

Networking the TEK Pool EMS System

How the TEK Pool EMS System Communicates over Internet



Maktinta Energy
Campbell, CA 95011-0426
Tel: 408-432-9900
Maktinta@gmail.com

The TEK Pool EMS controller

The TEK Pool EMS is a piece of equipment designed to connect to sensors and meters to collect data. Typical use is to monitor electric use, temperature and control thermostats, but the system is flexible and can be used in a wide variety of applications. The TEK Pool EMS controller communicates with dedicated servers via the Internet. The servers are managed by The System and provide the user interface for the system. Users cannot access the TEK Pool EMS controller directly through the network. All communication to/from the controllers must go through the servers.



The TEK Pool EMS software/firmware design

The TEK Pool EMS controller hardware is designed to be very secure and reliable. It uses a small ARM processor (Cortex-M3) that has built-in flash (256kB) and RAM (64kB). The code is running directly in flash memory, so there is no bootloader and no interface that would allow the code to be altered in any way. The operating system is a custom “tasker”. As such, it only includes the services required for the TEK Pool EMS custom application, and all code has been tested and analyzed by The System. The network software is based on the uIP open source code ([http://en.wikipedia.org/wiki/UIP_\(micro_IP\)](http://en.wikipedia.org/wiki/UIP_(micro_IP))), and heavily customized for the TEK Pool EMS. The firmware only includes support for the services absolutely necessary for the system. Any TCP-support has been removed completely.

TEK Pool EMS startup operation

At startup, the TEK Pool EMS will attempt to acquire a dynamic IP address from a DHCP server. As soon as an address has been assigned, the TEK Pool EMS will attempt to resolve the address of the server(s). The controller is preconfigured with a list of about eight (8) servers for redundancy reasons. When a server IP has been returned by the DNS assigned from the DHCP server, the controller will attempt to send an encrypted UDP message to that server on port 8844, via the assigned gateway. The controller will go down the list until it finds a server that replies. If it falls through the whole list, it will start over from the top.

UDP communications

The TEK Pool EMS strictly uses UDP traffic to communicate with the servers. Each UDP message is between 24 and 1024 bytes long, and all the payload is encrypted with a unique 128-bit key. Messages from the TEK Pool EMS to the server always use port 8844. Port UDP 8844 needs to be open for OUTGOING traffic - from the LAN to the servers - and allow any return traffic from the servers (like a normal router / NAT would).

Return traffic from the servers to the TEK Pool EMS use a port in the range 28672 to 32767 (hex 7000-7FFF). The return port number will be randomly selected for each new attempt to contact a server.

in the event that there is a need to limit the return open IP addresses you can limit the list to the following list of server IP's:

136.243.42.73
136.243.42.74
144.76.220.233
64.85.169.160

We strongly advise against filtering on server IP though. If we change anything in the data center, there's a chance that these addresses will change and your systems will go offline.

Security considerations

Unlike TCP, UDP does not have any support for retransmits or packet serialization. UDP simply encapsulates raw data, and it is up to the application to make sure the packets are received correctly. This means that there is no existing "attack" that works on the UDP protocol in itself. TCP on the other hand has some vulnerabilities that can cause excessive memory use or blocking of traffic. Note that the TEK Pool EMS does not have any support for TCP. Only UDP traffic is supported. Each TEK Pool EMS has a unique 128 bit encryption key. This key is used to encrypt all communication with the servers. When a message is received, the controller will decrypt the data and then run a number of checks on the decrypted data. If the message does not pass the tests, it will be dropped with no further action. The

tests include, but are not limited to, sequence counters, checksums, length and range control. This means that only traffic from the server is accepted. Any other traffic will be completely ignored. Since the TEK Pool EMS will only process recognized packets, and since it has no support for TCP, the TEK Pool EMS poses no risk to any network. It is impossible to “bounce traffic” off a controller, and there is no way to load other software on it.

Firewall / Gateway requirements

DHCP configuration The TEK Pool EMS will attempt to configure its network settings from a DHCP server. The controller will need an IP address, net mask, default gateway and a DNS server. Outgoing UDP port 8844 with stateful routing. The TEK Pool EMS needs to be able to transmit UDP traffic to port 8844 on the public servers. The firewall needs to be configured for “stateful routing”, so that the reply-to endpoint (IP + port) is allowed for returning traffic from the servers. Stateful routing is default in most NAT-style networks. In our experience, most networks support this, unless it has been explicitly disabled.

Filtering based on server

IP's While possible, whitelisting the server IP addresses to allow traffic to flow from/to the TEK Pool EMS is not recommended. The System manages multiple data centers, and the server IP's may change as the infrastructure is upgraded.

Fixed IP configuration

The TEK Pool EMS can be configured with fixed IP if needed. Note that if there is an error in the fixed IP configuration that prevents the controller from communicating with the servers, the controller needs to be connected to a network with DHCP service and “reset” in order to allow reconfiguration.

Setting a manual (Fixed) IP

The TEK Pool EMS by default expect a DHCP service to provide the correct network settings for the device when it is connected to the network. In some installations, it is required to supply specific network settings manually to each device to allow it to communicate on the network. To apply manual network settings, navigate to the Configure->System screen and enter IP addresses in the Ethernet settings section (see image).



The image shows a screenshot of a software window titled "Ethernet settings". It contains several input fields for network configuration:

- IP:** 192.168.1.123 (with a "(blank for auto)" note to the right)
- Net mask:** 255.255.255.0
- Gateway:** 192.168.1.1
- DNS:** 8.8.8.8
- External server URL:** (empty field)
- Extended timeout:** An unchecked checkbox, with a note "(Normal=4min, Extended=20min)" to its right.

Please make sure all settings are correct before applying them. Wrong settings will cause communication to fail.

NOTE: In order for the settings to be downloaded to the TEK Pool EMS, the TEK Pool EMS needs to be online with the servers. Thus, the TEK Pool EMS needs to be connected to a network that supports

DHCP temporarily. As soon as the settings are synced the TEK Pool EMS can be moved to the network that requires fixed IP. Also note that the TEK Pool EMS will lose contact with the servers via the DHCP network if manual IP settings are applied!

Restoring DHCP functionality

To restore DHCP support, first remove the fixed IP settings on the server by blanking out the IP field and click Save Changes. If the TEK Pool EMS is still communicating via fixed IP, the settings will be automatically synced and applied after the next reset of the TEK Pool EMS. If the TEK Pool EMS is not communicating, the reset procedure



Remove power from the TEK Pool EMS.

Open the enclosure and locate the holes marked **HALT** (see picture to the right).

Apply a jumper between the two holes and make sure it stays in place, connecting the holes.

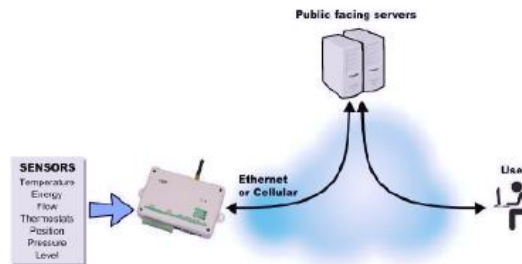
Connect power to the TEK Pool EMS, keeping the jumper in place. The LED's will blink very fast, and the TEK Pool EMS will attempt to use DHCP to connect to the servers.

Verify that the TEK Pool EMS connects by checking the status on ezecontrol.com.

When the “spinner” indicator stops and shows a green dot, the new configuration is saved.

Public IP

The TEK Pool EMS does not need an assigned public IP or static route accessible from the public Internet. That said, the controller does not have to be behind a firewall. It will work on a public IP with no filter or protection. The controller can be “double-NAT:ed” as long as the routers allow return traffic.



Summary

- Standard DHCP configuration (fixed IP possible)
- Outgoing UDP traffic to port 8844 on multiple public servers.
- Reply traffic from servers to random UDP port 28672 to 32767.
- No support for TCP. No standard OS.
- No direct user access to controller – all communication goes via servers.
- All UDP traffic is encrypted with per-controller unique encryption keys.
- Typical transfer per controller is very low: 5-8MB/month depending on configuration.

GSM/3G/GPS module

When configured with a built-in GSM modem, the TEK Controller can communicate with the Internet via cell service. This requires service from a local cell provider and only GSM systems are supported. The controller will use the physical Ethernet path if it is available, but automatically switches to GSM if it can't communicate over Ethernet.

The TEK Controller™ Controllers equipped with a GSM/3G/GPS module can communicate with the Internet via mobile cell service. The GSM/3G signal is used to communicate with the server if the Ethernet connection is not available. The switch between Ethernet and GSM is automatic. When the Ethernet connection is available, the TEK Controller automatically communicates via the wire. If the Ethernet connection is not usable, the TEK Controller uses the cellular service to connect to the servers.

Your GSM service must allow data connectivity. The controller only use cellular data. It does not use voice minutes or text messages. Typical data usage for a full month is about 5-10 MB (million bytes), but may vary depending on how frequently logging data is captured and other configuration parameters.


GSM Settings

With most operators, the APN, Login and Password fields can be left blank. In some cases - depending on operator - you may need to enter the GPRS APN, GPRS Login and GPRS Password on the system configurations screen. These settings are different depending on your wireless carrier. You should have received this information with your SIM card if they are required.

Note that these settings must be downloaded into your TEK Controller before the GSM will work. After making the changes, make sure you connect the controller to a working network before you insert the SIM card.

Radio indicator

The Radio LED indicates the status of the cell radio as described in the table below. 'on-blink' refers to that the LED is on most of the time, and pulses off.



Blink pattern	Meaning
off	GSM radio is turned off
on	Waiting for the GSM module to switch on
5 on-blink	Attempting to initialize GSM module
4 on-blink	GSM module requested SIM-PIN.
3 on-blink	Module active. Waiting for GPRS network.
2 on-blink	GPRS network ok. Establishing IP connection.
1 on-blink	Server link dropped. Reinitializing.
Normal blinks	1-5 blinks. Reception quality (e.g. 1-5 "bars" on a cellphone)

GSM Frequencies

The usage of frequencies within the United States is regulated by the [Federal Communications Commission](#) (FCC). The US is then divided geographically into several Trading Areas.

The following table shows the various frequencies used by use cell phone carriers:

CARRIER	NETWORK	3G BANDS	3G FREQUENCIES	4G LTE BANDS	4G LTE FREQUENCIES
AT&T	GSM/UMTS/HSPA+	2, 5	1900, 850	2, 4, 12, 17	1900, 1700 abcde, 700 bc
VERIZON	CDMA	0, 1	850, 1900	2, 4, 13	1900, 1700 f, 700 c
T-MOBILE	GSM/UMTS/HSPA+	2, 4	1900, 1700/2100	2, 4, 12	1900, 1700 def, 700 a
SPRINT	CDMA	10, 1	800, 1900	25, 26, 41	1900 g, 850, 2500
US CELLULAR	CDMA	0, 1	850, 1900	5, 12	850, 700 ab