Technote 88 – Security Best Practices for AcquiSuite/AcquiLite Products as of October 2016

Last Updated: October 11, 2016 1:46 PM

20497 SW Teton Ave, Tualatin, OR 97062
Ph: +1-503-601-2099 Fax: +1-503-601-6878

1 Introduction

This document recommends how to configure the AcquiSuite/AcquiLite products for best security in a variety of situations. These recommendations apply to models:

- A8812 (AcquiSuite),
- A8810 AcquiSuite EMB aka Embedded AcquiSuite),
- A7810 (AcquiLite) and
- A8814 (AcquiSuite+).

In this document, “AcquiSuite” will be used generically to mean both the AcquiSuite and AcquiLite models.

2 Physical Security (including LCD & Button Access)

The AcquiSuite must be physically secured against unauthorized access to the circuit board, to prevent access to the MENU and SELECT buttons, which allow changing the network configuration and (worst case) clearing the unit’s flash memory to factory defaults.

On the A8812 and A8814, this means padlocking the case.

On the A8810 and A7810, this means installing the units in a locked enclosure.

The A8814 has a graphics LCD which may be locked with a user-selected PIN code via the web UI’s “Security >> Touchscreen” menu.

The LCD menu may not be used to reset the “admin” password without also deleting all customer data and configurations, and restoring the unit to factory defaults.

Note that the nature of flash memory means that the “admin” password may still be recoverable if one is able to desolder and directly read the AcquiSuite’s flash memory chip. See Secure Decommissioning.

3 Default Usernames and Passwords

The AcquiSuite has three built-in user accounts, the names of which cannot be changed, plus the standard "root" account used for Tech Support. These are:

- “admin” -- This account has full access to modify any of the system settings. The default password is “admin”.
- “operator” -- This account may view settings, however may only change modbus alarm ranges and device names.
- “user” -- This account can view some system settings including the modbus device status pages and can change nothing.
- "root" -- An internal account which always shares the same password as the "admin" account. It is possible to login as "root" using Telnet, FTP or SSH, assuming these services are enabled, and the other guard conditions mentioned below are satisfied. "Root" bypasses all normal permission checks, and should only be used as directed by Tech Support.

By default, only “admin/root” is enabled.

Internally, the AcquiSuite uses other user accounts, such as "nobody" and "asmodule", to "sandbox" network-facing daemons. The user cannot login to these accounts, and the precise names and purposes are subject to change without notice.

4 Choosing Strong Passwords

Choosing strong passwords is absolutely vital to the overall system security.

As of October 2016 (v02.16.0919), the AcquiSuite allows 64 character, case-sensitive passwords, containing upper- or lowercase, digits and punctuation.

To resist brute force password guessing attacks, the AcquiSuite implements a 3 second delay before responding to invalid login attempts.

“Password Manager” applications for Windows, Android and iOS are one convenient way to create and store these passwords.

See https://en.wikipedia.org/wiki/List_of_password_managers

5 Checking Firmware Versions

Obvius recommends installing the latest available firmware.

Obvius releases firmware updates once or twice per year at no cost to customers.

The versions of all firmware, both core firmware and add-on modules, may be checked via the web UI’s “System >> Firmware Versions” menu.

5.1 Updating to Latest Firmware

Firmware may be installed manually or automatically over Internet for AcquiSuites which have Internet access, or for those that do not, firmware files may be manually uploaded through the browser or via FTP.

To check if you have the latest firmware, go to the “System >> Firmware Versions” page and click “Check for Updates Now”.

Firmware files may be requested from:

Obvius Tech Support
support@obvius.com
+1-503-601-2099

5.2 Auto-Updates?

Automatic firmware updates are enabled by default, and are checked once per week during a normal data-upload cycle.

Automatic updates may be enabled or disabled via the “System >> Firmware Versions” page.

Obvius recommends using automatic updates as the best security trade-off for unattended units accessible from the Internet.

Customers wishing precise control or private LANs without internet access may choose to disable automatic updates and either manually install firmware over the Internet (via "System >> Firmware Versions >> Check for Updates") or request the files from Obvius Tech Support and upload them through the browser (via "System >> Firmware Versions >> Have Disk").

6 Disabling Unneeded Logins

Any of the AcquiSuite’s two optional login accounts (“operator” and “user”) which are not needed should be disabled, via the web UI’s “Security” menu. These accounts are disabled by default.

6.1 Reasons to Use Alternate Accounts (e.g., XML queries)

Many day-to-day functions of the AcquiSuite can be performed using the “operator” and “user” accounts, and this is recommended if possible as it avoids the use of the “admin” password and thereby helps protect that password.

For instance, the AcquiSuite allows querying real-time meter data via XML. These XML requests require HTTP Basic authentication using one of the 3 login accounts. Using the “user” account for these types of machine-to-machine queries helps protect the “admin” and “operator” passwords.

The “user” account may also be used with Obvius’ Enertrax software and with FTP (though for read-only access only).

7 Network Services

7.1 Reviewing Open Ports

Currently open TCP and UDP ports are displayed in “Networking >> Status”.

7.2 Telnet, FTP, SSH – Disabled by Default

Telnet, FTP and SSH are disabled by default.

These services are not required for normal operation, and are used for remote debugging, tech support and file transfers.

These may be enabled via “Networking >> Setup”, but Obvius recommends leaving Telnet and FTP disabled unless absolutely necessary.

SSH ("Secure Shell") and SCP ("Secure Copy") are a modern replacement for Telnet and FTP, providing industry-standard strong encryption and authentication. Obvius recommends using SSH and SCP; Telnet and FTP should only be used for legacy compatibility.

To help you avoid accidentally leaving these services enabled, the AcquiSuite provides an option to enable these services for a limited amount of time (5 minutes, 1 hour or 24 hours).

7.3 Telnet, FTP, SSH Disallowed from "Public IP's" Until Admin Password Has Been Changed

As a further safe-guard, even if Telnet, FTP or SSH have been enabled, logins are not accepted from "Public" IPv4 addresses until the "admin" password has been changed.

"Public" IPv4 addresses mean all addresses except those reserved for private IP networks, i.e.,

- 192.168.*.*
- 172.16-31.*.*
- 10.*.*.*
- 169.*.*.*

A typical use-case for this feature is to allow the AcquiSuite to be physically installed at the end of a DSL or cable modem line (with no intervening firewall for protection, and with its factory default password of "admin"), and to then be remotely configured over the Internet, where the password is changed to its final one.

See https://en.wikipedia.org/wiki/Private_network

7.4 UPNP – Disable after Installation

The UPnP (Universal Plug-and-Play) service allows the AcquiSuite to "announce" itself to other computers on the network, to simplify initial set up. This service is enabled by default, and is especially convenient when a DHCP server isn't available and a Ethernet cross-over cable is being used to directly connect between a laptop and the AcquiSuite.

Obvius recommends disabling the UPnP service after set up. This may be done via "Network >> Setup".

The AcquiSuite's current IP address will always be available on its LCD. On the A8812, A8810 and A7810 models, press the SELECT button repeatedly to cycle through the display information.

7.5 Modbus/TCP, BACnet/IP Access Control – Ports 502, 503, etc. and 47808

The Modbus/TCP and (optionally) BACnet/IP protocols allow sharing of meter data from the AcquiSuite via these protocols.

Ports 502, and optionally 503 thru 511 are used for Modbus/TCP.

Port 47808 (unless changed) is used for BACnet/IP (based on UDP).

The AcquiSuite allows 3 levels of access control for these services, which is configured in the “Modbus >> Setup” page:

- No access
- Access from local IP subnet only
- Access from any IP subnet

These access control settings are inherited by other protocols, such as BACnet/IP.

Obvius recommends setting the *minimum sufficient level* of access.

7.6 SSH Algorithms, Keys and Features

As of October 2016, the AcquiSuite supports SSH and SCP as a "secure" alternative to Telnet and FTP.

If enabled, SSH listens on TCP port 22.

The AcquiSuite uses the open-source "Dropbear SSH" implementation, and includes the "ssh", "scp", "dropbearkey" and "dropbearconvert" command-line utilties for advanced users.

The AcquiSuite supports ECDSA, DSS and RSA host keys. An ECDSA host key is generated at first boot, and the DSS and RSA host keys are generated on first use of these algorithms. The host keys are stored at /etc/sysconfig/dropbear_{ecdsa,rsa,dss}_host_key in the AcquiSuite's filesystem and are only accessible to "root". SSH host keys are deleted as part of resetting the AcquiSuite to factory defaults (see Secure Decommissioning).

The AcquiSuite supports SSH port forwarding, both local (-L) and remote (-R).

Users may force these host keys to be regenerated by logging in as "root" and deleting the existing files, and then rebooting the AcquiSuite with the "reboot" command.

8 SSL/TLS

The AcquiSuite supports the SSL/TLS family of protocols for:

- uploading data,
- web login access and
- real-time meter data queries via XML.
- automatic and manual firmware updates from https://www.BuildingManagerOnline.com.

Using these features requires first installing two add-on software modules, which are available at no cost to all customers. These modules are:

- Obvius_SSLUpload – provides SSL/TLS upload and remote login, via OpenSSL.
- AcquiSuite_RootCerts – provides the current trusted Root CA certificate database.

These add-on modules may be installed via the AcquiSuite's "System >> Firmware Versions" menu, by clicking "Check for Updates Now", then clicking "Show Optional Modules", and installing each one, or contacting Obvius Tech Support to request the files for manual installation.

Obvius generally reviews and updates these modules once per year.

8.1 OpenSSL

As of October 2016, Obvius_SSLUpload is based on OpenSSL 1.0.1p.

Once the Obvius_SSLUpload module is installed, the version of OpenSSL is displayed on the "SSL >> Setup" web page.

8.2 OpenSSL "Heartbleed" Bug

The so-called "Heartbleed" bug affected many systems using OpenSSL, including the AcquiSuite.

As of July 2015, Obvius_SSLUpload includes an updated OpenSSL 1.0.1h to fix the "heartbleed" bug and also disables the TLS Heartbeat extension to make it easier to verify that the problem is fixed by remote scanning.

As of October 2016, Obvius_SSLUpload includes OpenSSL 1.0.1p.

Because of the nature of the "Heartbleed" vulnerability, which potentially allowed password and private key information to be undetectably revealed to attackers, Obvius advises customers upgrading from earlier versions of Obvius_SSLUpload on AcquiSuites *which were accessible for SSL/TLS login from the Internet* to also take the following steps:

- Change all passwords on the AcquiSuite after upgrading.
- Revoke and change all custom certificates installed on the AcquiSuite.
- Change server upload passwords.

8.3 SSL/TLS Protocols Supported

What is informally called "SSL/TLS" is actually a family of protocols: SSL, SSLv2, SSLv3, TLSv1.0, TLSv1.1, etc.

As of October 2016, Obvius supports TLS 1.0. SSLv3 and earlier are disabled.

8.4 FIPS 140-2 Mode

"FIPS 140-2" is a U.S. Government security standard for cryptography modules.

See https://en.wikipedia.org/wiki/FIPS_140-2

The Obvius_SSLUpload add-on module supports FIPS 140-2 mode, which is enabled by default via a checkbox on the "SSL >> Setup" page.

Obvius recommends using FIPS 140-2 mode for best security.

If FIPS 140-2 mode is disabled, connections will still be encrypted via SSL/TLS to current industry standards, but the cipher suites chosen will favor speed over security and may not be FIPS 140-2 certified.

8.4.1 FIPS 140-2 Certification

Obvius' FIPS 140-2 certification is inherited from the OpenSSL project.

As of October 2016, Obvius uses OpenSSL's v2.0.x "cryptographic module", which has received FIPS 140-2 certificate number 1747. This certificate is available from NIST.GOV at the following URL:

http://csrc.nist.gov/groups/STM/cmvp/documents/140-1/140val-all.htm#1747

See also: https://www.openssl.org/docs/fips/fipsvalidation.html

8.5 Uploading over SSL/TLS

Once Obvius_SSLUpload and Acquisuite_RootCerts are installed, the AcquiSuite will have several new upload protocol options in its "Log File Data >> Setup/Upload" page.

To begin uploading meter data over SSL/TLS,

- the upload server must support SSL/TLS,
- a new upload protocol must be selected and
- the appropriate HTTPS:// URL must be entered in the "Log File Data >> Setup/Upload" page.

Both Obvius' "BuildingManagerOnline.com" (BMO) and Leviton' "LevitoBMO.com" servers support SSL/TLS uploads at no additional cost, using the same URL as is used for unencrypted uploads.

Obvius' recommends uploading over SSL/TLS as it protects privacy of the data, the privacy of the upload password and authenticates the upload server.

When validating an upload server's certificate, the AcquiSuite supports Subject Alternative Name (SAN) certificates and domain wildcard certificates.

8.6 Login via SSL/TLS

The Obvius_SSLUpload add-on module also enables HTTPS web browser access to the AcquiSuite.

8.6.1 Force HTTPS Login

The "Force HTTPS Login" option in "SSL >> Setup" redirects all unencrypted HTTP (port 80) connections to the AcquiSuite to HTTPS (port 443).

Obvius recommends the “Force HTTPS Login” option for best security; it is off by default.

Obvius strongly recommends this option if the AcquiSuite is accessible from the public Internet.

Note that if real-time meter data is being queried via XML, this option will redirect those queries to use SSL/TLS connections as well.

8.6.2 Custom certificate with Fixed Hostname or Static IP Address

For secure web login via SSL/TLS, the AcquiSuite must be configured with a validly-signed web server certificate.

This certificate must be obtained from a legitimate Certificate Authority. See https://en.wikipedia.org/wiki/Certificate_authority

This certificate must contain the AcquiSuite’s hostname or IP address, which implies that the AcquiSuite must be installed with either a permanent, fully-qualified domain name or with a static IP address.

Once obtained, this certificate can be uploaded to the AcquiSuite via the “SSL >> Setup” page.

8.6.3 Self-signed, auto-generated certificate

To facilitate initial set up, the AcquiSuite will generate a temporary, invalid, self-signed certificate when the Obvius_SSLUpload module is first installed.

A self-signed certificate is, by definition, not properly signed by a legitimate Certificate Authority, and will be rejected by web browsers.

A self-signed certificate should not be used for normal operation as it is vulnerable to Man-in-the-Middle impersonation attacks.

8.7 Root CA Certificates aka "Trust Store"

The AcquiSuite's Root CA certificate database is provided by an AcquiSuite Module named "AcquiSuite_RootCerts.asmodule.cramfs", which may be installed or updated via "System >> Firmware Versions" free of charge.

"AcquiSuite_RootCerts" tracks the Root CA certs provided by The Mozilla Project for the Firefox browser, and includes specific additions such as the US Government DoD PKI certificates.

Obvius periodically reviews these certificates and may remove certificates from CA's deemed not trustworthy.

Details and fingerprints of the particular Root CA Certificates included may be viewed two ways:

1. Go to "SSL >> Setup", and click "trusted root certificates".
   If the above link is not present, Obvius recommends updating the Obvius_SSLUpload module

and the AcquiSuite_RootCerts module to their latest versions, via "System >> Firmware Versions".

2. Alternately, go to "System >> Firmware Versions", locate the "AcquiSuite_RootCerts" module and click the "?" (help) icon.

9 Firewall Minimum Requirements

This section discusses the absolute minimum firewall requirements for customers installing the AcquiSuite behind firewalls.

9.1 Firewall Configuration for DNS and Time Servers

Generally speaking, if the AcquiSuite is uploading to a server specified by a hostname as opposed to an IP address, the AcquiSuite will require access to a DNS server to resolve that hostname. If this DNS server is outside the firewall, the firewall should be configured to allow DNS traffic on UDP port 53 both in and out.

The AcquiSuite may also be configured to synchronize its clock to a time server using either the NTP or RDATE protocols. By default, the AcquiSuite will automatically select a time server and protocol. The NTP protocol requires that the firewall allow UDP traffic to and from destination port 123, and the RDATE protocol requires that the firewall allow TCP connections to destination port 37.

See https://tools.ietf.org/html/rfc868 for RDATE and https://tools.ietf.org/html/rfc1305 for NTP.

9.2 Firewall Configuration for Data Upload via "Building Manager Online" (BMO) Protocol

The Obvius "Building Manager Online" or "BMO" protocol is based on HTTP, and requires an outgoing TCP connection to destination port 80.

If the SSL/TLS version of this protocol is being used, it will require an outgoing TCP connection to destination port 443.

9.3 Firewall Configuration for Data Upload via FTP

The Obvius FTP Upload protocol uses the unencrypted FTP protocol, and supports both FTP Active and Passive modes. The FTP mode is automatically detected based on the firewall configuration between the AcquiSuite and the FTP server.

Obvius recommends AGAINST using FTP where security is a concern, because FTP connections are not encrypted nor strongly authenticated.

If FTP must be used, Obvius strongly recommends configuring your firewall and/or FTP server to allow Passive-mode connections.

The required firewall configuration for FTP Passive Mode is to allow outgoing connections on TCP destination ports 20 and 21. *Note this is for a firewall at the AcquiSuite end of the connection.* Any

firewall protecting the FTP server would need to allow incoming TCP connections to ports 20 and 21.

9.4 Firewall Configuration for Remote Web Login Access

If you wish to allow remote login access to the AcquiSuite via a web browser, Obvius strongly recommends installing the Obvius_SSLUpload add-on module, and enabling the "Force HTTPS Login" option and other options as discussed above.

To allow remote login access via the web, the firewall must allow incoming TCP connections on port 80 (if not using Obvius_SSLUpload) or on port 443 (if using Obvius_SSLUpload).

9.5 Firewall Configuration for Automatic Firmware Updates

To allow automatic firmware updates, your firewall must allow outgoing connections on TCP port 80, to the host www.buildingmanageronline.com. If Obvius_SSLUpload is installed, the AcquiSuite will check for firmware updates over HTTPS, and your firewall should allow TCP port 443.

9.6 Firewall Configuration for Telnet, FTP and SSH

Telnet, FTP and SSH are all disabled by default. Obvius recommends that customer firewalls be configured to block incoming TCP connections to these services:

FTP -- TCP port 20 and 21
SSH -- TCP port 22
Telnet -- TCP port 23

If remote Tech Support access is required, Obvius' "Remote Access" feature discussed below is a safer and easier alternative.

9.7 Firewall Configuration for AcquiSuite "Remote Access"

As of October 2016, the AcquiSuite includes a feature called "Remote Access", which is off by default. This feature allows the customer to grant secure, remote access to an AcquiSuite to Obvius Tech Support, while avoiding the dangers and complications of opening holes in firewalls.

See TN97 "AcquiSuite Remote Access" for full details.

If enabled, "Remote Access" makes an *outgoing* TCP connection to TCP port 2022 on www.buildingmanageronline.com. The "Remote Access" feature is based on the mature SSHv2 protocol.

This feature should only be enabled at the direction of Obvius Tech Support. It is enabled or disabled via the AcquiSuite's LCD menu and/or "Networking >> Setup" page.

Even if "Remote Access" is enabled, the "admin" password is still required to login to the AcquiSuite.

10 "Allow Remote Configuration" and Upload Channel 1

Obvius' "Building Manager Online" upload protocol includes the ability to synchronize configuration files with the AcquiSuite (upload or download). Obvius calls this feature "remote configuration", and it is available when using the "Building Manager Online" protocol, whether to an Obvius server or to a 3rd party server.

As of July 2015, the AcquiSuite supports up to four upload channels, each to a different server. Upload channel 1 is unique in two ways:

- All upload channels using the "Building Manager Online" protocol will receive configuration files from the AcquiSuite (upload). Only channel 1 allows downloading (changing or modifying) of configuration files to the AcquiSuite, and only if the "Allow remote configuration" option in "Log FIle Data >> Setup/Upload" is checked (which is so by default).
- The "Building Manager Online" server on channel 1 (if any) will receive configuration files containing the passwords of all other upload channels (this is necessary to allow remote configuration). "Building Manager Online" servers on channels 2 through 4 (if any) will receive configuration files, such sensitive fields such as passwords for other channels will be suppressed.

The bottom line is, if you are using multiple upload channels and if channel 1 is set for the "Building Manager Online" protocol, channel 1's server will be able to "see" the upload passwords and server URLs of all other upload channels in the uploaded configuration files. If you do not wish to reveal this information, use the "Building Manager Online" protocol on channels 2 through 4 instead of 1.

Note that the upload server passwords discussed above have no relation to the AcquiSuite's login passwords (for "admin", "operator" and "user").

11 Anti-Virus Software

The AcquiSuite product family are embedded devices with limited CPU and memory resources, and so is unable to execute the anti-virus software typically used on desktop PCs.

11.1 AcquiSuite Security Hardening

The AcquiSuite has numerous features designed to minimize the risk of introducing malicious code, such as:

- The AcquiSuite runs a custom Linux kernel in which all unnecessary features have been disabled and compiled out.
- "Loadable kernel modules", a feature common on desktop computers, has been permanently disabled to block a common path for loading rootkits and malicious code.
- The AcquiSuite's network servers which listen for connections either run as a non-"root" user, or are configured so that access from the general network without password authentication is disabled by default.
- The AcquiSuite's filesystem permissions are configured by default to provide the minimal access to non-root processes.
- The AcquiSuite's filesystem mount options are configured so that the filesystem is not both "writable" and "executable" at the same time, preventing the execution of malicious code if it

somehow is able to be loaded, even if loaded by user “root”.

- The command shell and command utilities (e.g., Busybox) are configured with the minimum required functionality.
- Telnet and FTP services are disabled by default to prevent automated password guessing.
- If Telnet is enabled, Telnet login is still disallowed from non-local subnets (e.g., any public IP address) unless the system’s administrator (root) password has been changed from the default.
- Access to particularly troublesome command utilities like “wget” are blocked from Telnet login sessions, to prevent their use for propagating viruses.
- With our SSLUpload module, the AcquiSuite can be configured to require SSL/TLS authentication for administrative login.
- The AcquiSuite is configured by default to check for and automatically install firmware updates once per week.
- Any known weak point that is found is taken care of with a firmware update should none of the existing feature set have a method to prevent the unit from being exploitable.

12 Logging

The AcquiSuite provides several logs for diagnosing and auditing system behavior. All logs are accessible via "System >> System Log Files". A summary of recent activity is shown on the AcquiSuite's "Welcome" page.

For security purposes, the most relevant logs are these:

1. "System Boot Log" -- shows system reboots and recent logins and login attempts, with source IP address.
2. "Install Log" -- shows manual and automatic firmware installation attempts.
3. "Time Change Log" -- shows major adjustments to the system clock.
4. "FTP Connection Log" -- shows file transfers via FTP.

13 Transparency

The AcquiSuite includes diagnostic and inspection tools such as:

1. "root" login,
2. "Processes >> Advanced" page, accessible via "System >> Processes >> Advanced".

The "Processes >> Advanced" tool allows viewing near real time statistics on all processes running on an AcquiSuite.

Process List

PID	PPID	PGRP	PRI	NI	UPTIME	RSS	Priv RSS	ST	WCHAN	cpu U+S	% awake	childs' cpu U+S	% active	COMMAND
5134	5133	366	20	0	0	652	96	St	pipe_wait	0+0	0	0+0	0	/usr/local/thttpd/thttpd -M 900 -D
5133	366	366	5	-15	0	476	136	R<	(running)	14+18	100.00	0+0	100.00	statprocv.cgi
2232	1	2232	20	0	58m	304	108	S	hrtimer_nanosleep	1+3	0.00	0+0	0.00	/sbin/rungetty Dialin disabled
456	1	456	20	0	2h28m34	524	132	S	hrtimer_nanosleep	2011+1219	0.36	0+0	0.36	/as/bin/uibconsole
399	398	399	20	0	2h39m49	368	84	S	do_sys_poll	3+7	0.00	15+21	0.00	-sh
398	365	398	20	0	2h39m49	340	76	S	do_select	3+29	0.00	0+0	0.00	/sbin/telnetd
394	386	386	20	0	2h39m58	1836	1620	S	do_sys_poll	371+12	0.04	0+0	0.04	Obvius_SSLUpload/bin/stunnel /var
387	1	387	20	0	2h40m7	292	100	S	hrtimer_nanosleep	179+411	0.06	0+0	0.06	Obvius_Xmem/xmemd running
386	1	386	20	0	2h40m7	400	200	S	do_select	9+21	0.00	374+105	0.05	Obvius_SSLUpload/bin/stund idle, s
385	1	385	20	0	2h40m7	520	148	S	do_select	114+182	0.03	0+0	0.03	/as/bin/miniupnpd -i eth0 -a eth0
384	1	384	20	0	2h40m7	520	144	S	hrtimer_nanosleep	5+10	0.00	0+0	0.00	/as/bin/ra-agentd R-A disabled
382	1	382	25	5	2h40m7	660	208	SN	do_select	89+248	0.04	519+621	0.15	/as/bin/senddata @ Tuesday, Octob
358	1	358	18	-2	2h40m12	292	84	S<	hrtimer_nanosleep	77+88	0.02	0+0	0.02	/sbin/tempmon 33.7C BL:on p30 B
366	1	366	20	0	2h40m12	764	164	S	do_sys_poll	540+1408	0.20	4931+8434	1.59	/usr/local/thttpd/thttpd -M 900 -D
365	1	365	20	0	2h40m12	316	76	S	do_select	0+2	0.00	352+81	0.05	/sbin/inetd -f
364	1	364	20	0	2h40m12	340	56	S	do_sys_poll	0+8	0.00	0+0	0.00	/bin/sh
363	1	363	24	4	2h40m12	484	132	SN	hrtimer_nanosleep	6+73	0.01	0+0	0.01	/as/bin/mhdatalog Disabled
362	1	362	24	4	2h40m12	720	152	SN	hrtimer_nanosleep	81+42	0.01	0+0	0.01	/as/bin/modbusdiscover Idle
361	1	361	20	0	2h40m12	1032	424	S	hrtimer_nanosleep	77+203	0.03	0+0	0.03	/as/bin/modbusloggerd idle/updates

Typically uses of the "Process Advanced" page include:

1. Detecting process crashes by sorting by UPTIME.
2. Auditing security by examining open file handles of each process ("o" option).
3. Locating unexpected processes.

14 Development Process

Obvius develops and maintains the AcquiSuite products with the following engineering processes:

1. Design and code reviews;
2. Unit tests;
3. Automated hardware and software stress testing;
4. Source code control and version tracking;
5. All firmware built from sources -- no pre-built binaries used;
6. Continuous monitoring of software security news for relevant open-source packages;
7. Automatic (entirely unattended) firmware update mechanism available for customers who wish to use it;
8. Vulnerability scanning with common security tools such as: nmap, ncrack, Nessus, Qualys' SSL Labs Server Test, HP's WebInspect, etc.
9. System health monitoring of units in the field, uploaded during checking for firmware updates or of meter data to www.buildingmanageronline.com (examples: uptime, reason for reboot, PCB temperature and voltage, firmware versions; full details of uploaded statistics may be seen by going to "Log File Data >> Setup/Upload", and setting "Upload debug information" = "Full Debug with Trace").

15 Secure Decommissioning

At minimum, to securely decommission the AcquiSuite, the unit should be reset to the factory default state, which deletes all meter data and all configuration files. This can be performed via the LCD even if the "admin" password is not known.

Resetting to the factory default state deletes all stored passwords, meter data and configuration settings, but due to the nature of flash memory this data may still be recoverable if one has the ability to directly probe the AcquiSuite's flash memory chip.

For further security when decommissioning, the AcquiSuite's login passwords should be not reused, any upload passwords should be changed and any SSL/TLS certificates should be revoked.

If an even more secure decommissioning is required, Obvius recommends that the AcquiSuite PCB be physically melted.

Revisions to this document:
July 8, 2015: initial publication.
July 10, 2015: minor updates, review comments.
October 11, 2016: updates for the v02.16.0919 security improvements and for SSH/SCP.