Evaluation of Government Exposed Building Automation Systems

Brought to you by:

WhiteScope LLC and QED LLC

Concerns

- Exposure of devices to the Internet is the *number one risk* for building automation systems
  - Allows remote attacker to create cyber-physical effects
  - Provides potential access to corporate networks
  - Provides attack vectors to devices without detection
- Lack of capability to identify Internet facing devices
  - Multiple critical buildings exposed across myriad agencies
  - No insight into the magnitude of the risk or exposure

BASec: Government Facilities

- Over the past year
  - Scanned the Internet for building automation systems
  - Hundreds of exposed government facilities identified
  - Default configurations are the norm
  - Weak/default passwords and unpatched systems
  - Exposed devices extremely vulnerable to attack
- Reporting
  - List of exposed government facilities provided to DHS, GSA, GAO and DoD over the past year
  - Risk still exists
  - Who's role is it to accept responsibility

Example Findings

What is the exposure?

Numerous government building automation systems exposed to the Internet

IP Address/Hostname	Device Identifying Information
[redacted]	US_Forest_Service
	Texas_Forest_Service
	USDA_Forest_Service
	USDA
	SocialServices
	FederalBuilding_Phase2_2
	ABERDEEN_DSHS - ABERDEEN Department of Social Health and Services
	South_Quincy_Tower1 - Virginia Department of Social Services
	Butterfly House - Smithsonian National Zoo
	RoyalNorwegianEmbassy
	Brazilian_Embassey
	MadisonBuilding
	Reston Executive Center I
	USUHS_ENS - Uniformed Services University of Health Science

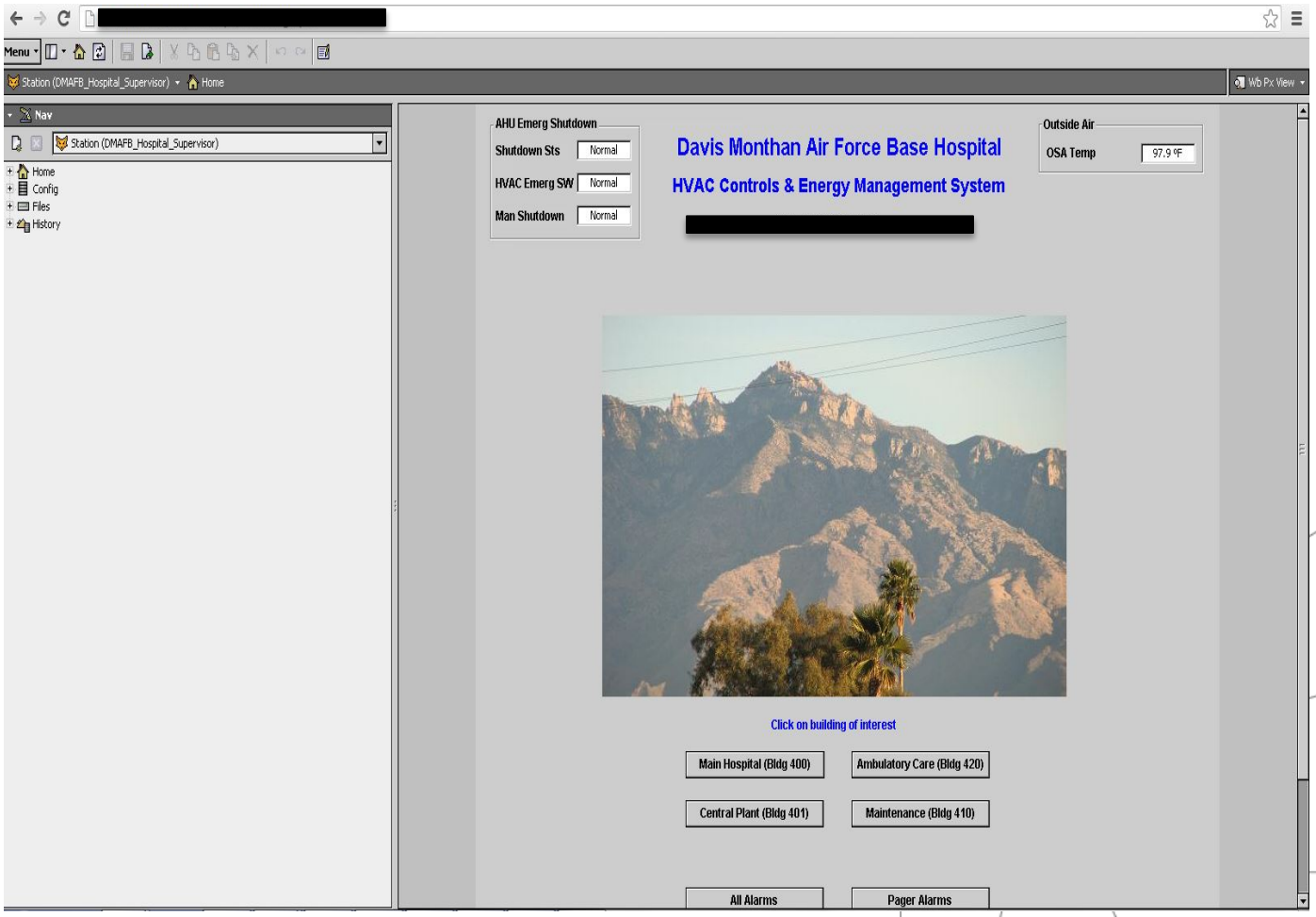
Example Findings

IP Address/Hostname	Device Identifying Information
[redacted]	FBI409
	US Secret Service - station.name=s:US_SECRET_SERVICE_JACE01
	Navy_Stadium
	GSA
	GSA_Tenant
	Fairchild Building - EPA
	PatriotRidgeSup
	Watergate South Building Automation Server
	Aegis70DCNationalArchives
	GSA Camden for use at Camden Federal Court House
	US DOT for use at Federal D.O.T.
	IRS
	Customs and Border Protection
	US Navy for use at NAB Little Creek
	US Citizenship & Immigration
	V.A. Medical Center Aspinwall
	West Point Alumni Center
	VA Care Center
	V.A. Medical Center
	Social_Security_WCary
	SocialSecurity

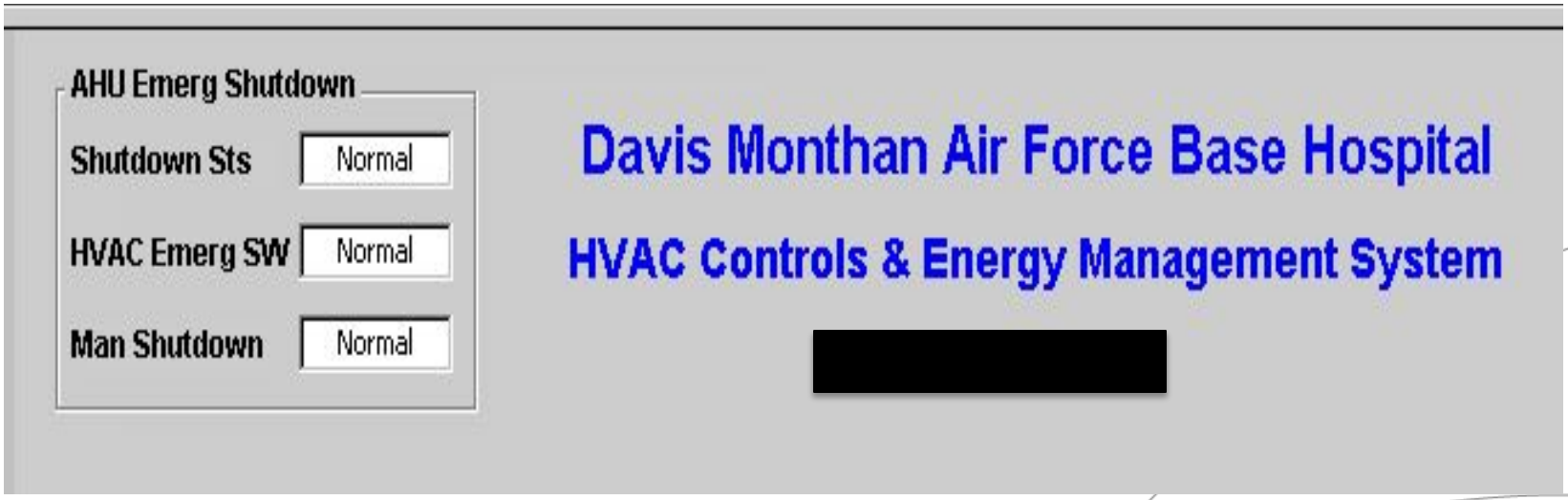
Example Findings

IP Address/Hostname	Device Identifying Information
[redacted]	CFedBldg
	Federal_Reserve
	Federal_Reserve
	Federal_Reserve
	Federal_Reserve
	federal3
	Langley Federal Credit Union
	LANGLEY_200
	NatFedCtHs
	FOX SJ_GSA_G3
	SJGSA_ENC_MAIN
	FedCourtSupervisor
	FedCourtSupervisor
	FedCourtSupervisor
	FedCourtSupervisor
	VanceFedBldg
	Annapolis Junction Lot6J1
	The_Lion_Building - Vietnam and Sudan Missions
	Embassy of the Gabonese
	Natural Resource Center/Homeland Security
	B426 BLS Building - Bureau of Labor and Stats
	c7125ColumbiaGatewayDr - ATT government solutions

DoD Example


Menu
Station (DMAFB_Hospital_Supervisor)
Home
Wb Px View
Nav
Station (DMAFB_Hospital_Supervisor)
Home
Config
Files
History
AHU Emerg Shutdown
Shutdown Sts
Normal
HVAC Emerg SW
Normal
Man Shutdown
Normal
Davis Monthan Air Force Base Hospital
HVAC Controls & Energy Management System
Outside Air
OSA Temp
97.9 °F
Click on building of interest
Main Hospital (Bldg 400)
Ambulatory Care (Bldg 420)
Central Plant (Bldg 401)
Maintenance (Bldg 410)
All Alarms
Pager Alarms

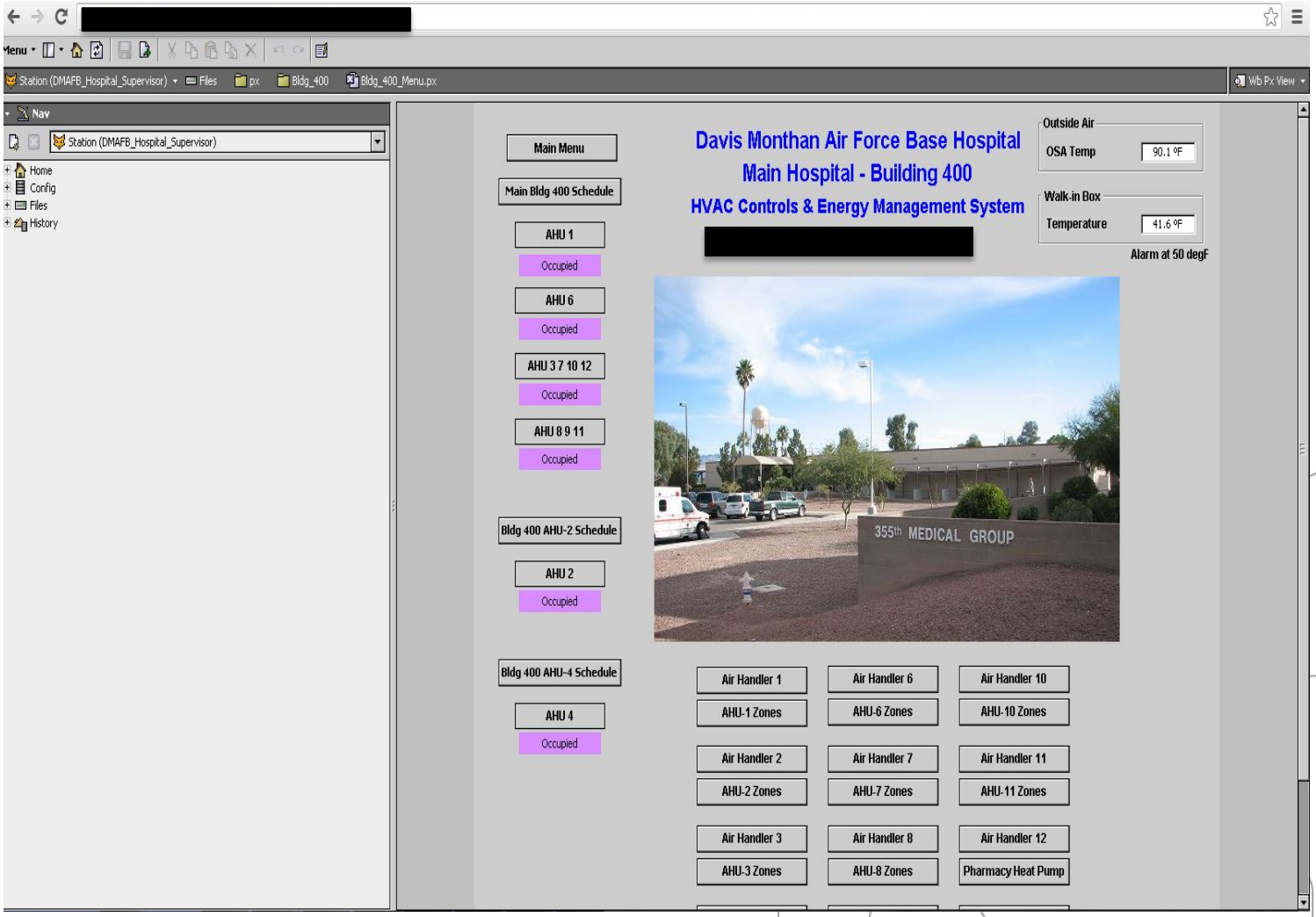
DoD Example


AHU Emerg Shutdown
Shutdown Sts
Normal
HVAC Emerg SW
Normal
Man Shutdown
Normal
Davis Monthan Air Force Base Hospital
HVAC Controls & Energy Management System
[redacted]

DoD Example


Click on building of interest
Main Hospital (Bldg 400)
Ambulatory Care (Bldg 420)
Central Plant (Bldg 401)
Maintenance (Bldg 410)
All Alarms
Pager Alarms

DoD Example


Station (DMAFB_Hospital_Supervisor)
Files
px
Bldg_400
Bldg_400_Menu.px
Nav
Station (DMAFB_Hospital_Supervisor)
Home
Config
Files
History
Main Menu
Main Bldg 400 Schedule
AHU 1
Occupied
AHU 6
Occupied
AHU 3 7 10 12
Occupied
AHU 8 9 11
Occupied
Bldg 400 AHU-2 Schedule
AHU 2
Occupied
Bldg 400 AHU-4 Schedule
AHU 4
Occupied
Davis Monthan Air Force Base Hospital
Main Hospital - Building 400
HVAC Controls & Energy Management System
[redacted]
Outside Air
OSA Temp
90.1 °F
Walk-in Box
Temperature
41.6 °F
Alarm at 50 degF
355th MEDICAL GROUP
Air Handler 1
AHU-1 Zones
Air Handler 6
AHU-6 Zones
Air Handler 10
AHU-10 Zones
Air Handler 2
AHU-2 Zones
Air Handler 7
AHU-7 Zones
Air Handler 11
AHU-11 Zones
Air Handler 3
AHU-3 Zones
Air Handler 8
AHU-8 Zones
Air Handler 12
Pharmacy Heat Pump

DoD Example

Air Handler 1	Air Handler 6	Air Handler 10
AHU-1 Zones	AHU-6 Zones	AHU-10 Zones
Air Handler 2	Air Handler 7	Air Handler 11
AHU-2 Zones	AHU-7 Zones	AHU-11 Zones
Air Handler 3	Air Handler 8	Air Handler 12
AHU-3 Zones	AHU-8 Zones	Pharmacy Heat Pump
Air Handler 4	Air Handler 9	Floor Plan
AHU-4 Zones	AHU-9 Zones	Pager Alarms

Challenges

- Reliance on third-party vendors and system integrators
- Lack of common configuration/implementation standards
- Interconnection of multiple devices over common networks
- Use of commercial network infrastructure by vendors for monitoring/control
- Government has no ability to identify, monitor or track systems that rely on commercial network infrastructure

Government agencies lack awareness of the magnitude of the cyber security risks and are taking no actions to mitigate that risks

Government is not Alone

But wait there's more!


GoogleWharf7
Username:
Password:
Login

```
<!-- /Services/UserService -->
<p n="UserService" h="3" t="b:UserService">
 <p n="admin" h="446a" t="b:User">
  <p n="fullName" f="r" v="Default Admin User"/>
  <p n="enabled" f="r"/>
  <p n="expiration" f="r"/>
  <p n="permissions" f="r" v="super"/>
  <p n="language" f="r"/>
  <p n="email" f="ro"/>
  <p n="password" f="ro" v="AH9rlmVx/CQaelOgisXSjPHYjstiD8Gq/Aczo+Gh7cA+h/CNCg=="/>
  <p n="facets" f="ro"/>
  <p n="navFile" f="r" v="file:^nav/NavFile.nav"/>
  <p n="prototypeName" f="r" v="superuser"/>
  <p n="networkUser" f="r" v="true"/>
  <p n="version" v="ControlworksOfficeServer:1297258428625"/>
```


C:\Users\bk\Desktop\java>java -cla
t2
Enter Password to be Decoded: AH9
==
anyonesguess
C:\Users\bk\Desktop\java>

Google Tenancy - Wharf 7

Temperature Outside : 20.74 °C

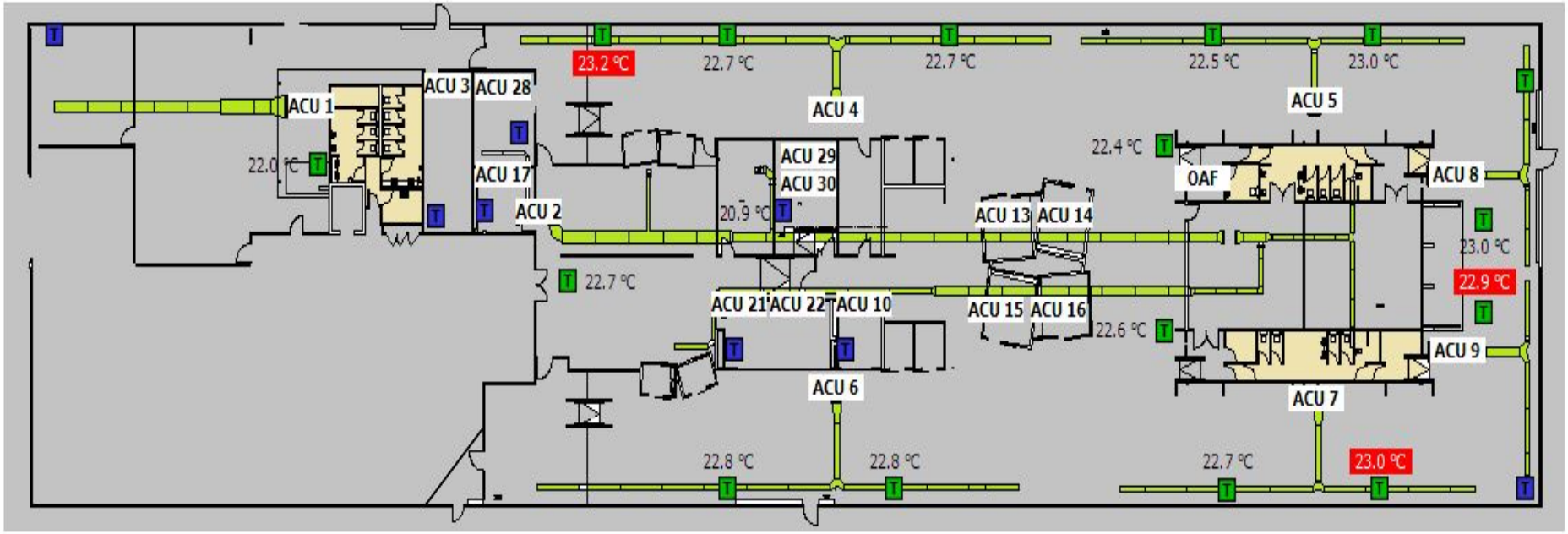
- BaseBuilding
- EnergyMeter
- VRF Summary
- History
- Users
- Schedule
- Alarm Console
- Active Overrides
- Active Alarms
- BMS Key
- Help
- LAN Diagram
- Functional Description

AfterHoursButton

- Roof
- Mezzanine
- Level 3
- Back

LEVEL 3

Current Time : 17-Apr-13 5:28 PM E



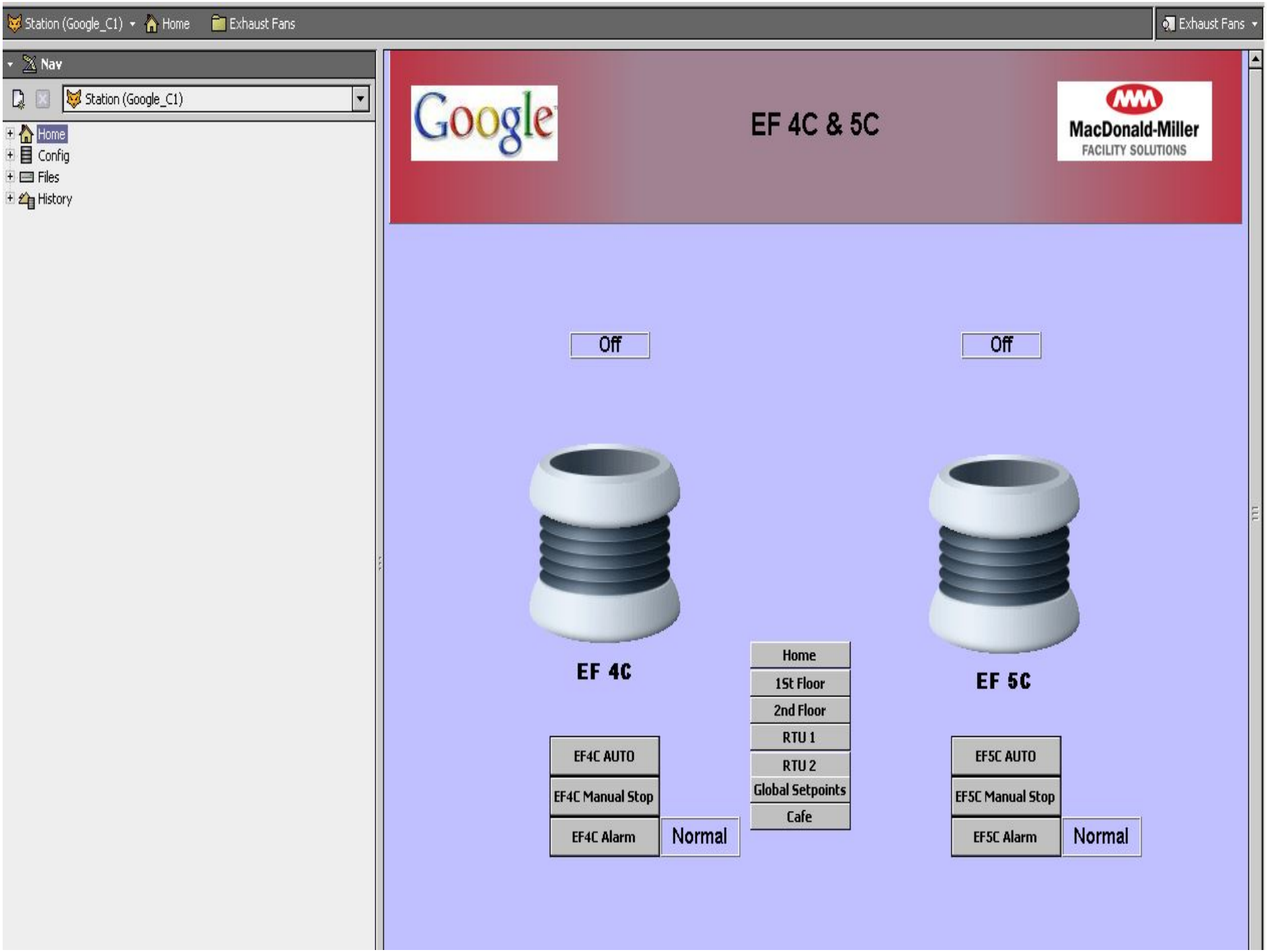
History
Active Overrides
Active Alarms
EnergyMeter
VRF Summary
Users

	Leak	Shut Off	Usage
North Kitchen	No Leak	Open	26940 L
South Kitchen	Leak Detected	Open	241140 L

Roof
Mezzanine
Level 3

QED Secure Solutions

WhiteScope


Station (Google_C1)
Home
Exhaust Fans
Exhaust Fans
Nav
Station (Google_C1)
Home
Config
Files
History
Google
EF 4C & 5C
MacDonald-Miller
FACILITY SOLUTIONS
Off
Off
EF 4C
EF 5C
Home
1St Floor
2nd Floor
RTU 1
RTU 2
Global Setpoints
Cafe
EF4C AUTO
EF4C Manual Stop
EF4C Alarm
Normal
EF5C AUTO
EF5C Manual Stop
EF5C Alarm
Normal

Station (Google_C1) ▾ Home Cafe VFD EF 7 VFD ▾

Nav

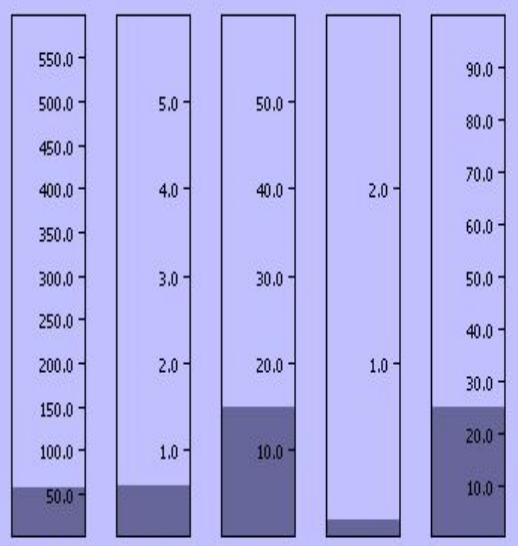
Station (Google_C1)

- Home
  - 1st Floor
  - RTU 1C
  - RTU_2C
  - Cafe
  - Exhaust Fans
  - Global Points
  - Google_C1
- Config
- Files
- History

Home
HP 101
HP 102
MUA 1
MUA 2
VFD EF 7
VFD HP 101
VFD HP 102
VFD MUA 1
VFD MUA 2

VFD EF 7

Run Status	ON
Fault Status	NORMAL
Run Hours	7379 hr
Drive Temp	82.22 °F



Top 10 – BAS Security Questions

- Are any our devices are facing the Internet? Have we confirmed?
- Are our devices patched with the latest version of vendor software?
- Do we know if any devices were recently replaced? If so, were they deployed matching our security policy?
- Are any of our old devices deployed to locations we longer manage?
- How do we audit our devices in a cost effective and repeatable way?

Top 10 – BAS Security Questions

- Are our devices configured securely, how can we verify?
- Do we have a security policy deployed to all of our devices?
- Are the log files being monitored for intrusion or malicious activity?
- How would we know if any of our devices have been compromised?
- How can we confirm the network segmentation or 'air gap' is secure?

Contact

http://smartbuildingsecurity.com

contact@whitescope.io

Questions?