

Group Policy

Erik Fredericks (fredericks@oakland.edu)

CSI3670 // Winter 2019

First, FTP

Roles & Services → IIS → FTP
(Reboot)

Tools → IIS Manager

- Expand your machine

- Right click on Sites → Add FTP site

- Make sure to put *your* IP address into the IP Address field

Update firewall

Most importantly...

- REBOOT (otherwise it is inaccessible)

Overview

What is GROUP POLICY!?!?!?

- Centrally manage Windows machines

 - Configuration

 - Software deployment

 - Restrictions

First released back in 2000

Previously had to manually edit registry/
system policies



Terms

Group policy

Infrastructure for creating and applying settings for configuring/controlling Windows computers

Group policy **processing**

Method for downloading and applying Group Policy settings to workstations

Group policy **object** (GPO)

Collection of settings applied to workstation: linking GPO to container

Terms

Group policy **setting**

Single setting in a GPO : applied in 'Policies' section of GPO

Group policy **preferences**

Simple approach for configuring GPO settings with dialog boxes

May be changed by users to override admin preferences

Preference item

Similar to group policy setting, but a preference

Setting vs Preference?

GP Setting

- Will not **tattoo**
- Supersede application setting
 - (Application aware)
- Recognized by application
 - (Grayed out)

GP Preference

- **Will** tattoo
- Overwrite application setting
- Not be recognized by application
 - (Changeable)

Tattoo?

GPO goes out of scope, preference remains in registry
(Otherwise it's removed)

What can we do with Group Policy?

Centrally control machines in our environment

- Disable Registry editing

- Disallow access to Control Panel

- Distribute software to workstations

Applies to containers

- What's a container?

- When GPO linked, applies all settings to container

 - Can change so that it only applies to specific users/computers in container



QUICK Q&A TIME GO GO GO

What would you setup? Each group come up with (2) items and we'll discuss in eggsactly:

<http://e.ggtimer.com/6%20minutes%2030%20seconds>

Common Uses (not all-inclusive)

Disabling guest account

Disable LM/NTLMv1 (use Kerberos/NTLMv2)

Minimum password length / time to expire / etc.

Enable event logging

Enable UAC

Disable anonymous access



Group Policy / Groups

GPOs do **not** apply to groups

Why not?

Groups don't login to computers

Users do

And policy settings are applied on logon...

But

Groups *can* control GPO application

So

GPO applied to containers (site/domain/organizational unit/etc.)

But GPO can be tweaked to be applied individually

Place all users in group

Tweak GPO to apply to group

Group Policy / Groups

Why is this helpful?

- Software distribution

- Automated installation of programs

Why not just a container?

- Assume you have a sub-group of people (10 users) within Accounting (60 users)

- Not enough licenses to cover more than 10

- Create GPO to deploy software and link GPO to Accounting container

- Create group : AccountingSoftware

 - Add 10 users to that group

- Modify permissions on GPO so that AccountingSoftware can **only** apply GPO

Group Policy Prerequisites

What do we need to run group policy?

- Active Directory

- Hopefully self-evident why...

- Must be able to access DCs on network

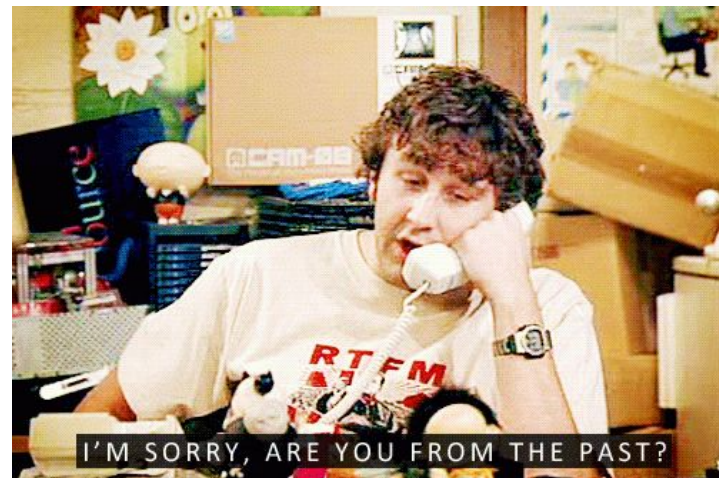
- Be members of domain

- DCs contain GPO copies (replication → synchronized automatically)

- Windows 2000 or later

- NT, 95, 98, ME do not support Group Policy application

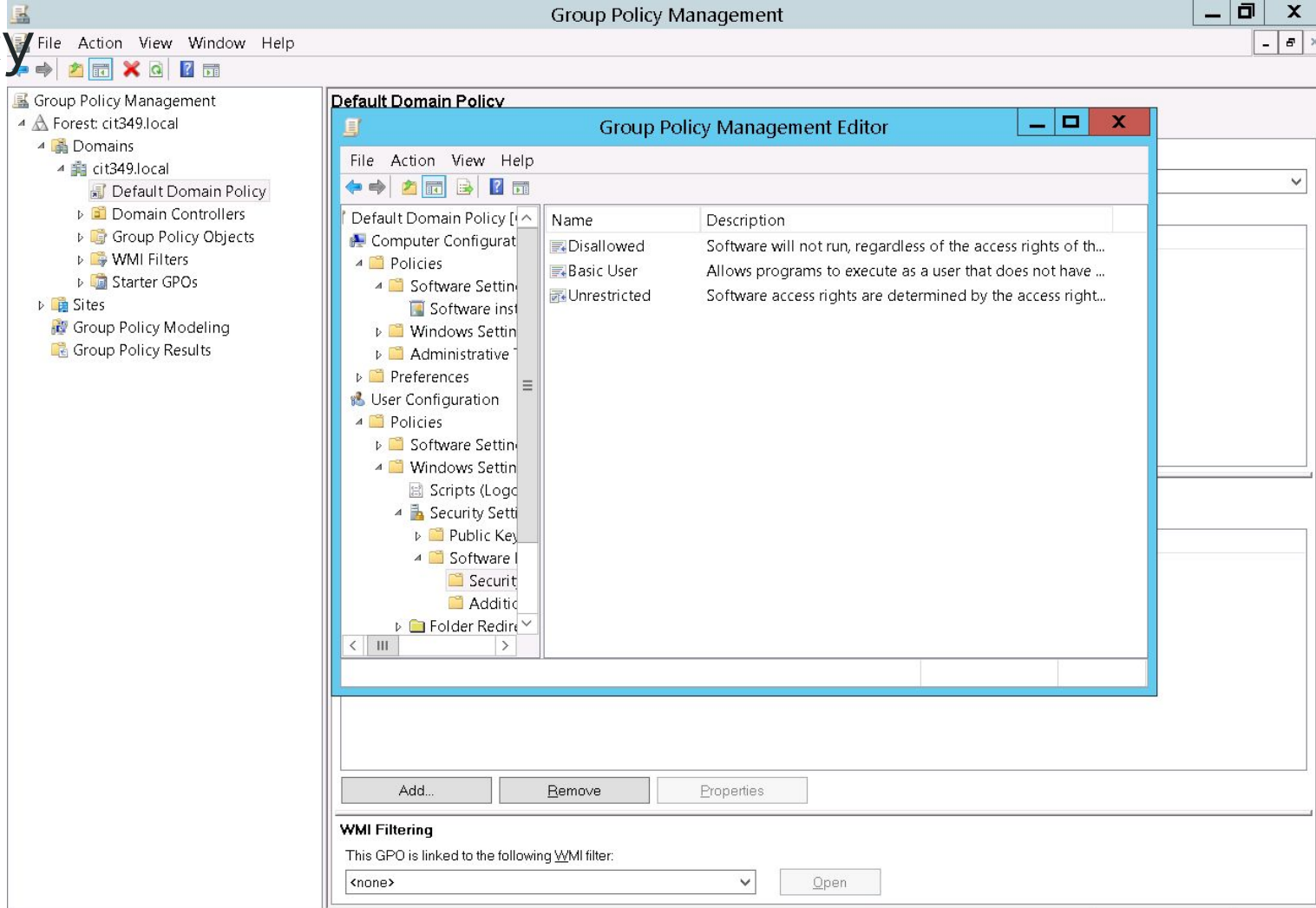
- Shouldn't be an issue unless if we're from the past



<https://www.youtube.com/watch?v=82BwEOeTbMA>

Group Policy Tools

Group Policy Management Console (GPMC)



Demo

- 1) Create new GPO
- 2) Edit GPO → Disable Control Panel
 - a) User Configuration → Admin. Templates → Control Panel → Prohibit Access → Edit
 - b) Make sure it is enforcing because otherwise this doesn't **work**
- 3) Delegate to user
 - a) Delegation → Advanced → Authenticated Users (untick Apply Group Policy)
 - b) Add user → tick Apply Group Policy

Then delete and run gpupdate /force

PowerShell

```
PS> Import-Module GroupPolicy
```

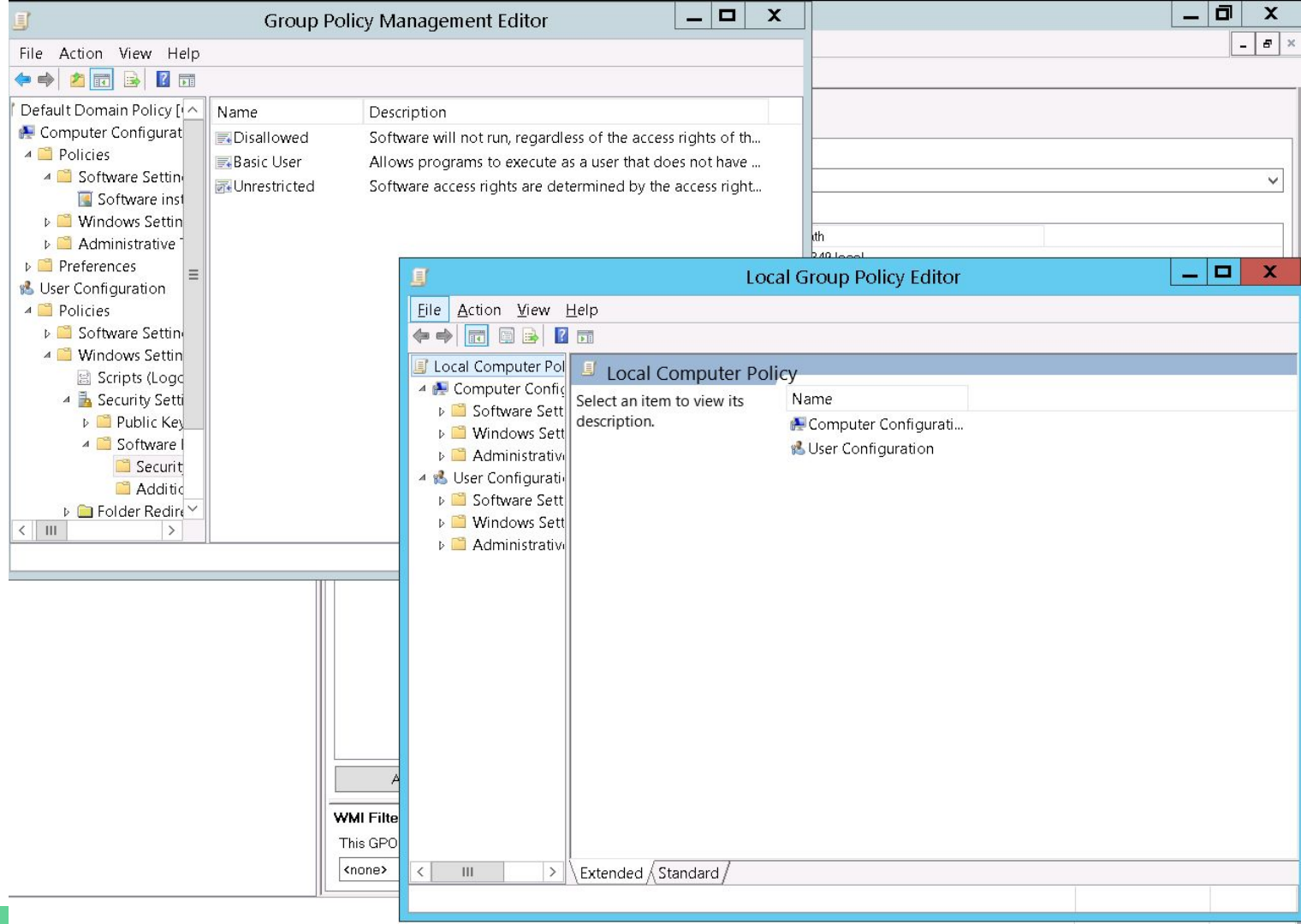
```
PS> Get-Command -Module GroupPolicy
```

gpedit.msc

Local group
policy editor

Direct access
to GP settings

Can configure
multiple
GPOs locally



Sections and Categories

Policy settings

User-inherited: applies to user across any login on any machine in domain

Example: SECS login

Computer-inherited: applied to any user logging into that computer

Called a **section (GPO nodes)**

Sections include **categories (child nodes):**

- Software settings

- Windows settings

- Administrative templates

Include further subcategories

Sections and Categories

Many settings exist in both User and Computer sections

E.g., deploy software

But, Administrative Templates are unique to section

Why?

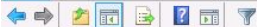
Admin. Templates apply to HKEY_LOCAL_MACHINE for computer

HKEY_LOCAL_USER for user

So it applies to different parts of the Registry

And therefore gets a different name

> 100 categories



CIT349-GPO [CIT349-MA...

All Settings

- Computer Configuration
 - Policies
 - Preferences
 - Windows Setting
 - Control Panel Se
- User Configuration
 - Policies
 - Software Setting
 - Windows Setting
 - Administrative T
 - Control Panel
 - Desktop
 - Network
 - Shared Folder
 - Start Menu an
 - System
 - Windows Con
 - All Settings
 - Preferences

Select an item to view its description.

Setting	State	Comment	Path
.Net Framework Configuration	Not configu...	No	\Windows Components\Mic
Ability to change properties of an all user remo...	Not configu...	No	\Network\Network Connecti
Ability to delete all user remote access connecti...	Not configu...	No	\Network\Network Connecti
Ability to Enable/Disable a LAN connection	Not configu...	No	\Network\Network Connecti
Ability to rename all user remote access connec...	Not configu...	No	\Network\Network Connecti
Ability to rename LAN connections	Not configu...	No	\Network\Network Connecti
Ability to rename LAN connections or remote a...	Not configu...	No	\Network\Network Connecti
Access data sources across domains	Not configu...	No	\Windows Components\Inte
Access data sources across domains	Not configu...	No	\Windows Components\Inte
Access data sources across domains	Not configu...	No	\Windows Components\Inte
Access data sources across domains	Not configu...	No	\Windows Components\Inte
Access data sources across domains	Not configu...	No	\Windows Components\Inte
Access data sources across domains	Not configu...	No	\Windows Components\Inte
Access data sources across domains	Not configu...	No	\Windows Components\Inte
Access data sources across domains	Not configu...	No	\Windows Components\Inte
Access data sources across domains	Not configu...	No	\Windows Components\Inte
Access data sources across domains	Not configu...	No	\Windows Components\Inte
Access data sources across domains	Not configu...	No	\Windows Components\Inte
Action on server disconnect	Not configu...	No	\Network\Offline Files
Active Directory Domains and Trusts	Not configu...	No	\Windows Components\Mic
Active Directory Sites and Services	Not configu...	No	\Windows Components\Mic
Active Directory Users and Computers	Not configu...	No	\Windows Components\Mic
ActiveX Control	Not configu...	No	\Windows Components\Mic
Add "Run in Separate Memory Space" check bo...	Not configu...	No	\Start Menu and Taskbar
Add a specific list of search providers to the use...	Not configu...	No	\Windows Components\Inte
Add default Accelerators	Not configu...	No	\Windows Components\Inte
Add Logoff to the Start Menu	Not configu...	No	\Start Menu and Taskbar
Add non-default Accelerators	Not configu...	No	\Windows Components\Inte
Add Search Internet link to Start Menu	Not configu...	No	\Start Menu and Taskbar
Add the Run command to the Start Menu	Not configu...	No	\Start Menu and Taskbar

Handling Windows Versions

What do we do if we have, god forbid, non-homogenous Windows systems?



Handling Windows Versions

Issues:

- Older versions don't support as many Group Policy settings

 - Keep in mind a client can be a normal workstation or a server

- Require a **management machine**

 - Running newest version of Windows

 - Be able to create GPOs for all versions up to management machine's level

- Management machine needs RSAT (Remote Server Administration Tools)

 - Assuming you don't already have GPMC from AD


Processing Order

You can apply multiple GPOs to an object

Default processing order

1. Local Group Policy
2. Site GPOs
3. Domain GPOs
4. OU GPOs (in order of hierarchy)

Example



GPO	Policy Setting / GPO	Linked Target / Container
Local policy setting	Prevent access to Registry editing tools	Local machine
Site	Site A GPO	Site A
Domain	Default domain policy GPO	Domain
OU	Marketing GPO	Marketing OU
OU	Marketing Management GPO	Management child OU under Marketing OU

Table 8.1 : Windows Server Administration Essentials

Processing Order

Hierarchical and cumulative

But, can change default behavior

1. Can configure GPO to be **enforced**
 - a. Lower-level GPOs cannot override higher-level GPOs if a conflict occurs
2. Configure container to **block inheritance**
 - a. Container will not allow any GPOs to be applied above it in hierarchy

Processing Order

What happens if:

- (1) a low-level container is configured to block inheritance
- (2) but the higher-level container is set to enforced?

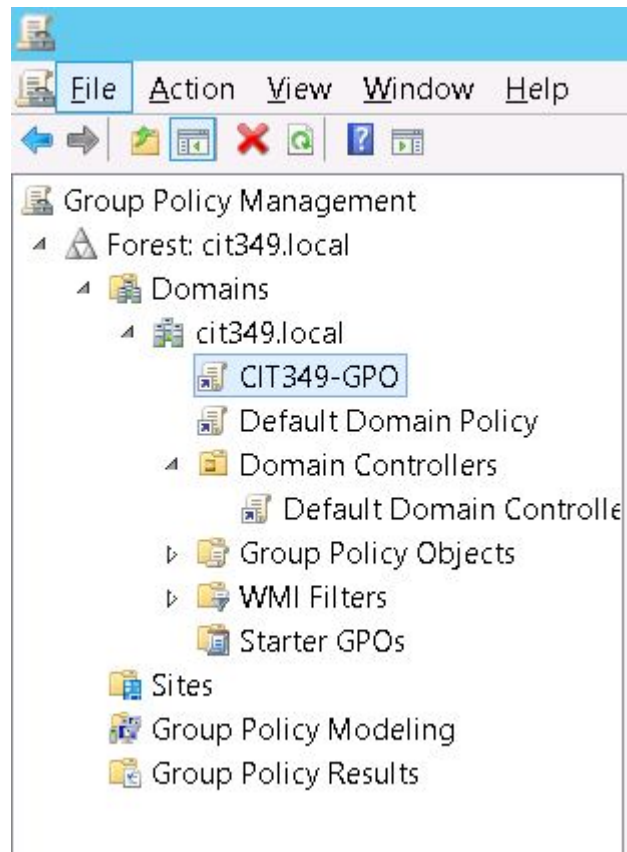
Enforced takes precedence

Higher-level GPO applied

Why?!?!?

- Assumed that higher-level enforcement has been done by a more powerful sysadmin

Nodes



Nodes in Console Tree

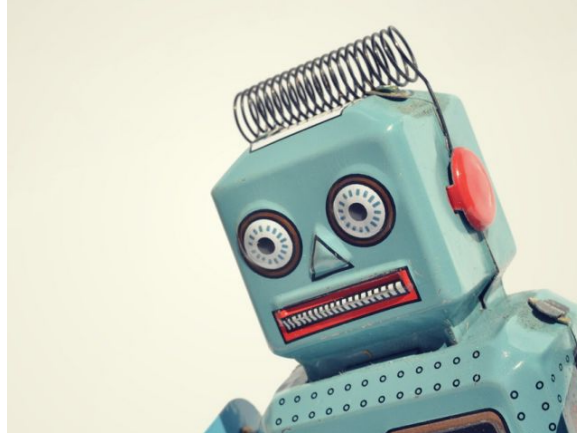
Forest	: Root node for the forest
Domain	: Child of forest → contains all domains
Domain Name	: Container for all GP related to domain
Domain Controller	: Contains references to all GPOs that apply to DC OU
OU Name	: Represent OU in AD → references all GPOs linked to OU
Group Policy Object	: Container of all GPOs in domain
WMI Filter	: Filters based on Windows Management Instrumentation
Starter GPO	: Node for sample GPO templates
Site	: Forest child → contains all configured sites
Group Policy Modeling	: Simulate GPO processing
Group Policy Results	: Reports results

Create a GPO → Determine Policy Settings

- GPO for policy settings that must be enforced for all users to domain
 - Link to domain
 - Designate as enforced so nothing else can override it
- GPO for policy settings that must be enforced for all members of OU
 - Same as above
- Use as few GPOs as possible
 - Without sacrificing your needs
 - Combine GPOs to improve processing and reduce network bandwidth
- Can use groups as necessary
- Create a test environment to try them out first

Create a GPO → Create a GPO

- Login as Administrator (hopefully obvious by this point)
- Group Policy Management
 - Expand forest / domain
 - Right click on Group Policy Objects → New
 - Name it NoReg
 - Right click on NoReg and Edit
 - User Configuration → Policies → Administrative Templates → System
 - Double click on Prevent Access to Registry and Enable



Create a GPO → Linking to Container

GPO is an **independent object**

- Right click on container of choice and Link

GPO -- CSI3670

Group Policy Management Editor

File Action View Help

← → ↗ ✕ ↶ ? ↷

CSI3670 [CSI3670-DC1.CSI3670.LOCAL] Policy

- Computer Configuration
 - Policies
 - Software Settings
 - Windows Settings
 - Name Resolution Policy
 - Scripts (Startup/Shutdown)
 - Security Settings
 - Account Policies
 - Password Policy
 - Account Lockout Policy

Policy	Policy Setting
Enforce password history	Not Defined
Maximum password age	Not Defined
Minimum password age	Not Defined
Minimum password length	Not Defined
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Not Defined

GP/PS Commands

1) Info

```
Get-Gpo <name>
```

```
Get-Gpo -all
```

2) Backup/Restore

```
Backup-Gpo -Name <name> -Path C:\gpo-backups -Comment "March18  
backup"
```

```
Restore-Gpo -Name <name> -Path <path>
```


GP/PS Commands

3) Produce reports

```
Get-GPResultantSetofPolicy -user domain\user -reporttype html  
-path <path>.html
```

gupdate /force and /sync

gpupdate: downloads a group policy from AD to the machine
(runs from PS)

Interesting flags

/force: applies **every policy** (regardless if new or old)

/sync: waits for network connectivity to download GP

/boot: restart after GP applied

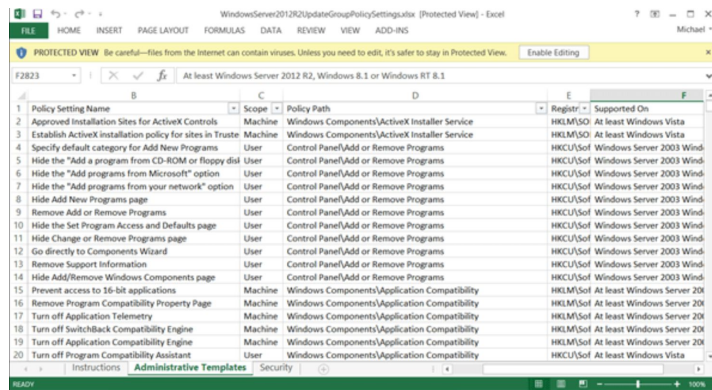
How does one...find a GP setting?

It's fun!

There's ... no search in the GP editor!

Options:

- Massive Excel sheet
- <http://gpsearch.azurewebsites.net/>
- Separate tools
- Google
- Filtering (right click Administrative Templates)



Groupwork

1. What software do you need to add to a Windows machine if you want it to be a **management machine** (and it doesn't already have that software from AD)
 - a. And, what does this software provide?
2. What is the order that group policy is applied?
3. What happens if a GPO is set to be Enforced
4. What is the difference between applying a GPO to a computer vs. a user?
5. It is now post-midterm. Time to get cracking on your project. At this point you should have a good idea of what you're doing. Assign a task to each team member to be done this week and simply itemize each member's task for this question, but you should each be doing something to move it forward!

~~Turn in via Moodle~~ **only by tomorrow night**