**Group Policy**

**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 to workstation: linking GPO to container

-Group policy **object** (GPO)

-Collection of settings applied to workstation: linking GPO to container

-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  
 -Tattoo?** GPO goes out of scope, preference remains in registry

-Supercede application setting

-(Application aware)

-Recognized by application

-(Grayed out)

-GP preference

-Will **tattoo**

-Overwrite application setting

-Not to be recognized by application

-(Changeable)

**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

**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

-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 container GPO copies (replication 🡪 synchronized automagically)

-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

**Sections and Categories**

-Policy settings

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

-ex) 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

-Many settings exist both User and Computer sections

-ex) 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