EDGEMATE
POWERING EDGE SOLUTIONS

# How to Provide Secure Remote Access to IoT Edge Devices via Web, SSH and Remote Desktop?

***Secure remote access to IoT edge devices is one of the fundamental building blocks of the Internet of Things. End users want to access and manage their devices via web or mobile app, service partners need access to devices installed at remote locations, and product support teams need to be able to log-in to devices installed at customer sites.***

Web-based user interfaces are standard in IoT edge devices and connected embedded systems, used for configuration, control and monitoring of devices from PCs, smart phones or tablets. Modern web-based user interfaces are powerful, visually attractive, and easy to use. Since their only requirement is a HTTP(S) connection between the web browser and the web server running on the device, they are perfectly fitted for remote access scenarios.

However, for this to work, the web browser on the client PC or mobile device must be able to create a network connection to the IoT device's web server. This is only possible if the IoT device is located in the same network as the device running the web browser, if the networks containing the client and server are linked, or if the IoT device can be directly reached over the internet. Unfortunately, this is rarely the case in practice. IoT edge devices in the field are often connected to private networks behind NAT routers or firewalls. This is especially true for industrial IoT devices, which are typically located behind a NAT router. Also, devices connected to a mobile 4G/LTE network in most cases do not have public IP addresses and thus are not directly reachable. This means that while these devices can open connections to servers on the internet, it is not possible to access the device's web server from the outside, unless additional measures are taken.

Port forwarding and Virtual Private Network (VPN) are widely known and established technologies for enabling internet-based remote access to computers and network devices behind NAT routers or firewalls. However, as detailed in the table at the end of this white paper, both technologies have severe drawbacks related to security and complexity, especially when being used with IoT edge devices. For this reason, Applied Informatics has created a new technology that is a great alternative to port forwarding and VPN.

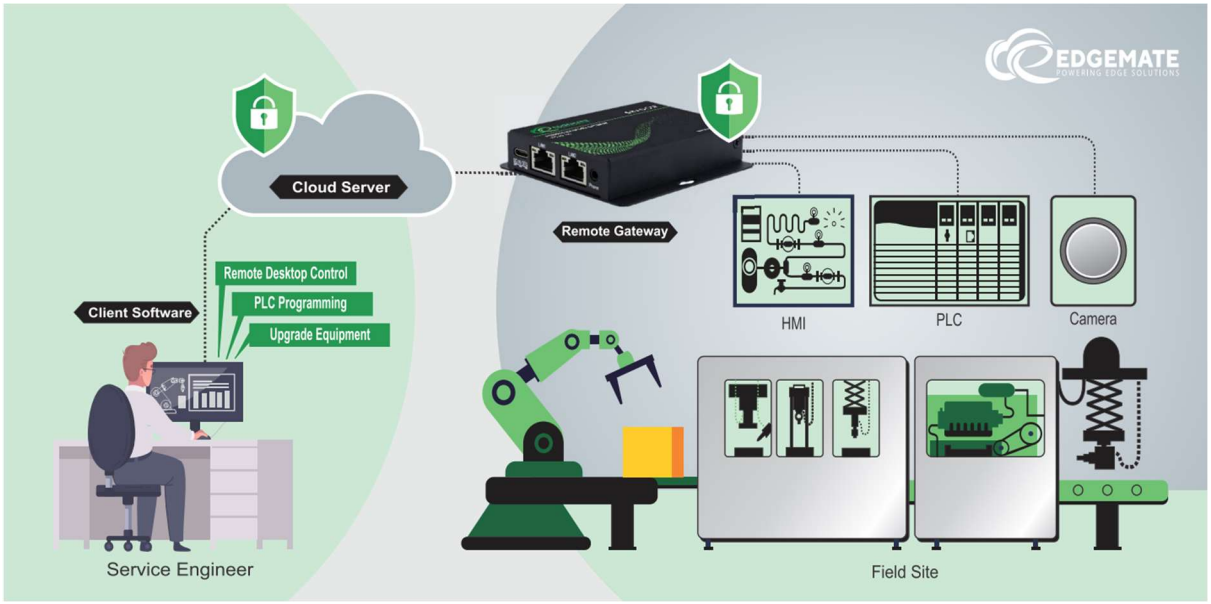
## WEB-BASED REMOTE ACCESS TO IOT EDGE DEVICES WITH REMOTE MANAGER

**Edgemate.io Remote Manager** enables easy and se-cure remote access to the web server and other TCP-based services such as secure shell (SSH) or remote desktop (VNC, RDP) of an IoT device, even if the device is located in a private or mobile network behind a NAT router or firewall. How this technology works will be explained in the following.

### Application Scenarios

- Remote access to IoT gateways, edge computing devices, data loggers, metering and monitoring devices, e.g. in renewable energy, environmental monitoring, traffic, transportation and infrastructure, etc.
- Remote access to mobile devices for data acquisition, tracking, fleet management, etc.
- Remote support, maintenance and servicing of consumer electronics, home/building automation, HVAC devices, industrial equipment, etc.
- Remote access to IP network cameras and DVRs
- Remote access to security and access control systems

## HOW REMOTE MANAGER WORKS



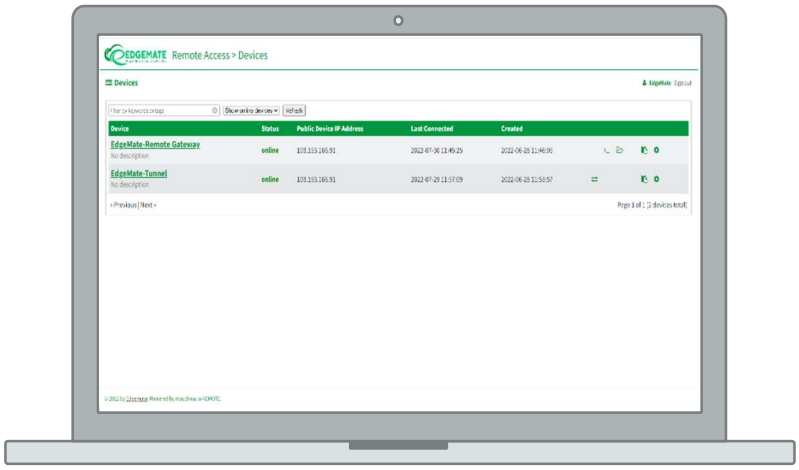

Edgemate.io Remote Manager is based on standard internet technologies, specifically, HTTPS and WebSockets. The IoT device needs to run a program called *WebTunnelAgent* that opens and maintains a secure, TLS-protected and always-on WebSocket connection to the Remote Manager server running in the cloud. Once the connection between the device and the Remote Manager server has been established, the Remote Manager server uses this connection to send ("tunnel") HTTP requests and other TCP-based network traffic to the device.

Where do these HTTP requests come from? The Remote Manager server also contains a web server, which accepts requests from clients (web browsers). These requests are then simply forwarded to the device, using the device's tunnel connection.

Setting up the initial tunnel connection between the device and the Remote Manager server is almost always possible as long as the device can access the internet. Since the tunnel connection opened by the device uses standard HTTPS and WebSocket protocols, it is very firewall-friendly and even works through an intermediate HTTP proxy server.

## IDENTIFYING AND ADDRESSING DEVICES

In a typical usage scenario, more than one device will be connected to a Remote Manager server. In fact, ten thousands of devices could be connected to a single server. Therefore, when the Remote Manager server receives a HTTP request from a client, it needs to find out to which device the request must be forwarded. This is done via the URL sent from the client to the Remote Manager server (e.g., *http://dev1.my-devices.net*) in the HTTP request. The mechanism relies on a wildcard DNS record in the DNS server which resolves all requests for **.my-devices.net* to the Remote Manager server *remote.my-devices.net*. The Remote Manager server can then use the *Host* header in the HTTP request together with an internal table to associate the request with a device (and its tunnel connection).




## RUNNING THE REMOTE MANAGER SERVER

There are multiple options for running the Remote Manager server. It can be deployed on an internet-facing server in a private datacenter (on-premises), or it can run on a virtual private server (VPS) provided by a cloud service provider such as Amazon (EC2), Azure or DigitalOcean. Running the Remote Manager server can also be outsourced to a dedicated service provider. Multiple Remote Manager servers can run in a loadbalancing setup, making it possible to handle 100.000s or even millions of connected IoT devices.

## SECURITY AND PRIVACY GUARANTEED

Since the Remote Manager server only transparently forwards HTTP requests and TCP connections, but does not store any data passed through it (except for optional caching of images and style sheets in order to improve performance), Edgemate.io Remote Manager does not introduce any additional data security and privacy risks – especially if the Remote Manager server is operated in a private data center. Of course, both the connection between the device and the Remote Manager server, as well as the connection between the client (web browser) and the Remote Manager server are encrypted and secured with state-of-the-art TLS.

A great advantage of this technology is that it is inherently secure. Since the device does not need to have any open ports to the internet, there is no danger of denial-of-service or other kinds of attacks against the device. Requests to the device can only be sent through the Remote Manager server, and the Remote

Manager server requires proper authentication of the user before forwarding requests to the device. Also, devices must authenticate themselves against the Remote Manager server when setting up the tunnel connection. Device authentication is done through a shared secret (password, or challenge-response) or certificate.

## USER ACCOUNTS, ROLES AND PERMISSIONS

The Remote Manager server supports user account management features and role- and permission-based access control, making it easy to specify which users may access and manage which devices.

## WORKS FOR WEB, SSH AND REMOTE DESKTOP

Edgemate.io Remote Manager is not just for accessing web pages. Virtually every TCP-based protocol can also be used over a Remote Manager tunnel connection, including web services based on REST, JSON-RPC or SOAP technologies, or secure shell (SSH) and remote desktop (VNC, RDP) protocols. Remote Manager even includes a web-based VNC client. This makes it a great foundation for automated device management applications and remote support/maintenance portals.

## EASY INTEGRATION AND CUSTOMIZATION

The software necessary for integrating Remote Manager into a device, as well as the Remote Manager server is provided by Applied Informatics. For devices where the necessary modification of the firmware is not possible or feasible, a low-cost gateway device can be used to connect the device to the Remote Manager server. The gateway is located in the same local area network as the device, and forwards requests from the Remote Manager server to the device's web server. It's also possible to install the gateway software on a mobile internet router.

The Remote Manager server can be integrated with other applications via its REST API. The default web user interface of the Remote Manager server can be customized to match customer-specific needs and

visual style.

The Remote Manager server optionally supports LDAP for user authentication.

## SECURE REMOTE ACCESS MADE EASY

Edgemate.io Remote Manager is a great and secure alternative to technologies like NAT port forwarding and virtual private networks to enable easy and secure remote access to IoT devices via web, shell or remote desktop. The technology can be used without touching the existing network infrastructure and is suitable for use with end users, service partners or internal support teams. The necessary Remote Manager server can be operated in "the cloud", and devices can be easily integrated, either by updating their firmware or by using a special gateway device or 4G/LTE router.

| Technology | Advantages | Disadvantages |
|---|---|---|

| | | |
|---|---|---|
| **Edgemate.io Remote Manager** | ▶ based on proven and proxy/firewallfriendly WebSocket protocol<br>▶ can be used without changes to the existing network infrastructure ▶ supports secure, encrypted (TLS) and authenticated connections ▶ secure forwarding of most TCPbased protocols, not just HTTP, including SSH for remote shell and VNC/RDP for remote desktop access<br>▶ the Remote Manager server can be operated in the cloud<br>▶ high scalability, up to ten thousands of devices per Remote Manager server instance (multiple servers can be clustered to increase capacity up to millions of devices)<br>▶ integrated user management and detailed role-and permission-based access control | ▶ Edgemate.io Remote Manager agent software must be integrated into device, or a gateway device must be used to integrate legacy devices<br>▶ some TCP-based protocols cannot be forwarded (e.g., FTP)<br>▶ cannot be used with UDP-based protocols |
| **Port Forwarding** | ▶ simple and widely supported by NAT routers<br>▶ allows access to any TCP or UDPbased network service provided by the device | ▶ NAT router configuration for port forwarding can be complex, especially if multiple devices must be accessible (every device needs a unique public port number)<br>▶ a Dynamic DNS service is needed if the NAT router does not have a static public IP address<br>▶ public IPv4 addresses are becoming scarce<br>▶ the device is directly exposed to the internet – very high risk and danger of denial-of-service and other kinds attacks |
| **Virtual Private Network** | ▶ the device is directly integrated into a remote network using a secure tunnel through the internet<br>▶ secure, encrypted connection<br>▶ proven, standardized and widely available technology | ▶ VPNs may be blocked by network provider or legally restricted<br>▶ necessary network and VPN server infrastructure is difficult to setup and to maintain, especially if lots of devices must be integrated<br>▶ all clients must have access to VPN in order to access the devices – therefore not suitable for end-user access<br>▶ additional measures must be taken to isolate devices in the VPN from one another and to prevent users from |

| | | |
|---|---|---|
| | | accessing devices they should not have access to |