IT2654: Systems Administration & Security

TOPIC 2: USER & COMPUTER ACCOUNTS

Objectives

- Understand the purpose of user accounts
- Understand the user authentication process
- Understand and configure local, roaming, and mandatory user profiles
- Configure and modify user accounts using different methods
- Troubleshoot user account and authentication problems
- Computer accounts

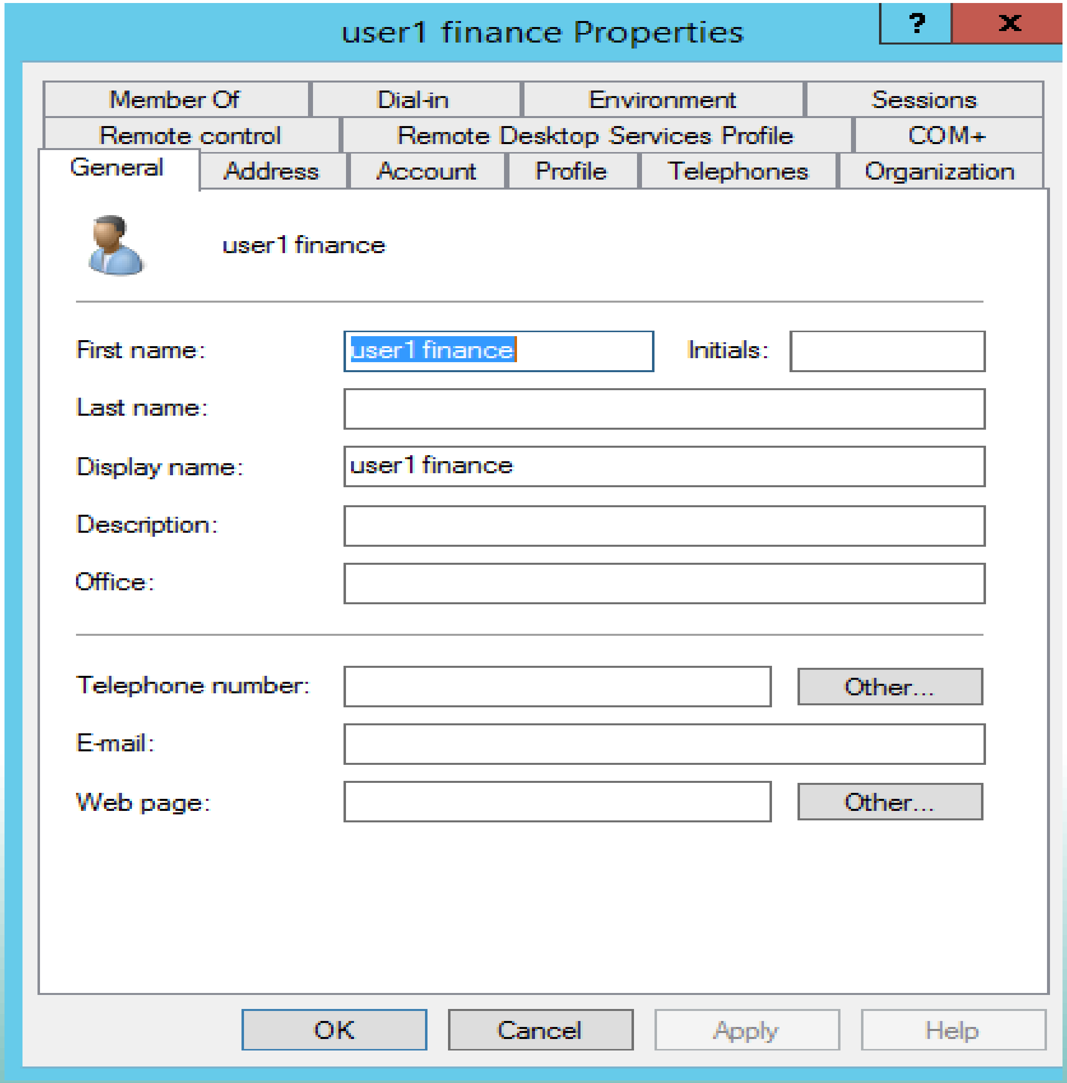
Introduction to User Accounts

- A user account is an Active Directory object
- Represents information that defines a user with access to network (first name, last name, password, etc.)
- Required for anyone using resources on network
- Assists in administration and security
- Must follow organizational standards
  - Last name and first name
  - First name and last name

User Account Properties

- Primary tool for creating and managing accounts is Active Directory Users and Computers
- Active Directory is extensible so additional tabs may be added to property pages
- Major account properties that can be set include:
  - General
  - Address
  - Account
  - Profile
  - Sessions
    - Session parameters for the user utilizing terminal services, such as session time limits, limits on how long a session can be idle …

Properties Associated with User Accounts



user1 finance

First name: user1 finance

Initials:

Last name:

Display name: user1 finance

Description:

Office:

Telephone number:

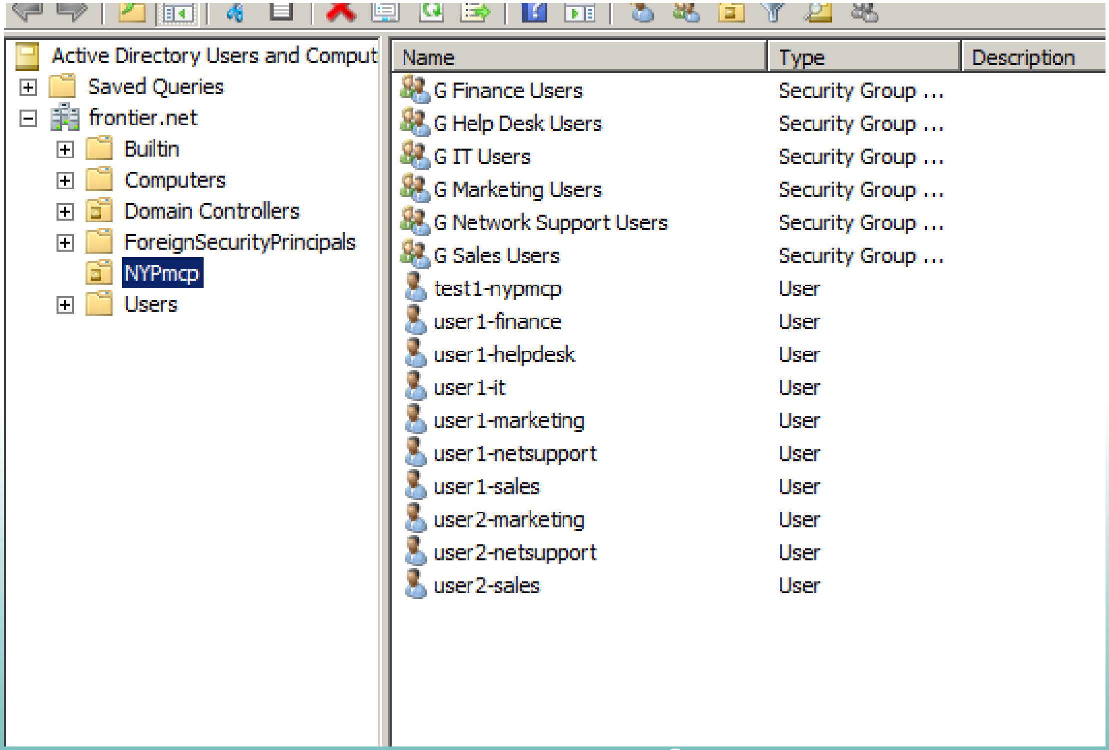
E-mail:

Web page:

Diploma in Infocomm & Security

Creating and Managing User Accounts

- Standard tool is Active Directory Users and Computers
- Also a number of command line tools and utilities



- Active Directory Users and Comput
  - Saved Queries
  - frontier.net
    - Builtin
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - NYPmcp
    - Users

Name	Type	Description
G Finance Users	Security Group ...	
G Help Desk Users	Security Group ...	
G IT Users	Security Group ...	
G Marketing Users	Security Group ...	
G Network Support Users	Security Group ...	
G Sales Users	Security Group ...	
test1-nypmcp	User	
user1-finance	User	
user1-helpdesk	User	
user1-it	User	
user1-marketing	User	
user1-netsupport	User	
user1-sales	User	
user2-marketing	User	
user2-netsupport	User	
user2-sales	User	

Active Directory Users and Computers

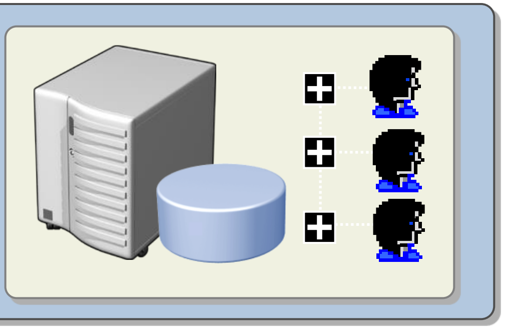
- Available from Server Manager → Tools menu
- Can be added to a Microsoft Management Console (MMC)
- Can be run from command line (dsa.msc)
- Graphical tool
  - Can add, modify, move, delete, search for user accounts
- Can configure multiple objects simultaneously

User Authentication

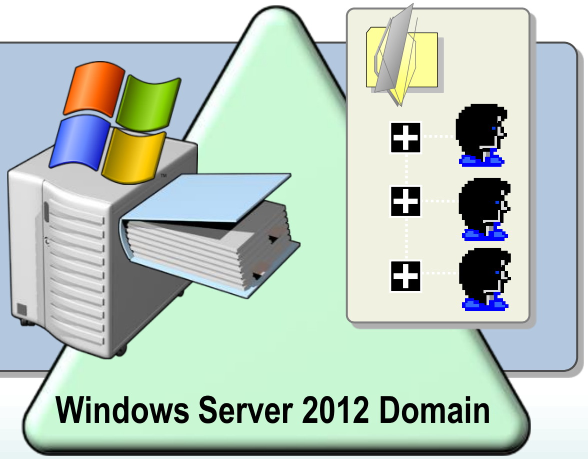
- The process by which a user’s identity is validated
- Used to grant or deny access to network resources
- From a client operating system
  - Name, password, resource required (such as a particular domain or the local computer)
- In Active Directory environment - Domain controller authenticates
- In a Workgroup - Local SAM database authenticates

Local vs. Domain User Account

- **Local user accounts (stored on local computer)**



- **Domain user accounts (stored in Active Directory)**

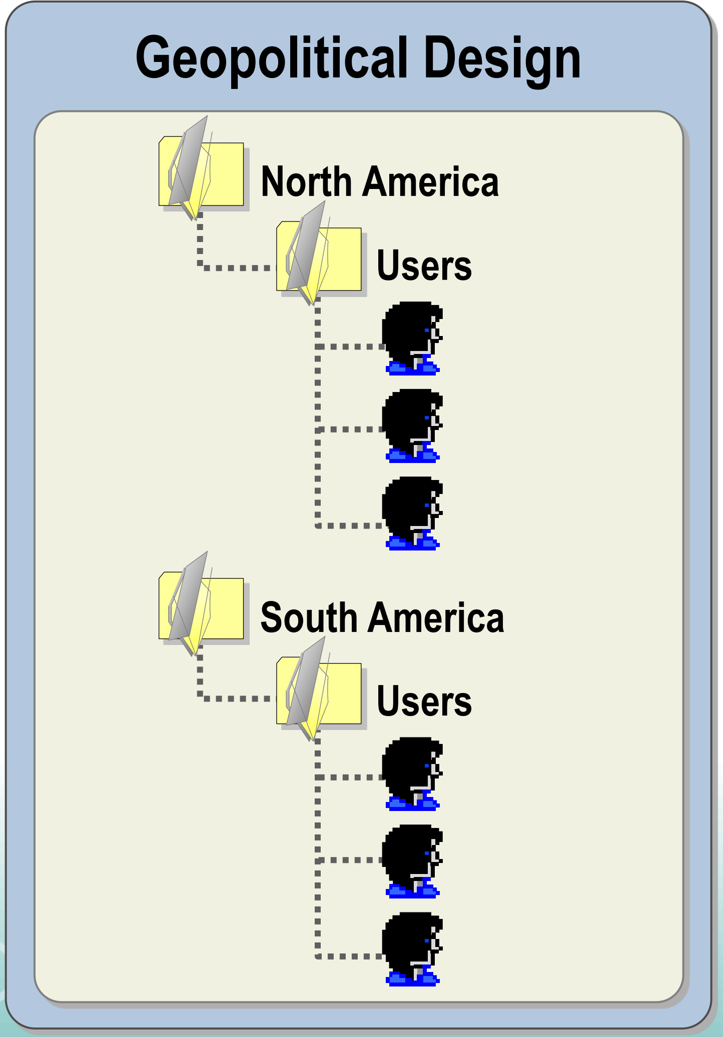


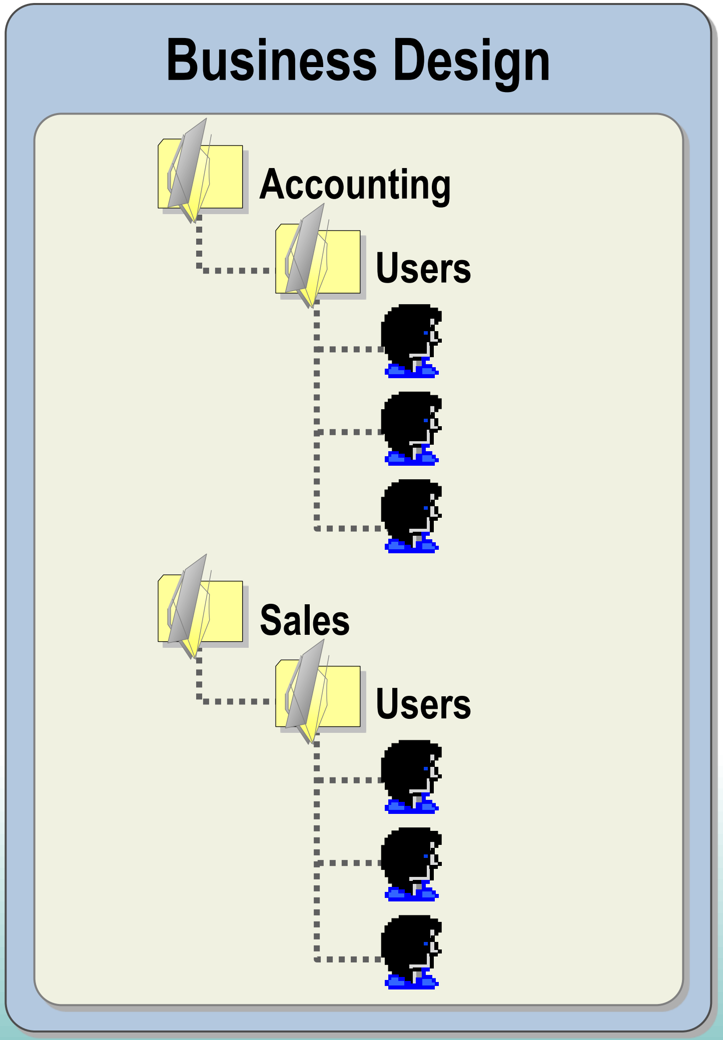
Guidelines for Creating a User Account Naming Convention

A convention for naming user accounts should accommodate:

- Employees with duplicate names
- Different types of employees, such as temporary or contract employees

User Account Placement in a Hierarchy





User Account Password Options

Account options	Description
User must change password at next logon	Users must change their passwords the next time they log on to the network
User cannot change password	A user does not have the permissions to change their own password
Password never expires	A user password is prevented from expiring
Account is disabled	A user cannot log on by using the selected account

When to Require or Restrict Password Changes

Option	Use this option when you:
Require password changes	Create new domain accounts Reset passwords
Restrict password changes	Create local and domain service accounts Create new local accounts that will not log on locally

Best Practices for Creating User Accounts

Best practices for creating local user accounts

- Do not enable the Guest account
- Limit the number of people who can log on locally

Best practices for creating domain user accounts

- Disable an account that will not be used immediately
- Require users to change their passwords the first time that they log on

Authentication Methods

- Two main processes
  - Interactive authentication
    - User account information is supplied at log on
  - Network authentication
    - User’s credentials are confirmed for network access

to continue .....

Interactive Authentication

- The process by which a user provides a user name and password for authentication
- For domain logon, credentials compared to centralized Active Directory database
- For local logon, credentials compared to local SAM database
- In domain environments, users normally don’t have local accounts

Network Authentication

- The process by which a network service confirms the identity of a user
  - Example: access the contents of a shared folder on the network
- For a user who logs on to domain, network authentication is transparent
  - Credentials from interactive authentication valid for network resources
    - Since the user is already authenticated in the domain, they are not prompted to provide their user name and password again.
- A user who logs on to local computer will be prompted to log on to network resource separately

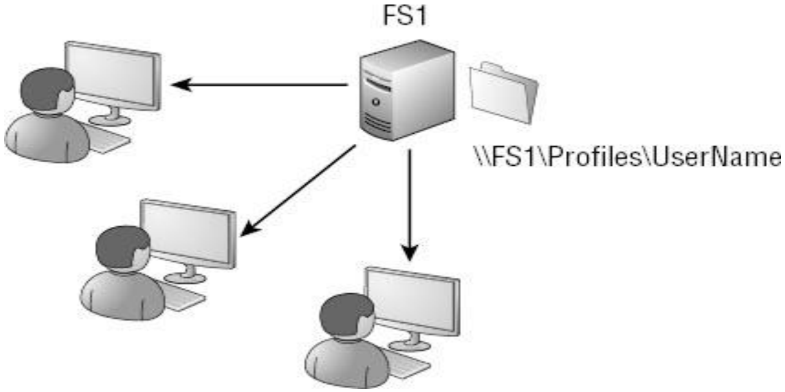
User Profiles

- A collection of settings specific to a particular user
- Stored locally by default
  - Do not follow user logging on to different computers
- Can create a **Roaming** profile
  - Does follow user logging on to different computers
- Administrator can create a **Mandatory** profile
  - User cannot alter it

Local Profiles

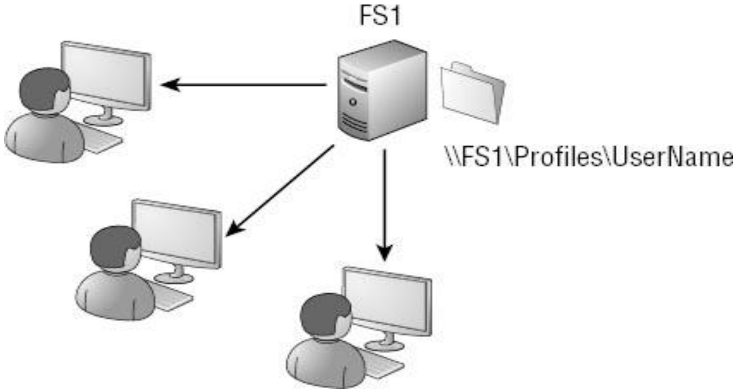
- New profiles are created from Default User profile folder
- User can change local profile and changes are stored uniquely to that user
- Administrator can manage various elements of profile
  - Change Type
  - Delete
  - Copy To

Roaming Profiles



- Roaming profiles
  - Allow a profile to be stored on a central server and follow the user
  - Provide advantage of a single centralized location (helpful for backup)
- Configured from Profiles page of Active Directory Users and Computers
- Changing a profile from local to roaming requires care – should copy first

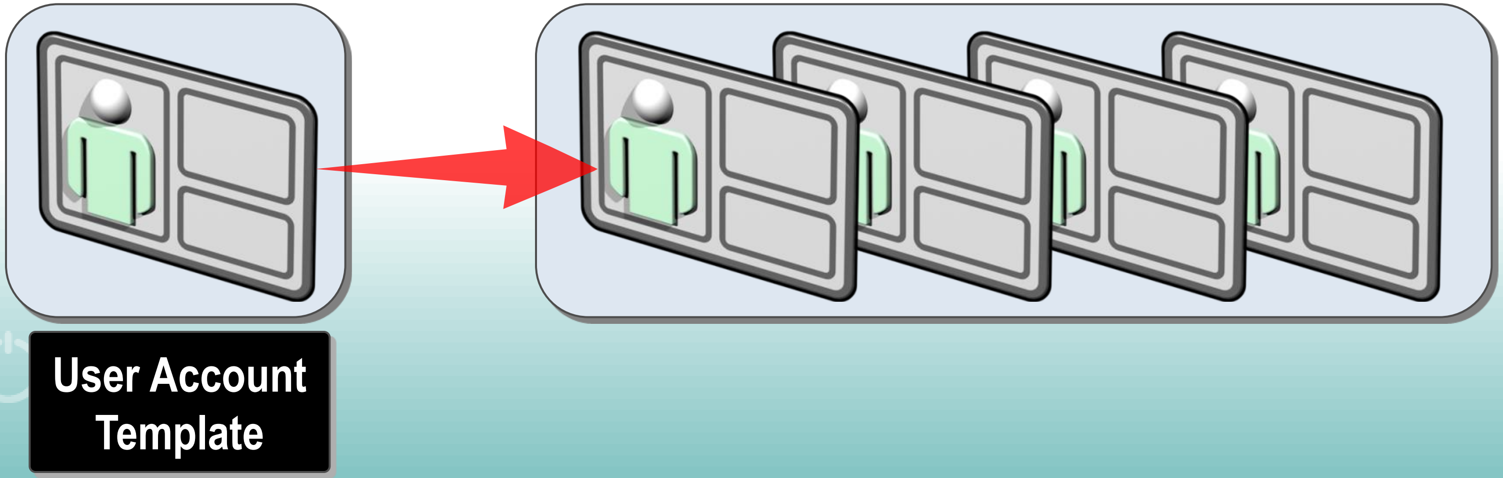
Mandatory Profiles



- Local and roaming profiles allow users to make permanent changes
- Mandatory profiles allow changes only for a single session
- Local and roaming profiles can both be configured as mandatory
  - ntuser.dat → ntuser.man

What Is a User Account Template?

- A user account template is a user account that contains the properties that apply to users with common requirements
- User account templates make creating user accounts with standardized configurations more efficient



Command Line Utilities

- Some administrators prefer working from command line
- Can be used to automate creation or management of accounts more flexibly
- DSADD
- DSMOD
- DSQUERY
- DSMOVE
- DSRM

Key codes From RFC 2253

- DC: Domain Component
  - Specify domain or application partition objects
- CN: Common Name
- L: Locality Name
- ST: State or Province Name
- O: Organization Name
- OU: Organizational Unit Name
- C: Country
- STREET: Street Address
- UID: Userid

Distinguished Name (DN)

- Used to uniquely reference an object in a Directory Information Tree (DIT)
- Example:
  - cn=Administrator, cn=Users, dc=frontier, dc=net
  - cn=it-user1, ou=it, dc=frontier, dc=net
- A relative distinguished name (RDN) is the name used to uniquely reference an object within its parent container in a DIT.
- Example:
  - cn=Administrator

DSADD

- Allows object types to be added to directory
  - Computer accounts, contacts, quotas, OUs, users, etc.
- Syntax for user account is
  - DSADD USER *distinguished-name switches*
- Switches include
  - -pwd (password), -memberof, -email, -profile, -disabled

Example:

```
dsadd user “cn=John Smith,ou=Sales,dc=london,dc=net”
-disabled no –pwd C^h3Bdo9# -mustchpwd yes
```

DSMOD

- Allows object types to be modified from the command line
  - Computer accounts, users, quotas, OUs, servers, etc.
- Syntax for modifying user account is
  - DSMOD USER *distinguished-name*⁺ *switches*⁺
- Can modify multiple accounts simultaneously

Example: To reset the password for Don Funk and force him to change his password when he next logs on to the network

```
dsmod user "CN=Don Funk,CN=Users,DC=Contoso,DC=Com" -pwd A1b2C3d4 -mustchpwd yes
```

DSQUERY

- Allows various object types to be queried from command line
- Supports wildcard (*)
- Output can be redirected to another command (piped)
- Example: return all user accounts that have not changed passwords in 14 days
  - **dsquery user domainroot –name * -stalepwd 14**

DSMOVE

- Allows various object types to be moved from current location to a new location
- Allows various object types to be renamed
- Only moves within the same domain (otherwise use MOVETREE)
- Example: to move a user account into a marketing OU
  - dsmove "cn=Paul Kohut,cn=users,dc=domain01, dc=dovercorp,dc=net" –newparent "ou=marketing, dc=domain01,dc=dovercorp,dc=net"

DSRM

- Allows objects to be deleted from directory
- Can delete single object or entire subtree
- Has a confirm option that can be overridden
- Example: to delete the Marketing OU and all its contained objects without a confirm prompt:
  - dsrm –subtree –noprompt –c "ou=marketing, dc=domain01,dc=dovercorp,dc=net "

Bulk Import and Export

- Allows an organization to import existing stores of data rather than recreating from scratch
- Allows an organization to export data that is already structured in Active Directory to secondary databases
- Two command line utilities for import and export
  - CSVDE
  - LDIFDE

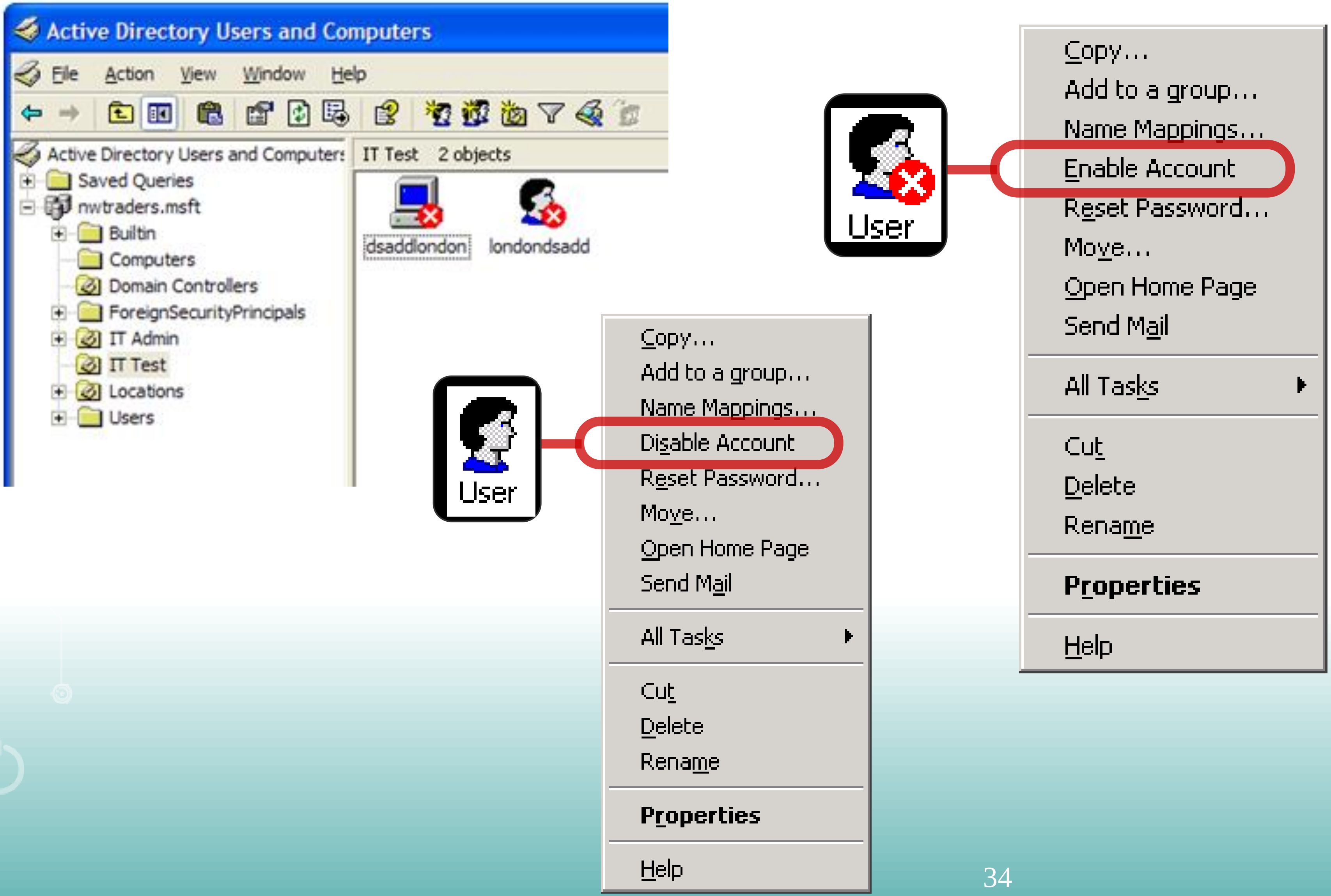
CSVDE

- Command-line tool to bulk export and import Active Directory data to and from Comma-Separated Value (CSV) files
- CSV files can be created/edited using text-based editors
- Example:
  - csvde –f output.csv

LDIFDE

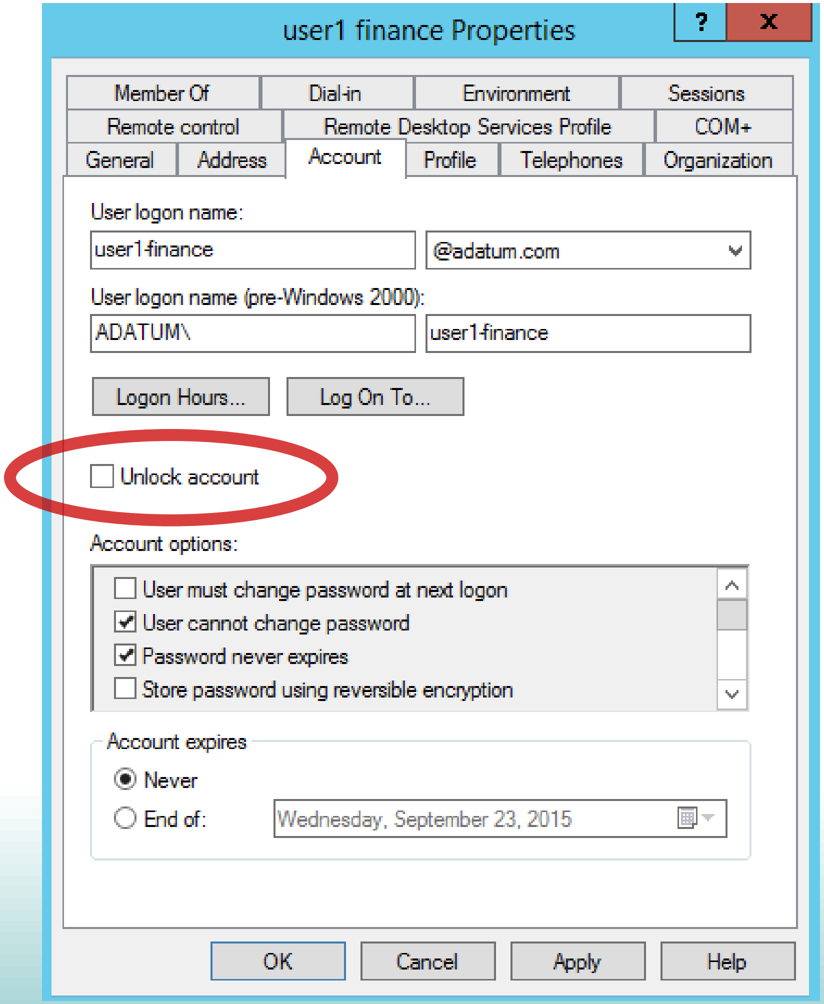
- Command-line tool to bulk export and import Active Directory data to and from LDIF files
  - LDAP Interchange Format
  - Industry standard for information in LDAP directories
  - Each attribute/value on a separate line with blank lines between objects
- Can be read in text-based editors
- Common uses: extending AD schemas, importing bulk data to populate AD, manipulating user and group objects

Enable or Disable User and Computer Accounts



What Are Locked-out User Accounts?

- The account lockout threshold:
  - Defines the number of failed logon attempts
  - Prevents hackers from guessing user passwords
- An account can exceed the account lockout threshold by too many failed logon attempts:
  - At the logon screen
  - At a screen saver protected by a password
  - When accessing network resources



User logon name: user1-finance @adatum.com

User logon name (pre-Windows 2000): ADATUM\ user1-finance

□ Unlock account

Account options:

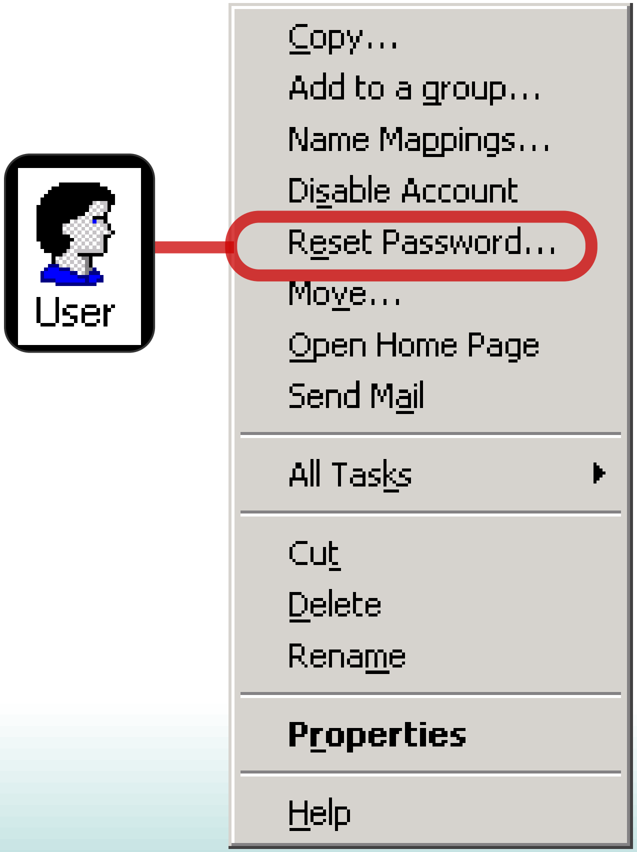
□ User must change password at next logon
☑ User cannot change password
☑ Password never expires
□ Store password using reversible encryption

Account expires

● Never
○ End of: Wednesday, September 23, 2015

When to Reset User Passwords

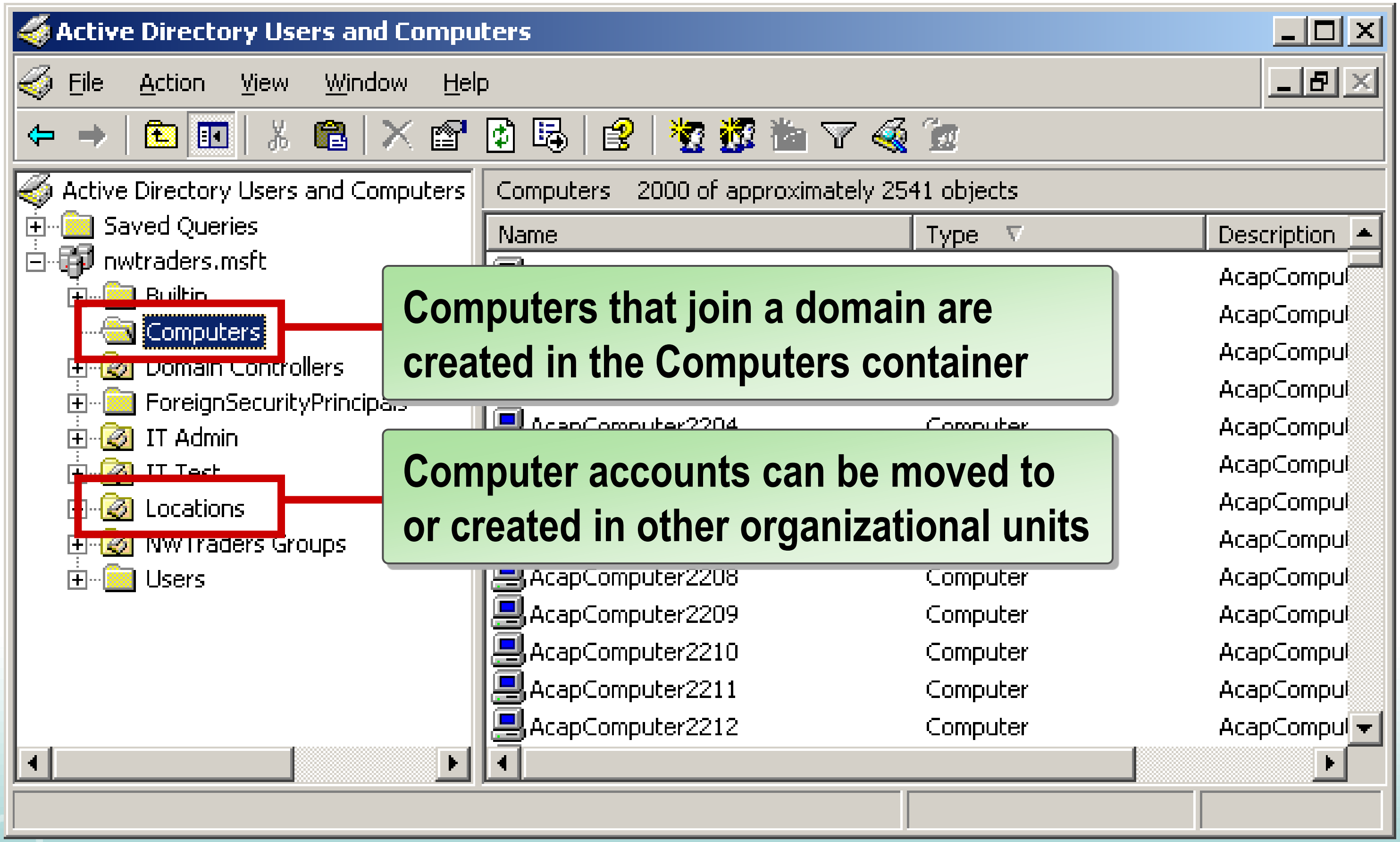
- Reset a password when a user forgets his or her password
- After resetting a password, a user can no longer access some types of information, including:
  - E-mail that is encrypted with the user’s public key
  - Internet passwords that are saved on the computer
  - Files that the user has encrypted



The Computer Account

- ❑ **Identifies a computer in a domain**
  - ✓ **AD requires that all logons not only come from a valid user, but that the logon attempt also comes from a valid computer**
  - ✓ **Domain controller won't accept a user logon, even if it is valid, if it is from a computer that does not belong to the domain**
- ❑ **Provides a means for authenticating and auditing computer access to the network and to domain resources**
- ❑ **Is required for every computer running:**
  - ✓ **Windows Server latest to 2003**
  - ✓ **Windows 8 / 7 / Vista / XP Professional**
  - ✓ **Windows 2000**
  - ✓ **Windows NT**
- ❑ **Assigned when joining a domain**

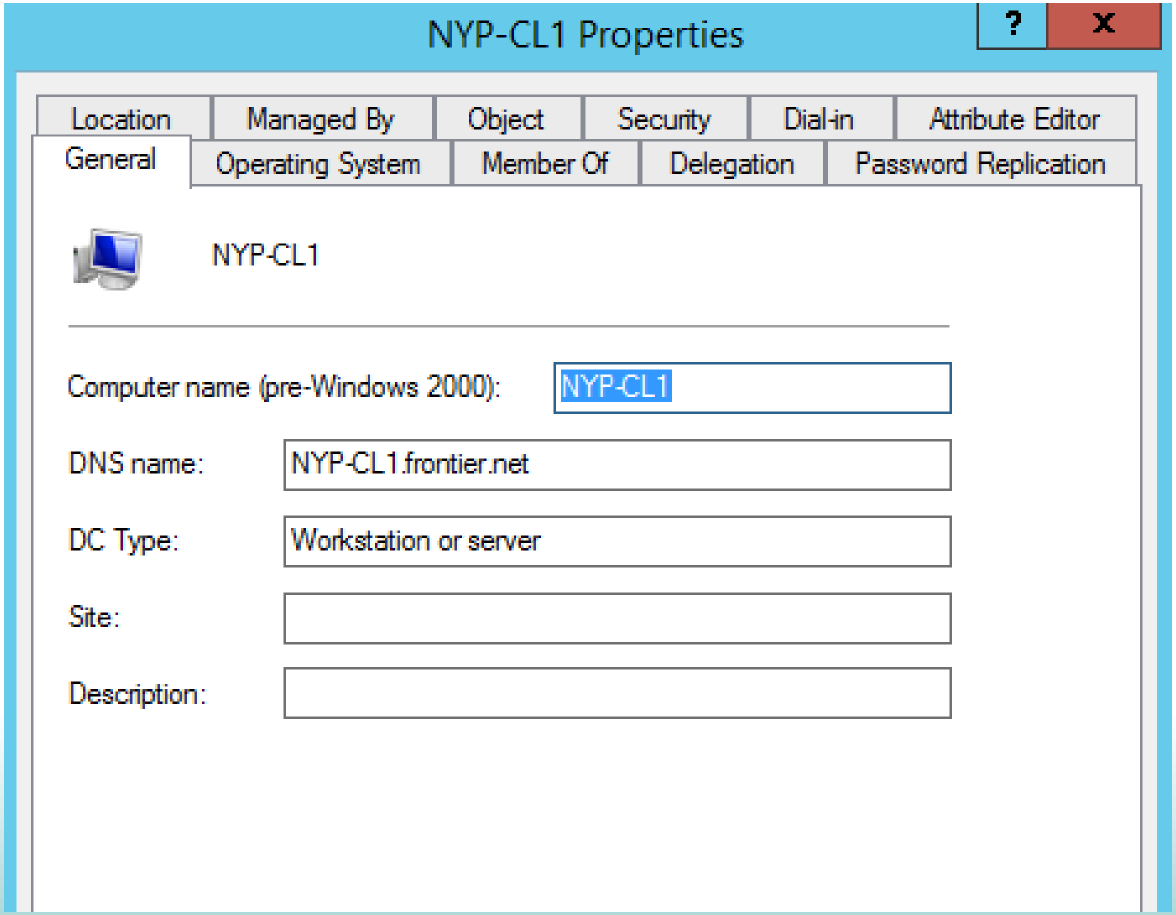
Where Computer Accounts Are Created in a Domain



Computers that join a domain are created in the Computers container

Computer accounts can be moved to or created in other organizational units

Properties Associated with Computer Accounts



NYP-CL1

Computer name (pre-Windows 2000): NYP-CL1

DNS name: NYP-CL1.frontier.net

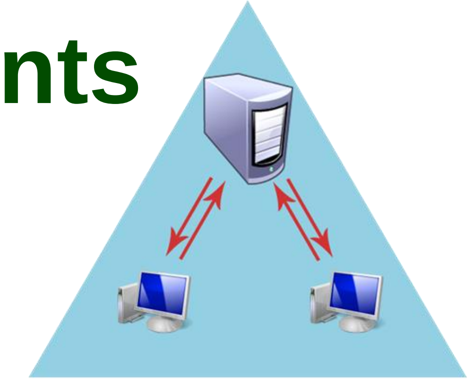
DC Type: Workstation or server

Site:

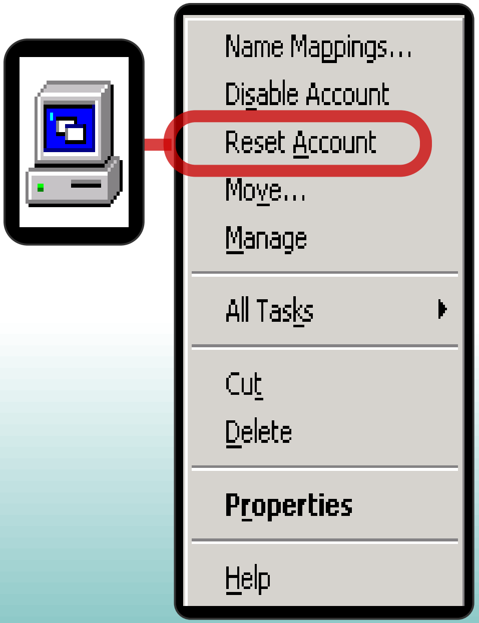
Description:

With Advanced features turned on

Resetting Computer Accounts



- Secure channel
  - Used by computers that are domain members to communicate with domain controller
  - Uses password that is changed every 30 days
  - Automatically synchronized between domain controller and workstation
- Occasional synchronization issues arise
  - Administrator must reset computer account
  - Using Active Directory Users and Computers or Netdom.exe command from Windows Support Tools



Summary

- A user account is an object stored in Active Directory
  - Information that defines user and access to network
- Primary tools to create and manage user accounts
  - Active Directory Users and Computers
  - Command line utilities (DSADD, DSMOD, DSQUERY, DSMOVE, DSRM)
- Two main authentication processes
  - Interactive authentication
  - Network authentication
- User profiles used to configure and customize desktop environment
  - Local, roaming, mandatory
- Utilities for bulk importing and exporting user data to and from Active Directory
  - LDIFDE and CSVDE