ISACA VA Chapter

Auditing Your Infrastructure

Presented By:
Bryan Miller
Syrinx Technologies

Agenda

- Speaker Introduction
- What's the Issue?
- Why Bother?
- Real World Examples
- So How Do We Fix Things?
- Summary
- Q&A

Speaker Introduction

- B.S., M.S. – VCU
- Adjunct Faculty Member in IS and CS @ VCU
- CISSP, former Cisco CCIE
- VA SCAN, VCU FTEMS presenter
- ISSA InfraGard member
- Published author with over 25 years in the industry
- President, Syrinx Technologies - 2007

What's the Issue?

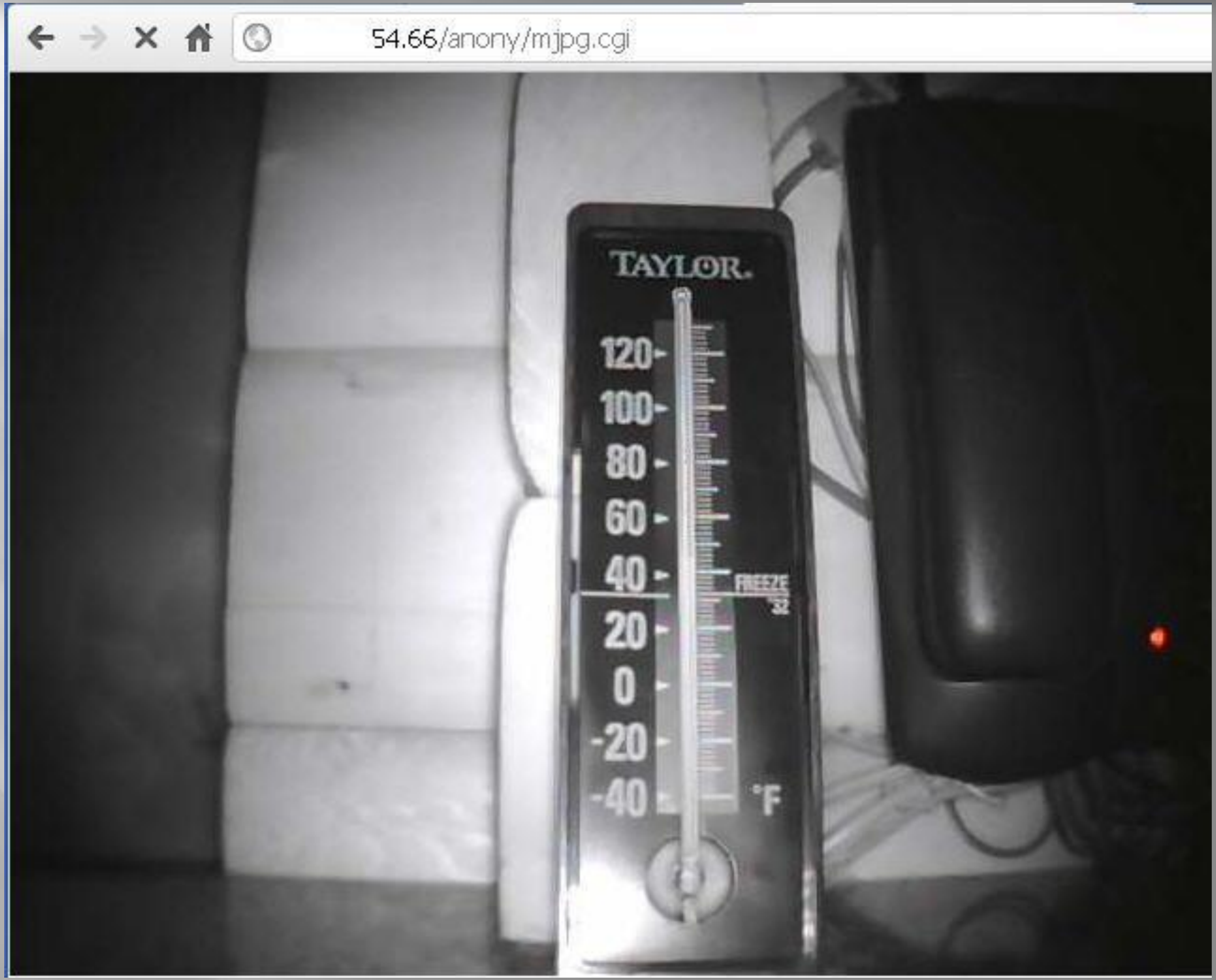
Potential Areas of Compromise

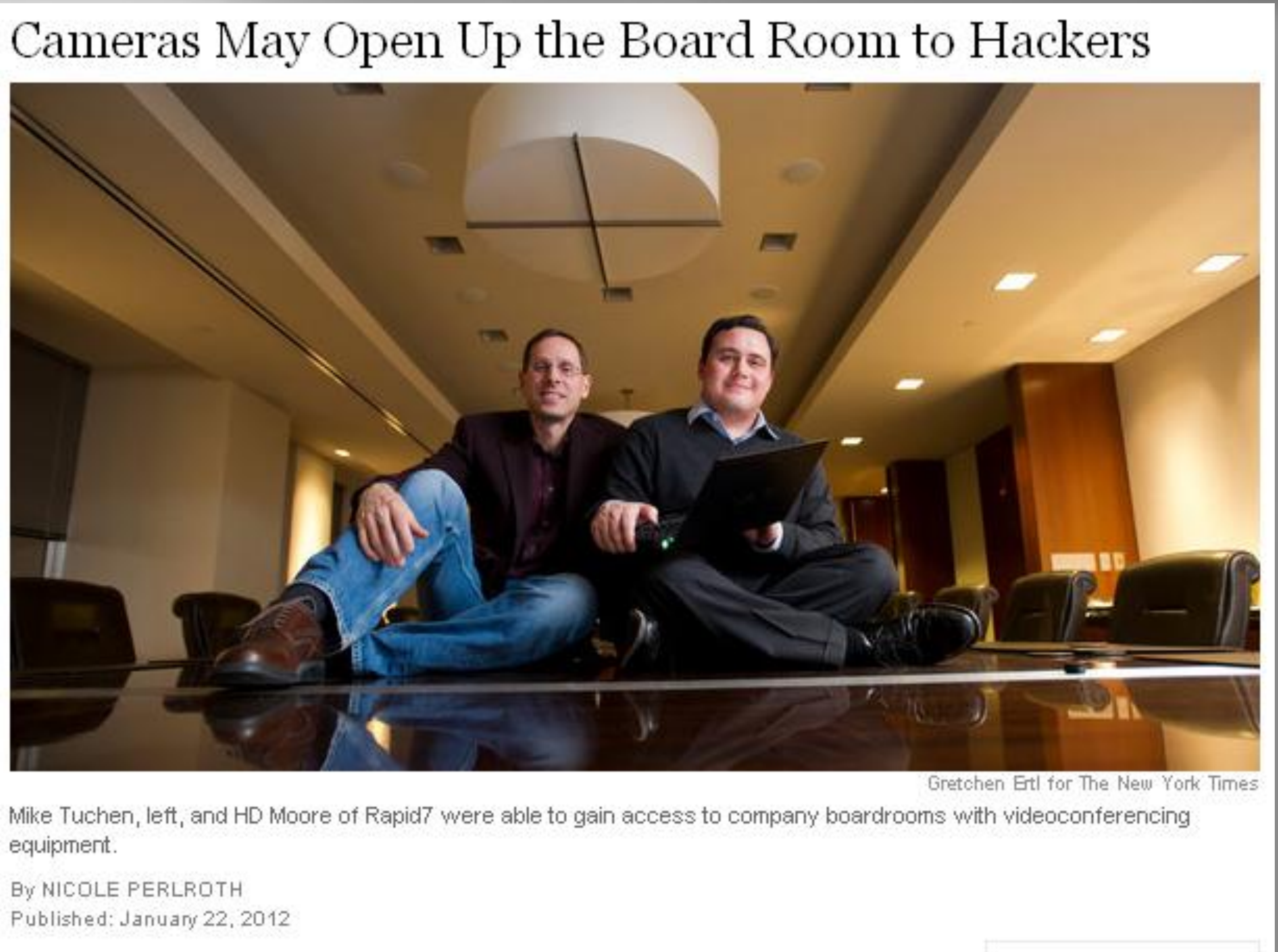
- Printers/Scanners/Copiers
- CCTV/NetDVR/Cameras
- Alarm Systems
- Fire Suppression Systems
- Videoconference Systems
- UPS
- KVM
- Industrial/Machine Control

- Recently in the news:
  - Feeds from thousands of Trendnet home security cameras have been breached, allowing any web user to access live footage without needing a password.
    - BBC News Technology, Feb. 6, 2012
  - NY Times Article discusses the issue of video conferencing systems that are vulnerable to compromise.
    - NY Times online, Jan. 12, 2012

Using Shodan, a quick search revealed "lots" of possibly vulnerable cameras.

Using the URL shown, we bypassed all authentication.





Cameras May Open Up the Board Room to Hackers

Gretchen Ertl for The New York Times

Mike Tuchen, left, and HD Moore of Rapid7 were able to gain access to company boardrooms with videoconferencing equipment.

By NICOLE PERLROTH
Published: January 22, 2012

Notable Points

- Commercial Printers Accountable for Identity Theft Protection Under FTC Enforcement of FACTA 'Red Flag Rules‘ – www.send2press.com, 4/10/09

- Electric Utilities Investing $4.1 Billion by 2018 to Secure Smart Grids – eWeek.com, 8/25/11

- State of SCADA Security Worries Researchers – eWeek.com, 2/5/12

ISACA VA Chapter

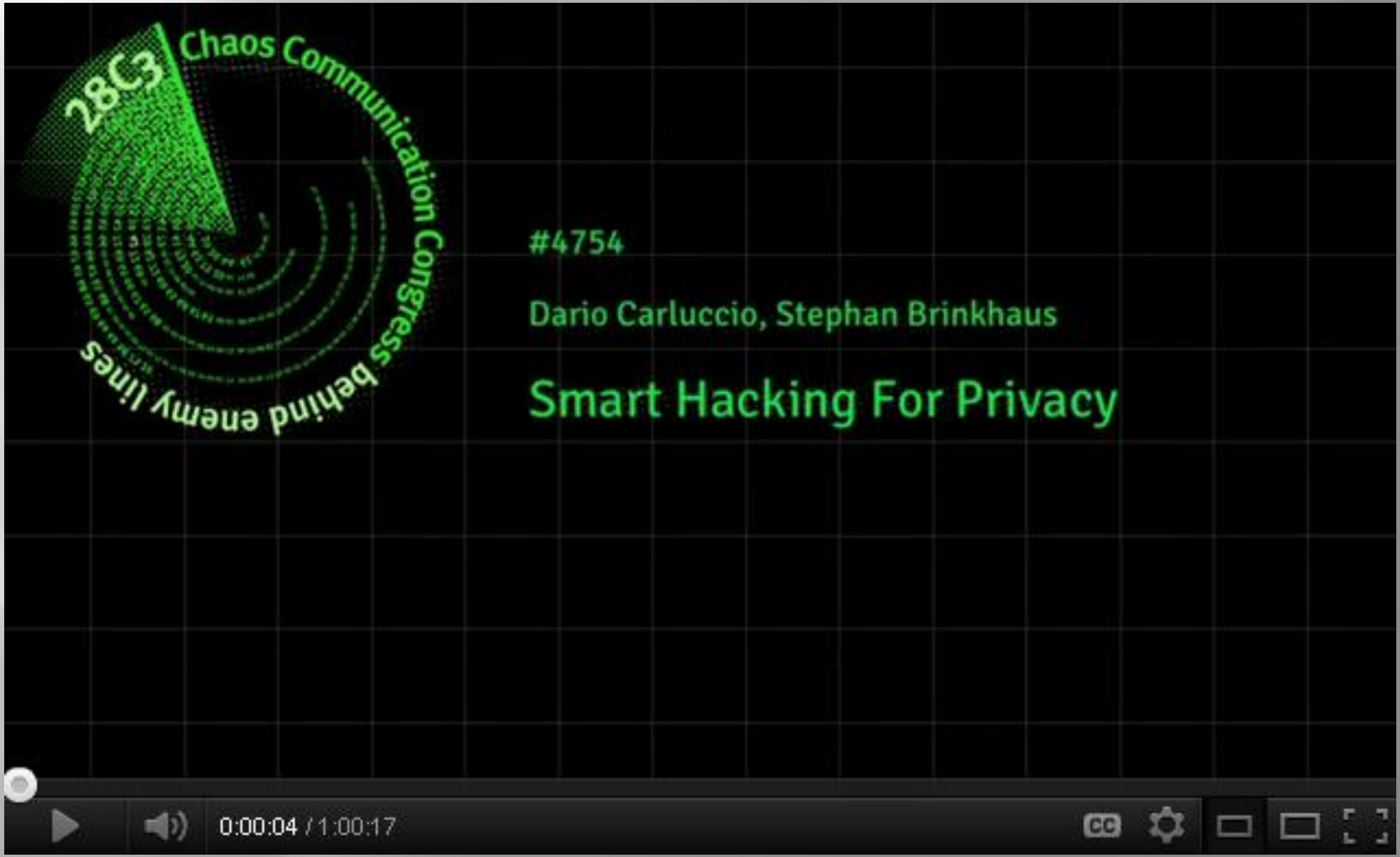
CBS News report by Armen Keteyian on the issues involved with data stored on printers.

April 20, 2010

ISACA VA Chapter

28th Chaos Computing Congress Presentation

It could be possible to discover what movies you watch by their power signature. Can you say Shazam?



28C3 Chaos Communication Congress behind enemy lines

#4754

Dario Carluccio, Stephan Brinkhaus

Smart Hacking For Privacy

ISACA VA Chapter

STUXNET:
-Spread by USB sticks
-Attacks PCs that control Siemens PLCs
-MS SQL password is released

Stuxnet is now an "open source weapon" that can be downloaded and improved upon.

- And the often forgotten….DUQU
  - Shares a code base with STUXNET
  - Signed using stolen digital certificates from the same Japanese company as STUXNET
  - DUQU appears to be an intelligence gathering agent while STUXNET just wants to do physical damage
  - Perhaps DUQU is gathering information for the next generation of STUXNET….

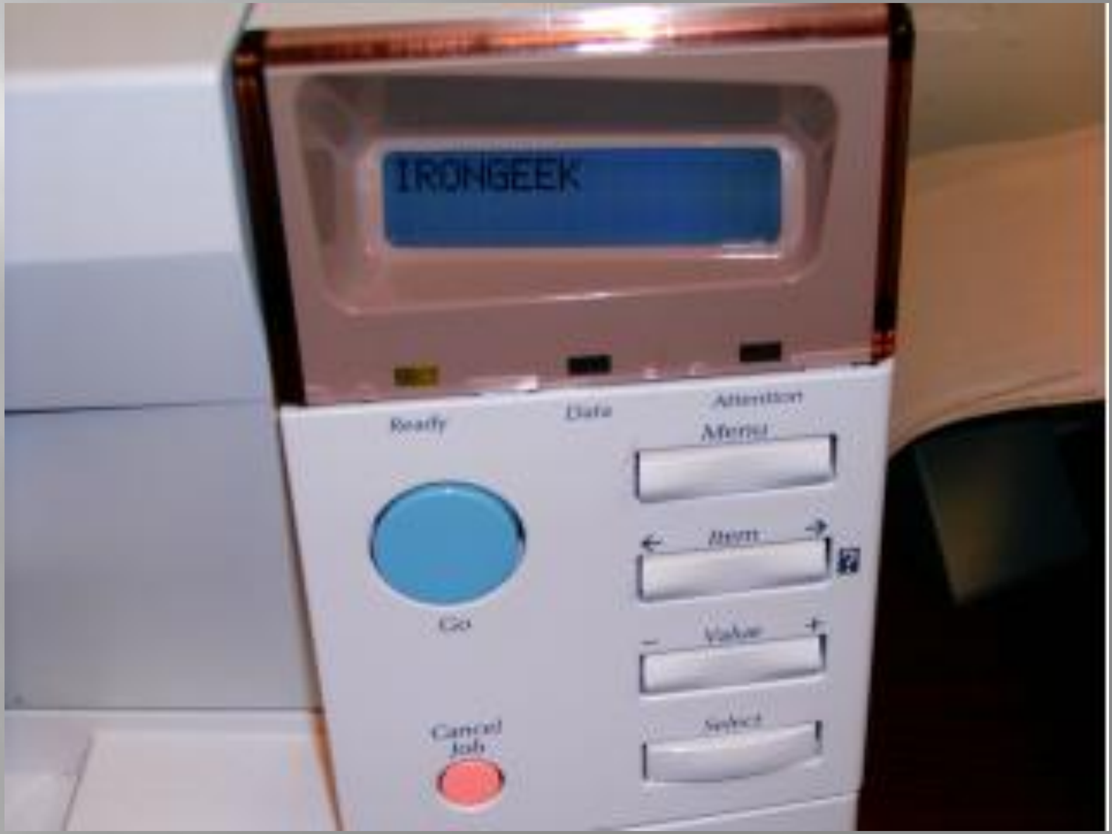
Why Bother?

- Every device on your network can possibly be leveraged to mount an attack.
- New issues are making the news every week.
- These devices can be configured correctly during initial installation and remove the risk.
- You have enough to worry about with the complex issues.

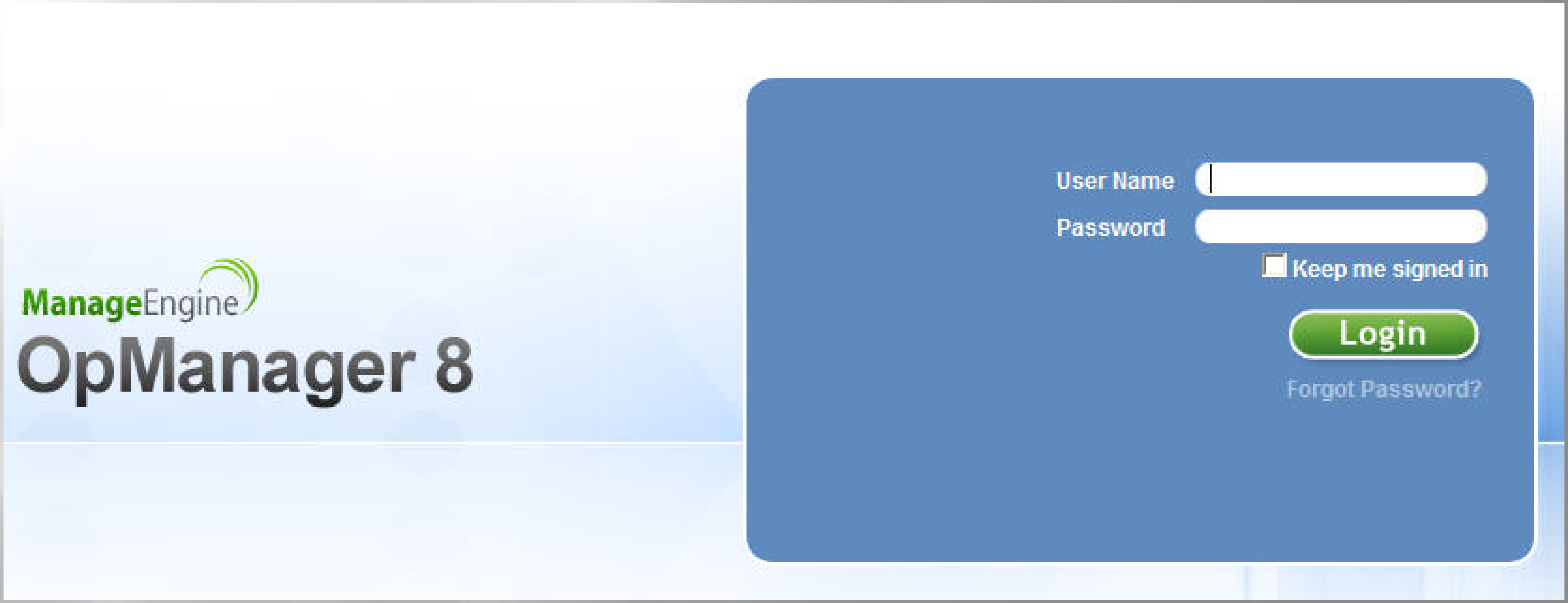
Wouldn’t it be really annoying if all your printers suddenly asked users to deposit $0.25 before printing?

You don’t even need a tool:

```
prompt> telnet 192.168.1.2  9100
@PJL RDYMSG DISPLAY=“foo”
^]quit
```



A True Story…

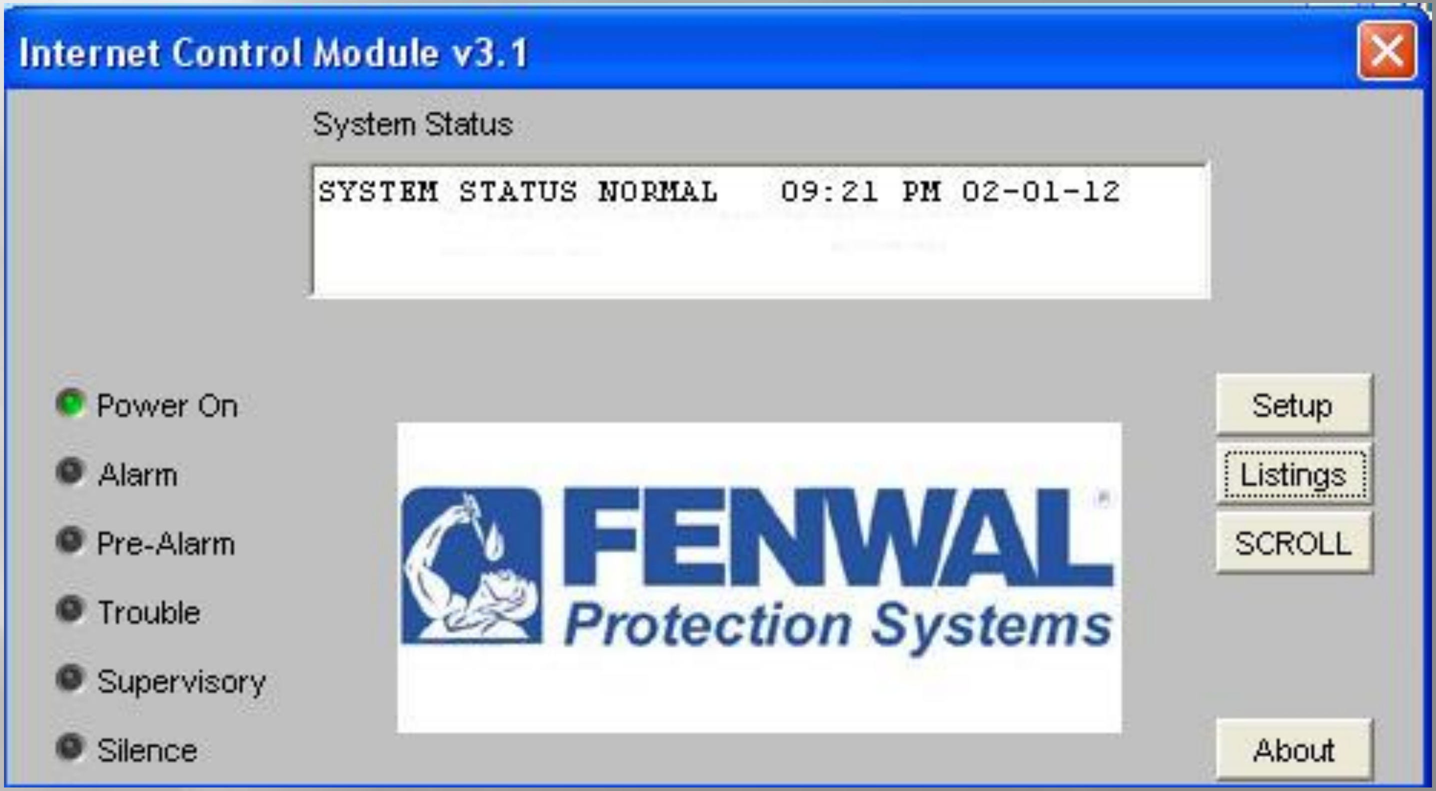


ManageEngine
OpManager 8
User Name
Password
□ Keep me signed in
Login
Forgot Password?

Real World Examples

Console Screen to Fire Suppression System.

Downloaded manual from the Internet. Installation password still valid.

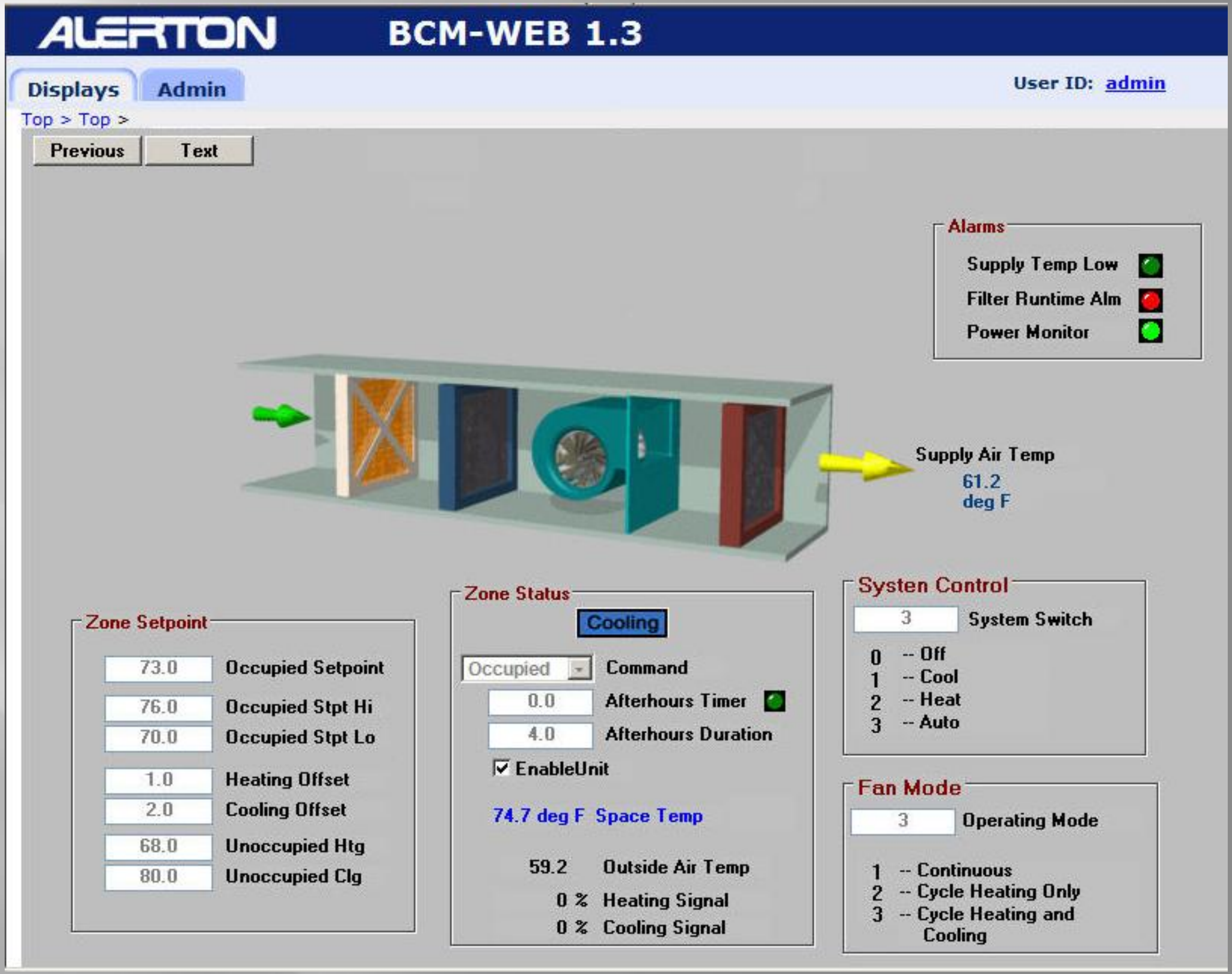

Internet Control Module v3.1

System Status

SYSTEM STATUS NORMAL   09:21 PM 02-01-12

Building HVAC controls.

Downloaded manual from the Internet. Admin password was valid.



ALERTON BCM-WEB 1.3

Displays | Admin

User ID: admin

Top > Top >

Previous | Text

Alarms
- Supply Temp Low 🟩
- Filter Runtime Alm 🟥
- Power Monitor 🟩

Supply Air Temp 61.2 deg F

Zone Setpoint

73.0	Occupied Setpoint
76.0	Occupied Stpt Hi
70.0	Occupied Stpt Lo
1.0	Heating Offset
2.0	Cooling Offset
68.0	Unoccupied Htg
80.0	Unoccupied Clg

Zone Status

Cooling

Occupied	Command
0.0	Afterhours Timer 🟩
4.0	Afterhours Duration

☑ EnableUnit

74.7 deg F Space Temp

59.2	Outside Air Temp
0 %	Heating Signal
0 %	Cooling Signal

Systen Control

3 System Switch

0 -- Off
1 -- Cool
2 -- Heat
3 -- Auto

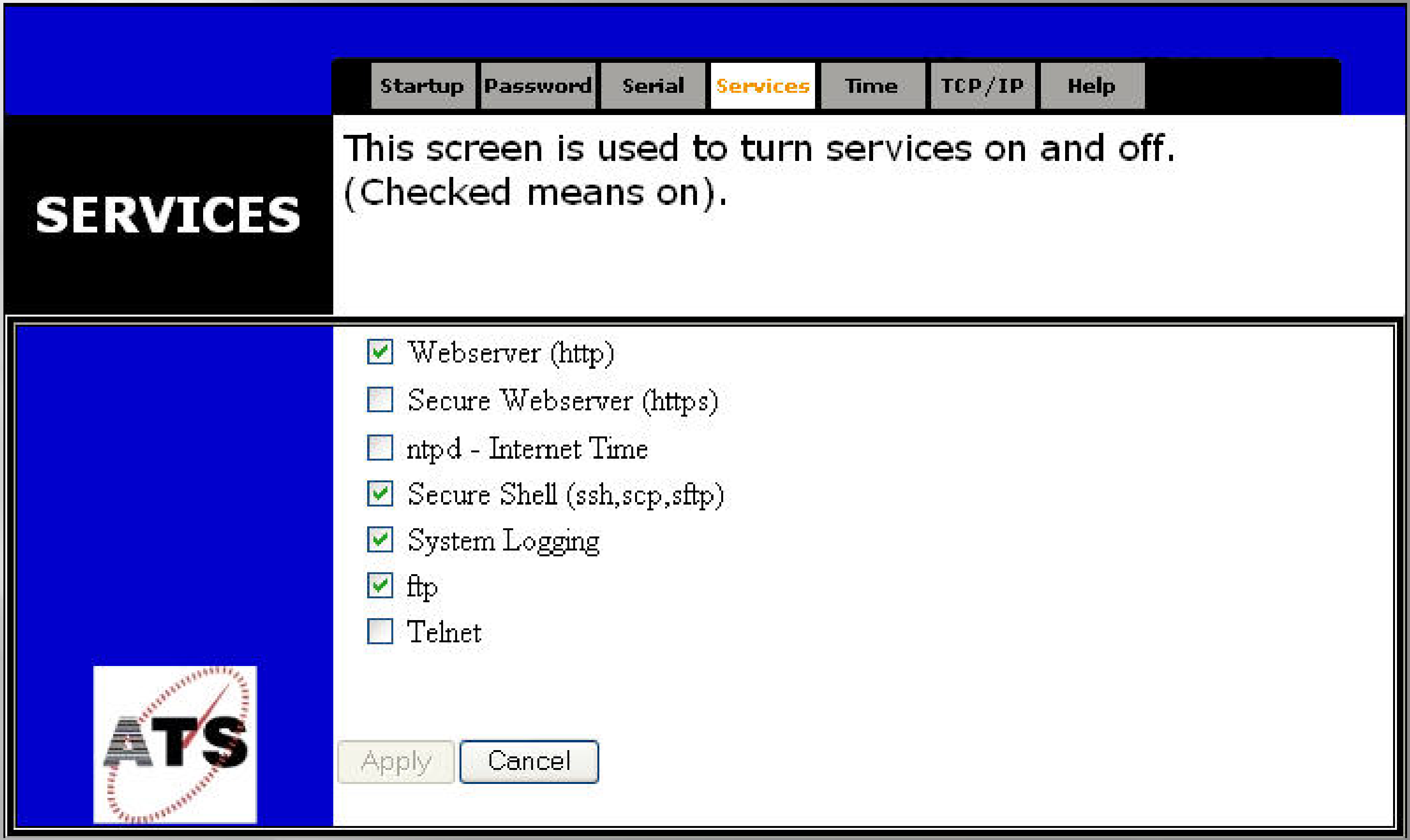
Fan Mode

3 Operating Mode

1 -- Continuous
2 -- Cycle Heating Only
3 -- Cycle Heating and Cooling

Time clock system.

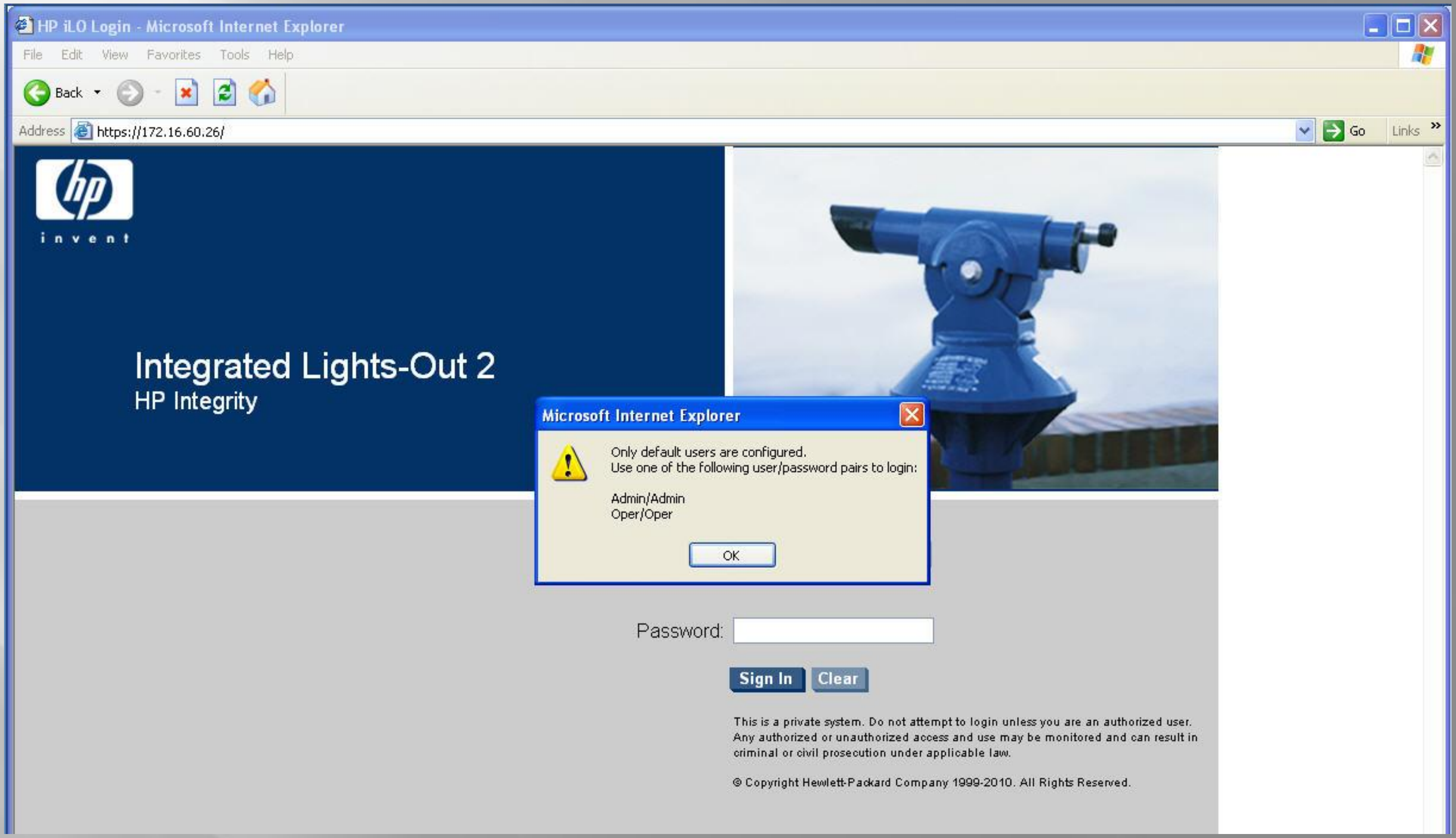
No credentials required for admin access.



This screen is used to turn services on and off. (Checked means on).

- ☑ Webserver (http)
- □ Secure Webserver (https)
- □ ntpd - Internet Time
- ☑ Secure Shell (ssh,scp,sftp)
- ☑ System Logging
- ☑ ftp
- □ Telnet

HP Integrated Lights Out (ILO) being very helpful in regards to usernames and passwords.


HP iLO Login - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back
Address https://172.16.60.26/
Go
Links
hp invent
Integrated Lights-Out 2
HP Integrity
Microsoft Internet Explorer
OK
Password:
Sign In
Clear

Only default users are configured.
Use one of the following user/password pairs to login:

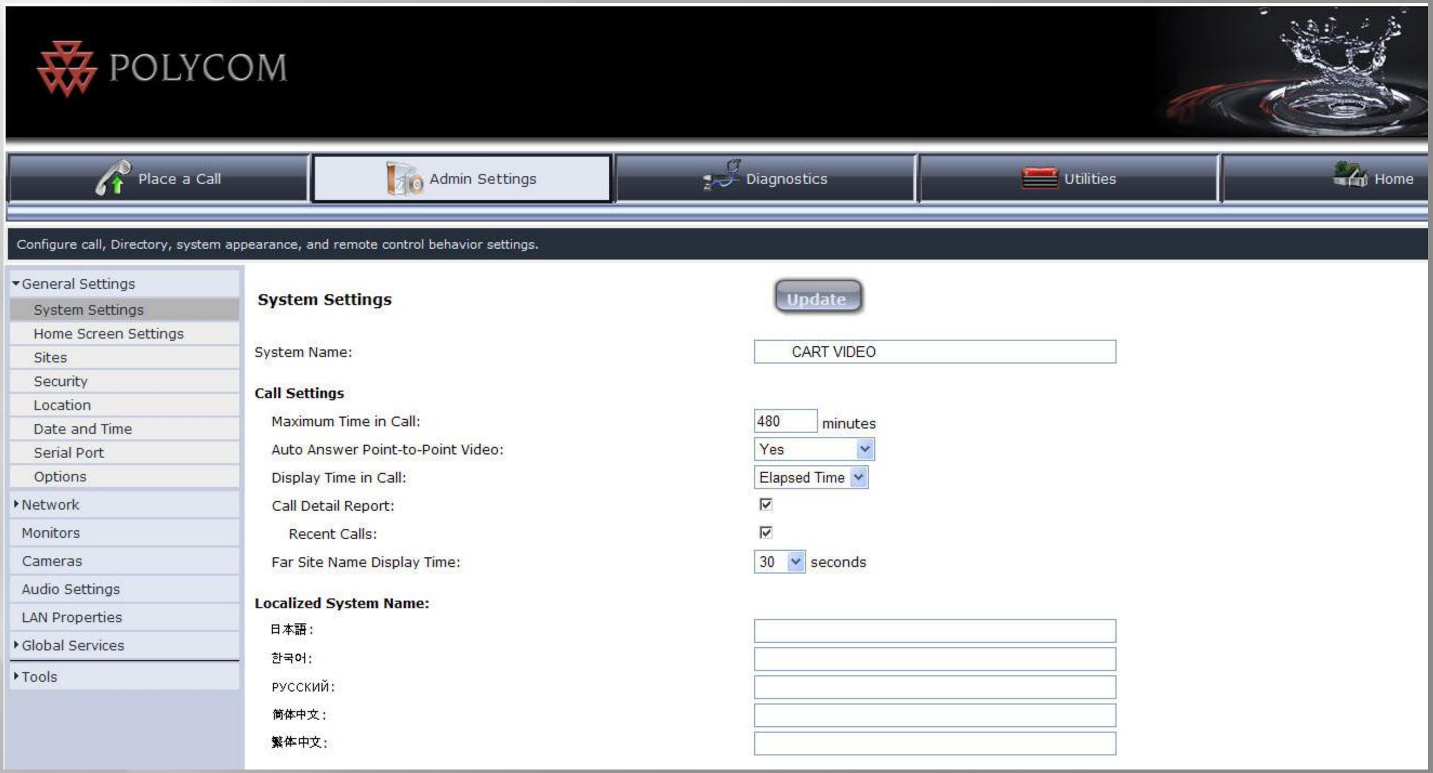
Admin/Admin
Oper/Oper

This is a private system. Do not attempt to login unless you are an authorized user. Any authorized or unauthorized access and use may be monitored and can result in criminal or civil prosecution under applicable law.

© Copyright Hewlett-Packard Company 1999-2010. All Rights Reserved.

Polycom VSX 7000.

Downloaded the manual from the Internet and logged in with default credentials.



Configure call, Directory, system appearance, and remote control behavior settings.

System Settings

System Name: CART VIDEO

Call Settings

Maximum Time in Call: 480 minutes

Auto Answer Point-to-Point Video: Yes

Display Time in Call: Elapsed Time

Call Detail Report: ☑

Recent Calls: ☑

Far Site Name Display Time: 30 seconds

Localized System Name:

日本語：

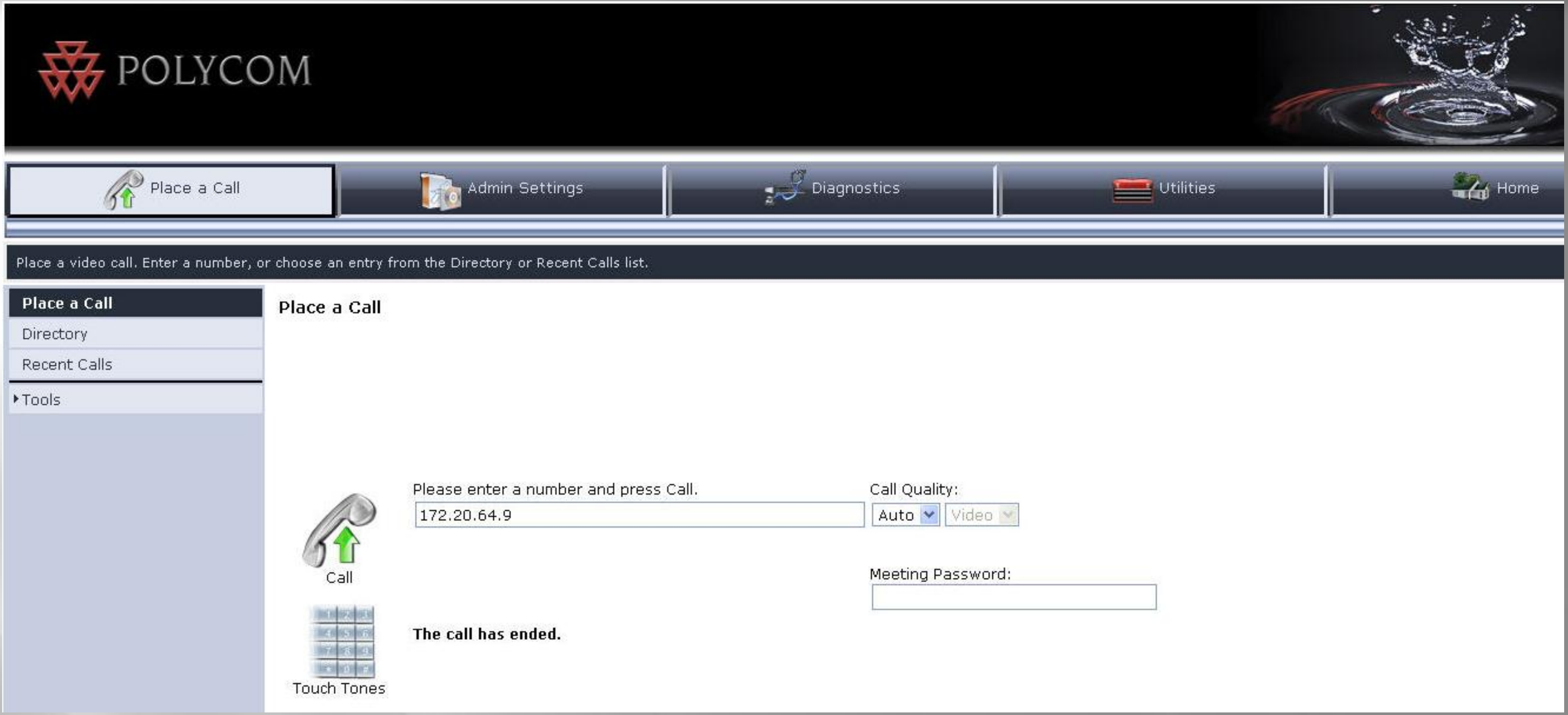
한국어:

РУССКИЙ:

简体中文：

繁体中文：

ISACA VA Chapter



Place a video call. Enter a number, or choose an entry from the Directory or Recent Calls list.

Place a Call

Please enter a number and press Call.
172.20.64.9

Call Quality: Auto Video

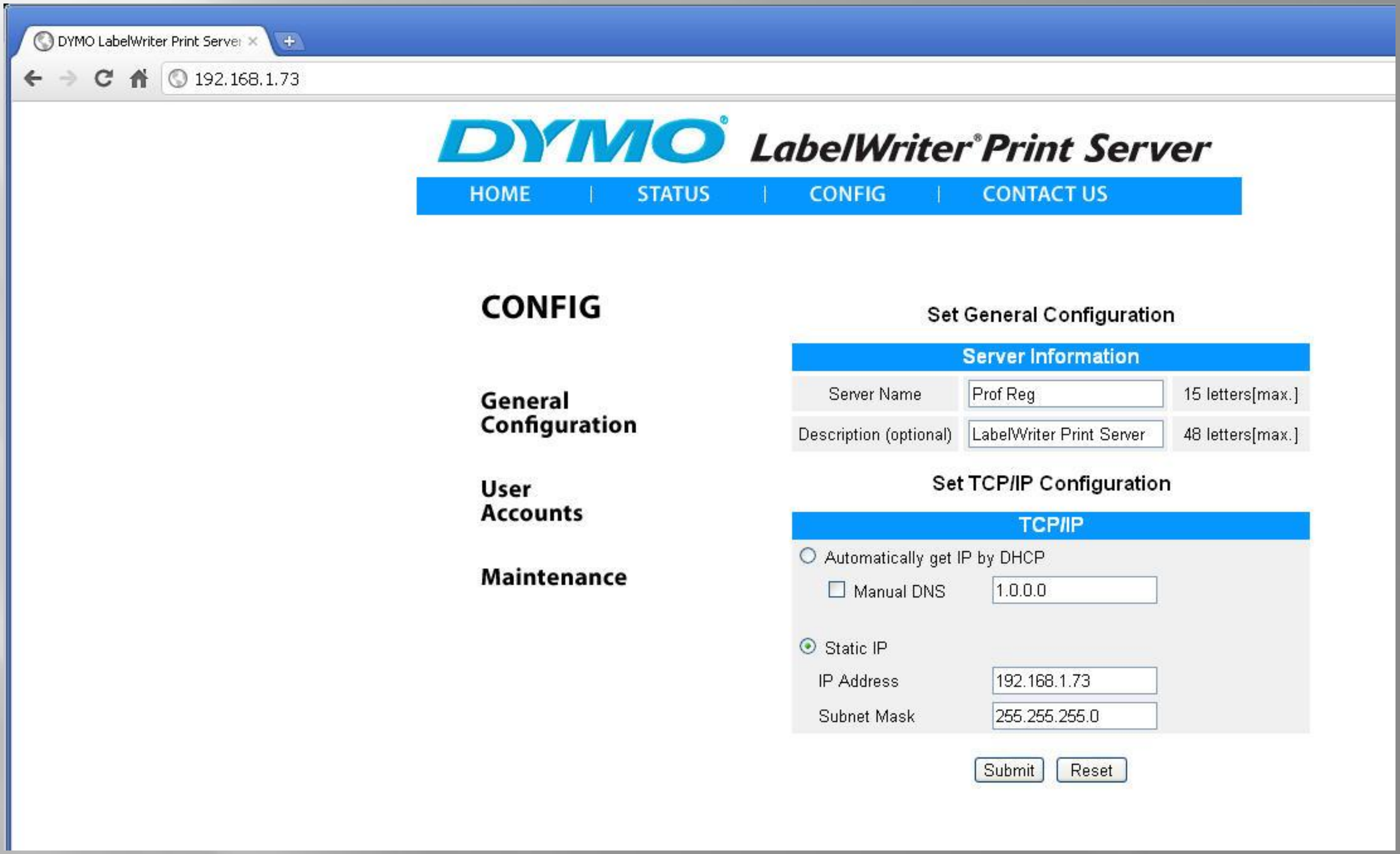
Meeting Password:

The call has ended.

No credentials….the Directory was loaded with interesting destinations.

Dymo LabelWriter Print Server.

Logged in with default credentials from manual downloaded from the Internet.


DYMO LabelWriter Print Server
192.168.1.73
DYMO LabelWriter® Print Server
HOME | STATUS | CONFIG | CONTACT US

CONFIG

General Configuration

User Accounts

Maintenance

Set General Configuration

Server Information		
Server Name	Prof Reg	15 letters[max.]
Description (optional)	LabelWriter Print Server	48 letters[max.]

Set TCP/IP Configuration

TCP/IP

○ Automatically get IP by DHCP

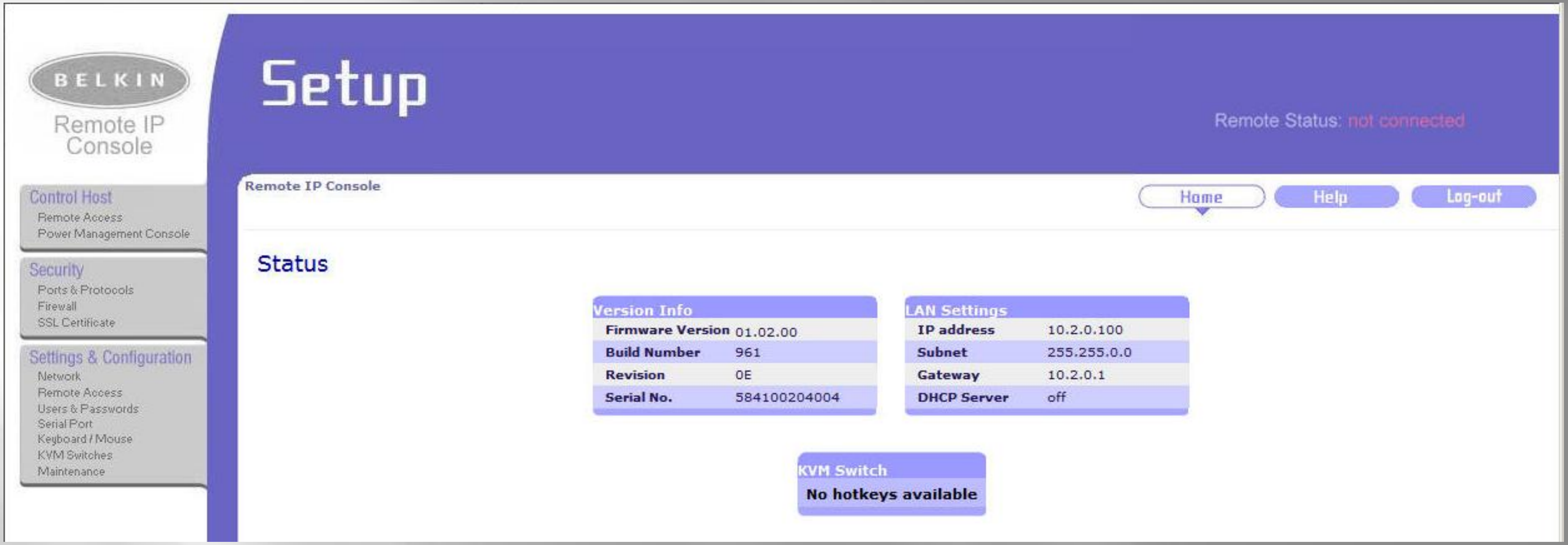
□ Manual DNS 1.0.0.0

● Static IP

IP Address 192.168.1.73

Subnet Mask 255.255.255.0

Submit Reset



Status

Version Info	
Firmware Version	01.02.00
Build Number	961
Revision	0E
Serial No.	584100204004

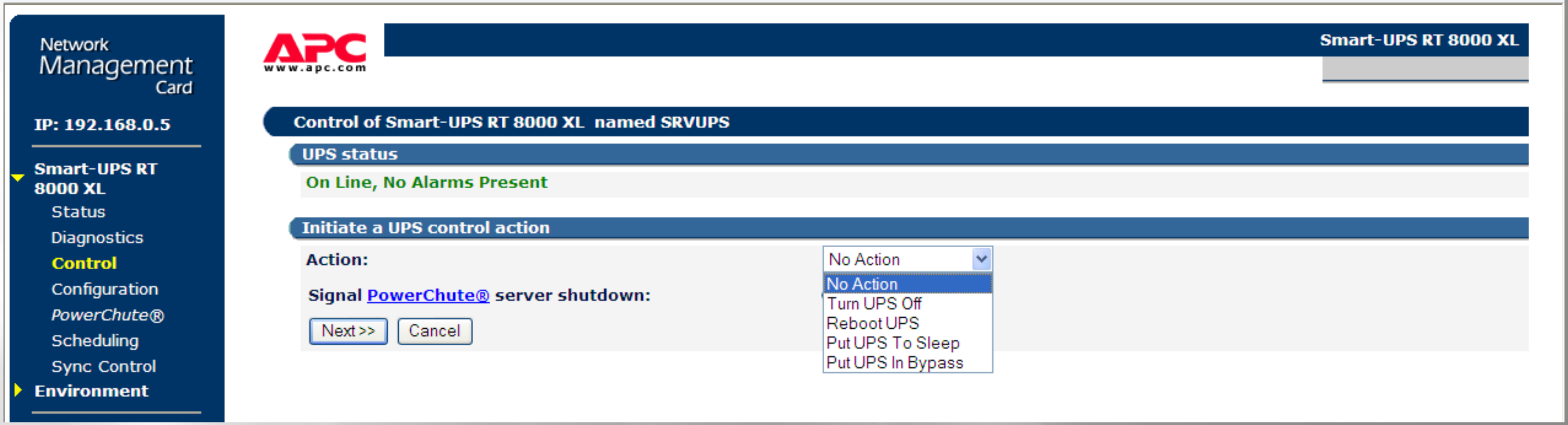
LAN Settings	
IP address	10.2.0.100
Subnet	255.255.0.0
Gateway	10.2.0.1
DHCP Server	off

KVM Switch

No hotkeys available

Belkin Remote IP-based KVM.

Logged in with default credentials.



Control of Smart-UPS RT 8000 XL named SRVUPS

UPS status

On Line, No Alarms Present

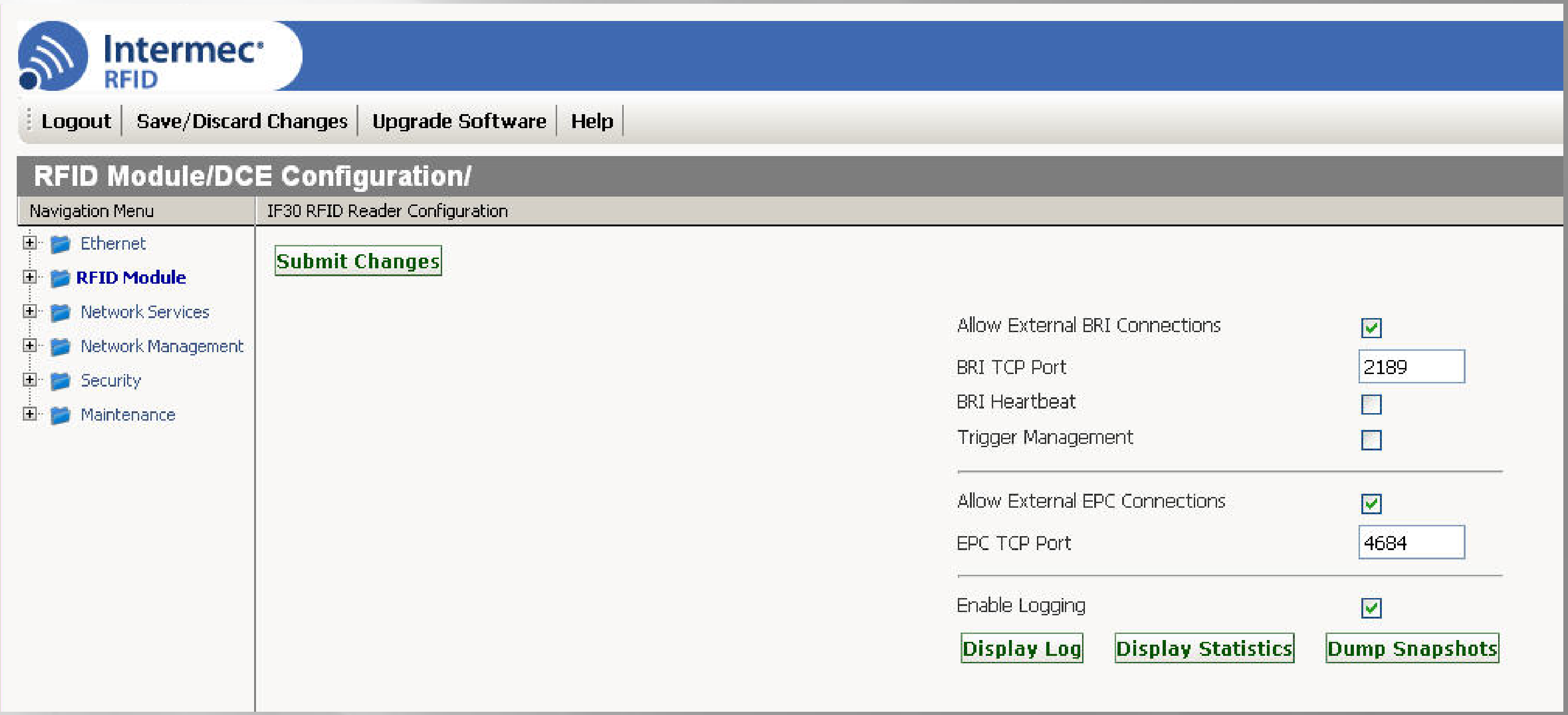
Initiate a UPS control action

Action: No Action

Signal PowerChute® server shutdown:

APC Smart-UPS 8000 XL web interface.

Logged in with default credentials from manual. Notice the ability to turn off the UPS, reboot it or put it to sleep.



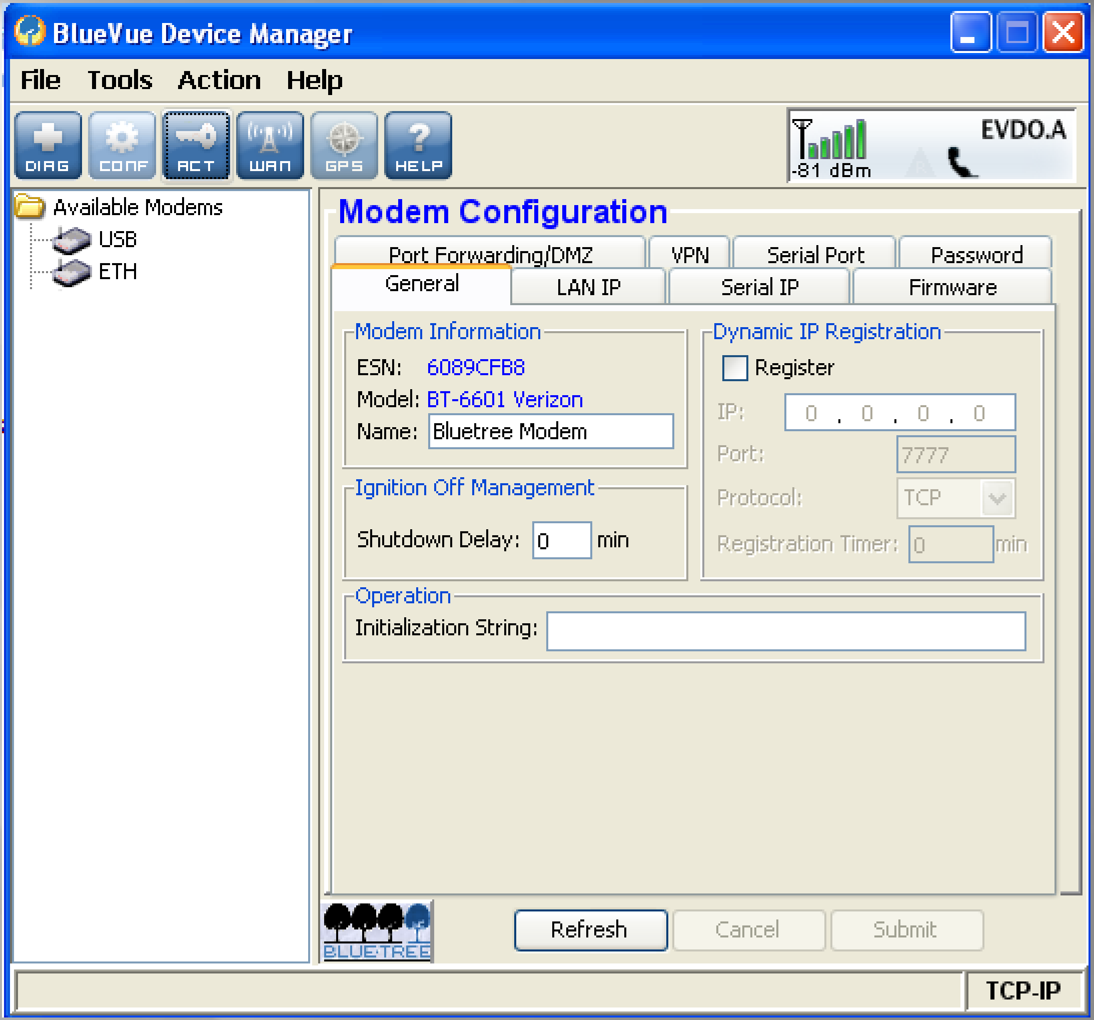
Allow External BRI Connections ☑
BRI TCP Port 2189
BRI Heartbeat □
Trigger Management □

Allow External EPC Connections ☑
EPC TCP Port 4684

Enable Logging ☑

Intermec RFID reader. Logged in with default credentials from manual.

BlueTree Modems. Often used as Remote Terminal Units (RTU) in SCADA applications.



Modem Information

ESN: 6089CFB8

Model: BT-6601 Verizon

Name: Bluetree Modem

Dynamic IP Registration

□ Register

IP: 0 . 0 . 0 . 0

Port: 7777

Protocol: TCP

Registration Timer: 0 min

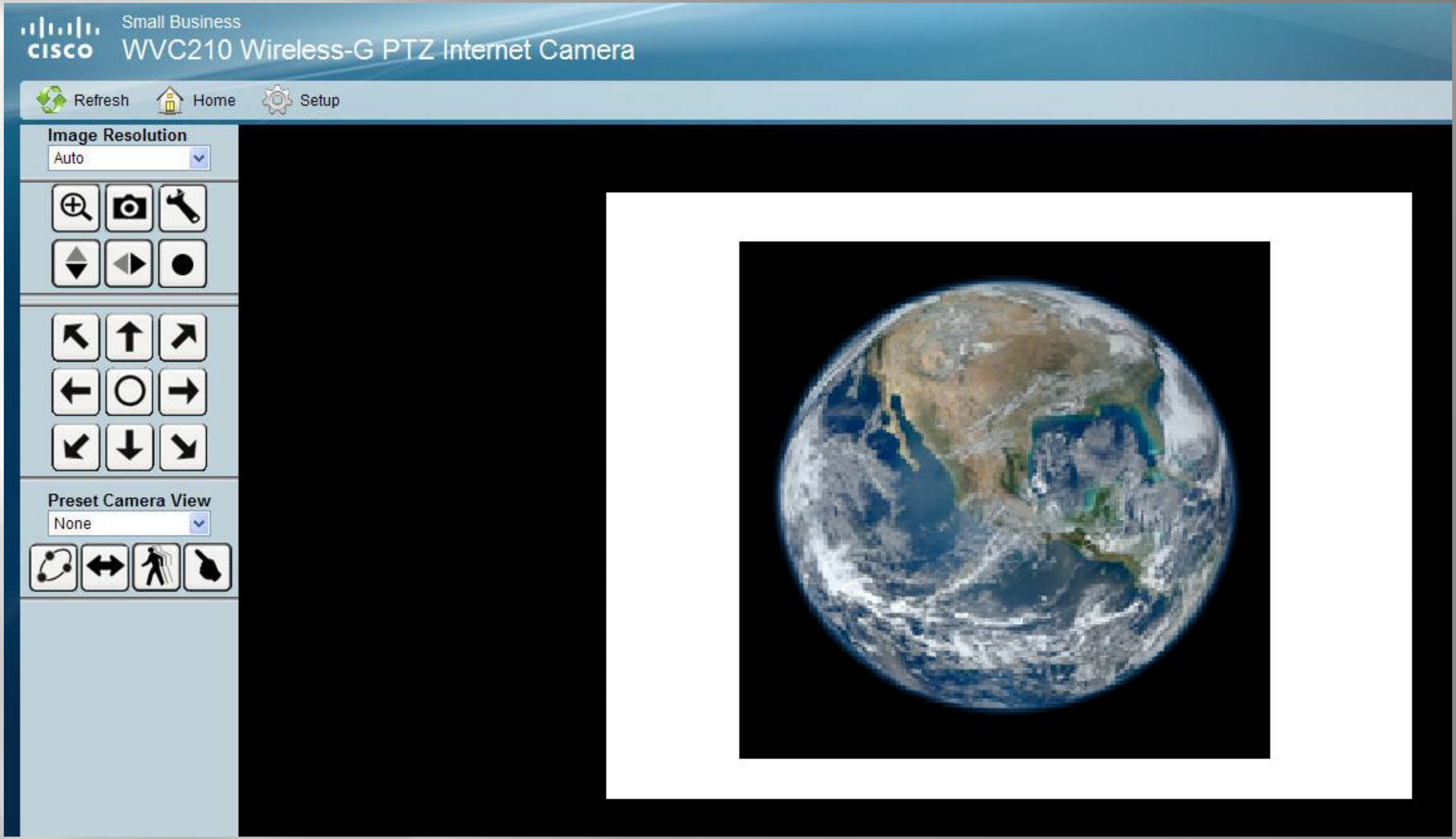
Ignition Off Management

Shutdown Delay: 0 min

Operation

Initialization String:

ISACA VA Chapter



Small Business

WVC210 Wireless-G PTZ Internet Camera

Image Resolution: Auto

Preset Camera View: None

Cisco Wireless camera. The Earth replaced the actual image of the room. No credentials required for access.

So How Do We Fix Things?

- Start by recognizing that ALL network devices can be used by an attacker.
  - If it has an IP address and some method of storage, it can probably be used by somebody to do something bad.

- Develop build lists for all devices, not just servers and desktops.
  - Turn off unused access methods such as HTTP, HTTPS, Telnet, FTP, SNMP.
  - Be careful with TCP port 9100! Where possible, control this port with a firewall.

ISACA VA Chapter

- Ensure that all default login credentials are changed BEFORE connecting the device.
  - Never leave a device connected to your network with blank passwords.
  - Remember, it only takes the bad guys a few minutes to download the manual from the Internet.

- Routinely test all infrastructure devices for compliance with all applicable policies.
  - Do this on a quarterly basis to catch the low-hanging fruit.

ISACA VA Chapter

- Include the Facilities Management/Physical Security groups in the overall security and systems management process.

- Help these non-IT groups develop build lists for devices that connect to the corporate networks.

- Offer to include their devices in the network scans and penetration tests.

Summary

- The issues discussed in this presentation are real and they're not going away.
- They don't get a lot of attention but they create opportunities for massive data breaches.
- More research into applicable controls is needed to help reduce the risk.
- We need to push vendors to build in more security controls and disable "features" by default.

Q&A