Managing Elevated Privileges in the Enterprise Environment

Erik Burgess
@erikburgess_

whois

- Industry Veteran
- Many Roles During Career (Help Desk, Servers, Management, Security)
- Experience In Military, Government, Private Sectors
- Lazy Admin a.k.a. Doing More With Less
- Tinkerer, photographer, security enthusiast
- Contact: @erikburgess_

Why THIS talk?

- Too many conversations with peers about this issue
  - People keep ignoring the issue
- Too many end users operating as admin
- Corporate culture needs to change
- Compliancy requirements
- Commercial solutions overly expensive

Least Privileges

- The principle of least privilege translates to giving people the lowest level of user rights that they can have and still do their jobs. (NIST)
- Elevated Privileges is Privilege Escalation, but….
  - Elevated Privileges most often equals Admin Rights
- What about Power User?


SAY LEAST PRIVILEGES
ONE MORE TIME!
memegenerator.net

Possible End User Damages

- Virus/Malware
- Broken Systems
- File Deletion
- Unwanted Applications
  - From undesirable locations
- Potentially More Work for SA's / Higher Costs

Getting Started

- Management Approval / Sell to Users
- Identify Trouble Users/Applications
  - Surveys, Testing, Tickets
- Implement EP Workflow
  - Approve / Track / Verify
  - Include Rules and Responsibilities
- Pilot Test / Audit Mode
- Implement at Low Hanging Fruit (Secretaries, Tech/Report Writers, Desktop Users, etc)
- Identified End Users Complete Workflow
- Remove Existing EP from Unapproved Users
- End User Training

End User Challenges

- Believe Machine is Their Personal Machine
- They Are Too Important and/or Busy
- Will Run And Hide At The Sight Of An SA
- Learn What Works And They **All** Use It
- Some Do Not Abide By Rules And Regulations
- Vindictive End Users
- Never-ending Battle


RESISTANCE IS FUTILE
memegenerator.net

Possible Solutions

- Third-Party Commercial Solutions
- Grant EP On Demand / 24 Hour EP
- Open-Source Tools
- Secondary Local or Domain Admin Account
- Windows UAC (User Account Control)
- Roll Your Own

Limiting Access

- Sudo / WinSudo
- Install Applications in User Space
- Directory / Registry Permissions
- Ability to Manipulate Services
- Authorization Database (OSX)

Possible Scenarios

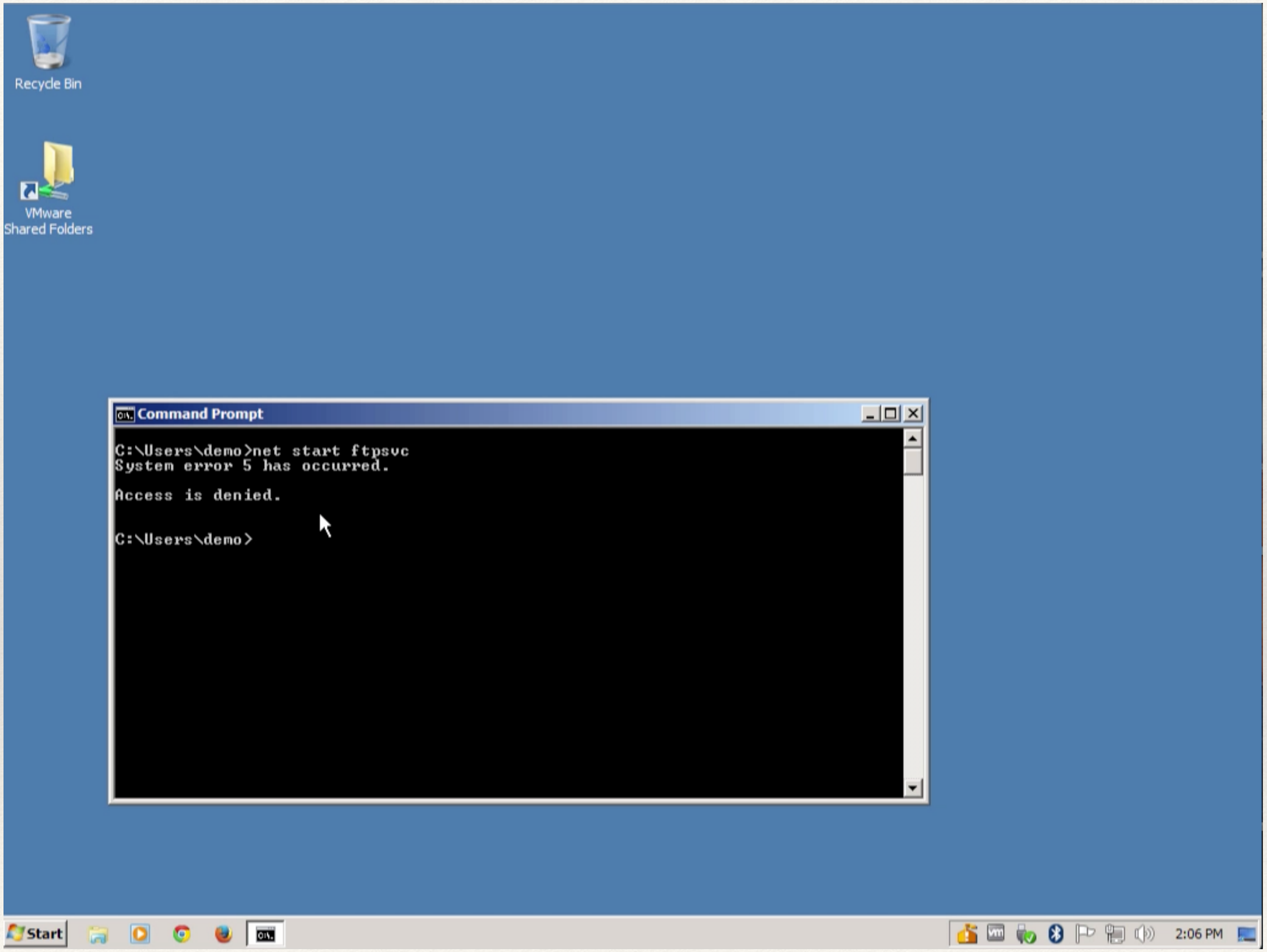
- Service Control
- Specific Application Elevation Requirements
- Registry Access Requirements
- Designing Device Drivers
- Interacting with the Kernel
- SCADA Systems
- Specific Hardware Components (FPGA, Custom Boards)

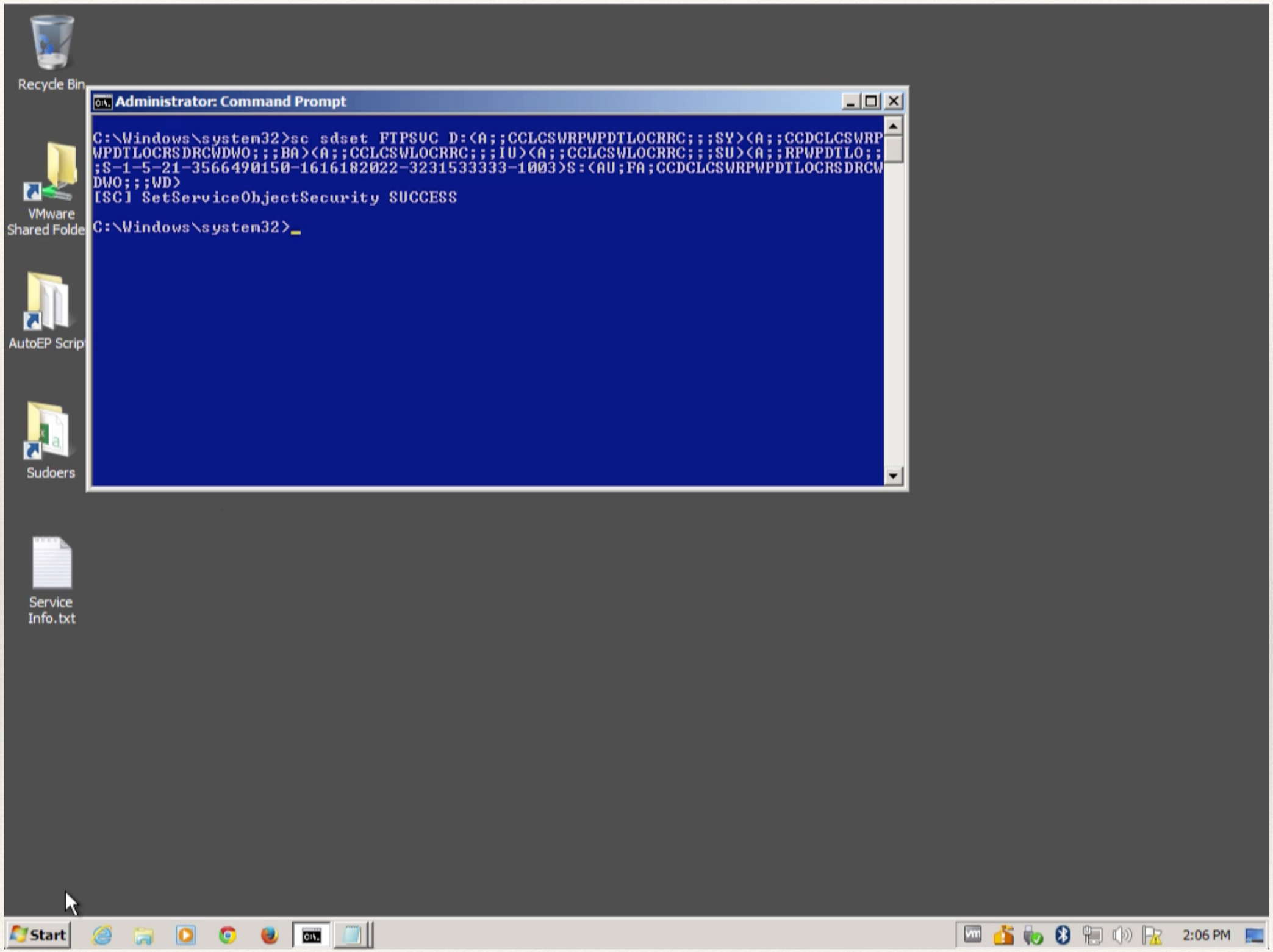
Editing Service Permissions

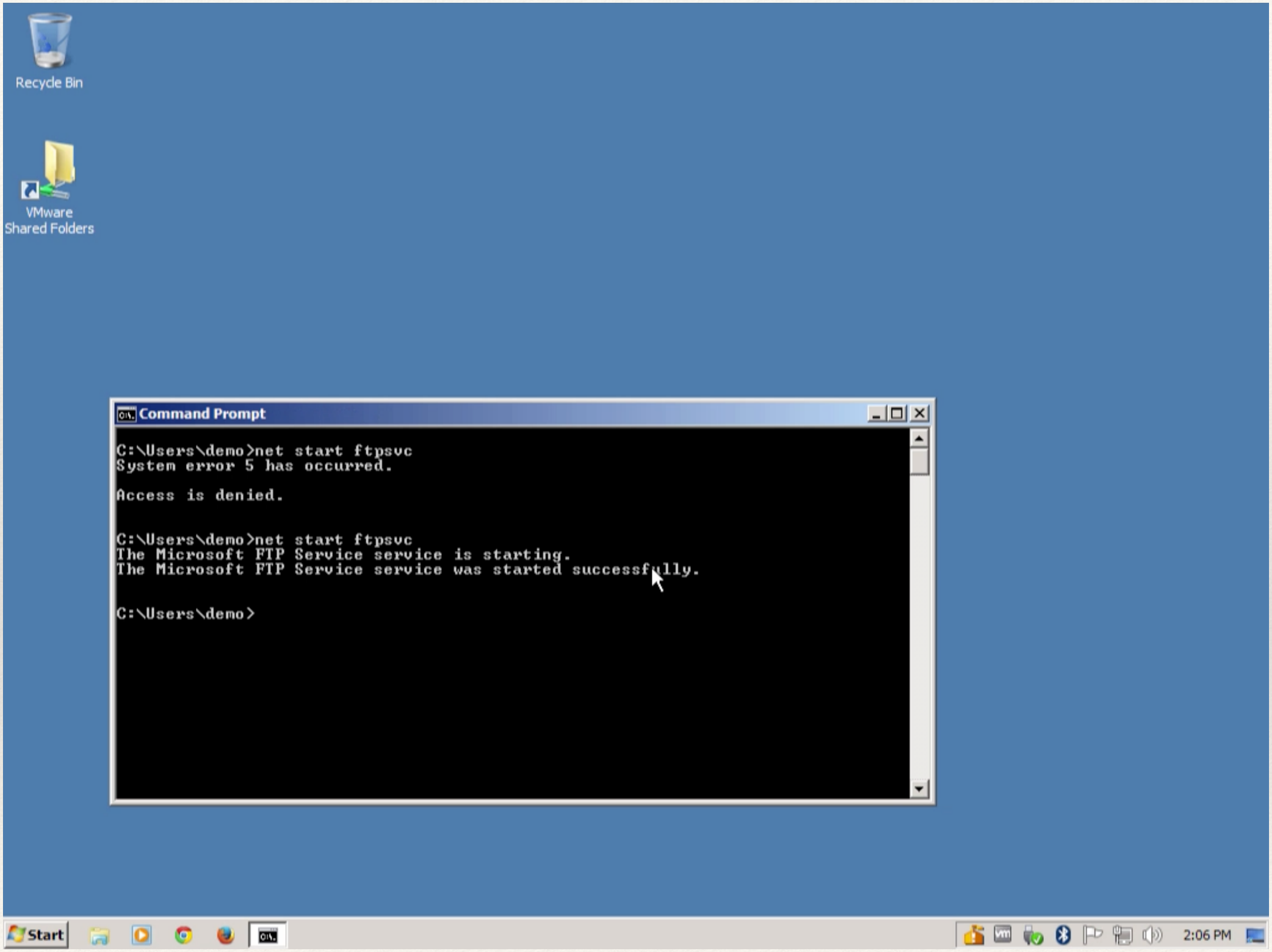
- sc query
- sc sdshow
- whoami /user
- sc sdset

C:\> sc sdshow FTPSVC

C:\> sc sdset FTPSVC D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)
(A;;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;BA)
(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)
(A;;RPWPDTLO;;;S-1-5-21-3566490150-1616182022-3231533333-1003)S:
(AU;FA;CCDCLCSWRPWPDTLOCRSDRCWDWO;;;WD)


Recycle Bin
VMware
Shared Folders
Command Prompt
C:\Users\demo>net start ftpsvc
System error 5 has occurred.
Access is denied.
C:\Users\demo>
Start
2:06 PM


Recycle Bin
VMware Shared Folde
AutoEP Scrip
Sudoers
Service Info.txt
Administrator: Command Prompt
C:\Windows\system32>sc sdset FTPSVC D:(A;;CCLCSWRPWPDTLOCRRC;;;SY)(A;;CCDCLCSWRP
WPDTLOCRSDRCWDWO;;;BA)(A;;CCLCSWLOCRRC;;;IU)(A;;CCLCSWLOCRRC;;;SU)(A;;RPWPDTLO;;
;S-1-5-21-3566490150-1616182022-3231533333-1003)S:(AU;FA;CCDCLCSWRPWPDTLOCRSDRCW
DWO;;;WD)
[SC] SetServiceObjectSecurity SUCCESS
C:\Windows\system32>
Start
2:06 PM


Recycle Bin
VMware
Shared Folders
Command Prompt
C:\Users\demo>net start ftpsvc
System error 5 has occurred.
Access is denied.
C:\Users\demo>net start ftpsvc
The Microsoft FTP Service service is starting.
The Microsoft FTP Service service was started successfully.
C:\Users\demo>
Start
2:06 PM

Typical Application Scenario

- End User states that application X isn't working.
- Work is critical/time sensitive.
  - Gets Management involved.
- EP often granted system-wide for a single application.
- End User never has time for admin to troubleshoot.

Windows Custom Solution

- Tracking/Management Workflow (Auto Provisioned)
- WinSudo
- Patching Agent
- Scripting
- Logging

Workflow / Tracking

Systems EP is needed on

* System Name

System ECN

* When is EP no longer needed? (Date Picker BROKEN)

07/04/2015

* System Operating System

Select

* Justification for EP

* Select the corresponding System Security Plan the user is requesting Elevated Privileges on. Most systems will fall under the AETD Laboratory Systems

Select

+ Add

*

I have read and agree to the User Acknowledgement Statement

Windows Scripting Solution

- Leveraged Patching Agent
  - AutoEP Scripts Run Every ~2 Hours
- Consists of a PowerShell script and three text files
  - Global Admins, Ignored Accounts, EP Users
- Can Use Either AD Groups or Users

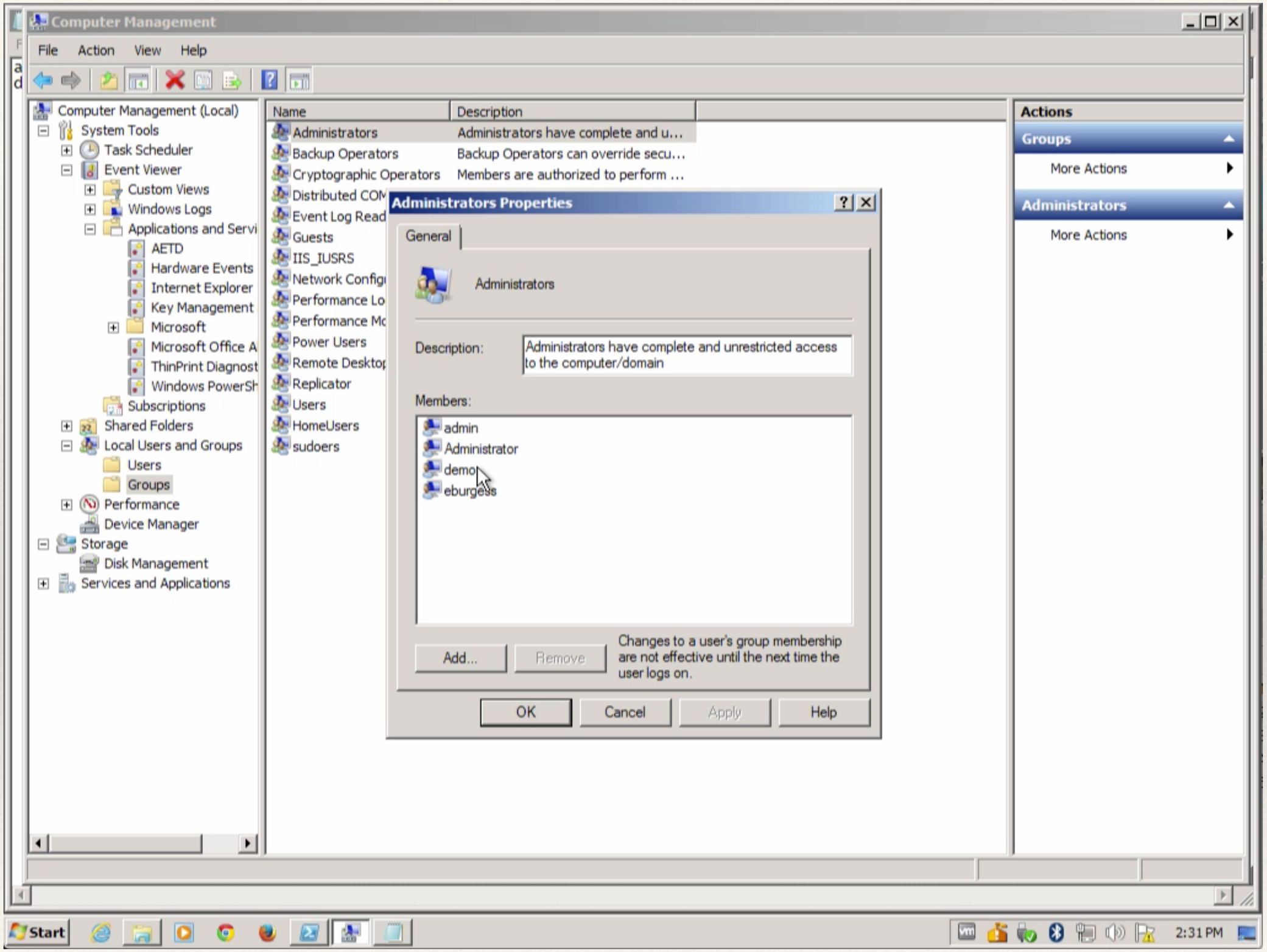
Windows Script File Format

- Two .txt Files and a .csv

#Erik's VMs
domain\eburgess,Windows7VM
domain\eburgess,Windows8VM

#computername, username, expiration date
windows7vm,domain\eburgess,02/09/2013*
windows8vm,domain\eburgess

* Expiration Date Ignored


Computer Management
File Action View Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Custom Views
Windows Logs
Applications and Servi
AETD
Hardware Events
Internet Explorer
Key Management
Microsoft
Microsoft Office A
ThinPrint Diagnost
Windows PowerSh
Subscriptions
Shared Folders
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Name
Description
Administrators
Administrators have complete and u...
Backup Operators
Backup Operators can override secu...
Cryptographic Operators
Members are authorized to perform ...
Distributed COM
Event Log Read
Guests
IIS_IUSRS
Network Config
Performance Lo
Performance Mo
Power Users
Remote Desktop
Replicator
Users
HomeUsers
sudoers
Administrators Properties
General
Administrators
Description:
Administrators have complete and unrestricted access to the computer/domain
Members:
admin
Administrator
demo
eburgess
Add...
Remove
Changes to a user's group membership are not effective until the next time the user logs on.
OK
Cancel
Apply
Help
Actions
Groups
More Actions
Administrators
More Actions
Start
2:31 PM

Computer Management

File Action View Help

Computer Management (Local)
- System Tools
  - Task Scheduler
  - Event Viewer
    - Custom Views
    - Windows Logs
    - Applications and Servi
      - AETD
      - Hardware Events
      - Internet Explorer
      - Key Management
      - Microsoft
      - Microsoft Office A
      - ThinPrint Diagnost
      - Windows PowerSh
    - Subscriptions
  - Shared Folders
  - Local Users and Groups
    - Users
    - Groups
  - Performance
  - Device Manager
- Storage
  - Disk Management
- Services and Applications

Name	Description
Administrators	Administrators have complete and u…
Backup Operators	Backup Operators can override secu…
Cryptographic Operators	Members are authorized to perform …
Distributed COM	
Event Log Read	
Guests	
IIS_IUSRS	
Network Config	
Performance Lo	
Performance Mo	
Power Users	
Remote Desktop	
Replicator	
Users	
HomeUsers	
sudoers	

Actions
- Groups
  - More Actions
- Administrators
  - More Actions

Administrators Properties

General

Administrators

Description: Administrators have complete and unrestricted access to the computer/domain

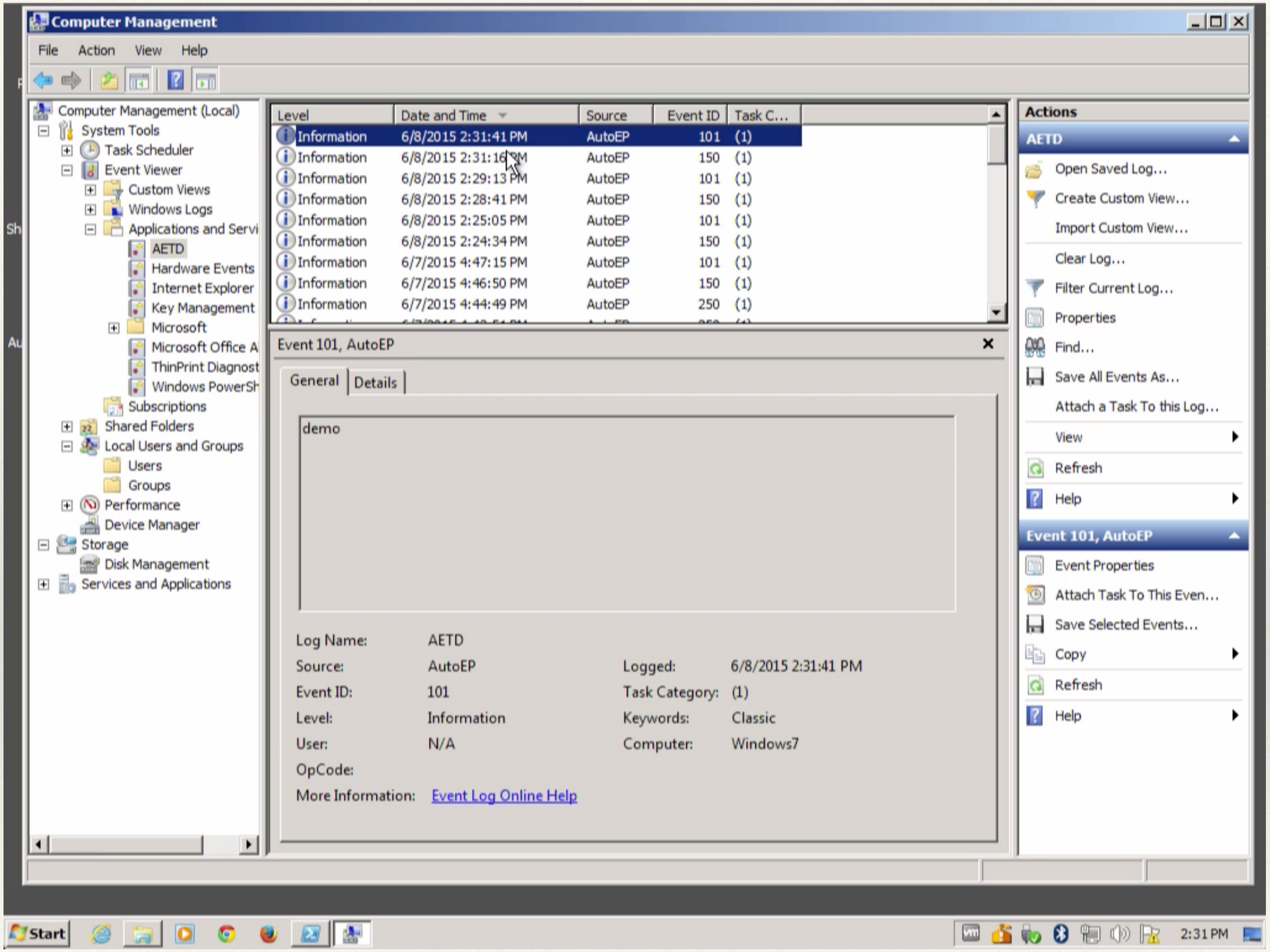
Members:
- admin
- Administrator
- eburgess

Add... Remove

Changes to a user's group membership are not effective until the next time the user logs on.

OK Cancel Apply Help

Start 2:31 PM


Computer Management
File Action View Help
Computer Management (Local)
System Tools
Task Scheduler
Event Viewer
Custom Views
Windows Logs
Applications and Servi
AETD
Hardware Events
Internet Explorer
Key Management
Microsoft
Microsoft Office A
ThinPrint Diagnost
Windows PowerSh
Subscriptions
Shared Folders
Local Users and Groups
Users
Groups
Performance
Device Manager
Storage
Disk Management
Services and Applications
Level Date and Time Source Event ID Task C...
Information 6/8/2015 2:31:41 PM AutoEP 101 (1)
Information 6/8/2015 2:31:16 PM AutoEP 150 (1)
Information 6/8/2015 2:29:13 PM AutoEP 101 (1)
Information 6/8/2015 2:28:41 PM AutoEP 150 (1)
Information 6/8/2015 2:25:05 PM AutoEP 101 (1)
Information 6/8/2015 2:24:34 PM AutoEP 150 (1)
Information 6/7/2015 4:47:15 PM AutoEP 101 (1)
Information 6/7/2015 4:46:50 PM AutoEP 150 (1)
Information 6/7/2015 4:44:49 PM AutoEP 250 (1)
Event 101, AutoEP
General Details
demo
Log Name: AETD
Source: AutoEP
Logged: 6/8/2015 2:31:41 PM
Event ID: 101
Task Category: (1)
Level: Information
Keywords: Classic
User: N/A
Computer: Windows7
OpCode:
More Information: Event Log Online Help
Actions
AETD
Open Saved Log...
Create Custom View...
Import Custom View...
Clear Log...
Filter Current Log...
Properties
Find...
Save All Events As...
Attach a Task To this Log...
View
Refresh
Help
Event 101, AutoEP
Event Properties
Attach Task To This Even...
Save Selected Events...
Copy
Refresh
Help
Start
2:31 PM

(Win)Sudo Solution

- Custom Build
- Good for Granting EP to a Single Application
- Can Validate File Checksums
- Automatically Updates System Config ~24 Hours
- User Can Manually Update

C:\inetpub\wwwroot.secure\aetd\sudoers.csv - Notepad++

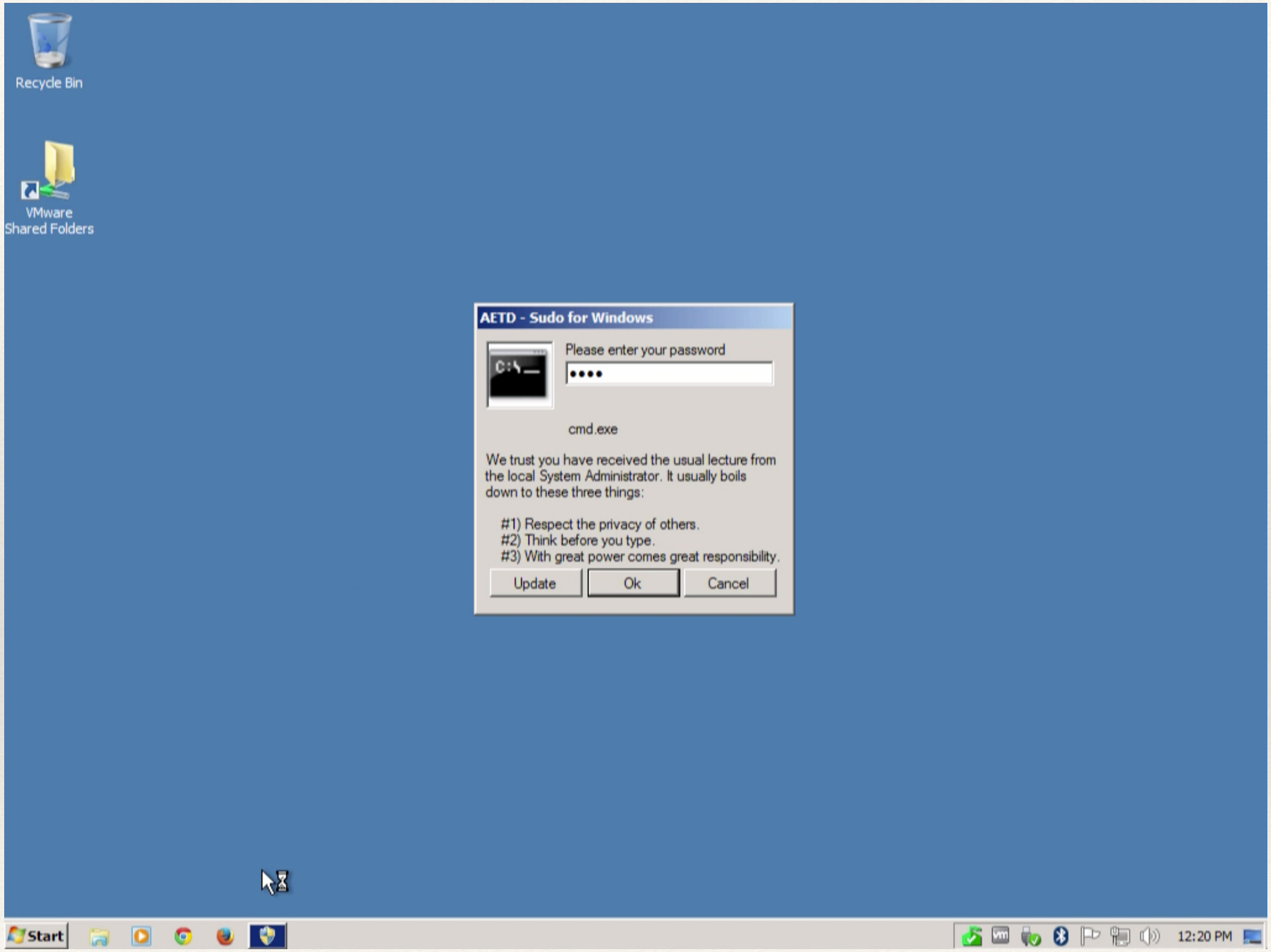
File Edit Search View Encoding Language Settings Macro Run Plugins Window ?

autoep.ps1 | Service Info.txt | sudoers.csv

```
1  system,username,path,checksum,arguments
2  windows7,windows7\eburgess,C:\Windows\notepad.exe,,
3  windows7,windows7\eburgess,C:\Windows\system32\cmd.exe,,
4  windows7,windows7\admin,C:\Windows\system32\cmd.exe,,
5  windows7,windows7\demo,C:\Windows\system32\cmd.exe,,
```

Normal text file | length : 259 lines : 5 | Ln : 5 Col : 23 Sel : 0 | 0 | Dos\Windows | UTF-8 w/o BOM | INS

Start 12:19 PM


Recycle Bin
VMware
Shared Folders
AETD - Sudo for Windows
Please enter your password
cmd.exe
We trust you have received the usual lecture from the local System Administrator. It usually boils down to these three things:
#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.
Update
Ok
Cancel
Start
12:20 PM

Linux / OSX Custom

- Sudo
- Patching Agent
- Scripting
- Authorization Database (Mac Only)
- Logging

OS X Authorization Database

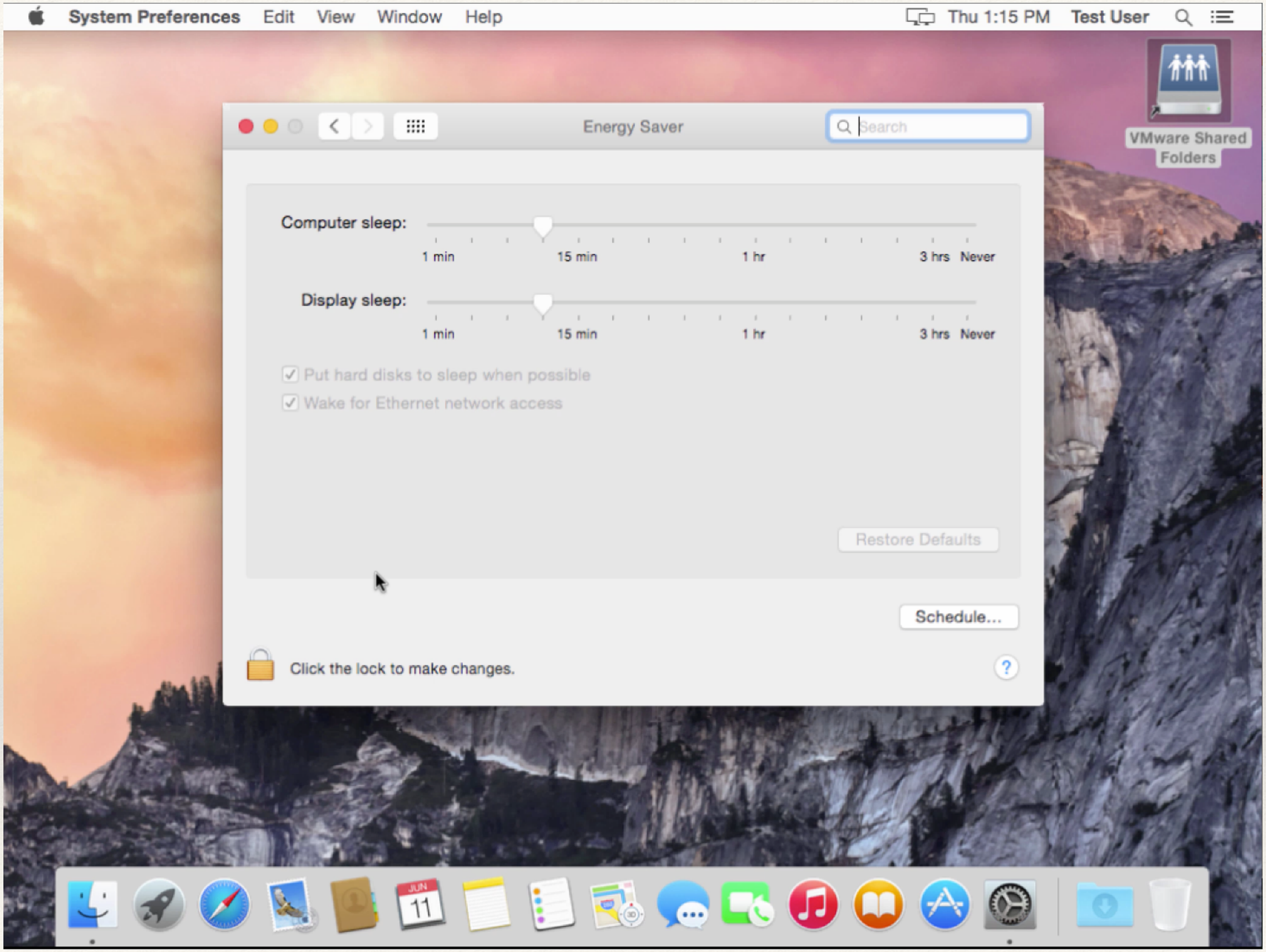
- Sqlite database that controls access rights to various commands.
- Energy, Network, Printers, App Store Updates, Time Zone, Time Machine, Xcode
- Can unlock many other things

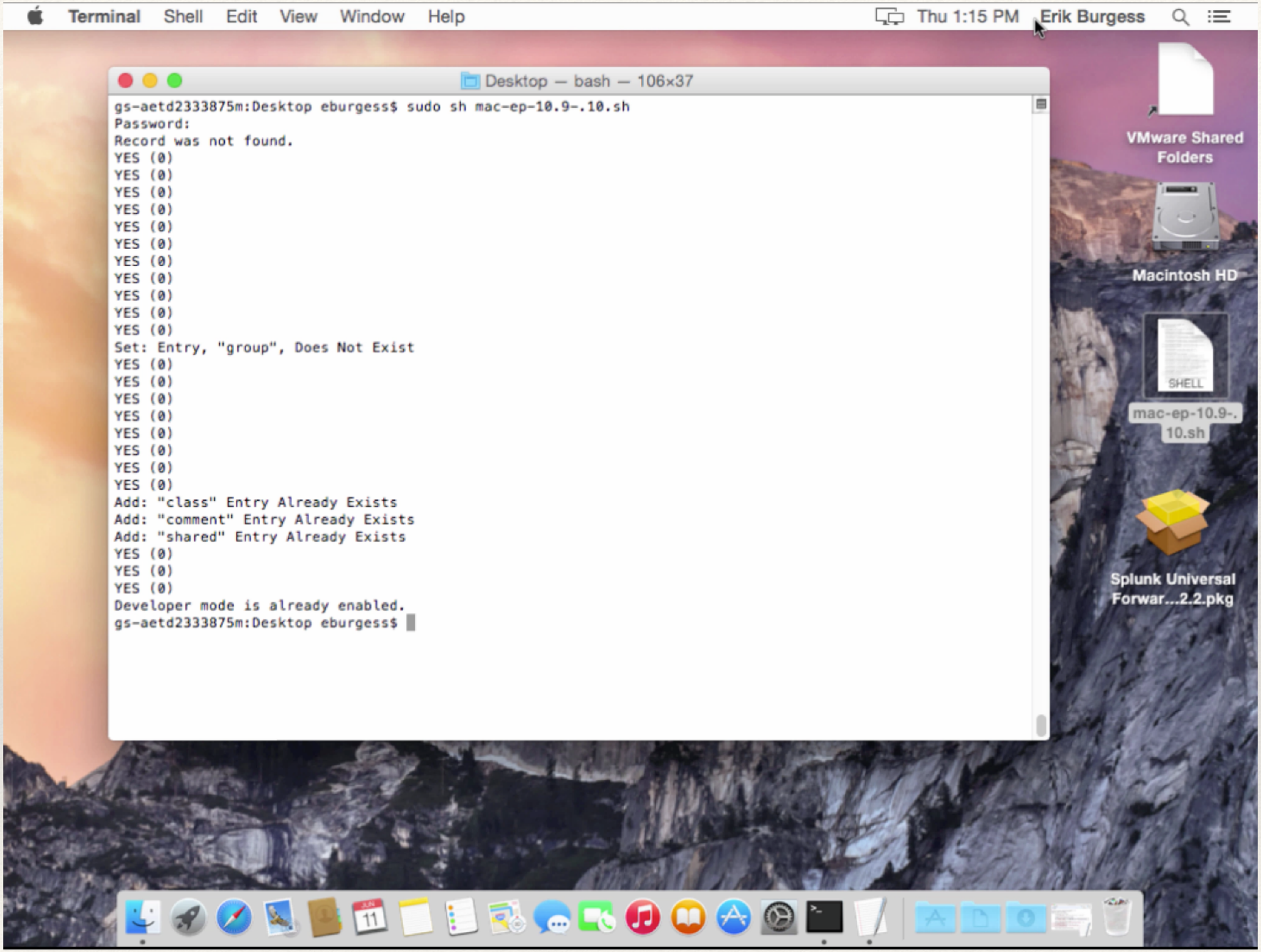
AuthDB Example

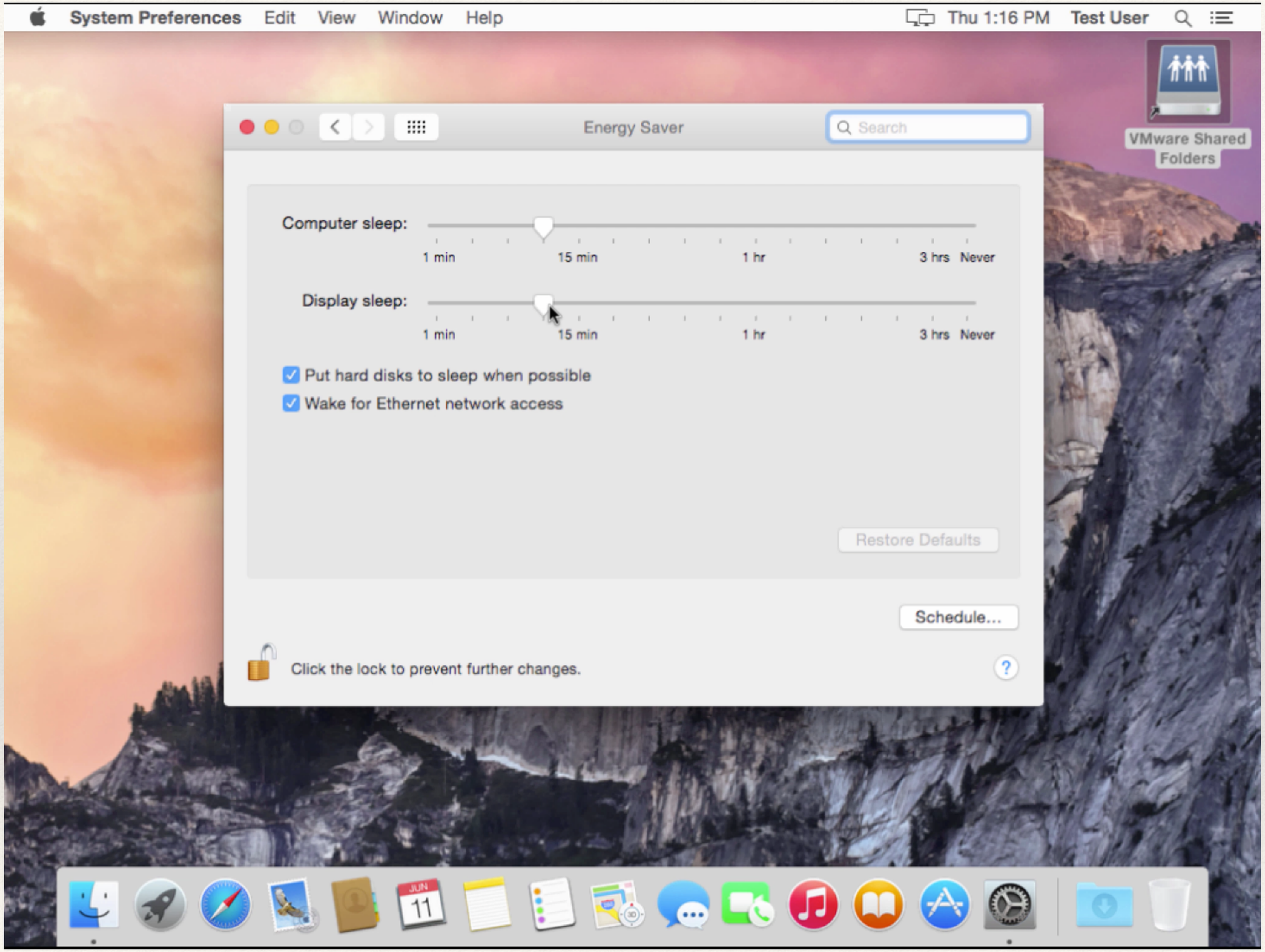
```
# Unlock Energy Saver preference pane.

security authorizationdb read system.preferences.energysaver > /tmp/system.preferences.energysaver.plist

/usr/libexec/PlistBuddy -c "set group staff"  /tmp/system.preferences.energysaver.plist
        security authorizationdb write system.preferences.energysaver < /tmp/
system.preferences.energysaver.plist
```

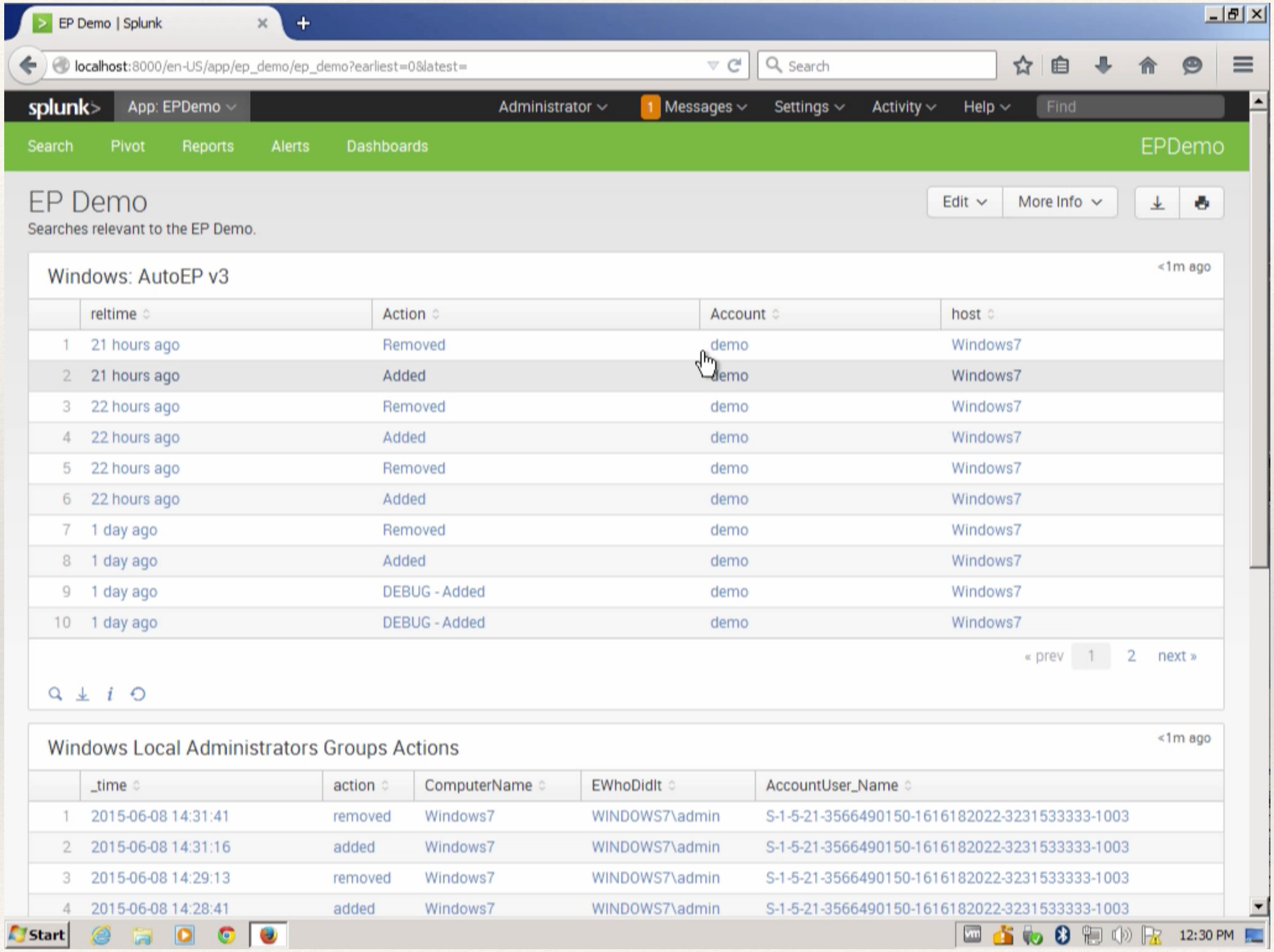

System Preferences
Edit
View
Window
Help
Thu 1:15 PM
Test User
VMware Shared Folders
Energy Saver
Search
Computer sleep:
1 min
15 min
1 hr
3 hrs
Never
Display sleep:
1 min
15 min
1 hr
3 hrs
Never
Put hard disks to sleep when possible
Wake for Ethernet network access
Restore Defaults
Schedule...
Click the lock to make changes.


Terminal Shell Edit View Window Help
Thu 1:15 PM Erik Burgess
Desktop — bash — 106×37
gs-aetd2333875m:Desktop eburgess$ sudo sh mac-ep-10.9-.10.sh
Password:
Record was not found.
YES (0)
YES (0)
YES (0)
YES (0)
YES (0)
YES (0)
YES (0)
YES (0)
YES (0)
YES (0)
YES (0)
Set: Entry, "group", Does Not Exist
YES (0)
YES (0)
YES (0)
YES (0)
YES (0)
YES (0)
YES (0)
YES (0)
Add: "class" Entry Already Exists
Add: "comment" Entry Already Exists
Add: "shared" Entry Already Exists
YES (0)
YES (0)
YES (0)
Developer mode is already enabled.
gs-aetd2333875m:Desktop eburgess$
VMware Shared Folders
Macintosh HD
SHELL
mac-ep-10.9-.10.sh
Splunk Universal Forwar...2.2.pkg


System Preferences
Edit
View
Window
Help
Thu 1:16 PM
Test User
VMware Shared Folders
Energy Saver
Search
Computer sleep:
1 min
15 min
1 hr
3 hrs
Never
Display sleep:
1 min
15 min
1 hr
3 hrs
Never
Put hard disks to sleep when possible
Wake for Ethernet network access
Restore Defaults
Schedule...
Click the lock to prevent further changes.
?

Monitoring and Tracking Elevation

- Log, log, log
- Visualize where possible
- Can track changes to Windows admin groups
- Can track Sudo attempts


EP Demo | Splunk
localhost:8000/en-US/app/ep_demo/ep_demo?earliest=0&latest=
Search
splunk>
App: EPDemo
Administrator
1 Messages
Settings
Activity
Help
Find
Search
Pivot
Reports
Alerts
Dashboards
EPDemo
EP Demo
Searches relevant to the EP Demo.
Edit
More Info
Windows: AutoEP v3
<1m ago
reltime
Action
Account
host
1 21 hours ago Removed demo Windows7
2 21 hours ago Added demo Windows7
3 22 hours ago Removed demo Windows7
4 22 hours ago Added demo Windows7
5 22 hours ago Removed demo Windows7
6 22 hours ago Added demo Windows7
7 1 day ago Removed demo Windows7
8 1 day ago Added demo Windows7
9 1 day ago DEBUG - Added demo Windows7
10 1 day ago DEBUG - Added demo Windows7
« prev 1 2 next »
Windows Local Administrators Groups Actions
<1m ago
_time
action
ComputerName
EWhoDidIt
AccountUser_Name
1 2015-06-08 14:31:41 removed Windows7 WINDOWS7\admin S-1-5-21-3566490150-1616182022-3231533333-1003
2 2015-06-08 14:31:16 added Windows7 WINDOWS7\admin S-1-5-21-3566490150-1616182022-3231533333-1003
3 2015-06-08 14:29:13 removed Windows7 WINDOWS7\admin S-1-5-21-3566490150-1616182022-3231533333-1003
4 2015-06-08 14:28:41 added Windows7 WINDOWS7\admin S-1-5-21-3566490150-1616182022-3231533333-1003
Start
12:30 PM

EP Demo | Splunk

localhost:8000/en-US/app/ep_demo/ep_demo?earliest=0&latest=

Search

« prev 1 2 next »

Windows Local Administrators Groups Actions

<1m ago

	_time	action	ComputerName	EWhoDidIt	AccountUser_Name
1	2015-06-08 14:31:41	removed	Windows7	WINDOWS7\admin	S-1-5-21-3566490150-1616182022-3231533333-1003
2	2015-06-08 14:31:16	added	Windows7	WINDOWS7\admin	S-1-5-21-3566490150-1616182022-3231533333-1003
3	2015-06-08 14:29:13	removed	Windows7	WINDOWS7\admin	S-1-5-21-3566490150-1616182022-3231533333-1003
4	2015-06-08 14:28:41	added	Windows7	WINDOWS7\admin	S-1-5-21-3566490150-1616182022-3231533333-1003
5	2015-06-08 14:25:05	removed	Windows7	WINDOWS7\admin	S-1-5-21-3566490150-1616182022-3231533333-1003
6	2015-06-08 14:24:34	added	Windows7	WINDOWS7\admin	S-1-5-21-3566490150-1616182022-3231533333-1003
7	2015-06-07 16:47:15	removed	Windows7	WINDOWS7\admin	S-1-5-21-3566490150-1616182022-3231533333-1003
8	2015-06-07 16:46:50	added	Windows7	WINDOWS7\admin	S-1-5-21-3566490150-1616182022-3231533333-1003
9	2015-06-07 16:35:20	removed	Windows7	WINDOWS7\admin	S-1-5-21-3566490150-1616182022-3231533333-1003
10	2015-06-07 16:34:21	added	Windows7	WINDOWS7\admin	S-1-5-21-3566490150-1616182022-3231533333-1003

« prev 1 2 3 next »

Windows Sudo Actions

<1m ago

	_time	host	who	result	command
1	2015-06-09 12:20:14	Windows7	WINDOWS7\demo	SudoK	C:\Windows\system32\cmd.exe
2	2015-06-09 12:17:22	Windows7	WINDOWS7\demo	SudoK	C:\Windows\system32\cmd.exe

Start 12:30 PM

Easing The Administrative Burden

- Automated Patching
- Centralized Software Installations
  - Self Install Portal / AD & GPOs / SCCM / WSUS (Windows)
  - Munki / Spacewalk / Satellite Server (OSX / Linux)
  - Updates & Approved Applications
- Other Solutions (BigFix / NiNite / PDQ Deploy / Etc)

Positive Effects

- Better Overall Security Posture
- Potentially Fewer Security Incidents
  - Helps Stop Malware, Limits Data Access When Compromised, Protects Data From Users
- Can Help With Data Classification
- Culture Can Spread

Negative Effects

- Major Culture Change
- Cranky End Users
- Potentially More Help Desk Tickets
- Security Team is EVIL

What Next?

- Application White/Black Listing
- Your Ideas?

EP Justifications

* **Justification for EP**

I currently have 2 computers (1 desktop, 1 laptop). I am replacing both systems with a new laptop. IT has taken the laptop but left me with the desktop until it is determined that nothing else is needed from that system. I will need EP on my new system ASAP so I can relinquish the old desktop.

EP Justifications

*** Justification for EP**

My wavefront sensing and control work involves extensive numerical and scientific computing work. The tools and software package required for this work generally require elevated privileges for installation, maintenance, and configuration. Because of the large number of tools, their specialized nature, and frequent need for updates and configuration requiring all EP operations to be done by the regular system administrator would be an unreasonable burden on their time. Software tools include parallel computing libraries (mpi4py), compilers (mingw and MSVC), various python distributions (including Anaconda and the official Python distribution), integrated development environments (PyCharm), as well as profilers and debuggers.

Q & A