



**BATCH** : BATCH 85

**LESSON** : **Windows Server**

**DATE** : 19.07.2022

**SUBJECT** : **AD Services  
Objects**



techproeducation



techproeducation



techproeducation



techproeducation



techproedu



# Module Overview

- Managing User Accounts
- Managing Groups
- Managing Computer Accounts
- Delegating Administration



# Lesson 1: Managing User Accounts

- AD DS Administration Tools
- Creating User Accounts
- Configuring User Account Attributes
- Creating User Profiles



# AD DS Administration Tools

To manage AD DS objects, you can use the following graphical tools:

- Active Directory Administration snap-ins
- Active Directory Administrative Center



You can also use the following command-line tools:

- Active Directory module in Windows PowerShell
- Directory Service commands





# Creating User Accounts

The Account section of the Active Directory Administrative Center Create User window

First name:	<input type="text"/>	Account expires:	<input checked="" type="radio"/> Never
Middle initials:	<input type="text"/>		<input type="radio"/> End of <input type="text"/>
Last name:	<input type="text"/>		
Full name:	<input type="text"/>		
User UPN login:	<input type="text"/> @ <input type="text"/>		
User SamAccountName:	<input type="text"/> \ <input type="text"/>		
Password:	<input type="password"/>		
Confirm password:	<input type="password"/>		
Create in:	OU=Managers,DC=Adatum,DC=com		
	<a href="#">Change...</a>		
<input type="checkbox"/> Protect from accidental deletion			
<a href="#">Log on hours...</a>		<a href="#">Log on to...</a>	

Password options:

☒ User must change password at next log on

☐ Other password options

☐ Smart card is required for interactive log on

☐ Password never expires

☐ User cannot change password

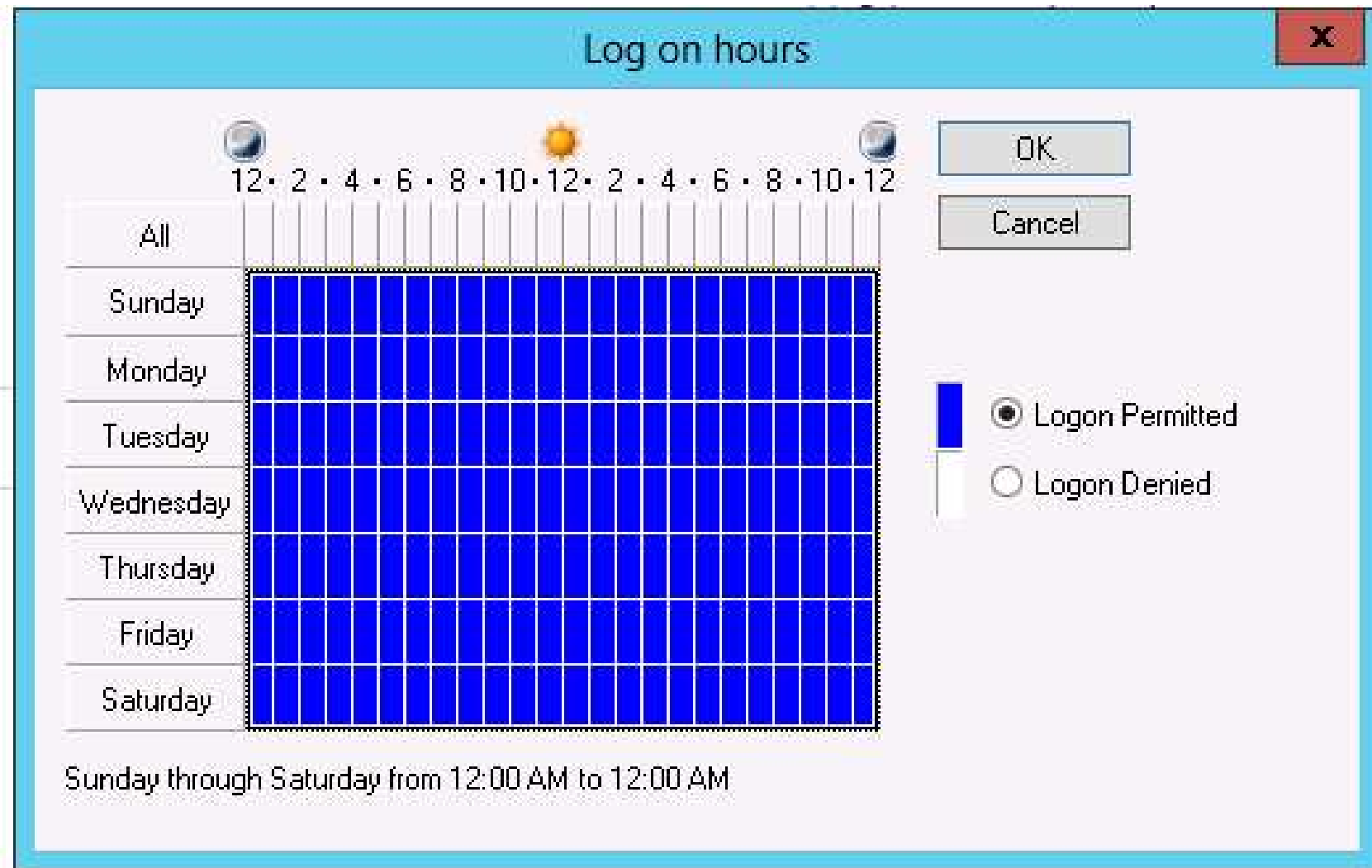
Encryption options:

Other options:



# Configuring User Account Attributes

## The Log on hours dialog box





# Creating User Profiles

The Profile section of the User Properties window

Profile

Profile path:  Log on script:

Home folder:

☐ Local path:

☒ Connect   To:



## Lesson 2: Managing Groups

- Group Types
- Group Scopes
- Implementing Group Management
- Default Groups
- Special Identities
- Demonstration: Managing Groups





# Group Types

- **Distribution groups**

- Used only with email applications
- Not security-enabled (no SID); cannot be given permissions



- **Security groups**

- Security principal with a SID; can be given permissions
- Can also be email-enabled

Both security groups and distribution groups can be converted to the other type of group





# Default Groups

- Carefully manage the default groups that provide administrative privileges, because these groups:
  - Typically have broader privileges than are necessary for most delegated environments
  - Often apply protection to their members

Group	Location
Enterprise Admins	Users container of the forest root domain
Schema Admins	Users container of the forest root domain
Administrators	Built-in container of each domain
Domain Admins	Users container of each domain
Server Operators	Built-in container of each domain
Account Operators	Built-in container of each domain
Backup Operators	Built-in container of each domain
Print Operators	Built-in container of each domain
Cert Publishers	Users container of each domain



# Special Identities

- Special identities:
  - Are groups for which membership is controlled by the operating system
  - Can be used by the Windows Server operating system to provide access to resources:
    - Based on the type of authentication or connection
    - Not based on the user account
- Important special identities include:
  - Anonymous Logon
  - Authenticated Users
  - Everyone
  - Interactive
  - Network
  - Creator Owner



# What Is the Computers Container?

Active Directory Administrative Center, opened to the  
Adatum (local)\Computers container

Distinguished Name is cn=Computers,DC=Adatum,DC=com

← → ▾ ◀ Adatum (local) ▶ Computers

Active Directory... ◀

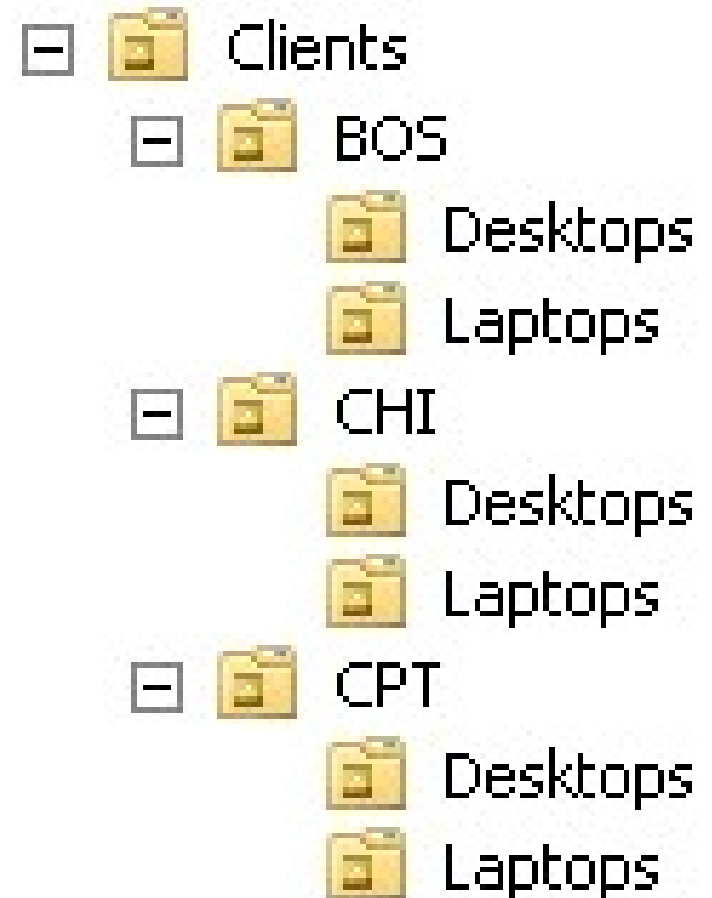
Filter 🔍

Name	Type	Description
LON-CL1	Computer	
LON-CL2	Computer	
LON-RTR	Computer	
LON-SVR1	Computer	
LON-SVR2	Computer	
LON-SVR4	Computer	



# Specifying the Location of Computer Accounts

- Best practice is to create OUs for computer objects
  - Servers
    - Typically subdivided by server role
  - Client computers
    - Typically subdivided by region
- Divide OUs:
  - By administration
  - To facilitate configuration with Group Policy





# Controlling Permissions to Create Computer Accounts

The Delegation of Control Wizard window  
The administrator is creating a custom delegation for computer objects



The image shows a screenshot of the 'Delegation of Control Wizard' window. The title bar is light blue with the text 'Delegation of Control Wizard' and a red close button. The main area has a light blue header with the text 'Active Directory Object Type' and a key icon. Below this, it says 'Indicate the scope of the task you want to delegate.' The 'Delegate control of:' section has two radio buttons: 'This folder, existing objects in this folder, and creation of new objects in this folder' (unselected) and 'Only the following objects in the folder:' (selected). Below the selected radio button is a list box containing several object types with checkboxes: 'account objects', 'aCSResourceLimits objects', 'applicationVersion objects', 'bootableDevice objects', 'certificationAuthority objects', and 'Computer objects' (checked). At the bottom, there are two checked checkboxes: 'Create selected objects in this folder' and 'Delete selected objects in this folder'. The bottom of the window has four buttons: '< Back', 'Next >', 'Cancel', and 'Help'.

**Delegation of Control Wizard**

**Active Directory Object Type**  
Indicate the scope of the task you want to delegate.

Delegate control of:

☐ This folder, existing objects in this folder, and creation of new objects in this folder

☒ Only the following objects in the folder:

- ☐ account objects
- ☐ aCSResourceLimits objects
- ☐ applicationVersion objects
- ☐ bootableDevice objects
- ☐ certificationAuthority objects
- ☒ Computer objects

☒ Create selected objects in this folder

☒ Delete selected objects in this folder

< Back   Next >   Cancel   Help



# Computer Accounts and Secure Channels

- Computers have accounts
  - sAMAccountName and password
  - Used to create a secure channel between the computer and a domain controller
- Scenarios in which a secure channel can be broken
  - Reinstalling a computer, even with same name, generates a new SID and password
  - Restoring a computer from an old backup, or rolling back a computer to an old snapshot
  - Computer and domain disagree about what the password is





# AD DS Permissions

## Advanced Security Settings for IT

Owner: Domain Admins (ADATUM\Domain Admins) [Change](#)

Permissions Auditing Effective Access

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

Type	Principal	Access	Inherited from	Applies to
Deny	Everyone	Special	None	This object only
Allow	Account Operators (ADATU...	Create/delete InetOrg...	None	This object only
Allow	Account Operators (ADATU...	Create/delete Comput...	None	This object only
Allow	Account Operators (ADATU...	Create/delete Group o...	None	This object only
Allow	Print Operators (ADATUM\Pr...	Create/delete Printer o...	None	This object only
Allow	Account Operators (ADATU...	Create/delete User obj...	None	This object only
Allow	Domain Admins (ADATUM\...	Full control	None	This object only
Allow	ENTERPRISE DOMAIN CONT...	Special	None	This object only
Allow	Authenticated Users	Special	None	This object only
Allow	SYSTEM	Full control	None	This object only

Add Remove View Restore defaults

Disable inheritance



# AD DS Permissions

- Advanced Security Settings for IT

