalmachines.io</td>
<td>123</td>
<td>UDP</td>
<td>time synchronization</td>
</tr>
<tr>
<td>*.balena-cloud.com</td>
<td>443</td>
<td>TCP</td>
<td>device management</td>
</tr>
<tr>
<td>vpn.balena-cloud.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>api.balena-cloud.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>registry2.balena-cloud.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>registry-data.balenacloud.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*.docker.com</td>
<td>443</td>
<td>TCP</td>
<td>for verified operating system images</td>
</tr>
<tr>
<td>*.docker.io</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*.pubnub.com</td>
<td>443</td>
<td>TCP</td>
<td>secure IoT device messaging</td>
</tr>
<tr>
<td>*.pubnub.net</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>*.pndsn.com</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>8.8.8.8</td>
<td></td>
<td></td>
<td>Google’s Public DNS server (Balena</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>default, can be reconfigured)</td>
</tr>
</tbody>
</table>

For All Devices, no inbound ports need to be opened. Security vulnerability using the above configuration is prevented as follows:

- Internet communication over Port 80, 123, and 443
- Device must be able to transmit outward to the Internet on 443
- Clients do not open inbound ports
- There is no need to open the firewall to receive on port 80, 123, or 443
- There is no way for outside users to get into the user’s network
- No ports are listened to by Elemental Machines, that is the case even if the user opened ports 80 or 443 for receipt

**Elemental Insights Dashboard**

Communication between the Dashboard and web browsers always uses HTTPS. User access to the Dashboard is restricted to invite-only, requires hardened passwords, and can be revoked by admins at any time. Users are further restricted in what they can access or edit by role-based account policies.
Supplemental Security Information

**Elemental Tablet Gateway** is based on Android technology and therefore enjoy the security benefits of the Android Development Network and Google. Security benefits, as listed in a security whitepaper from Google about Android, are as follows:

- Strives to prevent security issues from occurring through design reviews, penetration testing, and code audits
- Performs security reviews prior to releasing new versions of Android and Google Play
- Publishes the source code for Android, thus allowing the broader community to uncover flaws and contribute to making Android the most secure mobile platform
- Works hard to minimize the impact of security issues with features like the application sandbox Detects vulnerabilities and security issues by regularly scanning Google Play applications for malware, and removing them from devices if there’s a potential for serious harm to the user devices or data
- Has a rapid response program in place to handle vulnerabilities found in Android by working with hardware and carrier partners to quickly resolve security issues and push security patches

**Elemental Gateway Models GW2, GW3** as well as **Element-C, Element-D, and Element-U Model EU1** devices are based on the balenaOS, a thin Linux environment that supports the balenaCloud services and user application containers. Balena offers security by design:

- API access control
- Multiple authentication methods
- Minimized available attack surfaces
- Balena operates its own Virtual Private Cloud (VPC) on Amazon Web Services (AWS) This isolation gives Balena an added layer of security

Elemental Machines Cloud Services

Elemental Machines’ data ingestion and server infrastructure are hosted on Google Cloud Platform, which provides a managed security layer for Google services (PubSub, BigQuery, etc.) and are automatically updated by Google. Other components such as Ruby-on-Rails, Influx, and Postgres databases are maintained to at least the minimum supported version and are updated for any high/critical security vulnerabilities per vendor guidance.

Elemental Machines Network Information

**Wireless Requirements:**

- SSID: Not hidden is preferred
- Security: WEP, WPA, or WPA2
- IP Assignment: Dynamic is preferred
- Number of Unique Devices: Sum of the Gateways and Element-C, Element-D, and Element-U1 devices
- Captive Portal: Not Supported

**Local Wireless Network Information:**

- SSID:
- Password: