SAGE™

REFERENCE MANUAL

Contents

General Description

A Fully Integrated Solution

SAGE™ works seamlessly with all of our real-time monitoring products (SteamEye®, AIM®, The Brain®) ensuring that it always has access to the most current data on your critical steam traps and hot water systems. As a current Armstrong smart-product customer, our experts will be there to ensure that your transition to SAGE™ is smooth and easy.

SAGE™ Mobile – Our Exclusive Mobile App

Survey your steam traps with efficiency and accuracy using the free, native Apple application included with SAGE™. SAGE™ Mobile enables you to perform steam trap surveys with your iPhone, iPad or iTouch device—even when no Internet connection is available. It includes our Squares Status Updates, and an intuitive user interface that provides the quickest way to manually update the condition of your traps. SAGE™ Mobile saves you time and increases accuracy as it quickly gathers your data and stores it locally, automatically pushing it to SAGE™ as soon as you have access to a network connection.

Manual Collection and Input

If you rely on manual data collection from the field, SAGE™ offers all the flexibility you need. SAGE™ easily accommodates the manual input of all your collected data until the time is right to begin using real-time monitoring or our mobile app.

High-Level Security

SAGE™ was designed with your security in mind. YOU OWN YOUR DATA and SAGE™ keeps it safe and protected. The enterprise-class cloud-managed IaaS is built on recognized technology platforms and operated from a Tier 3+ data center for 99.982% uptime. Our fully hosted solution is backed by guaranteed high-level security that includes automated backups, https encryption and SSAE 16 compliance.

Unprecedented Flexibility

Whether you have one building or multiple facilities throughout the world, 10 traps or 10,000, one Brain® or 10, SAGE™ allows you to manage your entire organization or company, regardless of size. Use SAGE™ Nests and Groups to organize and manage your equipment population with ease, as well as to customize how your data is filtered throughout the system. Viewing only relevant equipment increases the efficiency of maintenance personnel, while seeing the entire organization gives global energy managers the advantage of comprehensive information.

Complete Accessibility

SAGE™ is easily accessible from virtually any device, wherever you are, at any time. It performs beautifully on tablets, laptops and desktop computers, and it is compatible with most common Internet browsers, including Google Chrome, Internet Explorer and Safari. SAGE™ is designed to be responsive, so whether you're using a PC in your office or an iPad out in the field, the format will adapt to the size and resolution of your screen.

Adding A New User

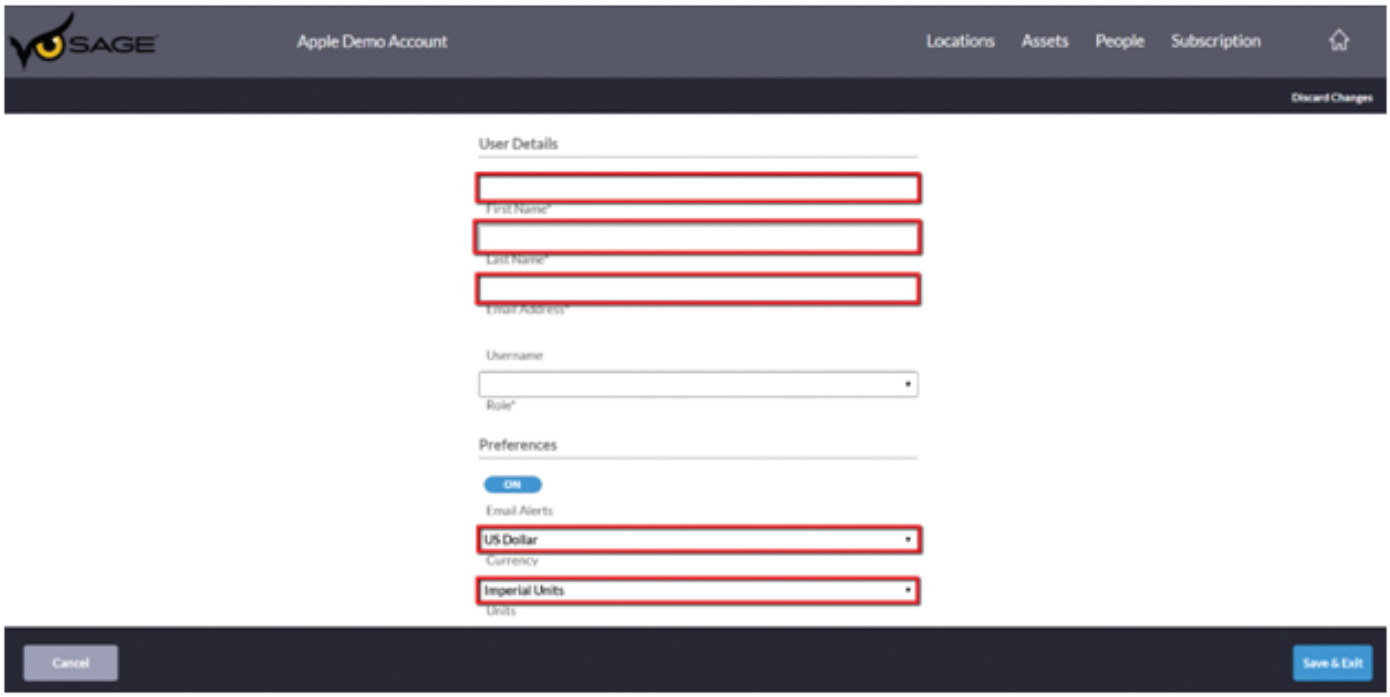
To add a new user

1) Click the cogwheel

2) Click **People**

3) Click **Add**

4) Add
   a. First Name
   b. Last Name
   c. Email Address
   d. Currency
   e. Units



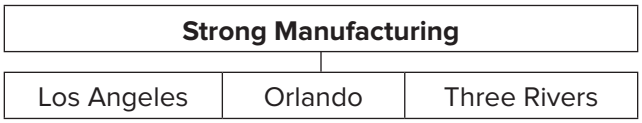
5) The user will receive an automated email to finalize account setup

SAGE™ - Locations, Nests & Groups

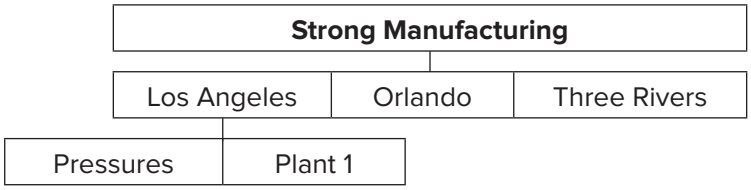
SAGE™ makes it easy to organize the information about your locations and systems. It uses a structure as follows:

The **Company Name** is at the top of the structure. Let's use Strong Manufacturing as an example.

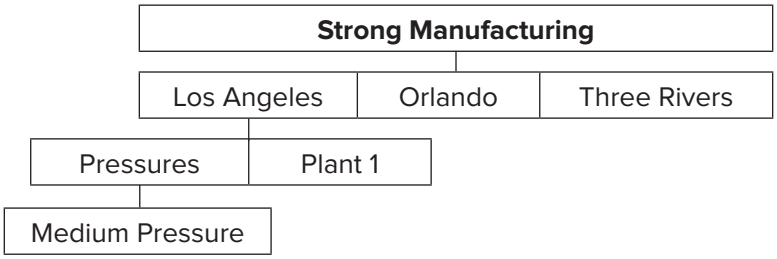
You can have multiple Locations within the Company. Strong Manufacturing has locations in Los Angeles, Orlando & Three Rivers



You can create Nests within the Locations – like several buildings in one area. In the Los Angeles area, there is a Pressures & Plant 1.



And Groups can be buildings and equipment within those Nests. We can have a group named 'Medium Pressure' and that group includes all of the equipment for that particular building.



You might think of the relationship between groups and nests this way: A group of eggs goes into a nest.

Let's see how it works within SAGE™

Strong Manufacturing is the Company Name.

Click the cogwheel to see Strong Manufacturing's three locations. Let's look at just the Three Rivers location. Select it, and click 'Apply' (see Figure 1 below).

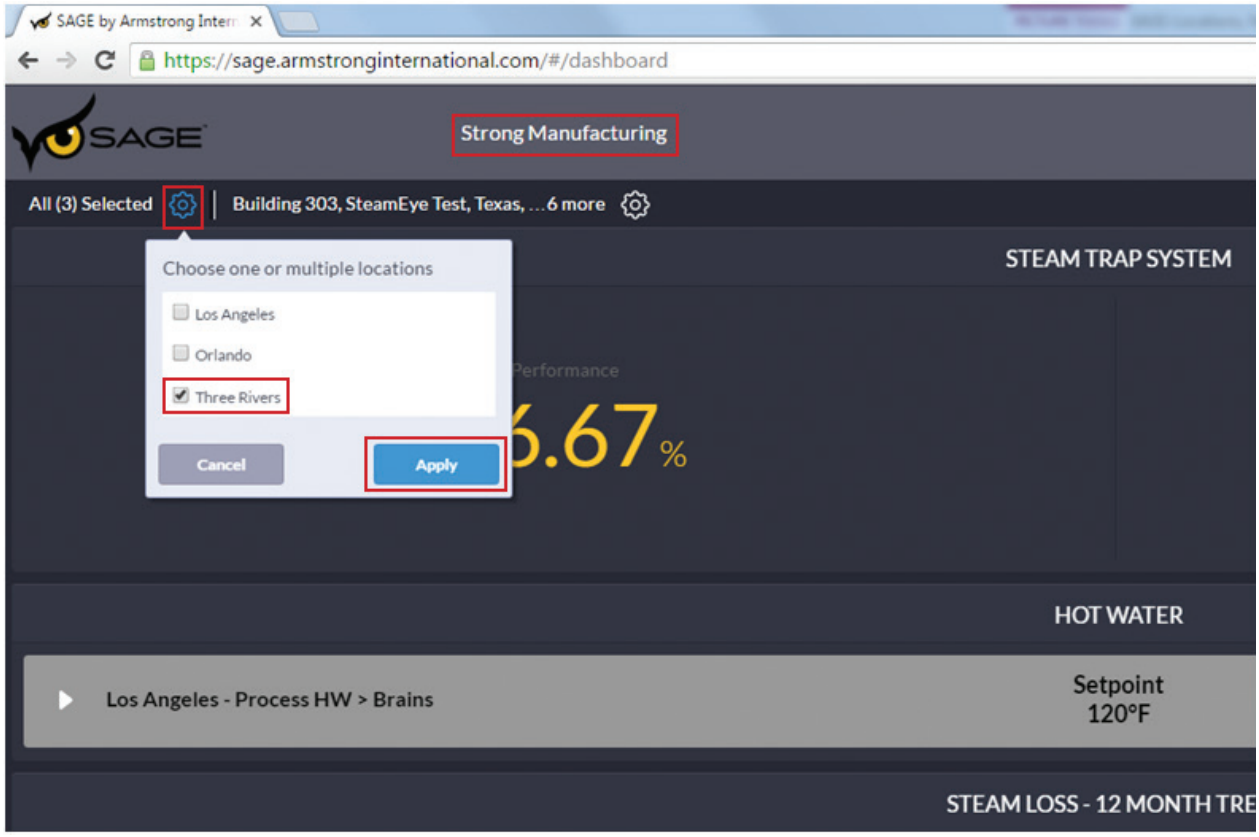


Figure 1

Click the cogwheel to the right, and you'll see there are two Nests, 'Plant 1' and 'Pressures'. We'll select just 'Pressures'. Within the 'Pressures' nest, we will select the Medium Pressure group. Click 'Apply' and the Dashboard will display the data for the Medium Pressure (see Figure 2 below).

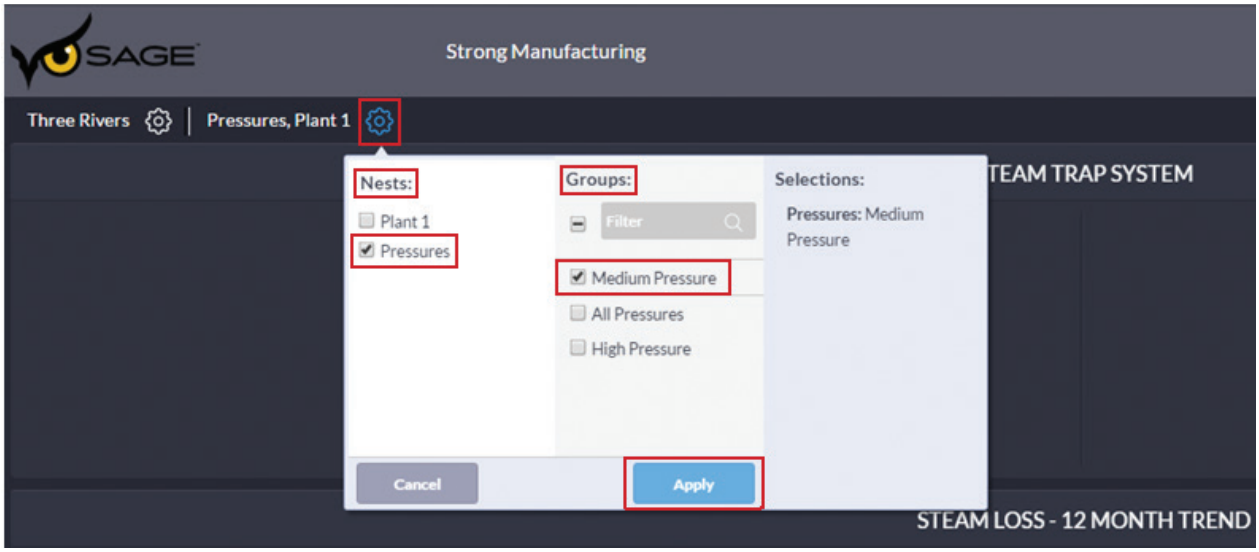


Figure 2

You can add Locations, Nests and Groups as follows.

To add a Location

Click the SAGE™ icon to return to the Dashboard. Click the cogwheel at the upper right (see Figure 3 below).

Figure 3

Select ‘Locations.’ You will see the three locations already in SAGE™. Click ‘Add Location,’ enter the Location Name, and change the Currency, if necessary. Click ‘Add Row’ to enter Steam Pressure and Steam Cost. If the Location uses multiple Steam Pressures, click ‘Add Row’ again. When you’re done, click ‘Save’ (see Figure 4 below).

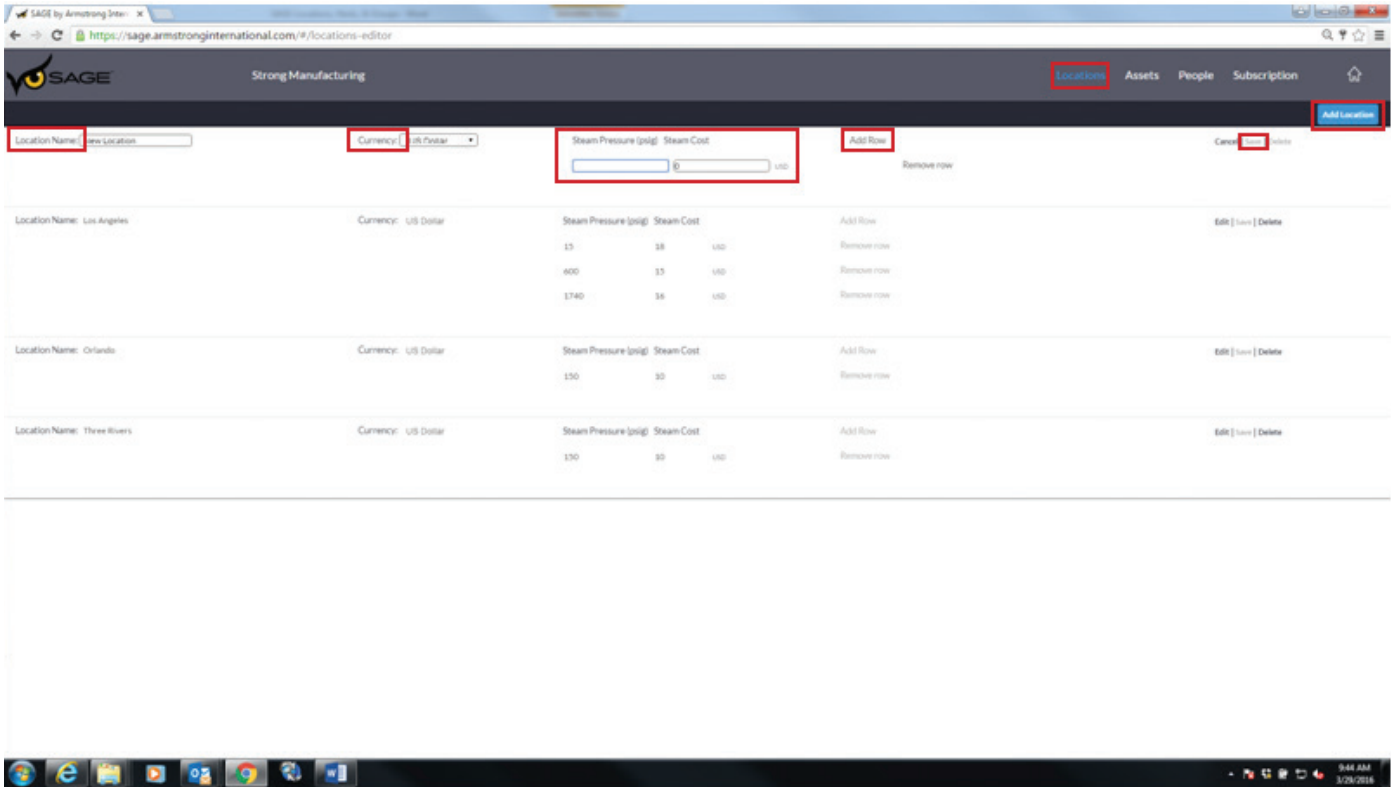


Figure 4

To add a Nest

Click the SAGE™ icon to return to the Dashboard. Click the cogwheel at the upper right (see Figure 5 below).

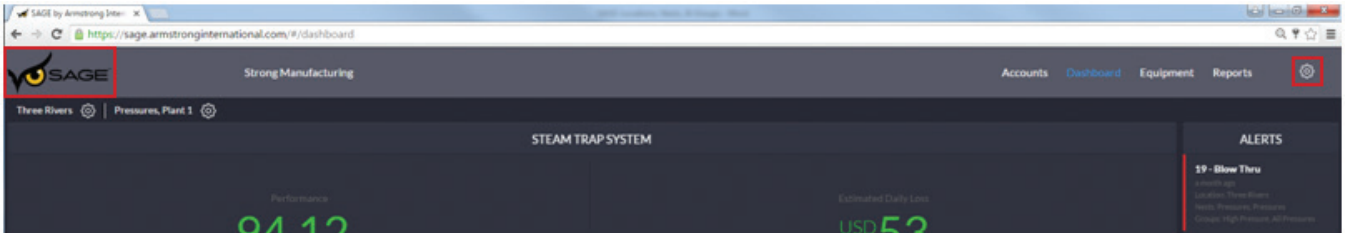


Figure 5

On the left, you'll find the current list of nests. Click 'Add Nest' (see Figure 6). Give the new nest a name. To assign groups already created to the nest check the box, then click 'Save and Exit' (see Figure 7 below).

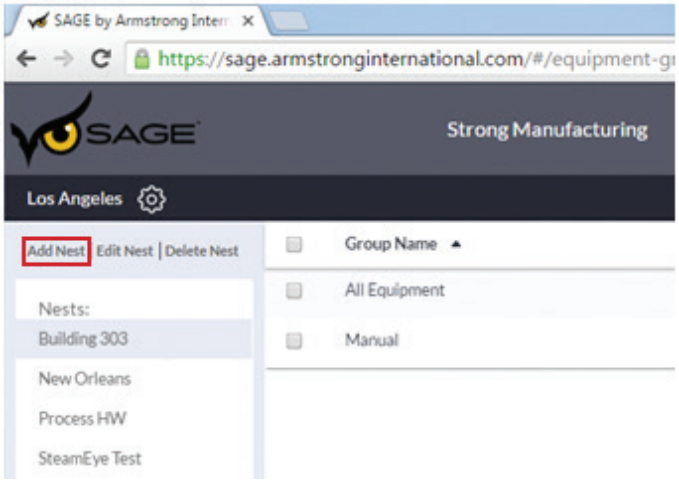


Figure 6

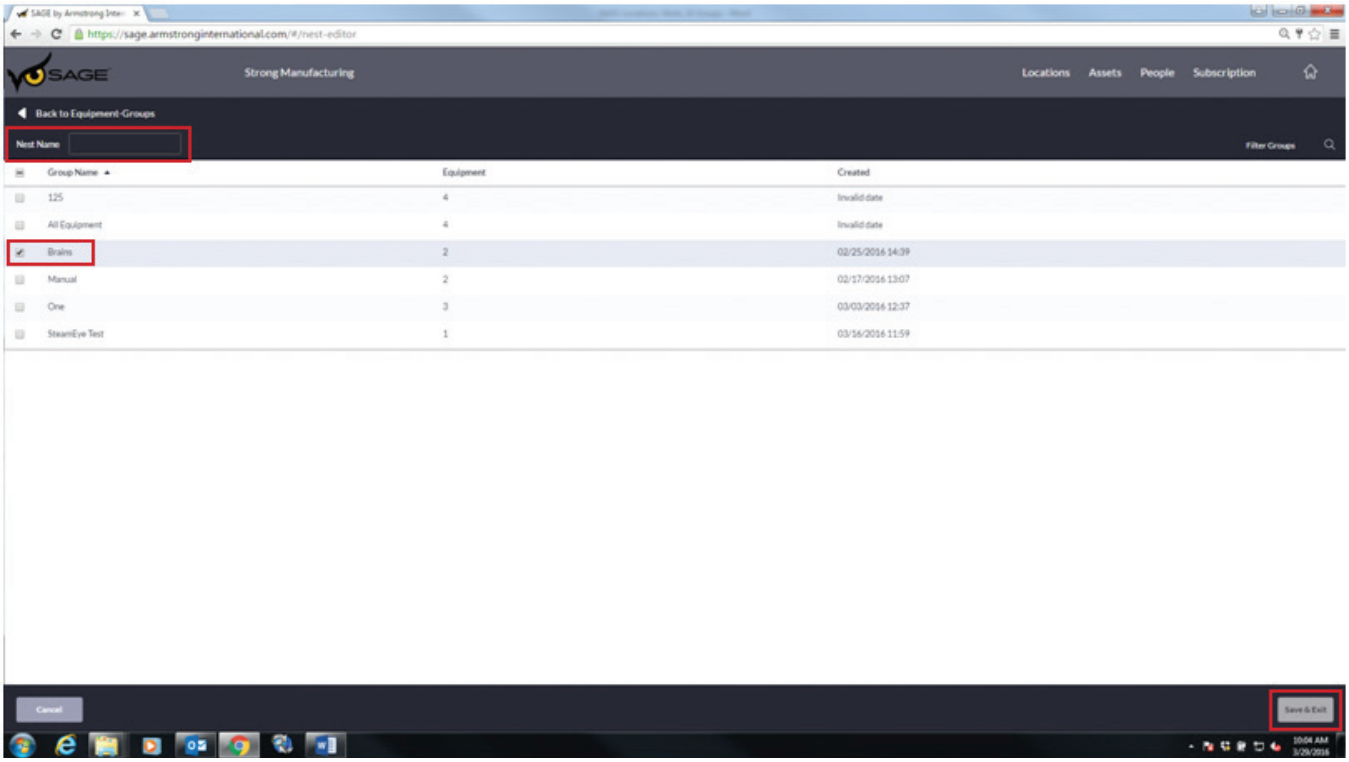


Figure 7

To add a Group

Click the SAGE™ icon to return to the Dashboard. Click the cogwheel at the upper right (see Figure 8 below).

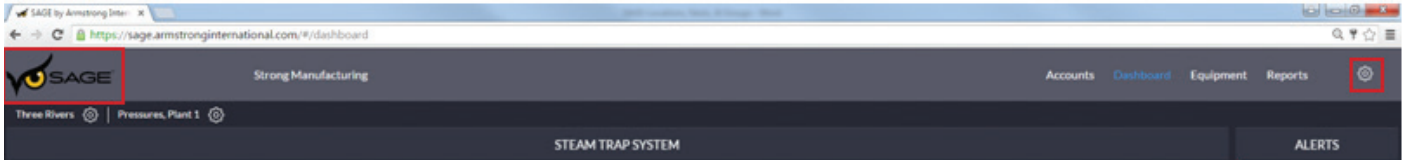


Figure 8

Click 'Add group,' enter the Group Name, and indicate which nest it is under (see Figure 9 below). Select the equipment that will be part of that group, then click 'Save and Exit' (see Figure 10 below).

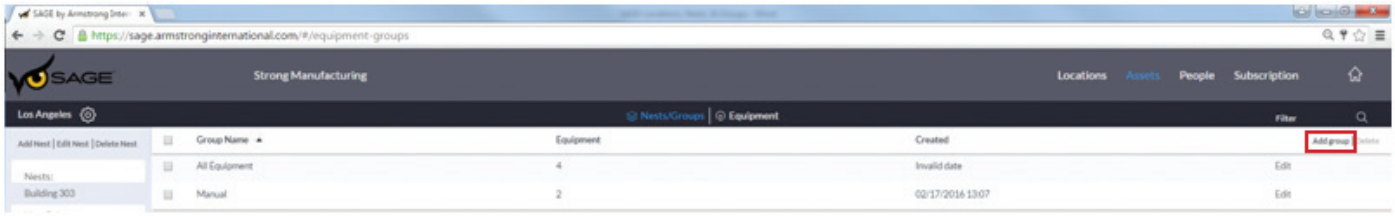


Figure 9

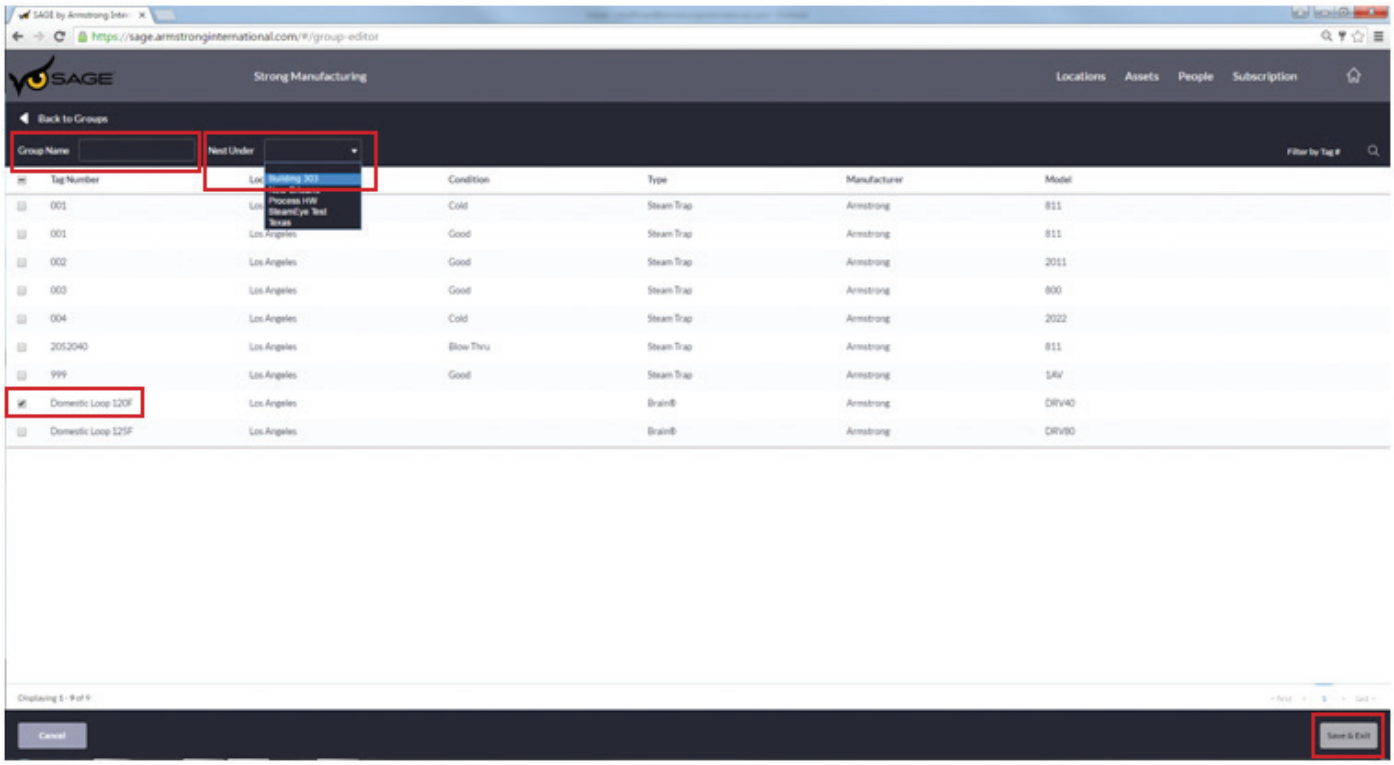


Figure 10

SAGE™ Support

As always, SAGE™ support is readily available via video chat, telephone or email (see Figure 11 below).

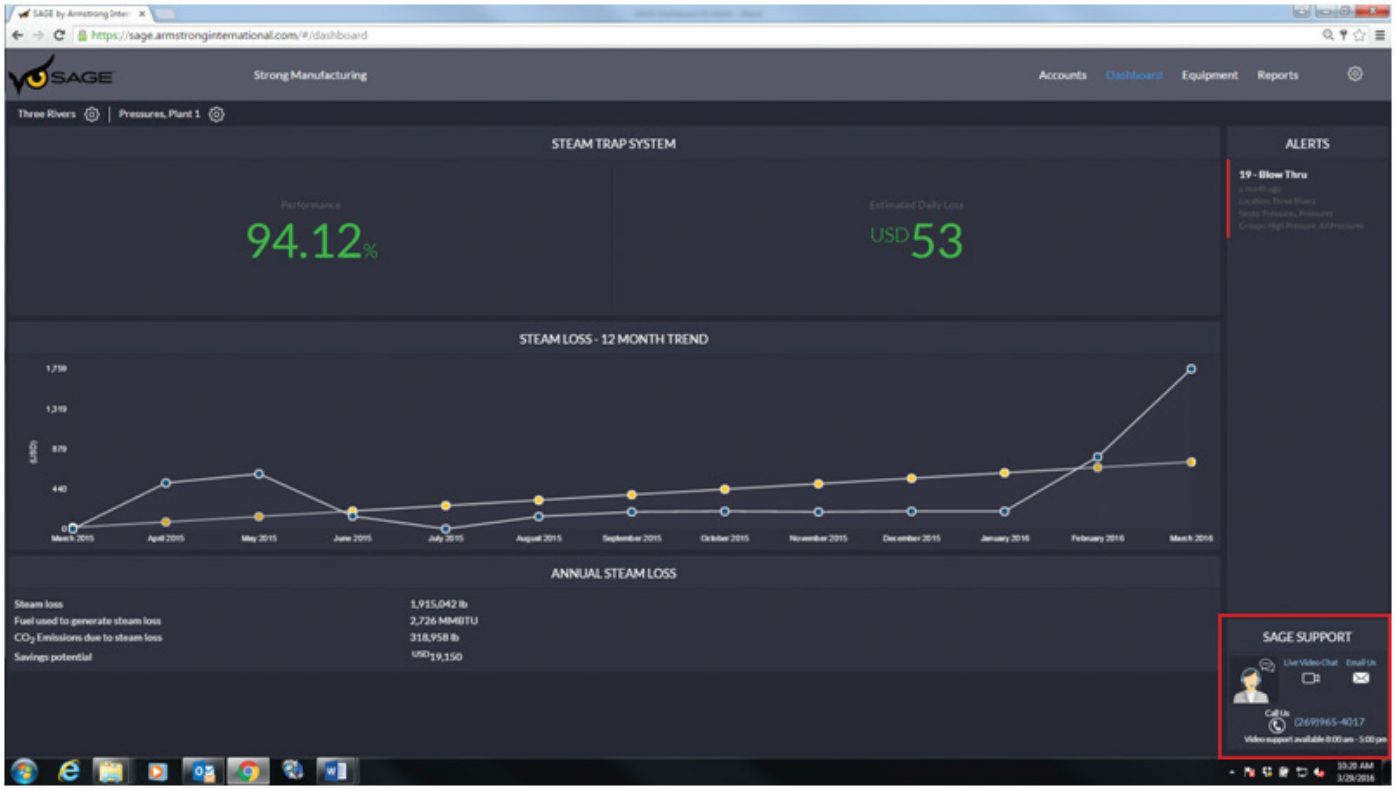


Figure 11

SAGE™ - Equipment (Hot Water)

It's easy to add equipment to SAGE™.

From the home page, click the top right cogwheel (see Figure 1 below).

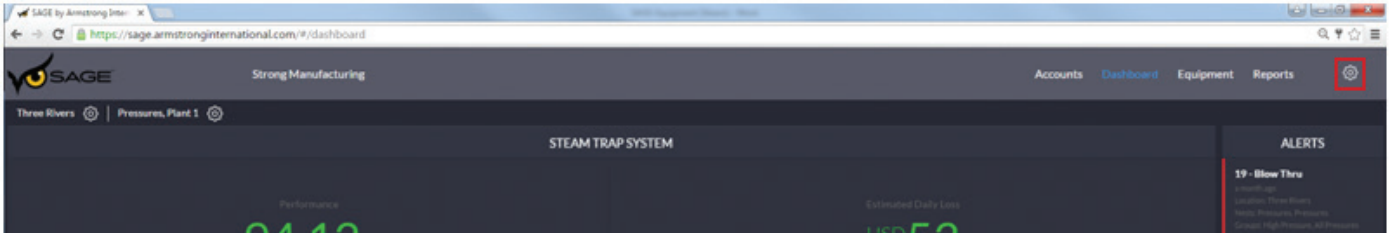


Figure 1

The complete assets list is displayed and you can add a steam trap or add The Brain®. Let's add The Brain®. Click 'Add brain.' (see Figure 2 below).

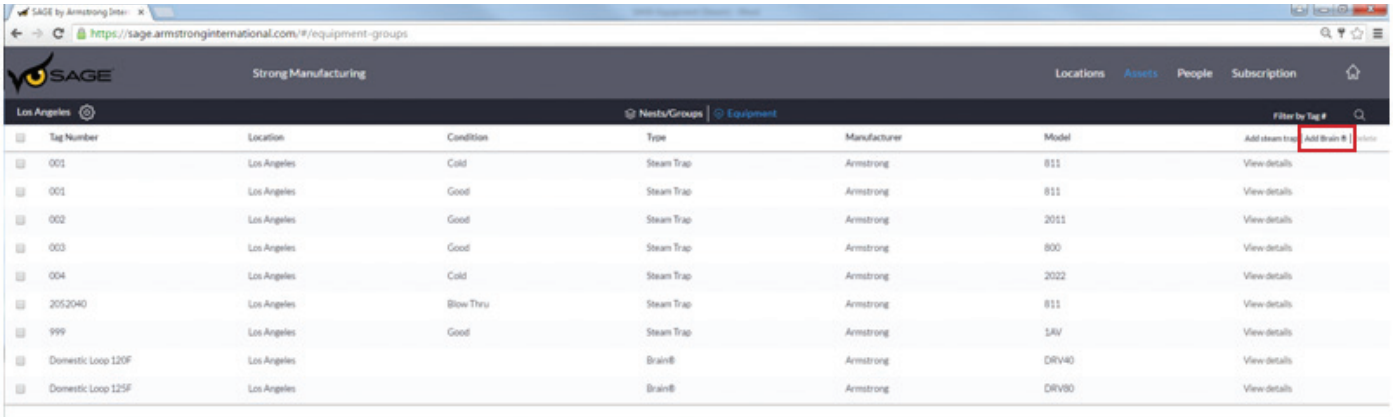


Figure 2

Start by entering the Tag number for The Brain®. Alternatively, some customers like to use the temperature loop name to differentiate it – like Domestic Loop 120°F or Domestic Loop 125°F. You can also add an image of the trap itself.

The Brain® scan ID is a unique ID number assigned to that specific Brain – much like a serial number.

Valve number indicates which valve; 'Valve 1' or 'Valve 2' it is in the system if the system contains more than 1 valve.

Armstrong is the exclusive manufacturer of The Brain®.

Finally, indicate the model number.

Once The Brain® is connected to SAGE™, the serial number, Last disinfection date will be filled in automatically. The user must fill in the commissioned date.

When you have entered all the information for this new Brain, click ‘Save and Exit,’ and you will be returned to the equipment list. (see Figure 3 below).

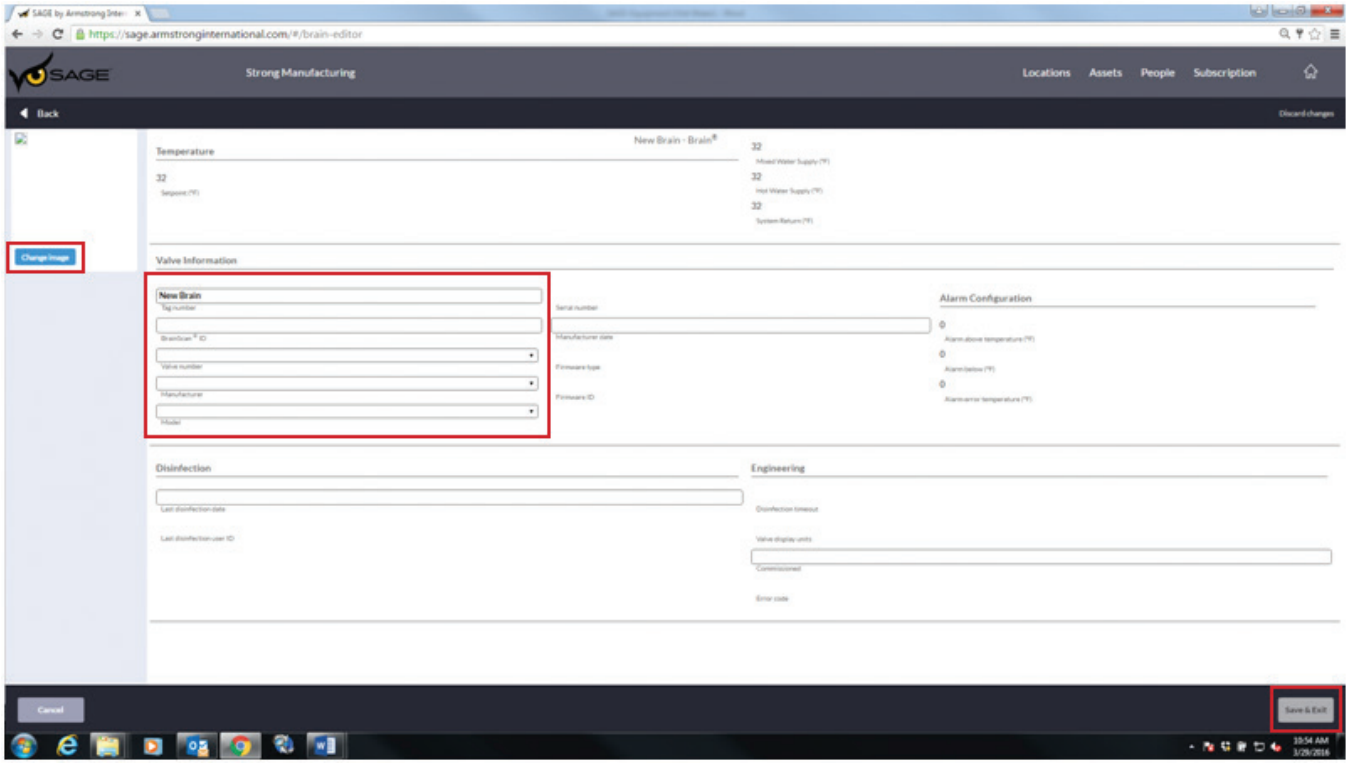


Figure 3

You can then sort the equipment list by Tag Number and see that the new Brain has been added to the list. Or, you can type in the Tag Number to search and find it (see Figure 4 below).

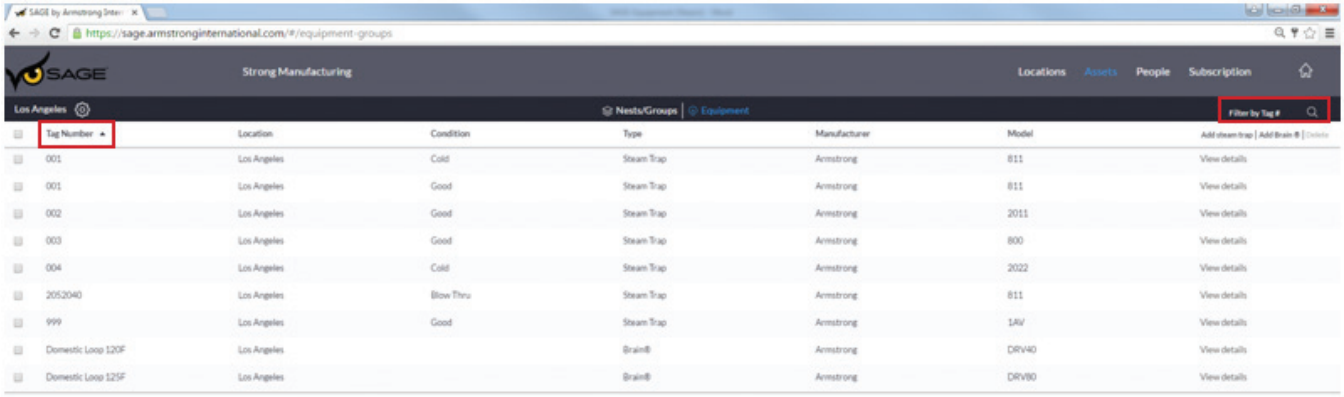


Figure 4

As always, SAGE™ support is readily available via video chat, telephone or email (see Figure 5 below).

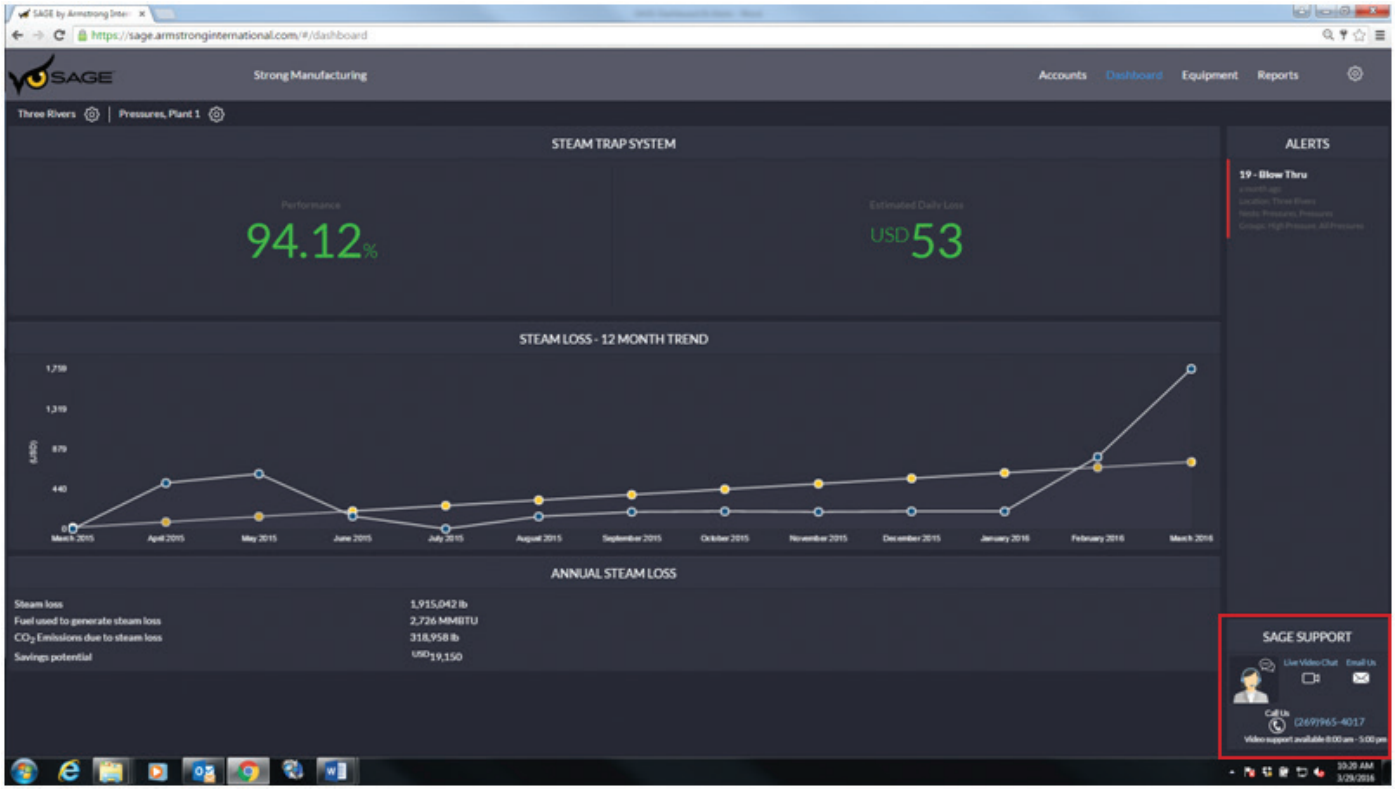


Figure 5

SAGE™ - Equipment (Steam)

It's easy to add equipment to SAGE™.

From the home page, click the top right cogwheel (see Figure 1 below).

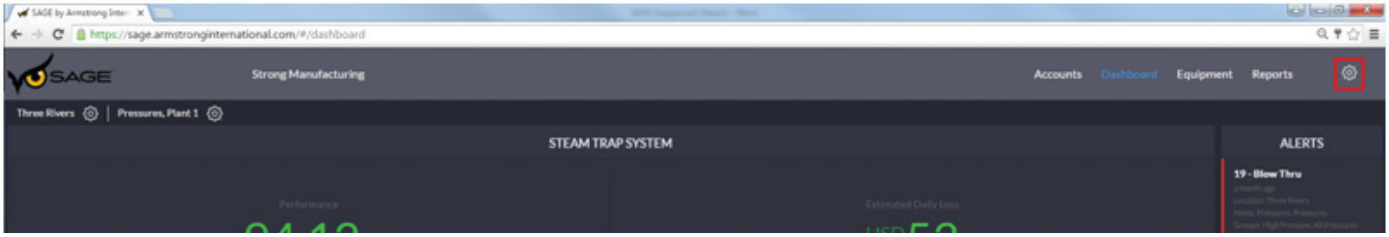


Figure 1

The complete assets list is displayed and you can add a steam trap or add a Brain. Let's add a steam trap. Click 'Add steam trap' (see Figure 2 below).

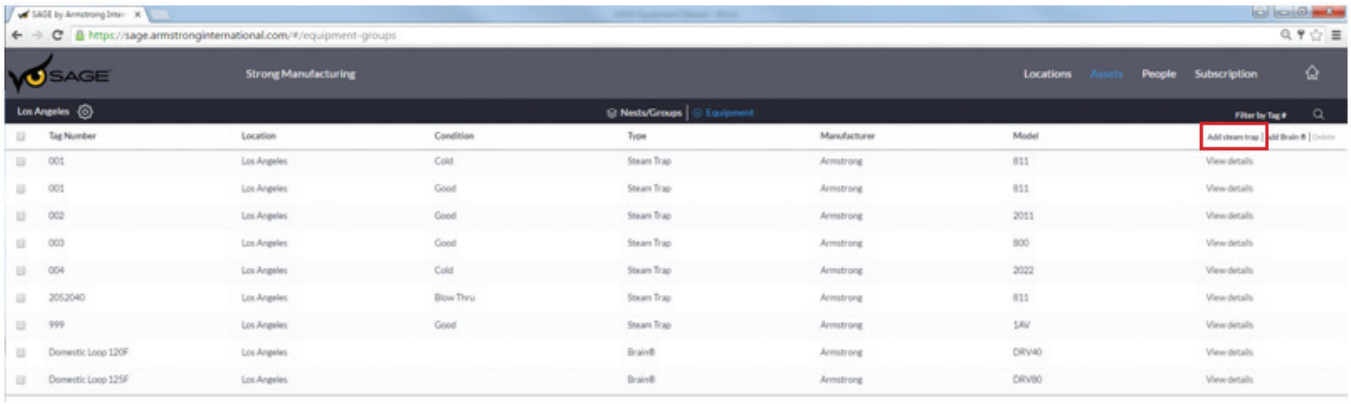


Figure 2

Start by indicating the condition of the trap. You can also add an image of the trap itself. Data entry fields circled in red are required items. Start with the Installation date, then continue to fill in the required fields. Some of the fields are pre-populated, so you simply click, scroll to the item you want, then click it to select it. If the field does not have a dropdown menu, simply input the necessary information manually.

You can optionally include additional information, such as Connection type, Line size in, Pipe orientation, and more. Adding this information can help you to replace a failed steam trap without first having to go out into the field – all of that information is saved in SAGE.

You can add specifics about the valves surrounding the trap, and there is a freeform section for Notes. This could be useful if, for example, the trap is in an unusual location – you can add details on where to find it.

When you have entered all the information for this new steam trap, click 'Save and Exit,' and you will be returned to the equipment list (see Figure 3 below).

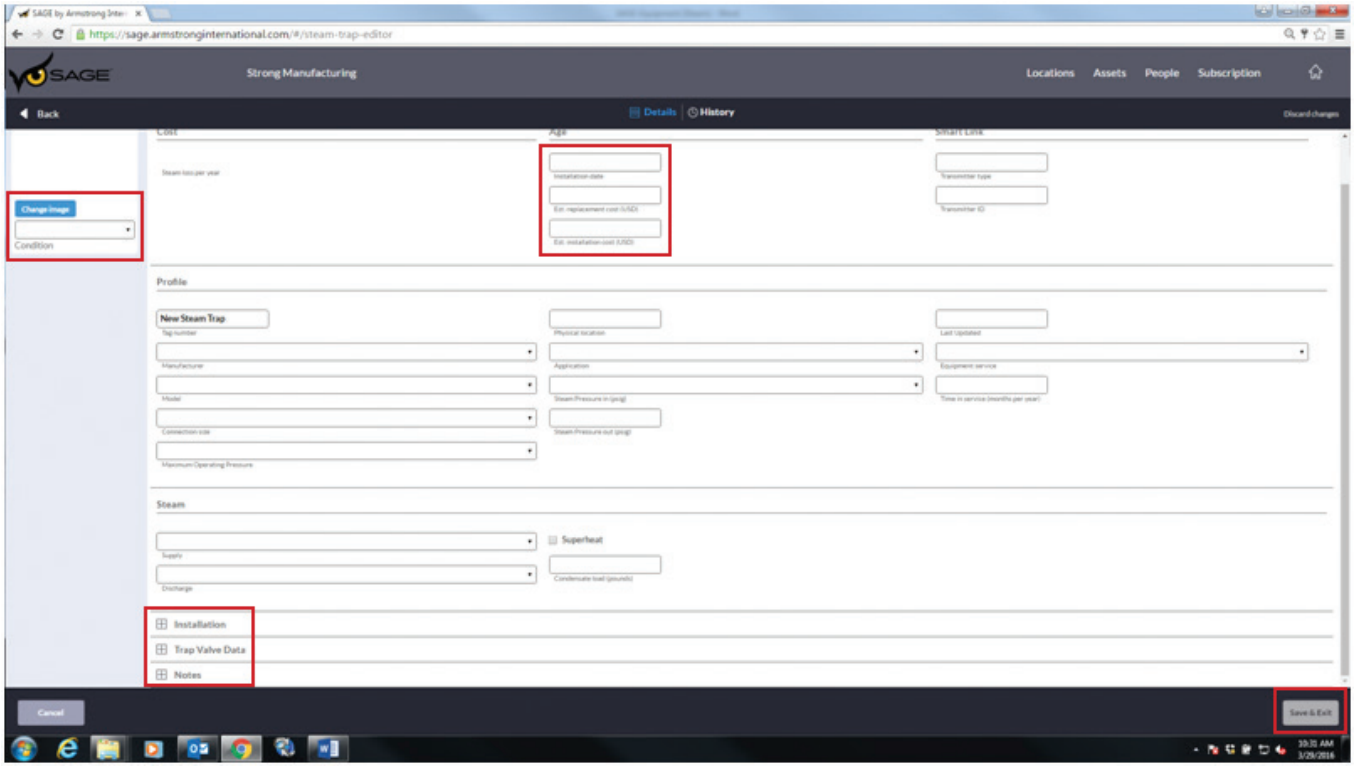


Figure 3

You can then sort the equipment list by Tag Number and see that the new trap has been added to the list. Or, you can type in the Tag Number to search and find it (see Figure 4 below).

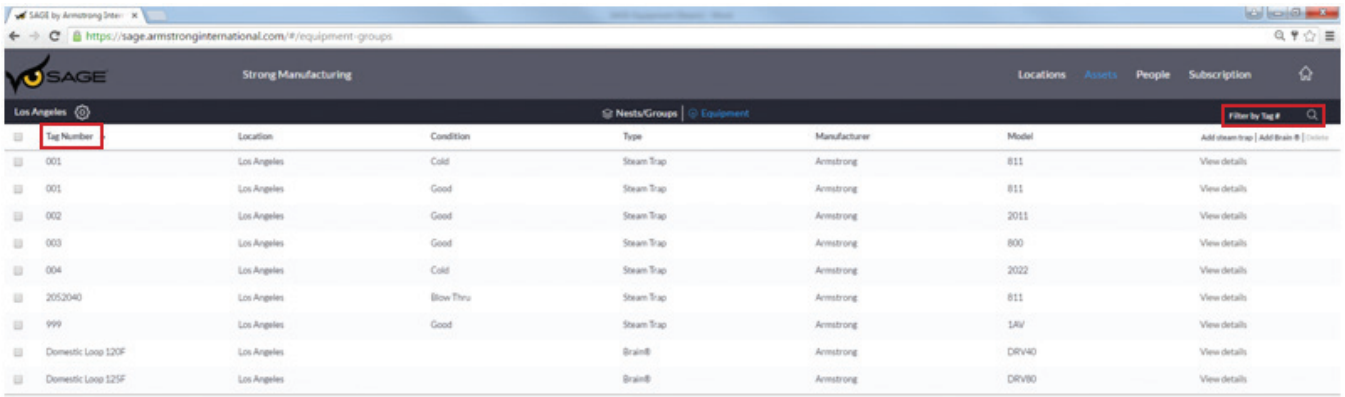


Figure 4

As always, SAGE™ support is readily available via video chat, telephone or email (see Figure 5 below).

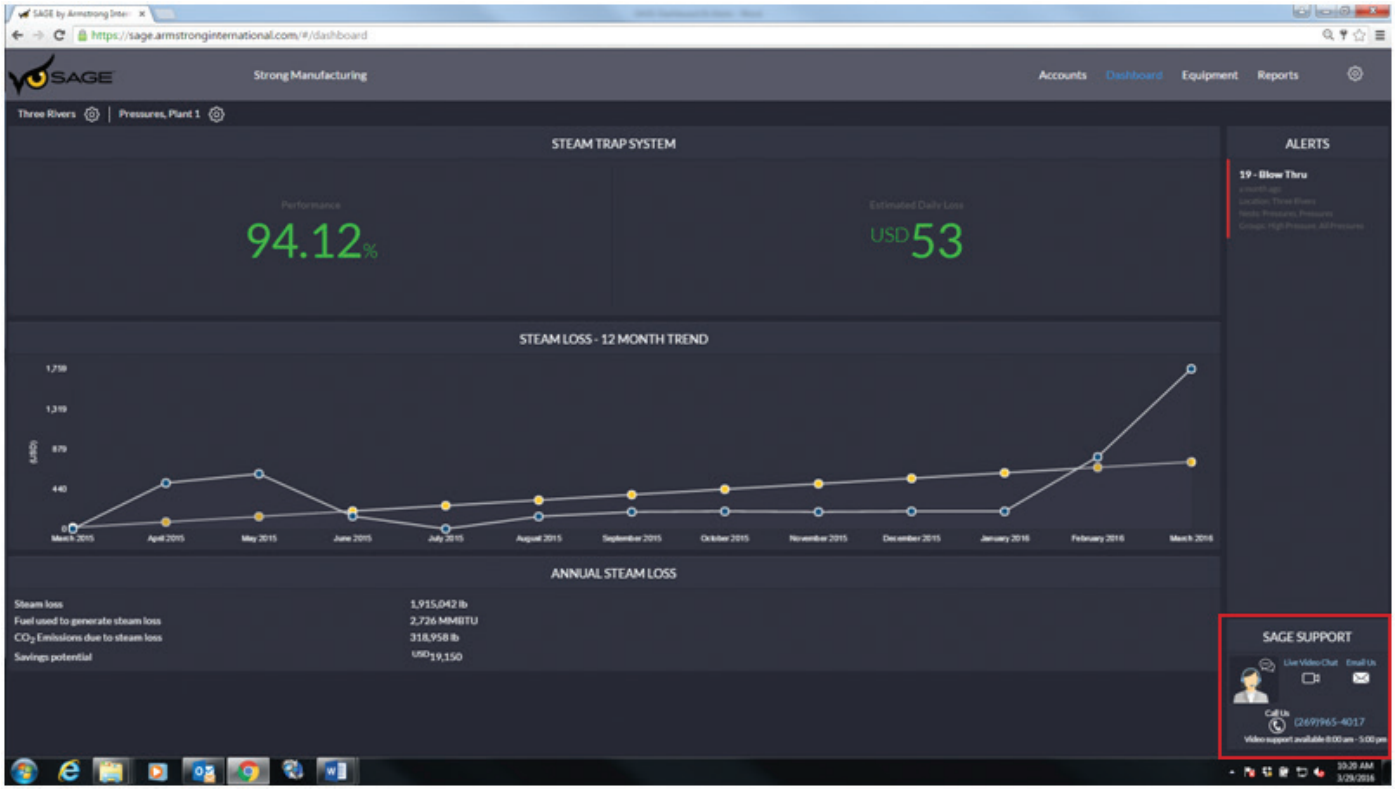


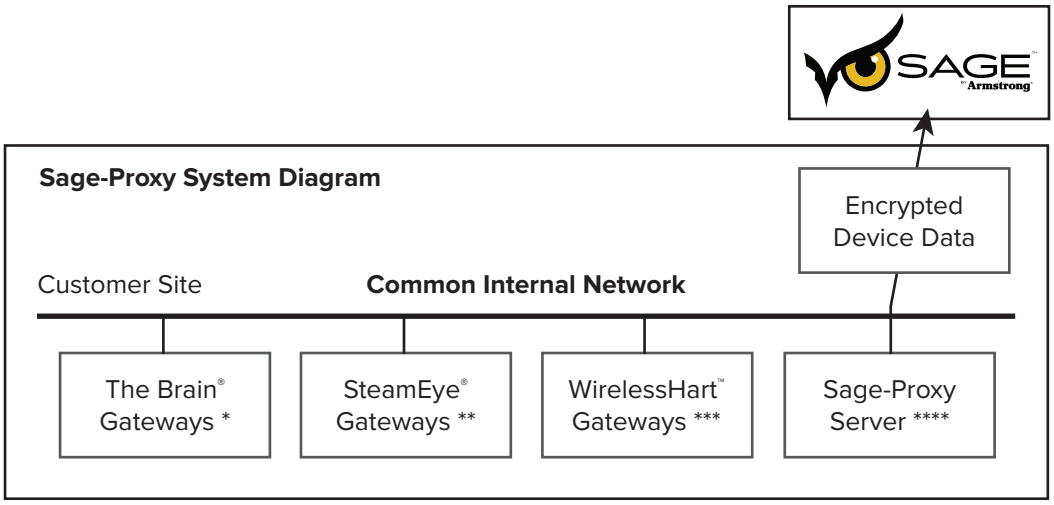
Figure 5


Armstrong®
SAGE™ PROXY SOFTWARE

Installing Sage™ Proxy on Windows – 1.0.6 (current)

Introduction

Sage-Proxy is the real-time monitoring piece of SAGE™ that allows collecting and viewing of equipment data virtually as it happens. The Proxy is an application that is usually installed on a local machine of the Site where real time monitoring is to be performed. It runs as a service in the background and can be accessed by its web interface using a web browser. Although Sage-Proxy can be installed on multiple operating system platforms, this manual refers to installation on Windows. Sage-Proxy collects the device data and sends it to SAGE™ as it is collected where the data is stored and analyzed for alerting and reporting.



* The Brain® gateways monitor Armstrong hot water valves that regulate temperature, called Brains.

** SteamEye® gateways capture status changes of steam traps.

*** WirelessHart™ gateways record status data for every monitored steam trap at fixed intervals, usually 5 minutes.

**** Sage-Proxy (server can be a pc) collects the data from all gateways and sends it to SAGE™ for permanent storage and analytical processing.

Requirements

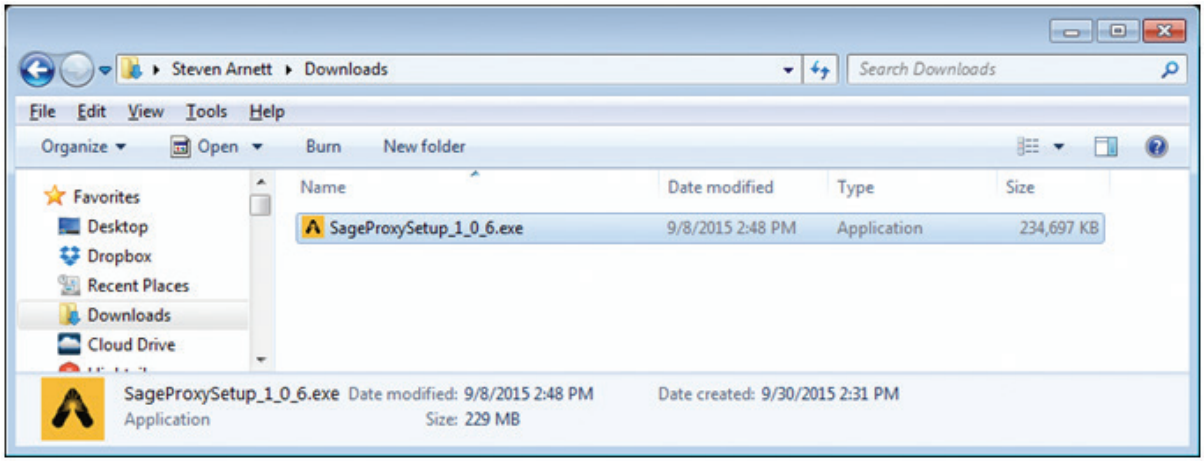
1. PC or Server - Windows 7 or later 32 or 64 bit. Recommended: at least Windows 7 (64-bit). Windows Server 2008 R2 SP1 (64-bit) or Windows Server 2012 (64-bit).
2. Minimum Hardware:

Windows	OS Bits	CPU (minimum)	CPU (recommended)	RAM (minimum)	RAM (recommended)	Free Disk Space
7	32	1.0 GHz	2.6 GHz	1 GB	2 GB	20 GB
7	64	1.0 GHz	2.6 GHz	2 GB	4 GB	20 GB
8.1	32 and 64	2.6 GHz	Dual 2.6 GHz	2 GB	4 GB	40 GB
Server 2008	64	1.4 GHz	2.6 GHz	1 GB	2 GB	40 GB
Server 2012	64	1.4 GHz	2.6 GHz	1 G	2 GB	40 GB

3. Internet Explorer 9.0 or greater, Chrome or Firefox browser (does not have to be on the same computer, but on the same network).
4. The Sage Proxy machine needs to run 24/7/365 to collect all data.
5. Internet access for sending data to Sage and downloading installer.
6. Network access to the gateways that are to be monitored.
7. It's recommended that Sage Proxy should run on a dedicated machine for large scale monitoring.

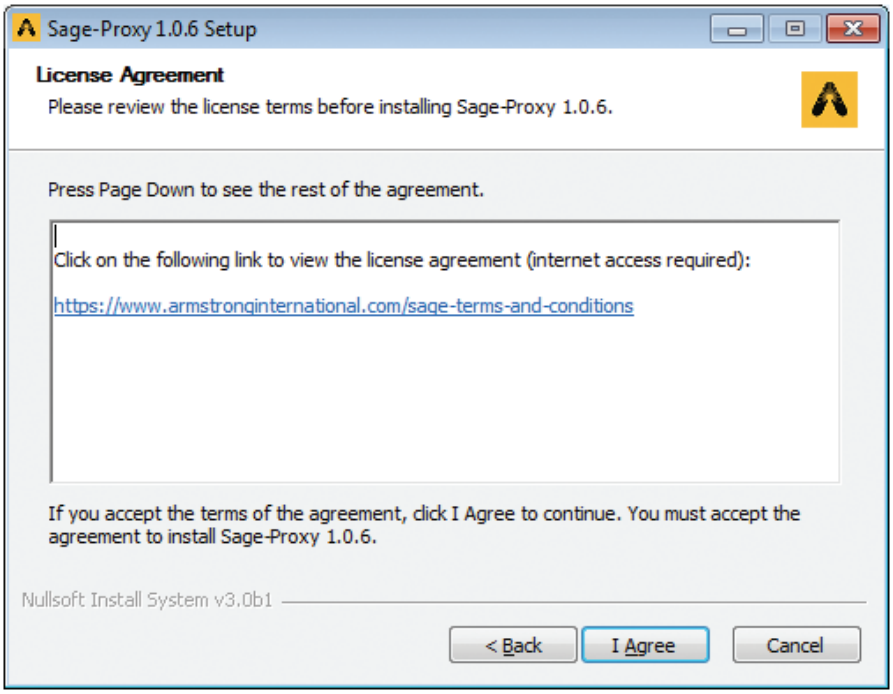
Requirements

Download the window installer at Download Sage-Proxy. By default, it will end up in your Downloads folder.

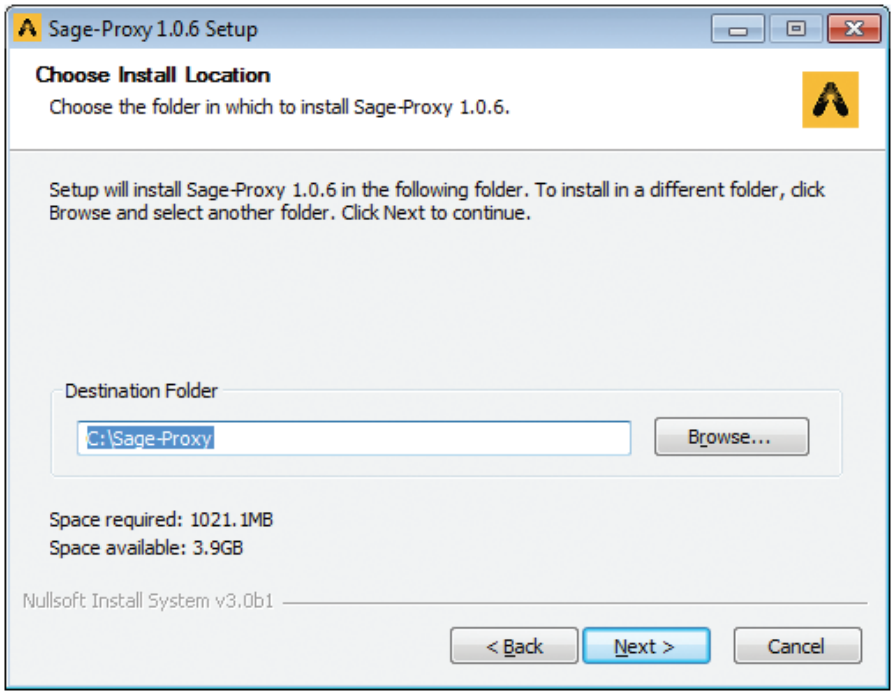


Double click it to run the installer.

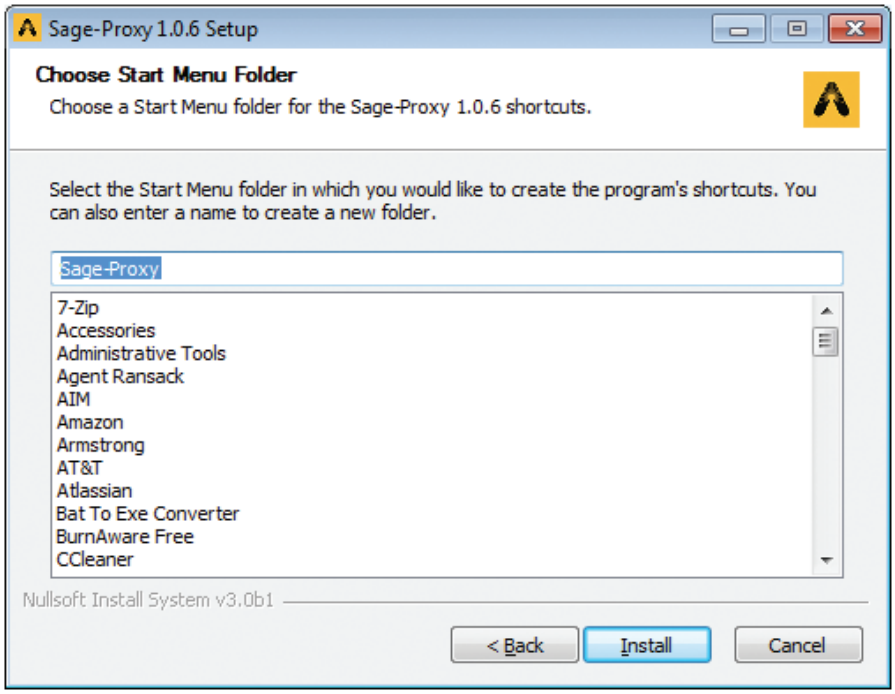
Click Next >



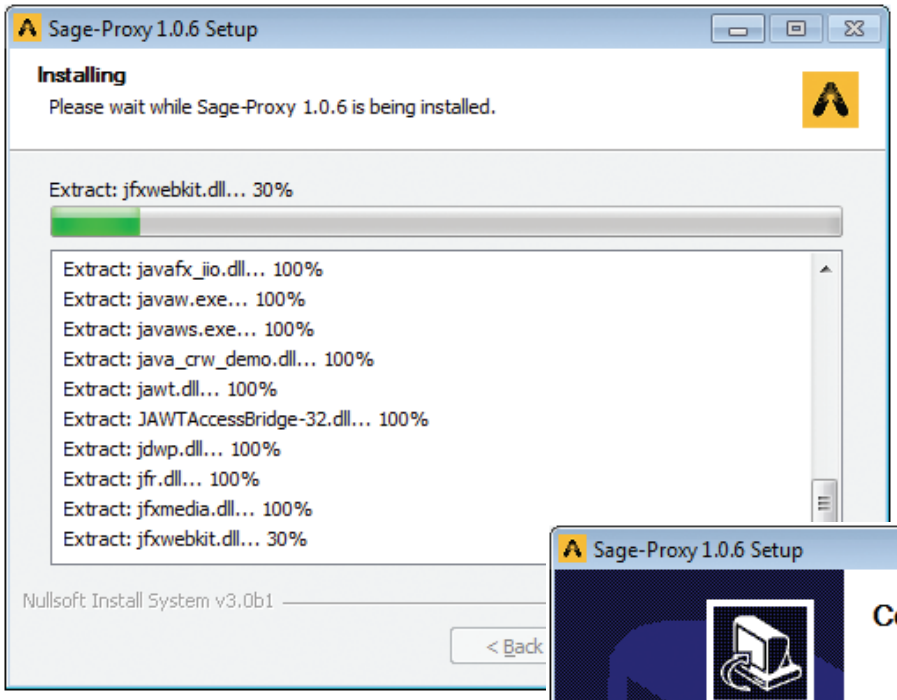
Click the link to read the License agreement and click “I Agree” to install.

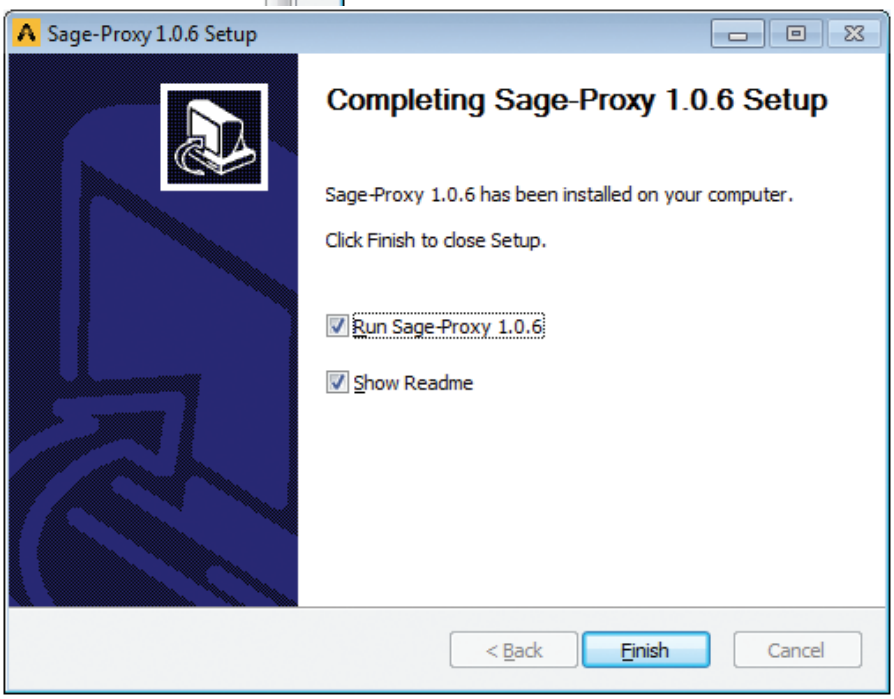


You can change the Destination folder or accept the default. Make sure the Space Available exceeds the **Requirements** table above and click Next >.



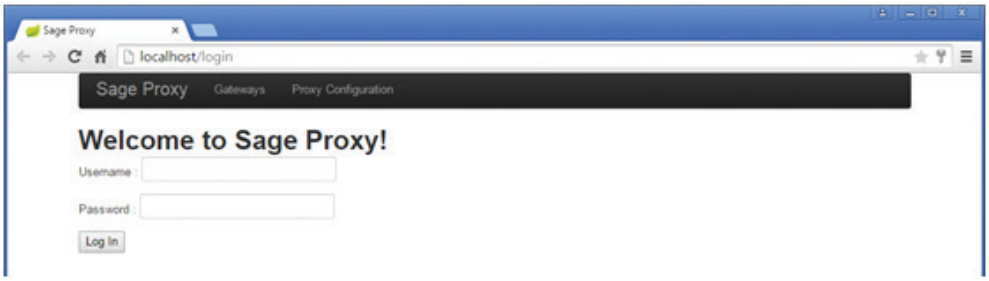
You can change the name of the Start Menu application folder, select an already existing one, or accept the default and click Install. **The Installer will begin installing:**





When the install is complete, click finish. Do not uncheck **Run Sage-Proxy 1.0.6**. Your default web browser will open the Sage-Proxy web interface automatically. It may take a couple of minutes to start up completely. Refresh the page, if necessary until it does.

NOTE: If you uncheck it, you still have several ways to start up the web interface manually from the Start Menu shortcut or Desktop icons named OpenProxy.



You can then log in using the username/password of **admin/sage**.

Click **here** if you are ready to configure Sage-Proxy. Configuration is necessary to start the monitoring process.

Sage™ Proxy Configuration Guide – 1.0.7 (current)

Introduction

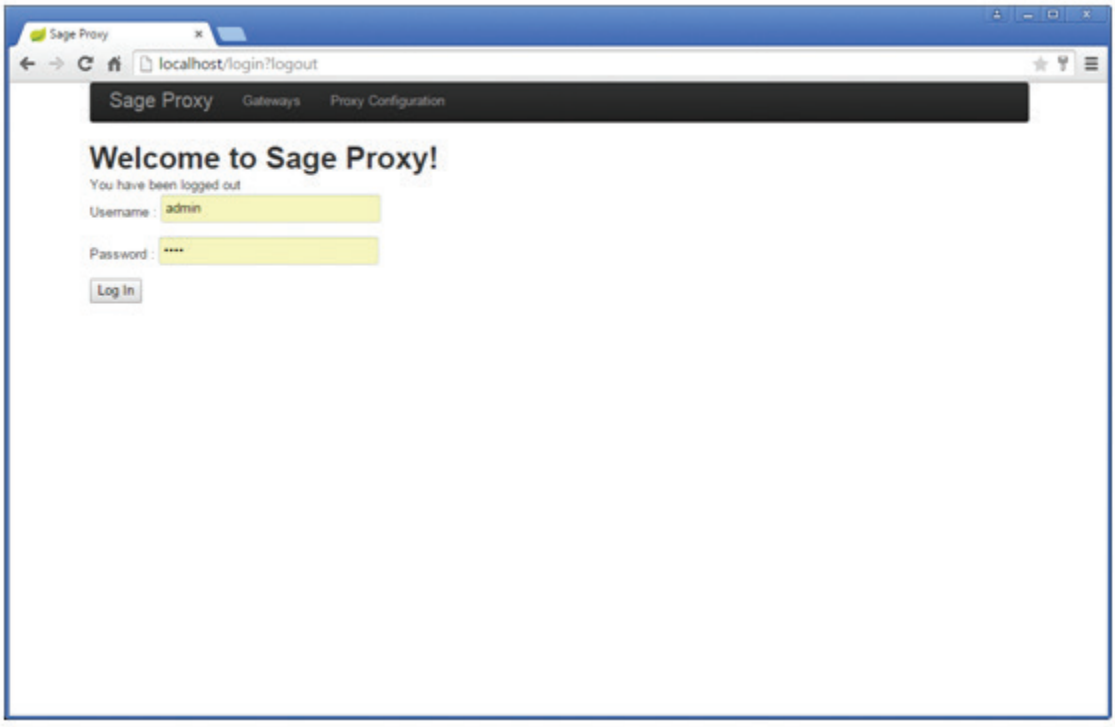
Sage-Proxy is the real-time monitoring piece of SAGE™ that allows collecting and viewing of equipment data virtually as it happens. The Proxy is an application that is usually installed on a local machine of the Site where real time monitoring is to be performed. It runs as a service in the background and can be accessed by its web interface using a web browser. Although Sage-Proxy can be installed on several platforms, this manual refers to installation on Windows and Ubuntu. Sage-Proxy collects the device data and sends it to SAGE™ as it is collected where the data is stored and analyzed for alerting and reporting.

Configuring Sage-Proxy

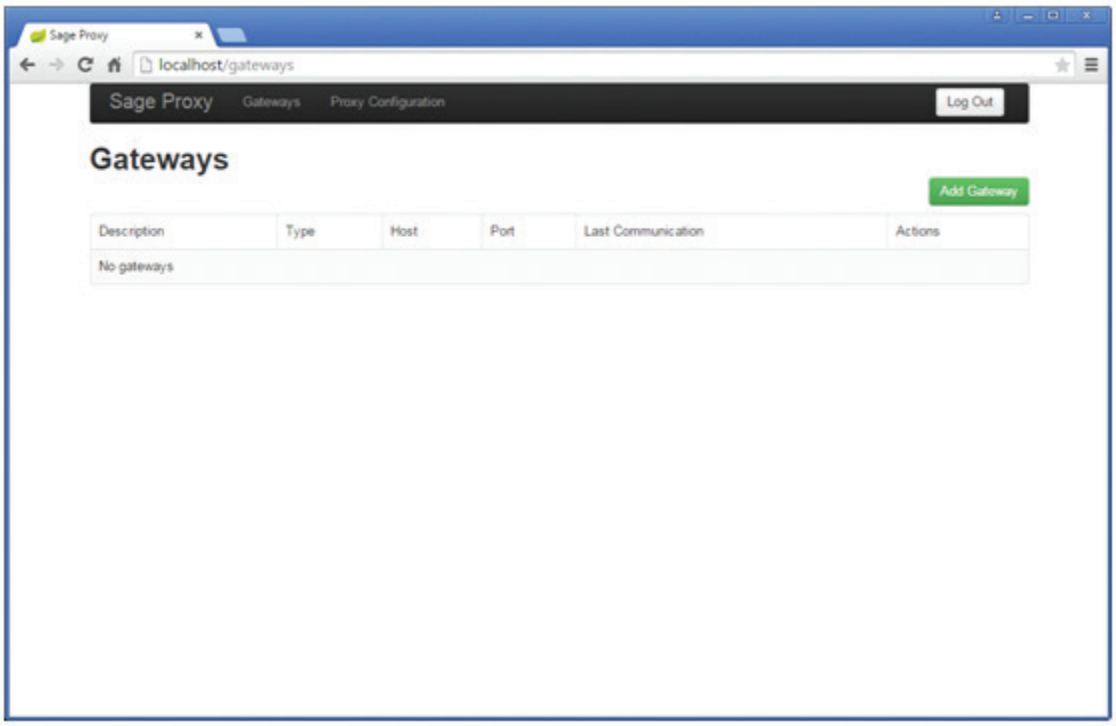
Once installed, Sage-Proxy will have to be configured so it can access the devices to be monitored. That is what the web interface is for, configuring and viewing the latest data.

For Windows the web interface opens in a browser automatically after installation (if you did not un-check “Run Sage-Proxy 1.0.7” on the finish page. You can also start it up by double clicking on the OpenProxy desktop Icon or the Start Menu OpenProxy shortcut. Lastly, you could type localhost into the address bar of a browser to access it.

For both Ubuntu and Windows installations you can type in the IP Address of the Sage-Proxy machine into a browser address bar of another machine on then network. Whichever way you choose the web interface will appear as follows:

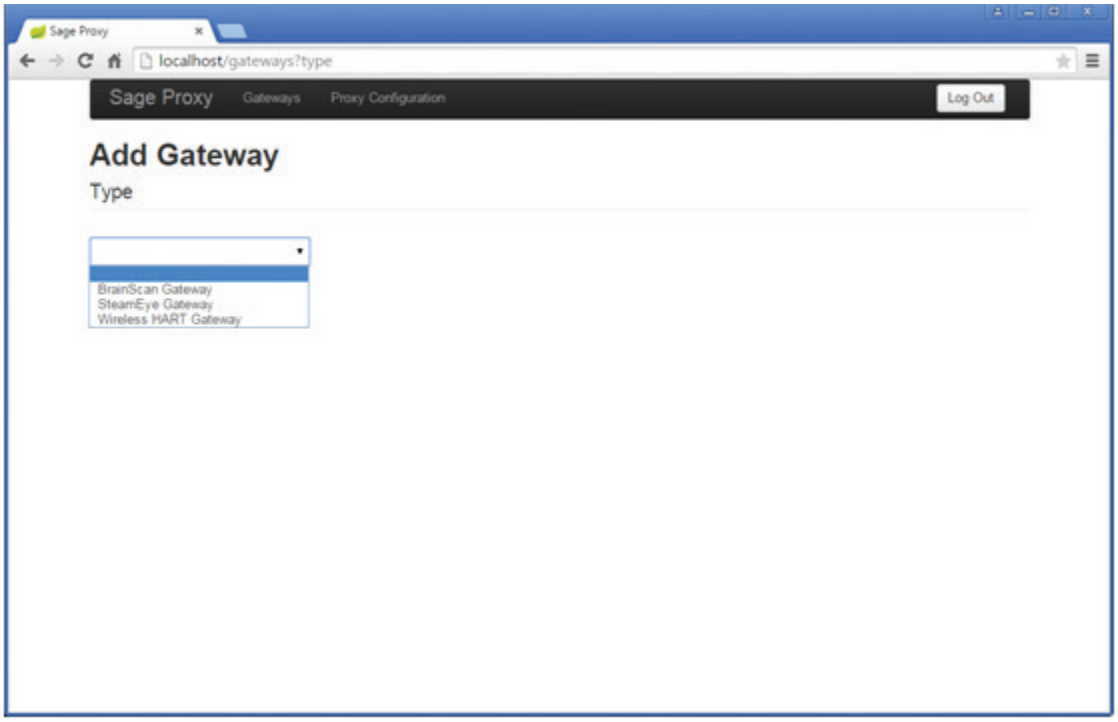


Log in by typing **admin** for the Username and **sage** for the password. That will take you to the gateway page where no gateways are being monitored.



Adding Gateways

Click Add Gateway. The Add Gateway page will display with a single drop down list for picking a gateway type

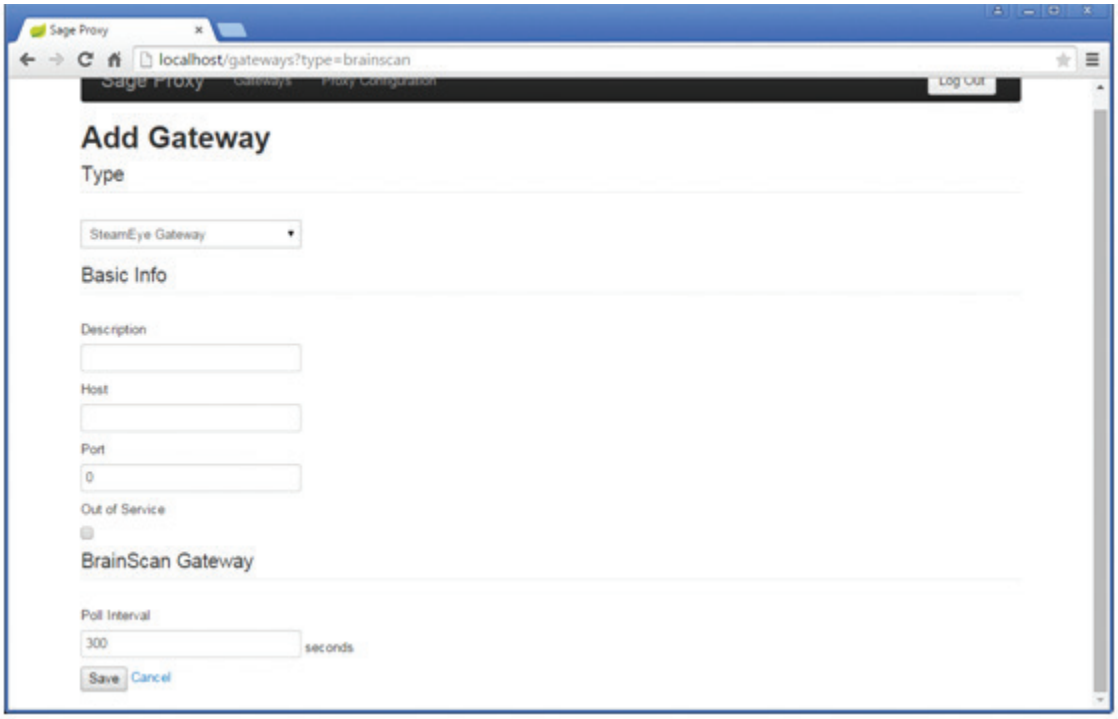


Depending on the devices you want to monitor, pick the correct gateway:

SAGE™ • SteamEye® • WirelessHart™

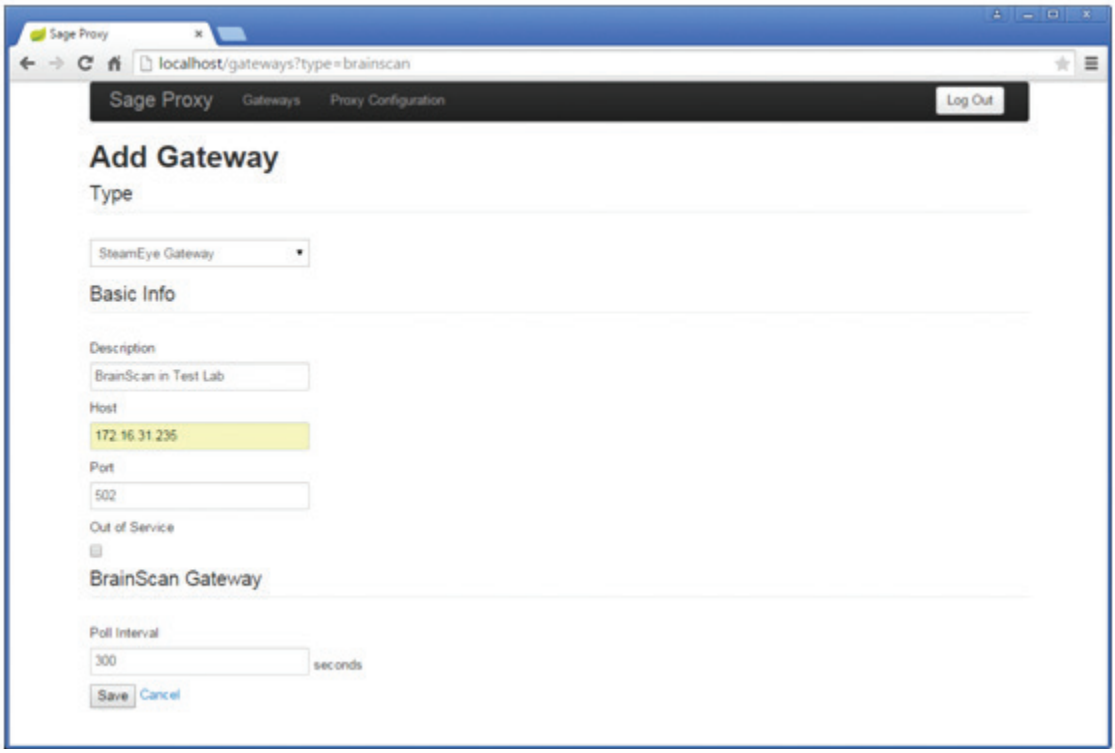
Adding a Brainscan Gateway

Select **BrainScan Gateway** from the dropdown.

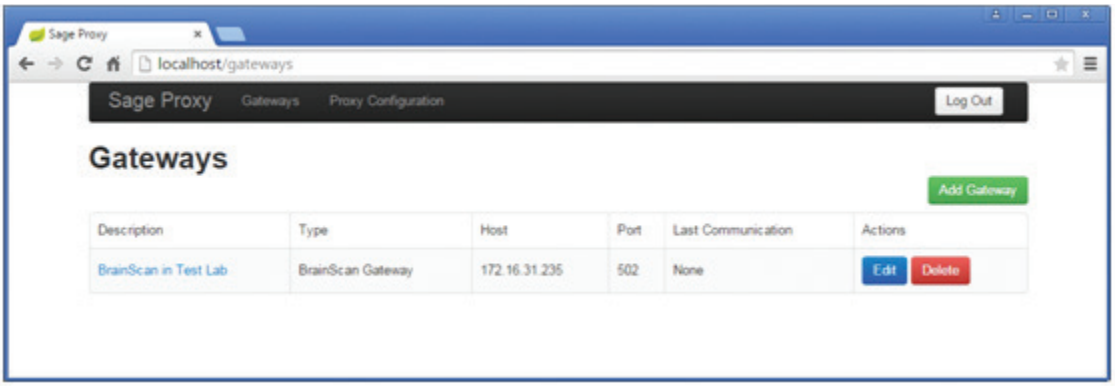


Enter the fields as follows:

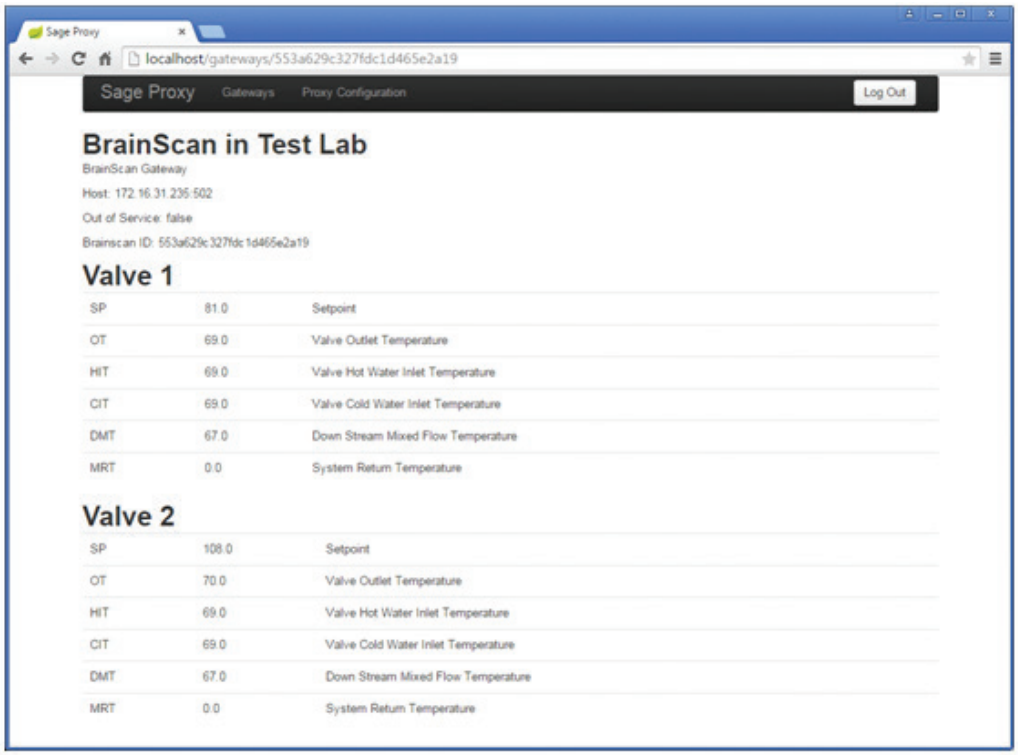
1. Description - A text, read only description for identifying the brainscan gateway.
2. Host - The IP Address or alias that represents the IP address of the brainscan gateway.
3. Port – The port number of the brainscan gateway (usually it's 502)
4. Out of Service – Check this if the Brainscan is currently unavailable due to maintenance.
5. Poll Interval – The amount of time in seconds between data collection. 600 or 900 is typical for Brainscan gateways.



Then click Save. You'll be sent back to the Gateway page with the new gateway now on the list.



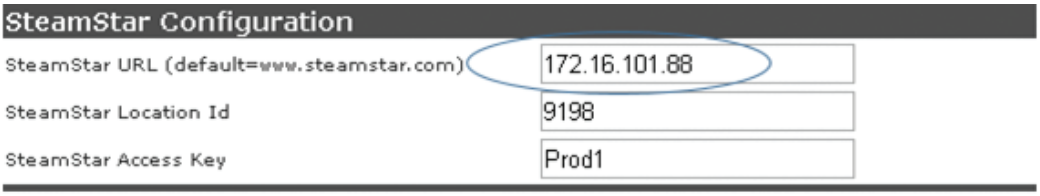
You can then click Edit to change the information you just enterd, click Delete to delete the gateway or click the Description to see the most current data for this gateway. Clicking the Description link displays as follows:

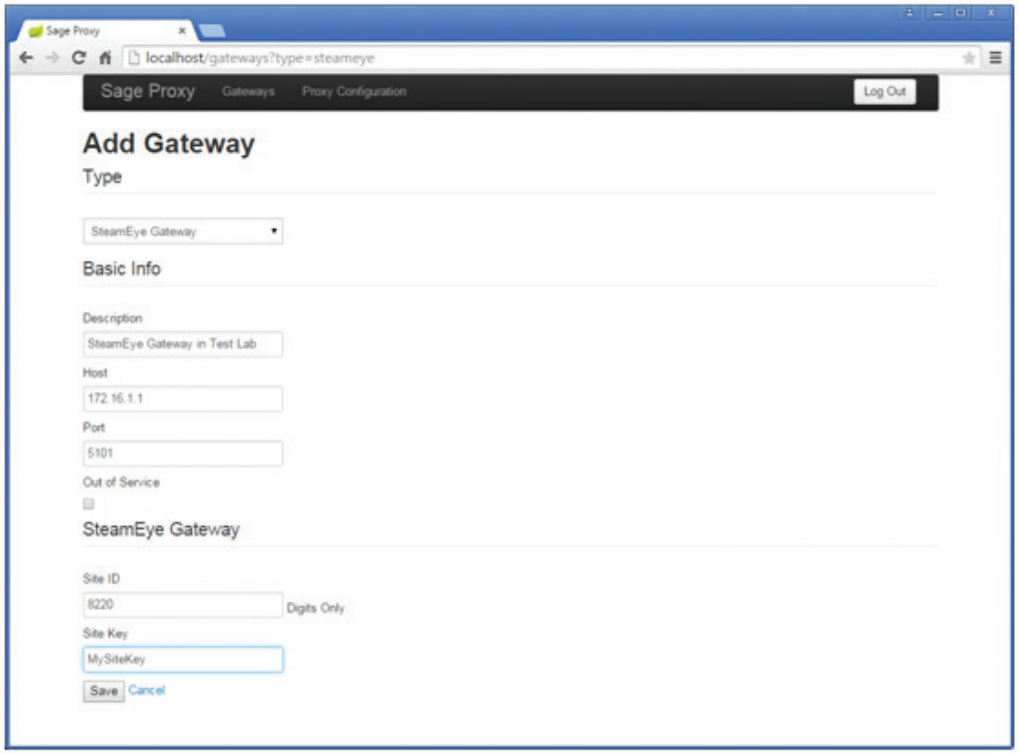


This example shows two Brains (DRVs) communicating with this brainscan and you can see the various temperatures, all in fahrenheit, for each. The data is updated every Polling Interval period of seconds. The page must be refreshed each time the data is updated to view the latest. The brainscan identification information is in the header: Description, gateway type, host:port, Out of Service status and ID number. When through reviewing the data click the Gateways link at the top of the page to go back to the Gateways page.

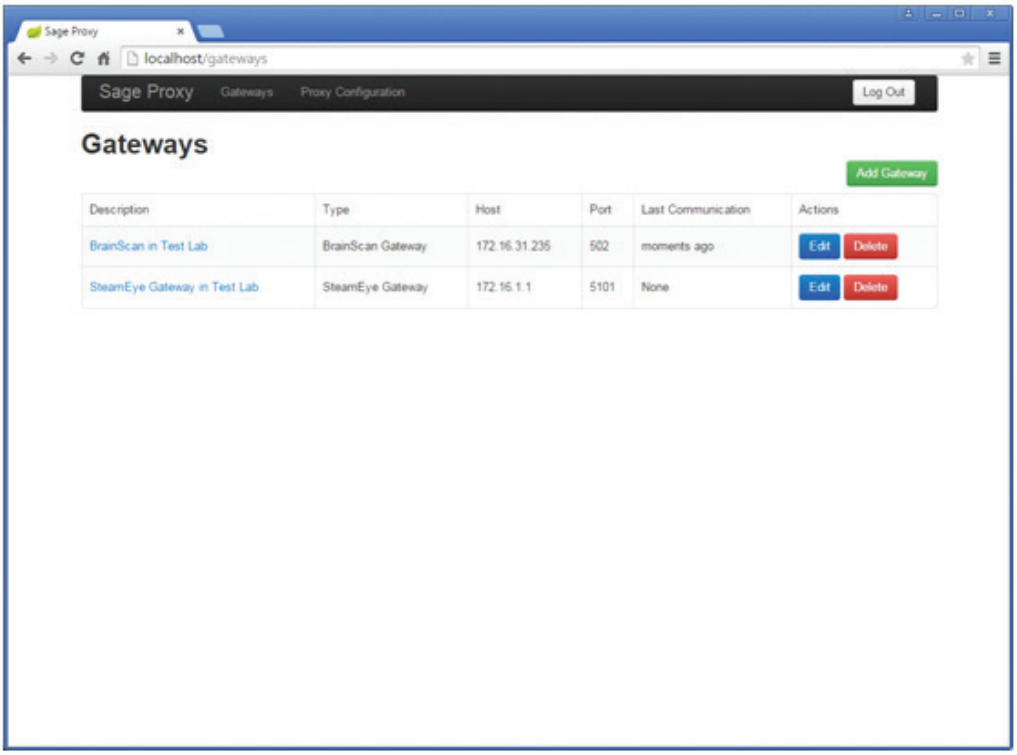
Adding a SteamEye® Gateway

Select SteamEye® Gateway. The information to enter will be the same as for the other gateways except for two additional fields: “Site ID” and “Site Key” and there is no Polling Interval. These values must match those on the SteamEye® gateway exactly for the data to be collected. Also the SteamEye® gateway will have to be configured to send the updates to Sage-Proxy. That is done by entering the IP Address of the Sage-Proxy machine into the SAGE™ configuration field in the SteamEye® gateway. Get the instructions on page 9 of this document: SteamEye® Manual.

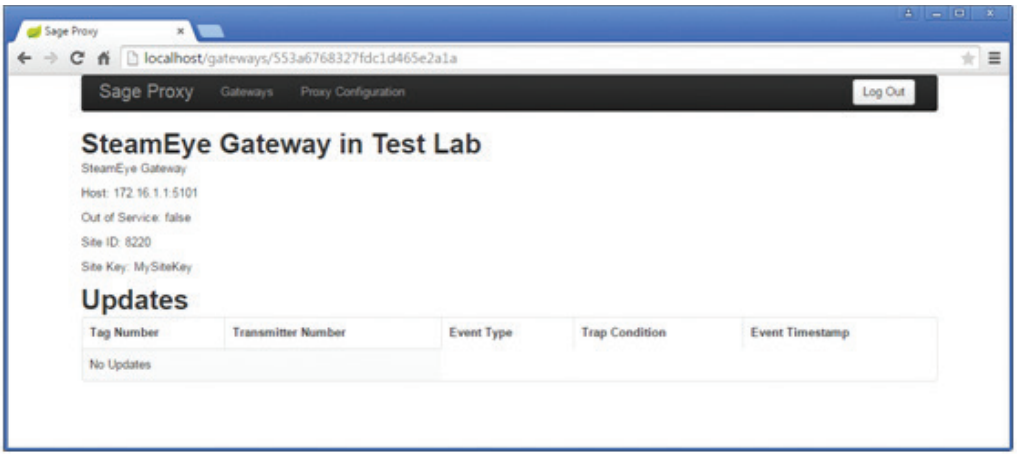




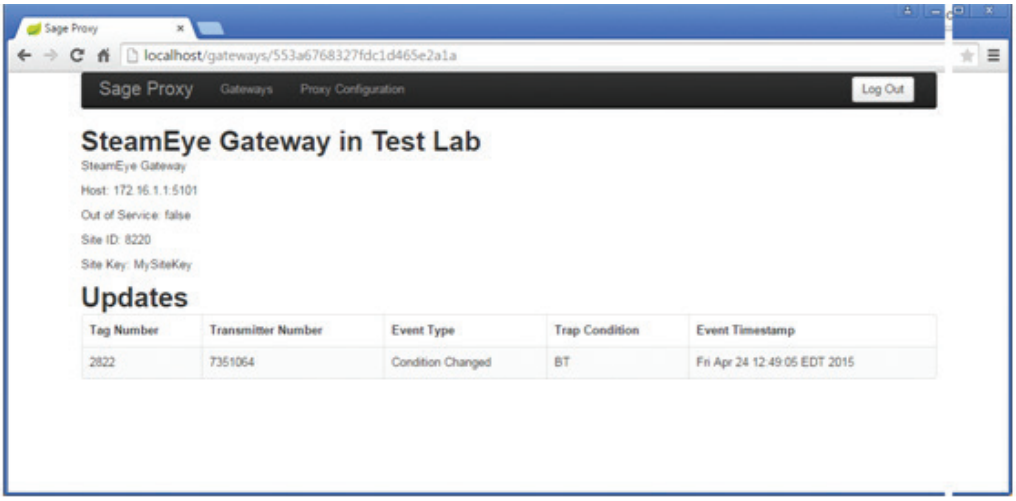
Click **Save**.



One difference between a SteamEye gateway and the others is that there will be no data displayed until a device on that gateway changes status. So what you eventually see is a list of status changes for each device that changes. But until a device changes status it is not displayed.



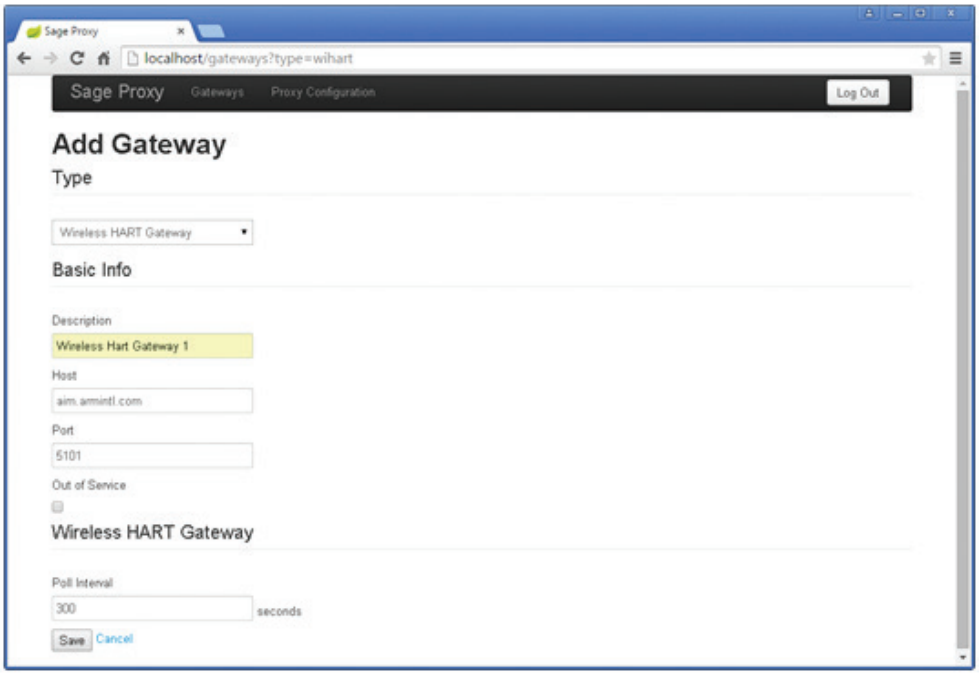
When a device changes status it will be displayed. In the following case device 2822 when Blow Thru (BT).



If the same device changes status again, the new status will replace the old, so that only the latest status is displayed. Each status change is sent to Sage, which stores all the data that is collected.

Adding a WirlessHart™ Gateway

Select **WirelessHart™ Gateway** and the page will re-display as follows:



In this example the gateway information was entered as follows:

Description: WirelessHart™ Gateway 1

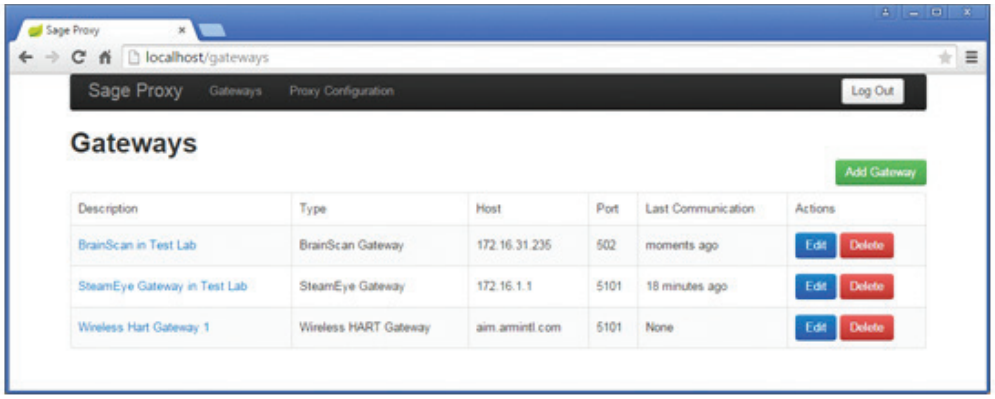
Host: aim.armintl.com (this is the alias used for IP Address 192.168.2.219. Putting in 192.168.2.219 for the host would work as well).

Port: 5101

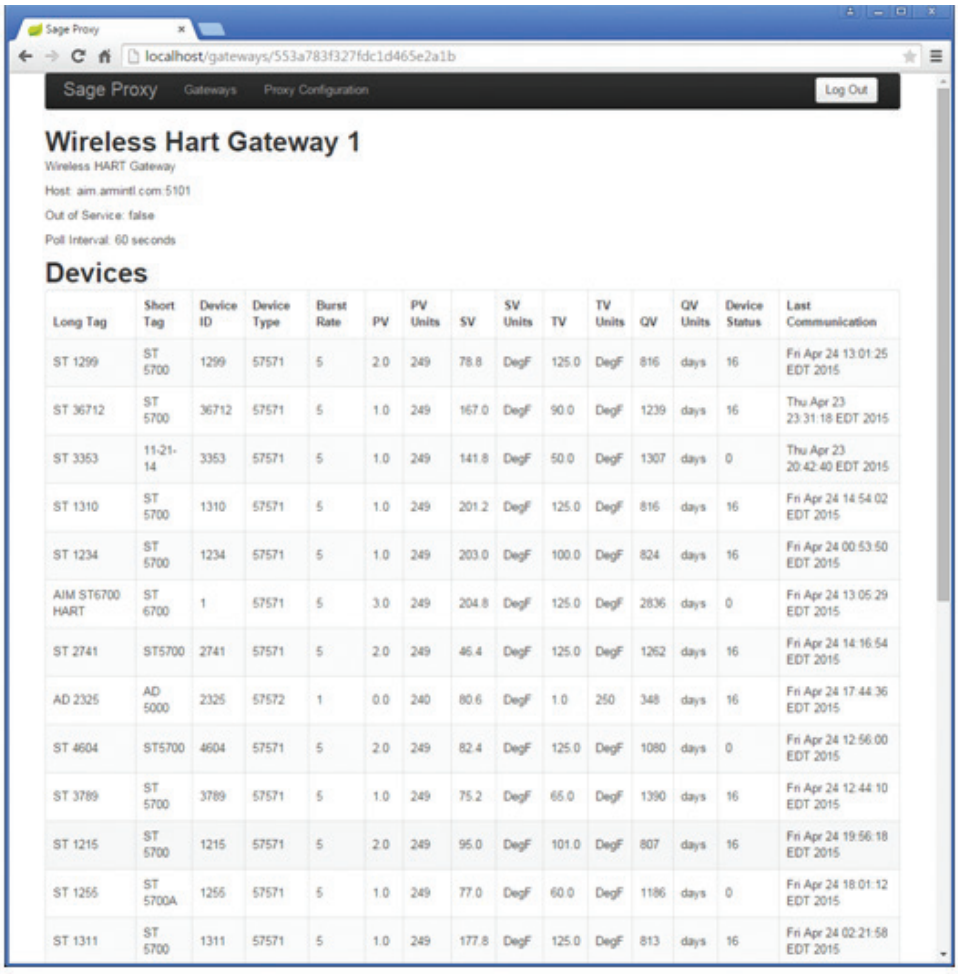
Out of Service: no

Poll Interval: 300 (seconds). This should be a minumum of 300 (5 minutes) for WierlessHart™ gateways.

Click **Save**



Click the Description of the WirelessHart™ gateway to see the data.



Long Tag	Short Tag	Device ID	Device Type	Burst Rate	PV	PV Units	SV	SV Units	TV	TV Units	QV	QV Units	Device Status	Last Communication
ST 1299	ST 5700	1299	57571	5	2.0	249	78.8	DegF	125.0	DegF	816	days	16	Fri Apr 24 13:01:25 EDT 2015
ST 36712	ST 5700	36712	57571	5	1.0	249	167.0	DegF	90.0	DegF	1239	days	16	Thu Apr 23 23:31:18 EDT 2015
ST 3353	11-21-14	3353	57571	5	1.0	249	141.8	DegF	50.0	DegF	1307	days	0	Thu Apr 23 20:42:40 EDT 2015
ST 1310	ST 5700	1310	57571	5	1.0	249	201.2	DegF	125.0	DegF	816	days	16	Fri Apr 24 14:54:02 EDT 2015
ST 1234	ST 5700	1234	57571	5	1.0	249	203.0	DegF	100.0	DegF	824	days	16	Fri Apr 24 00:53:50 EDT 2015
AIM ST6700 HART	ST 6700	1	57571	5	3.0	249	204.8	DegF	125.0	DegF	2836	days	0	Fri Apr 24 13:05:29 EDT 2015
ST 2741	ST5700	2741	57571	5	2.0	249	46.4	DegF	125.0	DegF	1262	days	16	Fri Apr 24 14:16:54 EDT 2015
AD 2325	AD 5000	2325	57572	1	0.0	240	80.6	DegF	1.0	250	348	days	16	Fri Apr 24 17:44:36 EDT 2015
ST 4604	ST5700	4604	57571	5	2.0	249	82.4	DegF	125.0	DegF	1080	days	0	Fri Apr 24 12:56:00 EDT 2015
ST 3789	ST 5700	3789	57571	5	1.0	249	75.2	DegF	65.0	DegF	1390	days	16	Fri Apr 24 12:44:10 EDT 2015
ST 1215	ST 5700	1215	57571	5	2.0	249	95.0	DegF	101.0	DegF	807	days	16	Fri Apr 24 19:56:18 EDT 2015
ST 1255	ST 5700A	1255	57571	5	1.0	249	77.0	DegF	60.0	DegF	1186	days	0	Fri Apr 24 18:01:12 EDT 2015
ST 1311	ST 5700	1311	57571	5	1.0	249	177.8	DegF	125.0	DegF	813	days	16	Fri Apr 24 02:21:58 EDT 2015

It should be kept in mind that this is the raw data from the devices and it is sent to sage as shown. The raw values have different meanings for different device types. SAGE™ will take this data and interpret it correctly, determining the device status for each device and keeping a historical record, complete with analytics. For ST 5700s (device type 57571) the PV value represents the device status. The values mean as follows:

1 – Good

2 – Cold

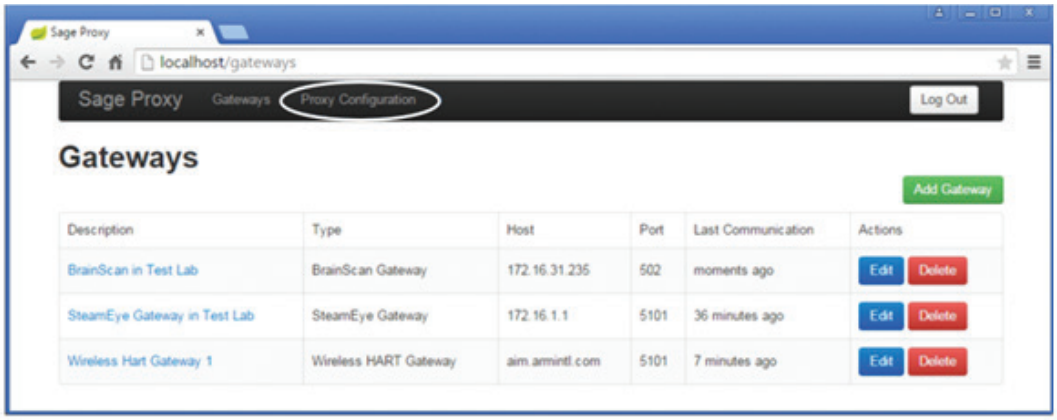
3 – Blow Thru

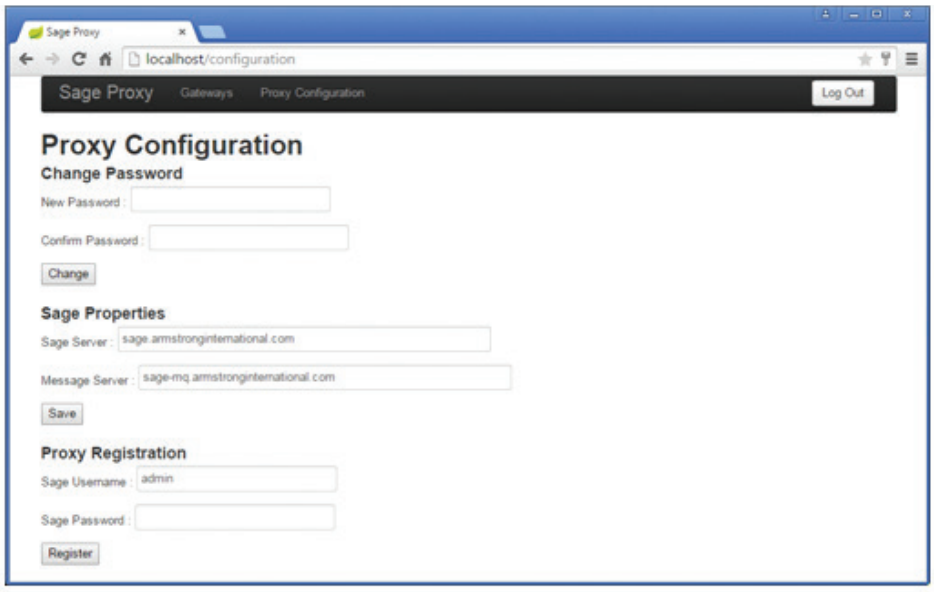
For AD 5000s (device type 57572) the device is good until the the PV exceeds the TV value, then it goes into alarm status. The device can also be configured to alarm when the TV is greater than the PV as well.

TD 5100 devices (device type 57573) work as AD 5000s except the PV and TV values are temperatures instead of acoustic noise counts. They can also be configured to alarm if the TV is greater than the PV.

Sage-Proxy Configuration Page

Sage-Proxy has a Configuration page that allows the user to change the password, change the name of the SAGE™ servers it communicates with, and register the Sage-proxy with SAGE™. To access it click **Proxy Configuration** in the SAGE™ Proxy shortcut bar at the top.





To change the password, type in the new password and then the same password in Confirm Password and click **Change**. The two entered passwords must match exactly including case.

The SAGE™ Properties are the settings for communicating with SAGE™. These should be left as the default values unless otherwise instructed by Armstrong International Technical services.

Proxy Registration is required before SAGE™ will start accepting the data from Sage-Proxy.

SAGE™ CONNECTIVITY PROCESS

Gateway Access for SAGE™ Proxy Cloud

Introduction

This document is intended to give a high-level overview of what needs to be done to allow SAGE™ to access gateway equipment inside a customer's network. This is necessary for SAGE™ to obtain readings for The Brain®.

Audience

This document is intended for a network administrator. It is expected that the administrator is familiar with configuring company network equipment and has permission to do so.

Glossary

Gateway

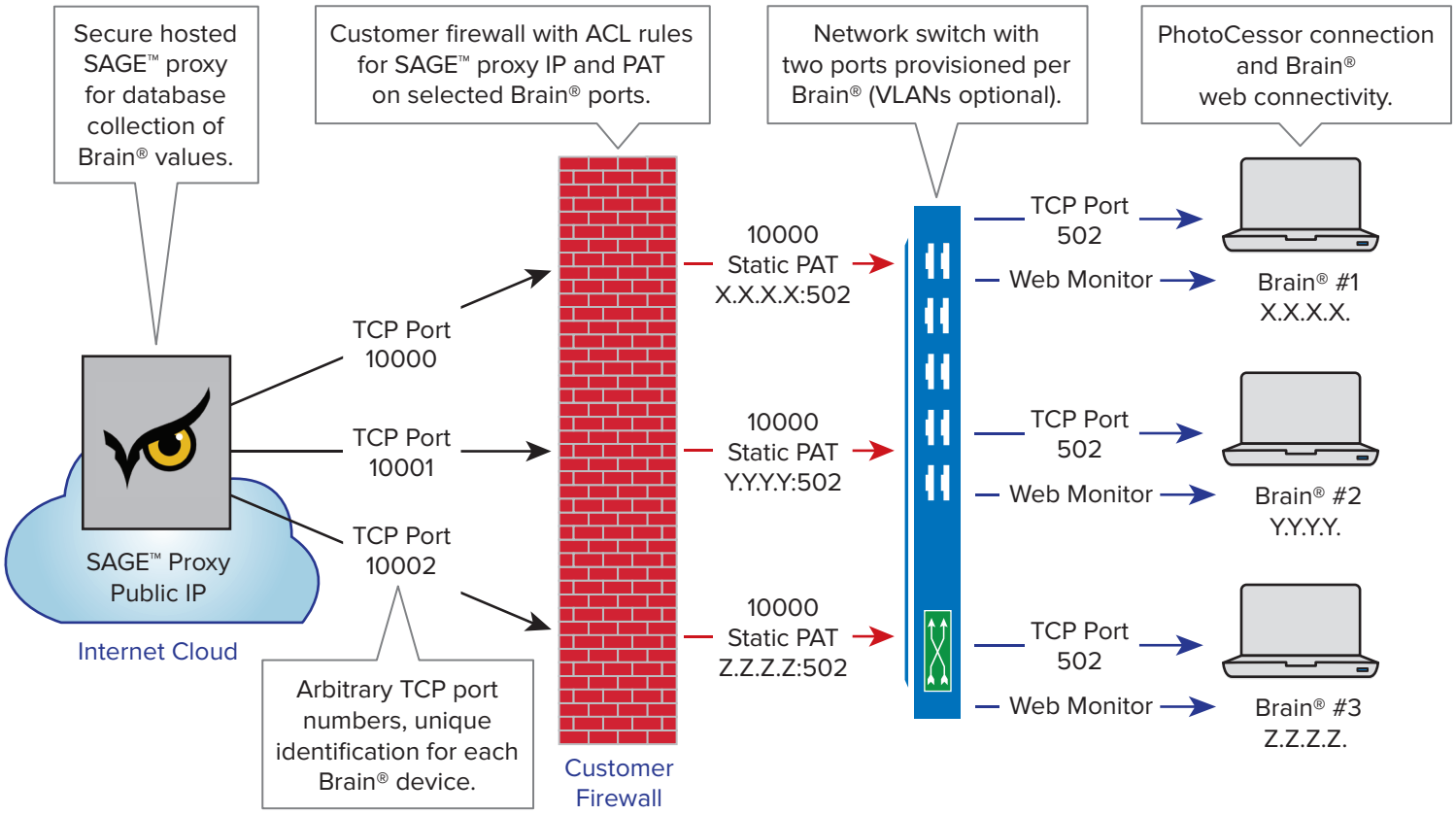
The device SAGE™ needs to access inside the customer's network. Examples include Brain® Building System (BS) gateway.

Common Ports

Gateway	Application Protocol	Transport Protocol	Port
Brain®	ModbusTCP	TCP	502

SAGE™

Brain® Web Proxy Connectivity and Monitoring



SAGE™ Proxy Cloud IP Address

72.44.243.230

Configuration

Option 1: DMZ

1. Obtain and assign an internal IP address for the gateway
2. Identify the port used by the gateway. See Common Ports, above, for a list of default ports used by various gateways.
3. Obtain and assign a static external IP for the customer network, if one does not already exist. Write down this IP address, it will be needed later to configure SAGE™.
4. Place gateway in DMZ in your router or firewall and configure using external IP address from step 3.
5. If possible, restrict to only traffic originating from one of the IP addresses listed in SAGE™ Proxy IP Addresses section, above.

Configuration

Option 2: Port Forwarding

With this option, an external IP address and port is mapped (forwarded) to an IP address and port on the internal customer network. This forwarding is typically configured on a router or firewall on the customer's network. For security, traffic can be restricted to only the IP address of SAGE™.

1. Obtain and assign an internal IP address for the gateway.
   - Example: 192.168.1.100
2. Identify the port used by the gateway. See Common Ports, above, for a list of default ports used by various gateways.
   - Example: 502
3. Obtain and assign a static external IP for the customer network, if one does not already exist. Write down this IP address, it will be needed later to configure SAGE™.
   - Example: 50.124.28.70
4. Choose an external port number where SAGE™ Proxy Cloud will connect. This choice is fairly arbitrary, and can be the same as #2. If you will be configuring multiple internal gateways, you will need to choose a different external port for each. You may refer to this list for some well-known and registered ports to help avoid conflicts:

   https://en.wikipedia.org/wiki/List_of_TCP_and_UDP_port_numbers

   Write down this port, it will be needed later to configure SAGE™.
   - Example: 10000
5. Configure port forwarding in your router or firewall. Instructions for this vary depending on the product, but the key concepts are:
   a. Forward traffic from external IP in step 3 on external port in step 4 to internal IP in step 1 on port in step 2.
      - Example: 50.124.28.70:10000 ⇨ 192.168.1.100:502
   b. Restrict to only traffic originating from one of the IP addresses listed in SAGE™ Proxy IP Addresses section, above.

SAGE™ - Dashboard & Alerts

SAGE™ enables you to maximize equipment reliability, efficiency and safety and raises utility system management to a groundbreaking new level.

To access the Dashboard, log into your SAGE™ account at sage.armstronginternational.com using your user name and password.

The Dashboard provides a quick overview of the performance of your steam trap system, the status of your hot water systems, a chart of your steam costs for the past year, steam loss detail, alerts on equipment performance and information on how to contact SAGE™ support. No matter where you are in the application, clicking the SAGE™ logo in the top left corner will return you to the Dashboard (see Figure 1 below).

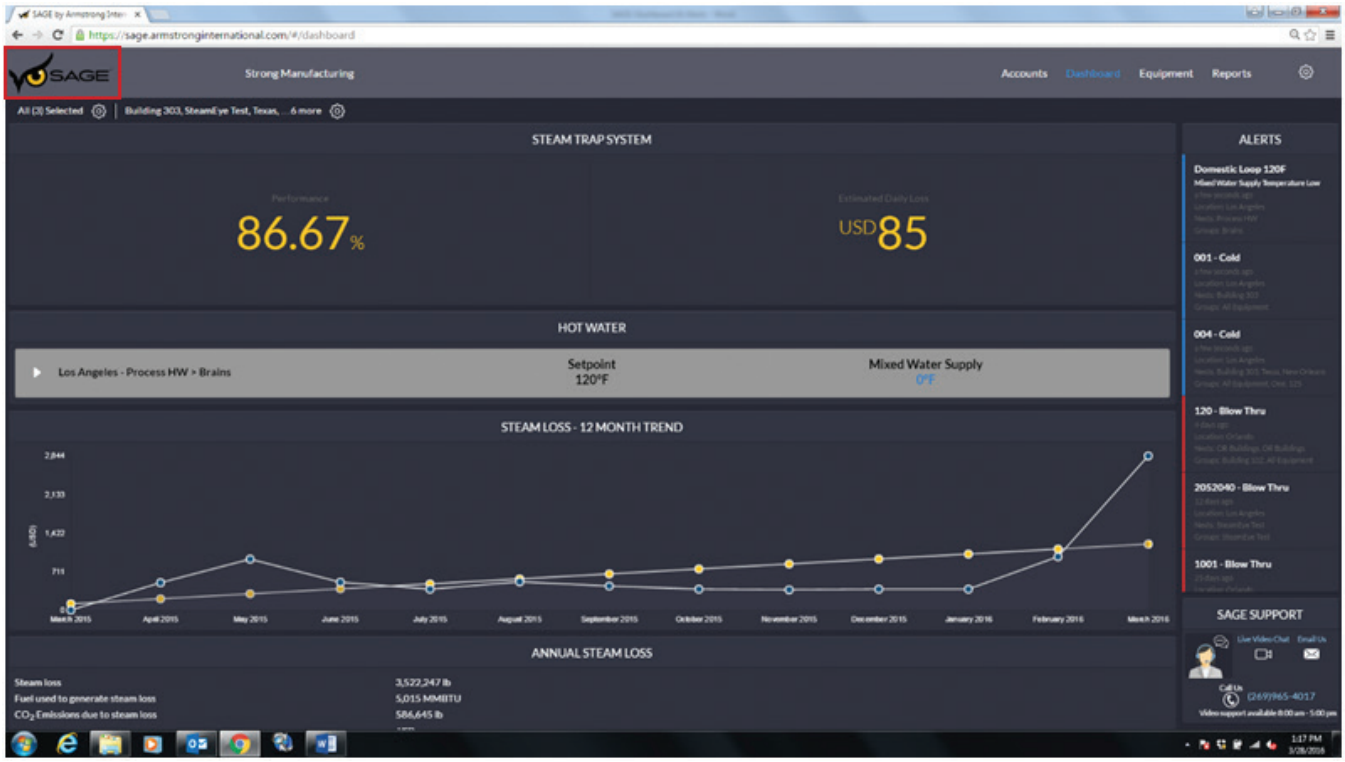


Figure 1

Let's look at some of the details

SAGE™ allows you to track multiple locations within a company. You can select one location, or multiple locations. When you have made your selection, click 'Apply' (see Figure 2 below).

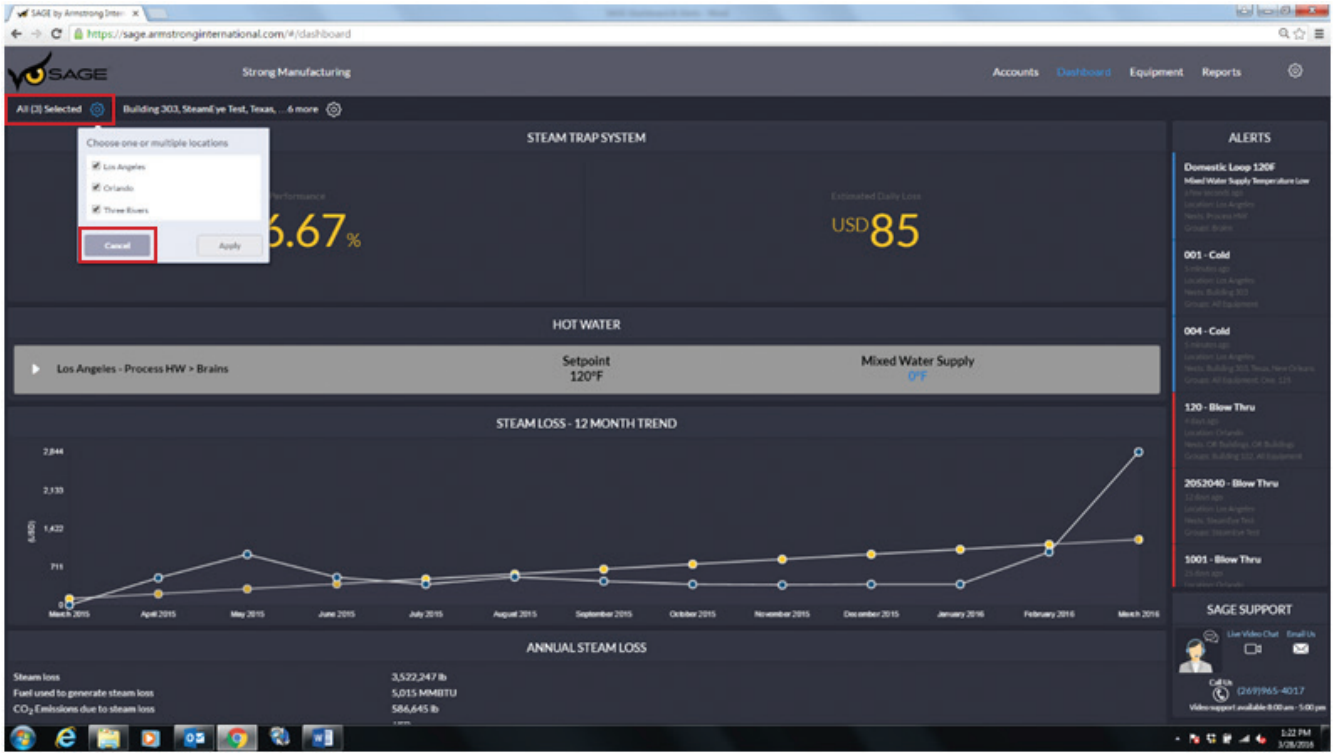


Figure 2

SAGE's flexible interface allows you to select any combination of Nests – which are sub-sections of a location, such as a West Plant and an East Plant – and Groups of buildings, facilities or specific equipment within those nests. When you've made your selections, click 'Apply.' The Dashboard will automatically update, providing filtered data based on your selection (see Figure 3 below).

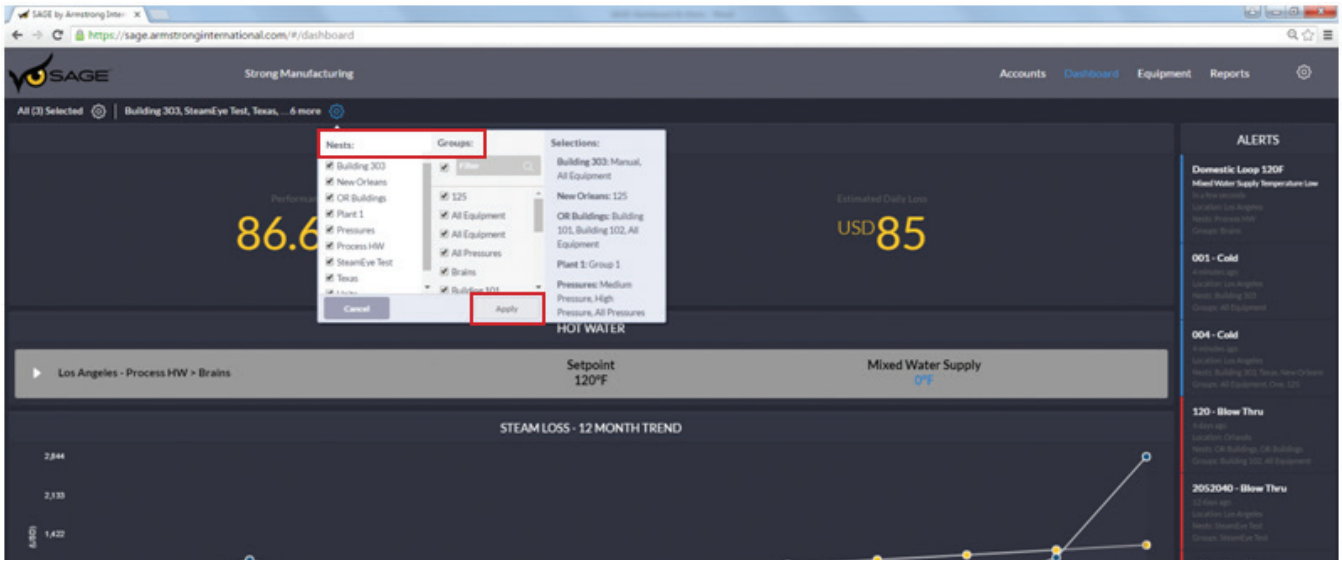


Figure 3

In this example, the steam trap system is operating at a performance rate of **86.67%**, resulting in an estimated daily loss of **$85** dollars (see Figure 4 below).

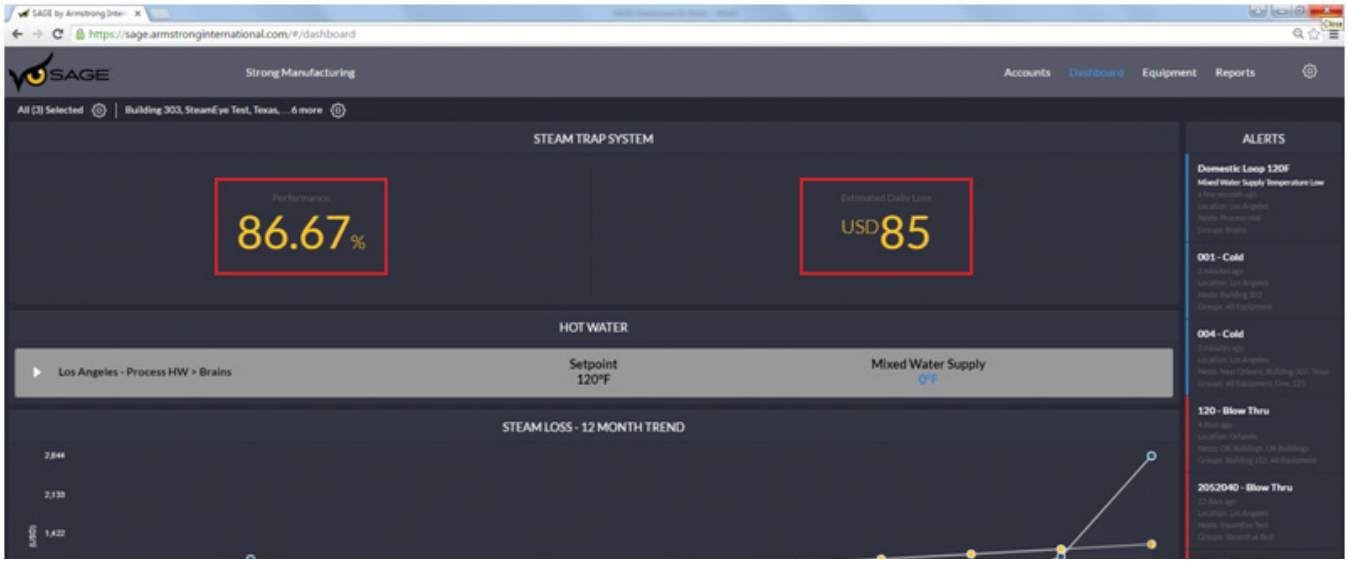


Figure 4

The 'ALERTS' column on the right highlights equipment in need of attention. The most recent issues are listed at top. The condition of the equipment is represented by the color bar on the left. Equipment that has a red color bar needs immediate attention, a blue color bar is cold and a yellow color bar needs attention in the near future (see Figure 5 below).

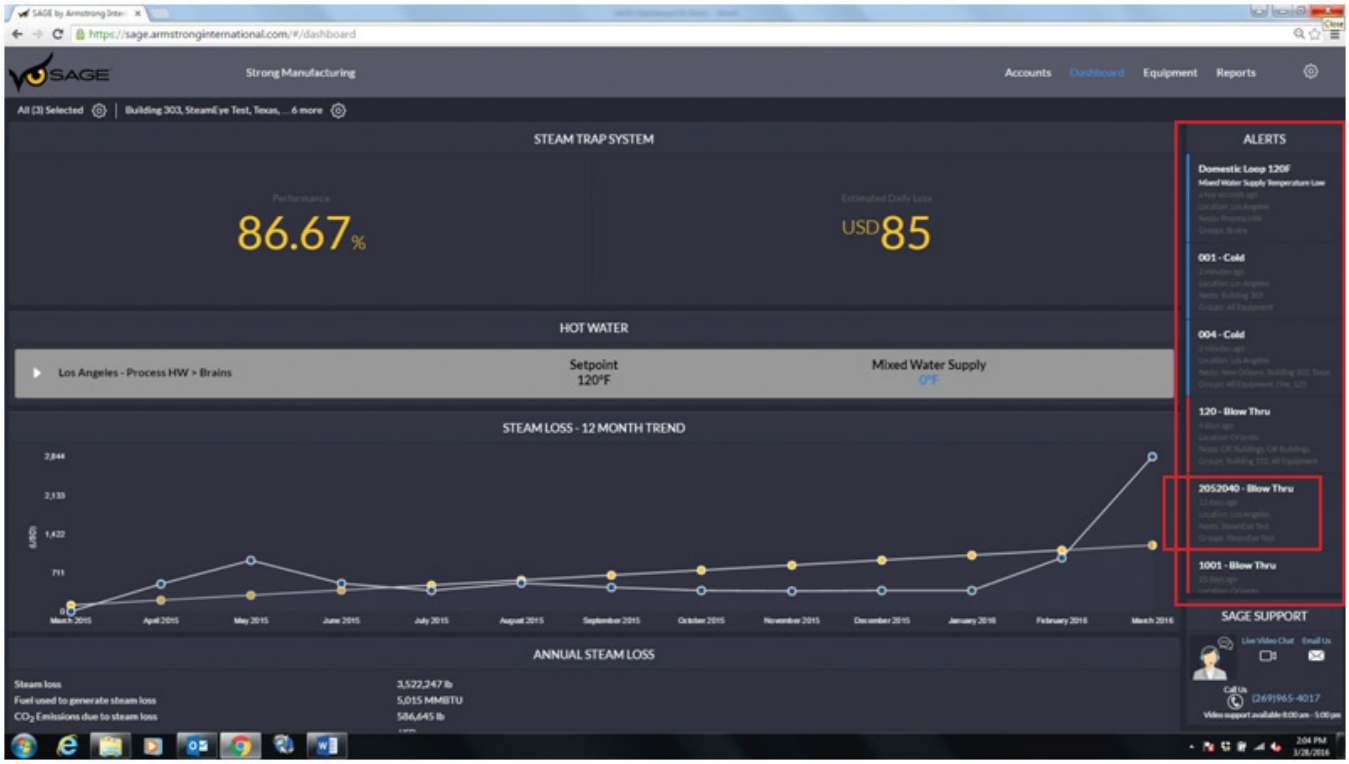


Figure 5

Clicking on an item – in this case a steam trap with a blow-through condition – displays detail on that trap including the installation date, manufacturer, connections sizes and more. Click the plus sign for additional information, like Trap Valve Data. You can also look at the history for that trap by clicking the 'History' link. This can help you determine if a particular trap is having recurring issues. Clicking the SAGE returns you to the Dashboard (see Figure 6 below).

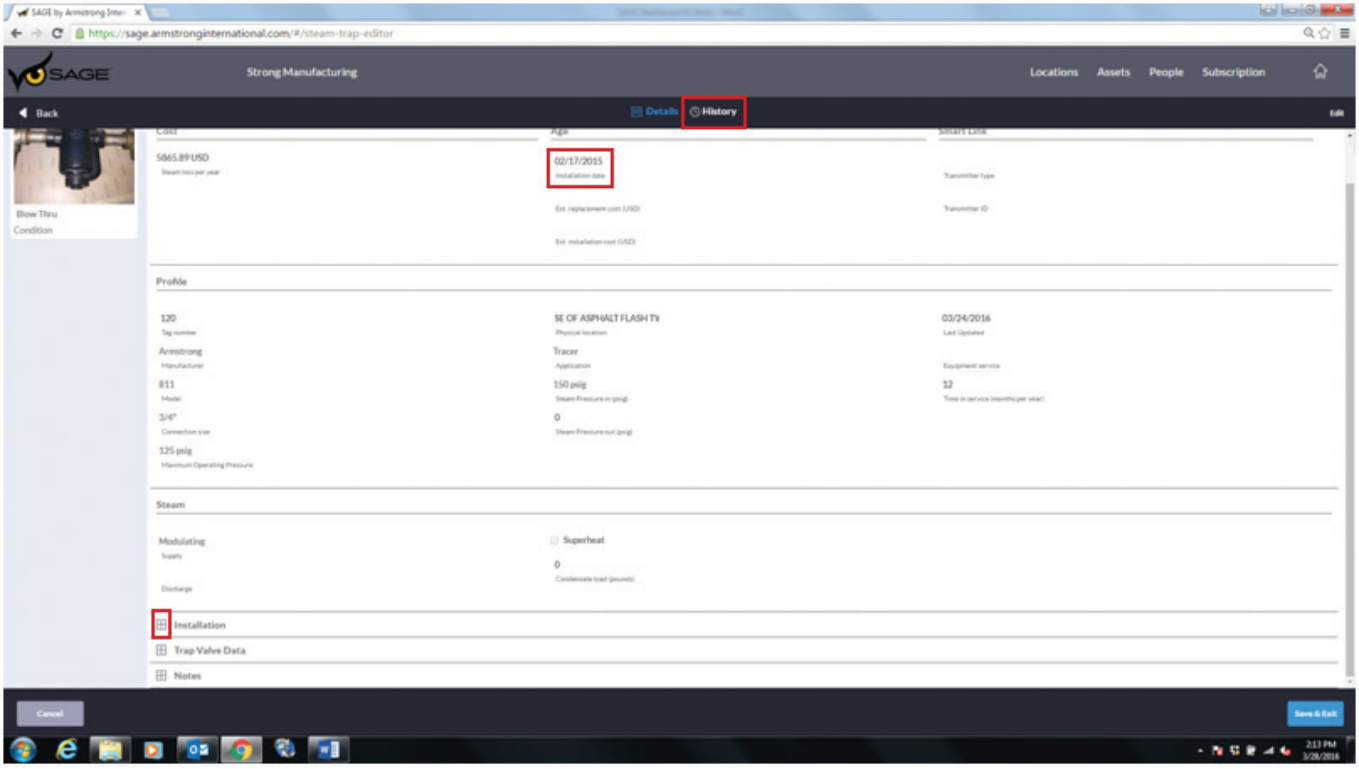


Figure 6

In the 'HOT WATER' section, the setpoint of the digital recirculating valve is shown alongside the Mixed Water Supply temperature (see Figure 7 below)..

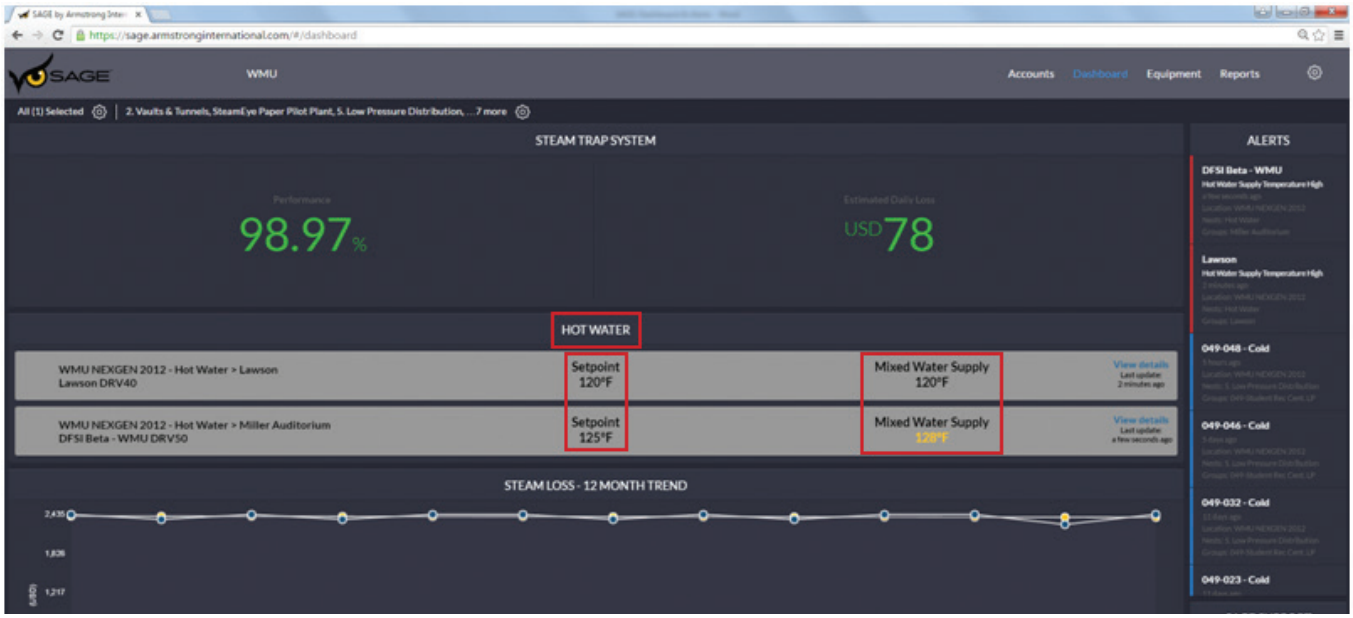


Figure 7

Clicking that display reveals the current Hot Water Supply and System Return temperatures. All values on the dashboard update in real time providing an instantaneous overview of that system (see Figure 8 below).

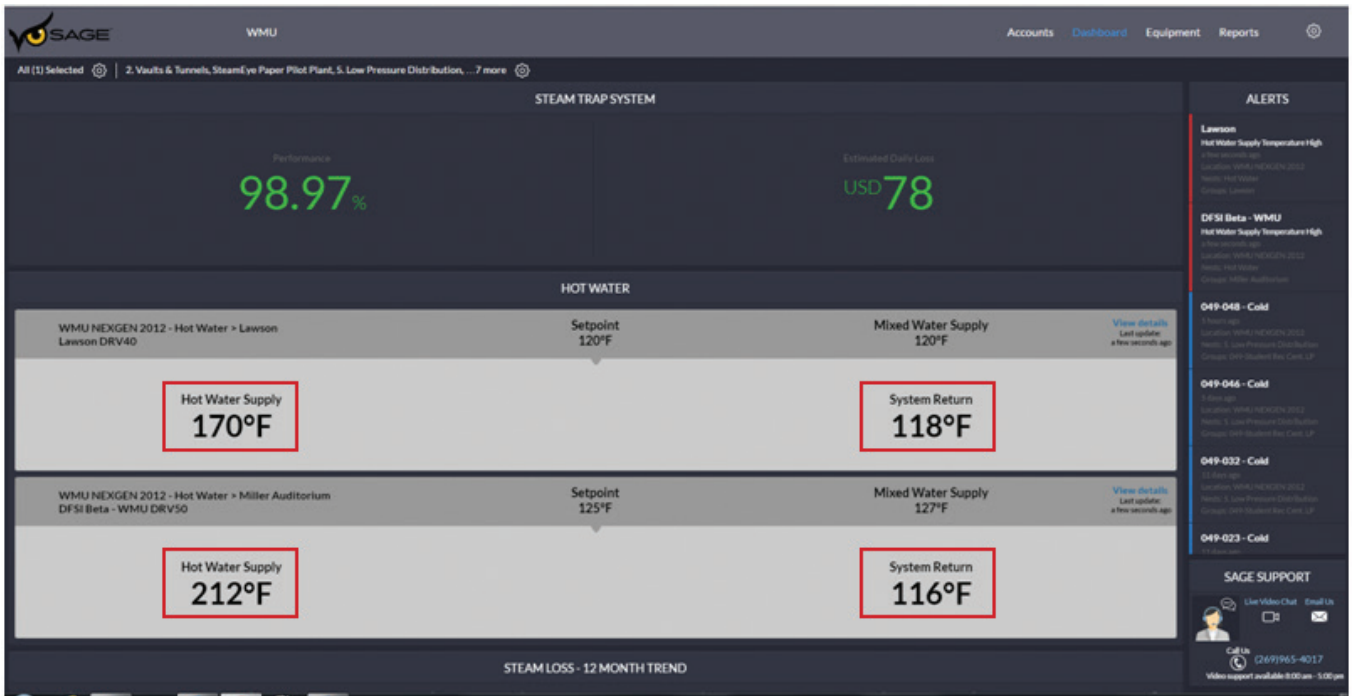


Figure 8

'STEAM COSTS' displays a 12-month trend line in yellow and the actual monthly values in blue. In this case, the monthly trend is 21 USD and the actual loss is 75 USD. On the bottom of the screen, 'ANNUAL STEAM LOSS' calculates the values over the course of the past year including the potential energy cost savings (see Figure 9 below).

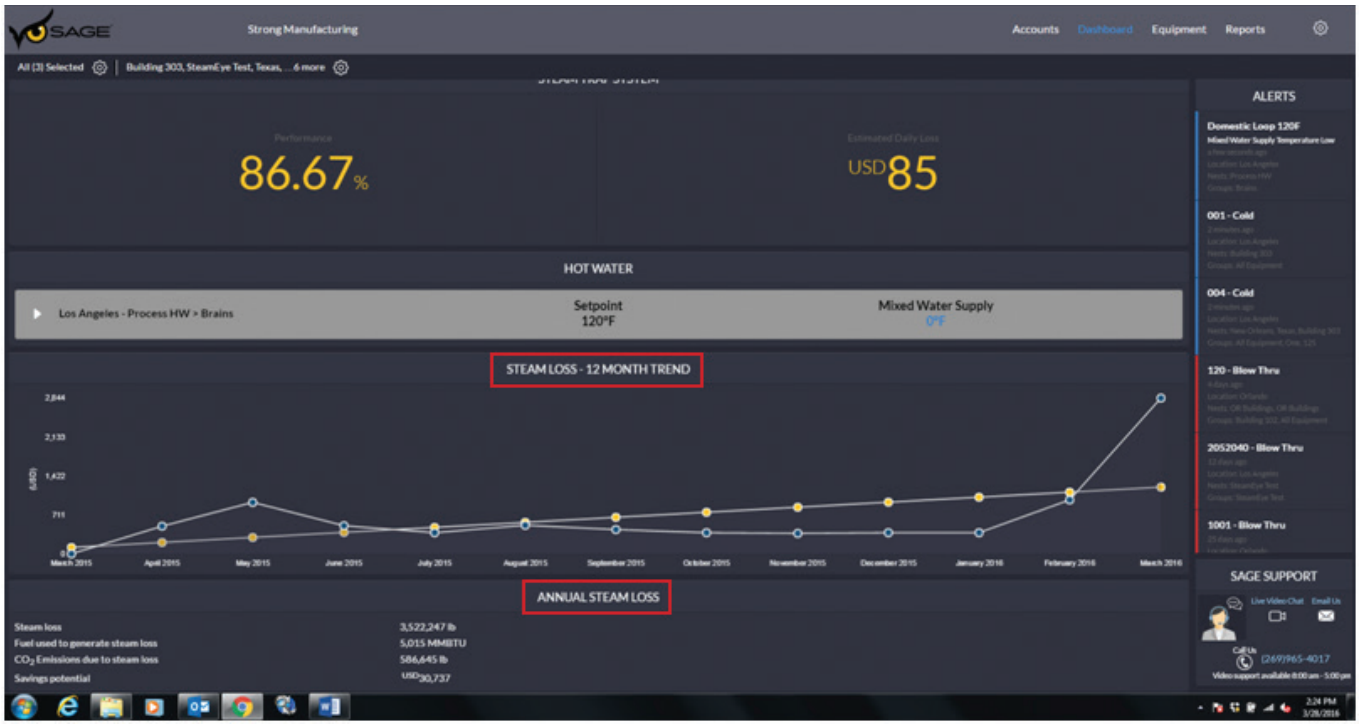


Figure 9

There are a number of ways to obtain SAGE™ support including email, telephone or even a live video chat. The SAGE™ support team can help with questions about your location, your account or additional 'how to' information (see Figure 10 below).

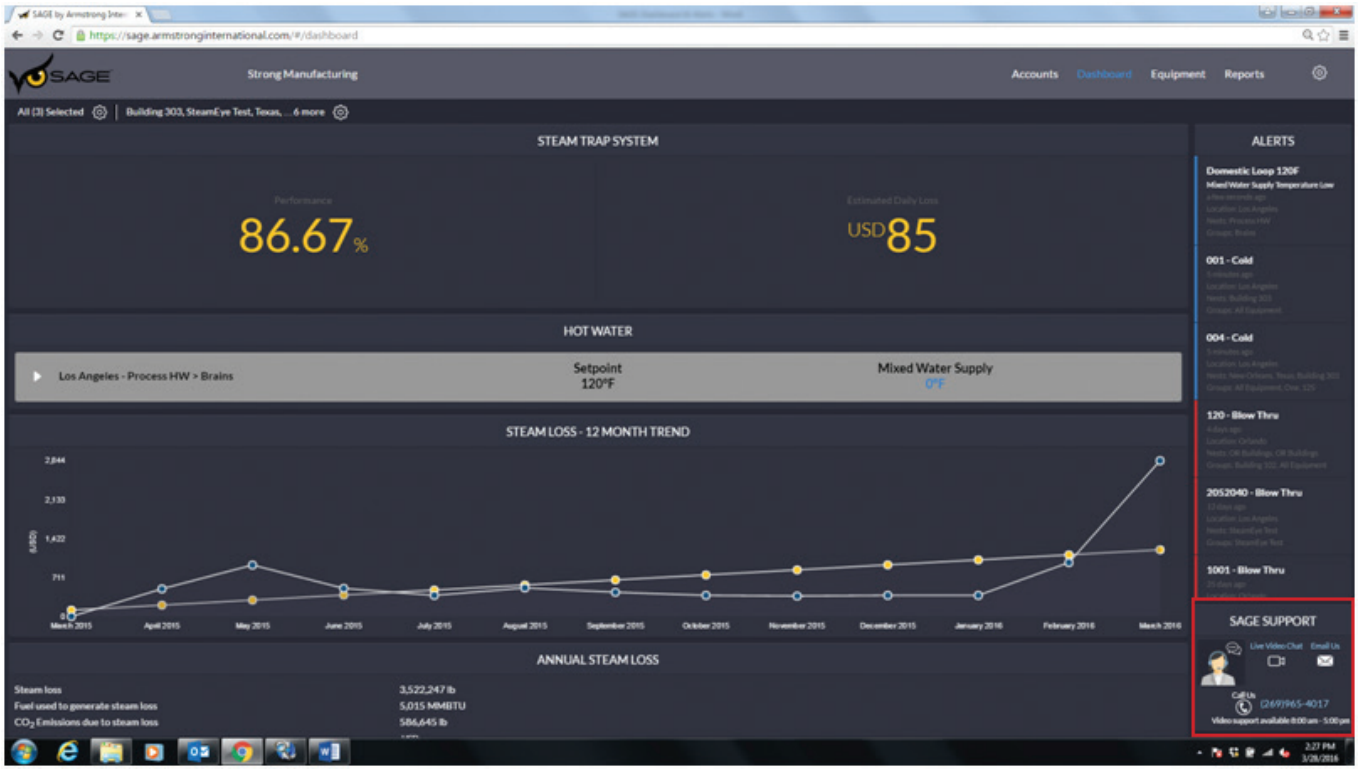


Figure 10

The SAGE™ Dashboard brings critical system information direct to your tablet or computer.

SAGE™ - Report Creation & Explanation

SAGE™ allows you to create detailed reports tailored to the period of time you desire with the click of just a few buttons.

From the home page, select 'Reports' located at the upper right hand of the page next to the configure cogwheel (see Figure 1 below).

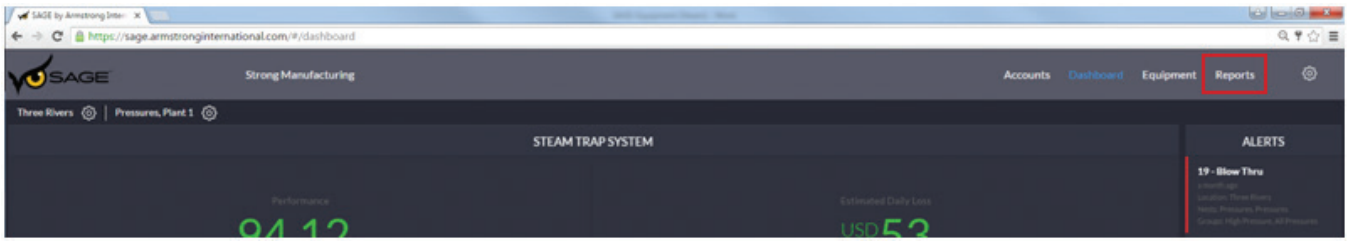


Figure 1

Once the list of available reports is populated select which location(s) you would like to run the report for by clicking the locations cogwheel and selecting from the drop down list (see Figure 2 below).

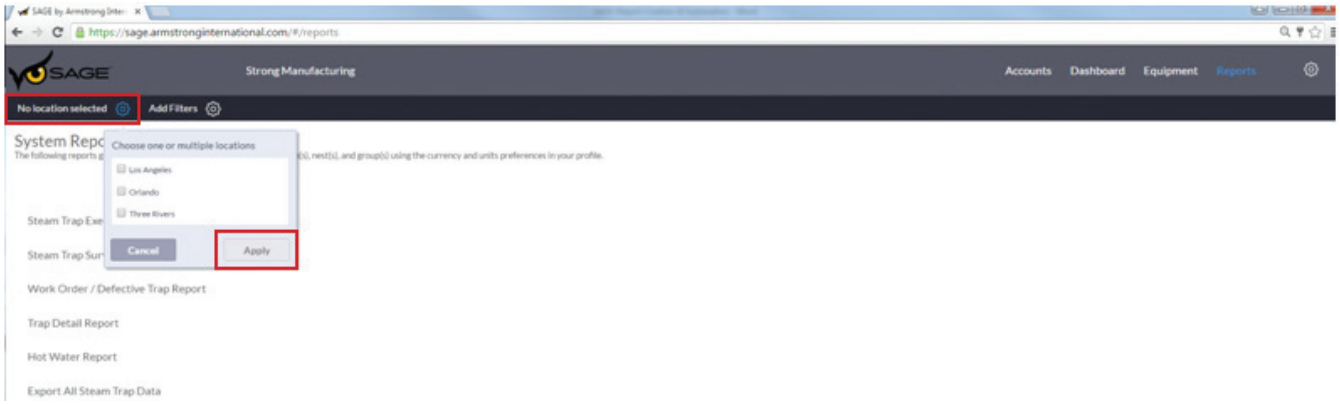


Figure2

Next simply select the type of report you would like to run, then choose the date range from either the pre-defined time periods available in the drop down or a custom time period selectable via the calendar and then click 'Apply' then 'Generate Report' at the bottom (see Figure 3 below).

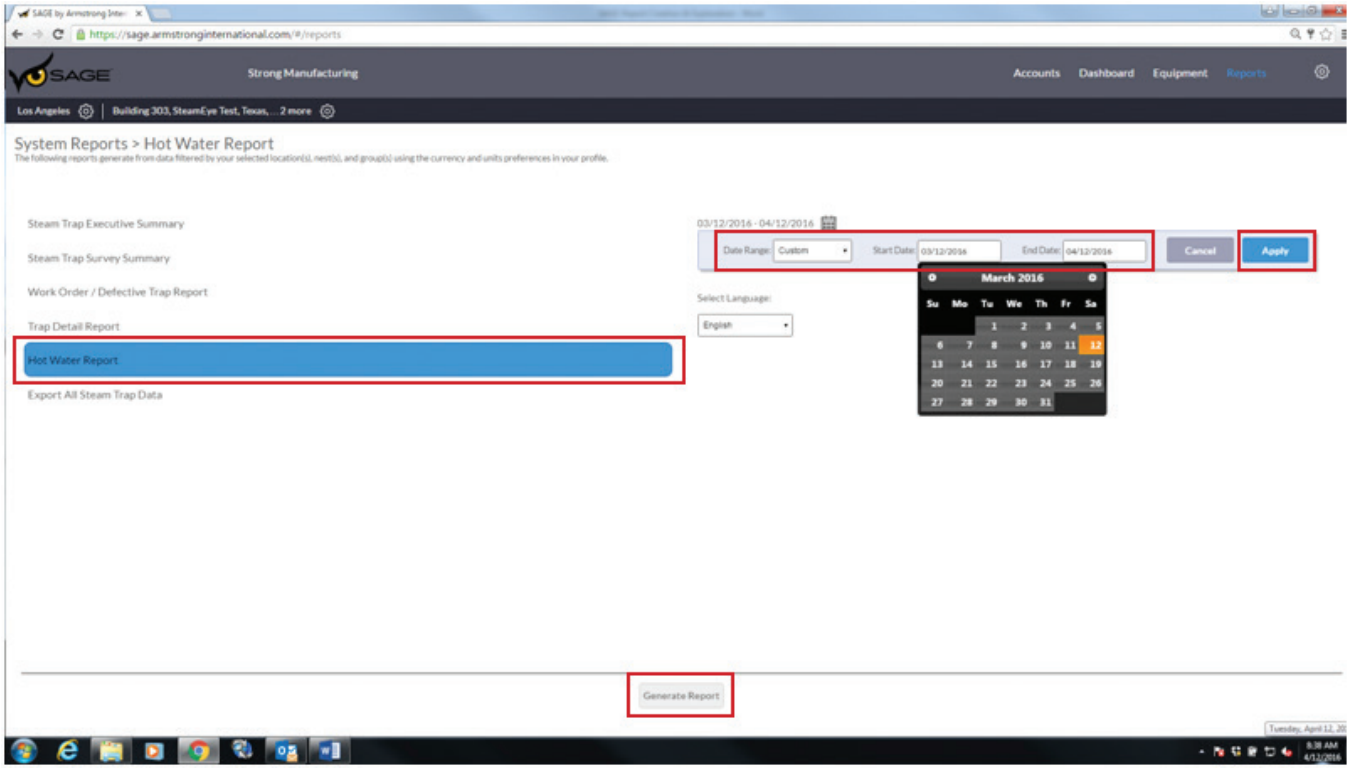


Figure3

Below is a brief explanation of each report available:

Steam Trap Executive Summary – Provides a totalized summary of the selected data for a given date. Summaries include: Monetary Loss, Fuel used, Repair cost, Payback period, and CO2 Emissions. Charts include: Trap Type Summary, Application Summary, and Condition Summary.

Steam Trap Survey Summary – Very similar to the Steam Trap Executive Summary except the data that is pulled will be from a selected period of time from select survey techs. This allows the user to run a report based on a performed survey.

Work Order/Defective Trap Report – Provides a list of the defective traps in the data selected. The defective trap list is broken up by the groups selected to make finding and repairing the traps easier.

Trap Detail Report – Creates a full-page report of all the trap details for each trap in the data selected. Notice: This report can be very large (hundreds of pages long) for large data selections. Please consider the amount of paper needed before printing large reports.

Hot Water Report – Provides a complete overview summary of the digital recirculation valve and hot water system performance over the time period selected. Included in this report will be an overall average of hot water inlet temperatures, recirculation return temperatures, actual outlet temperatures as well as a comprehensive list of all alarm/alert conditions monitored. Finally, the report will provide a temperature trend of the hot water system throughout the time period selected.

Export All Steam Trap Data – Exporting All Steam Trap Data will generate a spreadsheet containing all the raw data of the data selected.

Armstrong®

SAGE™ SECURITY

Secure Hosting Environment

Partnerships

In order to provide advanced levels of infrastructure security, Armstrong® has partnered with two entities. Logicalis Inc. is recognized as a Channel Company's 2015 CRN Managed Service Provider (MSP) Elite 150 (http://www.us.logicalis.com/about-us/awards/.) It is a global company that has won multiple industry awards from HP, IBM, Cisco, and VMware because of its success in hosting cloud solutions for 250 high-profile clients. Logicalis has a focus on IT Service Management (ITSM) through implementation of ITIL-based standards. Armstrong® has contracted with Logicalis to provide a secure hosted solution for SAGE™ intelligent energy management offerings. The services include the Enterprise Cloud Hosting Solution that provides 24x7x365 monitoring, management, and support of the SAGE™ solution using infrastructure-as-a-service (IaaS) framework. This ensures availability and reliability of servers needed to trend customer data.

In order to provide high availability (HA) and disaster recovery (DR) services to customers, Logicalis has chosen to contract data center hosting with IO® (https://www.io.com/.) This partnership provides a secure cloud computing environment with unlimited growth potential. IO provides data center as a service with a combination of colocation and cloud offerings for Logicalis customers. The world-class datacenter facilities feature physical security, physical customer equipment segmentation, raised floor, redundant power and HVAC, and a 100%-uptime SLA. IO® hosts North American data in data centers in New Jersey, Ohio, and Arizona. The cloud infrastructure, and corresponding customer data, can securely migrate from one location to another due to planned service or disaster.

Both Logicalis® and IO® have achieved SAS 70 and SSAE 16 Type 2 Certifications. This involves a regular and extensive security audit process. The data center has received Underwriters Laboratories (UL) Modular Data Center Safety Certification as well as Uptime Institute's Tier III Design Certification.

Physical Security

Physical security is provided by IO-hardened data center physical buildings. A combination of biometrics and extensive physical security measures are used to protect the physical hosts of the virtual servers. Logicalis has a secured modular colocation pod within the IO® facility to provide another layer of physical security and segmentation.

Environmental Security

Humidity, temperature, and power are continuously monitored in the hosted environment. The IO® facility is fed by multiple power grids and has redundant battery backup, in addition to redundant generator-power for unlimited run time during extensive power outages. The raised floor and facility elevation protect against floods. Humidity and temperature in the hosted environment is regulated by a redundant facility-wide HVAC system. The data center is under constant camera surveillance.

Secure Hosting Environment - Continued

Virtualization Security

Industry best practices for virtualization security are observed for SAGE™ hosting. Inherent in a virtualization solution is the ability to migrate servers and data stores in the live environment at any time. Additional resources can be allocated to the servers without the need to bring the system offline. The Hypervisor gives logical protected segmentation between virtual machines and between data stores. Private networks using secure private VLANs are configured for Armstrong®. In addition, virtual firewalls protect and limit data transmission between networks. Multiple firewalls and gateways monitor and protect traffic traversing the cloud infrastructure.

OS and Application Patching

Immediate notification of operating system patch availability is given to Armstrong® by Logicalis® Enterprise Cloud support technicians. The Red Hat Linux patches are applied and observed in the test server environment. Once the functionality and security has been validated, the patches are applied to the production server environment. This process typically spans a 48-hour timeframe from patch delivery to completion of patching process. Patch management is critical to the security of the SAGE™ solution.

Non-security patches for installed software (application server, database) are reviewed and applied quarterly. Critical bug or security vulnerability patches are deployed as-needed using the same process described above for operating system patches.

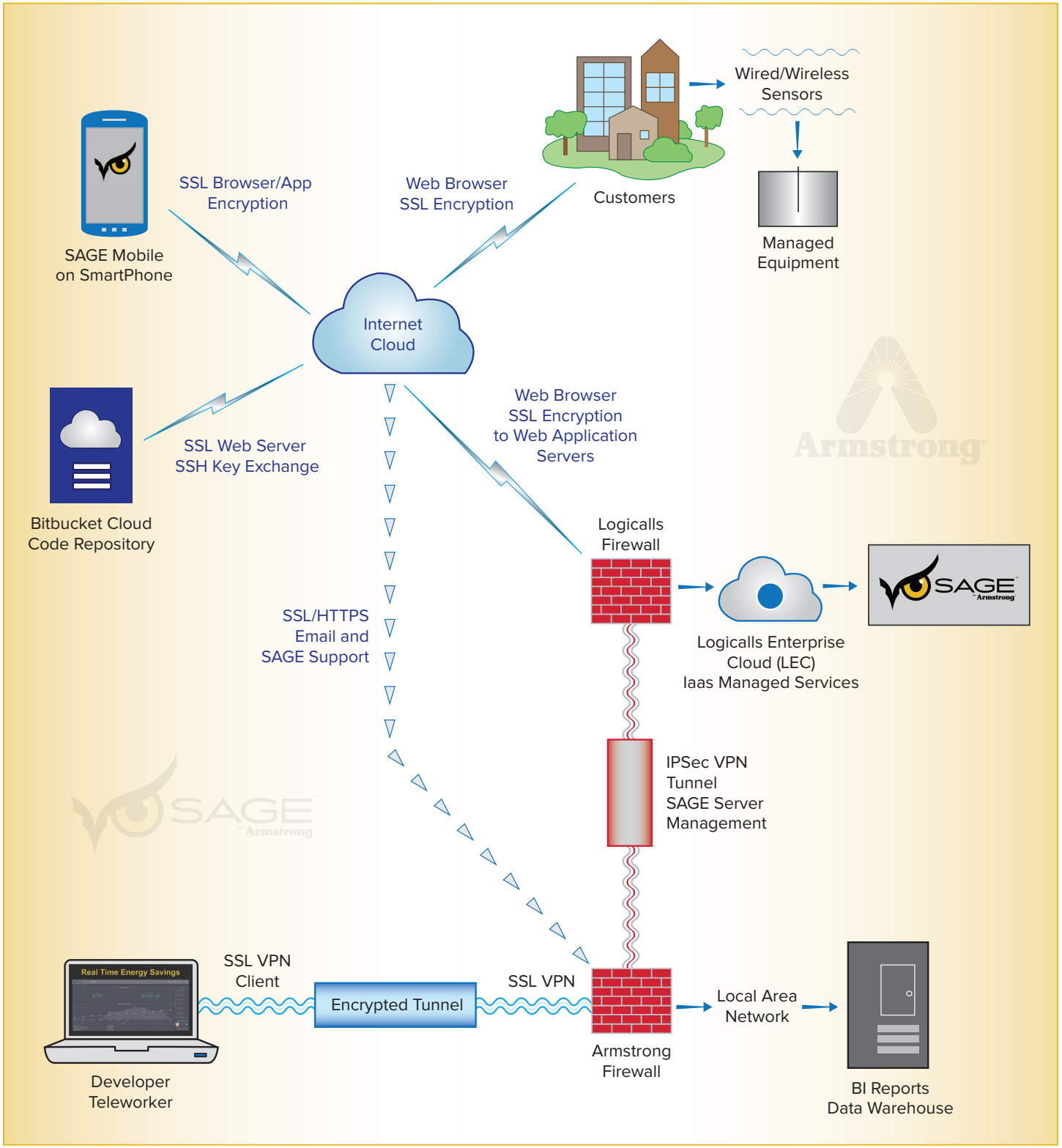
Remote Connectivity

Logicalis® and Armstrong® developers and support personnel may need to access the hosted application infrastructure. Remote connectivity best practices in security are used to provide a trusted connection between remote source and the data center. Infrastructure changes and updates are encrypted using a point-to-point IPSec virtual private network (VPN) tunnel with SSO SAML authentication. High-encryption settings are used to protect the data from the public cloud.

SSH access to the SAGE™ servers is protected with public/private keys. Database access is restricted by firewall rules to only other SAGE™ servers and is protected with a strong password.

SAGE™ Security by Armstrong®

With **SAGE**™ you can be confident in the secure storage of your data and all data transactions.



Secure Hosting Environment

Best Coding Practices

SAGE™ is a world-class utility system management software that is developed using best practices for application development security. The application is developed using simple and efficient code that reduces the likelihood for errors. Input validation is performed on data coming from trusted data sources; other input is dropped. Integral security is inherent in SAGE™ software by developing using the principle of defense in depth.

SAGE™ SDLC

The Armstrong® application development team creates software solutions using a mix of Waterfall and Agile programming practices as part of the Software Development Life Cycle. Periodic developer meetings during the design, coding, and testing phases ensure that security issues are identified and mitigated using the strength of the team. Iterative review of secure code and reported bugs ensures timely resolution of application vulnerabilities.

Coding Frameworks

Industry-tested common coding frameworks and libraries are used to enhance application reliability and integrity. The framework offers a comprehensive programming and configuration model. Development of SAGE™ uses a security framework to integrate authentication and authorization.

Access Control

Access control for Armstrong® applications involves the use of least privilege to limit access to include only identified monitoring and management users. Each user has unique credentials for login to the SAGE™ application. Secure application access is enforced using the access list configured in the authorization module.

Code Vault

Source code for custom applications must be protected from alteration. The patented SAGE™ monitoring system retains source code for client-server and mobile applications in a secure source code repository. The cloud format allows for secure development collaboration and code storage utilizing SSH access and public-key asymmetric encryption technology.

Testing

The security framework protects against common web application attacks such as CSRF, XSS, and injection attacks. Developers are aware of secure coding practices which prevent back-door vulnerabilities and the ability to alter program characteristics.

Mobile Application Development

The mobile app uses the same authentication, authorization, and encryption mechanisms as the web application. iCloud Keychain is used to store SAGE™ user login credentials.

Secure Operating Environment

Authentication

Centralized directory authentication is used to access the SAGE™ environment. The authentication is integral to the security of the environment. Passwords are encrypted as data at rest within the directory.

Transport Security (Network)

Front-end web access of the SAGE™ application relies on the security provided by SSL/TLS. The Public Key Encryption (PKI) algorithms provide 128-bits (or higher) of encryption. Authentication server traffic is encrypted using TLS-protected transactions.

Customer Data

Customer data created by energy management systems are not considered sensitive data. The live data consists of arbitrary data such as line pressures, temperatures, and acoustics. Stored data is comprised of aggregated equipment information. The power of the solution comes from calculations performed on the data and the cost savings that can be realized through analysis and trending.

Web and Application Security

Real-time transactions between the Proxy software and SAGE™ are encrypted using SSL encryption. A username, password, unique token are required to send real-time readings to SAGE™. Furthermore, readings are validated upon receipt and dropped if they fail validation.

Web application security is provided between the customer browser and the SAGE™ web servers. Developer management transactions to the SAGE™ servers are likewise authenticated, authorized and encrypted using web browser security. Please see figure 1 for more information.

Malware

All SAGE™ servers run Red Hat Enterprise Linux. Software is installed only from trusted and verified repositories, and kept up to date with security patches.

Security Audits

Logged entries are maintained regarding any system access and asset modification Alerts of threats to the technology infrastructure are reviewed. Security analysis covers all logical technology layers to ensure defense in depth: physical security, applications, operating systems, network transmissions, data storage, and access control. Internal audits are validated by external third-party audits and penetration testing that meet the requirements of industry-standard security regulations- PCI and HIPAA.

Business Continuity and Disaster Recovery

Data Backups

Backup of the infrastructure contents occurs at many levels. The virtual machine (VM) receives a snapshot every 24 hours. The snapshot can be used to restore a full VM, a volume from the VM, or specific files and directories. Retention of daily snapshots is available for a 2-week period. Monthly data backups of customer data is kept indefinitely for trending purposes. The SAN storage initiates hourly block-level snapshots for restoration in case of a failure or security incident.

Secondary Data Center

Although the primary data center for the hosted Logicalis® Enterprise Cloud solution is in Ohio, the servers and data could reside in other location based on circumstances. A natural disaster or prolonged environmental failure could force a replication to the secondary data center sites. The replication process is encrypted over a private network connecting the locations. Secondary data centers reside in New Jersey and Arizona. All facilities maintain the same level of SLAs and infrastructure security.

Connectivity

Lack of connectivity can create a Denial of Service (DoS) condition. In order to prevent this situation, multiple service providers are used to transmit data to and from the Logicalis® hosted cloud solution. The connectivity can load-balance and is fault-tolerant. This would prevent a failure of a single Internet Service Provider (ISP) from making the SAGE™ solution unavailable to Armstrong® customers.

SAGE™ Support

Installation

Installation of the SAGE™ solution for monitoring steam and hot water components is the responsibility of the authorized representatives. Proxy installation could be required of either Armstrong® or our customers, depending upon the agreed deployment topology. Customers will have to configure the appropriate connectivity (NAT and access lists) on their firewalls and security appliances. Hosting of the SAGE™ infrastructure is the privilege and responsibility of Armstrong®.

Application Support

Support for the SAGE™ application is provided by Armstrong® developers and engineers. The first contact should be to SAGE™ Support. Help can be provided through email, voice services, and video conferencing. Contact information can be found at:
https://www.armstronginternational.com/products-systems/sage%E2%84%A2-armstrong.

Incident Response

Availability of servers and applications is monitored around-the-clock. Application availability alerts have been set up to contact Armstrong® personnel in case of operating system or application failure. Logicalis® Enterprise Cloud Services also provide 5-minute granularity of performance data. Resources such as CPU, memory, network, and disk utilization are recorded and graphed for analysis and troubleshooting. Projected growth is implemented as resource upgrades to servers.

In the event of a security incident or data breach, Armstrong® will notify the customer immediately. Regular timely updates will be provided until a resolution is achieved. Any planned downtimes will be relayed to customers based on the list of organizational contacts that have been submitted to Armstrong®.

INTELLIGENT SOLUTIONS IN STEAM, AIR AND HOT WATER

Armstrong International

North America • Latin America • India • Europe / Middle East / Africa • China • Pacific Rim

armstronginternational.com

347-EN

Printed in USA - 4/16