Lesson 14: Creating and Managing Active Directory Users and Computers

MOAC 70-410: Installing and Configuring Windows Server 2012

Microsoft® Official Academic Course

WILEY

Overview

- Exam Objective 5.2: Create and Manage Active Directory Users and Computers
- Creating User Objects
- Creating Computer Objects
- Managing Active Directory Objects

Creating User Objects

Lesson 14: Creating and Managing Active Directory Users and Computers

Creating User Objects

- The user account is the primary method for authentication on a network.
- Usernames and passwords are validated at log on by comparing entered information to the information stored in the AD DS database.

Types of Users

- **Local users:** These accounts can only access resources on the local computer and are stored in the local **Security Account Manager (SAM)** database on the computer where they reside.
- **Domain users:** These accounts can access AD DS or network-based resources, such as shared folders and printers.
  - Account information for these users is stored in the AD DS database and replicated to all domain controllers within the same domain.

Built-In User Accounts

Administrator and **Guest**

- **On a member server or standalone server:** The built-in local Administrator account has full control of all files as well as complete management permissions for the local computer.
- **On a domain controller:** The built-in Administrator account created in Active Directory has full control of the domain in which it was created.

The Administrator account cannot be deleted, but it can be renamed.

Administrator Account Security Guidelines

- Rename the Administrator account
- Set a strong password
- Limit knowledge of administrator passwords to only a few people
- Do not use the Administrator account for daily non-administrative tasks

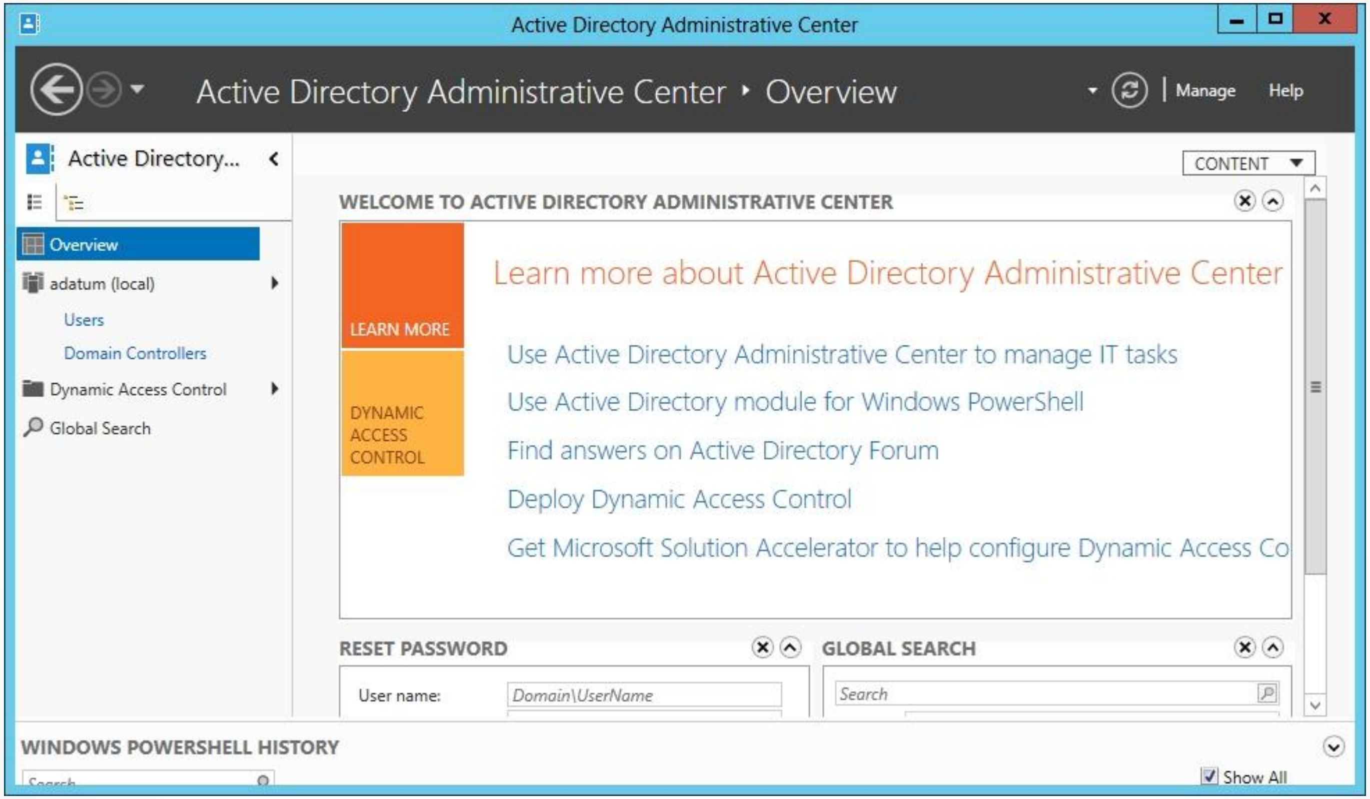
Guest Account

- This built-in account is used to provide temporary access to the network for a user such as a vendor representative or a temporary employee.
- It cannot be deleted, but it can and should be renamed.
- This account is disabled by default and is not assigned a default password.

User Creation Tools

- **Dsadd.exe:** The standard command line tool for creating AD DS leaf objects, which you can use with batch files to create AD DS objects in bulk.
- **Windows PowerShell:** The currently approved Windows maintenance tool, with which you can create object creation scripts of nearly unlimited complexity.
- **Comma-Separated Value Directory Exchange (CSVDE.exe):** A command line utility that can create new AD DS objects by importing information from a comma-separated value (.csv) file.
- **LDAP Data Interchange Format Directory Exchange (LDIFDE.exe):** LikeCSVDE, a utility that can import AD DS information and use it to add, delete, or modify objects, in addition to modifying the schema, if necessary.

Create a User with Active Directory Administrative Center



Learn more about Active Directory Administrative Center

Use Active Directory Administrative Center to manage IT tasks

Use Active Directory module for Windows PowerShell

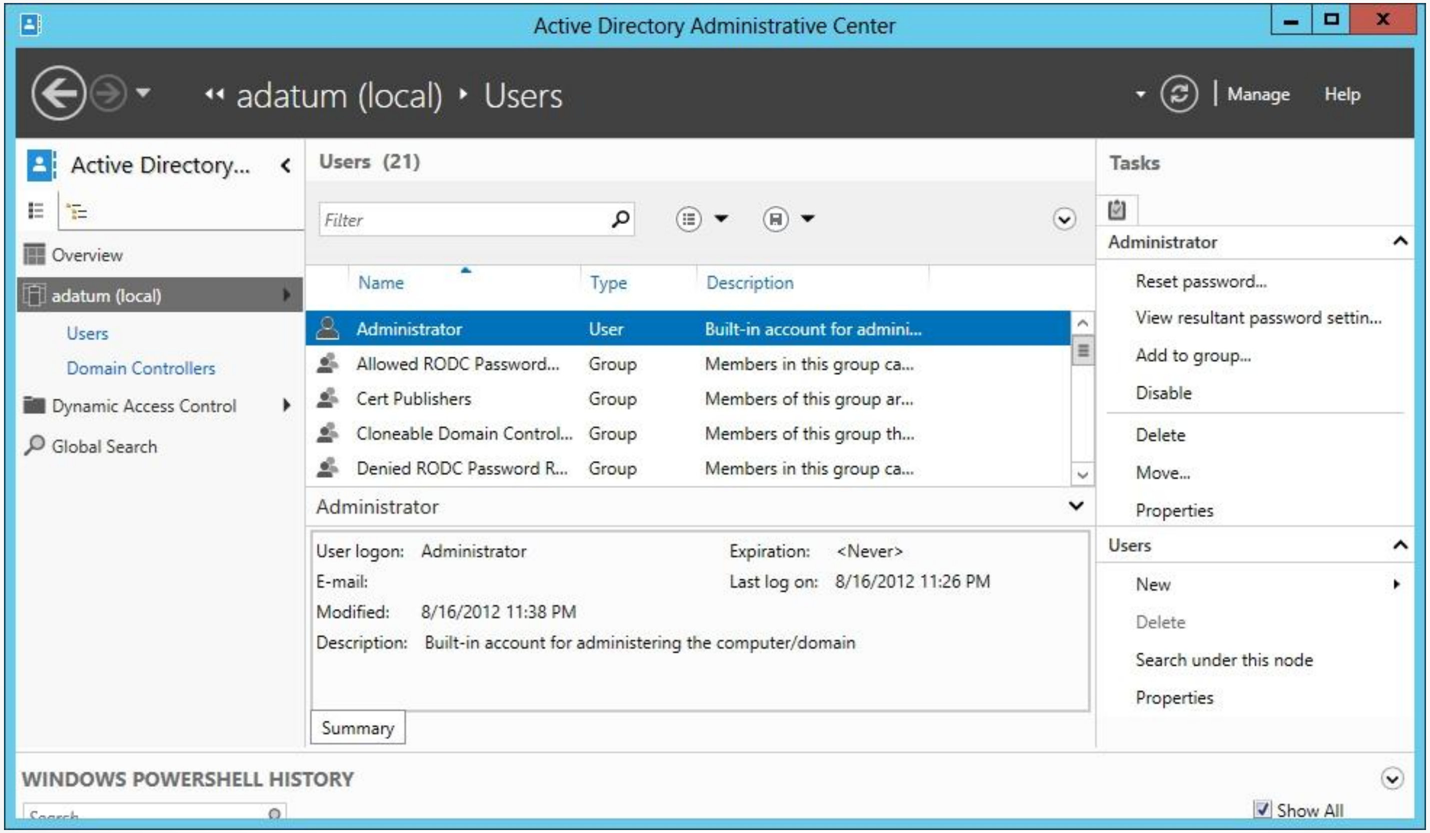
Find answers on Active Directory Forum

Deploy Dynamic Access Control

Get Microsoft Solution Accelerator to help configure Dynamic Access Co

The Active Directory Administrative Center console

Create a User with Active Directory Administrative Center



Users (21)

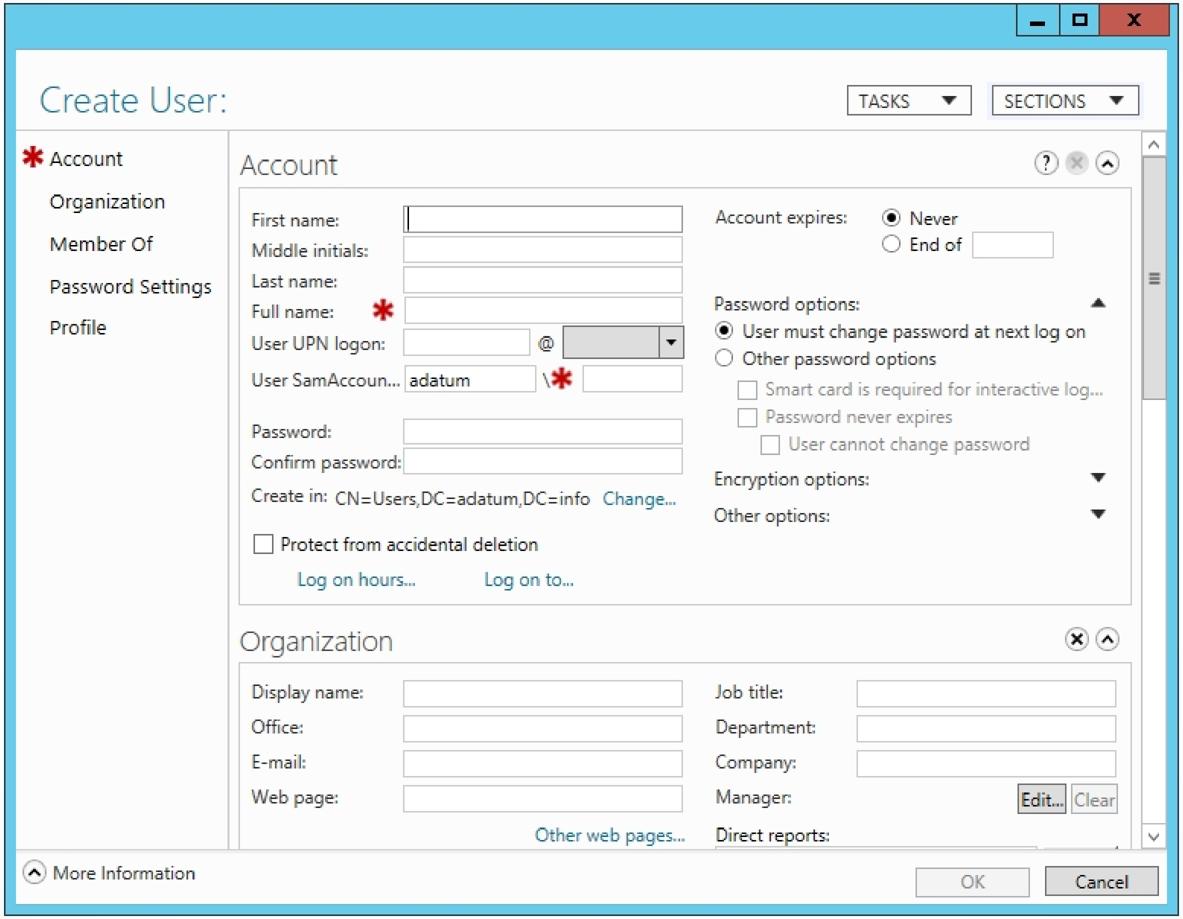
Name	Type	Description
Administrator	User	Built-in account for admini...
Allowed RODC Password...	Group	Members in this group ca...
Cert Publishers	Group	Members of this group ar...
Cloneable Domain Control...	Group	Members of this group th...
Denied RODC Password R...	Group	Members in this group ca...

Administrator

User logon: Administrator
E-mail:
Modified: 8/16/2012 11:38 PM
Description: Built-in account for administering the computer/domain
Expiration: <Never>
Last log on: 8/16/2012 11:26 PM

A container in the Active Directory Administrative Center console

Create a User with Active Directory Administrative Center



Create User:

TASKS ▼ SECTIONS ▼

- * Account
- Organization
- Member Of
- Password Settings
- Profile

Account

First name:

Middle initials:

Last name:

Full name: *

User UPN logon: @

User SamAccoun... adatum \ *

Password:

Confirm password:

Create in: CN=Users,DC=adatum,DC=info Change...

□ Protect from accidental deletion

Log on hours... Log on to...

Account expires: ● Never ○ End of

Password options: ▲

● User must change password at next log on

○ Other password options

□ Smart card is required for interactive log...

□ Password never expires

□ User cannot change password

Encryption options: ▼

Other options: ▼

Organization

Display name:

Office:

E-mail:

Web page:

Other web pages...

Job title:

Department:

Company:

Manager: Edit... Clear

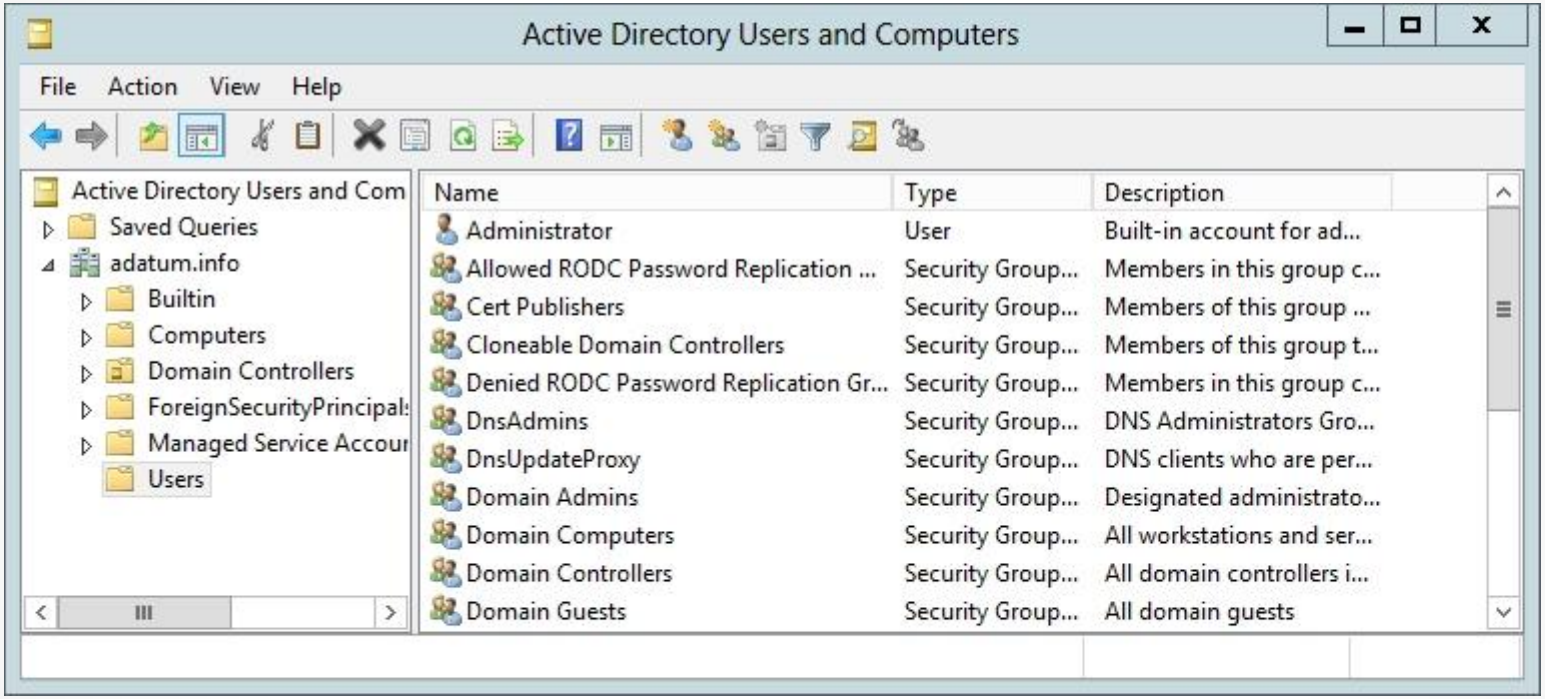
Direct reports:

More Information

OK Cancel

The Create User window in the Active Directory Administrative Center console

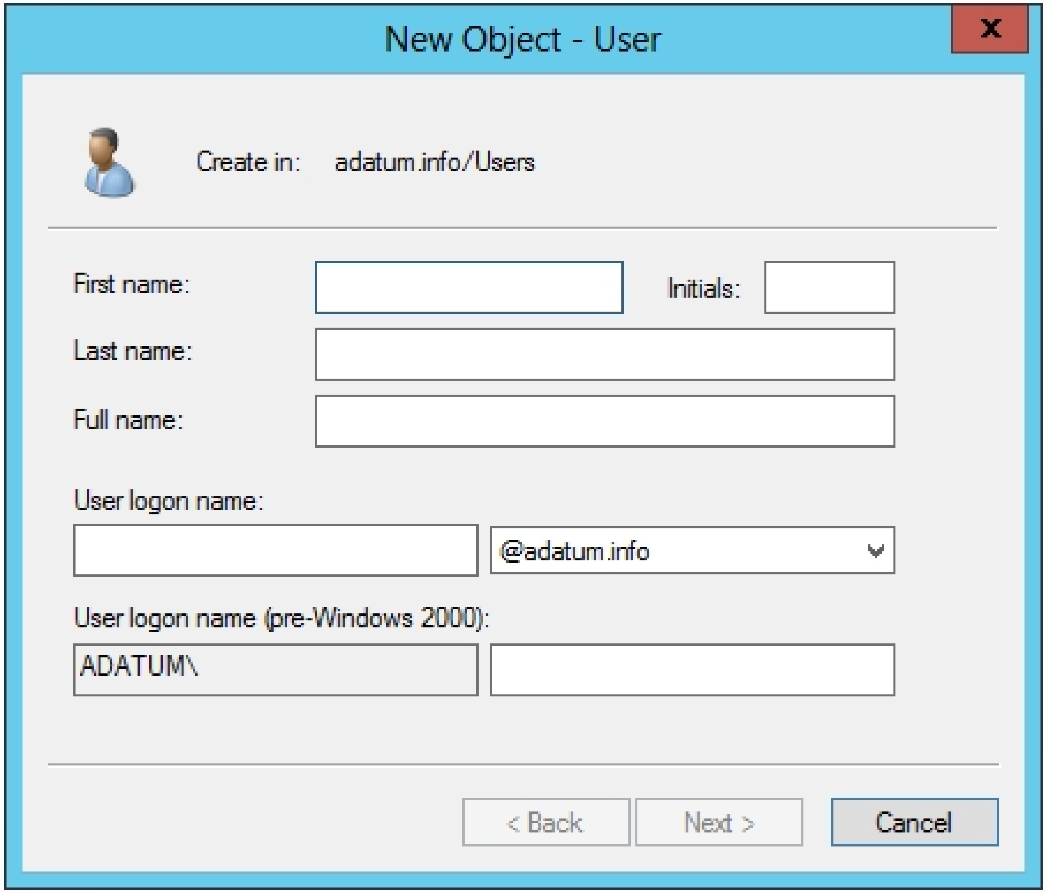
Create a User with Active Directory Users and Computers



Name	Type	Description
Administrator	User	Built-in account for ad...
Allowed RODC Password Replication ...	Security Group...	Members in this group c...
Cert Publishers	Security Group...	Members of this group ...
Cloneable Domain Controllers	Security Group...	Members of this group t...
Denied RODC Password Replication Gr...	Security Group...	Members in this group c...
DnsAdmins	Security Group...	DNS Administrators Gro...
DnsUpdateProxy	Security Group...	DNS clients who are per...
Domain Admins	Security Group...	Designated administrato...
Domain Computers	Security Group...	All workstations and ser...
Domain Controllers	Security Group...	All domain controllers i...
Domain Guests	Security Group...	All domain guests

The Active Directory Users and Computers console

Create a User with Active Directory Users and Computers



New Object - User

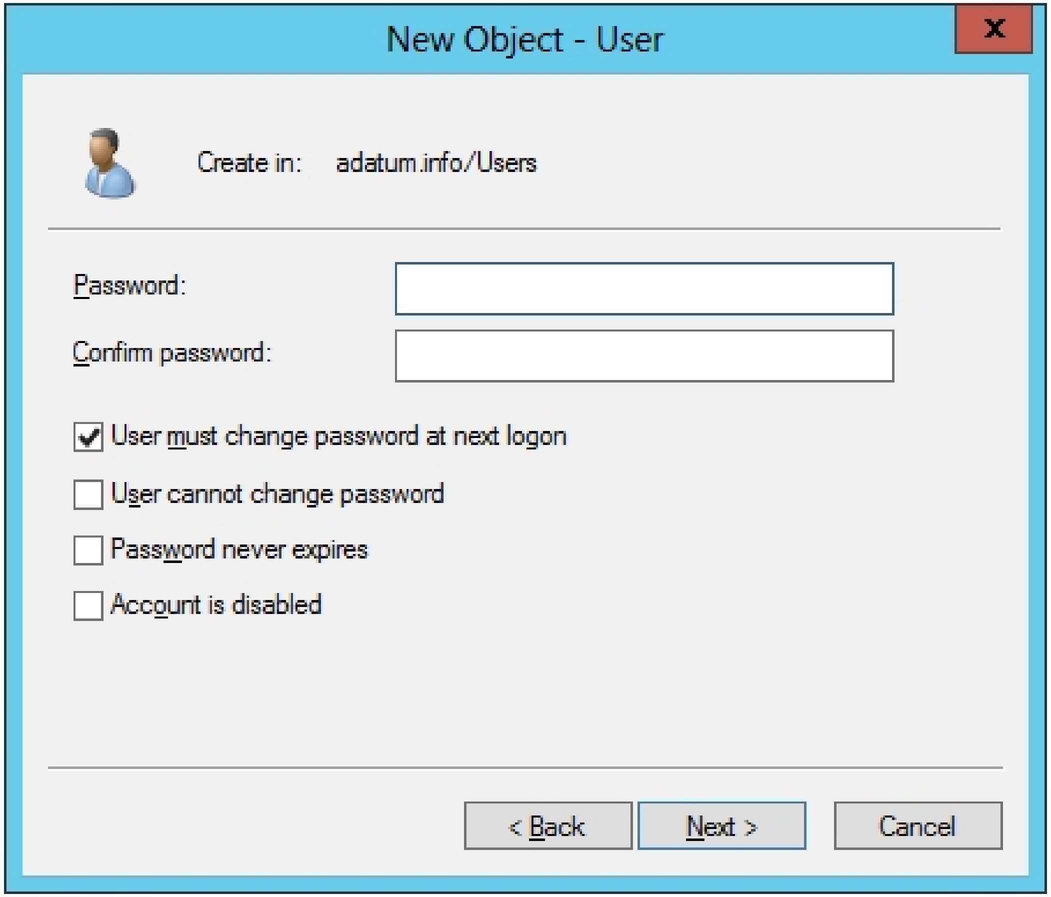
Create in: adatum.info/Users

User logon name: @adatum.info

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

The New Object - User Wizard

Create a User with Active Directory Users and Computers



Create in: adatum.info/Users

Password:

Confirm password:

☑ User must change password at next logon

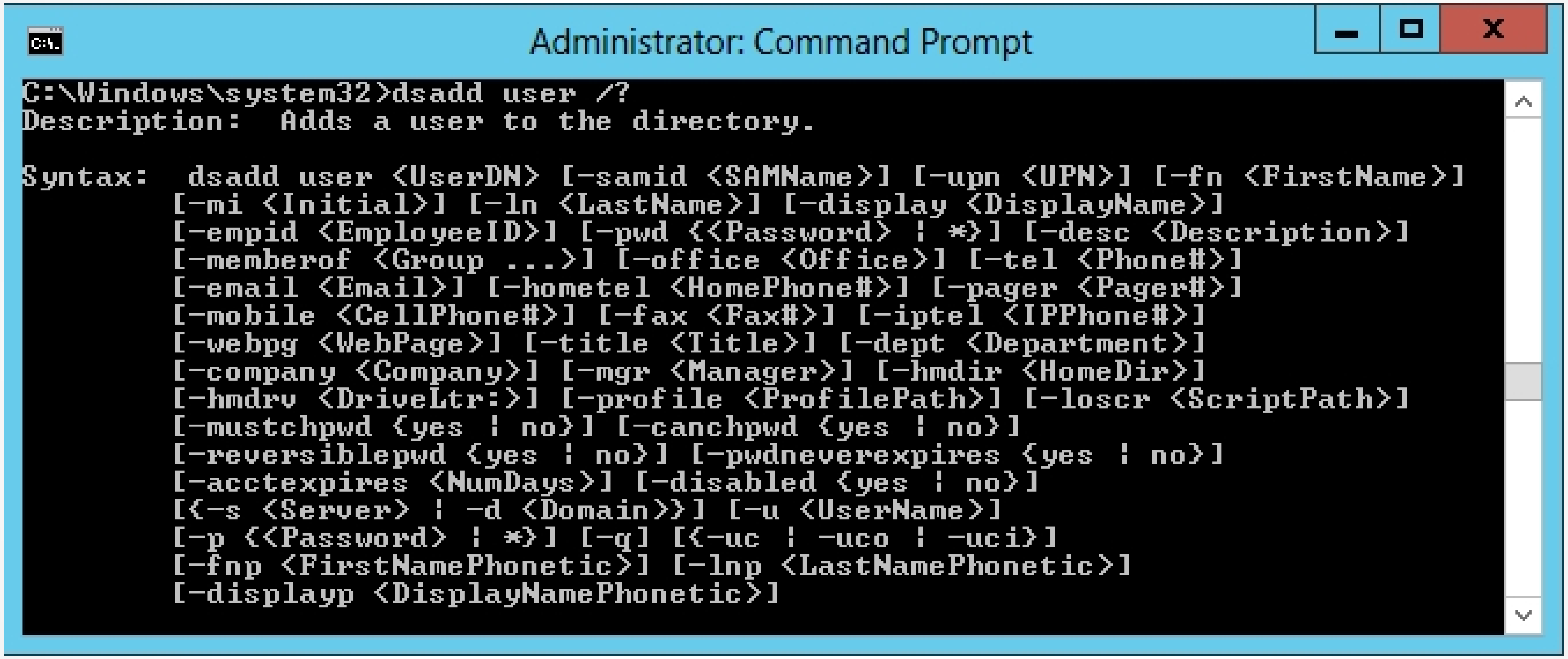
□ User cannot change password

□ Password never expires

□ Account is disabled

The second page of the New Object - User Wizard

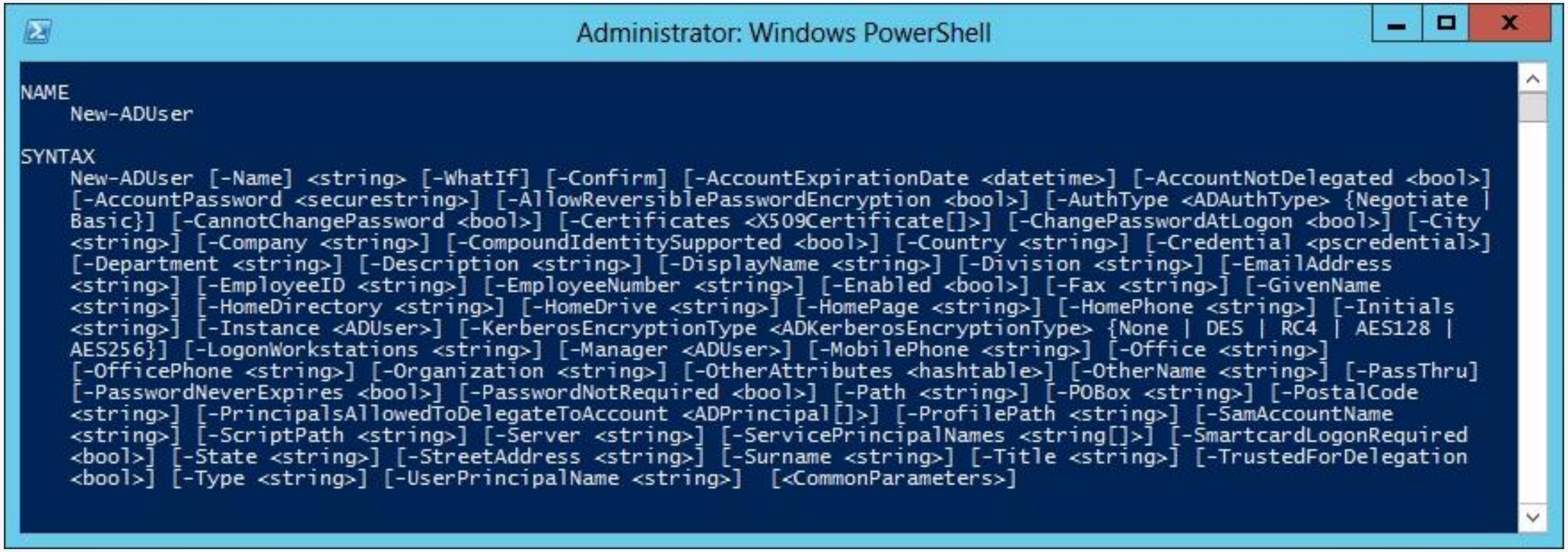
Using Dsadd.exe



```
C:\Windows\system32>dsadd user /?
Description:  Adds a user to the directory.

Syntax:  dsadd user <UserDN> [-samid <SAMName>] [-upn <UPN>] [-fn <FirstName>]
        [-mi <Initial>] [-ln <LastName>] [-display <DisplayName>]
        [-empid <EmployeeID>] [-pwd {<Password> | *}] [-desc <Description>]
        [-memberof <Group ...>] [-office <Office>] [-tel <Phone#>]
        [-email <Email>] [-hometel <HomePhone#>] [-pager <Pager#>]
        [-mobile <CellPhone#>] [-fax <Fax#>] [-iptel <IPPhone#>]
        [-webpg <WebPage>] [-title <Title>] [-dept <Department>]
        [-company <Company>] [-mgr <Manager>] [-hmdir <HomeDir>]
        [-hmdrv <DriveLtr:>] [-profile <ProfilePath>] [-loscr <ScriptPath>]
        [-mustchpwd {yes | no}] [-canchpwd {yes | no}]
        [-reversiblepwd {yes | no}] [-pwdneverexpires {yes | no}]
        [-acctexpires <NumDays>] [-disabled {yes | no}]
        [{-s <Server> | -d <Domain>}] [-u <UserName>]
        [-p {<Password> | *}] [-q] [{-uc | -uco | -uci}]
        [-fnp <FirstNamePhonetic>] [-lnp <LastNamePhonetic>]
        [-displayp <DisplayNamePhonetic>]
```

Syntax of the Dsadd.exe program

Using Windows PowerShell



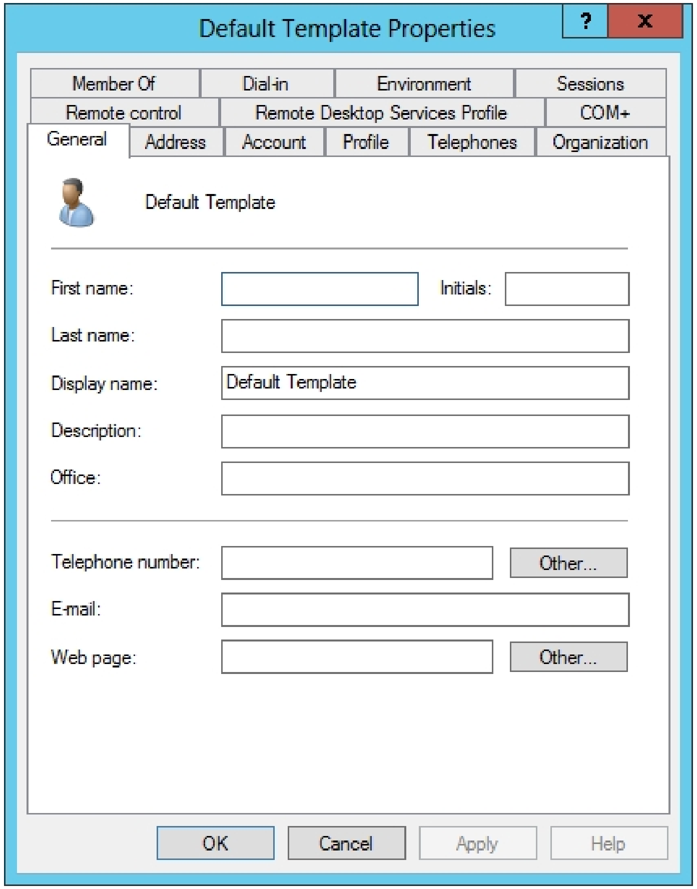
```
NAME
    New-ADUser

SYNTAX
    New-ADUser [-Name] <string> [-WhatIf] [-Confirm] [-AccountExpirationDate <datetime>] [-AccountNotDelegated <bool>]
    [-AccountPassword <securestring>] [-AllowReversiblePasswordEncryption <bool>] [-AuthType <ADAuthType> {Negotiate |
    Basic}] [-CannotChangePassword <bool>] [-Certificates <X509Certificate[]>] [-ChangePasswordAtLogon <bool>] [-City
    <string>] [-Company <string>] [-CompoundIdentitySupported <bool>] [-Country <string>] [-Credential <pscredential>]
    [-Department <string>] [-Description <string>] [-DisplayName <string>] [-Division <string>] [-EmailAddress
    <string>] [-EmployeeID <string>] [-EmployeeNumber <string>] [-Enabled <bool>] [-Fax <string>] [-GivenName
    <string>] [-HomeDirectory <string>] [-HomeDrive <string>] [-HomePage <string>] [-HomePhone <string>] [-Initials
    <string>] [-Instance <ADUser>] [-KerberosEncryptionType <ADKerberosEncryptionType> {None | DES | RC4 | AES128 |
    AES256}] [-LogonWorkstations <string>] [-Manager <ADUser>] [-MobilePhone <string>] [-Office <string>]
    [-OfficePhone <string>] [-Organization <string>] [-OtherAttributes <hashtable>] [-OtherName <string>] [-PassThru]
    [-PasswordNeverExpires <bool>] [-PasswordNotRequired <bool>] [-Path <string>] [-POBox <string>] [-PostalCode
    <string>] [-PrincipalsAllowedToDelegateToAccount <ADPrincipal[]>] [-ProfilePath <string>] [-SamAccountName
    <string>] [-ScriptPath <string>] [-Server <string>] [-ServicePrincipalNames <string[]>] [-SmartcardLogonRequired
    <bool>] [-State <string>] [-StreetAddress <string>] [-Surname <string>] [-Title <string>] [-TrustedForDelegation
    <bool>] [-Type <string>] [-UserPrincipalName <string>]  [<CommonParameters>]
```

Syntax of the New-ADUser cmdlet

User Templates

- A user template is a standard user object containing common attribute settings.
- To create a new user with these settings, you copy the template to a new user object and change the name.
- You can change any attributes that are different.

Create a User Template

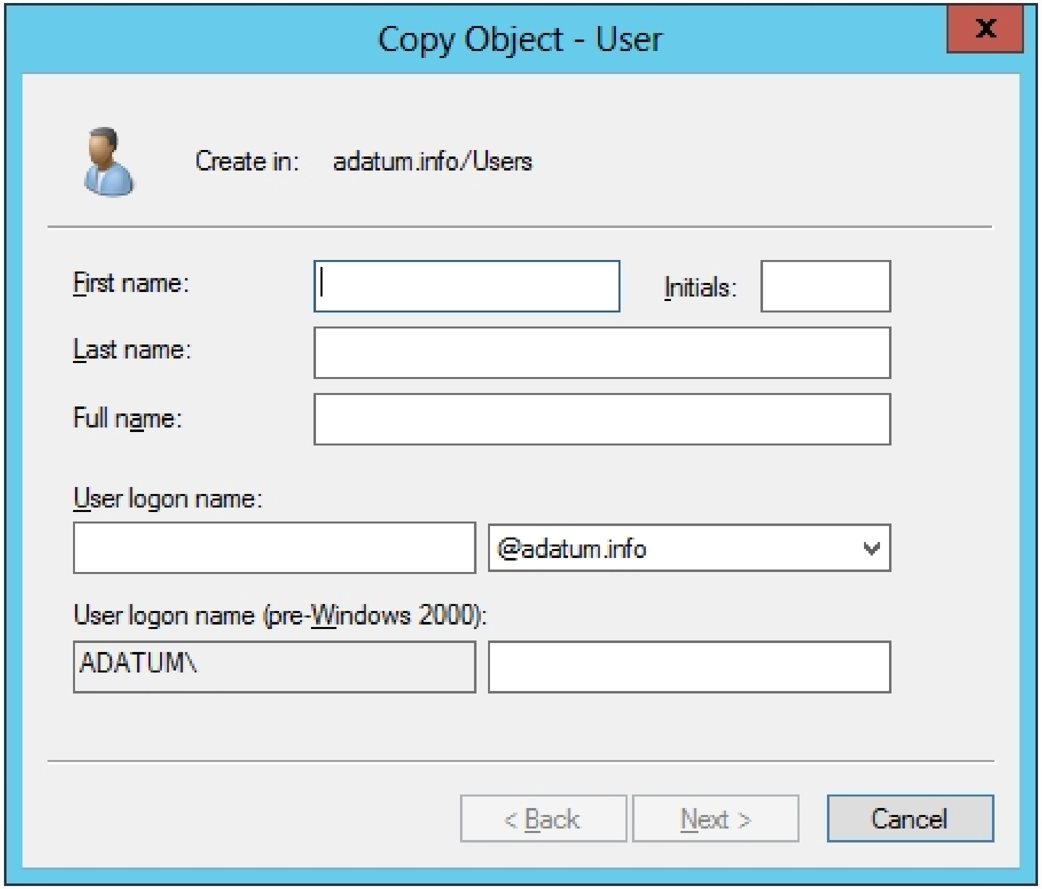


Default Template Properties

Display name: Default Template

A user object’s Properties sheet

Create a User Template



Copy Object - User

Create in: adatum.info/Users

First name:

Initials:

Last name:

Full name:

User logon name:

@adatum.info

User logon name (pre-Windows 2000):

ADATUM\

The Copy Object – User Wizard

Creating Multiple Users

- **Batch Files**
  - Text files that contain commands.
  - Open Notepad and use the Dsadd.exe syntax described earlier, placing a single command on each line.
- **CSVDE.exe**
  - A command-line utility enables administrators to import or export Active Directory objects using a CSV file.
- **LDIFDE.exe**
  - Similar to CSVDE, but also allows you to delete and modify objects later.
- **Windows PowerShell**
  - Use CSV files to create user objects with Windows PowerShell.

Creating Computer Objects

Lesson 14: Creating and Managing Active Directory Users and Computers

Computer Objects

- Consist of properties that specify the computer’s name, where it is located, and who is permitted to manage it.
- Inherit group policy settings from container objects such as domains, sites, and organizational units.
- Can be members of groups and inherit permissions from group objects.

Adding a Computer to a Domain

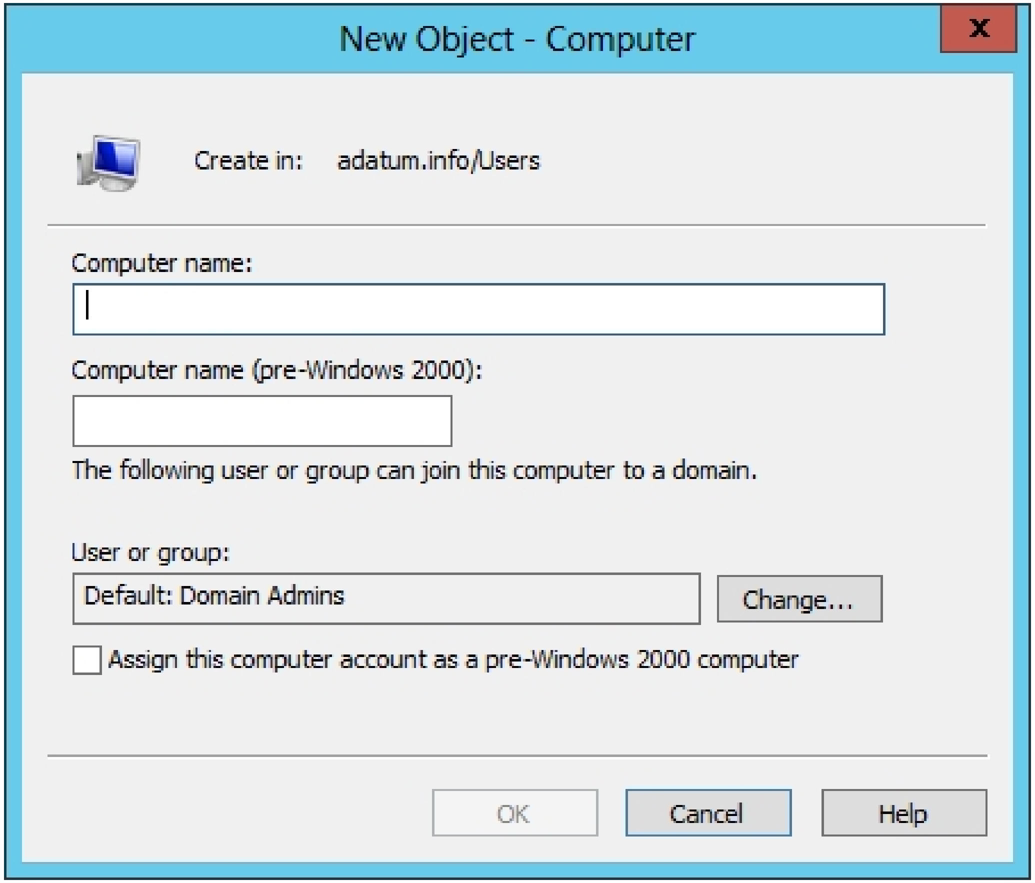
- **Creating a computer account:** Create a new computer object in Active Directory and assign the name of an actual computer on the network.
- **Joining the computer to the domain:** The system contacts a domain controller, establishes a trust relationship with the domain, locates (or creates) a computer object corresponding to the computer's name, alters its security identifier (SID) to match that of the computer object, and modifies its group memberships.

Adding a Computer to a Domain

Two ways to create AD computer objects:

- Create the computer objects in advance using an Active Directory tool, so that the computers can locate the existing objects when they join the domain.
- Begin the joining process first and let the computer create its own computer object.

Creating Computer Objects Using Active Directory Users and Computers



New Object - Computer

Create in: adatum.info/Users

Computer name:

Computer name (pre-Windows 2000):

The following user or group can join this computer to a domain.

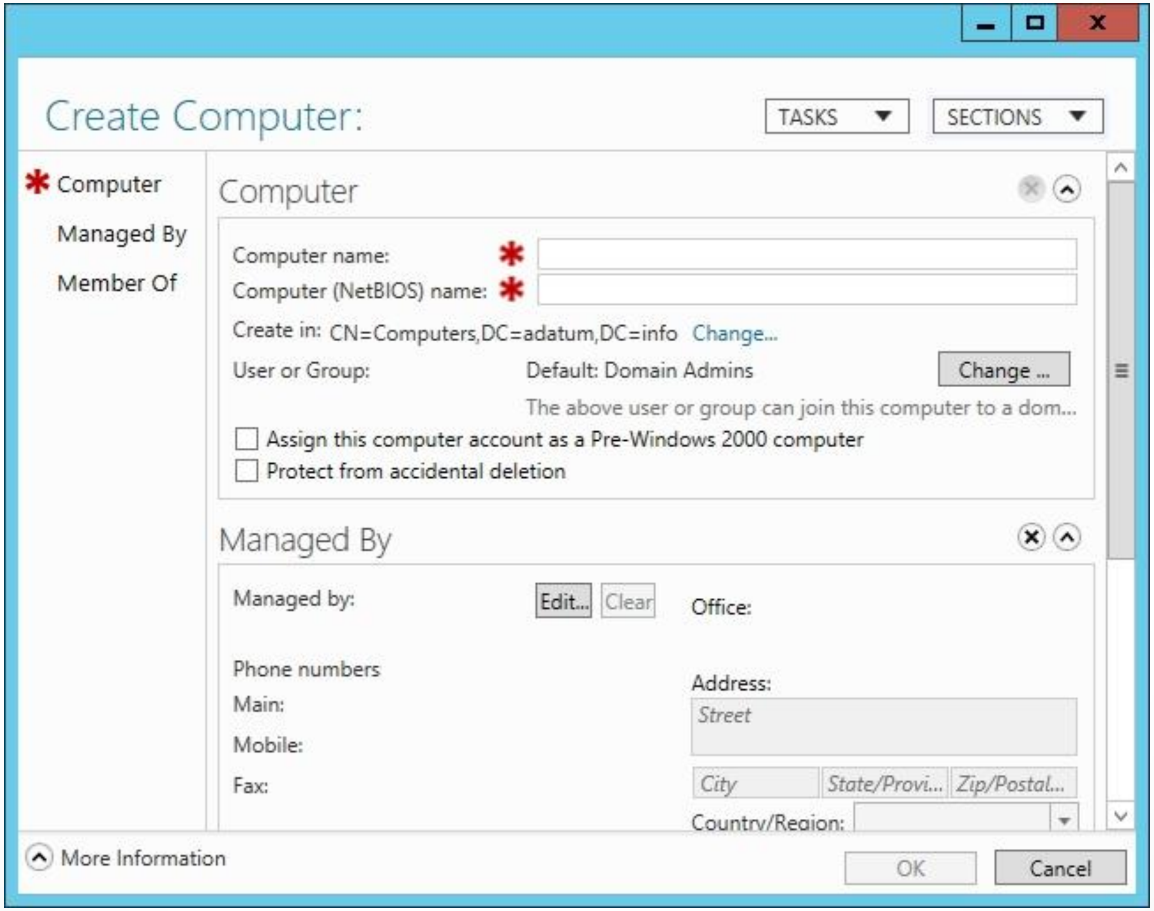
User or group:

Default: Domain Admins

☐ Assign this computer account as a pre-Windows 2000 computer

The New Object – Computer wizard

Creating Computer Objects with Active Directory Administrative Center



Create Computer:

TASKS ▼ SECTIONS ▼

✱ Computer

Managed By

Member Of

Computer

Computer name: ✱

Computer (NetBIOS) name: ✱

Create in: CN=Computers,DC=adatum,DC=info Change...

User or Group: Default: Domain Admins Change ...

The above user or group can join this computer to a dom...

□ Assign this computer account as a Pre-Windows 2000 computer

□ Protect from accidental deletion

Managed By

Managed by: Edit... Clear

Office:

Phone numbers

Main:

Mobile:

Fax:

Address:

Street

City State/Provi... Zip/Postal...

Country/Region:

More Information

OK Cancel

The Create Computer dialog box

Creating Computer Objects Using Dsadd.exe

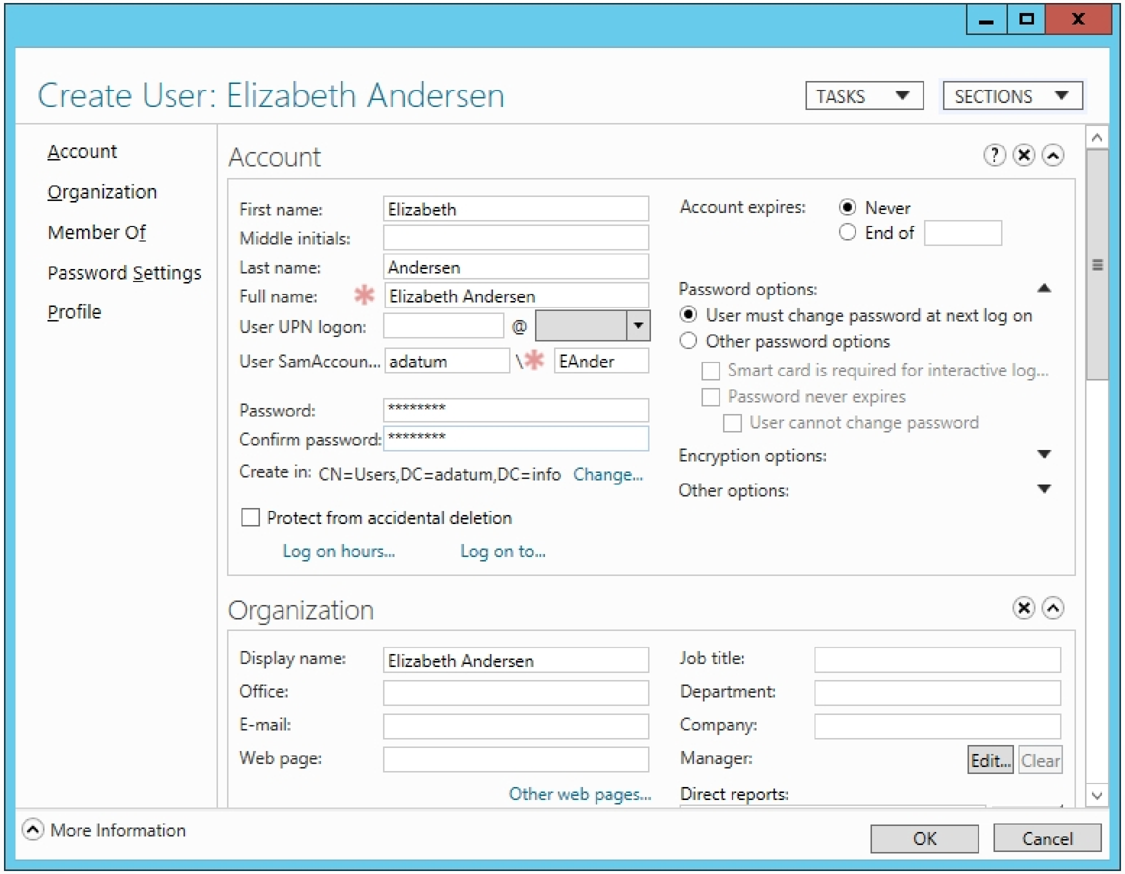
```
dsadd computer <ComputerDN>
```

The *<ComputerDN>* parameter specifies a distinguished name for the new group object you want to create.

Managing Active Directory Objects

Lesson 14: Creating and Managing Active Directory Users and Computers

Managing Active Directory Objects



Create User: Elizabeth Andersen

Account

First name: Elizabeth
Middle initials:
Last name: Andersen
Full name: * Elizabeth Andersen
User UPN logon: @
User SamAccoun... adatum * EAnder
Password: ********
Confirm password: ********
Create in: CN=Users,DC=adatum,DC=info Change...

□ Protect from accidental deletion

Log on hours... Log on to...

Account expires: ● Never ○ End of

Password options:
● User must change password at next log on
○ Other password options
□ Smart card is required for interactive log...
□ Password never expires
□ User cannot change password

Encryption options:
Other options:

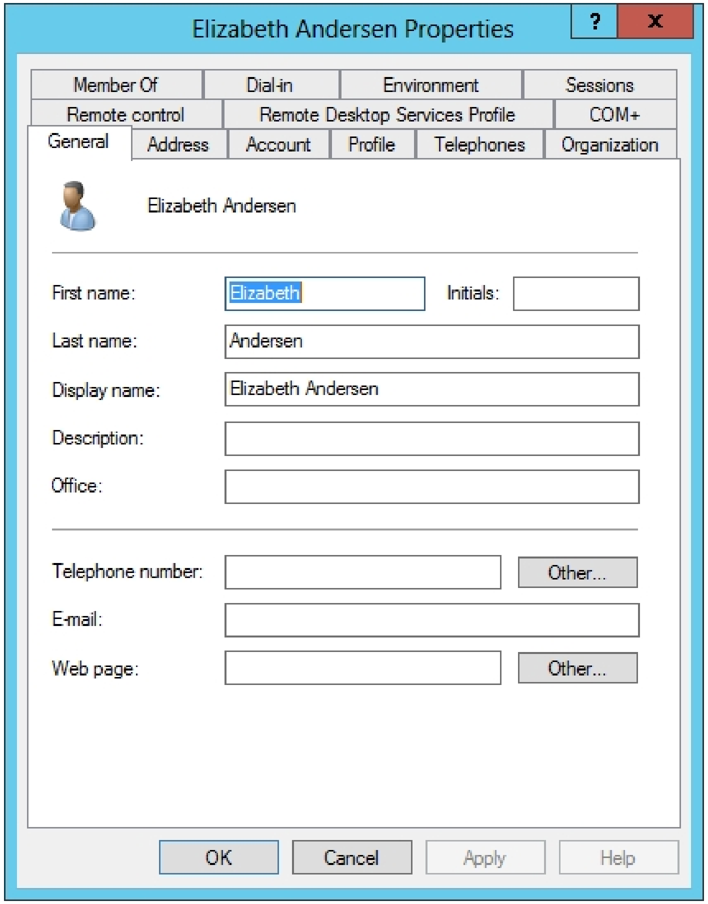
Organization

Display name: Elizabeth Andersen
Office:
E-mail:
Web page:
Other web pages...

Job title:
Department:
Company:
Manager: Edit... Clear
Direct reports:

A user object's Properties sheet in Active Directory Administrative Center

Managing Active Directory Objects



Elizabeth Andersen

First name: Elizabeth

Initials:

Last name: Andersen

Display name: Elizabeth Andersen

Description:

Office:

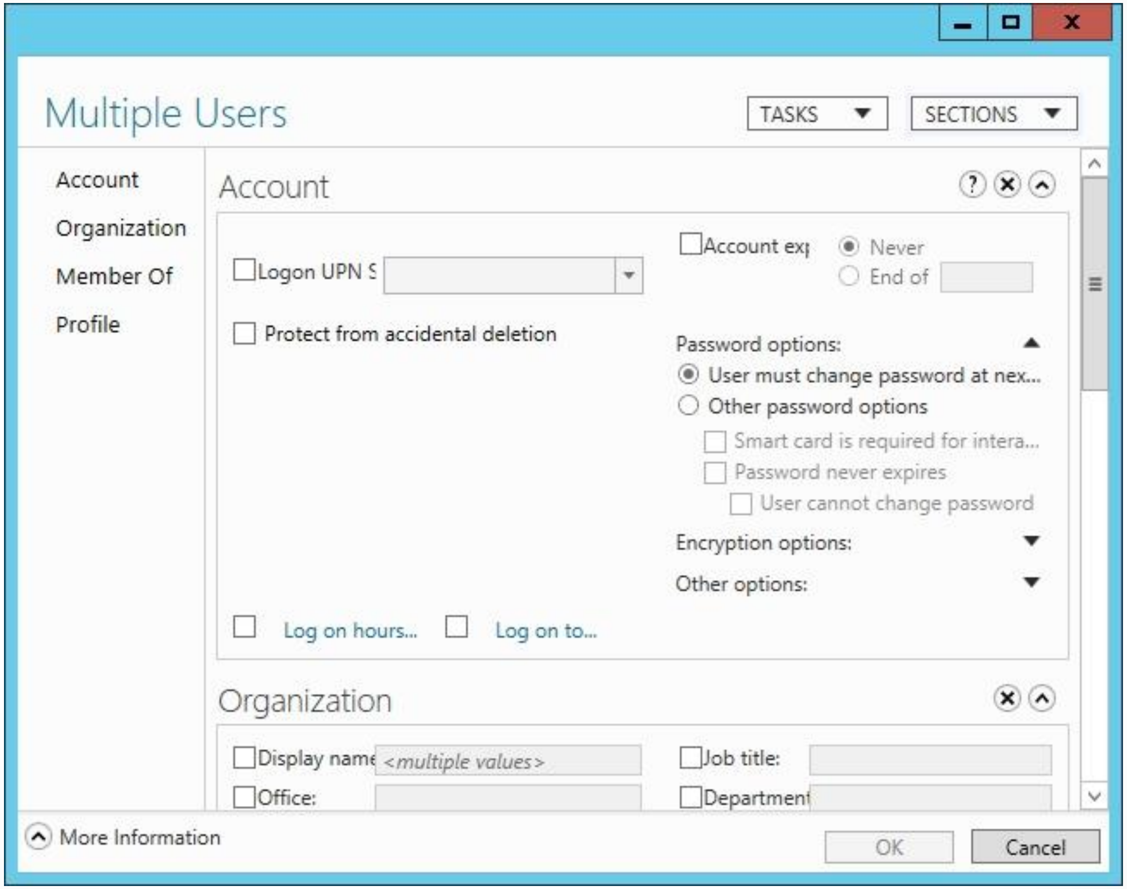
Telephone number:

E-mail:

Web page:

A user object's Properties sheet in Active Directory Users and Computers

Managing Multiple Users



Account

□ Logon UPN S

□ Protect from accidental deletion

□ Account exp ● Never ○ End of

Password options:

● User must change password at nex...

○ Other password options

□ Smart card is required for intera...

□ Password never expires

□ User cannot change password

Encryption options: ▼

Other options: ▼

□ Log on hours... □ Log on to...

Organization

□ Display name <multiple values>

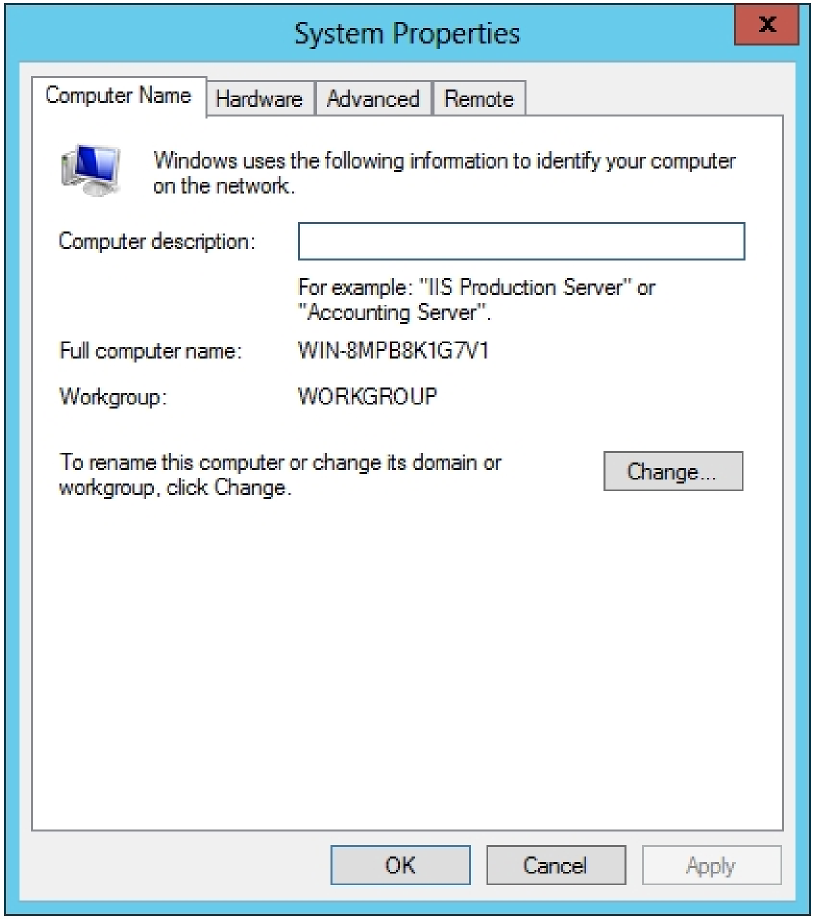
□ Job title:

□ Office:

□ Department

A Multiple Users Properties sheet in Active Directory Administrative Center

Joining Computers to a Domain



System Properties

Windows uses the following information to identify your computer on the network.

Computer description:

For example: "IIS Production Server" or "Accounting Server".

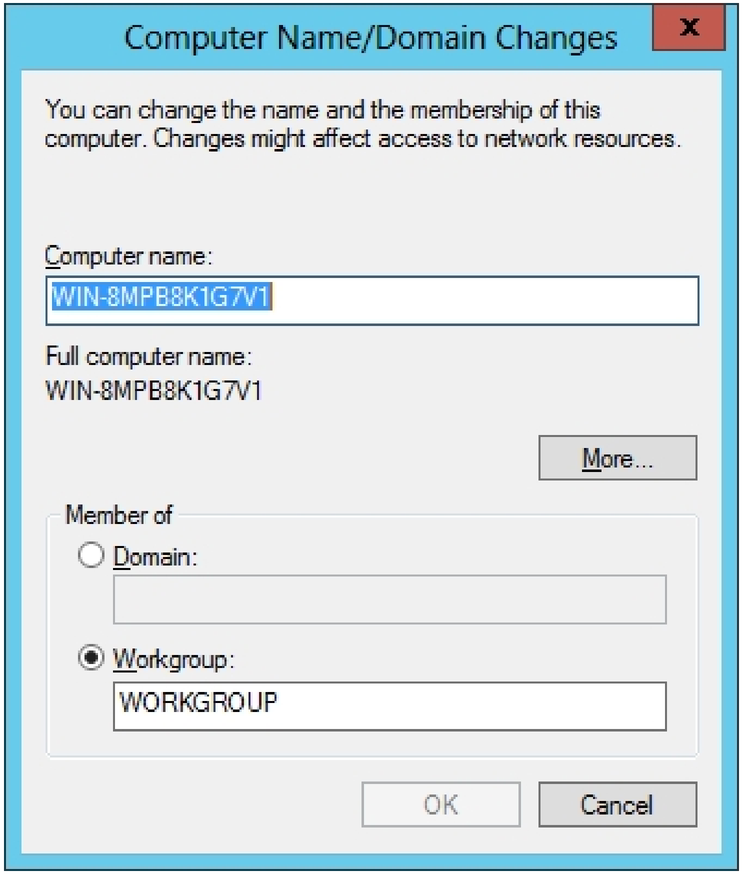
Full computer name: WIN-8MPB8K1G7V1

Workgroup: WORKGROUP

To rename this computer or change its domain or workgroup, click Change.

The Computer Name tab in the System Properties dialog box

Joining Computers to a Domain


Computer Name/Domain Changes

You can change the name and the membership of this computer. Changes might affect access to network resources.

Computer name:
WIN-8MPB8K1G7V1

Full computer name:
WIN-8MPB8K1G7V1

Member of
○ Domain:

● Workgroup:
WORKGROUP

The Computer Name Changes dialog box

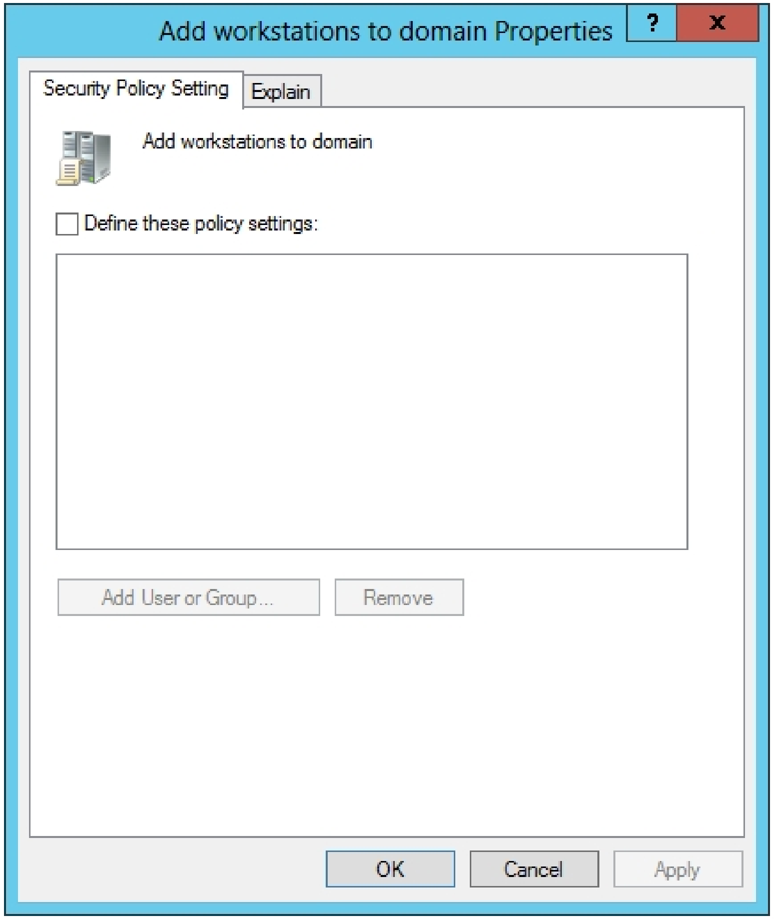
Joining a Domain Using Netdom.exe

```
netdom join <computername> /Domain:<DomainName>
   [/UserD:<User> /PasswordD:<UserPassword>]
   [/OU:OUDN]
```

Creating Computer Objects while Joining

- Domain users can also create computer objects themselves through an indirect process.
- The **Default Domain Controllers Policy GPO** grants a user right called **Add Workstations To The Domain** to the **Authenticated Users** special identity.
- Any user successfully authenticated to Active Directory is permitted to join up to ten workstations to the domain, and create ten associated computer objects.

Creating Computer Objects while Joining



Add workstations to domain Properties

Add workstations to domain

□ Define these policy settings:

The Default Domain Controllers Policy user rights assignments

Joining a Domain while Offline

- Use **Djoin.exe** program twice:
  1. On a computer with access to a domain controller
  2. On the computer to be joined.
- The syntax for phase 1 of the process:

```
djoin /provision /domain <domain name>
  /machine <computer name> /savefile
  <filename.txt>
```

- You then transport the metadata file to the computer to be joined and run **Djoin.exe** again.
- The syntax for the phase 2 of the process:

```
djoin /requestODJ /loadfile <filename.txt>
  /windowspath %SystemRoot% /localos
```

Managing Disabled Accounts

- Disabling a user account prevents anyone from using it to log on to the domain until an administrator with the appropriate permissions enables it again.
- You can disable user accounts manually.
- It is also possible for a system to automatically disable them for security reasons.
- It is a simple Disable/Enable option in the GUI interface.

Managing Disabled Accounts

To disable or enable a user or computer account with Windows PowerShell, use the following cmdlet syntax:

```
Disable-ADAccount –Identity <account name>
Enable-ADAccount –Identity <account name>
```

Lesson Summary

- The user account is the primary means by which people using an Active Directory Domain Services network access resources.
- One of the most common tasks for administrators is the creation of Active Directory user objects. Windows Server 2012 includes several tools you can use to create objects.
- Windows Server 2012 has redesigned the Active Directory Administrative Center (ADAC) application, first introduced in Windows Server 2008 R2, to fully incorporate new features such as the Active Directory Recycle Bin and fine-grained password policies. You can also use the tool to create and manage AD DS user accounts.

Lesson Summary

- Microsoft Excel and Microsoft Exchange are two common applications in which you can have a number of users, along with their accompanying information, to add to the AD DS database. In these cases, you can export information from the applications by saving it to a file in **Comma-Separated Values (CSV)** format.
- **LDIFDE.exe** is a utility that has the same basic functionality as CSVDE.exe and provides the ability to modify existing records in Active Directory.
- Because an AD DS network uses a centralized directory, there has to be some means of tracking the actual computers that are part of the domain. To do this, Active Directory uses computer accounts, which are realized in the form of computers objects in the Active Directory database.

Lesson Summary

- The process of actually joining a computer to a domain must occur at the computer itself and be performed by a member of the computer's local Administrators group.
- Administrators typically join computers to domains while the computers are connected to the network and have access to a domain controller. However, in some situations administrators may want to set up computers without access to a domain controller, such as a new branch office installation. In these cases, it is possible to perform an offline domain join, using a command line program called **Djoin.exe**.