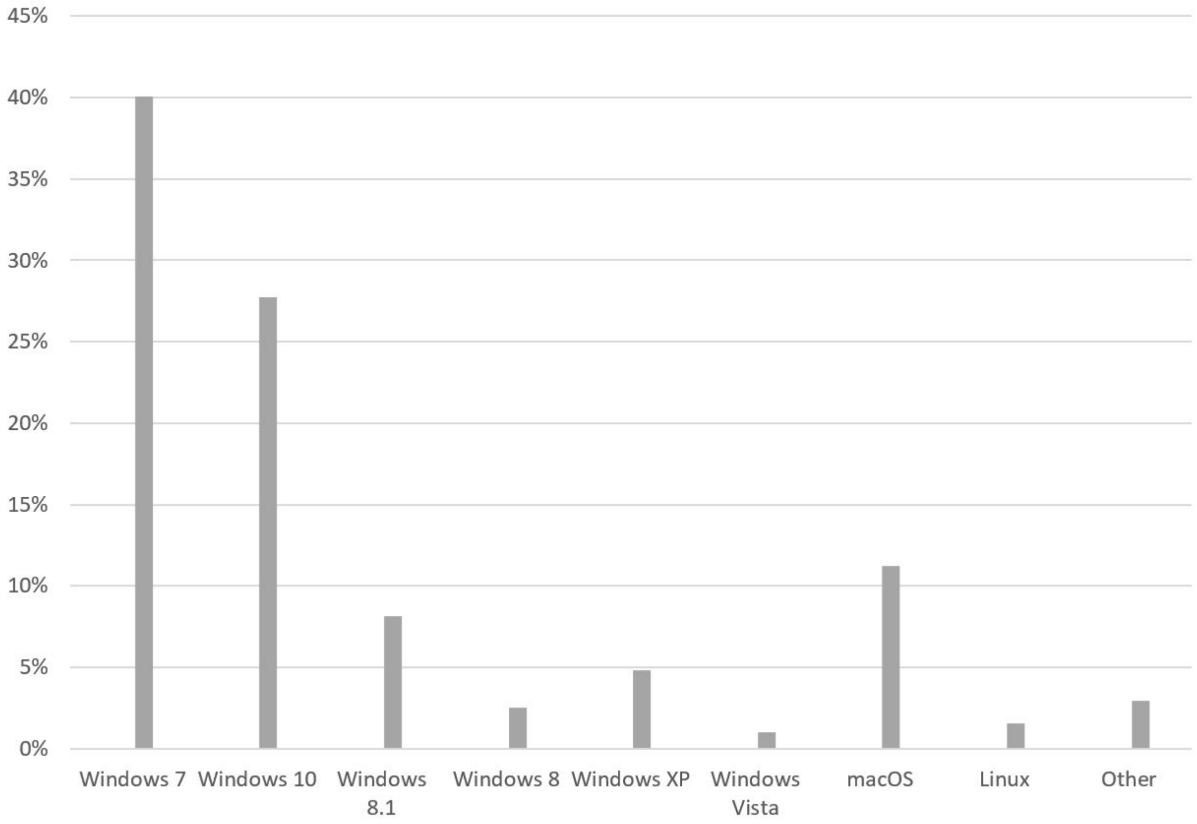
Windows

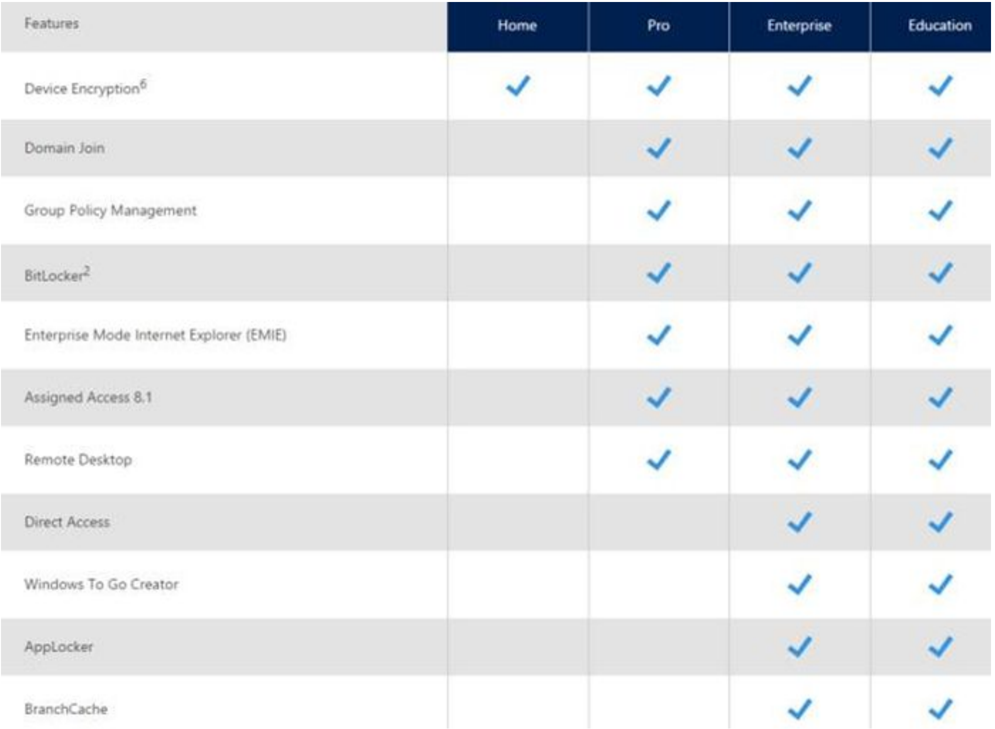
Not Just For Houses

Everyone Uses Windows!



Versions of Windows 10

- There are multiple different versions of Windows 10 that support different features
- The version of Windows that we will be using is Enterprise edition
- This supports features that are useful in controlling a Windows environment



Features	Home	Pro	Enterprise	Education
Device Encryption[6]	✓	✓	✓	✓
Domain Join		✓	✓	✓
Group Policy Management		✓	✓	✓
BitLocker[2]		✓	✓	✓
Enterprise Mode Internet Explorer (EMIE)		✓	✓	✓
Assigned Access 8.1		✓	✓	✓
Remote Desktop		✓	✓	✓
Direct Access			✓	✓
Windows To Go Creator			✓	✓
AppLocker			✓	✓
BranchCache			✓	✓

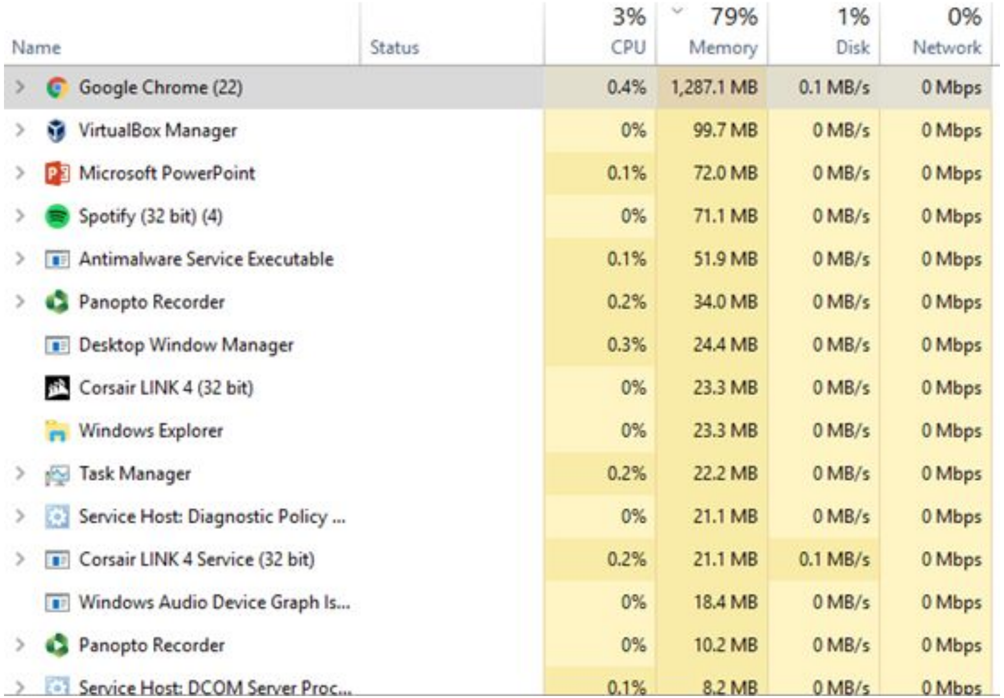
Users

- Accounts to separate people on a computer
- Multiple user accounts on a computer
  - Ex) shared family computer
- Access level can be set differently for each user
  - Ex) parent administrative account vs child standard account
  - Limit what can be done or installed

Command: Control userpasswords2

Processes in windows

- A process in the simplest terms, is an executing program
- All programs on your computer including Windows programs is a process
- Programs in Windows are launched in the form of an executable which is located on disk

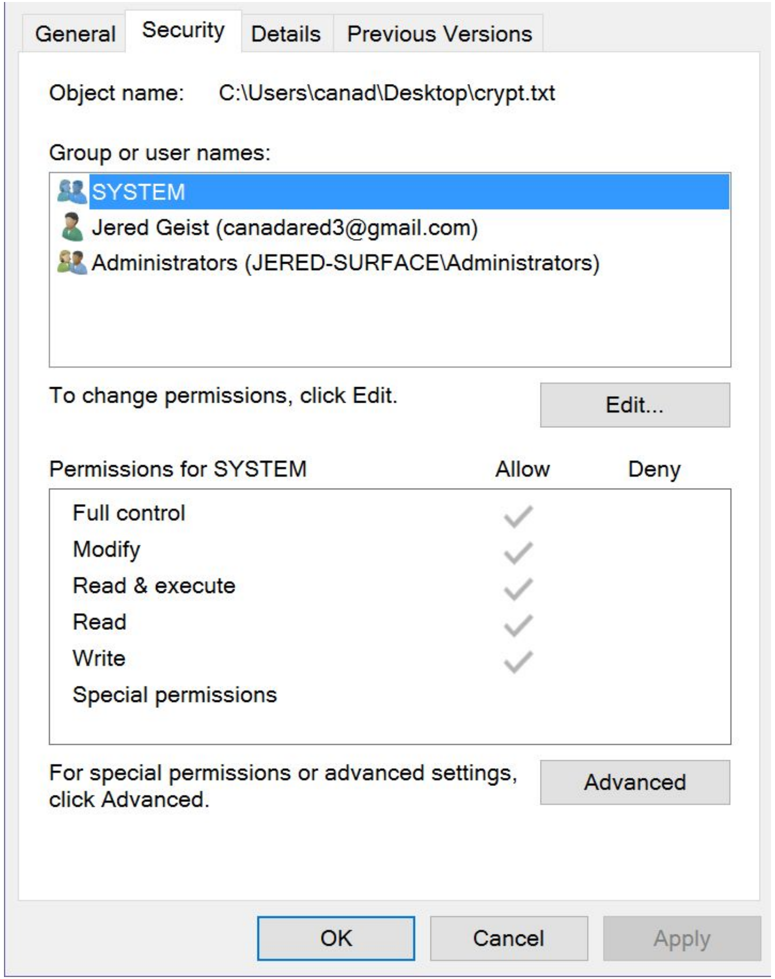


		3%	79%	1%	0%
Name	Status	CPU	Memory	Disk	Network
Google Chrome (22)		0.4%	1,287.1 MB	0.1 MB/s	0 Mbps
VirtualBox Manager		0%	99.7 MB	0 MB/s	0 Mbps
Microsoft PowerPoint		0.1%	72.0 MB	0 MB/s	0 Mbps
Spotify (32 bit) (4)		0%	71.1 MB	0 MB/s	0 Mbps
Antimalware Service Executable		0.1%	51.9 MB	0 MB/s	0 Mbps
Panopto Recorder		0.2%	34.0 MB	0 MB/s	0 Mbps
Desktop Window Manager		0.3%	24.4 MB	0 MB/s	0 Mbps
Corsair LINK 4 (32 bit)		0%	23.3 MB	0 MB/s	0 Mbps
Windows Explorer		0%	23.3 MB	0 MB/s	0 Mbps
Task Manager		0.2%	22.2 MB	0 MB/s	0 Mbps
Service Host: Diagnostic Policy ...		0%	21.1 MB	0 MB/s	0 Mbps
Corsair LINK 4 Service (32 bit)		0.2%	21.1 MB	0.1 MB/s	0 Mbps
Windows Audio Device Graph Is...		0%	18.4 MB	0 MB/s	0 Mbps
Panopto Recorder		0%	10.2 MB	0 MB/s	0 Mbps
Service Host: DCOM Server Proc...		0.1%	8.2 MB	0 MB/s	0 Mbps

Files

- Store digital data
- Security settings can be changed on files based on user accounts
- Can limit read, write, modify permissions
- Only allow certain people to view sensitive files
    - ex) tax information stored on family computer

Right click on a file and go to properties



Object name: C:\Users\canad\Desktop\crypt.txt

Group or user names:

- SYSTEM
- Jered Geist (canadared3@gmail.com)
- Administrators (JERED-SURFACE\Administrators)

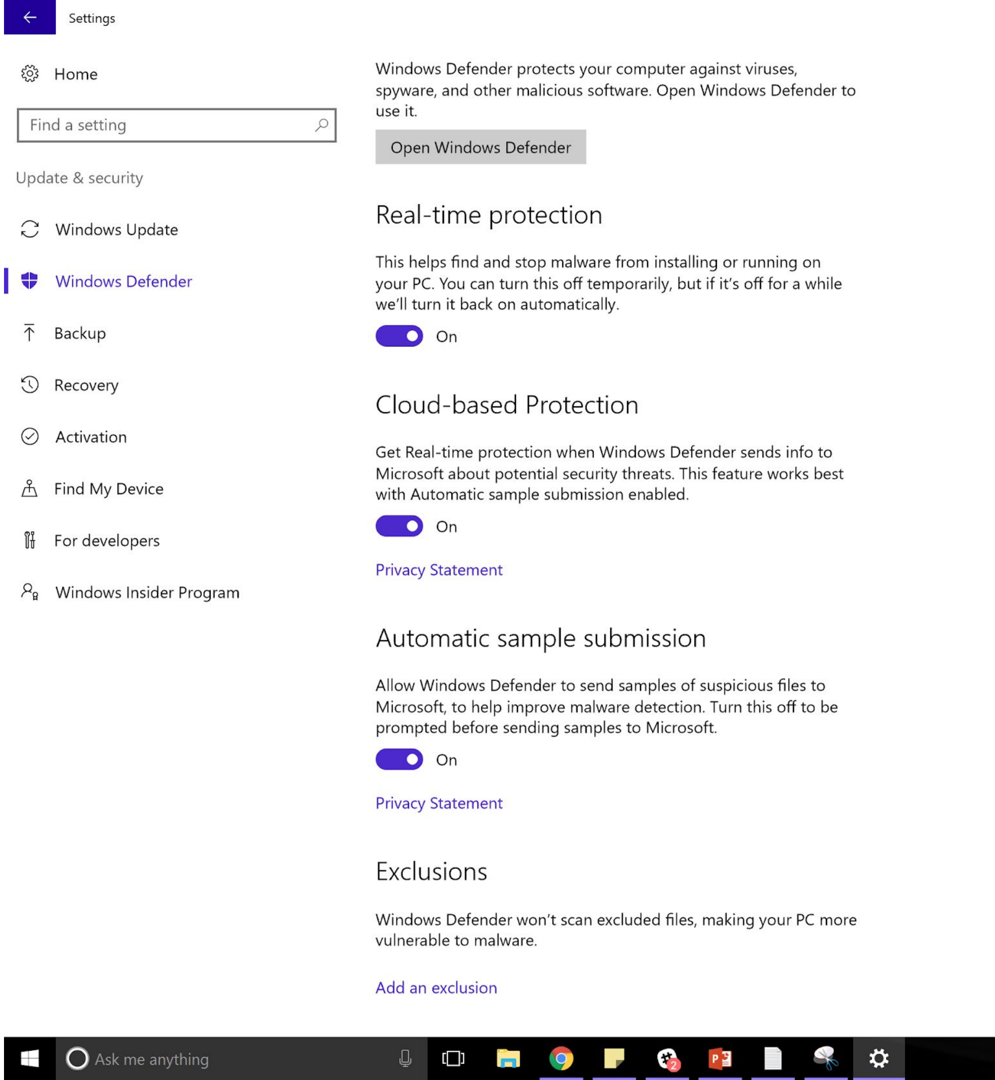
To change permissions, click Edit.

Permissions for SYSTEM	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
Read	✓	
Write	✓	
Special permissions		

For special permissions or advanced settings, click Advanced.

Settings

- Can change how your computer works
- Settings for everything!
    - Updates
    - anti -virus
    - Time zone
    - Brightness
    - etc.



Windows Defender protects your computer against viruses, spyware, and other malicious software. Open Windows Defender to use it.

Real-time protection

This helps find and stop malware from installing or running on your PC. You can turn this off temporarily, but if it's off for a while we'll turn it back on automatically.

On

Cloud-based Protection

Get Real-time protection when Windows Defender sends info to Microsoft about potential security threats. This feature works best with Automatic sample submission enabled.

On

Privacy Statement

Automatic sample submission

Allow Windows Defender to send samples of suspicious files to Microsoft, to help improve malware detection. Turn this off to be prompted before sending samples to Microsoft.

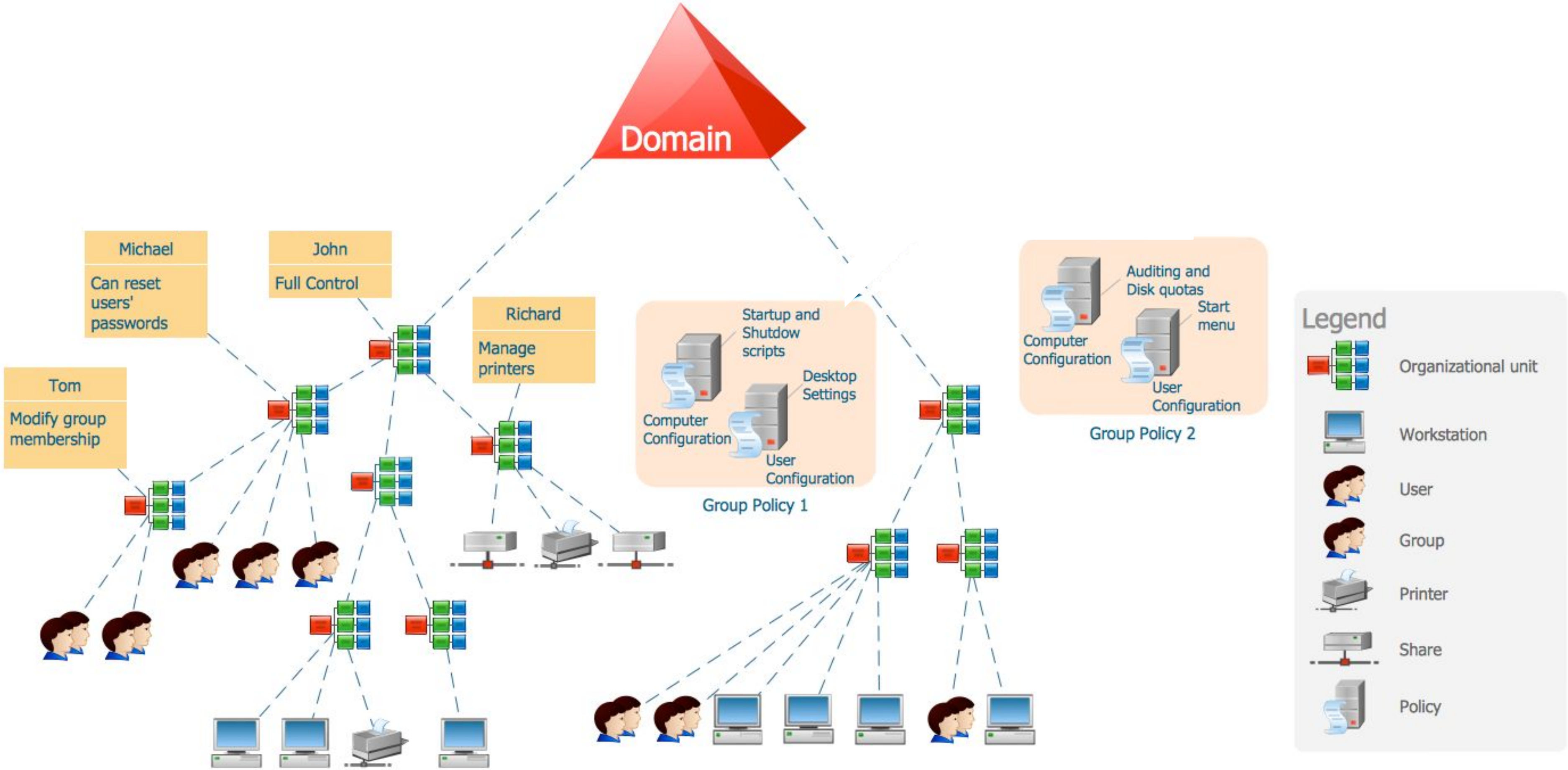
On

Privacy Statement

Exclusions

Windows Defender won't scan excluded files, making your PC more vulnerable to malware.

Add an exclusion


Domain
Michael
Can reset users' passwords
John
Full Control
Richard
Manage printers
Tom
Modify group membership
Startup and Shutdow scripts
Desktop Settings
Computer Configuration
User Configuration
Group Policy 1
Auditing and Disk quotas
Start menu
Computer Configuration
User Configuration
Group Policy 2
Legend
Organizational unit
Workstation
User
Group
Printer
Share
Policy

Networks are complex

- Need easy way to manage everything
  - Centralized login authentication
  - File sharing
  - Printer sharing
  - File security

- Specialized tools for easier management
  - Active Directory
  - Open LDAP
  - Free IPA

Windows Server

What can it do?

Can take on many roles, just like linux

- Email
- File storage
- User privileges
- Authentication
- Website
- DNS
- Many more

Active Directory and Group Policy

- Tools used for majority of windows based network management
- Interact and control many objects at once
  - Users
  - Computers
  - Files

Other Common Roles and Features

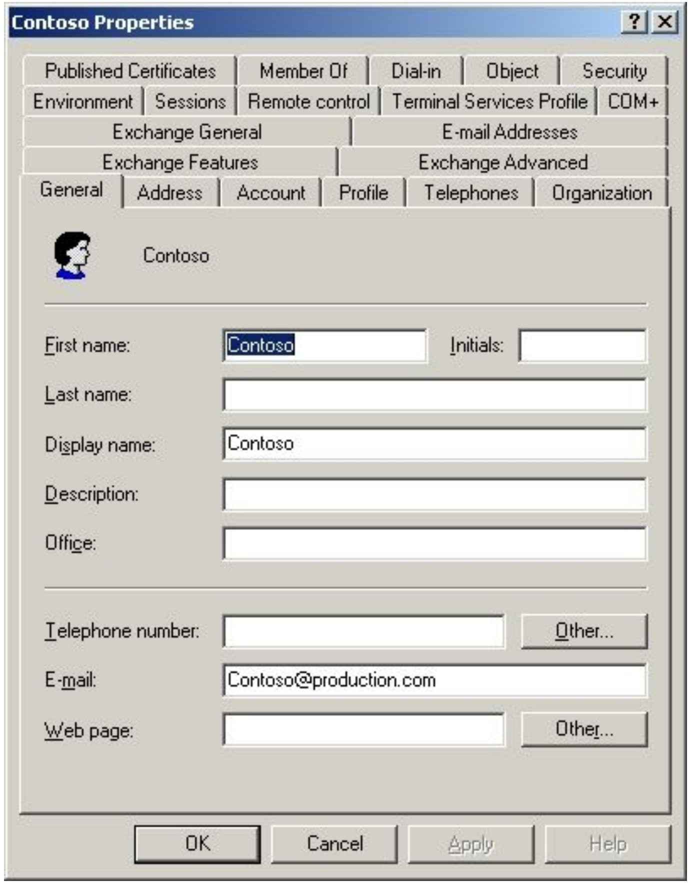
- SMB Server
- FTP Server
- Exchange Server
- Firewall
- Application deployment
- Centralized monitoring
- VPN
- DNS
- IIS (web server)

Active Directory

- Database of objects in a network (Domain)
  - Users
  - Computers
  - Printers
  - Security Groups
  - More
- Hosted on a Windows Server (Domain Controller)
- Stores objects in hierarchy
  - Called organizational units (OU)
  - Can be based on real world hierarchy of organization
  - Can be based on access rights

Users

- Stores information on user
  - Name
  - Email
  - Phone number
  - Address
  - Location in organization
  - Password (hashed)



Contoso Properties

Contoso

First name: Contoso

Initials:

Last name:

Display name: Contoso

Description:

Office:

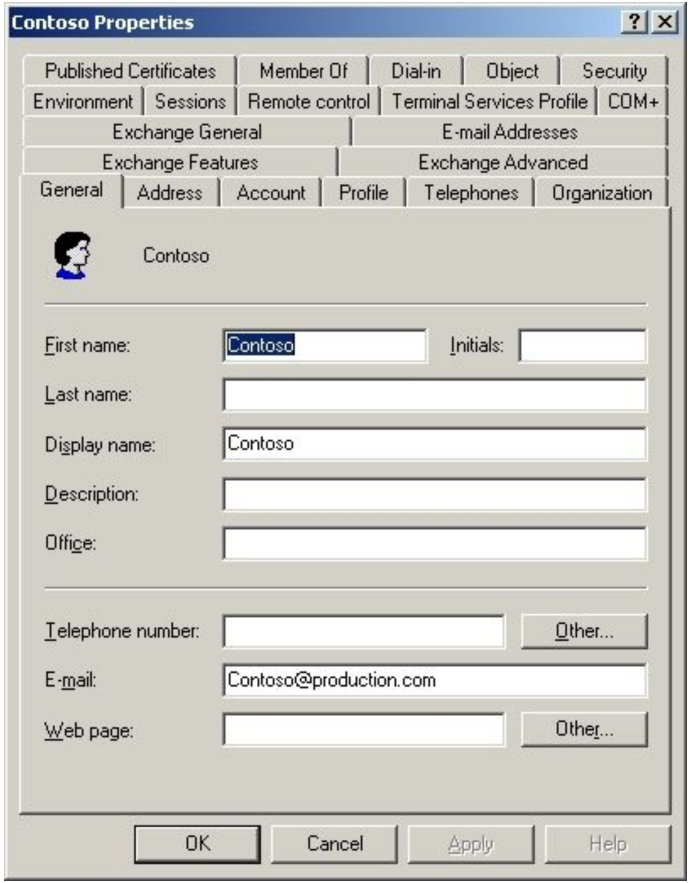
Telephone number:

E-mail: Contoso@production.com

Web page:

Users

- Controls permissions
  - File and folder access
  - VPN access
  - Password management
  - Active account
  - Access control
- Ability to control total network access
- Map drives to computer
- Folder redirection



Contoso Properties

Contoso

First name: Contoso

Initials:

Last name:

Display name: Contoso

Description:

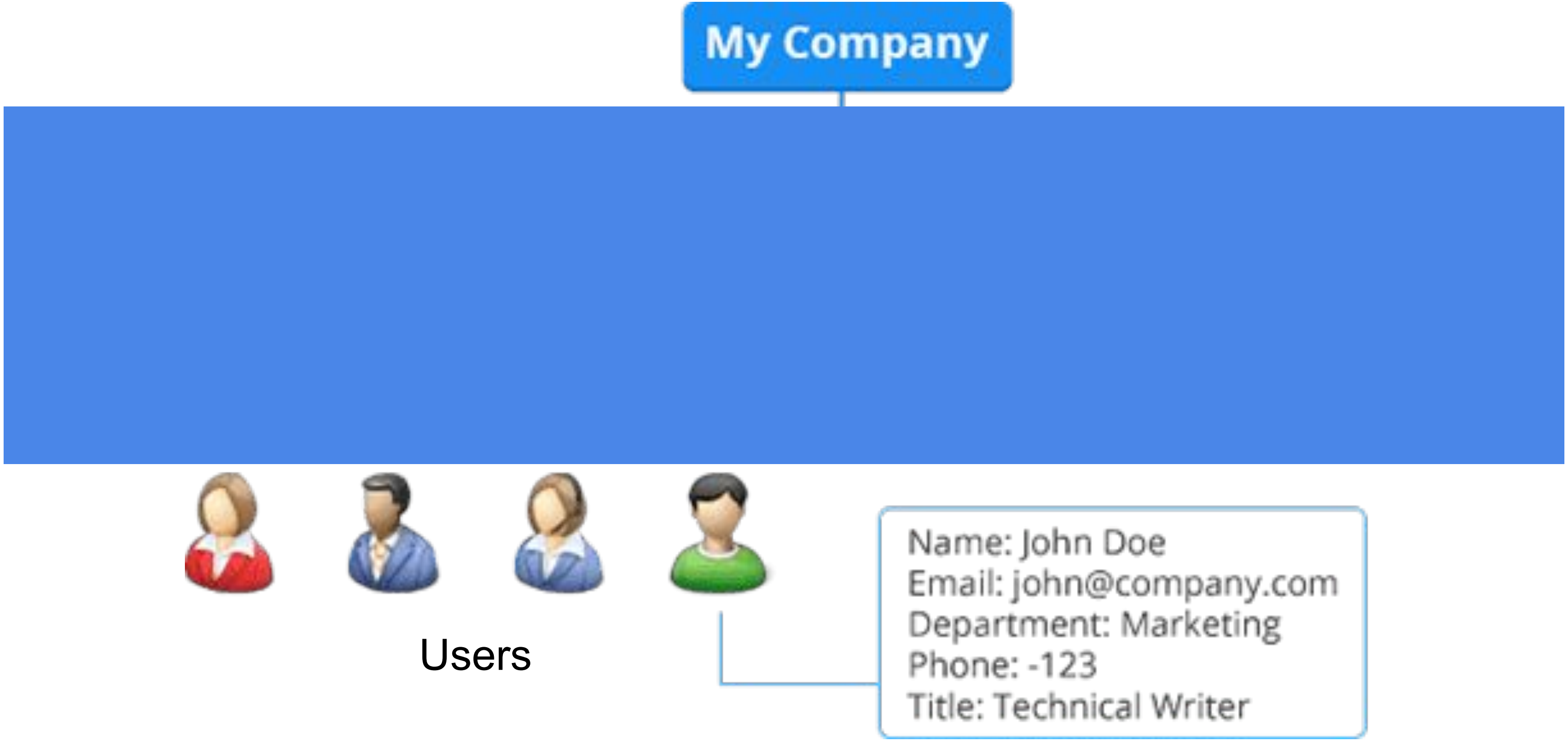
Office:

Telephone number:

E-mail: Contoso@production.com

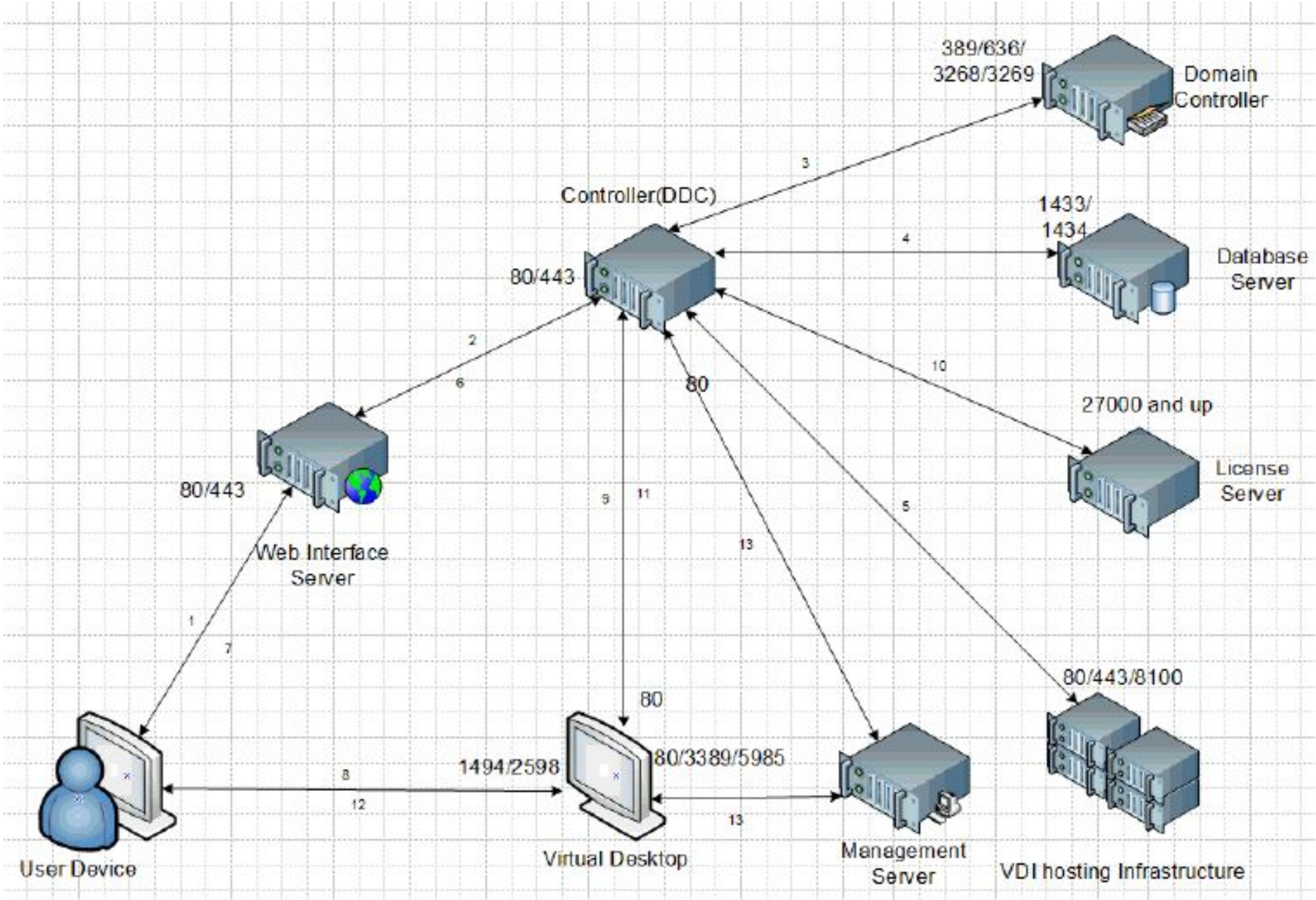
Web page:

Domain



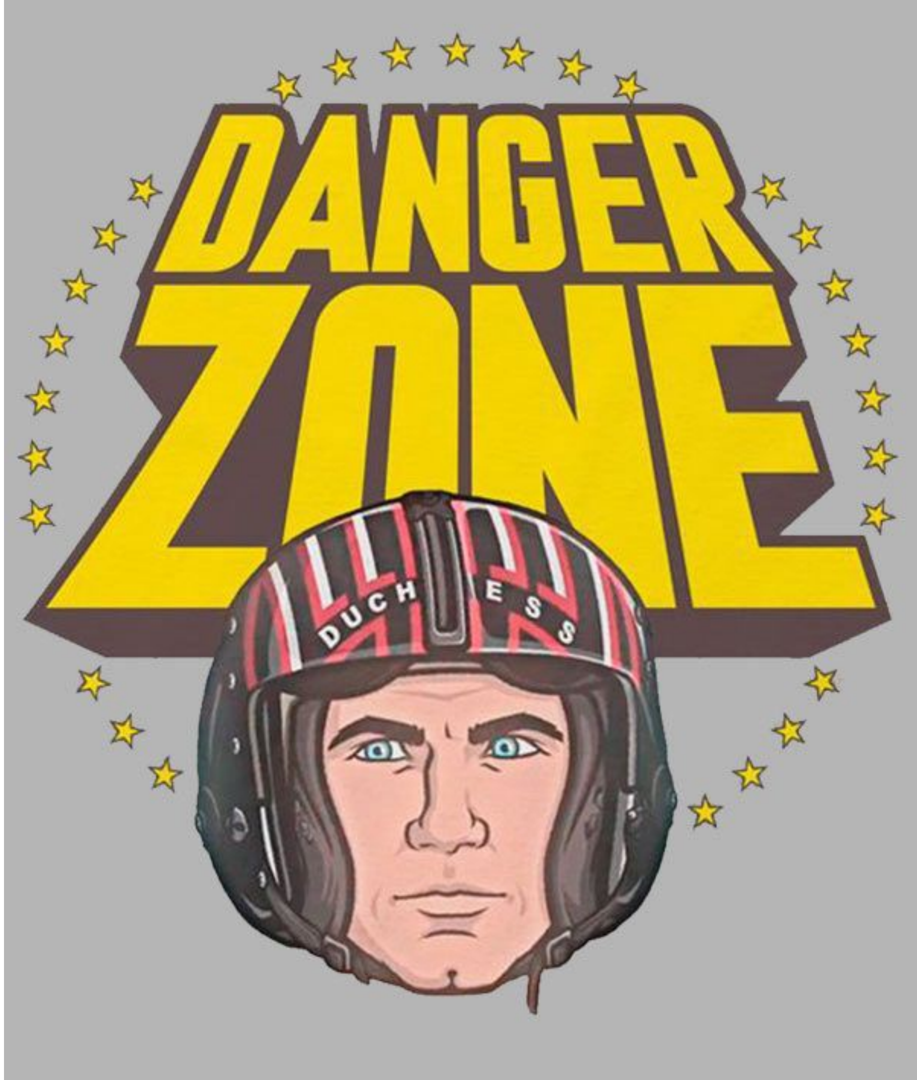
Name: John Doe
Email: john@company.com
Department: Marketing
Phone: -123
Title: Technical Writer

Users


389/636/
3268/3269
Domain
Controller
3
Controller(DDC)
1433/
1434
4
Database
Server
80/443
2
6
10
80
27000 and up
License
Server
80/443
9
11
5
13
Web Interface
Server
1
7
80/443/8100
80
80/3389/5985
1494/2598
8
12
13
User Device
Virtual Desktop
Management
Server
VDI hosting Infrastructure

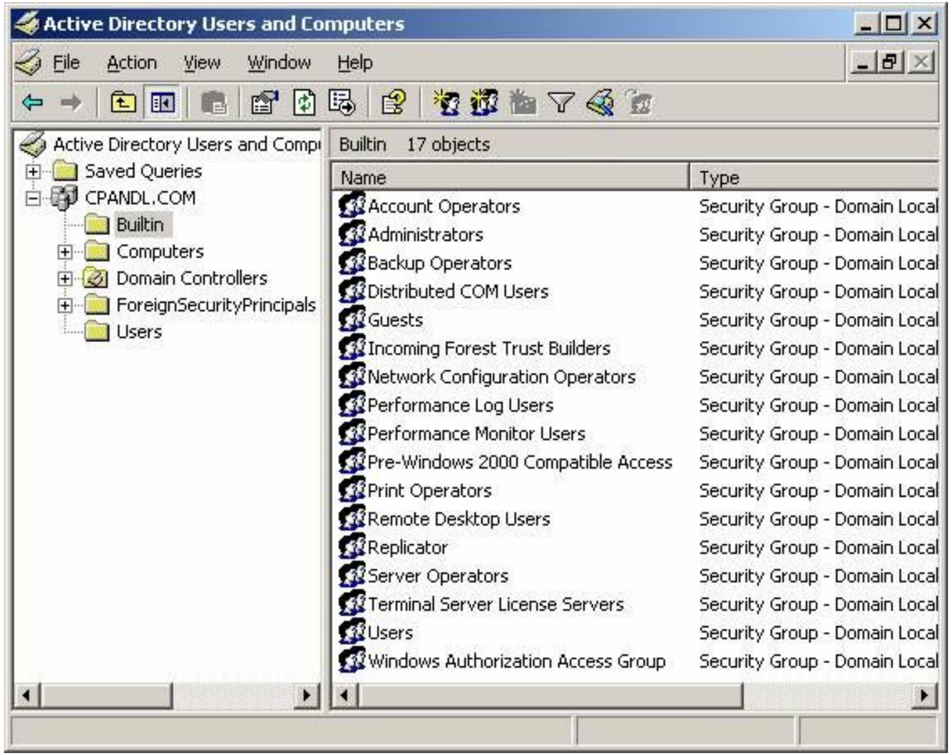
Danger Zone

- Too many users to manage them all
  - UB has ~ 50,000 users
- Can leave security holes
  - Terminated employee
  - Other permission changes can affect
- Use groups instead



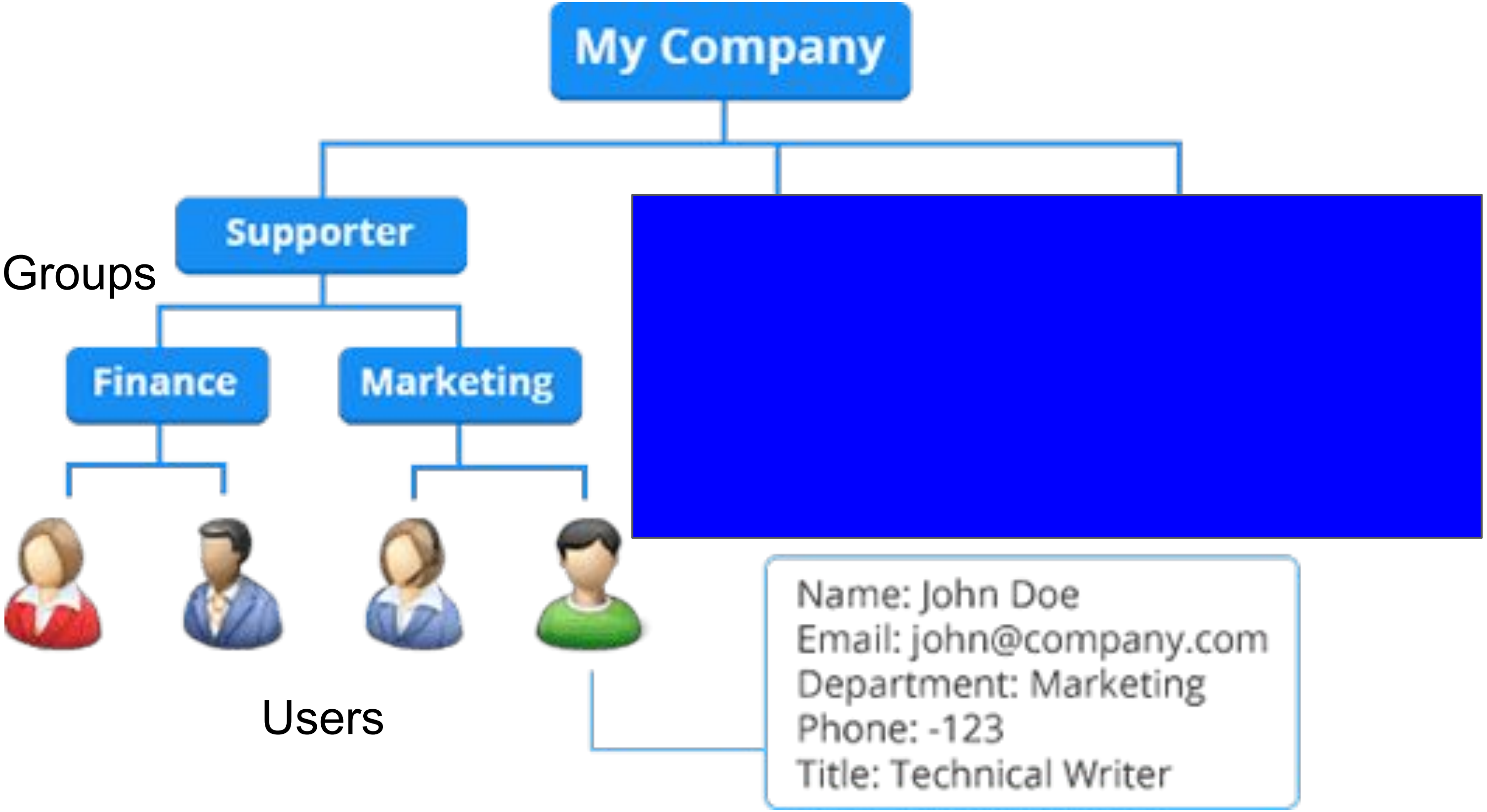
Security Groups

- Security groups are special folders inside Organizational Units (OU)
- Objects can be put in groups
- Helps keep organized
- Can assign settings to groups
- Acts similarly to users configuration
- Manage every user at once



Name	Type
Account Operators	Security Group - Domain Local
Administrators	Security Group - Domain Local
Backup Operators	Security Group - Domain Local
Distributed COM Users	Security Group - Domain Local
Guests	Security Group - Domain Local
Incoming Forest Trust Builders	Security Group - Domain Local
Network Configuration Operators	Security Group - Domain Local
Performance Log Users	Security Group - Domain Local
Performance Monitor Users	Security Group - Domain Local
Pre-Windows 2000 Compatible Access	Security Group - Domain Local
Print Operators	Security Group - Domain Local
Remote Desktop Users	Security Group - Domain Local
Replicator	Security Group - Domain Local
Server Operators	Security Group - Domain Local
Terminal Server License Servers	Security Group - Domain Local
Users	Security Group - Domain Local
Windows Authorization Access Group	Security Group - Domain Local

Domain



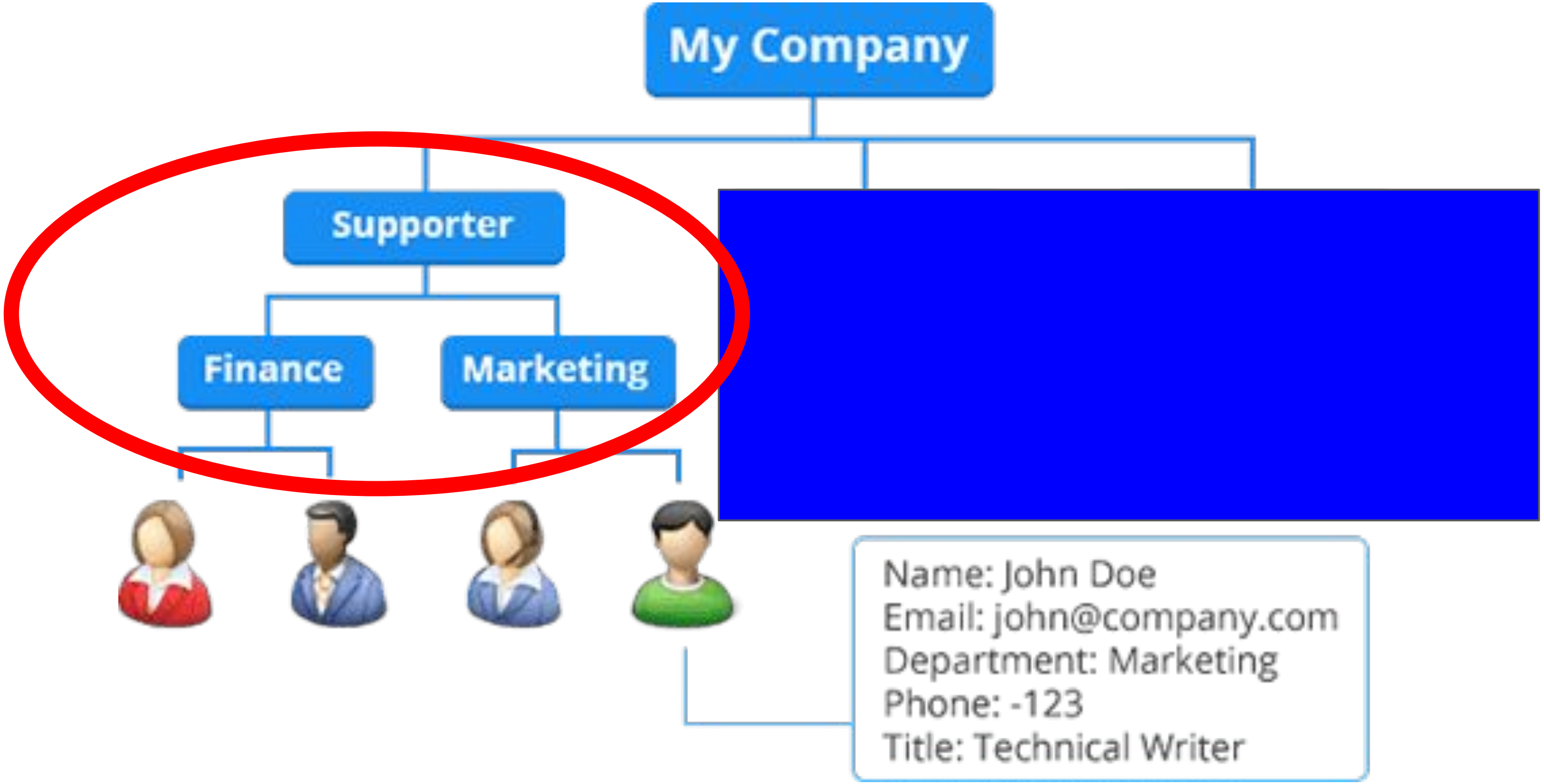
[redacted]

Groups

Users

Name: John Doe
Email: john@company.com
Department: Marketing
Phone: -123
Title: Technical Writer

Groups in Groups?



[redacted]

Name: John Doe
Email: john@company.com
Department: Marketing
Phone: -123
Title: Technical Writer

Nesting

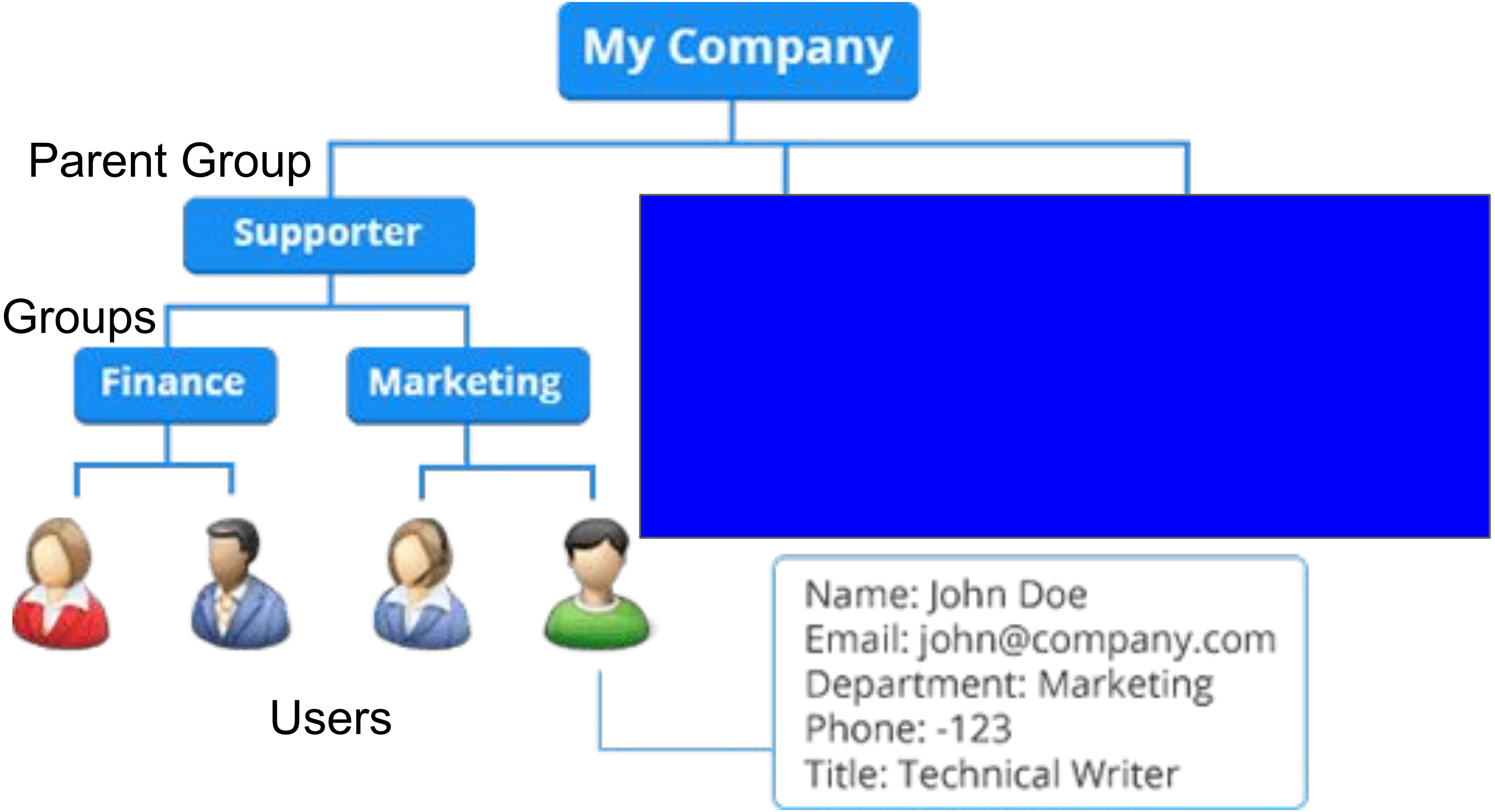
- Can put groups in groups
- Starts to get complicated
- Need to lay out organization before building AD
  - Build domain based on network layout and permissions
  - Does not always look the same as organization
- Leads to inheritance

Inheritance

Think of trickle down theory…..

- Sub groups (children objects) inherit permissions from group above (parent object)

- Users in a group, in a group, will get settings placed on top level group



Domain

Parent Group

Children Groups

Users

[redacted]

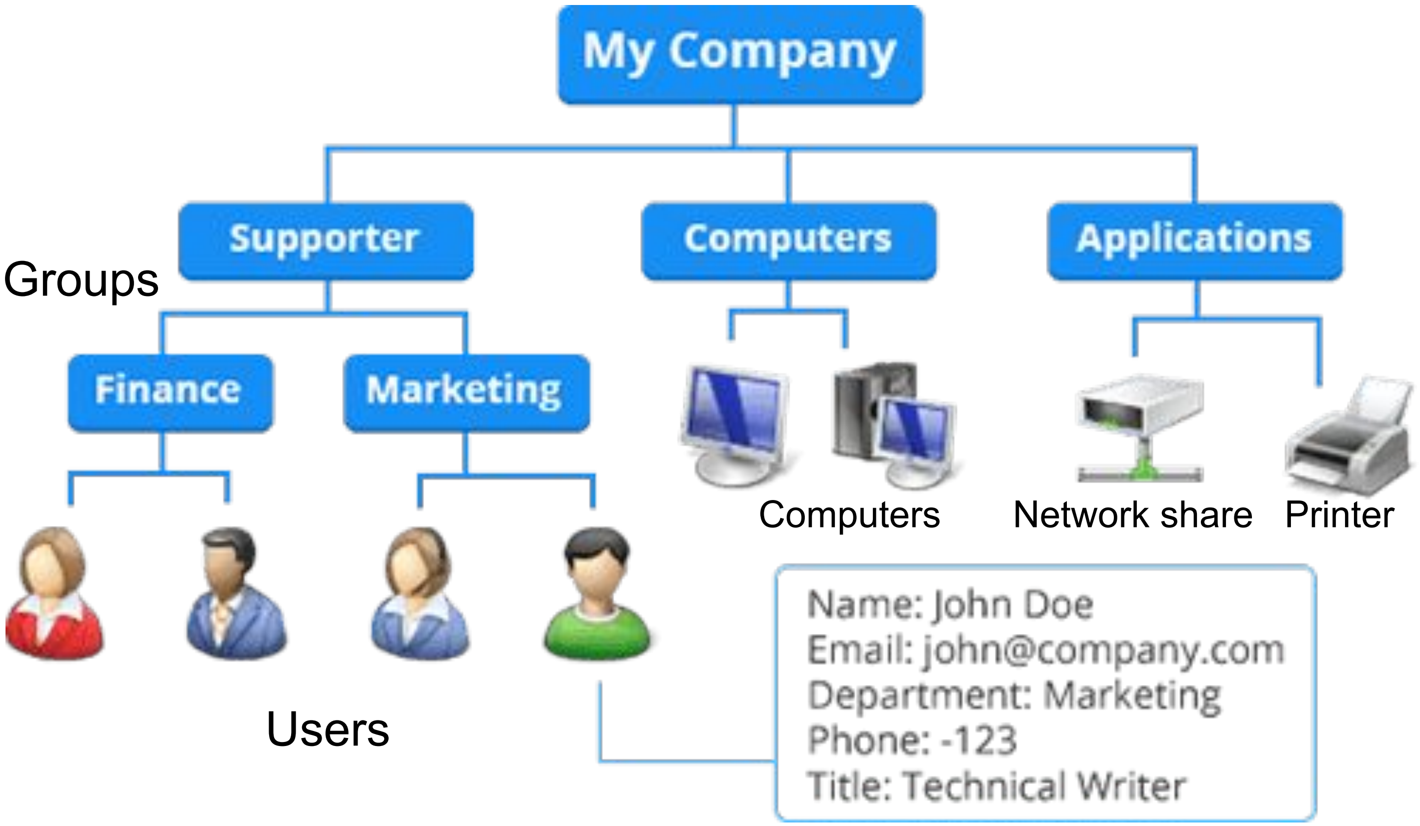
Name: John Doe
Email: john@company.com
Department: Marketing
Phone: -123
Title: Technical Writer

Computers and Devices

- Like users, devices can be managed in AD
- Computers
- Printers
- Other Servers

Can start to connect resources to each other

Domain



My Company

Supporter

Computers

Applications

Groups

Finance

Marketing

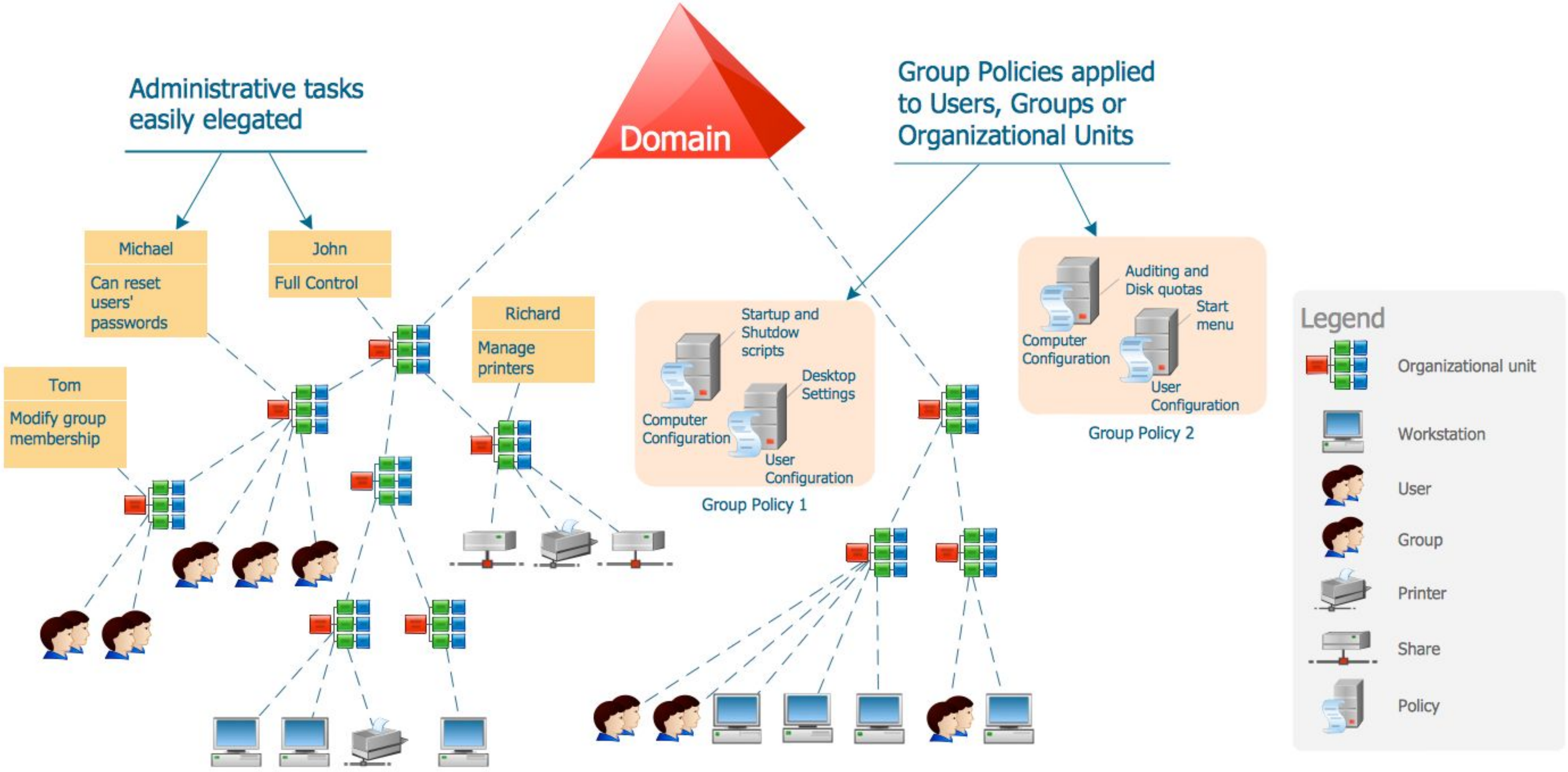
Computers

Network share

Printer

Users

Name: John Doe
Email: john@company.com
Department: Marketing
Phone: -123
Title: Technical Writer



Administrative tasks easily elegated

Domain

Group Policies applied to Users, Groups or Organizational Units

Michael

Can reset users' passwords

John

Full Control

Richard

Manage printers

Tom

Modify group membership

Startup and Shutdow scripts

Desktop Settings

Computer Configuration

User Configuration

Group Policy 1

Auditing and Disk quotas

Start menu

Computer Configuration

User Configuration

Group Policy 2

Legend

Organizational unit

Workstation

User

Group

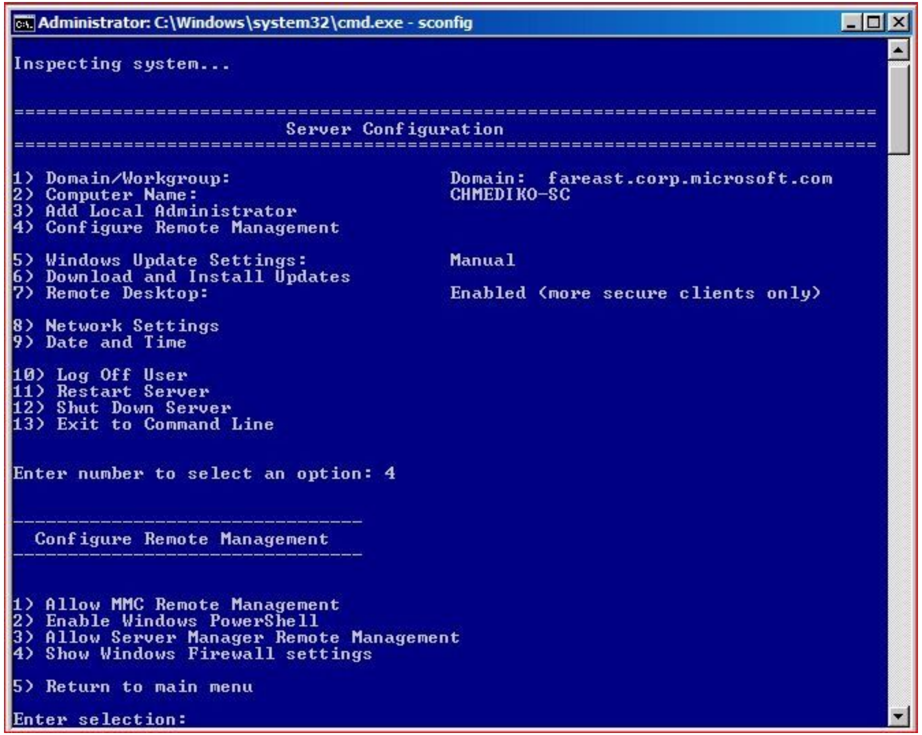
Printer

Share

Policy

Confused yet?

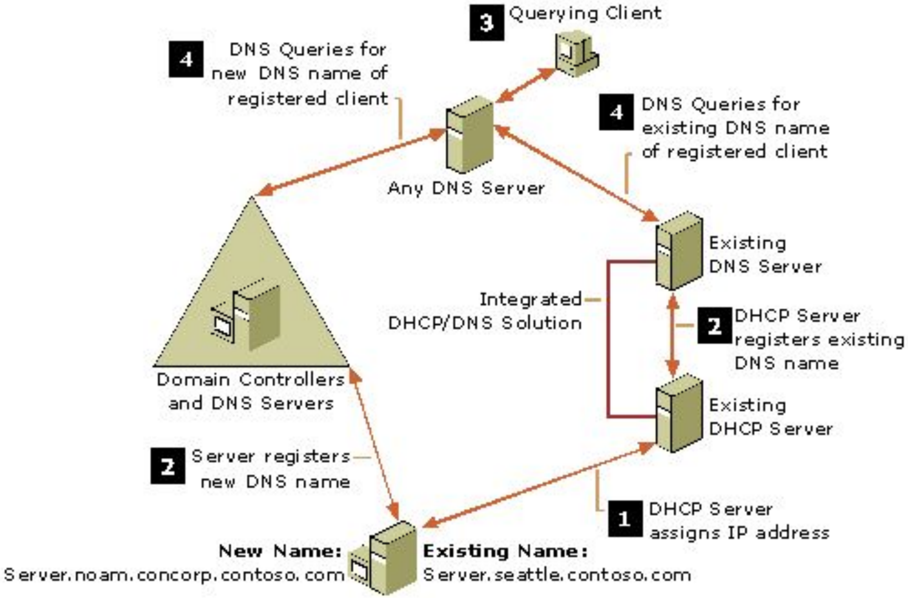
- Domains control network
- OU’s store information about things (Objects)
- Security Groups also contain objects
- Groups can go in groups
- Children objects inherit permissions from parent objects



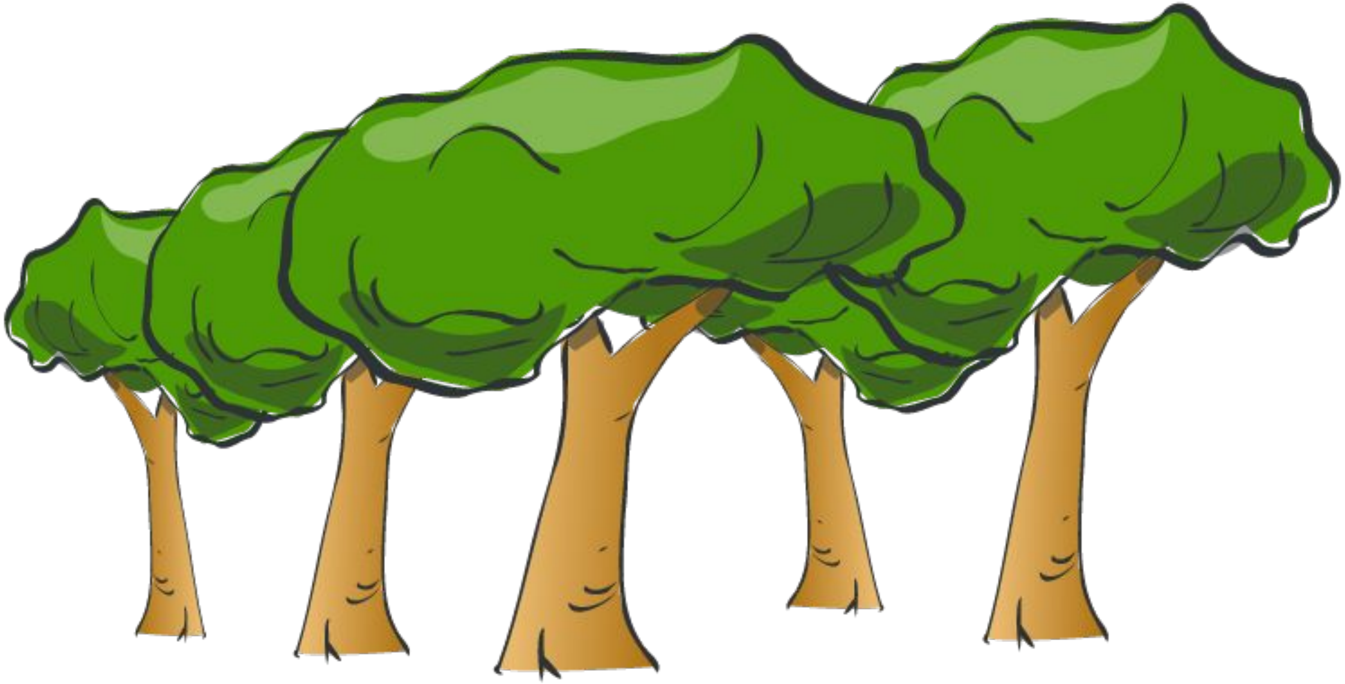
```
Inspecting system...

===============================================================================
                         Server Configuration
===============================================================================

1) Domain/Workgroup:                    Domain:  fareast.corp.microsoft.com
2) Computer Name:                       CHMEDIKO-SC
3) Add Local Administrator
4) Configure Remote Management

5) Windows Update Settings:             Manual
6) Download and Install Updates
7) Remote Desktop:                      Enabled (more secure clients only)

8) Network Settings
9) Date and Time

10) Log Off User
11) Restart Server
12) Shut Down Server
13) Exit to Command Line

Enter number to select an option: 4

--------------------------------
  Configure Remote Management
--------------------------------


1) Allow MMC Remote Management
2) Enable Windows PowerShell
3) Allow Server Manager Remote Management
4) Show Windows Firewall settings

5) Return to main menu

Enter selection:
```

AD Tips

DON’T LET DNS DIE

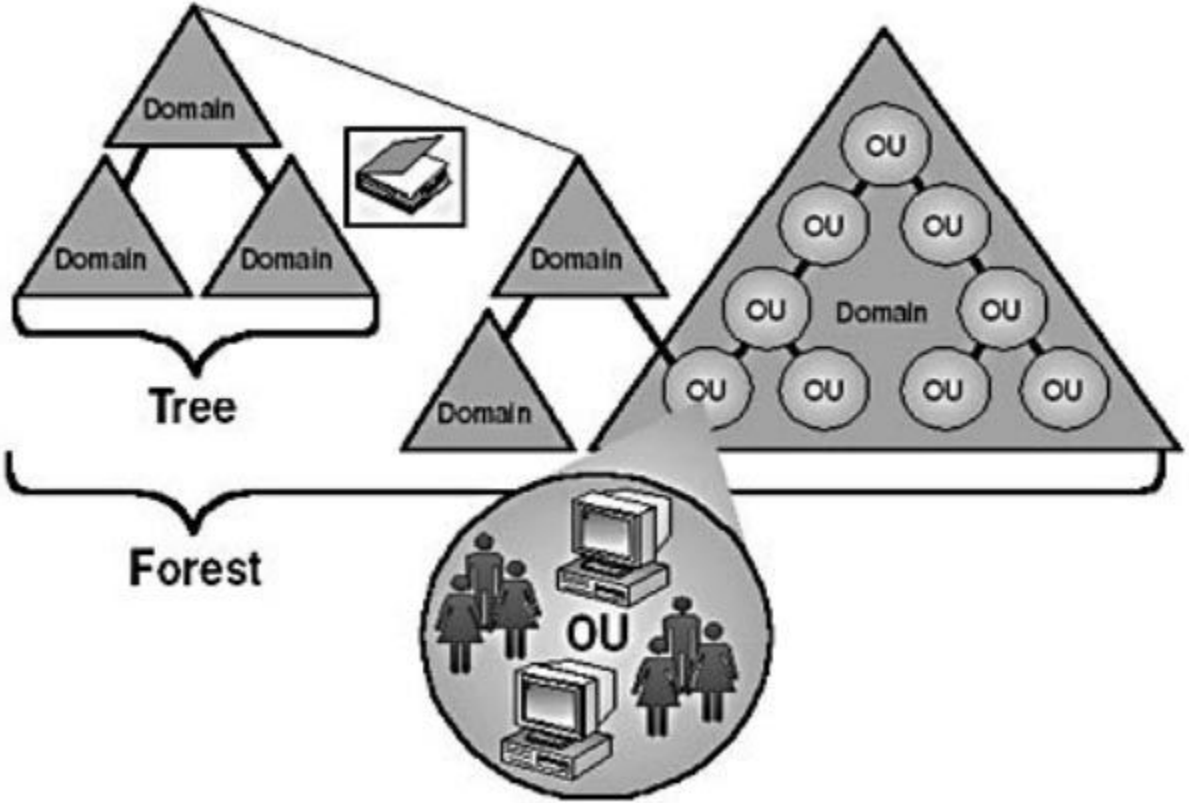

3 Querying Client
4 DNS Queries for new DNS name of registered client
Any DNS Server
4 DNS Queries for existing DNS name of registered client
Existing DNS Server
Integrated DHCP/DNS Solution
2 DHCP Server registers existing DNS name
Existing DHCP Server
Domain Controllers and DNS Servers
2 Server registers new DNS name
1 DHCP Server assigns IP address
New Name: Server.noam.concorp.contoso.com
Existing Name: Server.seattle.contoso.com

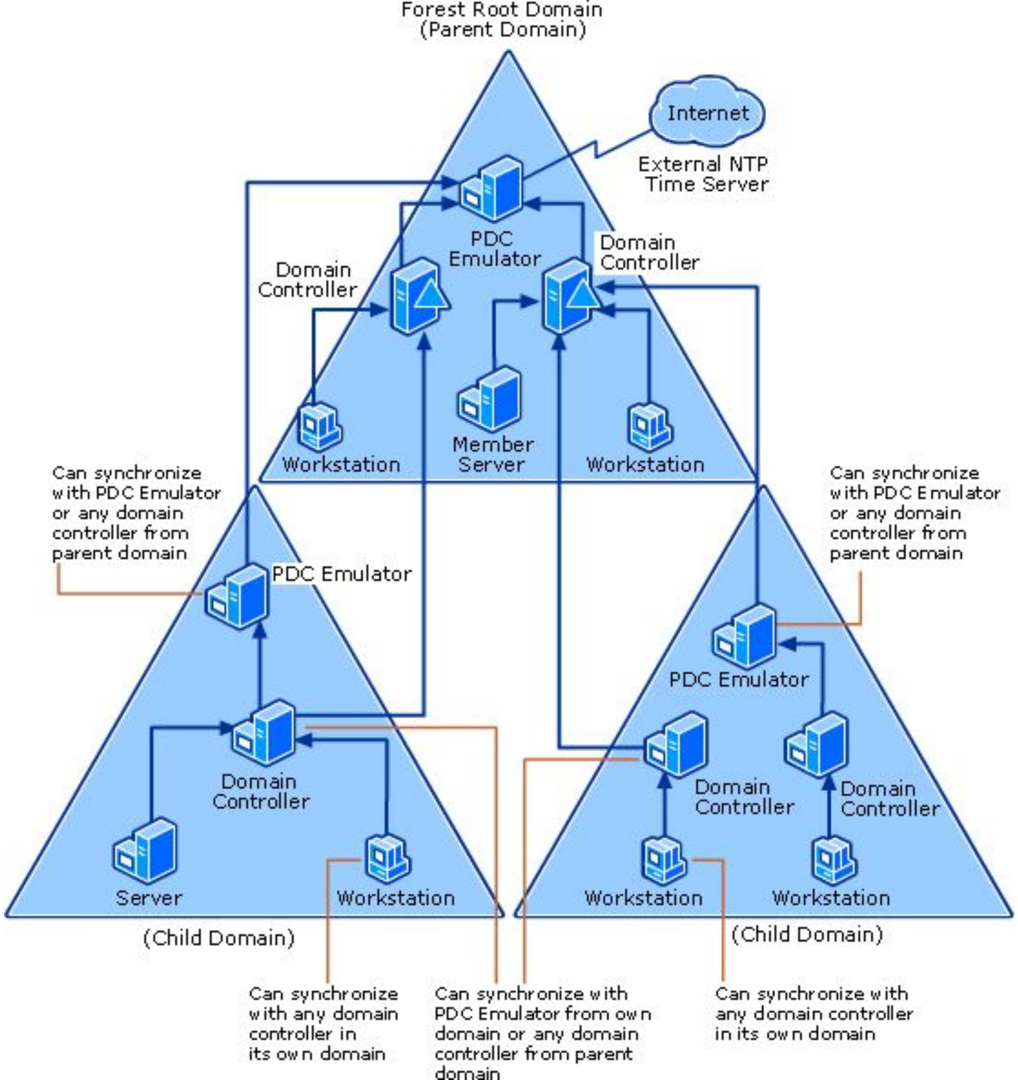
Forests, trees, and leaves



Forests, trees, and leaves

Forests, trees, and leaves





Can synchronize with PDC Emulator or any domain controller from parent domain

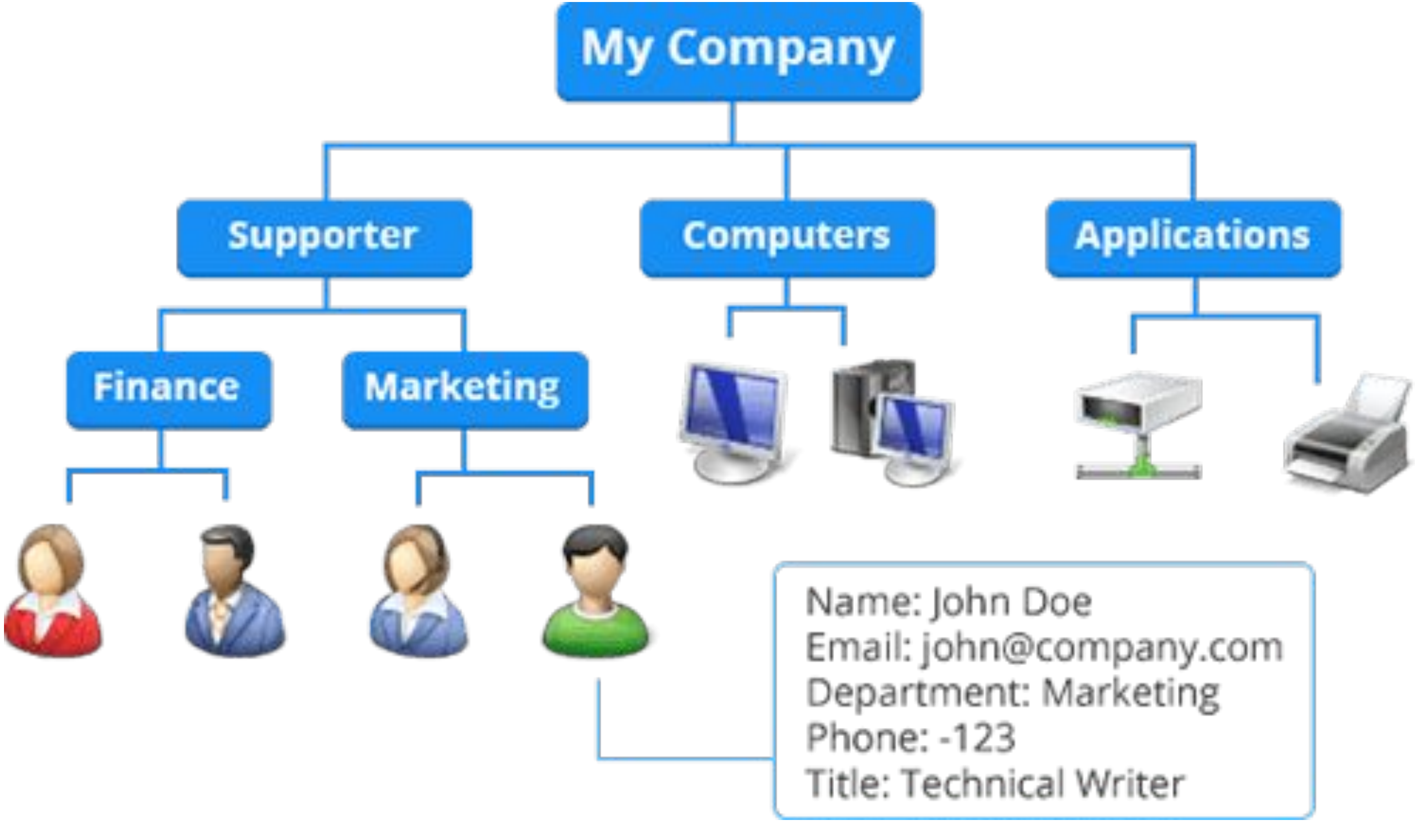
Can synchronize with PDC Emulator or any domain controller from parent domain

Can synchronize with any domain controller in its own domain

Can synchronize with PDC Emulator from own domain or any domain controller from parent domain

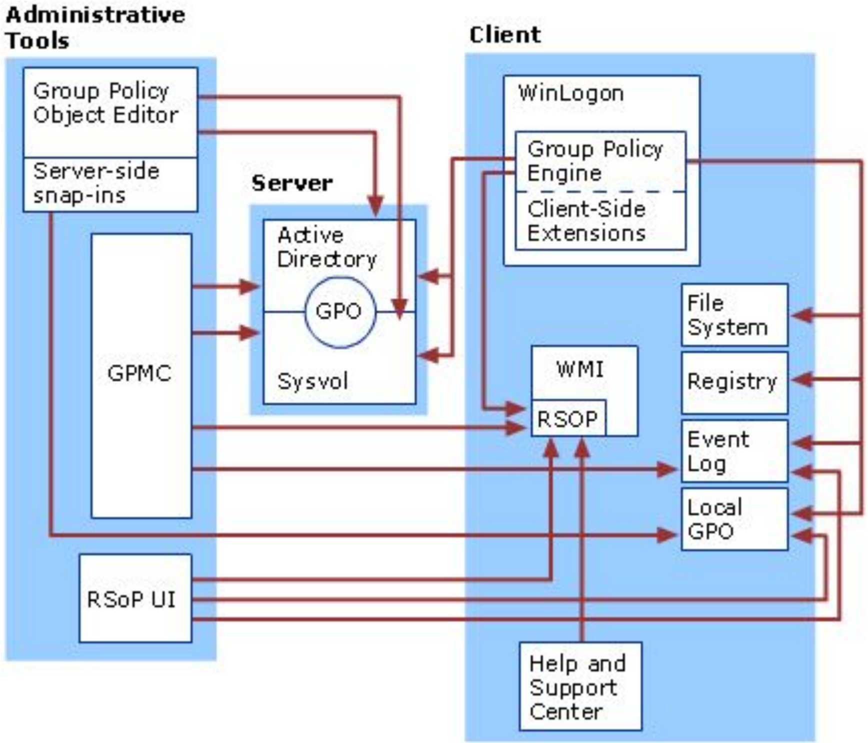
Can synchronize with any domain controller in its own domain

Active Directory



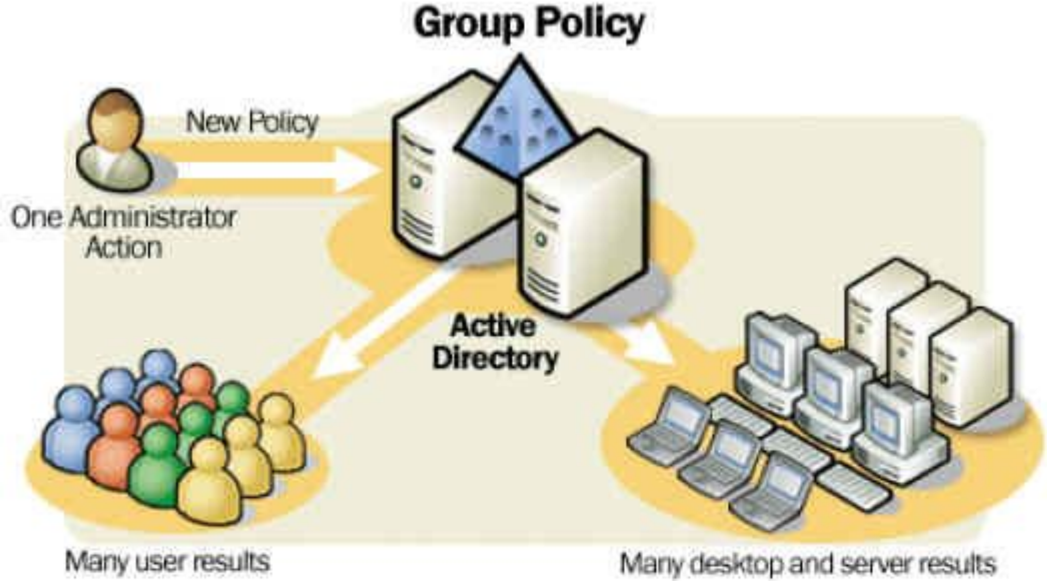
Group Policy

- Because this wasn't complicated enough already



Group Policy

- Centralized management tool for windows networks
- Can control pretty much every setting imaginable
- Works with Active Directory



For example…..

Mapped drives and folder redirection

Mapped Drives

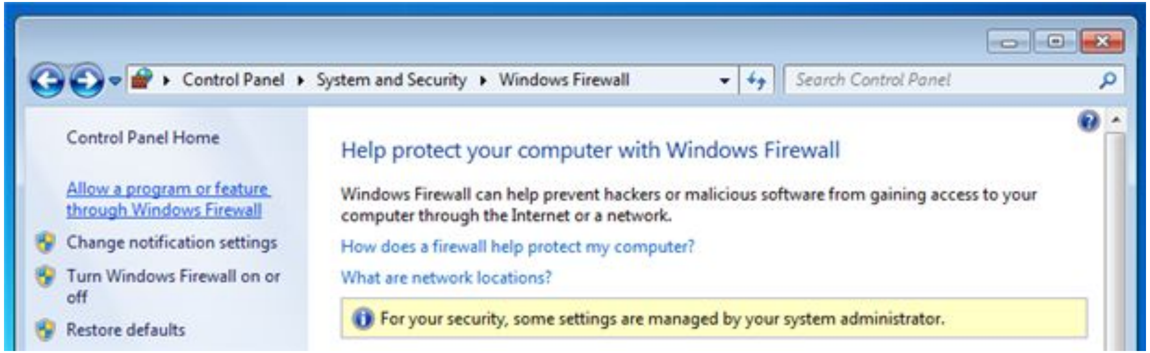
- Useful with many network drives
- Useful when user is moving computers
- Easy and seamless transition

Folder Redirection

- Nothing is stored locally
- Documents, pictures, desktop redirected to server
- Backups
- Mobility

Group Policy

- Can be used to force any setting on objects in AD
- Login scripts
- Mapped network drives
- Sleep settings
- Remote desktop access
- Password policy
- Set firewall policy
- Change background
- Change cursor
- Windows Update timing
- Pretty much anything you can think of


Control Panel ▸ System and Security ▸ Windows Firewall
Search Control Panel
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults

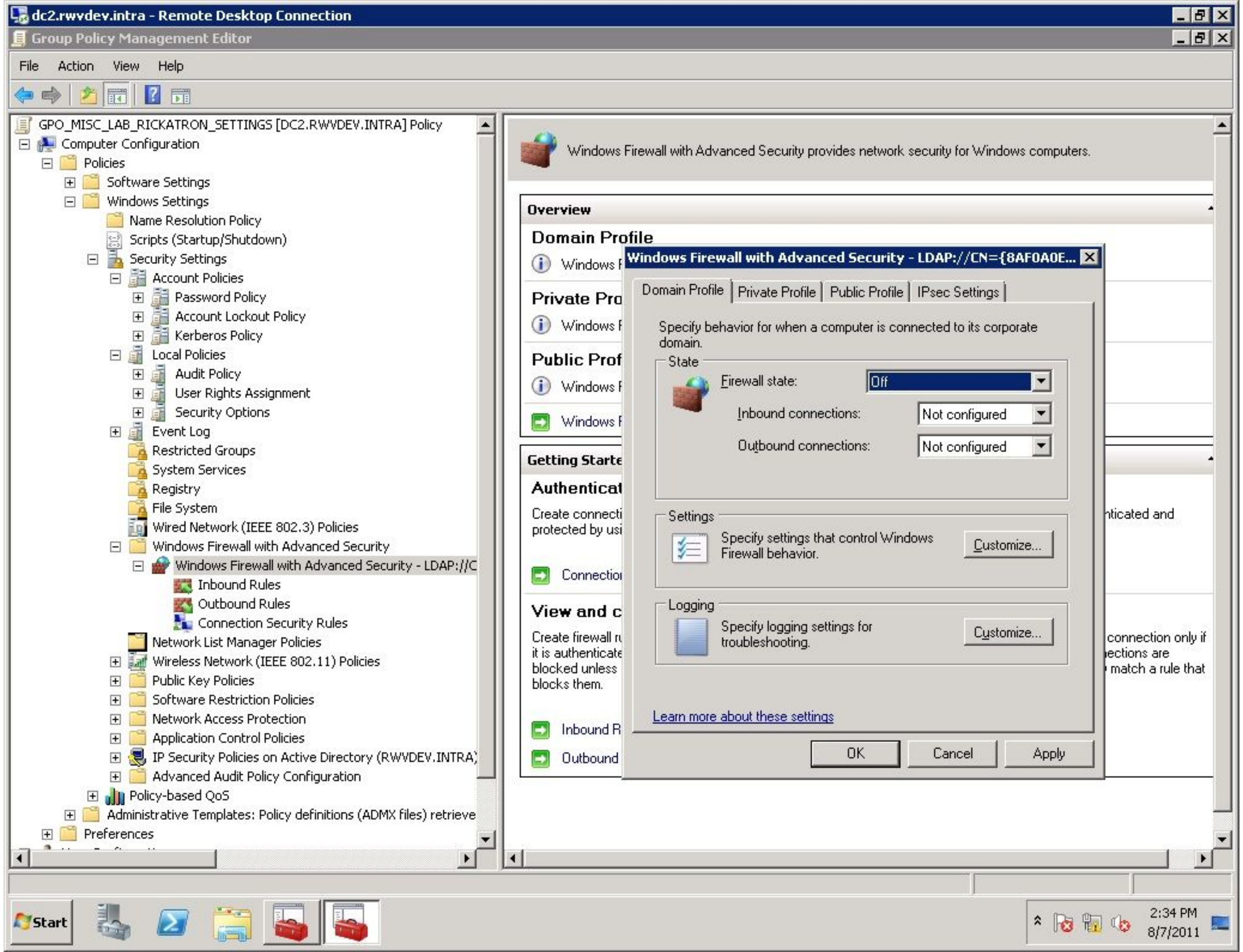
Help protect your computer with Windows Firewall

Windows Firewall can help prevent hackers or malicious software from gaining access to your computer through the Internet or a network.

How does a firewall help protect my computer?

What are network locations?

For your security, some settings are managed by your system administrator.


dc2.rwvdev.intra - Remote Desktop Connection
Group Policy Management Editor
File
Action
View
Help
Start
2:34 PM
8/7/2011

GPO_MISC_LAB_RICKATRON_SETTINGS [DC2.RWVDEV.INTRA] Policy

- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Security Settings
        - Account Policies
          - Password Policy
          - Account Lockout Policy
          - Kerberos Policy
        - Local Policies
          - Audit Policy
          - User Rights Assignment
          - Security Options
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System
        - Wired Network (IEEE 802.3) Policies
        - Windows Firewall with Advanced Security
          - Windows Firewall with Advanced Security - LDAP://C
            - Inbound Rules
            - Outbound Rules
            - Connection Security Rules
        - Network List Manager Policies
        - Wireless Network (IEEE 802.11) Policies
        - Public Key Policies
        - Software Restriction Policies
        - Network Access Protection
        - Application Control Policies
        - IP Security Policies on Active Directory (RWVDEV.INTRA)
        - Advanced Audit Policy Configuration
      - Policy-based QoS
    - Administrative Templates: Policy definitions (ADMX files) retrieve
  - Preferences

Windows Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile

Windows F

Private Pro

Windows F

Public Prof

Windows F

Windows F

Getting Starte

Authenticat

Create connecti ... nticated and protected by usi

Connection

View and c

Create firewall ru ... connection only if it is authenticate ... ections are blocked unless ... match a rule that blocks them.

Inbound R

Outbound

Windows Firewall with Advanced Security - LDAP://CN={8AF0A0E...

Domain Profile | Private Profile | Public Profile | IPsec Settings

Specify behavior for when a computer is connected to its corporate domain.

State

Firewall state: Off

Inbound connections: Not configured

Outbound connections: Not configured

Settings

Specify settings that control Windows Firewall behavior. Customize...

Logging

Specify logging settings for troubleshooting. Customize...

Learn more about these settings

OK | Cancel | Apply

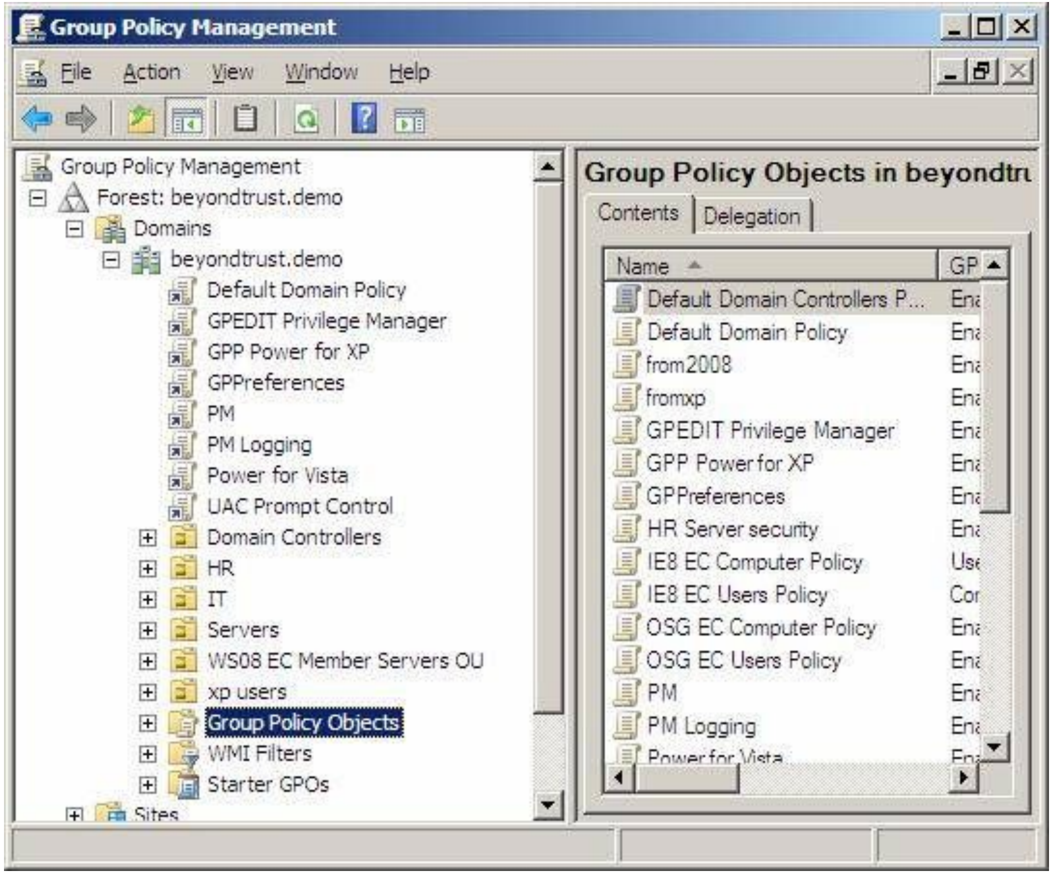
Group Policy

Key terms:

- Enforced
  - Can not be overwritten by other policy
- Linked
  - Link policy to specific OU
- Filtering
  - Can choose to apply Group policy to computers that meet criteria
  - < 4GB RAM
- Group Policy Object
  - A set of rules that can be applied to a network object

Multiple Group Policies

- Can have many sets of policies
- Helps keep network organized
- Different rules for each department or group



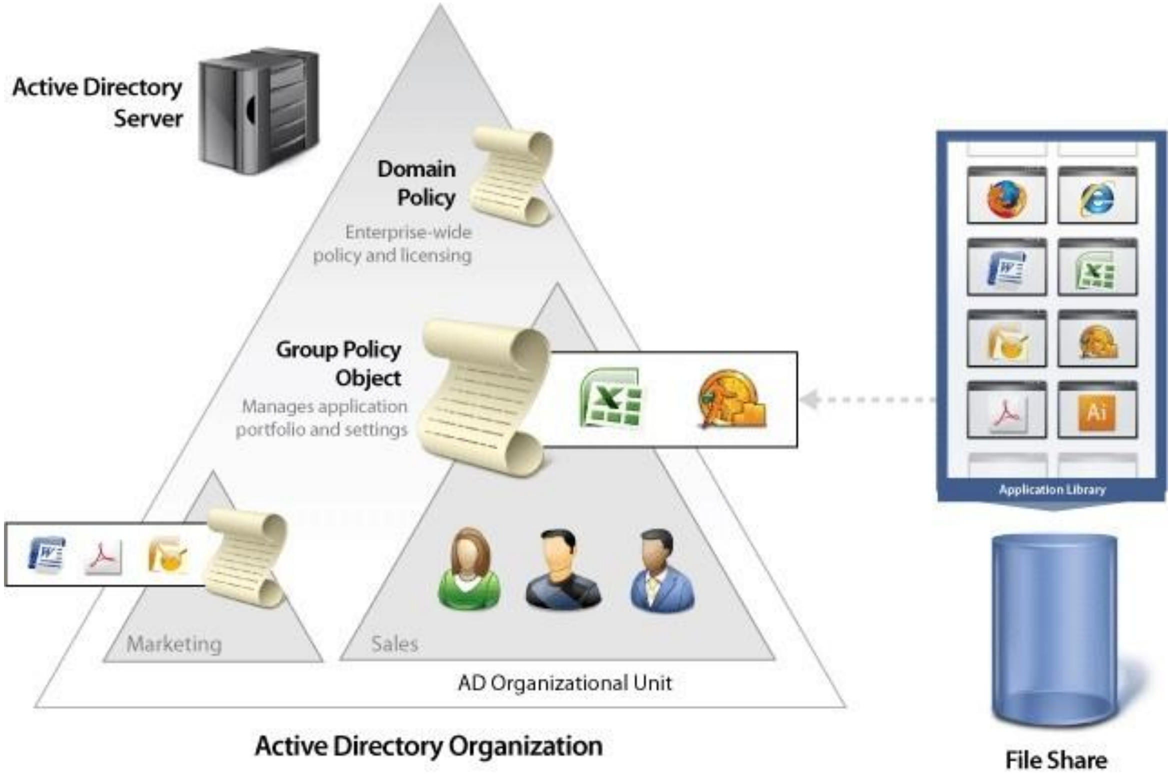
- Group Policy Management
  - Forest: beyondtrust.demo
    - Domains
      - beyondtrust.demo
        - Default Domain Policy
        - GPEDIT Privilege Manager
        - GPP Power for XP
        - GPPreferences
        - PM
        - PM Logging
        - Power for Vista
        - UAC Prompt Control
        - Domain Controllers
        - HR
        - IT
        - Servers
        - WS08 EC Member Servers OU
        - xp users
        - Group Policy Objects
        - WMI Filters
        - Starter GPOs
    - Sites

Group Policy Objects in beyondtru

Name	GP
Default Domain Controllers P...	Ena
Default Domain Policy	Ena
from2008	Ena
fromxp	Ena
GPEDIT Privilege Manager	Ena
GPP Power for XP	Ena
GPPreferences	Ena
HR Server security	Ena
IE8 EC Computer Policy	Use
IE8 EC Users Policy	Cor
OSG EC Computer Policy	Ena
OSG EC Users Policy	Ena
PM	Ena
PM Logging	Ena
Power for Vista	Ena

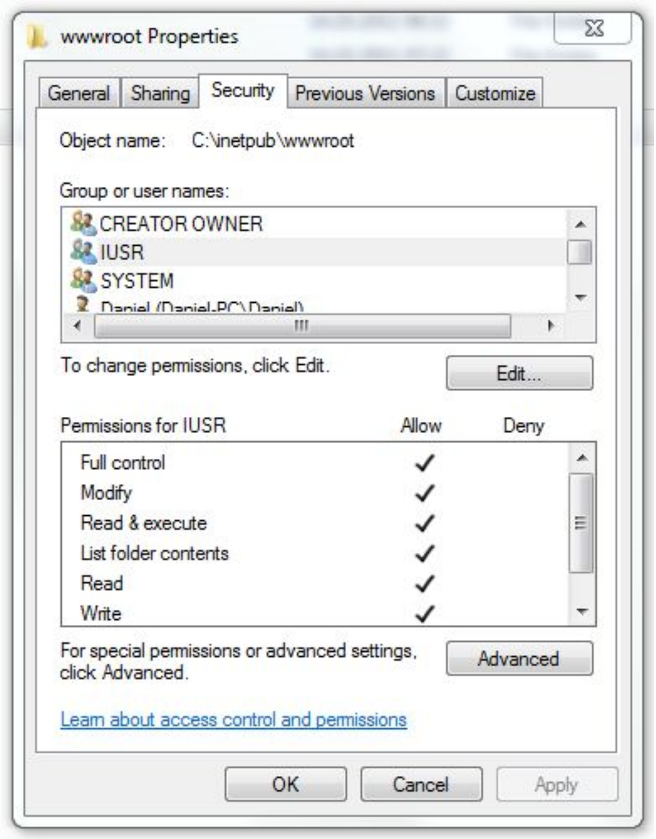
Active directory and Group Policy

- Some the the most powerful tools for an admin
- Can be used together to control 90% of functions
- Organization is key



File Permissions

- Can be set on individual files, folders, network shares, hard drives
- Can specify who has read, write, or modify permissions
- File permissions can be inherited from containing folder
- Ex) Can share whole folder instead of every file
- Can be set using group policy and Active Directory



Object name: C:\inetpub\wwwroot

Group or user names:

- CREATOR OWNER
- IUSR
- SYSTEM
- Daniel (Daniel-PC\Daniel)

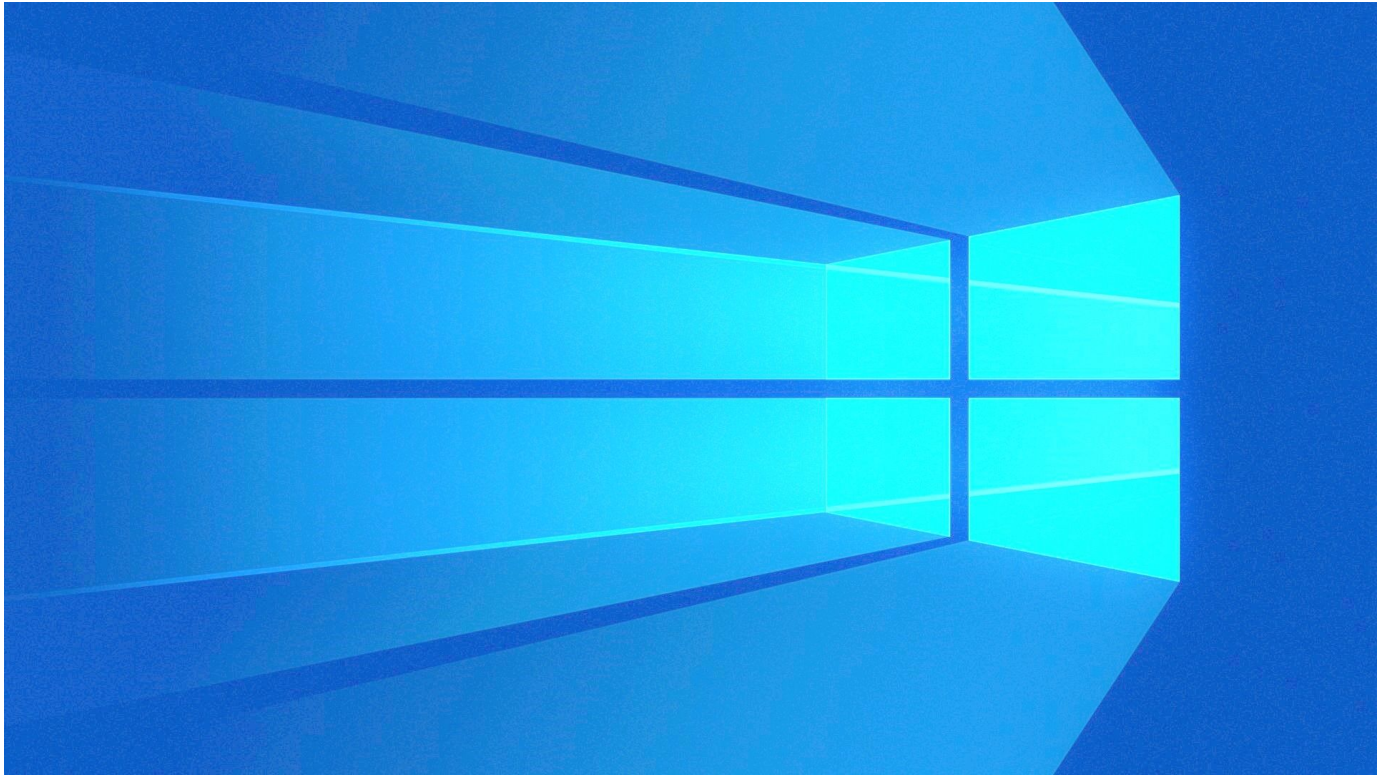
To change permissions, click Edit.

Permissions for IUSR	Allow	Deny
Full control	✓	
Modify	✓	
Read & execute	✓	
List folder contents	✓	
Read	✓	
Write	✓	

For special permissions or advanced settings, click Advanced.

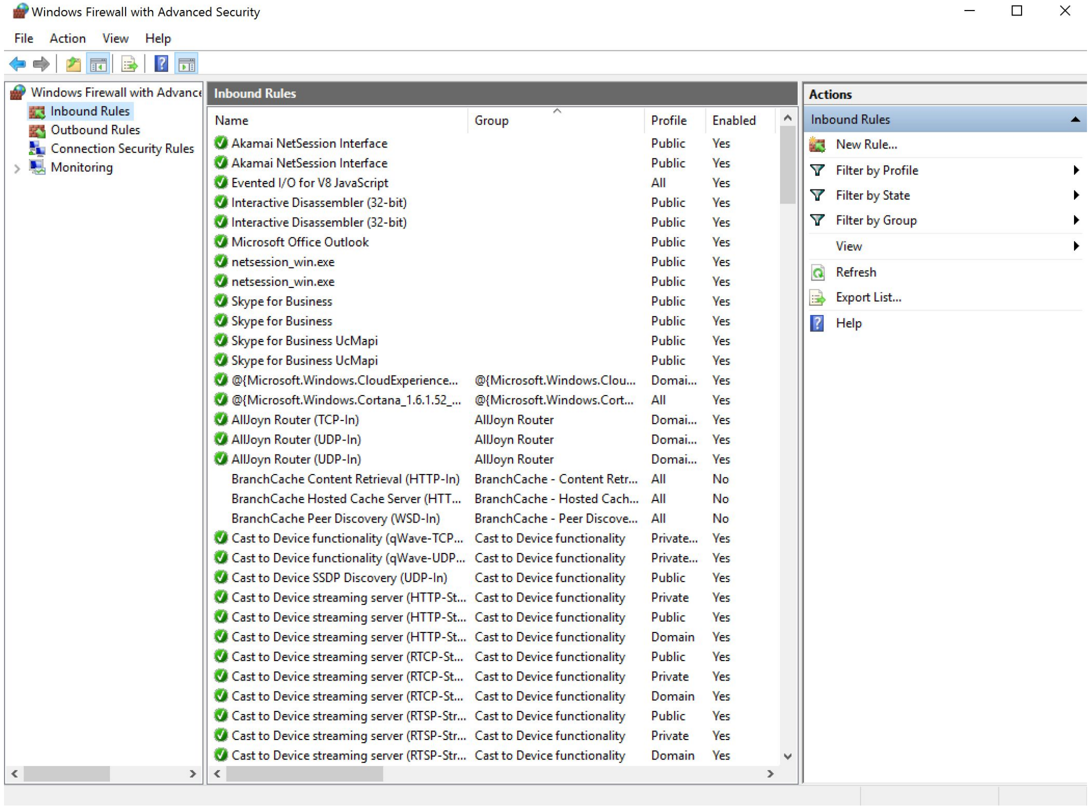
Learn about access control and permissions

More Windows!



Windows Firewalls

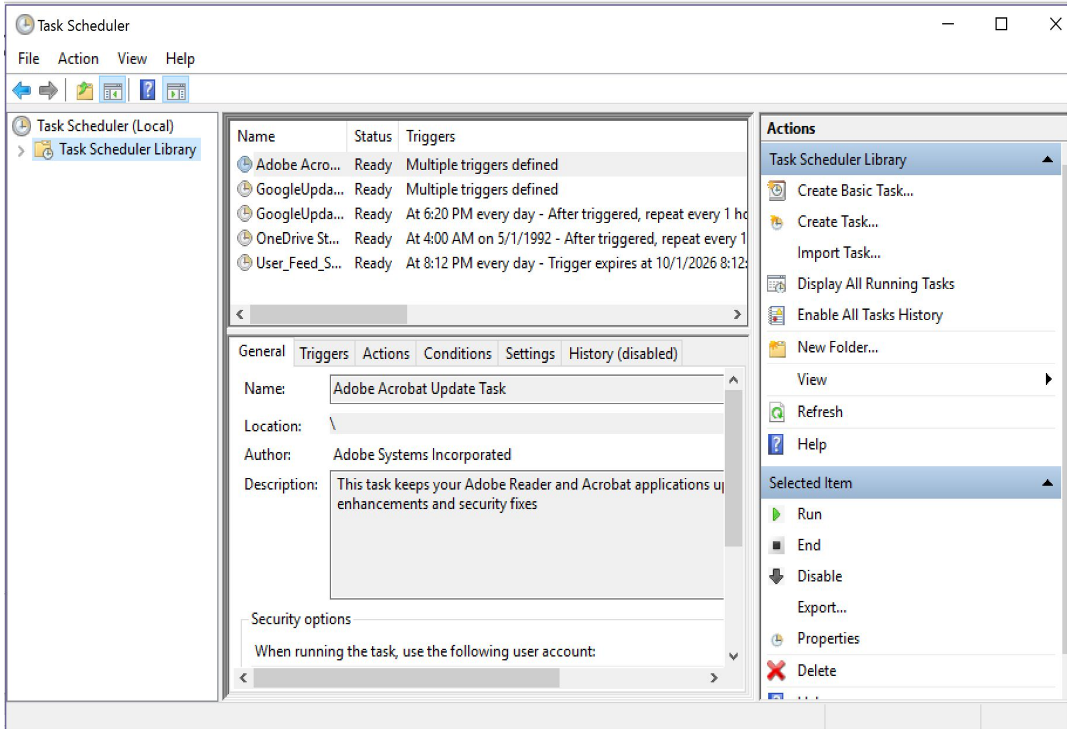
- Does not act like Linux
- Order does not matter
- Can block specific EXE’s, ports, or services
- Can specify which network to block on
    - Domain
    - Public
    - Private



Name	Group	Profile	Enabled
✓ Akamai NetSession Interface		Public	Yes
✓ Akamai NetSession Interface		Public	Yes
✓ Evented I/O for V8 JavaScript		All	Yes
✓ Interactive Disassembler (32-bit)		Public	Yes
✓ Interactive Disassembler (32-bit)		Public	Yes
✓ Microsoft Office Outlook		Public	Yes
✓ netsession_win.exe		Public	Yes
✓ netsession_win.exe		Public	Yes
✓ Skype for Business		Public	Yes
✓ Skype for Business		Public	Yes
✓ Skype for Business UcMapi		Public	Yes
✓ Skype for Business UcMapi		Public	Yes
✓ @{Microsoft.Windows.CloudExperience...	@{Microsoft.Windows.Clou...	Domai...	Yes
✓ @{Microsoft.Windows.Cortana_1.6.1.52_...	@{Microsoft.Windows.Cort...	All	Yes
✓ AllJoyn Router (TCP-In)	AllJoyn Router	Domai...	Yes
✓ AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes
✓ AllJoyn Router (UDP-In)	AllJoyn Router	Domai...	Yes
BranchCache Content Retrieval (HTTP-In)	BranchCache - Content Retr...	All	No
BranchCache Hosted Cache Server (HTT...	BranchCache - Hosted Cach...	All	No
BranchCache Peer Discovery (WSD-In)	BranchCache - Peer Discove...	All	No
✓ Cast to Device functionality (qWave-TCP...	Cast to Device functionality	Private...	Yes
✓ Cast to Device functionality (qWave-UDP...	Cast to Device functionality	Private...	Yes
✓ Cast to Device SSDP Discovery (UDP-In)	Cast to Device functionality	Public	Yes
✓ Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Private	Yes
✓ Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Public	Yes
✓ Cast to Device streaming server (HTTP-St...	Cast to Device functionality	Domain	Yes
✓ Cast to Device streaming server (RTCP-St...	Cast to Device functionality	Public	Yes
✓ Cast to Device streaming server (RTCP-St...	Cast to Device functionality	Private	Yes
✓ Cast to Device streaming server (RTCP-St...	Cast to Device functionality	Domain	Yes
✓ Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Public	Yes
✓ Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Private	Yes
✓ Cast to Device streaming server (RTSP-Str...	Cast to Device functionality	Domain	Yes

Task Scheduler

- Can be used to automate things
- Run at time intervals
- Run at specific events
- Run at startup
- Watch out for bad things, but use this for good things
- Use at work for backups



Name	Status	Triggers
Adobe Acro...	Ready	Multiple triggers defined
GoogleUpda...	Ready	Multiple triggers defined
GoogleUpda...	Ready	At 6:20 PM every day - After triggered, repeat every 1 ho
OneDrive St...	Ready	At 4:00 AM on 5/1/1992 - After triggered, repeat every 1
User_Feed_S...	Ready	At 8:12 PM every day - Trigger expires at 10/1/2026 8:12:

Name: Adobe Acrobat Update Task

Location: \

Author: Adobe Systems Incorporated

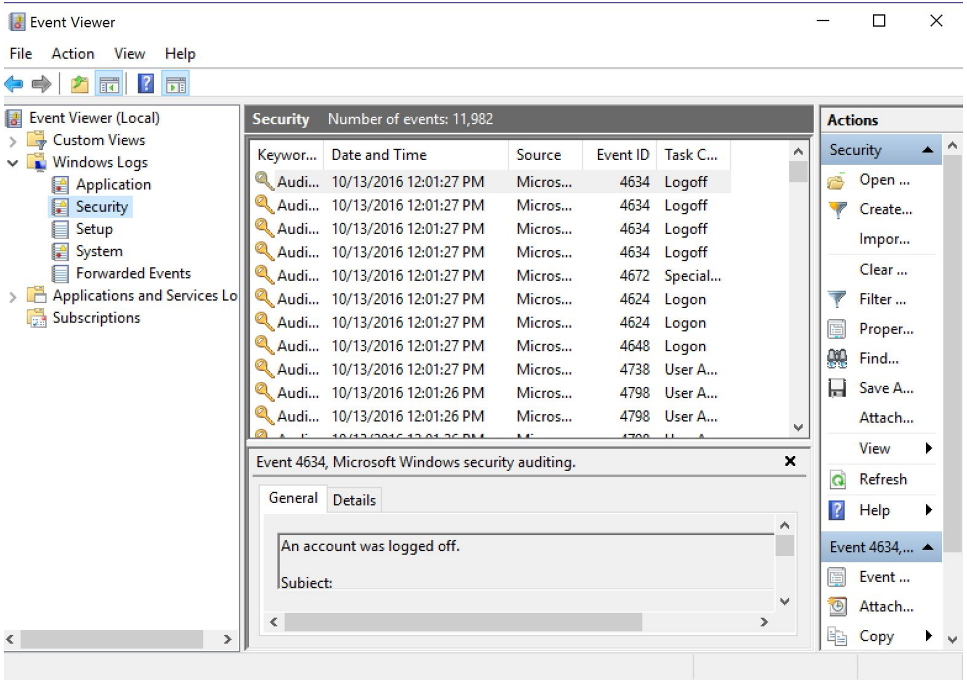
Description: This task keeps your Adobe Reader and Acrobat applications u enhancements and security fixes

Security options

When running the task, use the following user account:

Event Viewer

- Monitors all system and application events
- Can be overwhelming
- Useful for troubleshooting
- Useful for looking for bad guys
- Centralized logging
    - Can send all logs to one server, aggregate data for analysis



Security Number of events: 11,982

Keywor...	Date and Time	Source	Event ID	Task C...
Audi...	10/13/2016 12:01:27 PM	Micros...	4634	Logoff
Audi...	10/13/2016 12:01:27 PM	Micros...	4634	Logoff
Audi...	10/13/2016 12:01:27 PM	Micros...	4634	Logoff
Audi...	10/13/2016 12:01:27 PM	Micros...	4634	Logoff
Audi...	10/13/2016 12:01:27 PM	Micros...	4672	Special...
Audi...	10/13/2016 12:01:27 PM	Micros...	4624	Logon
Audi...	10/13/2016 12:01:27 PM	Micros...	4624	Logon
Audi...	10/13/2016 12:01:27 PM	Micros...	4648	Logon
Audi...	10/13/2016 12:01:27 PM	Micros...	4738	User A...
Audi...	10/13/2016 12:01:26 PM	Micros...	4798	User A...
Audi...	10/13/2016 12:01:26 PM	Micros...	4798	User A...

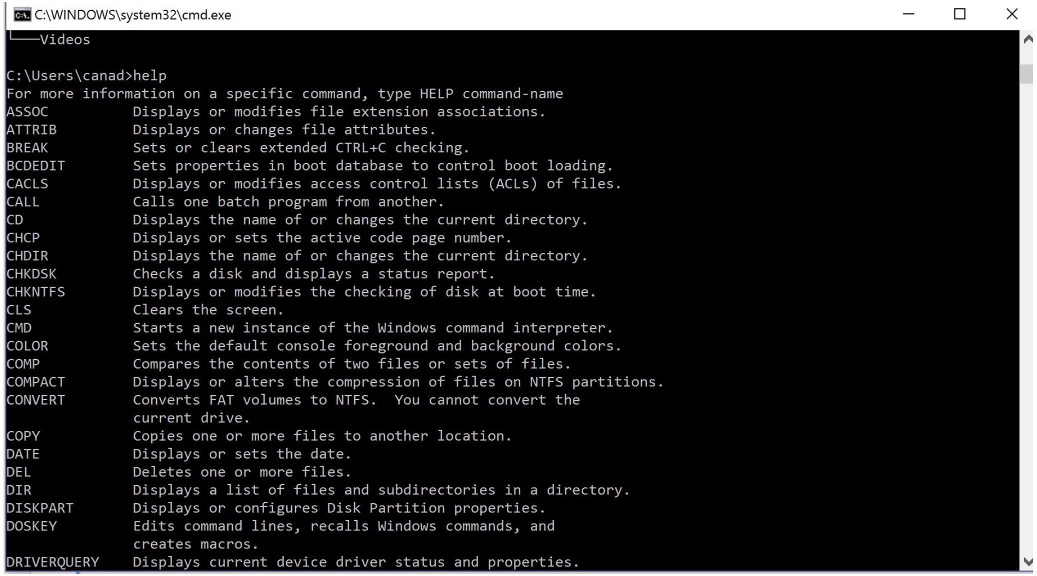
Event 4634, Microsoft Windows security auditing.

An account was logged off.

Subject:

Command line

- Basic windows commands
  - Ipconfig (Not Ifconfig!!!!)
  - Ping
  - Nslookup
  - Cd
  - Tracert
  - Tree
  - help



```
└───Videos

C:\Users\canad>help
For more information on a specific command, type HELP command-name
ASSOC          Displays or modifies file extension associations.
ATTRIB         Displays or changes file attributes.
BREAK          Sets or clears extended CTRL+C checking.
BCDEDIT        Sets properties in boot database to control boot loading.
CACLS          Displays or modifies access control lists (ACLs) of files.
CALL           Calls one batch program from another.
CD             Displays the name of or changes the current directory.
CHCP           Displays or sets the active code page number.
CHDIR          Displays the name of or changes the current directory.
CHKDSK         Checks a disk and displays a status report.
CHKNTFS        Displays or modifies the checking of disk at boot time.
CLS            Clears the screen.
CMD            Starts a new instance of the Windows command interpreter.
COLOR          Sets the default console foreground and background colors.
COMP           Compares the contents of two files or sets of files.
COMPACT        Displays or alters the compression of files on NTFS partitions.
CONVERT        Converts FAT volumes to NTFS.  You cannot convert the
               current drive.
COPY           Copies one or more files to another location.
DATE           Displays or sets the date.
DEL            Deletes one or more files.
DIR            Displays a list of files and subdirectories in a directory.
DISKPART       Displays or configures Disk Partition properties.
DOSKEY         Edits command lines, recalls Windows commands, and
               creates macros.
DRIVERQUERY    Displays current device driver status and properties.
```

Powershell

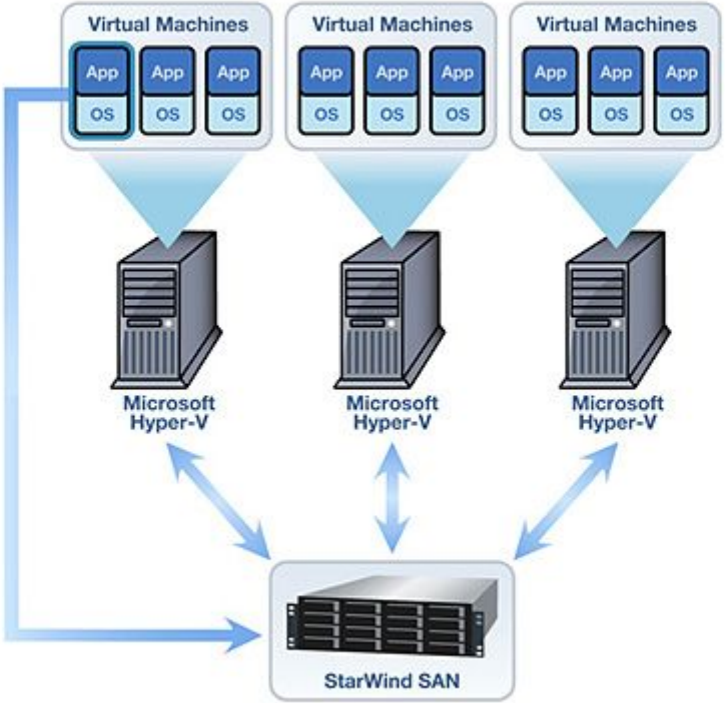
- Can do anything using powershell that you can do using GUI
- Just need to find the right commands
- Can create user and add them to group

```
Install-User -Username "User" -Description "LocalAdmin" -FullName "Local Admin by Powershell" -Password "Password01"
Add-GroupMember -Name 'Administrators' -Member 'User'
```

- Google is your friend

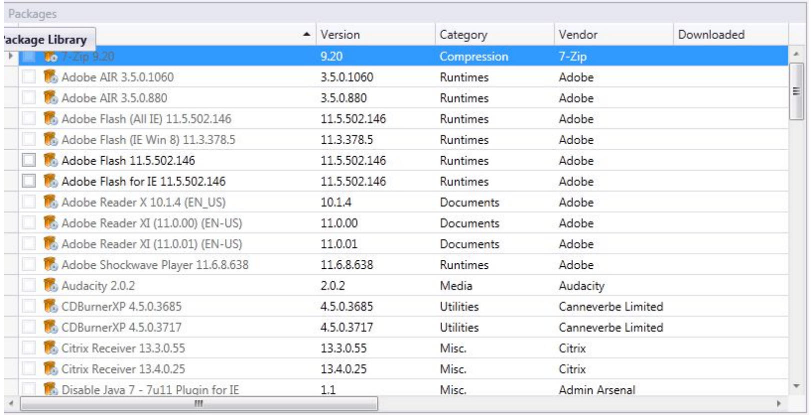
Virtualization

- Hyper-V is windows hypervisor
- Useful for segmentation of services
- Backup DC- probably don't want to virtualize



Windows Admin Tools

- View open folders and files
  - Can be useful for troubleshooting a locked file
  - Can be useful for keeping attackers out
- Storage spaces
  - Software raid
- WSUS
  - Centralized windows updates
- Application deployment
  - PDQ deploy
  - Uses powershell to push out applications
- Process explorer
  - Dive deeper into whats running

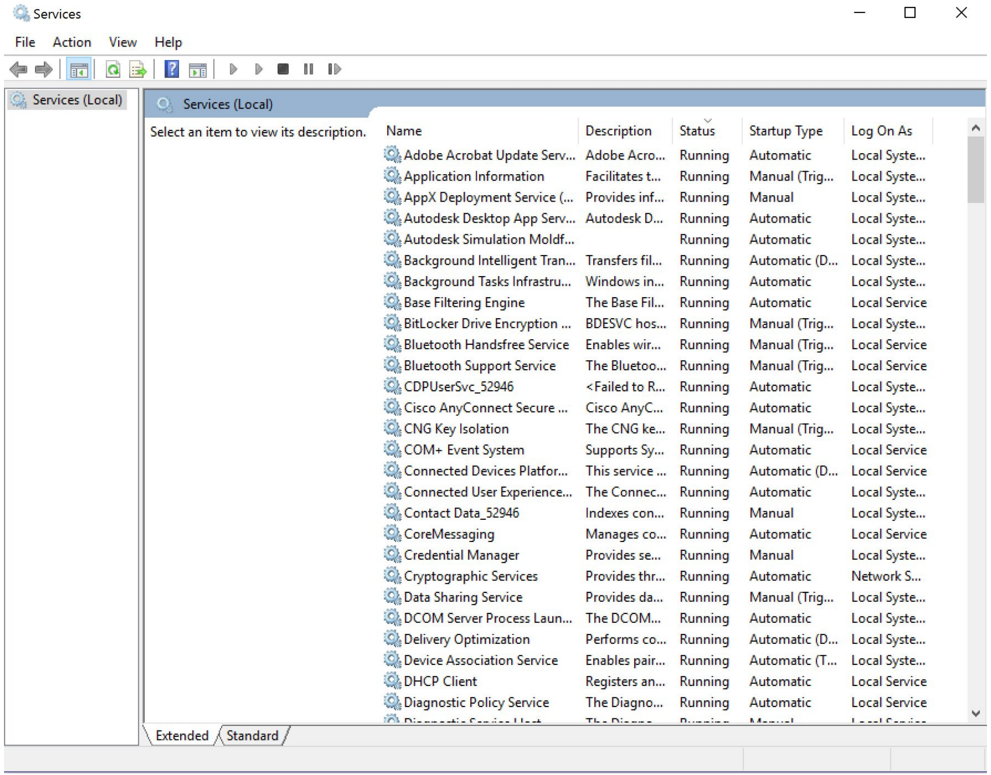


	Version	Category	Vendor	Downloaded
7-Zip 9.20	9.20	Compression	7-Zip	
Adobe AIR 3.5.0.1060	3.5.0.1060	Runtimes	Adobe	
Adobe AIR 3.5.0.880	3.5.0.880	Runtimes	Adobe	
Adobe Flash (All IE) 11.5.502.146	11.5.502.146	Runtimes	Adobe	
Adobe Flash (IE Win 8) 11.3.378.5	11.3.378.5	Runtimes	Adobe	
Adobe Flash 11.5.502.146	11.5.502.146	Runtimes	Adobe	
Adobe Flash for IE 11.5.502.146	11.5.502.146	Runtimes	Adobe	
Adobe Reader X 10.1.4 (EN_US)	10.1.4	Documents	Adobe	
Adobe Reader XI (11.0.00) (EN-US)	11.0.00	Documents	Adobe	
Adobe Reader XI (11.0.01) (EN-US)	11.0.01	Documents	Adobe	
Adobe Shockwave Player 11.6.8.638	11.6.8.638	Runtimes	Adobe	
Audacity 2.0.2	2.0.2	Media	Audacity	
CDBurnerXP 4.5.0.3685	4.5.0.3685	Utilities	Canneverbe Limited	
CDBurnerXP 4.5.0.3717	4.5.0.3717	Utilities	Canneverbe Limited	
Citrix Receiver 13.3.0.55	13.3.0.55	Misc.	Citrix	
Citrix Receiver 13.4.0.25	13.4.0.25	Misc.	Citrix	
Disable Java 7 - 7u11 Plugin for IE	1.1	Misc.	Admin Arsenal	

Windows Services (not roles and features)

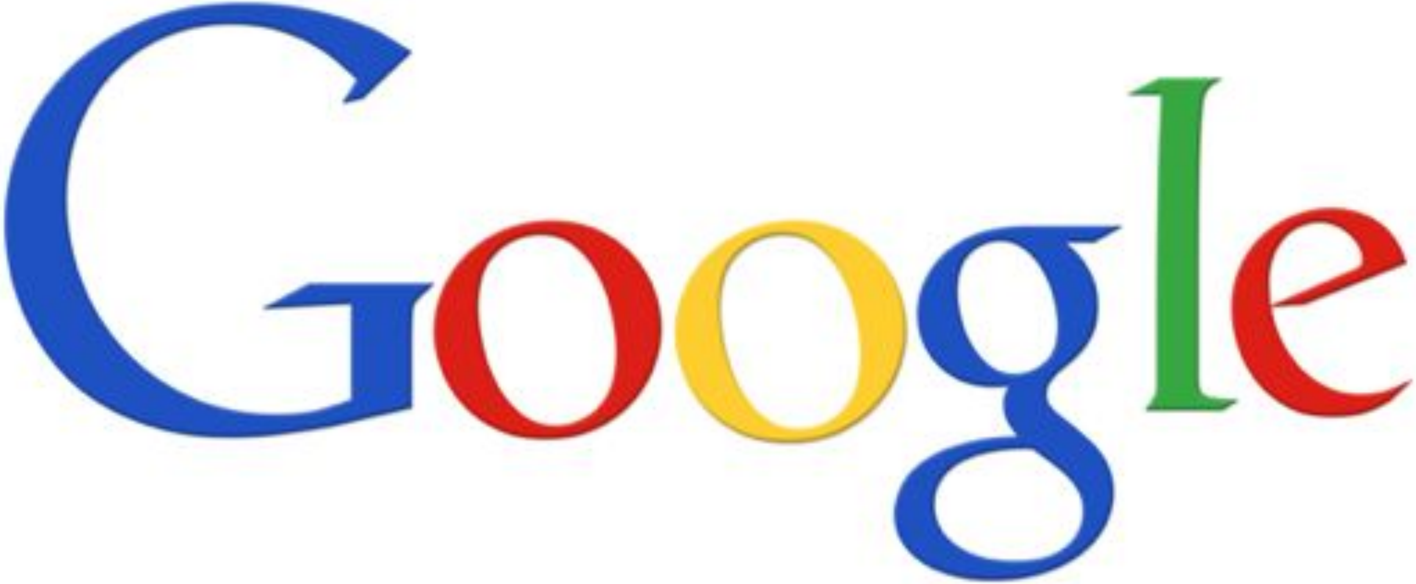
- Are simply long running processes managed by the Windows Service Manager

- Windows services have 5 different states: Start,Stop, Pause, Resume, and Restart



Select an item to view its description.

Name	Description	Status	Startup Type	Log On As
Adobe Acrobat Update Serv...	Adobe Acro...	Running	Automatic	Local Syste...
Application Information	Facilitates t...	Running	Manual (Trig...	Local Syste...
AppX Deployment Service (...	Provides inf...	Running	Manual	Local Syste...
Autodesk Desktop App Serv...	Autodesk D...	Running	Automatic	Local Syste...
Autodesk Simulation Moldf...		Running	Automatic	Local Syste...
Background Intelligent Tran...	Transfers fil...	Running	Automatic (D...	Local Syste...
Background Tasks Infrastru...	Windows in...	Running	Automatic	Local Syste...
Base Filtering Engine	The Base Fil...	Running	Automatic	Local Service
BitLocker Drive Encryption ...	BDESVC hos...	Running	Manual (Trig...	Local Syste...
Bluetooth Handsfree Service	Enables wir...	Running	Manual (Trig...	Local Service
Bluetooth Support Service	The Bluetoo...	Running	Manual (Trig...	Local Service
CDPUserSvc_52946	<Failed to R...	Running	Automatic	Local Syste...
Cisco AnyConnect Secure ...	Cisco AnyC...	Running	Automatic	Local Syste...
CNG Key Isolation	The CNG ke...	Running	Manual (Trig...	Local Syste...
COM+ Event System	Supports Sy...	Running	Automatic	Local Service
Connected Devices Platfor...	This service ...	Running	Automatic (D...	Local Service
Connected User Experience...	The Connec...	Running	Automatic	Local Syste...
Contact Data_52946	Indexes con...	Running	Manual	Local Syste...
CoreMessaging	Manages co...	Running	Automatic	Local Service
Credential Manager	Provides se...	Running	Manual	Local Syste...
Cryptographic Services	Provides thr...	Running	Automatic	Network S...
Data Sharing Service	Provides da...	Running	Manual (Trig...	Local Syste...
DCOM Server Process Laun...	The DCOM...	Running	Automatic	Local Syste...
Delivery Optimization	Performs co...	Running	Automatic (D...	Local Syste...
Device Association Service	Enables pair...	Running	Automatic (T...	Local Syste...
DHCP Client	Registers an...	Running	Automatic	Local Service
Diagnostic Policy Service	The Diagno...	Running	Automatic	Local Service
Diagnostic Service Host	The Diagno...	Running	Manual	Local Service



Google