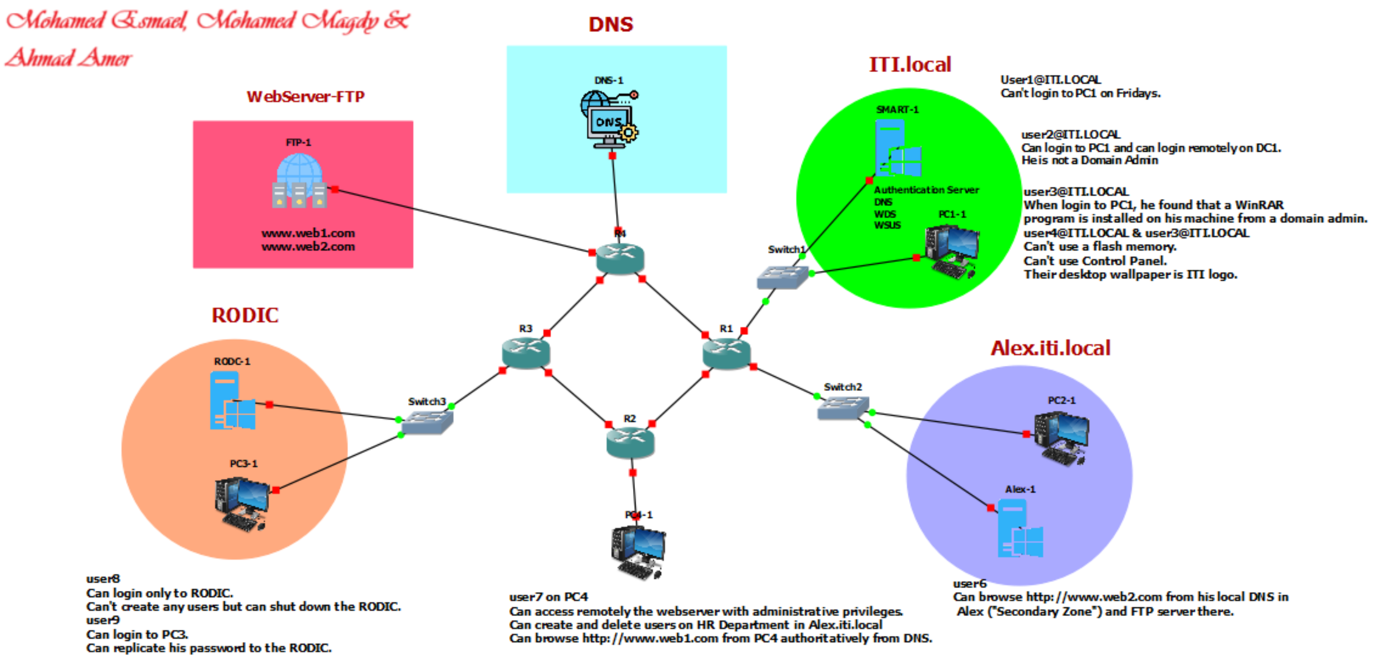


User1@ITI.LOCAL
Can't login to PC1 on Fridays.

user2@ITI.LOCAL
Can login to PC1 and can login remotely on DC1.
He is not a Domain Admin

user3@ITI.LOCAL
When login to PC1, he found that a WinRAR
program is installed on his machine from a domain admin.
user4@ITI.LOCAL & user3@ITI.LOCAL
Can't use a flash memory.
Can't use Control Panel.
Their desktop wallpaper is ITI logo.

user8
Can login only to RODIC.
Can't create any users but can shut down the RODIC.
user9
Can login to PC3.
Can replicate his password to the RODIC.

user7 on PC4
Can access remotely the webserver with administrative privileges.
Can create and delete users on HR Department in Alex.iti.local
Can browse http://www.web1.com from PC4 authoritatively from DNS.

user6
Can browse http://www.web2.com from his local DNS in
Alex ("Secondary Zone") and FTP server there.

WIN SERVER PROJECT

PRESENTED BY :

MOHAMED ESMAEL, MOHAMED MAGDY &
AHMAD AMER

Instructor: Eng/Peter Kamel

Windows Server

TABLE OF CONTENTS

Project Overview

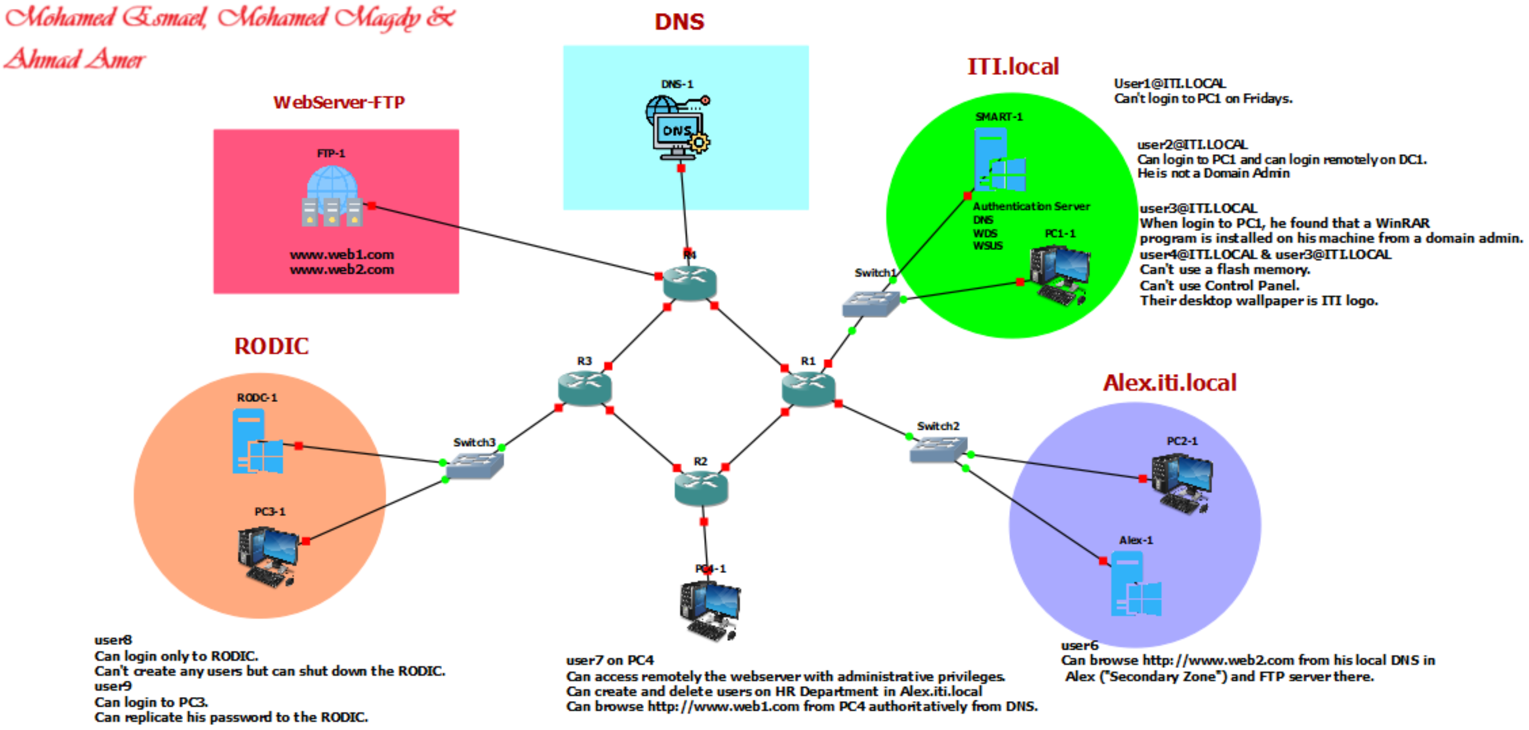
This project demonstrates the design and implementation of a simulated corporate network using Windows Server technologies.
The goal is to establish a secure, scalable, and efficient Active Directory infrastructure, incorporating various administrative roles and configurations. GNS3 was utilized to simulate network topology and configurations, providing a realistic environment for testing and validation.

Objectives

- **Active Directory Design:**
  - Establish a Primary Domain Controller (PDC).
  - Set up a Child Domain Controller (Alexandria Branch).
  - Configure a Read-Only Domain Controller (RODC).
- **Role-Based Access Control:**
  - Implement policies restricting user access to specific resources.
  - Manage user roles and permissions using Group Policy Objects (GPOs).
- **Network Services Configuration:**
  - Install and configure DNS, DHCP, WSUS, WDS, and FTP services.
- **Remote Management:**
  - Enable and test remote administrative access.
- **Testing and Validation:**
  - Verify restrictions and access policies for all configured users

Network Topology

- **Main Branch** (Smart Village): Contains the Primary Domain Controller (PDC).
- **Alex Branch**: Functions as a child domain.
- **Web FTP Server**: Centralized web and FTP services.
- **DNS:** for web1.com and web2.com.
- **RODC (Read-Only Domain Controller)**: In a remote branch for secure replication.



User1@ITI.LOCAL
Can't login to PC1 on Fridays.

user2@ITI.LOCAL
Can login to PC1 and can login remotely on DC1.
He is not a Domain Admin

user3@ITI.LOCAL
When login to PC1, he found that a WinRAR
program is installed on his machine from a domain admin.
user4@ITI.LOCAL & user3@ITI.LOCAL
Can't use a flash memory.
Can't use Control Panel.
Their desktop wallpaper is ITI logo.

user8
Can login only to RODIC.
Can't create any users but can shut down the RODIC.
user9
Can login to PC3.
Can replicate his password to the RODIC.

user7 on PC4
Can access remotely the webserver with administrative privileges.
Can create and delete users on HR Department in Alex.iti.local
Can browse http://www.web1.com from PC4 authoritatively from DNS.

user6
Can browse http://www.web2.com from his local DNS in
Alex ("Secondary Zone") and FTP server there.

Device and IP Address Table

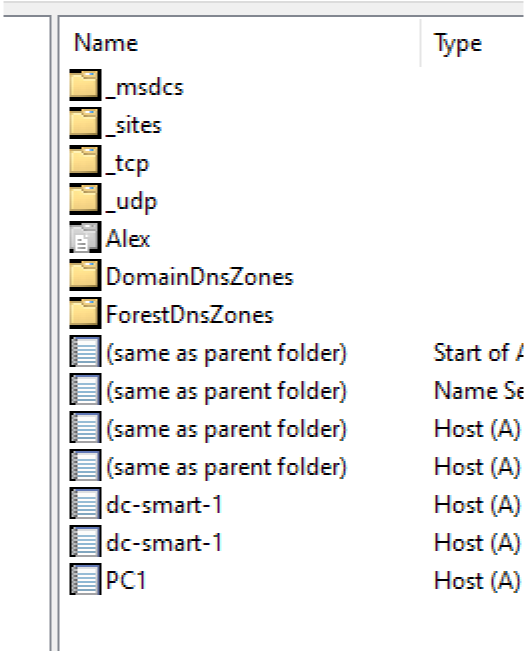
Device/Service	IP Address
SMART	192.168.200.10
RODC	192.168.200.15
DNS Server	192.168.200.100
WebServer-FTP	192.168.200.150
DC-Alex-1	192.168.200.20
www.web1.com	192.168.200.151
www.web2.com	192.168.200.152

MAIN BRANCH (SMART)

- **Domain Controller Configuration:**
- Set up a new Virtual Machine (VM) with Windows Server.
- Install the **Active Directory Domain Services (AD DS)** role.
- Promote the server to a Domain Controller with the domain name `iti.local`.
- Install additional roles: DNS, DHCP, WDS, and WSUS.

DNS Configuration:

- Purpose: Resolves domain names to IP addresses, enabling users to connect to websites and network resources.
- Steps:
- Open Server Manager and click on Add Roles and Features.
- Select DNS Server and complete the installation.
- Use the DNS Manager to create new zones and configure forward and reverse lookup zones.

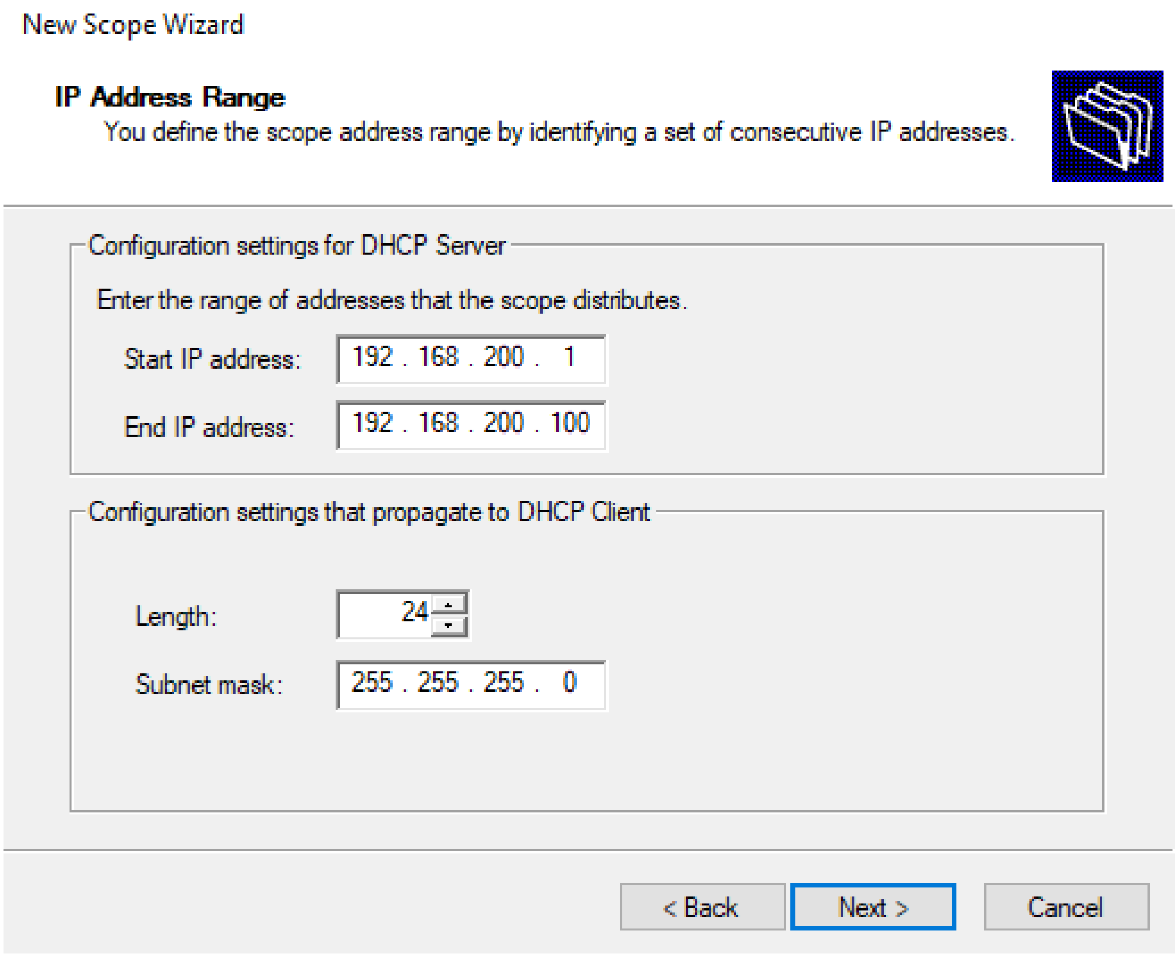


Name	Type
_msdcs	
_sites	
_tcp	
_udp	
Alex	
DomainDnsZones	
ForestDnsZones	
(same as parent folder)	Start of /
(same as parent folder)	Name Se
(same as parent folder)	Host (A)
(same as parent folder)	Host (A)
dc-smart-1	Host (A)
dc-smart-1	Host (A)
PC1	Host (A)

DHCP Configuration:

- **Purpose**: Automatically assigns IP addresses and network configuration to devices.
- **Steps**:

1. Open **Server Manager** and select **Add Roles and Features**.
2. Choose **DHCP Server** and complete the wizard.
3. Configure a new DHCP scope to define the range of IP addresses to assign.



New Scope Wizard

IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address: 192 . 168 . 200 . 1

End IP address: 192 . 168 . 200 . 100

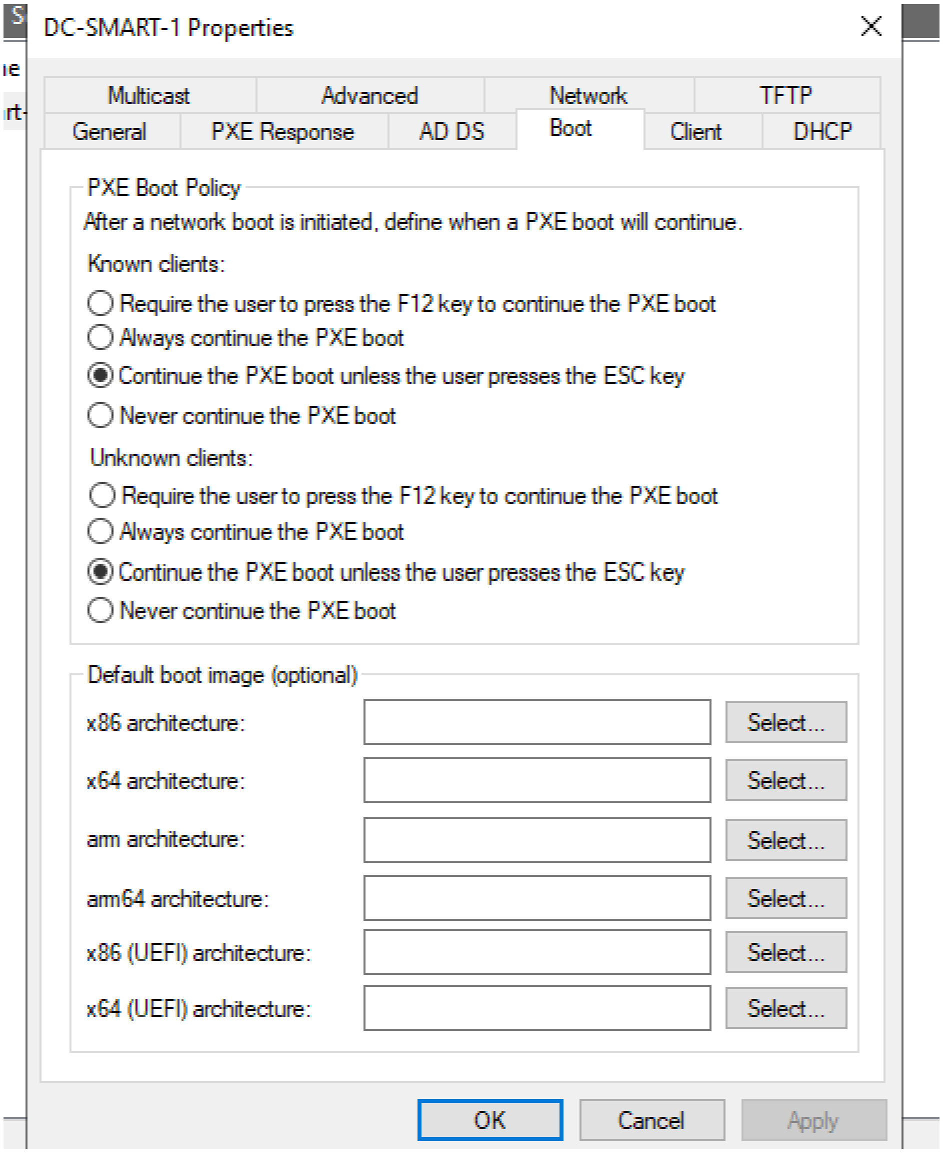
Configuration settings that propagate to DHCP Client

Length: 24

Subnet mask: 255 . 255 . 255 . 0

WDS (Windows Deployment Services) Configuration:

- **Purpose**: Allows network-based installation of Windows operating systems.
- **Steps**:
  1. Install **WDS** from the **Add Roles and Features** wizard.
  2. Configure WDS to use a pre-configured image for deployment.
  3. Set up a PXE boot configuration for client devices.



PXE Boot Policy

After a network boot is initiated, define when a PXE boot will continue.

Known clients:

○ Require the user to press the F12 key to continue the PXE boot
○ Always continue the PXE boot
● Continue the PXE boot unless the user presses the ESC key
○ Never continue the PXE boot

Unknown clients:

○ Require the user to press the F12 key to continue the PXE boot
○ Always continue the PXE boot
● Continue the PXE boot unless the user presses the ESC key
○ Never continue the PXE boot

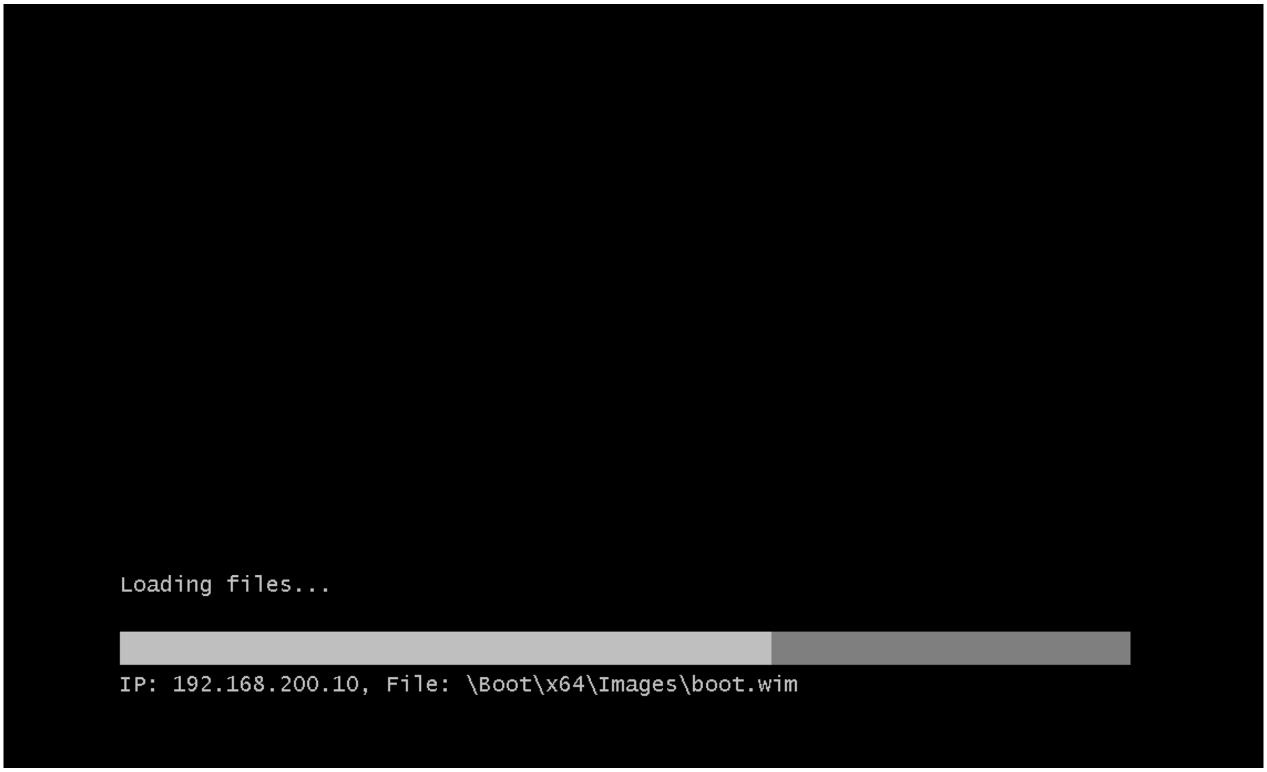
Default boot image (optional)

x86 architecture:		Select...
x64 architecture:		Select...
arm architecture:		Select...
arm64 architecture:		Select...
x86 (UEFI) architecture:		Select...
x64 (UEFI) architecture:		Select...

-

Test WDS on Windows 10 PC

1. **Boot the Windows 10 PC:**
    a. Restart the PC, and it should attempt to PXE boot.
    b. If PXE boot is enabled and properly configured, the PC will try to connect to the WDS server.
2. **Observe PXE Boot Process:**
    a. The PC should request a boot image from the WDS server.
    b. It will download the boot image (usually boot.wim) and begin the process of loading the Windows Preinstallation Environment (WinPE).
3. **Select the Install Image:**
    a. After loading the boot image, you'll see the WDS client interface.
    b. Select the appropriate installation image for Windows 10 from the list (if configured on the WDS server).
4. **Follow Installation Steps:**
    5. Once the image is selected, the installation process will begin.
    6. Follow the on-screen prompts to deploy Windows 10 to the PC.



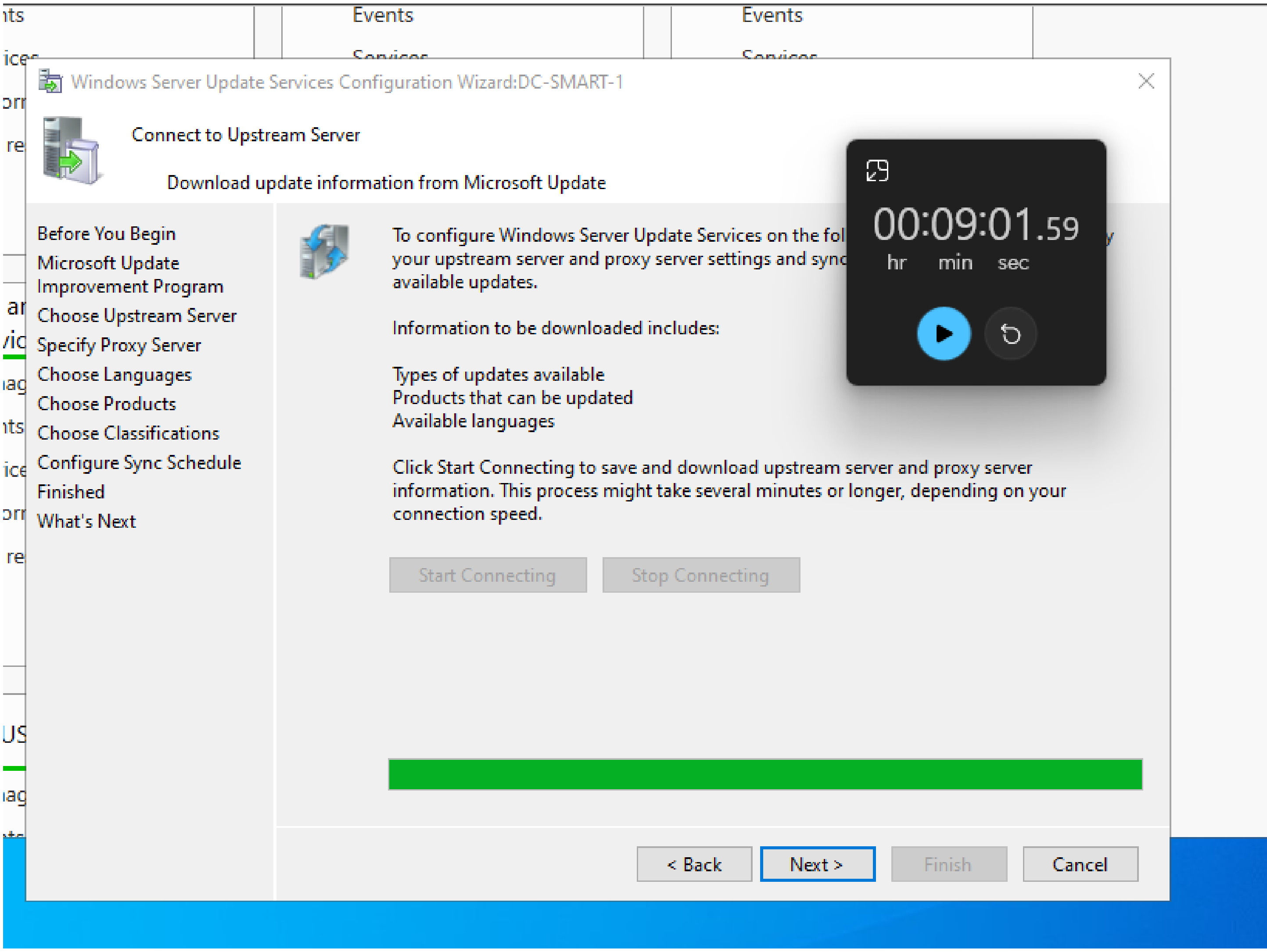
```
Loading files...

IP: 192.168.200.10, File: \Boot\x64\Images\boot.wim
```

WSUS (Windows Server Update Services):

- **Purpose**: Manages updates for Microsoft products within the network.
- **Steps**:

   1. **Install WSUS via Server Manager.**



Windows Server Update Services Configuration Wizard:DC-SMART-1

Connect to Upstream Server

Download update information from Microsoft Update

To configure Windows Server Update Services on the fol your upstream server and proxy server settings and sync available updates.

Information to be downloaded includes:

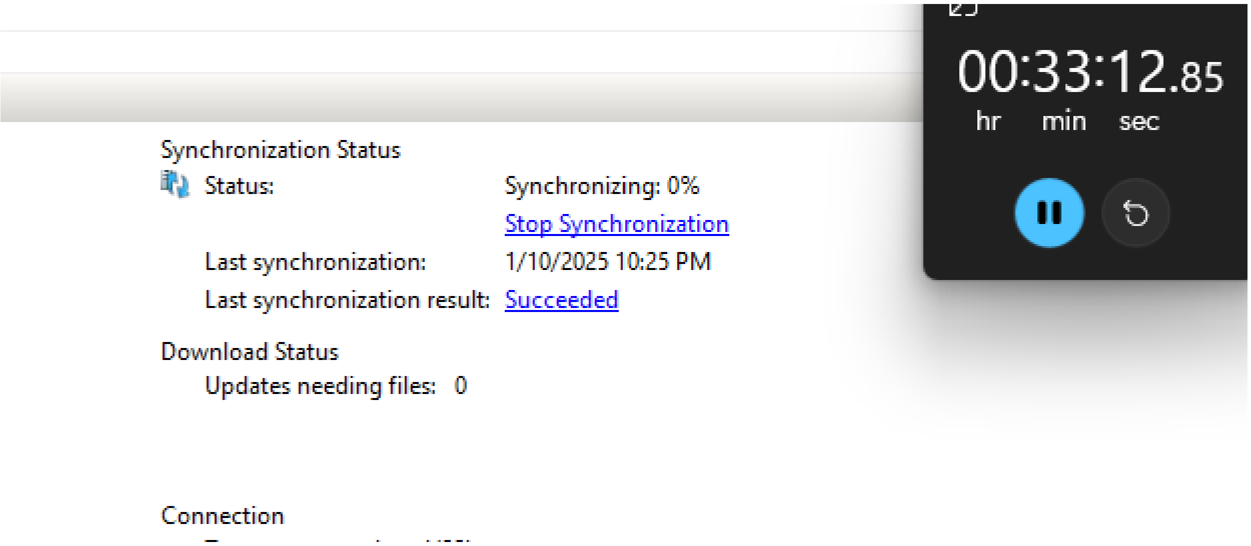
Types of updates available
Products that can be updated
Available languages

Click Start Connecting to save and download upstream server and proxy server information. This process might take several minutes or longer, depending on your connection speed.

-

2. Configuring WSUS and Reviewing Updates

- Open the **Update Services** console.
- Synchronize updates with Microsoft Update servers.



Synchronization Status

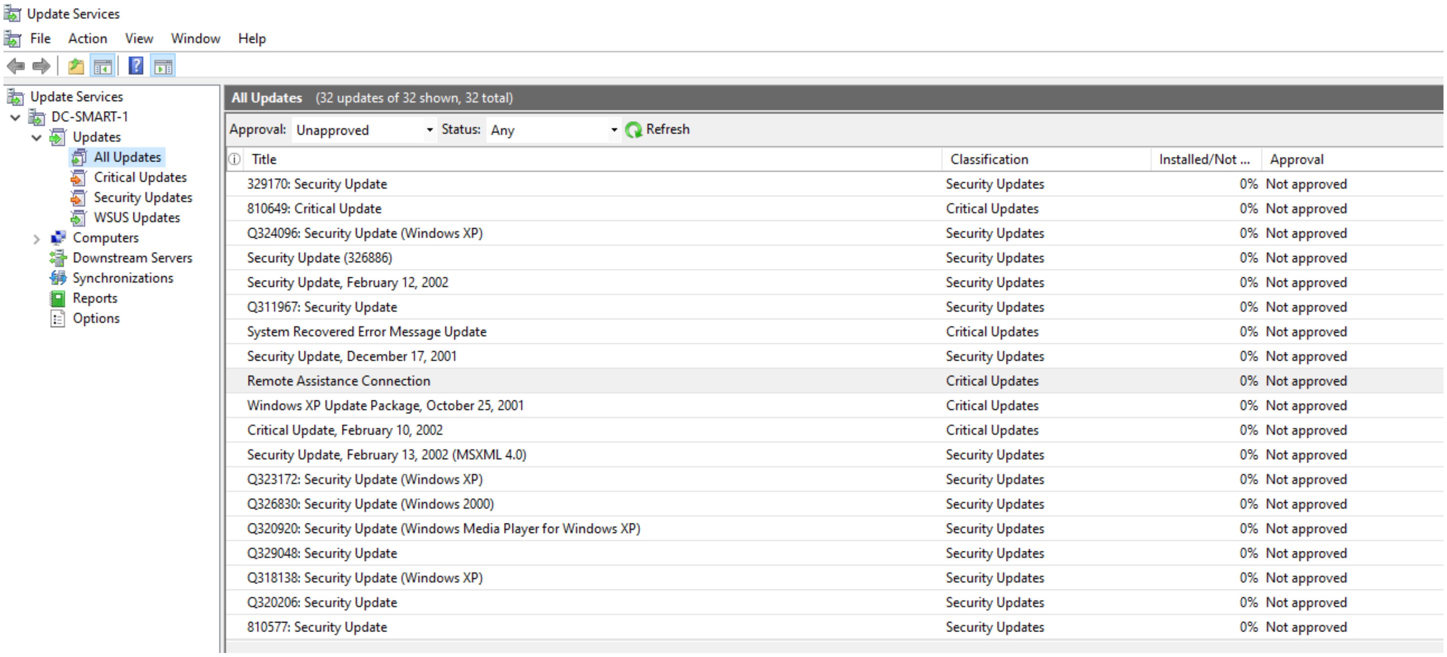
Status: Synchronizing: 0%
Stop Synchronization
Last synchronization: 1/10/2025 10:25 PM
Last synchronization result: Succeeded

Download Status

Updates needing files: 0

Connection

- Create a **group (“Win10”)** for all Pcs that require updates.
- Review updates under **All Updates**.
- Select updates you want to deploy and approve them for target groups ("Win10").



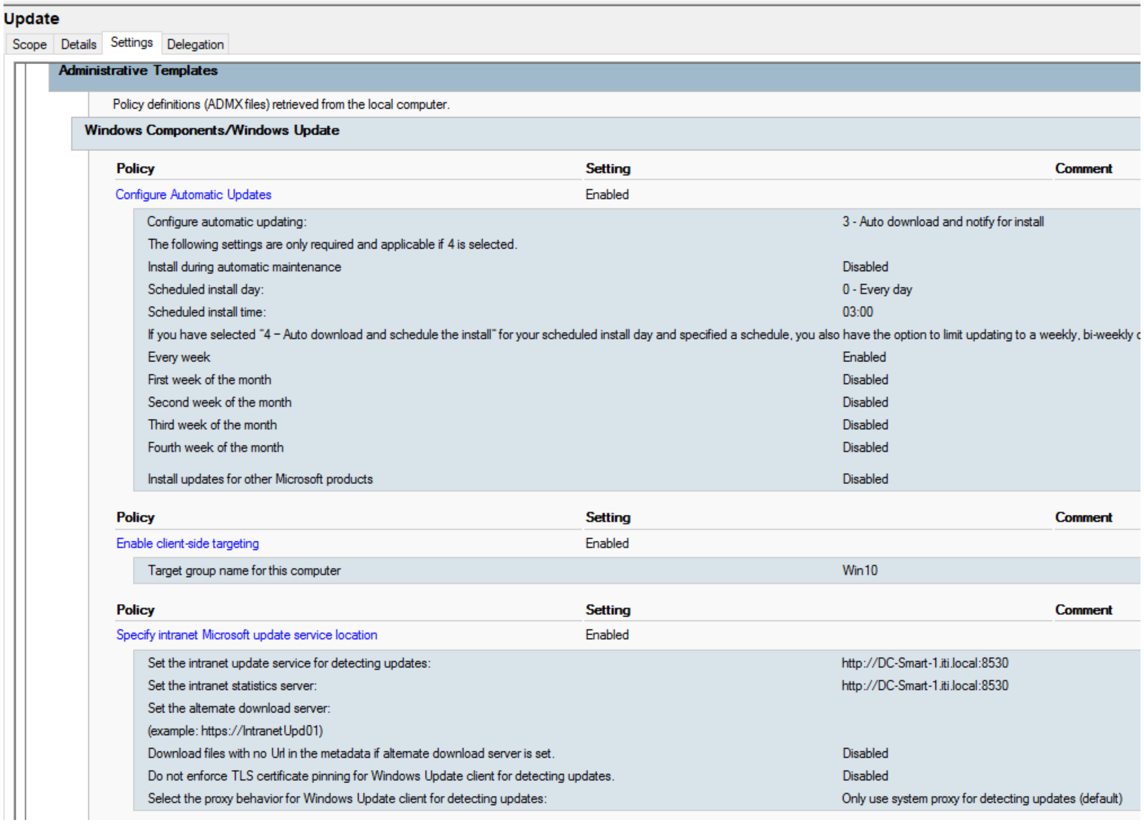
All Updates (32 updates of 32 shown, 32 total)

Approval: Unapproved Status: Any

Title	Classification	Installed/Not ...	Approval
329170: Security Update	Security Updates	0%	Not approved
810649: Critical Update	Critical Updates	0%	Not approved
Q324096: Security Update (Windows XP)	Security Updates	0%	Not approved
Security Update (326886)	Security Updates	0%	Not approved
Security Update, February 12, 2002	Security Updates	0%	Not approved
Q311967: Security Update	Security Updates	0%	Not approved
System Recovered Error Message Update	Critical Updates	0%	Not approved
Security Update, December 17, 2001	Security Updates	0%	Not approved
Remote Assistance Connection	Critical Updates	0%	Not approved
Windows XP Update Package, October 25, 2001	Critical Updates	0%	Not approved
Critical Update, February 10, 2002	Critical Updates	0%	Not approved
Security Update, February 13, 2002 (MSXML 4.0)	Security Updates	0%	Not approved
Q323172: Security Update (Windows XP)	Security Updates	0%	Not approved
Q326830: Security Update (Windows 2000)	Security Updates	0%	Not approved
Q320920: Security Update (Windows Media Player for Windows XP)	Security Updates	0%	Not approved
Q329048: Security Update	Security Updates	0%	Not approved
Q318138: Security Update (Windows XP)	Security Updates	0%	Not approved
Q320206: Security Update	Security Updates	0%	Not approved
810577: Security Update	Security Updates	0%	Not approved

3.Open Group Policy Management Console (GPMC) on your Domain Controller.

- Navigate to:
    - **Computer Configuration > Administrative Templates > Windows Components > Windows Update**.
- Enable the following policies:
    - **Configure Automatic Updates**:
        - Set to **Auto download and notify for install (3)**.
        - Schedule updates to install daily at **3:00 AM.**
- **Enable Client-Side Targeting**:
    - Enable this policy and set the target group name ("Win10").
- **Specify Intranet Microsoft Update Service Location**



Administrative Templates

Policy definitions (ADMX files) retrieved from the local computer.

Windows Components/Windows Update

Policy	Setting	Comment
Configure Automatic Updates	Enabled	

Configure automatic updating:	3 - Auto download and notify for install
The following settings are only required and applicable if 4 is selected.	
Install during automatic maintenance	Disabled
Scheduled install day:	0 - Every day
Scheduled install time:	03:00
If you have selected "4 – Auto download and schedule the install" for your scheduled install day and specified a schedule, you also have the option to limit updating to a weekly, bi-weekly c	
Every week	Enabled
First week of the month	Disabled
Second week of the month	Disabled
Third week of the month	Disabled
Fourth week of the month	Disabled
Install updates for other Microsoft products	Disabled

Policy	Setting	Comment
Enable client-side targeting	Enabled	

Target group name for this computer	Win10

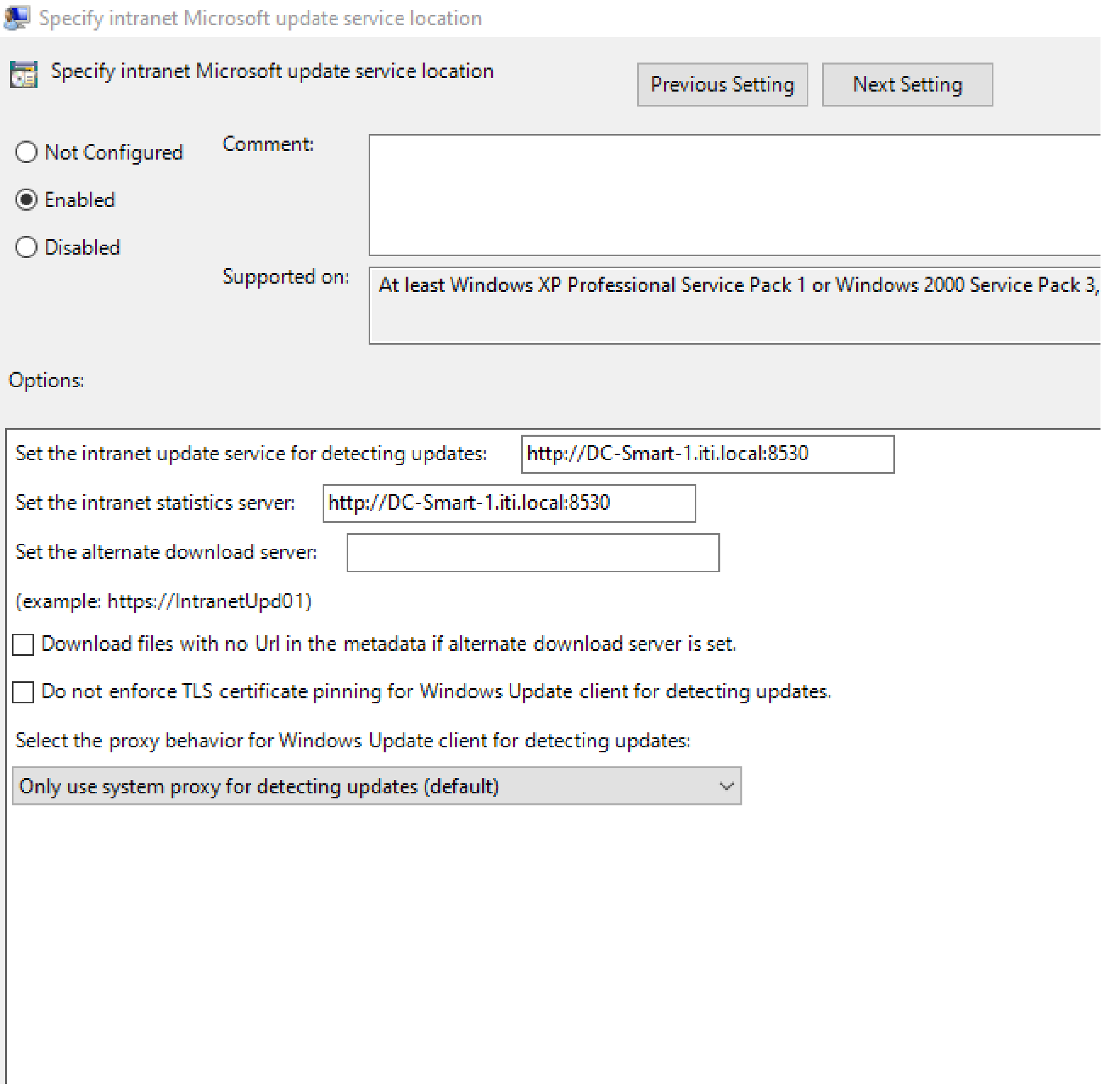
Policy	Setting	Comment
Specify intranet Microsoft update service location	Enabled	

Set the intranet update service for detecting updates:	http://DC-Smart-1.iti.local:8530
Set the intranet statistics server:	http://DC-Smart-1.iti.local:8530
Set the alternate download server:	
(example: https://IntranetUpd01)	
Download files with no Url in the metadata if alternate download server is set.	Disabled
Do not enforce TLS certificate pinning for Windows Update client for detecting updates.	Disabled
Select the proxy behavior for Windows Update client for detecting updates:	Only use system proxy for detecting updates (default)

4. Configuring the WSUS Service Location:

1. Navigate to the **Specify Intranet Microsoft Update Service Location** policy.

2. Enable the policy and configure the following:
   - **Intranet Update Service URL**:
     http://DC-SMART-1.iti.local:8530
   - **Statistics Server URL**: Same as above.
3. Leave other settings as default unless specific customizations are needed.



Specify intranet Microsoft update service location

Specify intranet Microsoft update service location

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows XP Professional Service Pack 1 or Windows 2000 Service Pack 3,

Options:

Set the intranet update service for detecting updates: http://DC-Smart-1.iti.local:8530

Set the intranet statistics server: http://DC-Smart-1.iti.local:8530

Set the alternate download server:

(example: https://IntranetUpd01)

□ Download files with no Url in the metadata if alternate download server is set.

□ Do not enforce TLS certificate pinning for Windows Update client for detecting updates.

Select the proxy behavior for Windows Update client for detecting updates:

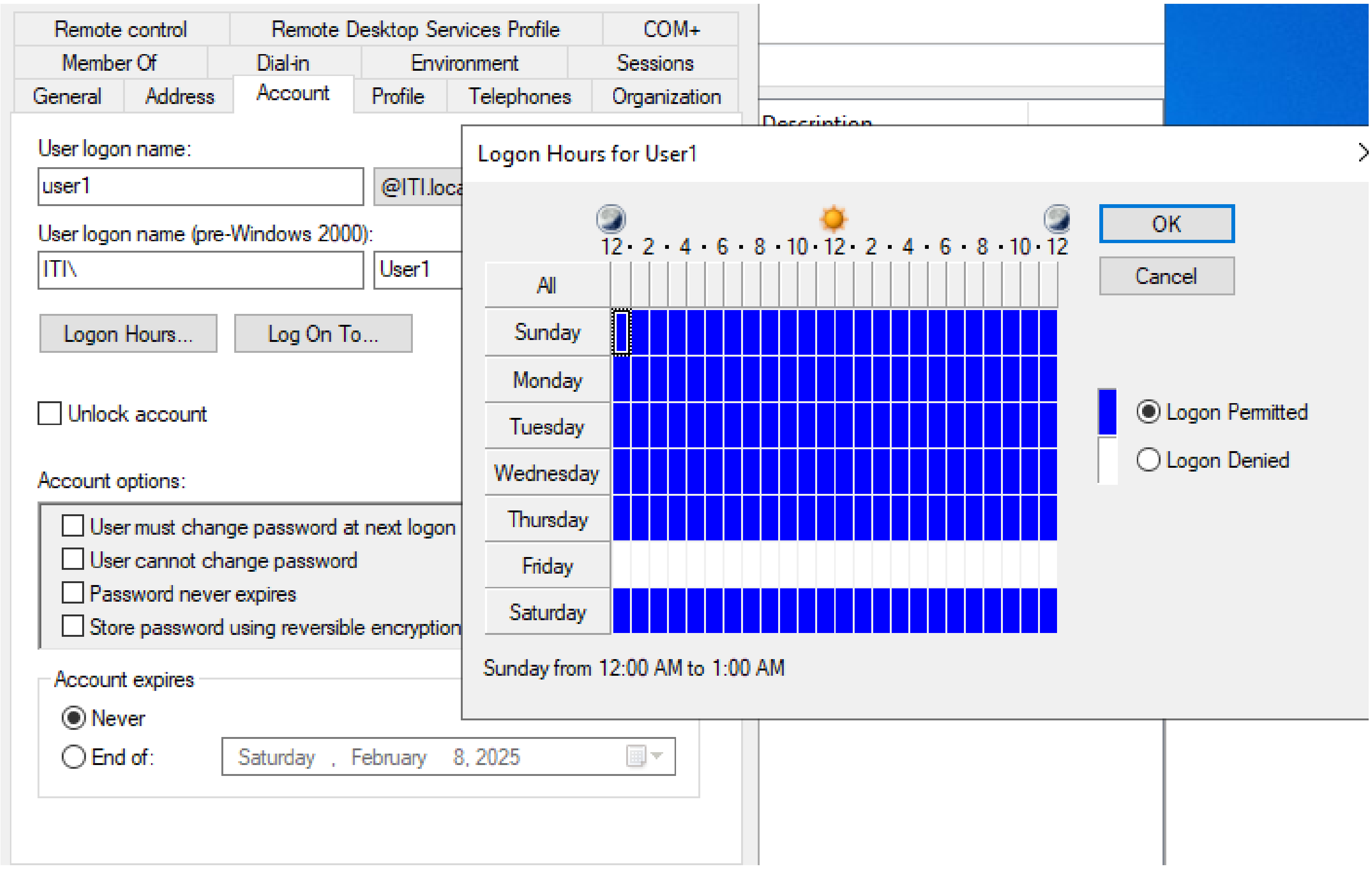
Only use system proxy for detecting updates (default)

5. Make sure to link the policy to OU with all the PCs that require update

Group Policies for Smart Users

a) Restrict User Login Times

- **Requirement**: User1@iti.local cannot log in on Fridays.
- **Configuration**:
    1. Open Group Policy Management.
    2. Edit the policy for User1 to set logon hours.



User logon name: user1 @ITI.loca

User logon name (pre-Windows 2000): ITI\ User1

□ 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: Saturday , February 8, 2025

Logon Hours for User1

12 · 2 · 4 · 6 · 8 · 10 · 12 · 2 · 4 · 6 · 8 · 10 · 12

Sunday	🟦 12 AM – 12 AM
Monday	🟦 12 AM – 12 AM
Tuesday	🟦 12 AM – 12 AM
Wednesday	🟦 12 AM – 12 AM
Thursday	🟦 12 AM – 12 AM
Friday	⬜ 12 AM – 12 AM
Saturday	🟦 12 AM – 12 AM

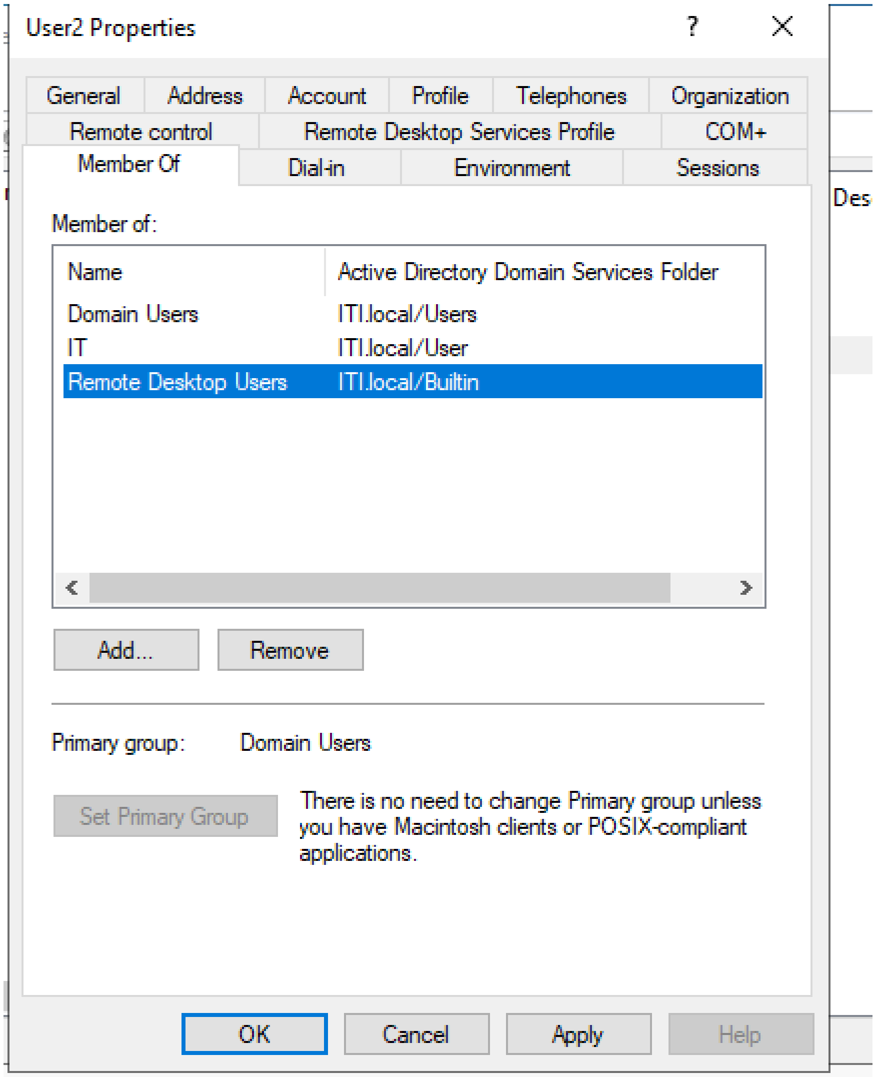
🟦 ● Logon Permitted
⬜ ○ Logon Denied

Sunday from 12:00 AM to 1:00 AM

b) Restrict Remote Login for Non-Admins

- **Requirement**: User2@iti.local can log in `PC1` remotely to the PDC but is not a Domain Admin.
- **Configuration**:

1. **Add User2 to the Remote Desktop Users group.**



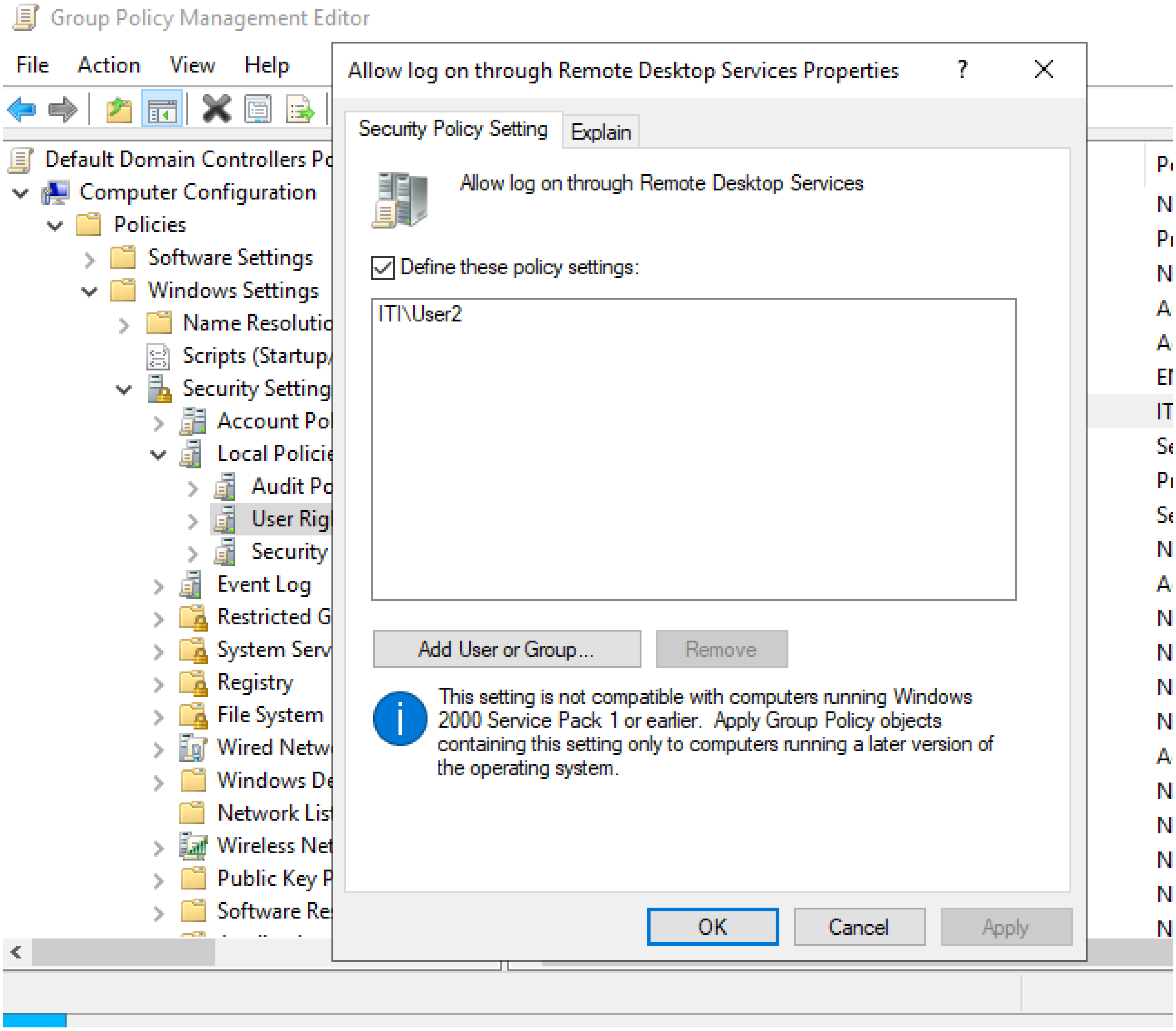
Member of:

Name	Active Directory Domain Services Folder
Domain Users	ITI.local/Users
IT	ITI.local/User
Remote Desktop Users	ITI.local/Builtin

Primary group: Domain Users

There is no need to change Primary group unless you have Macintosh clients or POSIX-compliant applications.

2. **Apply a Group Policy to allow remote login for User2.**



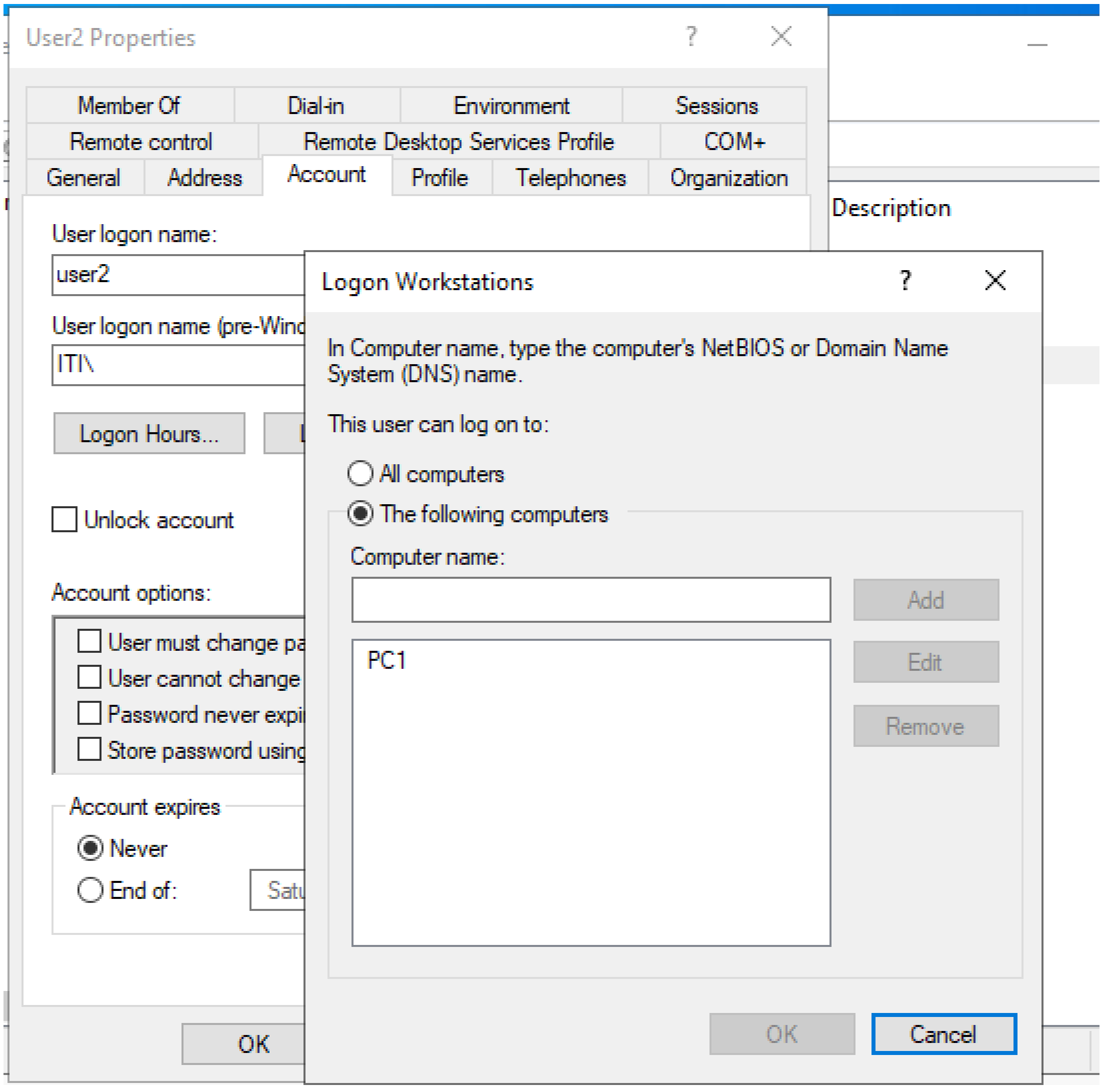
☑ Define these policy settings:

ITI\User2

This setting is not compatible with computers running Windows 2000 Service Pack 1 or earlier. Apply Group Policy objects containing this setting only to computers running a later version of the operating system.

-

3. Add `PC1` as logon workstation



User2 Properties

Member Of | Dial-in | Environment | Sessions | Remote control | Remote Desktop Services Profile | COM+ | General | Address | Account | Profile | Telephones | Organization

User logon name: user2

User logon name (pre-Wind

ITI\

Logon Hours...

☐ Unlock account

Account options:

☐ User must change pa

☐ User cannot change

☐ Password never expi

☐ Store password using

Account expires

● Never

○ End of: Satu

OK

Logon Workstations

In Computer name, type the computer's NetBIOS or Domain Name System (DNS) name.

This user can log on to:

○ All computers

● The following computers

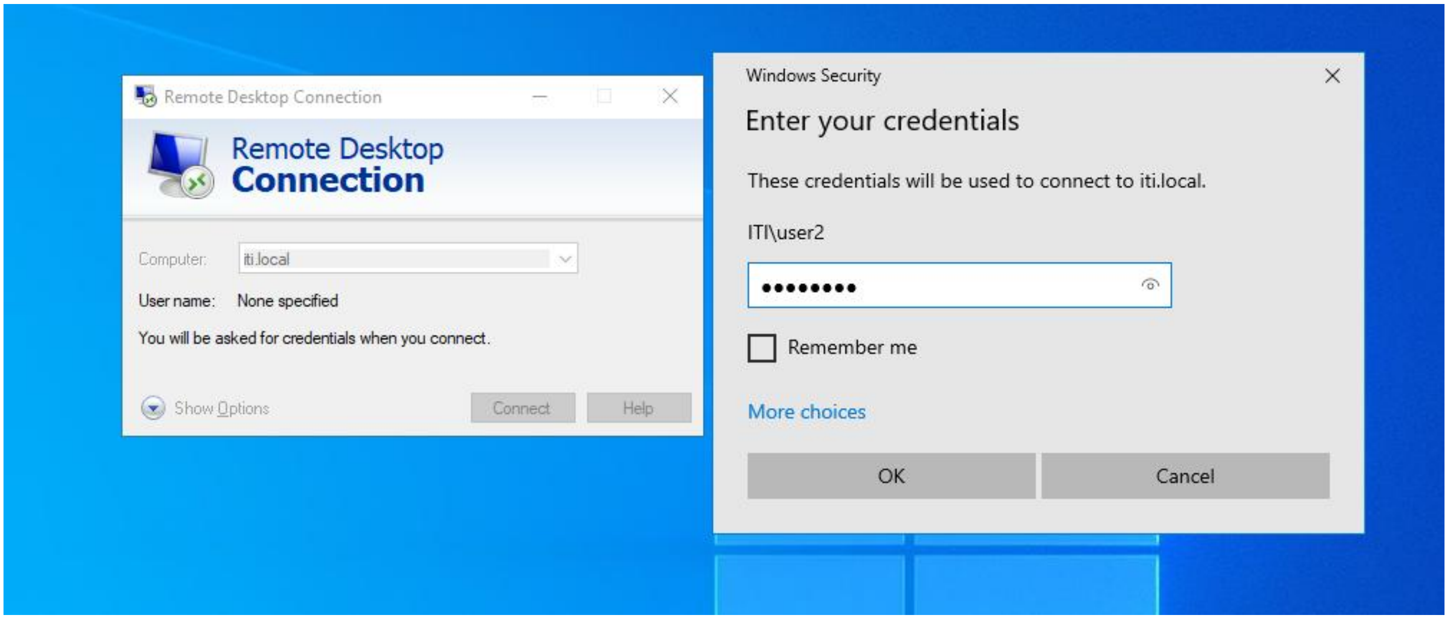
Computer name:

PC1

Add | Edit | Remove

OK | Cancel

4. **Test Remote Desktop connection.**



Remote Desktop Connection

Remote Desktop **Connection**

Computer: iti.local

User name: None specified

You will be asked for credentials when you connect.

Windows Security

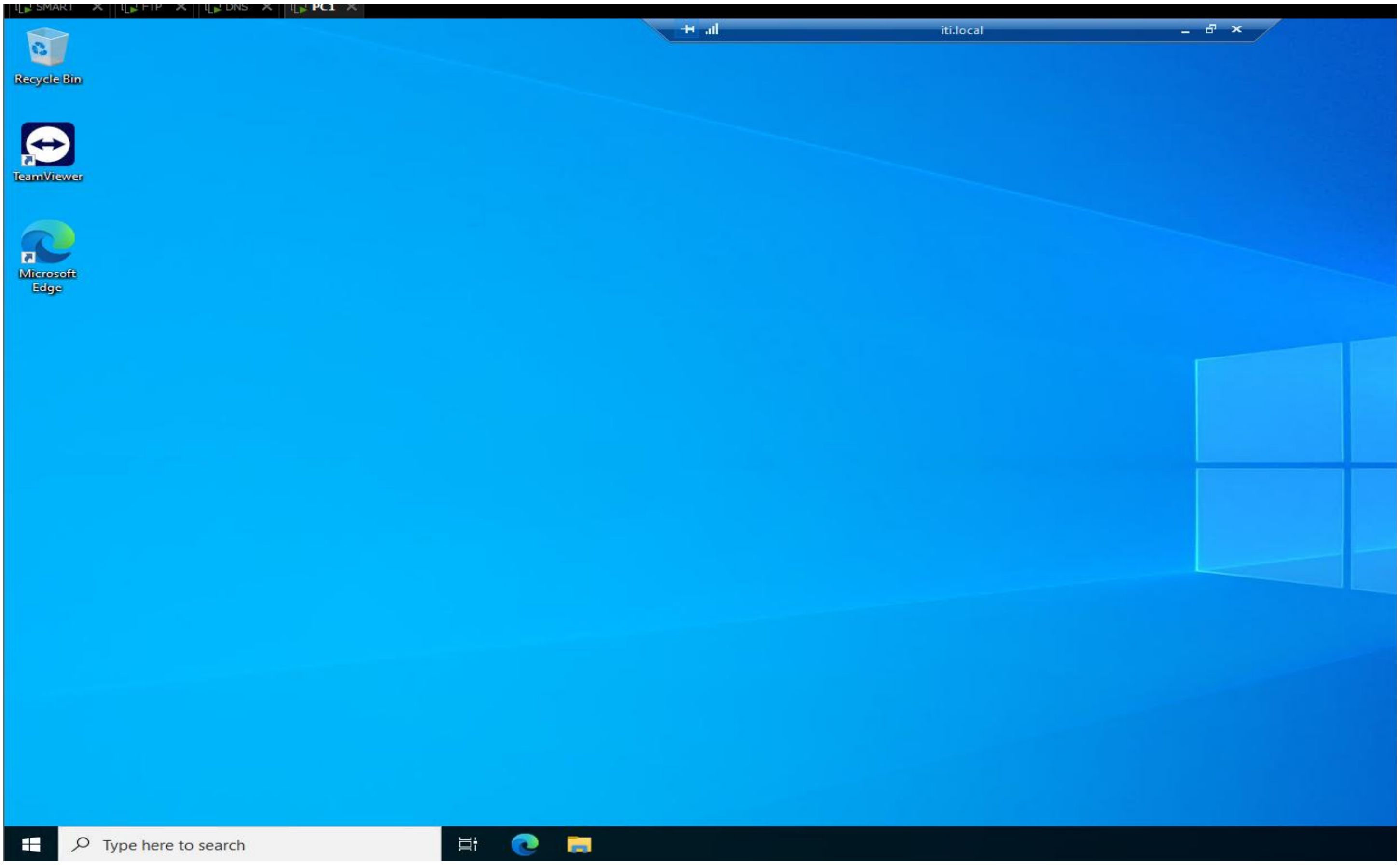
Enter your credentials

These credentials will be used to connect to iti.local.

ITI\user2

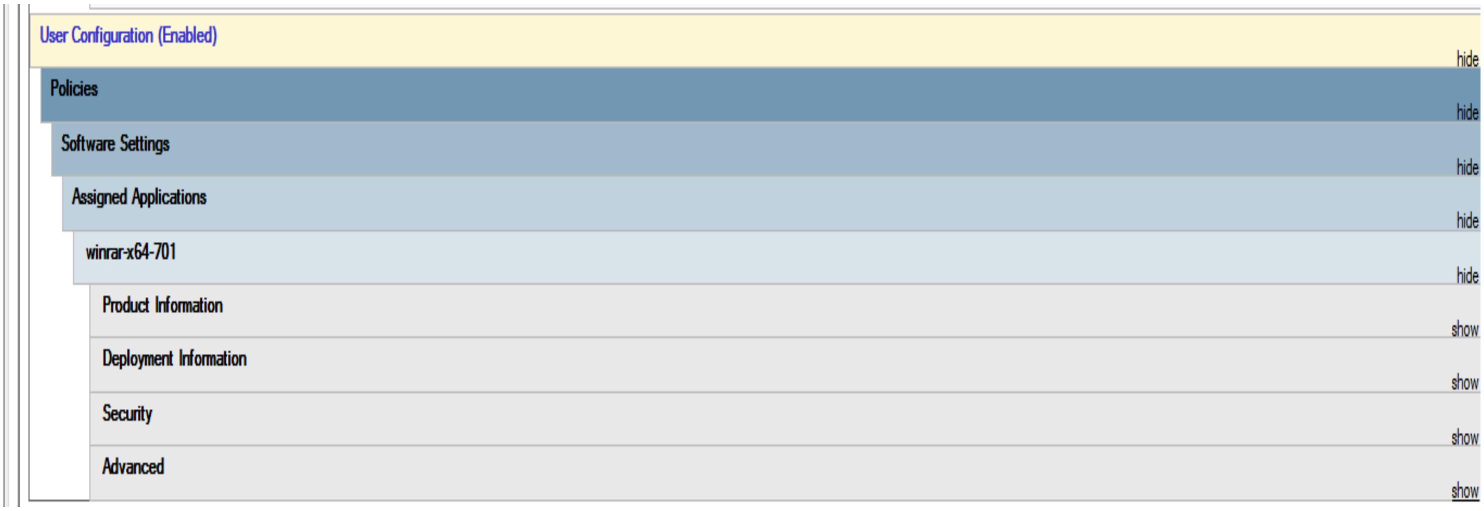
●●●●●●●●●

□ Remember me



c) Software Deployment via Group Policies

- **Requirement: User3@iti.local must have WinRAR installed automatically.**
- **Configuration:**
  1. **Create a new Group Policy Object (GPO) for software deployment.**
  2. **Assign WinRAR to User3 using User Configuration > Software Installation.**



User Configuration (Enabled) hide

Policies hide

Software Settings hide

Assigned Applications hide

winrar-x64-701 hide

Product Information show

Deployment Information show

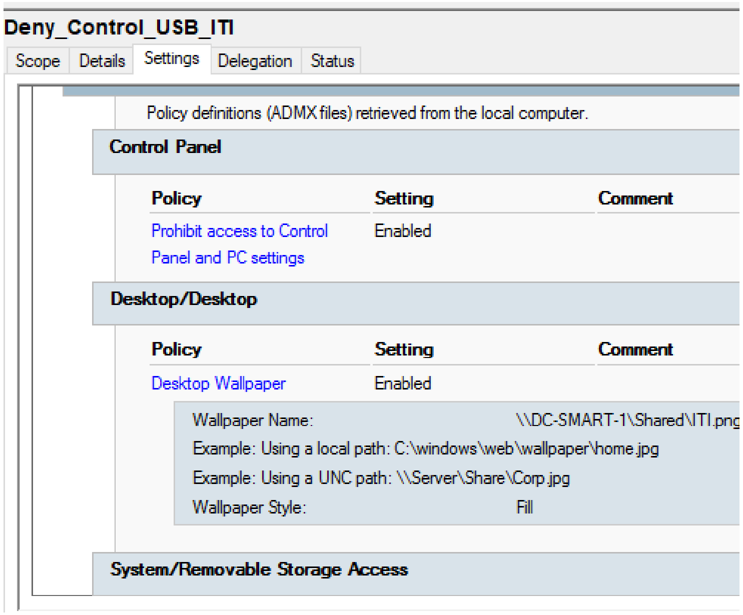
Security show

Advanced show

5. Device and Control Panel Restrictions & Desktop Customization

Requirement: `User3@iti.local` and `User4@iti.local` are restricted from using flash drives , accessing Control Panel and Set a custom wallpaper for `User3` and `User4`.

- **Configuration**:
  - Create GPOs:
    - `xFlashMemory` to deny USB storage.
    - `xControlPanel` to hide Control Panel access.
  - Apply these policies to their organizational unit (OU).
  - Use GPO to set desktop wallpaper under:
    - **User Configuration** > **Administrative Templates** > **Desktop** > **Desktop Wallpaper**.



Deny_Control_USB_ITI

Policy definitions (ADMX files) retrieved from the local computer.

Control Panel

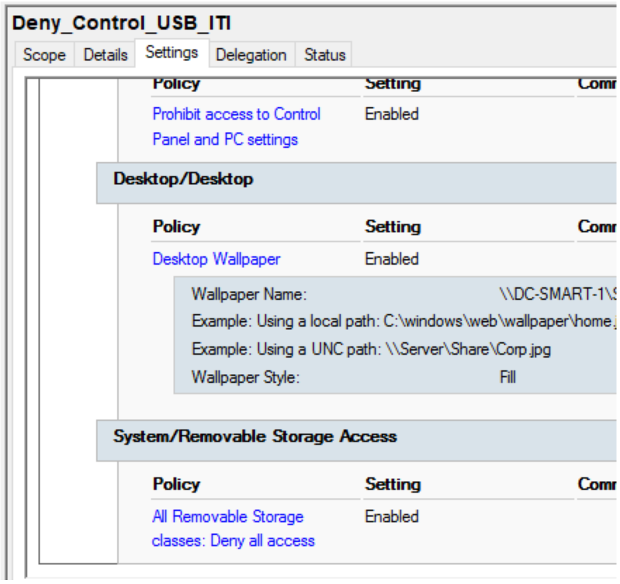
Policy	Setting	Comment
Prohibit access to Control Panel and PC settings	Enabled	

Desktop/Desktop

Policy	Setting	Comment
Desktop Wallpaper	Enabled	

Wallpaper Name:	\\DC-SMART-1\Shared\ITI.png
Example: Using a local path: C:\windows\web\wallpaper\home.jpg	
Example: Using a UNC path: \\Server\Share\Corp.jpg	
Wallpaper Style:	Fill

System/Removable Storage Access



Deny_Control_USB_ITI

Policy	Setting	Comr
Prohibit access to Control Panel and PC settings	Enabled	

Desktop/Desktop

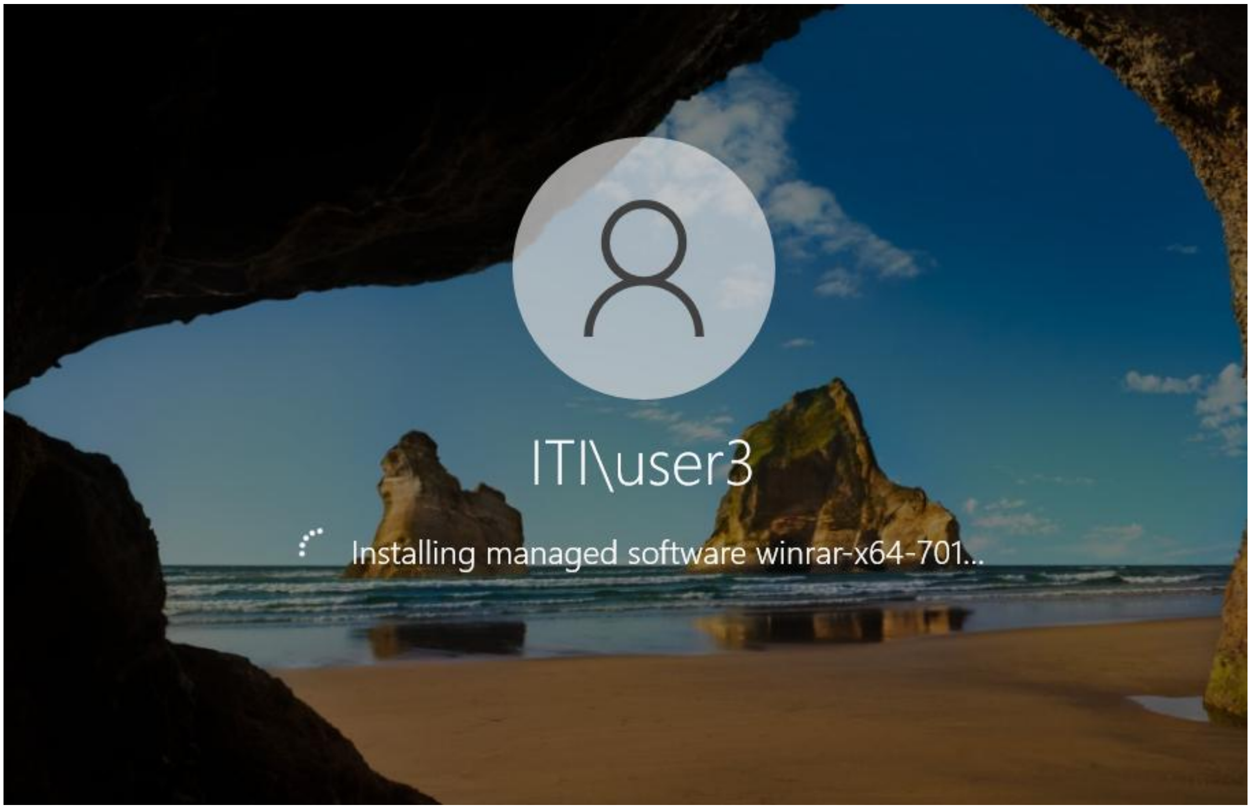
Policy	Setting	Comr
Desktop Wallpaper	Enabled	

Wallpaper Name:	\\DC-SMART-1\S
Example: Using a local path: C:\windows\web\wallpaper\home.j	
Example: Using a UNC path: \\Server\Share\Corp.jpg	
Wallpaper Style:	Fill

System/Removable Storage Access

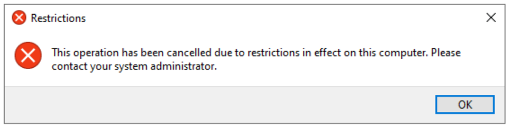
Policy	Setting	Comr
All Removable Storage classes: Deny all access	Enabled	

- Test Policies at User3



ITI\user3

Installing managed software winrar-x64-701...

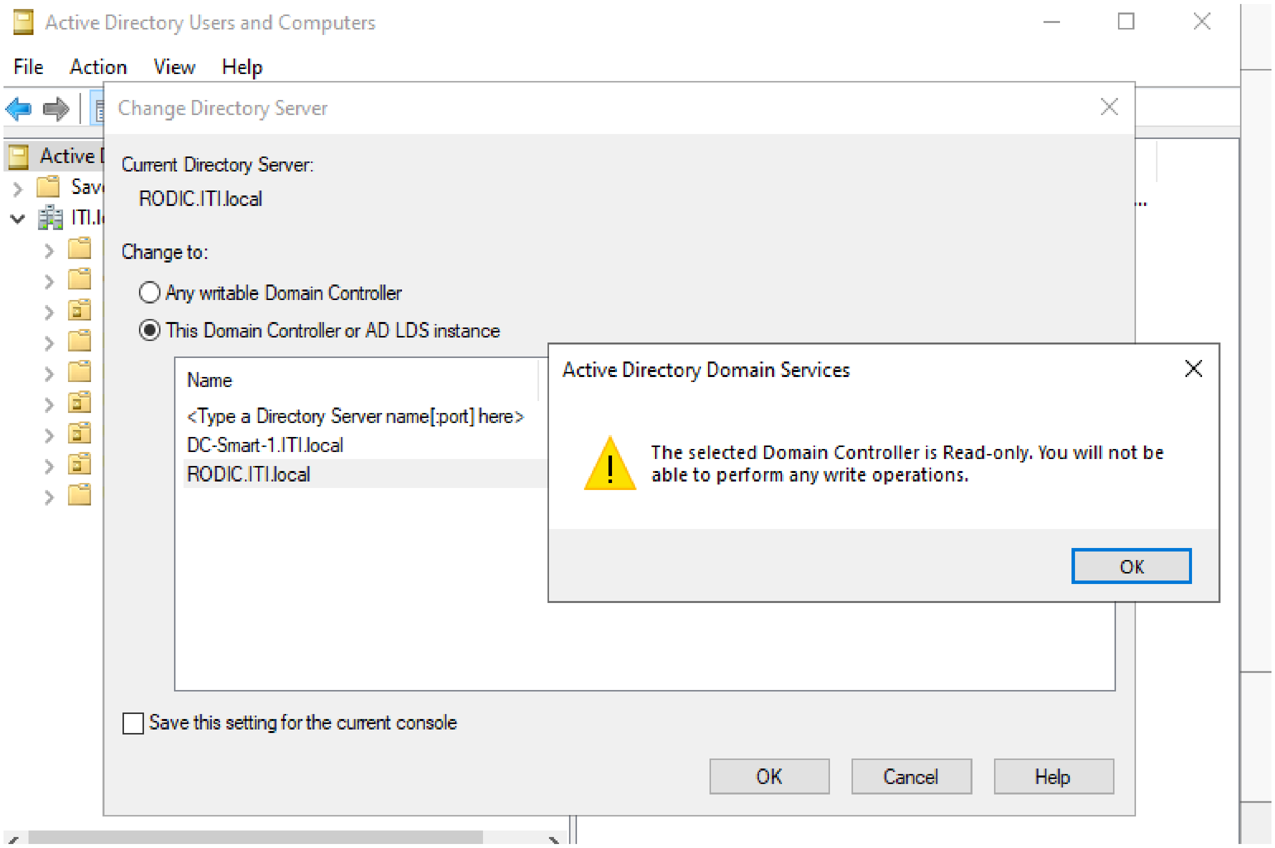


This operation has been cancelled due to restrictions in effect on this computer. Please contact your system administrator.

READ-ONLY DOMAIN CONTROLLER (RODC)

Configuration

- **Steps**:
    1. Install AD DS on a new server and promote it as an RODC.
    2. Configure **Password Replication Policy (PRP)** to limit permissions.
    3. Use Group Policy to apply access restrictions.



Current Directory Server:

RODIC.ITI.local

Change to:

○ Any writable Domain Controller

● This Domain Controller or AD LDS instance

Name
<Type a Directory Server name[:port] here>
DC-Smart-1.ITI.local
RODIC.ITI.local

□ Save this setting for the current console

Active Directory Domain Services

The selected Domain Controller is Read-only. You will not be able to perform any write operations.

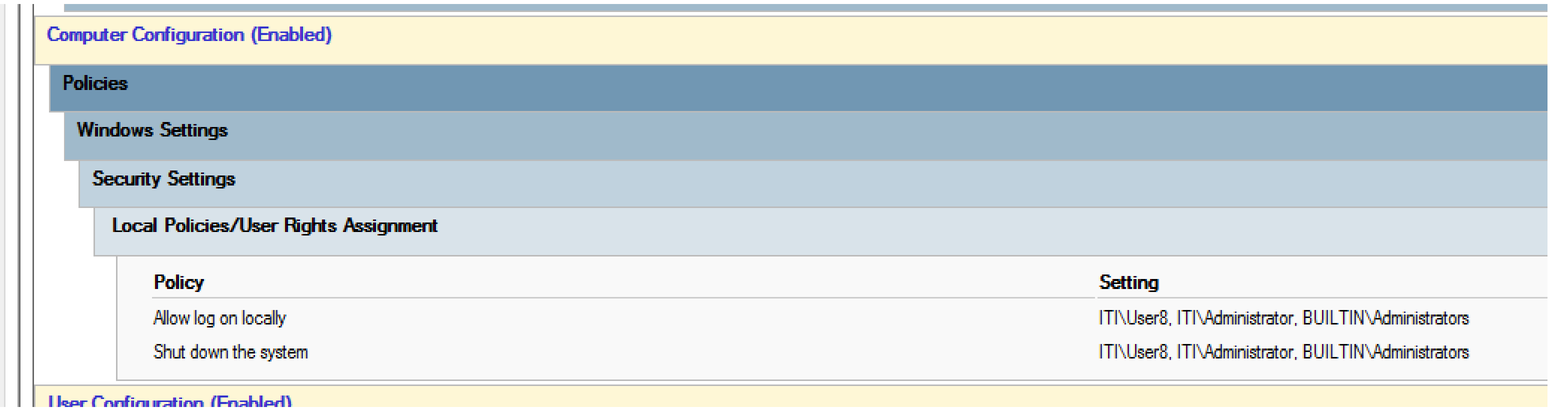
POLICIES FOR RODC USERS

a) Local Access and Shutdown Permissions

a) **Requirement**: User8 can log in locally to the RODC but cannot create users.

b) **Configuration**:

1. **Allow User8 to Shut Down the RODC and Logon Locally :**
    - Create a **GPO on DC.**
    - Go to **Security Settings > Local Policies > User Rights Assignment**.
    - Double-click **Shut down the system** and add **User8**.
    - Double-click **Allow log on locally** and add **User8**.
    - make sure to link the **GPO** to the **RODC**



Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Local Policies/User Rights Assignment

Policy	Setting
Allow log on locally	ITI\User8, ITI\Administrator, BUILTIN\Administrators
Shut down the system	ITI\User8, ITI\Administrator, BUILTIN\Administrators

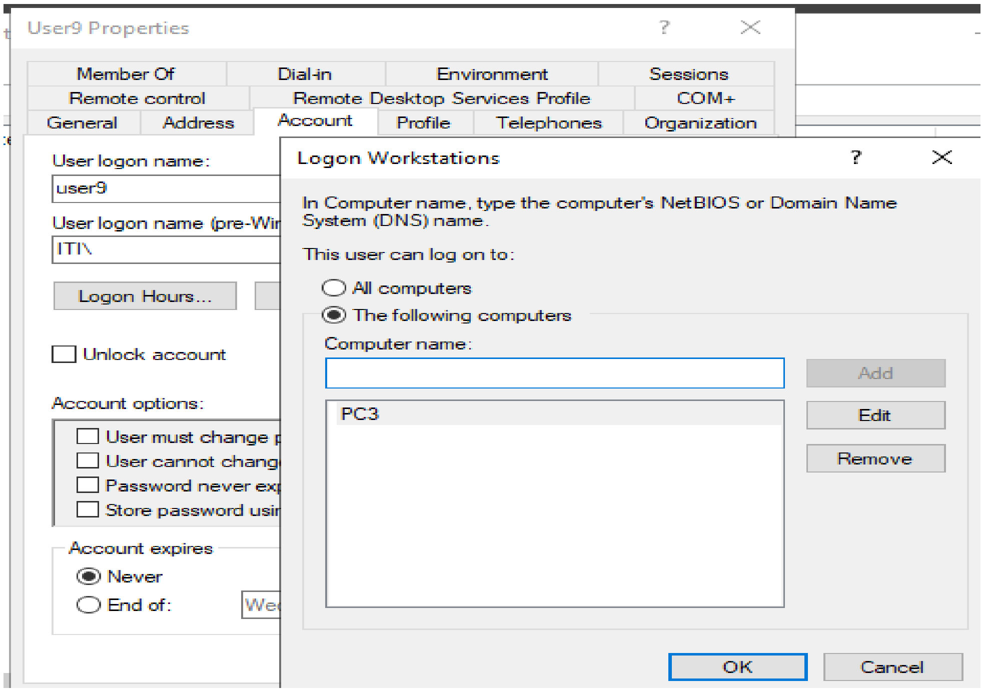
User Configuration (Enabled)

b) Login and Password Replication Policy

a)Requirement: User9 can login to pc3 and can replicate his password to the RODC

b)Configuration:

1. Allow User9 to Log in to PC3:



User logon name: user9

User logon name (pre-Wi ITI\

☐ Unlock account

☐ User must change p

☐ User cannot chang

☐ Password never ex

☐ Store password usi

● Never

○ End of: We

In Computer name, type the computer's NetBIOS or Domain Name System (DNS) name.

This user can log on to:

○ All computers

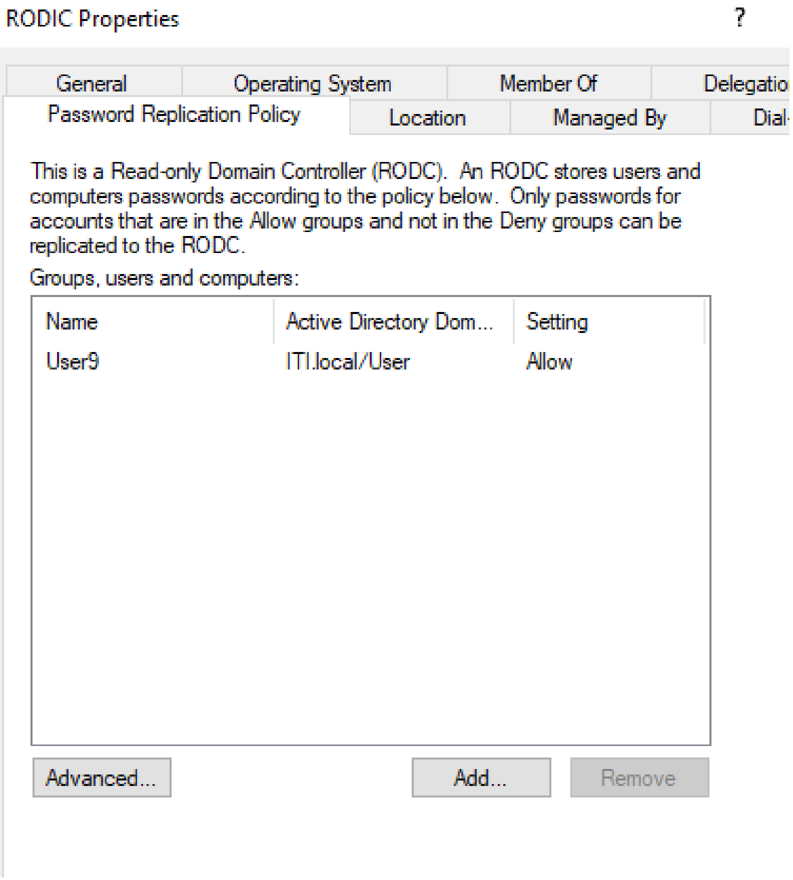
● The following computers

Computer name:

PC3

2. Enable Password Replication for User9

- Find the RODC:
- Right-click the RODC and select Properties.
- Go to the Password Replication Policy tab.
- Add User9 to the "Accounts whose passwords are allowed to replicate to this RODC" list.



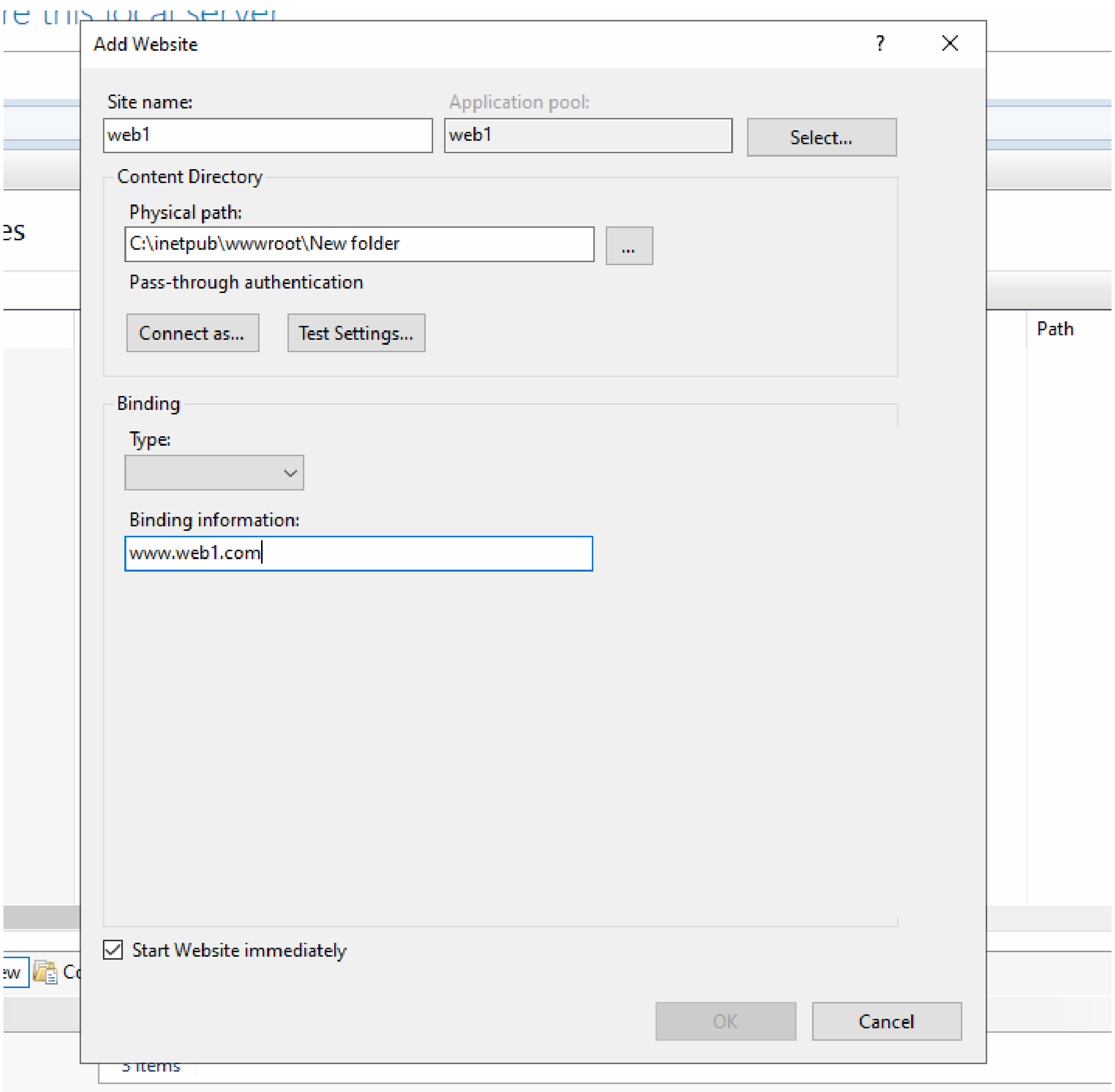
This is a Read-only Domain Controller (RODC). An RODC stores users and computers passwords according to the policy below. Only passwords for accounts that are in the Allow groups and not in the Deny groups can be replicated to the RODC.

Groups, users and computers:

Name	Active Directory Dom...	Setting
User9	ITI.local/User	Allow

Web and FTP Server

- **Configuration:**
  - **Requirement: Set up a Web and FTP Server for internal access.**
  - **Configuration:**
    - **Add the Internet Information Services (IIS) role.**
    - **Create two websites (www.web1.com and www.web2.com).**



Site name: web1

Application pool: web1

Content Directory

Physical path: C:\inetpub\wwwroot\New folder

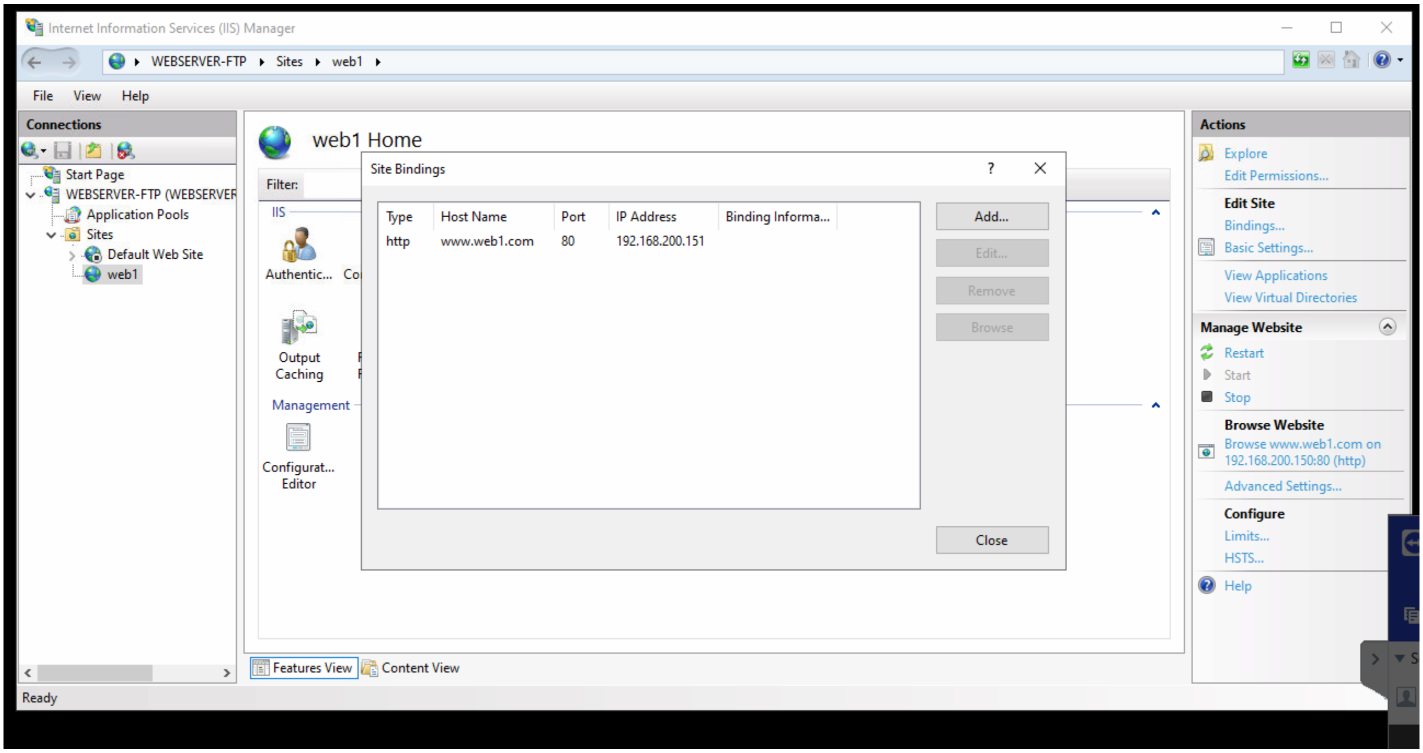
Pass-through authentication

Binding

Type:

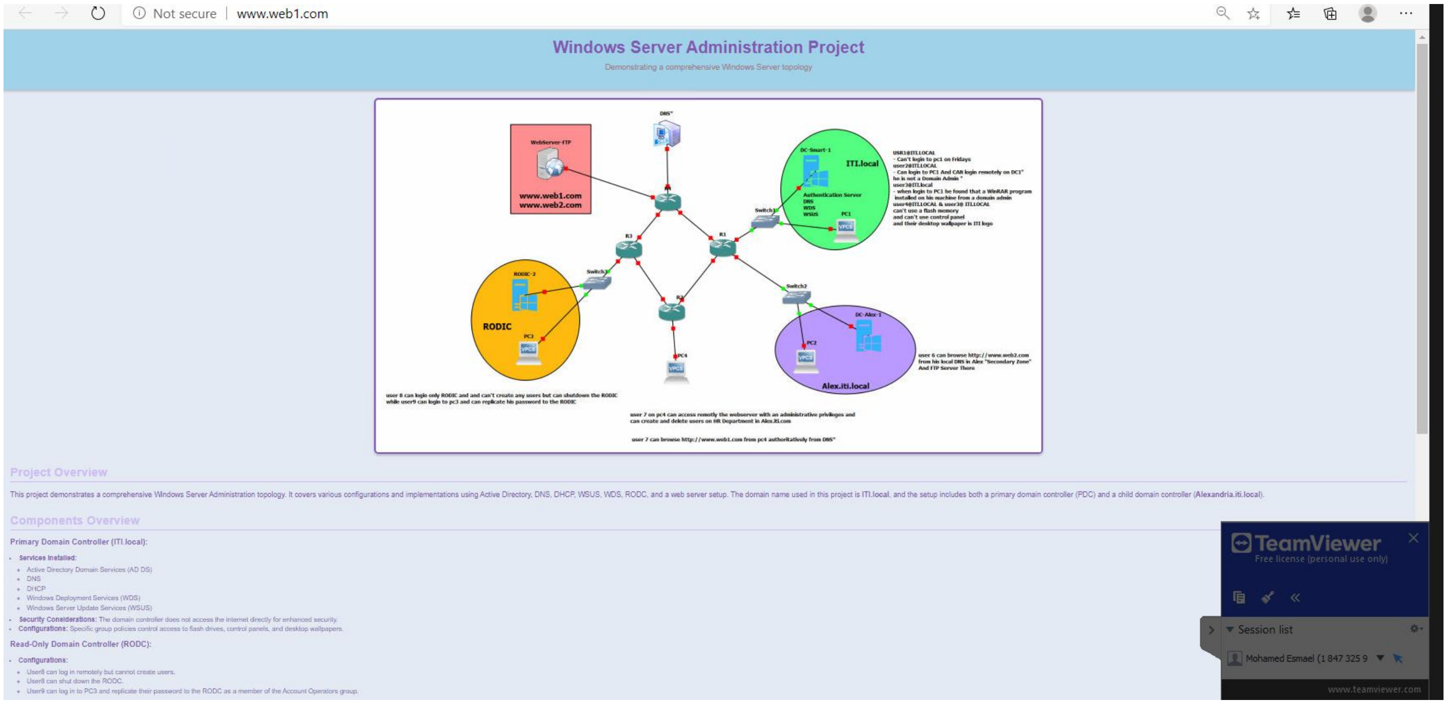
Binding information: www.web1.com

☑ Start Website immediately



Site Bindings

Type	Host Name	Port	IP Address	Binding Informa...
http	www.web1.com	80	192.168.200.151	



Windows Server Administration Project

Demonstrating a comprehensive Windows Server topology

USR1@ITI.LOCAL
- Can't login to pc1 on Fridays
user2@ITI.LOCAL
- Can login to PC1 And CAN login remotely on DC1"
he is not a Domain Admin "
user3@ITI.local
- when login to PC1 he found that a WinRAR program
installed on his machine from a domain admin
user4@ITI.LOCAL & user3@ ITI.LOCAL
can't use a flash memory
and can't use control panel
and their desktop wallpaper is ITI logo

user 6 can browse http://www.web2.com
from his local DNS in Alex "Secondary Zone"
And FTP Server There

user 8 can login only RODIC and and can't create any users but can shutdown the RODIC
while user9 can login to pc3 and can replicate his password to the RODIC

user 7 on pc4 can access remotly the webserver with an administrative privileges and
can create and delete users on HR Department in Alex.iti.com

user 7 can browse http://www.web1.com from pc4 authoritatively from DNS"

Project Overview

This project demonstrates a comprehensive Windows Server Administration topology. It covers various configurations and implementations using Active Directory, DNS, DHCP, WSUS, WDS, RODC, and a web server setup. The domain name used in this project is **ITI.local**, and the setup includes both a primary domain controller (PDC) and a child domain controller (**Alexandria.iti.local**).

Components Overview

Primary Domain Controller (ITI.local):

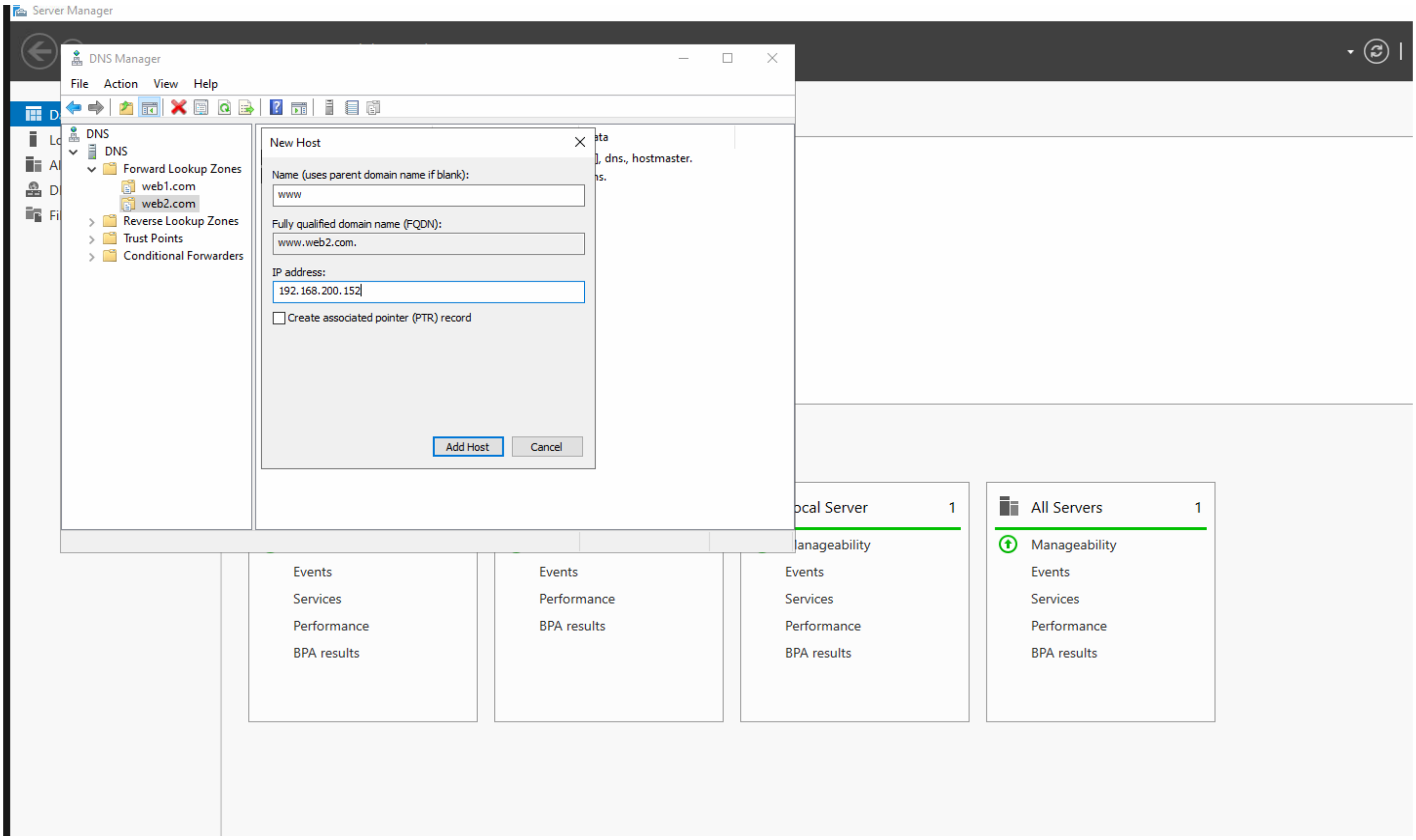
- **Services Installed:**
  - Active Directory Domain Services (AD DS)
  - DNS
  - DHCP
  - Windows Deployment Services (WDS)
  - Windows Server Update Services (WSUS)
- **Security Considerations:** The domain controller does not access the internet directly for enhanced security.
- **Configurations:** Specific group policies control access to flash drives, control panels, and desktop wallpapers.

Read-Only Domain Controller (RODC):

- **Configurations:**
  - User8 can log in remotely but cannot create users.
  - User8 can shut down the RODC.
  - User9 can log in to PC3 and replicate their password to the RODC as a member of the Account Operators group.

1. DNS (Domain Name System)

- **Purpose**: Resolves domain names to IP addresses, enabling users to connect to websites and network resources.
- **Steps**:
  1. Open **Server Manager** and click on **Add Roles and Features**.
  2. Select **DNS Server** and complete the installation.
  3. Use the **DNS Manager** to create new zones and configure forward and reverse lookup zones.



New Host

Name (uses parent domain name if blank): www

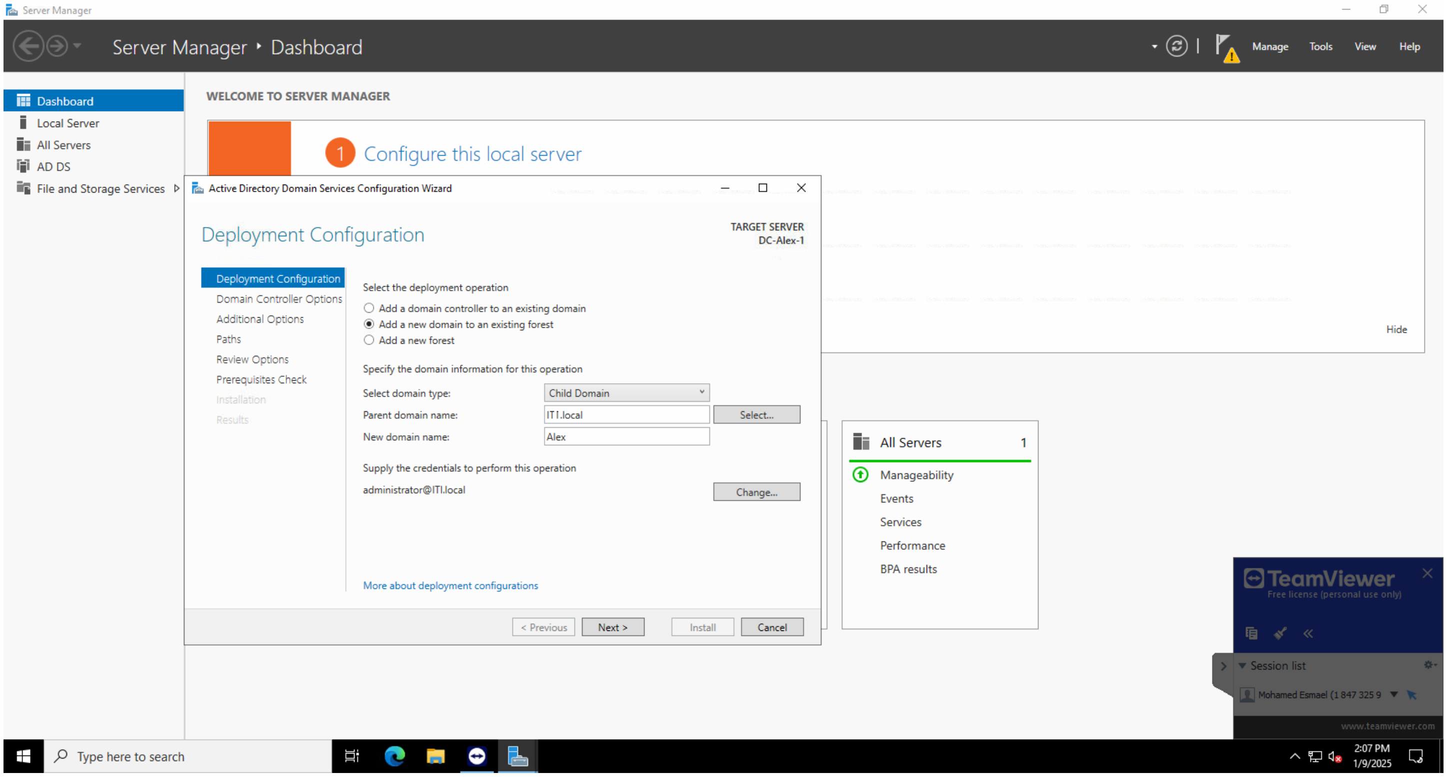
Fully qualified domain name (FQDN): www.web2.com.

IP address: 192.168.200.152

☐ Create associated pointer (PTR) record

Child Domain Setup (Alex)

- **Requirement**: Create a child domain alex.iti.local.
- **Configuration**:
  - Set up a new domain controller for the child domain.
  - Configure delegation of control for user management in Alexandria.



Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
DC-Alex-1

Select the deployment operation

○ Add a domain controller to an existing domain
● Add a new domain to an existing forest
○ Add a new forest

Specify the domain information for this operation

Select domain type: Child Domain

Parent domain name: ITI.local

New domain name: Alex

Supply the credentials to perform this operation

administrator@ITI.local

POLICIES FOR ALEX USERS

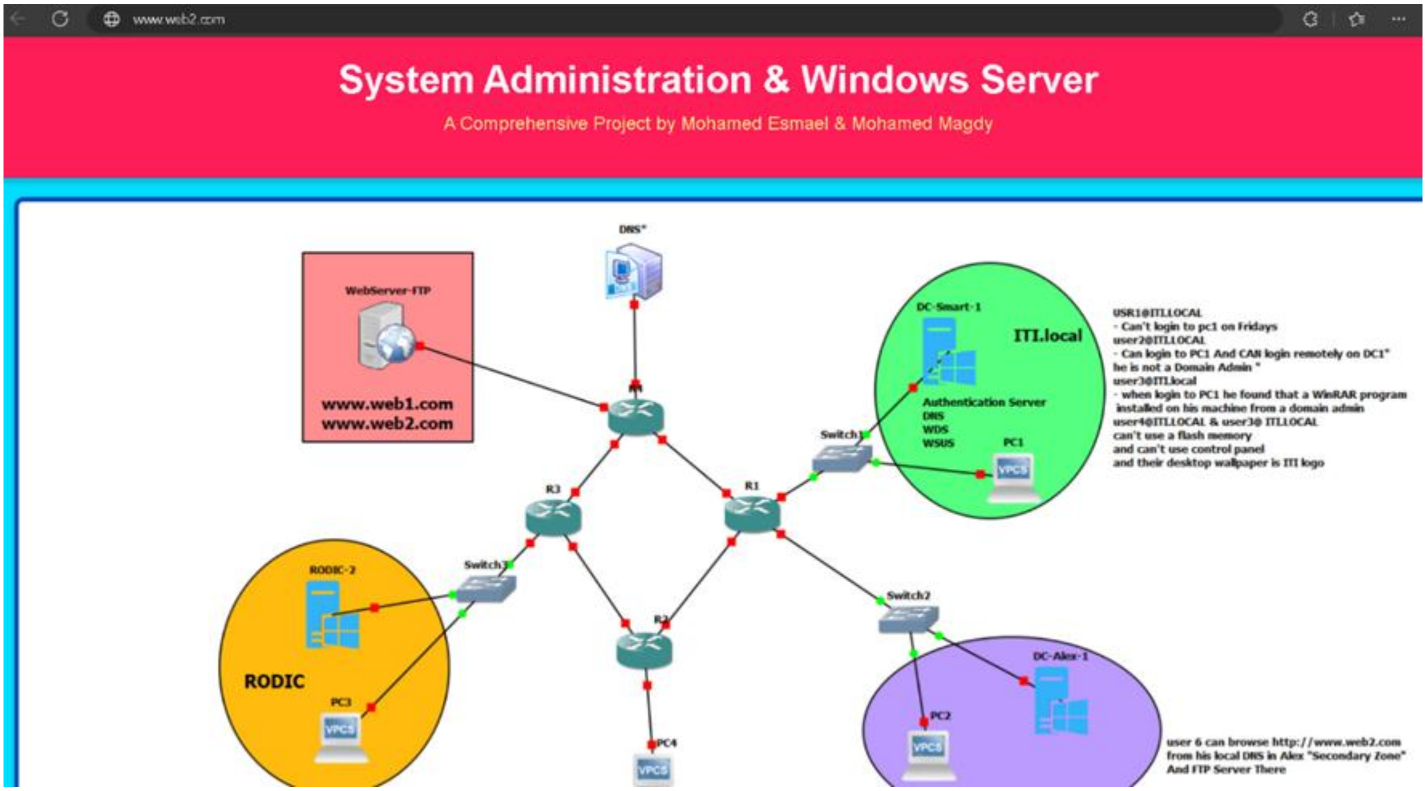
a)DNS Access and Local Resolution Policy

- **Requirement:**
  1. **Set Alex-1 as a Secondary DNS Zone for web2.com.**
  2. **Configure PC2-1 to use Alex-1 as its DNS server.**
  3. **Verify User6 can browse http://www.web2.com from PC2-1.**

- **Configure Alex-1 as a Secondary DNS Zone**:
  1. On **Alex-1 (DNS server)**:
     - Open **DNS Manager**.
     - Right-click **Forward Lookup Zones** and select **New Zone**.
     - Choose **Secondary Zone** and click **Next**.
     - Enter the zone name (web2.com) and click **Next**.
     - Specify the IP address of the **authoritative DNS server (192.168.200.100)** and click **Next**.
     - Finish the wizard and allow the zone to replicate.

- **Ensure Local DNS Resolution for User6**:
  - On **PC2-1 (User6's PC)**:
    - Set the **primary DNS server** to the IP address of **Alex-1 (192.168.200.20).**
    - This ensures that queries for web2.com will be resolved by Alex-1.

- **Verify Access to http://www.web2.com**:
  - Test browsing http://www.web2.com from User6’s PC



System Administration & Windows Server

A Comprehensive Project by Mohamed Esmael & Mohamed Magdy

USR1@ITI.LOCAL
- Can't login to pc1 on Fridays
user2@ITI.LOCAL
- Can login to PC1 And CAN login remotely on DC1"
he is not a Domain Admin "
user3@ITI.local
- when login to PC1 he found that a WinRAR program
installed on his machine from a domain admin
user4@ITI.LOCAL & user3@ ITI.LOCAL
can't use a flash memory
and can't use control panel
and their desktop wallpaper is ITI logo

user 6 can browse http://www.web2.com
from his local DNS in Alex "Secondary Zone"
And FTP Server There

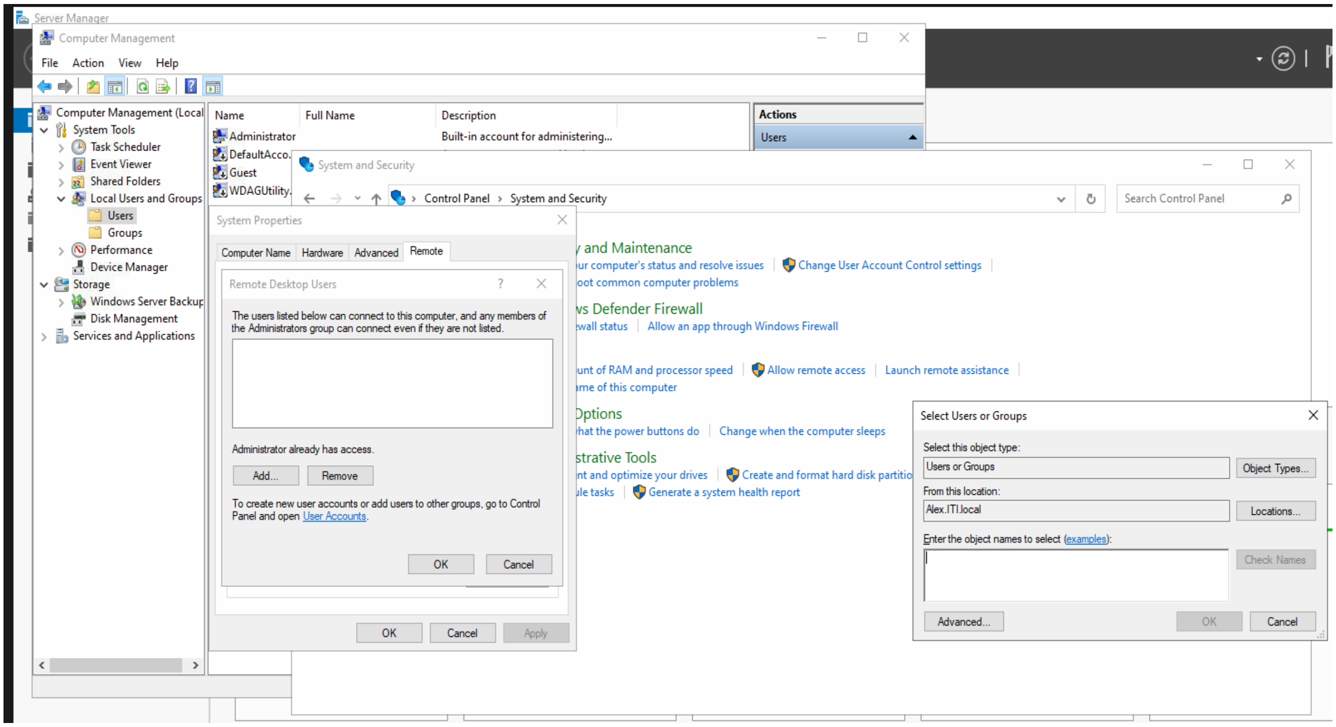
b)Administrative Access and DNS Resolution

- **Requirement:**

1. **Add User7 to the Administrators Group on the web server for remote access.**
2. **Configure PC4-1 to use 192.168.200.100 as its DNS server.**
3. **Verify User7 can browse http://www.web1.com and access the web server remotely.**

- **Configure Alex-1 as a Secondary DNS Zone:**
  - Set Authoritative DNS Server (192.168.200.100):
    1. On PC4-1 (User7's PC):
    2. Set the primary DNS server to **192.168.200.100.**
    3. This allows authoritative resolution for the web1.com zone.
  - Verify DNS Settings:
    1. Test browsing http://www.web1.com from PC4-1 to ensure it resolves using the authoritative DNS.
  - Enable Administrative Access:
    1. On the web server:
       - Add User7 to the Administrators Group or provide administrative rights.
       - Ensure User7 can log in remotely using Remote Desktop Protocol (RDP)

- **Remote Access Configuration**:


Remote Desktop Users

The users listed below can connect to this computer, and any members of the Administrators group can connect even if they are not listed.

Administrator already has access.

To create new user accounts or add users to other groups, go to Control Panel and open User Accounts.

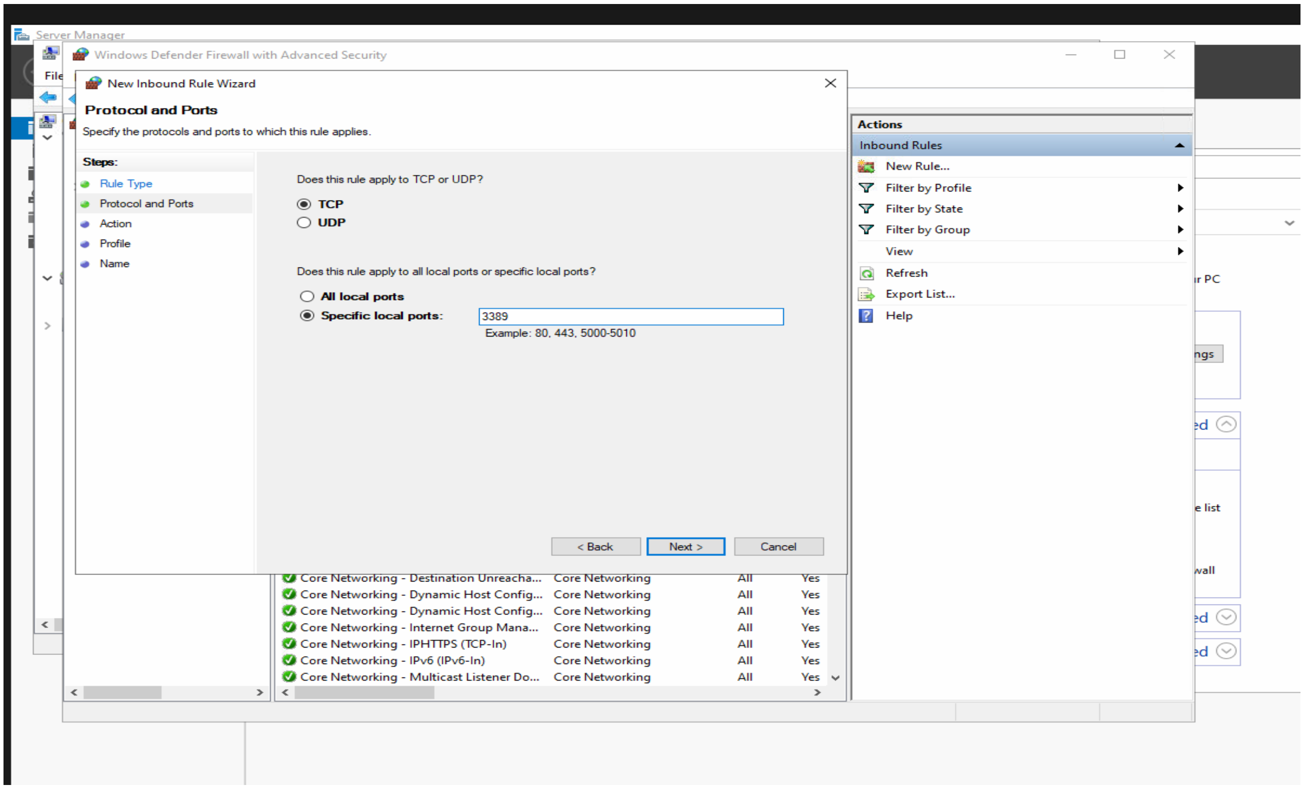
Select Users or Groups

Select this object type: Users or Groups

From this location: Alex.ITI.local

Enter the object names to select (examples):

- **Making Sure That port 3389 is open on Firewall:**



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:
- Rule Type
- Protocol and Ports
- Action
- Profile
- Name

Does this rule apply to TCP or UDP?

● TCP
○ UDP

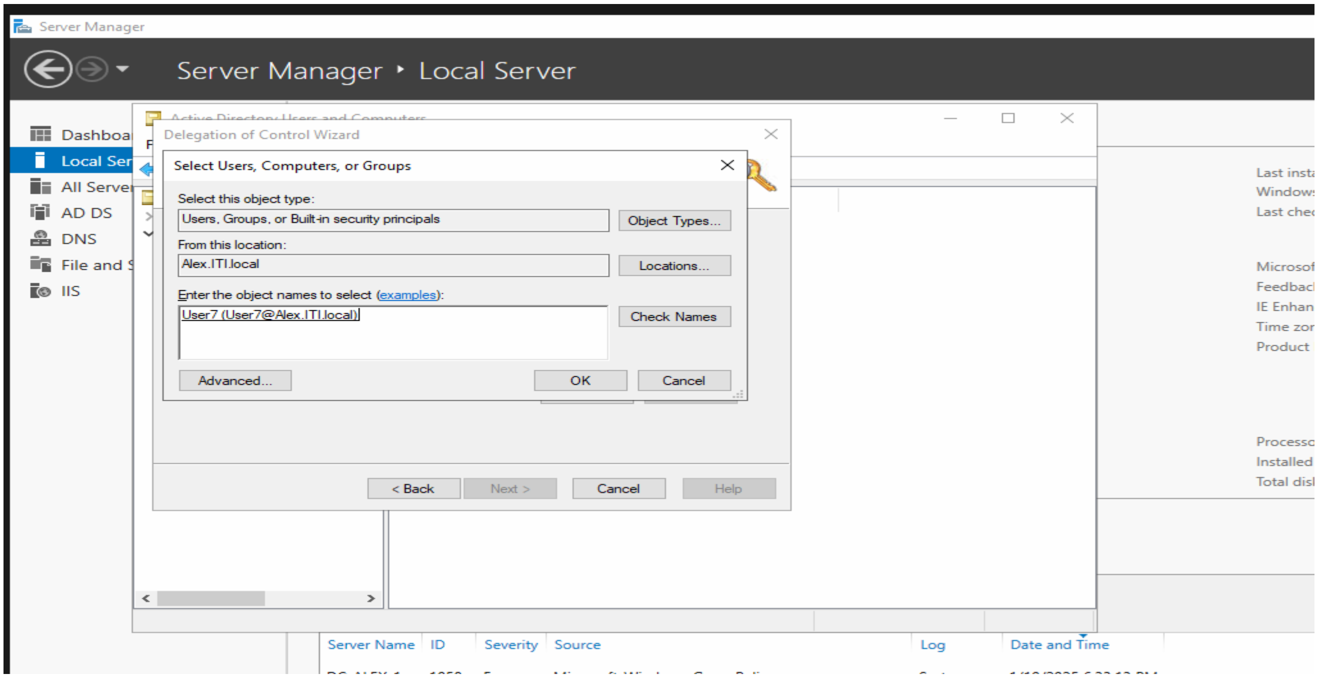
Does this rule apply to all local ports or specific local ports?

○ All local ports
● Specific local ports: 3389

Example: 80, 443, 5000-5010

Core Networking - Destination Unreacha...	Core Networking	All	Yes
Core Networking - Dynamic Host Config...	Core Networking	All	Yes
Core Networking - Dynamic Host Config...	Core Networking	All	Yes
Core Networking - Internet Group Mana...	Core Networking	All	Yes
Core Networking - IPHTTPS (TCP-In)	Core Networking	All	Yes
Core Networking - IPv6 (IPv6-In)	Core Networking	All	Yes
Core Networking - Multicast Listener Do...	Core Networking	All	Yes

- **Grant user7 a delegation control to create and delete users:**

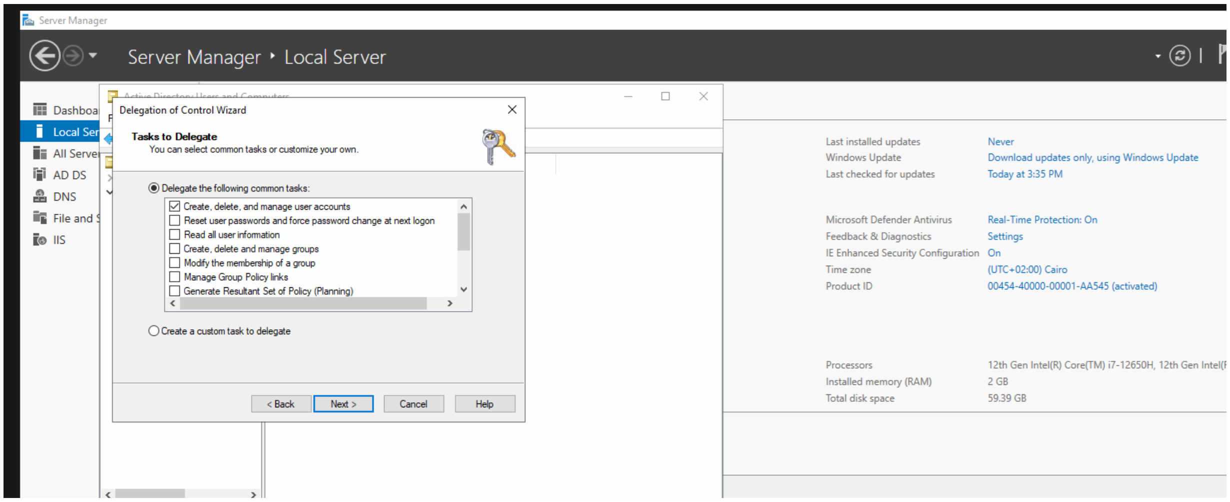


Select Users, Computers, or Groups

Select this object type: Users, Groups, or Built-in security principals

From this location: Alex.ITI.local

Enter the object names to select (examples): User7 (User7@Alex.ITI.local)


Server Manager
Server Manager ‣ Local Server
Dashboard
Local Server
All Servers
AD DS
DNS
File and Storage Services
IIS
Active Directory Users and Computers

Delegation of Control Wizard

Tasks to Delegate

You can select common tasks or customize your own.

● Delegate the following common tasks:

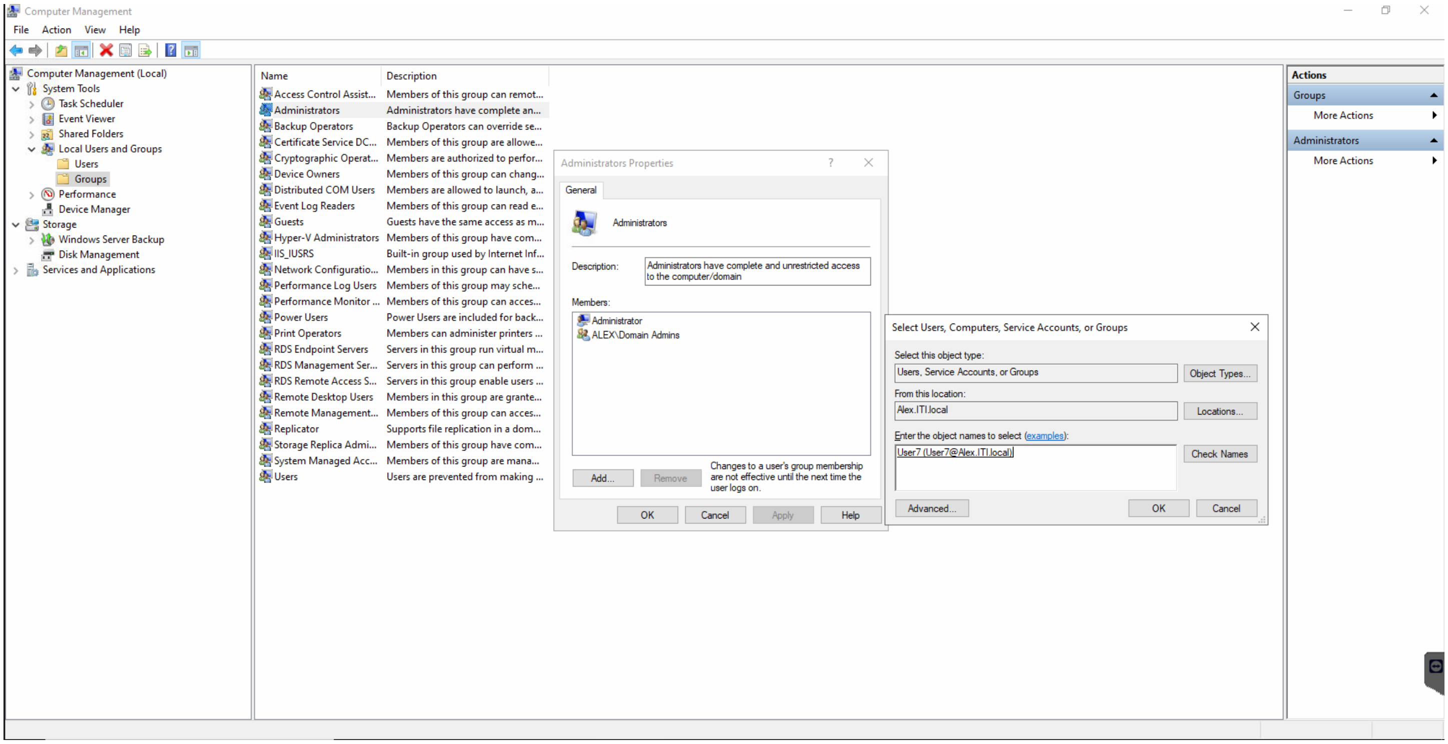
- ☑ Create, delete, and manage user accounts
- □ Reset user passwords and force password change at next logon
- □ Read all user information
- □ Create, delete and manage groups
- □ Modify the membership of a group
- □ Manage Group Policy links
- □ Generate Resultant Set of Policy (Planning)

○ Create a custom task to delegate

< Back | Next > | Cancel | Help

Last installed updates	Never
Windows Update	Download updates only, using Windows Update
Last checked for updates	Today at 3:35 PM
Microsoft Defender Antivirus	Real-Time Protection: On
Feedback & Diagnostics	Settings
IE Enhanced Security Configuration	On
Time zone	(UTC+02:00) Cairo
Product ID	00454-40000-00001-AA545 (activated)
Processors	12th Gen Intel(R) Core(TM) i7-12650H, 12th Gen Intel(R
Installed memory (RAM)	2 GB
Total disk space	59.39 GB

- **Add user7 to the Administrators group to get administrative rights:**



Name	Description
Access Control Assist...	Members of this group can remot...
Administrators	Administrators have complete an...
Backup Operators	Backup Operators can override se...
Certificate Service DC...	Members of this group are allowe...
Cryptographic Operat...	Members are authorized to perfor...
Device Owners	Members of this group can chang...
Distributed COM Users	Members are allowed to launch, a...
Event Log Readers	Members of this group can read e...
Guests	Guests have the same access as m...
Hyper-V Administrators	Members of this group have com...
IIS_IUSRS	Built-in group used by Internet Inf...
Network Configuratio...	Members in this group can have s...
Performance Log Users	Members of this group may sche...
Performance Monitor ...	Members of this group can acces...
Power Users	Power Users are included for back...
Print Operators	Members can administer printers ...
RDS Endpoint Servers	Servers in this group run virtual m...
RDS Management Ser...	Servers in this group can perform ...
RDS Remote Access S...	Servers in this group enable users ...
Remote Desktop Users	Members in this group are grante...
Remote Management...	Members of this group can acces...
Replicator	Supports file replication in a dom...
Storage Replica Admi...	Members of this group have com...
System Managed Acc...	Members of this group are mana...
Users	Users are prevented from making ...

Administrators Properties

General

Administrators

Description: Administrators have complete and unrestricted access to the computer/domain

Members:

Administrator
ALEX\Domain Admins

Add... | Remove

Changes to a user's group membership are not effective until the next time the user logs on.

OK | Cancel | Apply | Help

Select Users, Computers, Service Accounts, or Groups

Select this object type: Users, Service Accounts, or Groups [Object Types...]

From this location: Alex.ITI.local [Locations...]

Enter the object names to select (examples): User7 (User7@Alex.ITI.local) [Check Names]

Advanced... | OK | Cancel