

# **MCSA Project Documentation**

## **Team Members**

**Abdelrahim Badr**

**Emad Singab**

**Islam Yasser**

**Tasneem Adel**

**Yasmeen Mohamed**



# Overview

This project presents the implementation of a **Windows Server Active Directory infrastructure** that simulates a real enterprise environment. It applies key **MCSA concepts** including **Active Directory Domain Services (AD DS)**, **DNS**, **DHCP**, **Group Policy**, and **Domain Controller roles**.

The environment is based on a **root domain (ITI.local)** with multiple Domain Controllers to ensure **security, redundancy, and centralized management**. Client computers and user accounts are organized into departments, with **Group Policy Objects (GPOs)** used to enforce security settings and administrative control. The project demonstrates effective **domain design, service integration, and user management** within a Microsoft-based network.

DC1 is a primary Domain Controller  
DC2 is an additional Domain Controller  
DC3 is a RODC, DC4&DC5 are Chilled DC

A@ITI.local can only login to PC1 but can't login to pc1 on Fridays  
help@ITI.local can login to Rodc & his PSWD is replicated to Rodc  
c@ITI.local can't access Flash memory& control Panel & his wallpaper is ITI logo  
A@Ism.ITI.Local can login to PC5-PC1-PC4 (ROMING PROFILE)\*\*

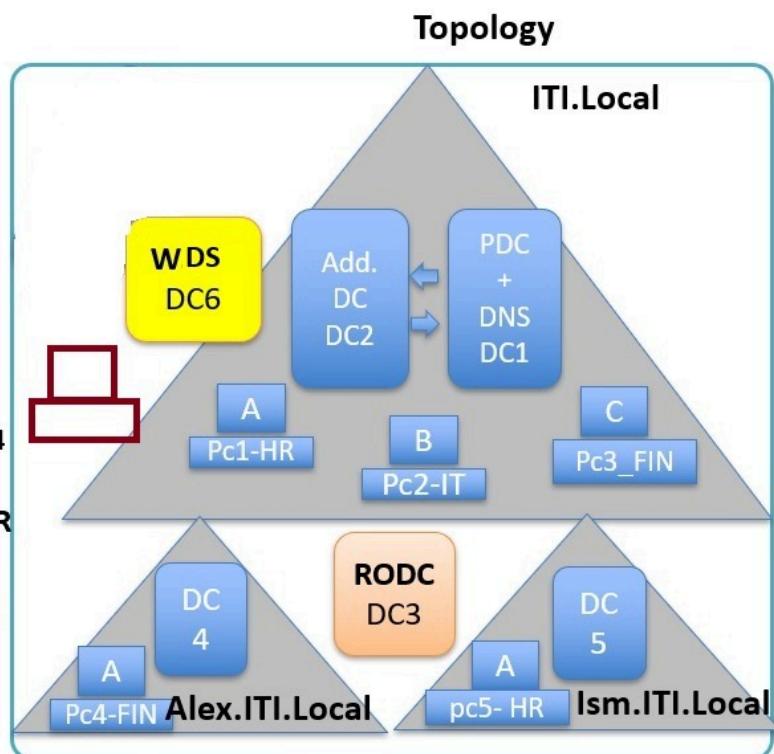
**DOMAIN ADMIN** need to install **WINRAR** on pc2 using GPO (how)\*\*

**DOMAIN ADMIN** delegate to B@iti.local to login remotely to DC1 (not member of administrators) \*\*

A@ITI.local check the website

<https://www.web2.com> from pc1

*you need to add 50 new computers with windows and 50 user to the domain (how to automate that?)  
WDS*



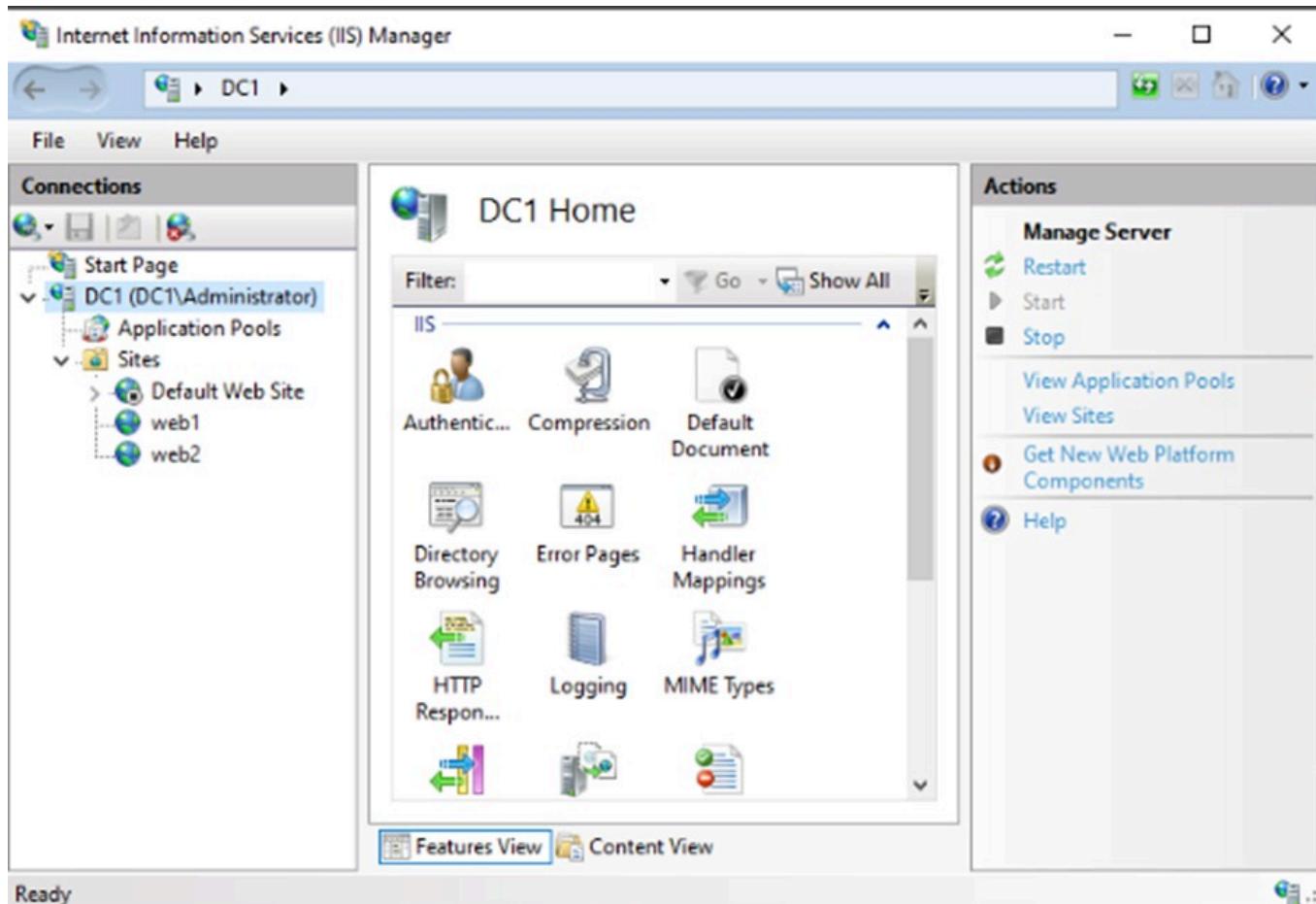
**D** is a local user on **pc6** but he can manage remotely (**RDP**) the webserver with administrative privileges ,his responsibilities is to check <http://www.web1.com> and get a **copy** of it using **FTP**

## 1. Web Server - DNS - DHCP

### 1.1. IIS Web Server Configuration (DC1)

The **IIS Manager** on **DC1** is the primary host for the project's internal websites.

- **Hosted Sites:** The console confirms that **web1** and **web2** are active and managed on this server.



## 1.2. Bindings

Specific bindings are set up so that users like [A@ITI.local](mailto:A@ITI.local) can access the sites from **pc1**.

- **web1 Binding:** The site [www.web1.com](http://www.web1.com) is configured on **Port 80** via **http**.
- **web2 Binding:** The site [www.web2.com](http://www.web2.com) is also configured on **Port 80** via **http**.

Type	Host Name	Port	IP Address	Binding Informa...	
http	www.web1.com	80	*		<button>Add...</button> <button>Edit...</button> <button>Remove</button> <button>Browse</button>

Type	Host Name	Port	IP Address	Binding Informa...	
http	www.web2.com	80	*		<button>Add...</button> <button>Edit...</button> <button>Remove</button> <button>Browse</button>

## 1.3. DNS

The **DNS Manager** on **DC1** handles name resolution and zone forwarding for the forest.

- **Forward Lookup Zones:** Authoritative zones are active for **web1.com** and **web2.com**.
- **web1.com Records:**
  - **www:** A **Host (A)** record points to the server IP **10.10.10.1**.
  - **ftp:** A **Host (A)** record points to **10.10.10.1**, enabling the requirement to retrieve site copies via FTP.
- **Conditional Forwarding:** A forwarder for **web2.com** is configured to point to **10.250.159.151**. This satisfies the requirement for **DC1** to act as the authoritative "Second

Z" for that domain.

The screenshot shows two separate instances of the Windows DNS Manager interface. Both instances display the same DNS zone configuration for a domain named 'DC1'. The left pane shows a tree view with 'DNS' at the root, followed by 'DC1', then 'Forward Lookup Zones' which contains 'web1.com' and 'web2.com'. Below these are 'Reverse Lookup Zones', 'Trust Points', and 'Conditional Forwarders'. The right pane is a table with three columns: 'Name', 'Type', and 'Data'. It lists four entries: '(same as parent folder)' with Type 'Start of Authority (SOA)' and Data '[1], dc1., hostmaster.', '(same as parent folder)' with Type 'Name Server (NS)' and Data 'dc1.', 'www' with Type 'Host (A)' and Data '10.10.10.1', and 'ftp' with Type 'Host (A)' and Data '10.10.10.1'. The second instance of the DNS Manager is identical to the first, showing the same tree structure and table data.

Name	Type	Data
(same as parent folder)	Start of Authority (SOA)	[1], dc1., hostmaster.
(same as parent folder)	Name Server (NS)	dc1.
www	Host (A)	10.10.10.1
ftp	Host (A)	10.10.10.1

## 1.4. DHCP

The **DHCP** console on **DC1** provides dynamic IP management for the entire topology.

- **Scope:** A scope named **scopel** is defined for the **10.0.0.0** network.
- **Address Pool:** IPs are distributed from **10.10.10.50** to **10.10.10.254**.
- **Active Lease:** The "Address Leases" table confirms **PC1** has successfully leased IP **10.10.10.50**.
- **Verification:** The lease is valid until **2/6/2026**, confirming the network is live and updating correctly.

The screenshot shows the Windows Server DHCP Management console. On the left, the navigation pane displays a tree structure under 'dc1' with 'IPv4' selected. Under 'IPv4', 'Scope [10.0.0.0] scope1' is expanded, showing 'Address Pool', 'Address Leases', 'Reservations', 'Scope Options', 'Policies', 'Server Options', 'Filters', 'Allow', and 'Deny'. To the right, a table provides details for this scope:

Start IP Address	End IP Address	Description
10.10.10.50	10.10.10.254	Address range for distribution

This screenshot shows the same DHCP management interface. The 'Address Leases' item under 'Scope [10.0.0.0] scope1' is now selected. A table lists a single lease entry:

Client IP Address	Name	Lease Expiration	Type	Unique ID
10.10.10.50	PC1	2/6/2026 10:30:01 AM	DHCP	000c29a2a...

```
C:\Users\Administrator>ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

  Connection-specific DNS Suffix  . :
  IPv4 Address. . . . . : 10.10.10.1
  Subnet Mask . . . . . : 255.0.0.0
  Default Gateway . . . . . :

Ethernet adapter Ethernet1:

  Connection-specific DNS Suffix  . :
  Link-local IPv6 Address . . . . . : fe80::a05b:cce2:21fa:ca1f%25
  IPv4 Address. . . . . : 10.250.159.151
  Subnet Mask . . . . . : 255.255.255.0
  Default Gateway . . . . . : 10.250.159.21

C:\Users\Administrator>
```

## 1.5. Websites

This section confirms the successful deployment of the web infrastructure on **DC1** as verified by the active browser results.

## Web 1

Accessing <http://www.web1.com> confirms the primary project site is live and reachable from the domain workstations.

The screenshot shows a web browser window with the title "ITILocal Project Documentation". The address bar displays "http://www.web1.com". The page content is titled "ITI.Local Infrastructure" and "Enterprise Active Directory & Network Automation Project". A "PROJECT TEAM" section lists five members: Emad Elsayed Singab (highlighted in blue), Islam Yasser Mahmoud, Tasneem Adel Khamis, Yasmeen Mohamed Talaat, and Abdelrahim Badr. Below this, three main sections are shown: "Network Topology", "Security & Policy", and "Automation & Services".

- Network Topology:**
  - **Multi-Domain Forest:** Root (ITILocal) & Child Domains (Alex, Ismailia).
  - **High Availability:** Primary (DC1) and Additional (DC2) Domain Controllers.
  - **Branch Security:** Read-Only DC (RODC) implementation.
  - **Branch Mgmt:** Dedicated Child DCs (DC4, DC5).
- Security & Policy:**
  - **Access Control:** Logon hours & workstation restrictions enforced via GPO.
  - **Hardening:** Disabled USB Storage & Control Panel for standard users.
  - **Delegation:** Granular RDP permissions for Helpdesk support.
  - **Roaming Profiles:** Centralized user data management.
- Automation & Services:**
  - **PowerShell Scripting:** Automated bulk user & computer creation.
  - **WDS Server:** Automated Windows OS deployment over network.
  - **Software Deploy:** MSI/Exe installation via Group Policy.
  - **Web Services:** IIS hosting for Intranet sites.

## web2

Accessing <http://www.web2.com> confirms that the secondary authoritative zone and its content are correctly deployed.

**System Specifications**  
Detailed breakdown of the ITI.Local forest implementation.

**Topology & Architecture**

- Multi-Domain Forest: Root domain 'ITI.Local' with child domains 'Alex' & 'Ism'.
- DC1 (PDC/DNS): Primary controller handling central authentication.
- DC2 (ADC): Additional Domain Controller for redundancy.
- DC3 (RODC): Read-Only DC for secure branch deployment.
- Child DCs: Dedicated controllers for regional branches.

**Security & GPO Policies**

- Access Control: User 'A' restricted to PC1 and blocked on Fridays.
- Hardening: Flash memory and Control Panel disabled for specific users via GPO.
- Least Privilege: 'B@iti.local' granted remote access without Admin rights.
- Password Policy: Configured PRP on RODC for helpdesk users.
- Roaming Profiles: Implemented for mobile users.

Deployment: Windows Server IIS  
Version: 2.0.2 (Stable)

## 1.6. FTP

This section verifies that the **FTP service** is functional and configured according to the project requirements.

The **DNS Manager** on **DC1** confirms a **Host (A) record** for `ftp` pointing to the server IP **10.10.10.1**.

FTP root at ftp.web1.com

To view this FTP site in File Explorer: press Alt, click View, and then click Open FTP Site in File Explorer.

01/29/2026 11:51AM      21 [index.html](#)

## 2. Parent Active Domain Directory

The root of the infrastructure is the **iti.local** domain, which serves as the forest parent for all subordinate branches.

- **iti.local**: This represents the top-level namespace for the entire Active Directory environment.

## 2.1. Active Domain Hierarchy

The organizational structure is defined by a parent-child relationship between the root and regional branch domains.

- **Domain Relationships:** The hierarchy displays **ALEX.iti.local** and **ISMAILIA.iti.local** as child domains under the **iti.local** root.



## 2.2. Primary Domain

This section lists the specific servers responsible for authentication within the root domain.

- **PDC:** This is the parent server and primary controller for the domain.

- **DC1:** This server is configured as the additional domain controller to provide redundancy.
- **Global Catalog (GC):** Both the **PDC** and **DC1** are designated as **GC** servers, allowing them to provide resource information across the entire forest.

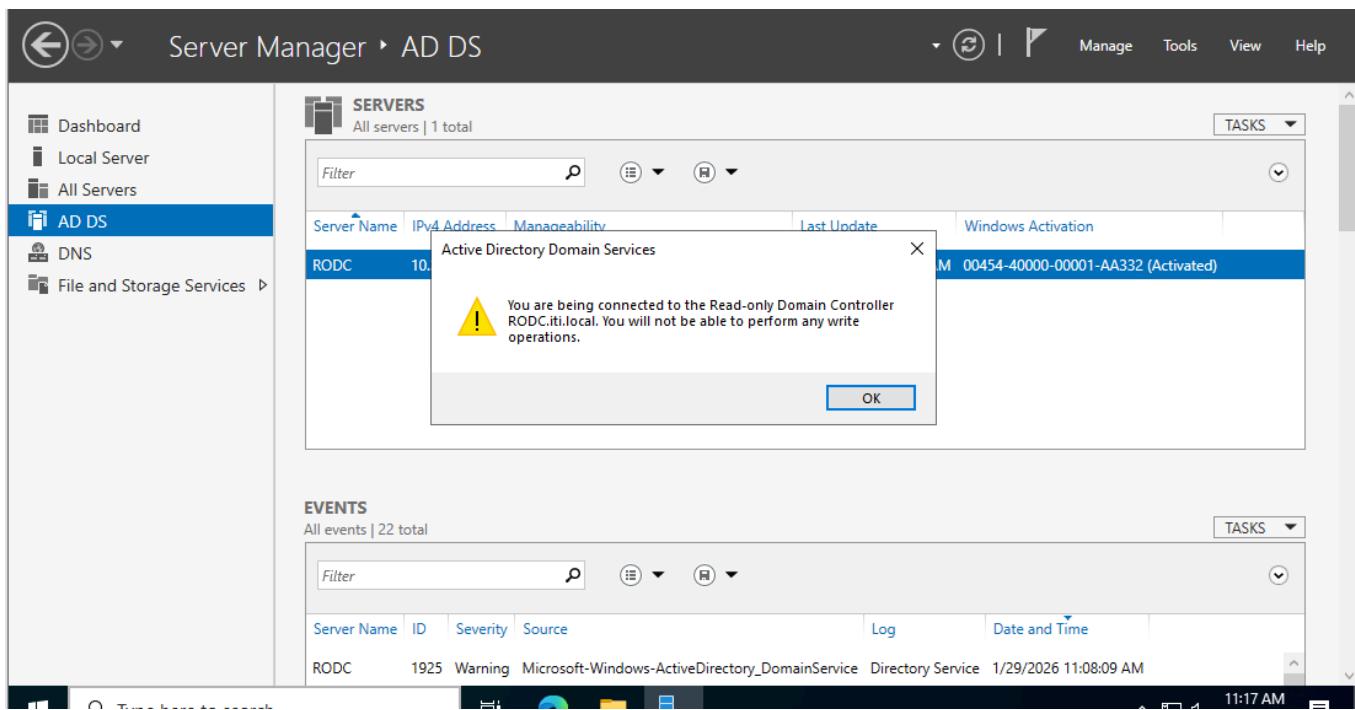
The screenshot shows the Windows Active Directory Users and Computers snap-in. On the left, the navigation pane shows the tree structure under 'Active Directory Users and Computers'. A folder named 'Domain Controllers' is selected, indicated by a blue selection bar. The main pane displays a table of domain controllers:

Name	Type	DC Type	Site	Description
DC1	Computer	GC	Default-First-Si...	
PDC	Computer	GC	Default-First-Si...	
RODC	Computer	Read-only, GC	Default-First-Si...	

## 2.3. RODC

The implementation of a Read-Only Domain Controller provides secure identity services to remote branches.

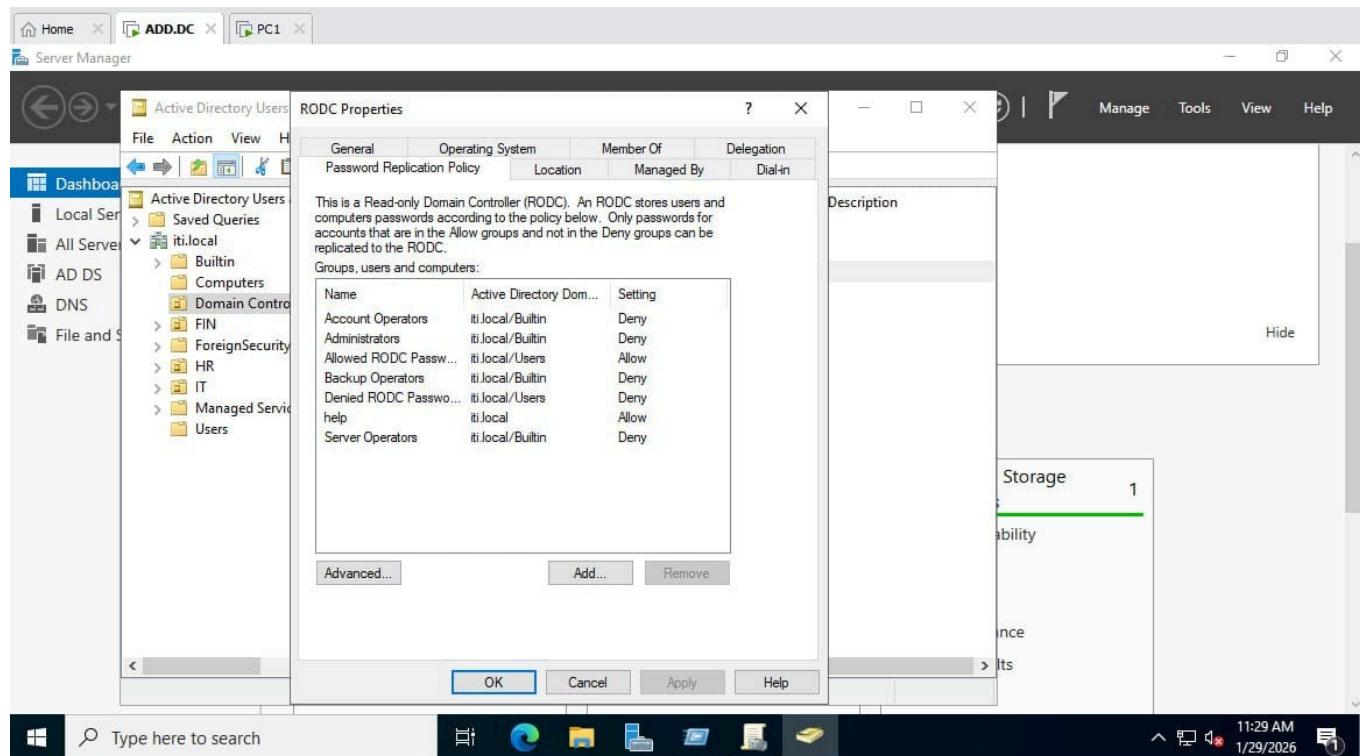
- **RODC Identity:** The server named **RODC** is the dedicated read-only controller for **iti.local**.
- **Write Restrictions:** The system identifies this machine as read-only and explicitly prevents any write operations to the Active Directory database.



## 2.3.1. Help user

The **help** user is a dedicated account within the domain hierarchy used to test branch accessibility and replication.

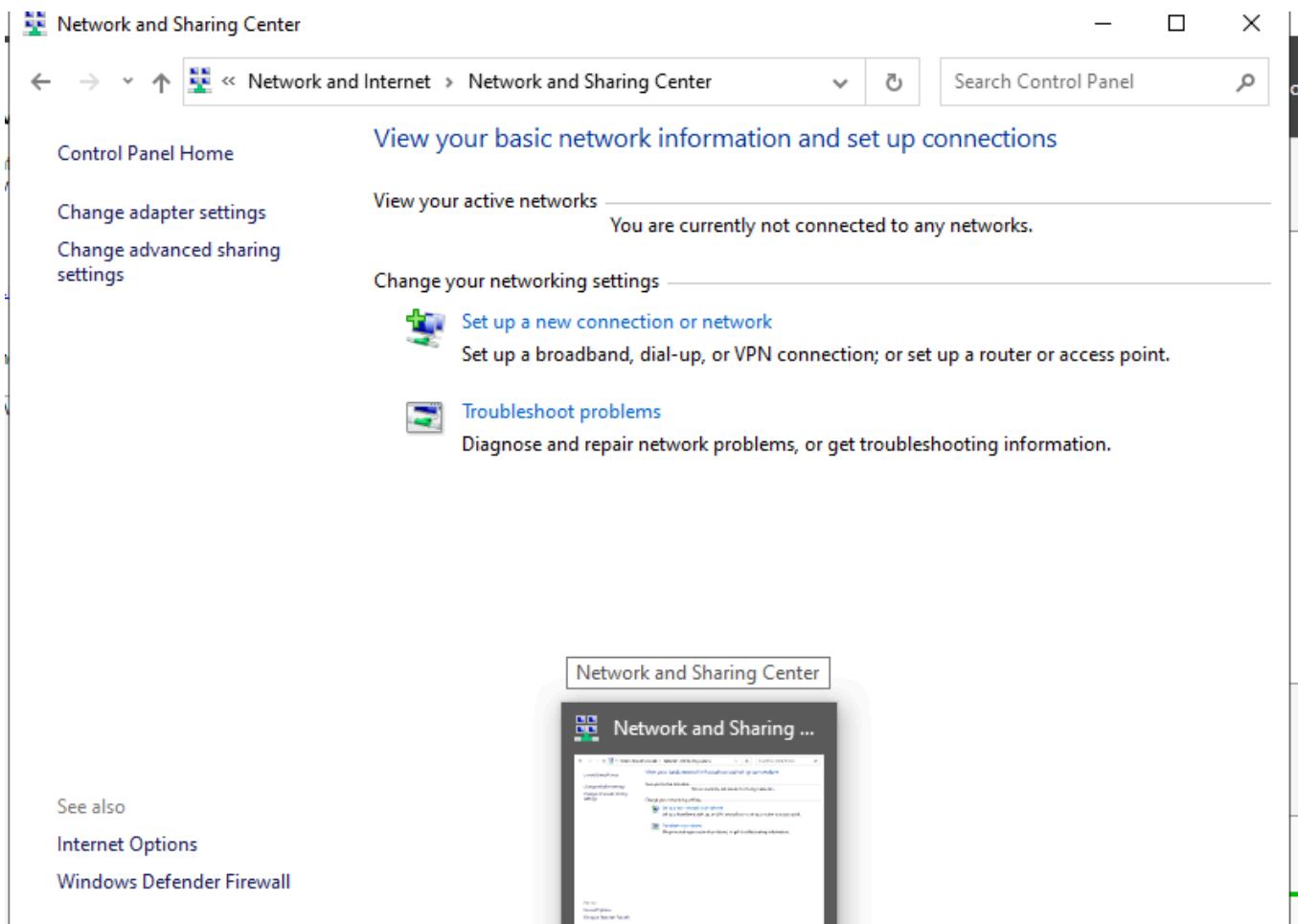
- **Account Status:** The user is identified as [help@ITI.local](mailto:help@ITI.local).
- **Server Access:** This user is granted the necessary permissions to log in and authenticate on the **RODC** server.

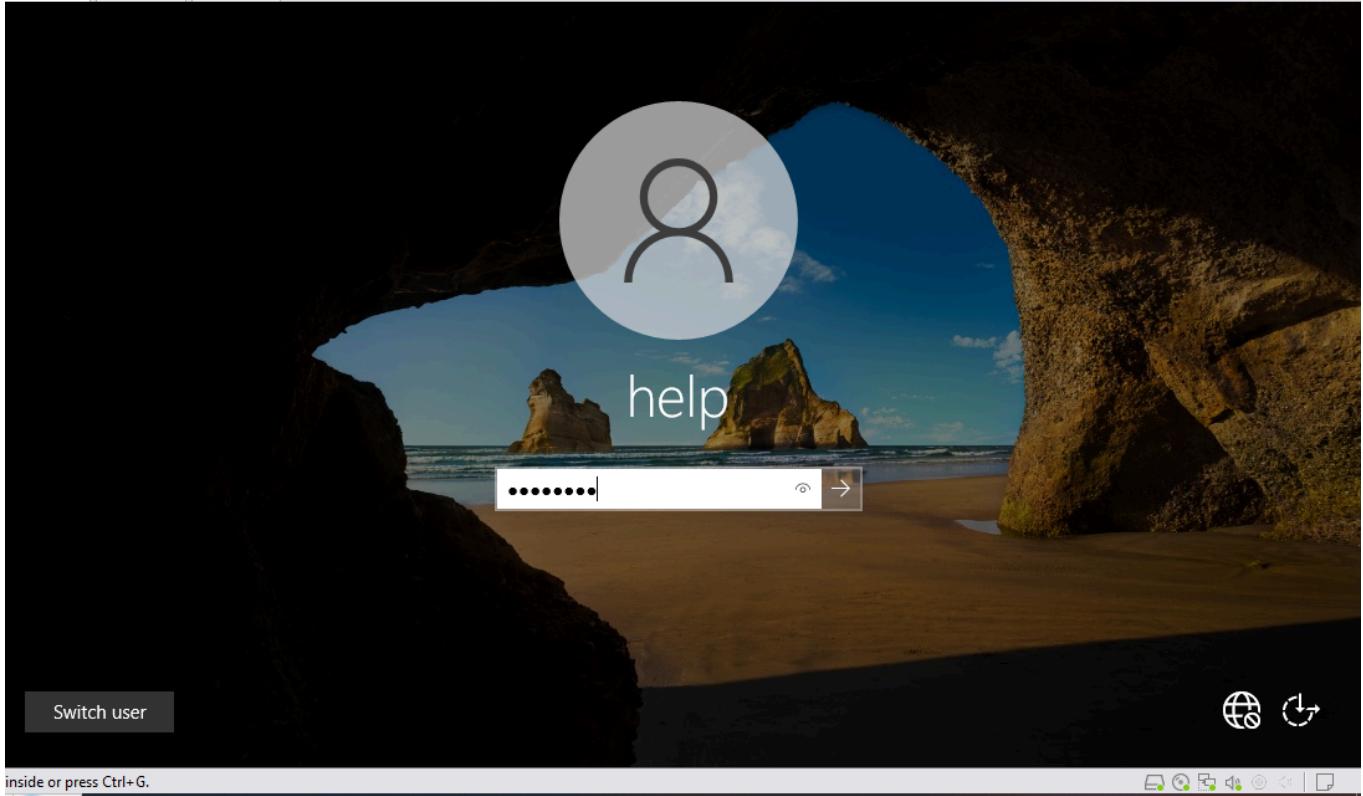


## 2.3.2. Password Replication

This policy manages credential caching to ensure branch users can log in even if the connection to the parent domain is lost.

- **Help Account:** Credentials for the **help** user are set to "**Allow**", permitting their password to be replicated locally to the **RODC**.
- **Standard Allowed Group:** The **Allowed RODC Password Replication Group** is also granted permission to replicate.
- **Restricted Groups:** High-privilege accounts, such as **Administrators**, **Backup Operators**, and **Server Operators**, are strictly set to "**Deny**" to prevent their passwords from being stored on branch hardware.



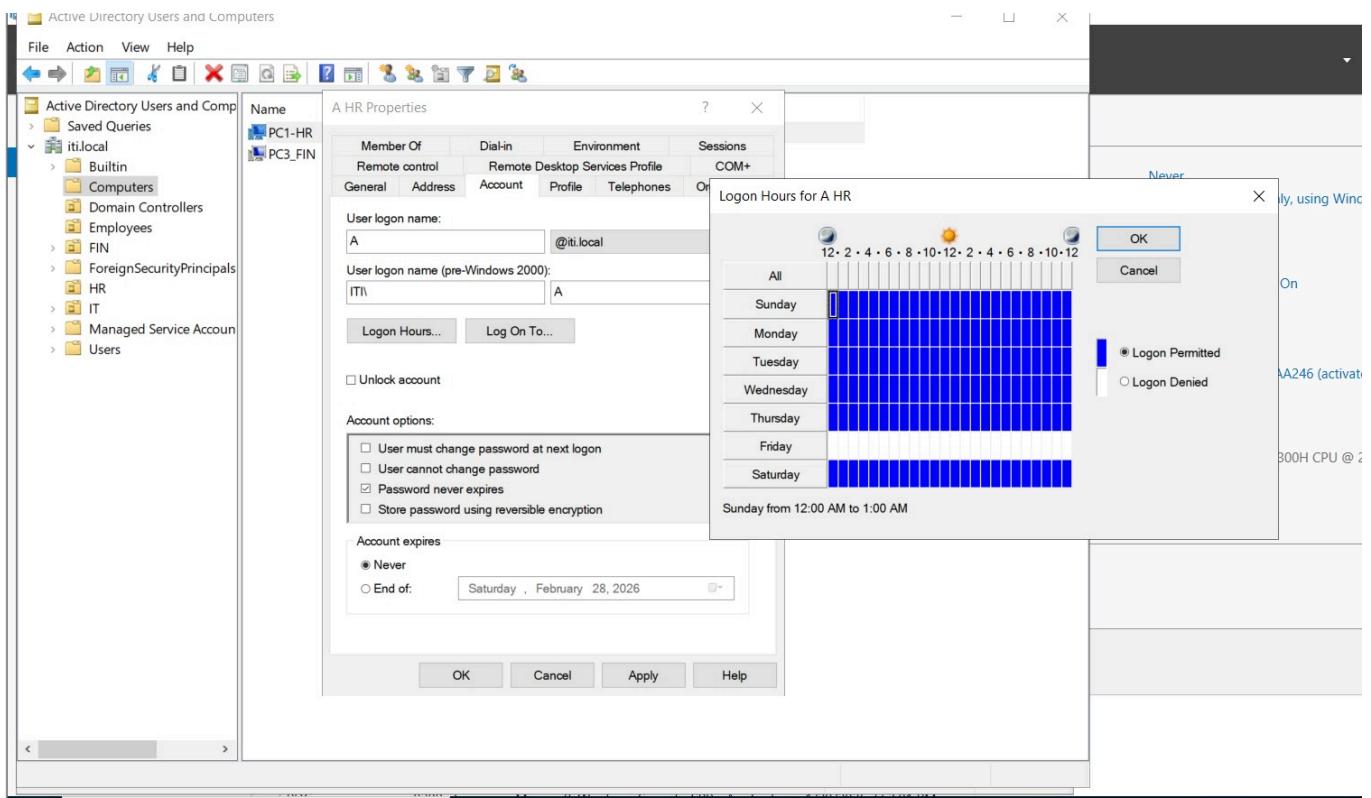


## 3. Policies

### 3.1. Blocking The User From Accessing PC on Friday

This policy implements time-based access control for the user [A@ITI.local](#) within the domain.

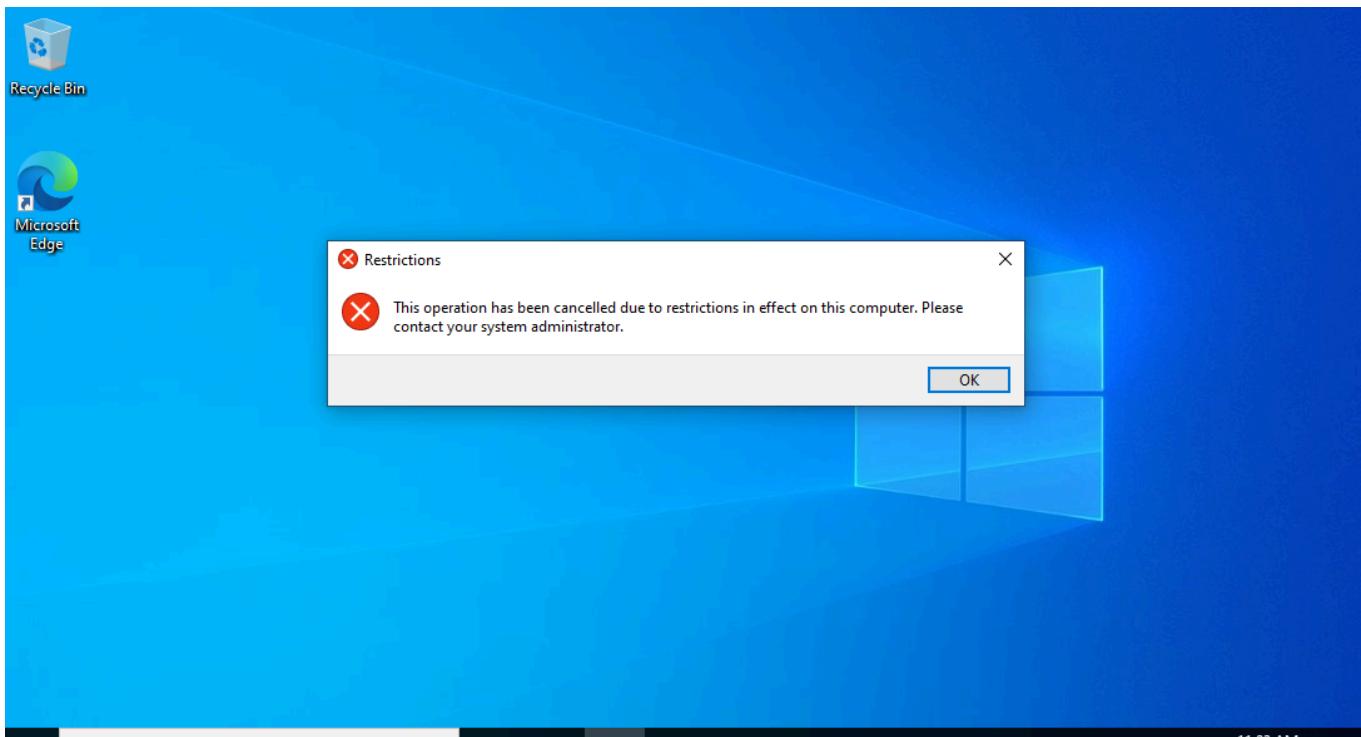
- **Logon Hours:** The configuration grid in Active Directory shows that logon is permitted from Sunday through Thursday.
- **Restriction:** The schedule for **Friday** is explicitly marked as "Logon Denied" for all 24 hours.
- **Result:** This ensures that User A is unable to authenticate or access the system on Fridays as per the project requirements.



## 3.2 Prevent Opening Control Panel

This Group Policy Object (GPO) is applied to secure the operating system environment for User C.

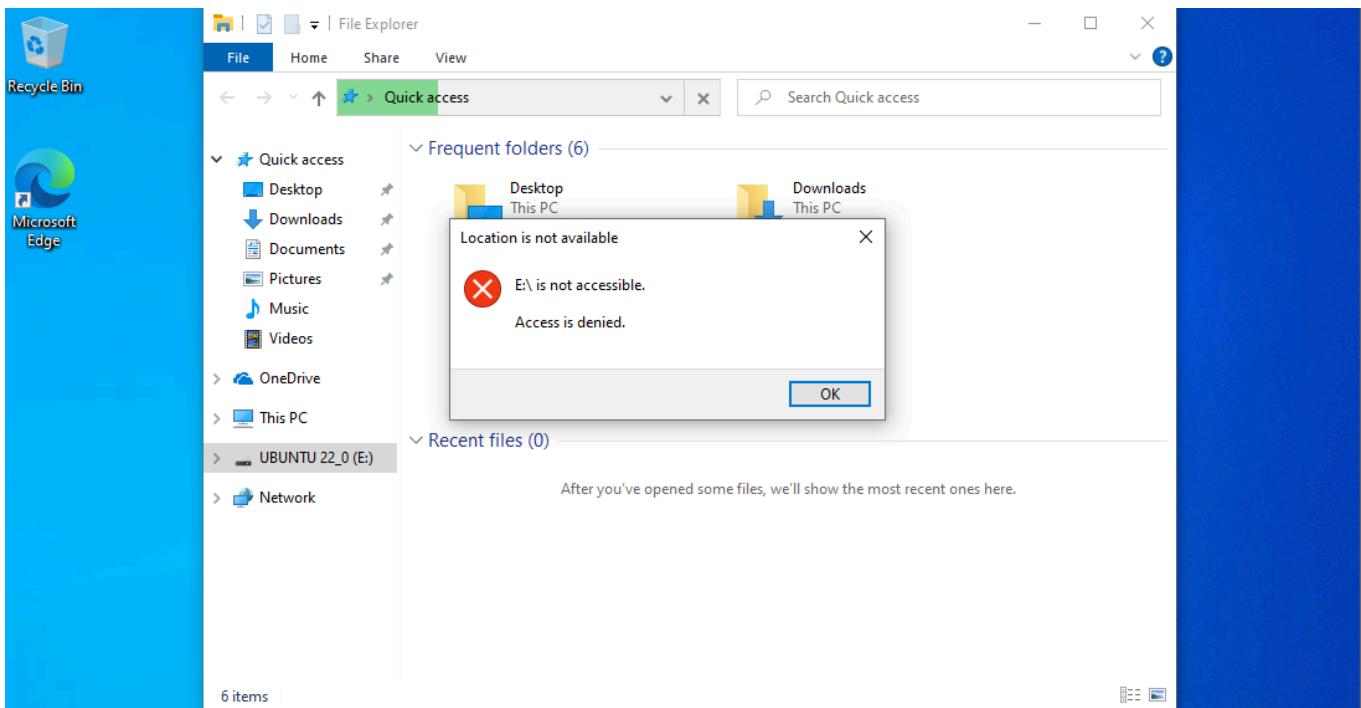
- GPO Enforcement:** The policy **"Prohibit access to Control Panel and PC settings"** is enabled and linked to the **FIN OU**.
- System Result:** When User C attempts to open the Control Panel, the system displays a **"Restrictions"** error message stating: "This operation has been cancelled due to restrictions in effect on this computer. Please contact your system administrator."



### 3.3 Can't Access Flash

Hardware security measures are enforced to prevent data exfiltration via removable storage.

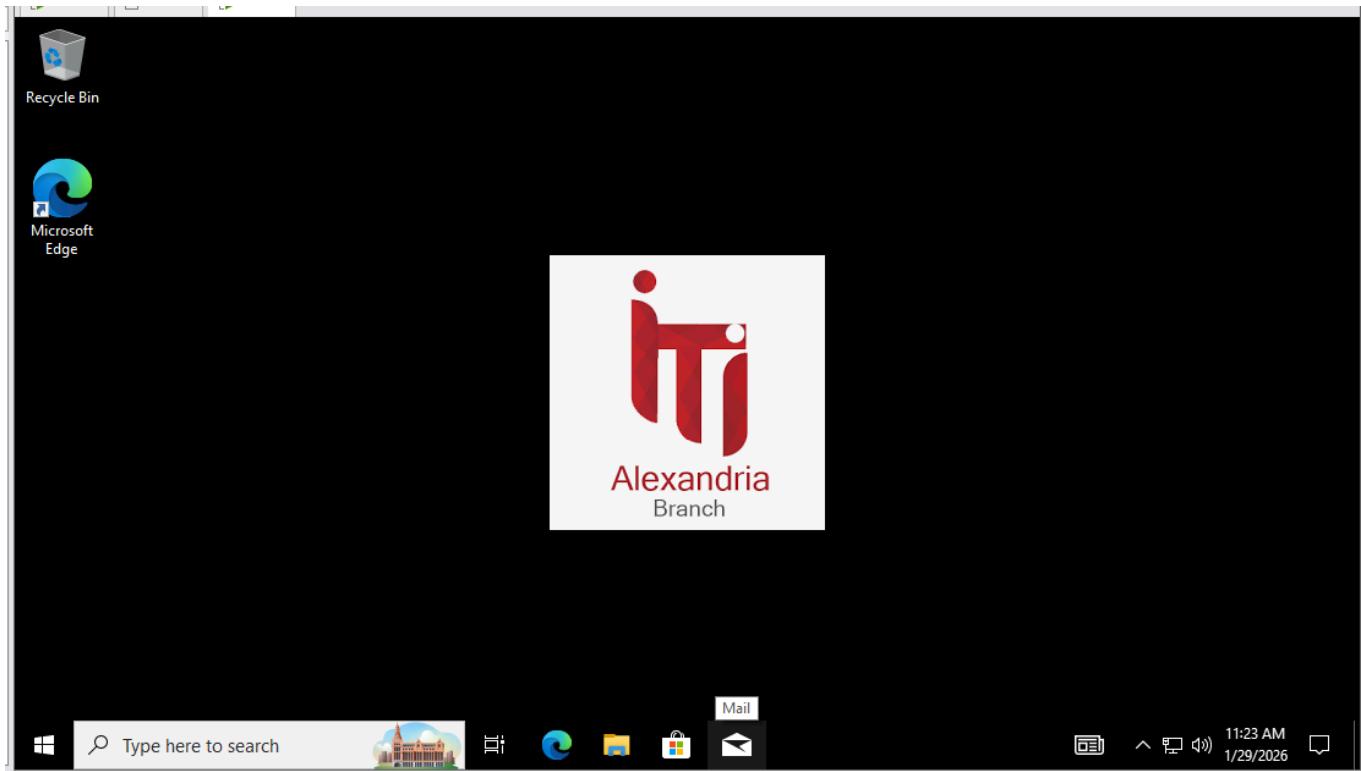
- **Removable Storage Block:** A GPO named "**can't access Flash memory**" is configured to deny read/write access to removable disks.
- **Verification Result:** When attempting to access an attached USB drive (E:), the system returns an "**Access is denied**" prompt, confirming the policy is active.



### 3.4 Wallpaper is ITI Logo

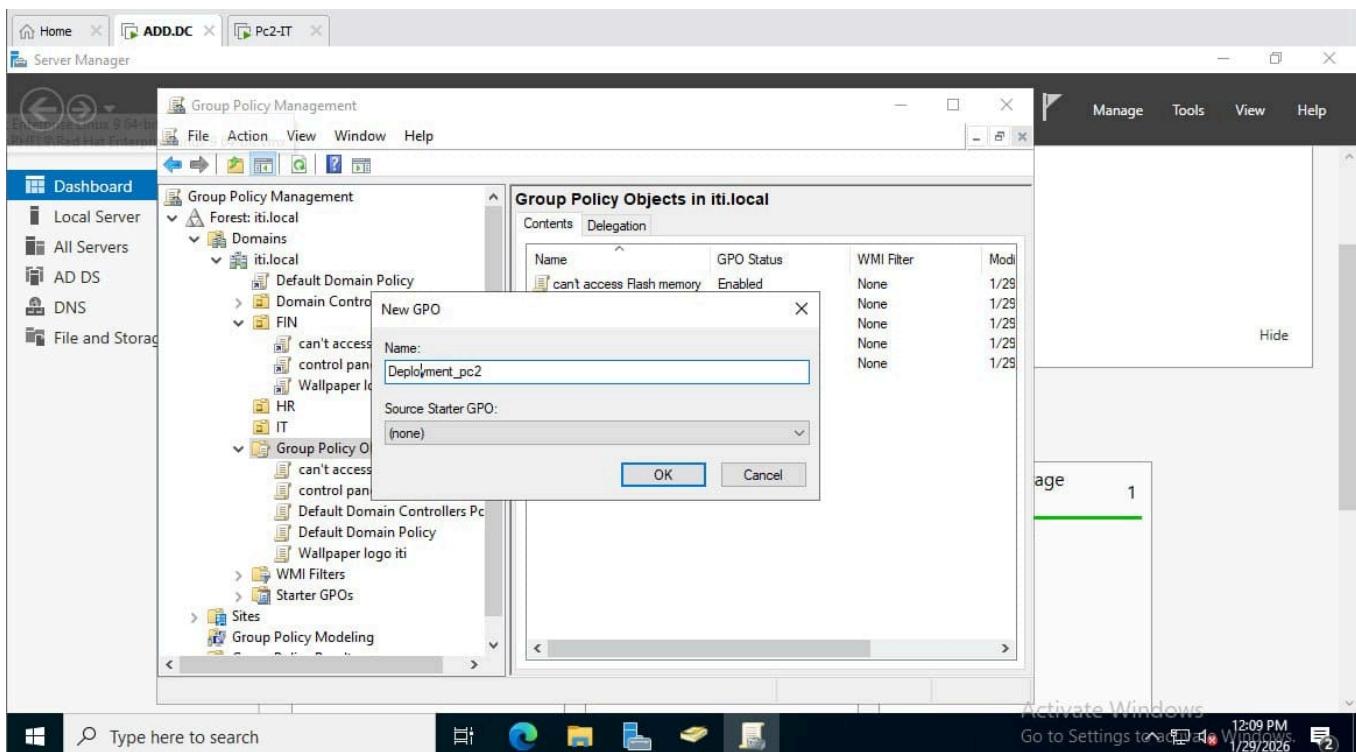
Mandatory branding is applied via GPO to maintain a uniform corporate identity across branch workstations.

- **Desktop Wallpaper Policy:** The "Desktop Wallpaper" setting is enabled within the GPO, pointing to the local path of the **ITI Alexandria Branch logo**.
- **Visual Result:** The specified ITI logo is locked as the desktop background for User C and cannot be changed by the end user.

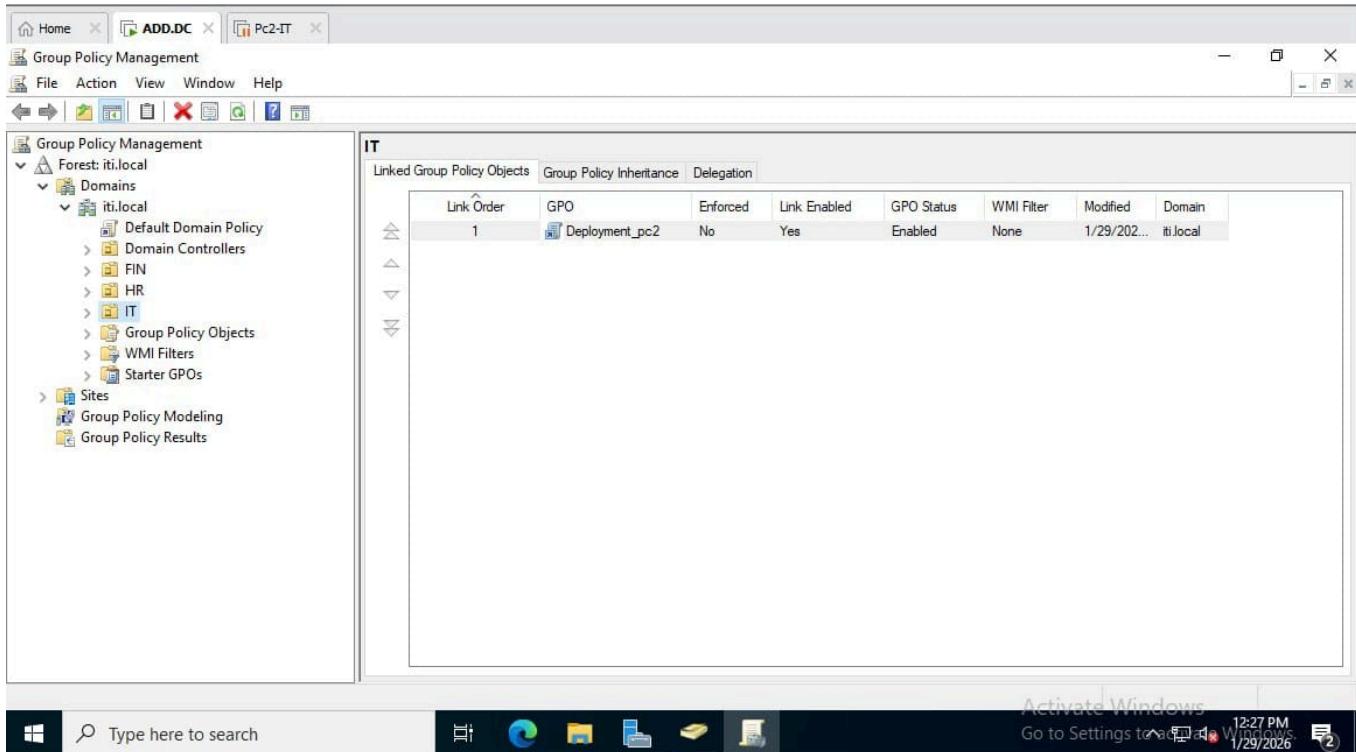


## 3.5 Installing WinRAR

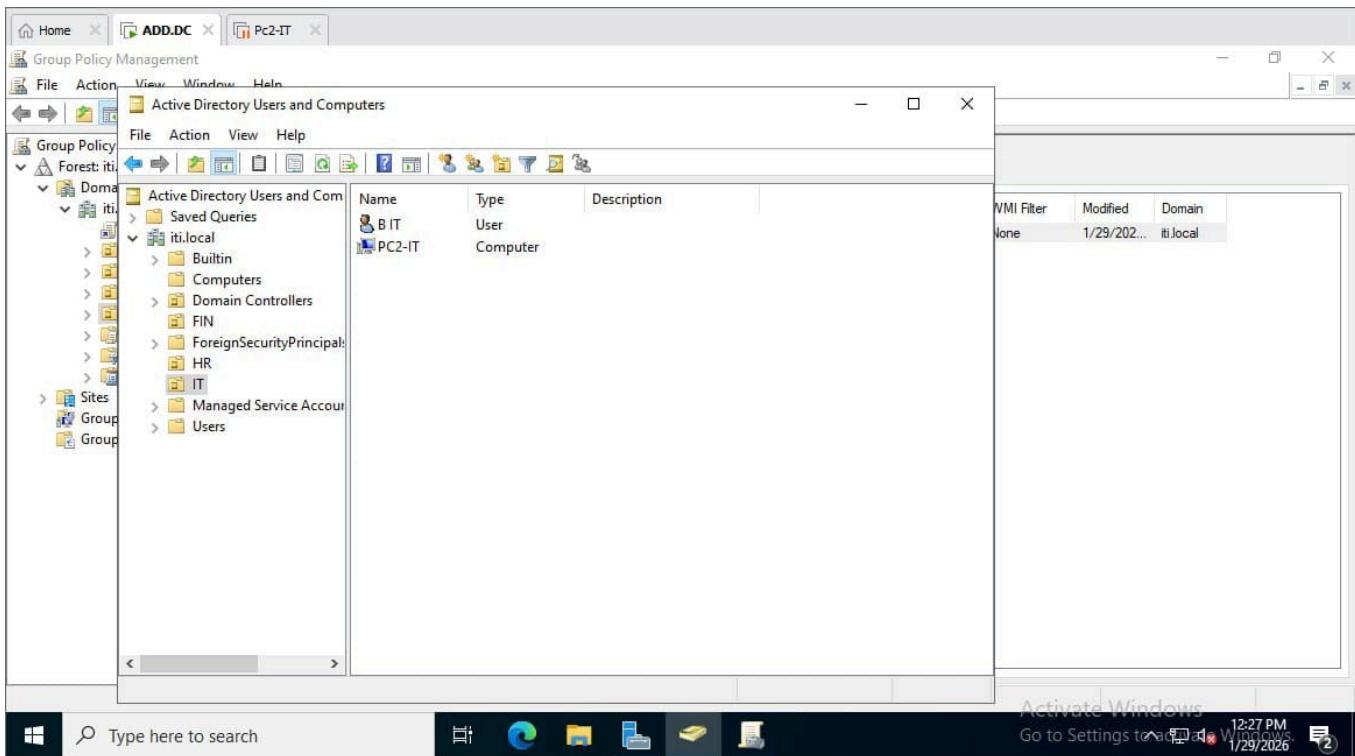
The **Group Policy Management Editor** shows the configuration of the software package. Under **Computer Configuration > Policies > Software Settings**, the WinRAR installation is established. This ensures that the deployment is handled at the machine level, targeting the computer's operating system environment.



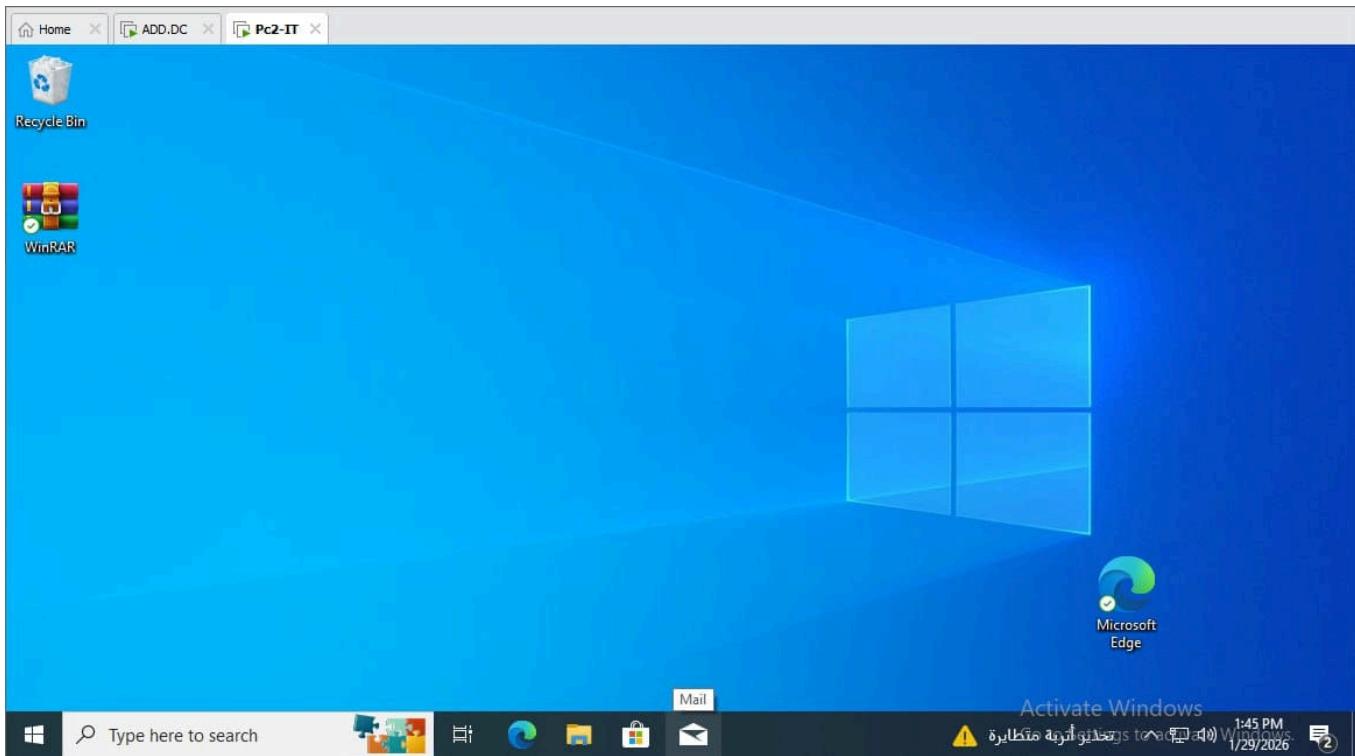
The deployment properties window confirms that the WinRAR package is set to **Assigned**. This specific configuration triggers the automatic installation of the software, ensuring that the package is deployed to the system without requiring any interaction from the user during the setup process.



The **Group Policy Management** console displays the "**Deploy\_pc2**" GPO as it is linked to the target Organizational Unit (OU) IT. This confirms the logical scope of the policy, ensuring that the software deployment is directed specifically to the computers within that defined container.



The result is verified on **PC1**, showing the **Start Menu** and **File Explorer** after the policy has been processed. **WinRAR** is present in the application list and fully integrated into the Windows shell, confirming that **PC1** successfully received the policy and completed the installation.



## 4. Child Domain

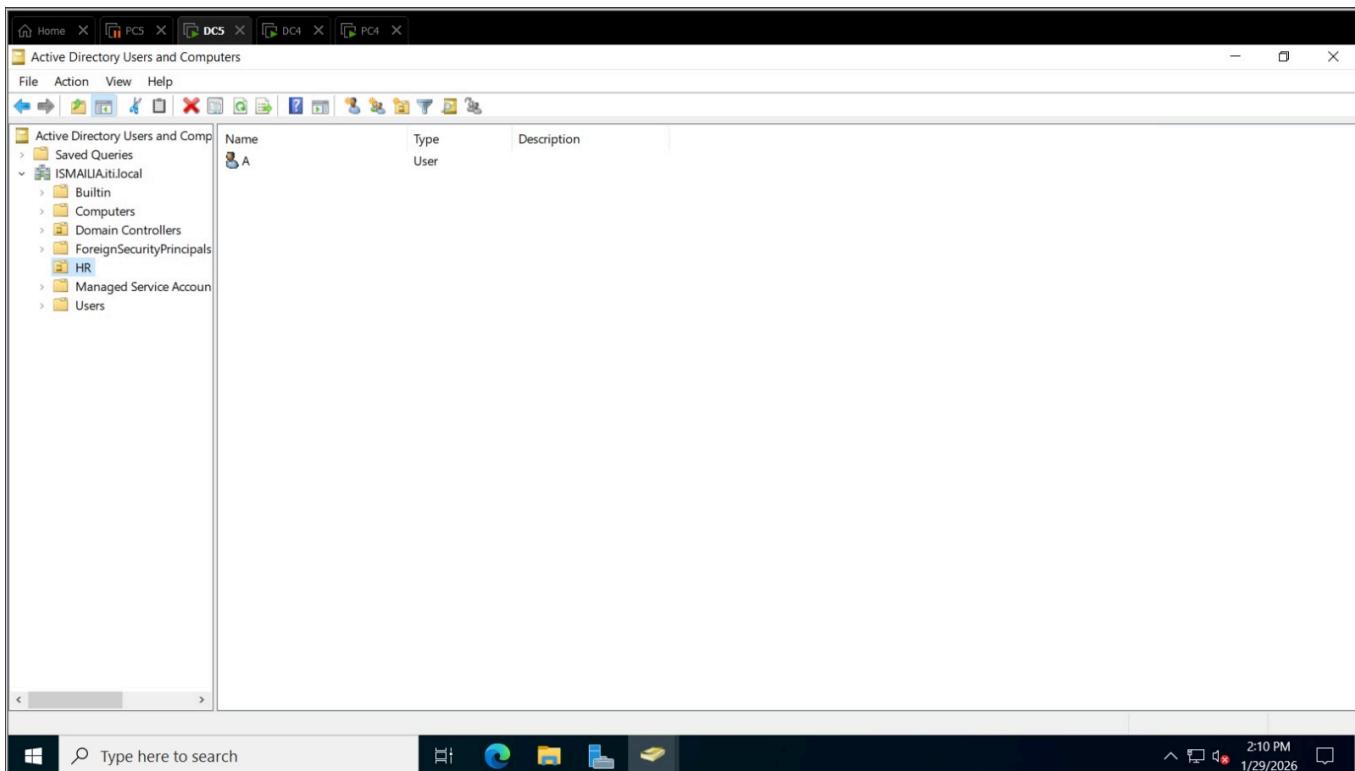
### 4.1. Alex

**ALEX.itilocal** This is the child domain established for the Alexandria branch with **DC4** as its domain controller. Inside this domain, a specific Organizational Unit (OU) named **FIN** has been created to manage the users and resources of the Alexandria finance department.

The screenshot shows the Windows Start menu and the Active Directory Users and Computers (ADUC) application window. The ADUC window displays the structure of the ALEX.itilocal domain under 'Active Directory Users and Computers'. The left pane shows the navigation tree with nodes like 'Saved Queries', 'ALEX.itilocal' (which is expanded to show 'Builtin', 'Computers', 'Domain Controllers' (where 'FIN' is selected), 'ForeignSecurityPrincipals', 'Managed Service Accounts', and 'Users'). The right pane lists a single user entry: Name 'A', Type 'User', and Description 'User'. The taskbar at the bottom shows the Windows logo, a search bar, and several pinned icons (File Explorer, Edge, File History, Task View, and File Explorer again). The system tray shows the date and time as 1/29/2026 at 2:09 PM.

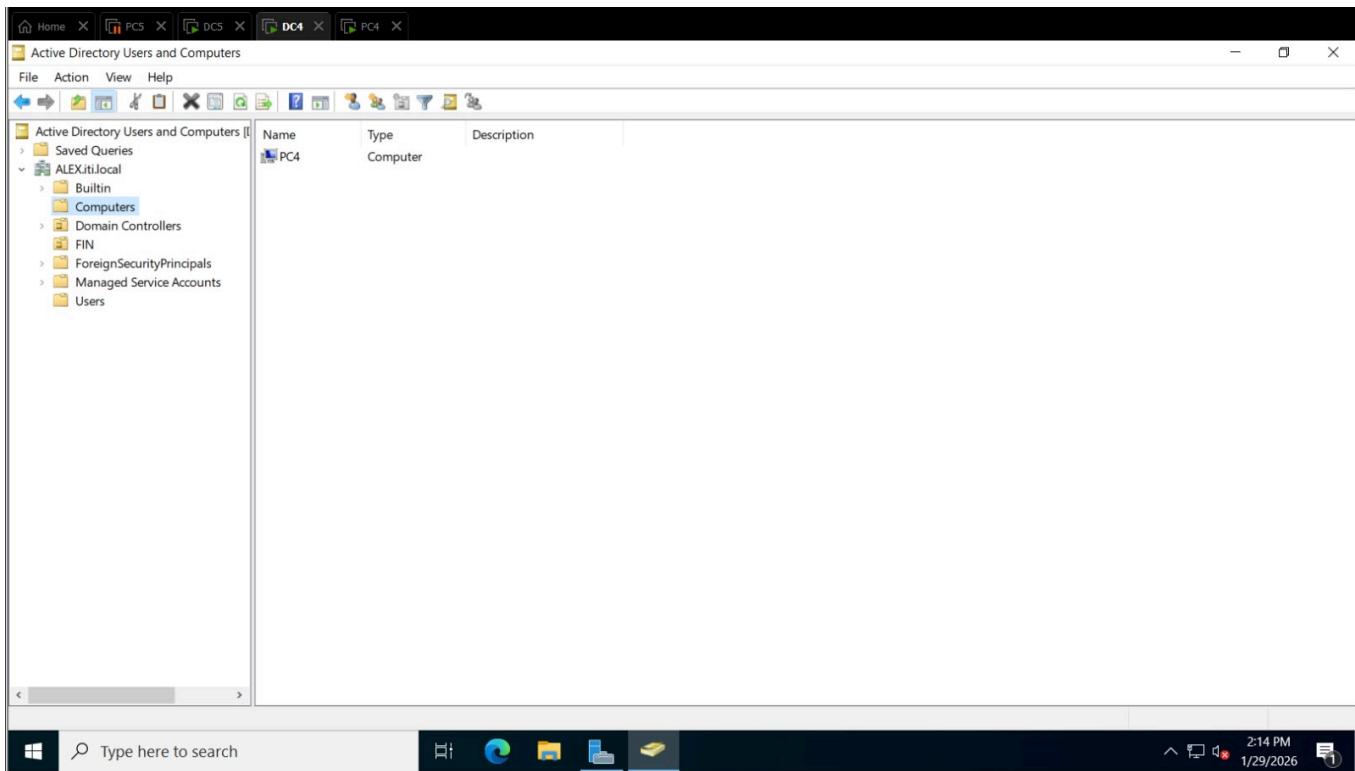
## 4.2. Ismailia

This is the child domain established for the Ismailia branch with **DC5** as its domain controller. Similarly, it contains an Organizational Unit (OU) named **FIN** to centralize and manage the accounts for the finance department in the Ismailia branch.

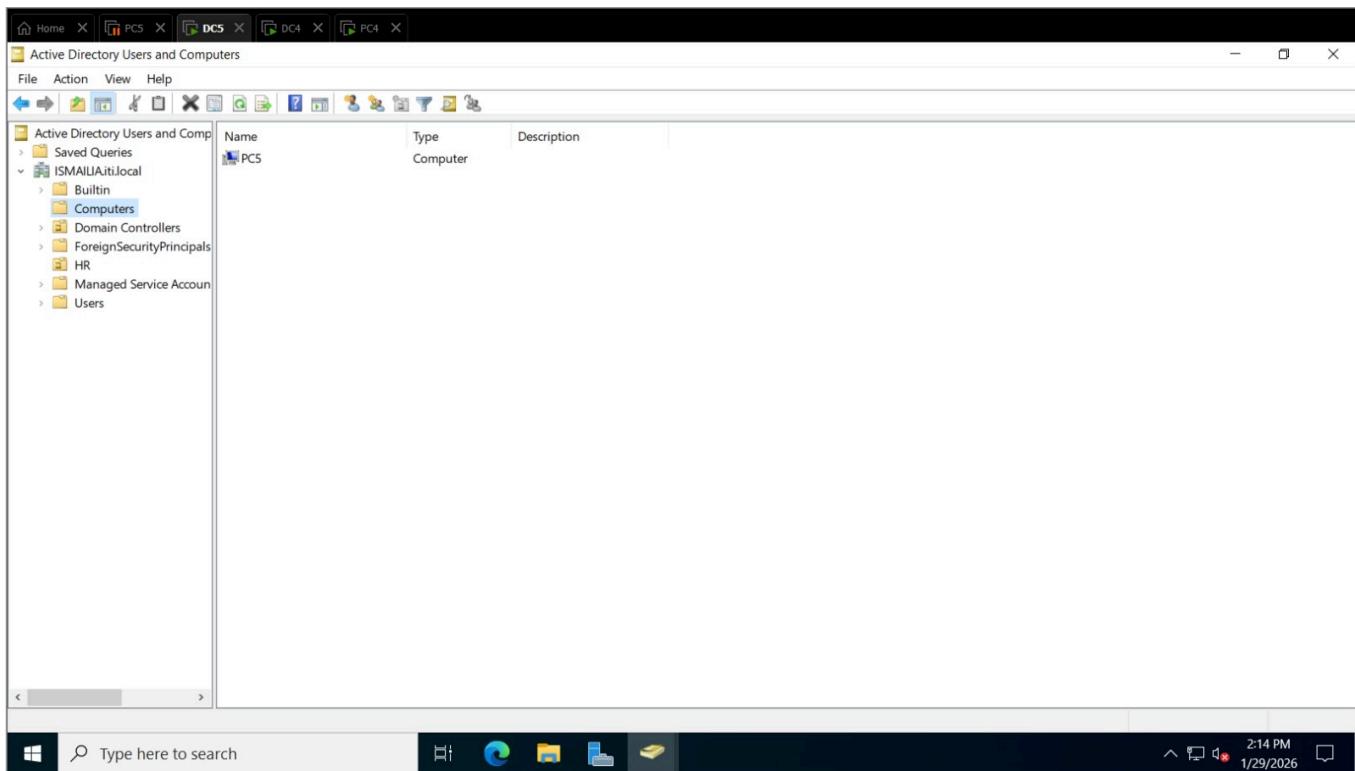


## 4.3. Branch Workstation Domain Integration

**PC4 Joined ALEX Domain** PC4 functions as a member workstation within the **ALEX.iti.local** child domain.



**PC5 Joined Ismailia Domain** PC5 is integrated into the **ISMAILIA.iti.local** child domain as a managed workstation.

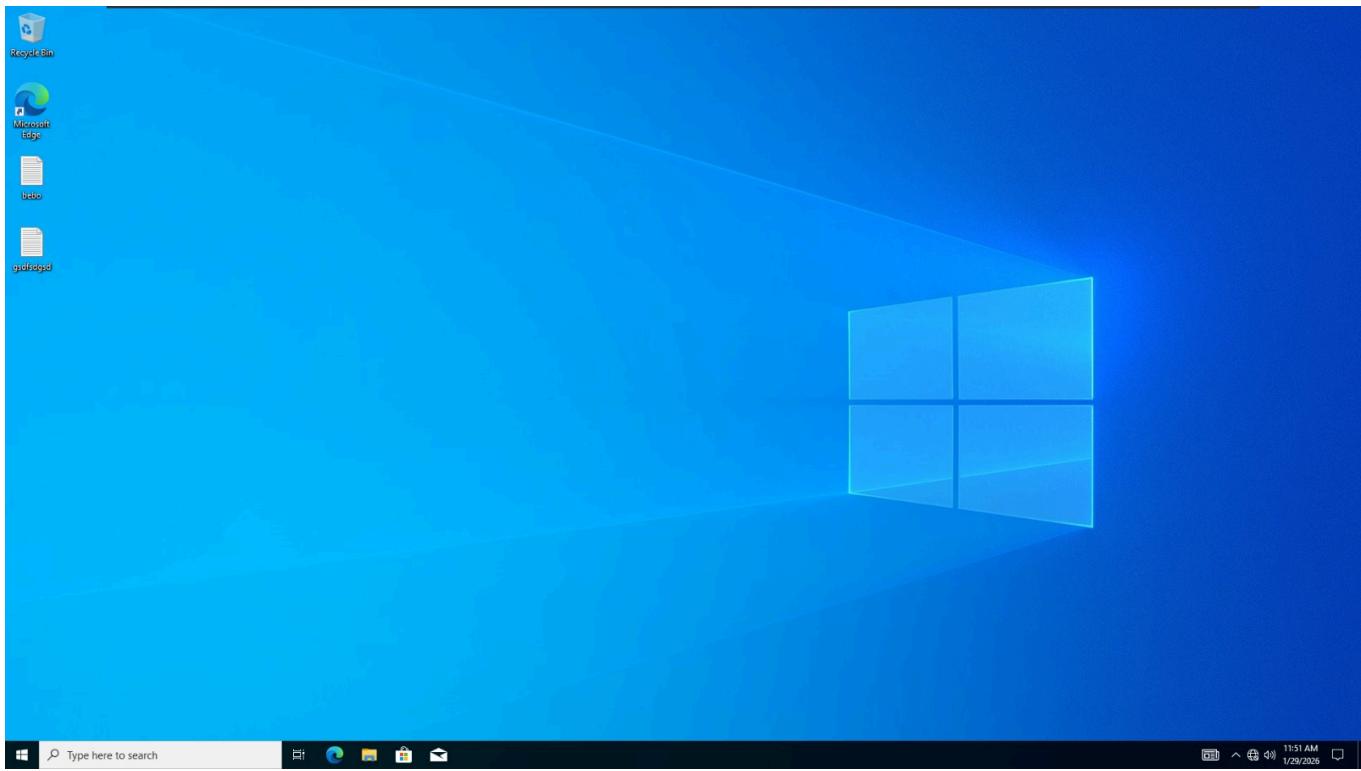


## 5. Roaming

A shared folder is created on the server to act as the central repository for user data. The sharing and NTFS permissions are configured to allow "Domain Users" to create their own profile folders while ensuring data privacy and security across the **iti.local** forest.

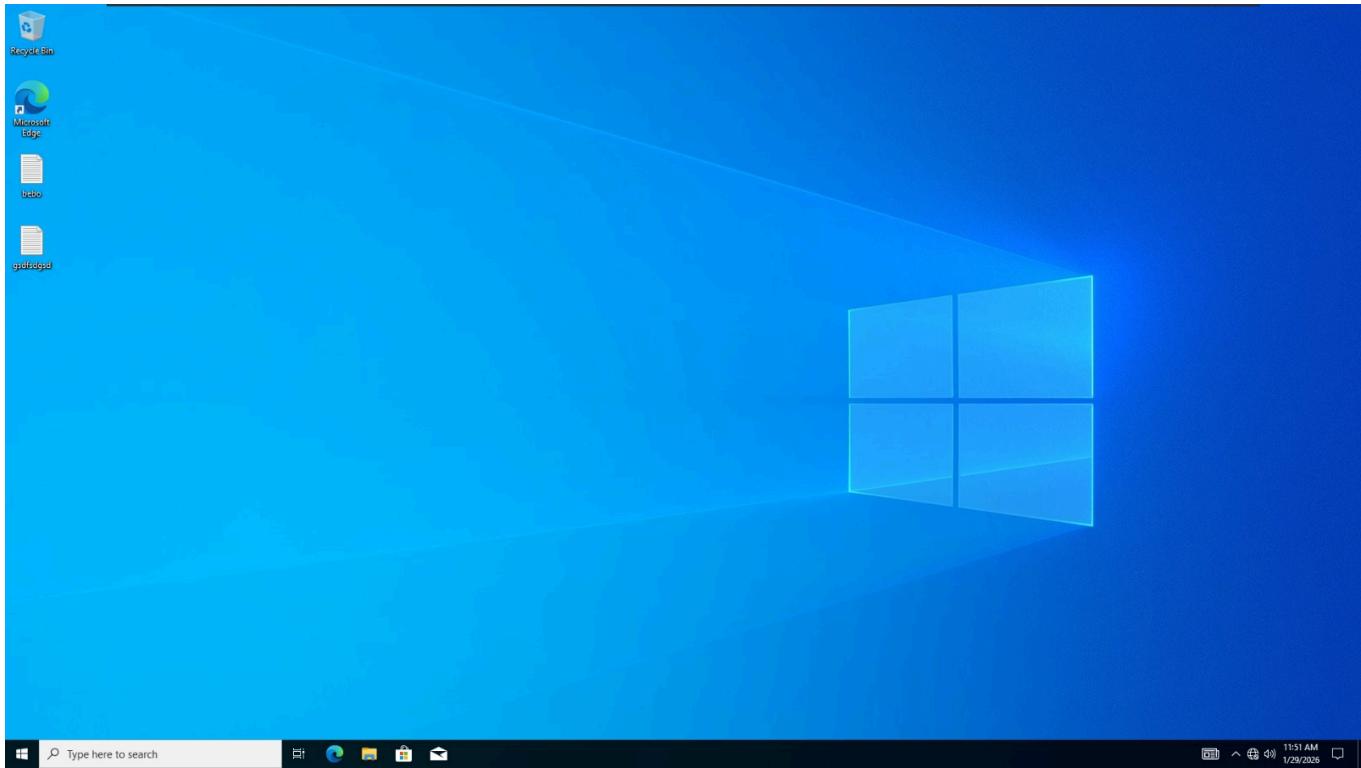
### 5.1. Environment Creation on PC1

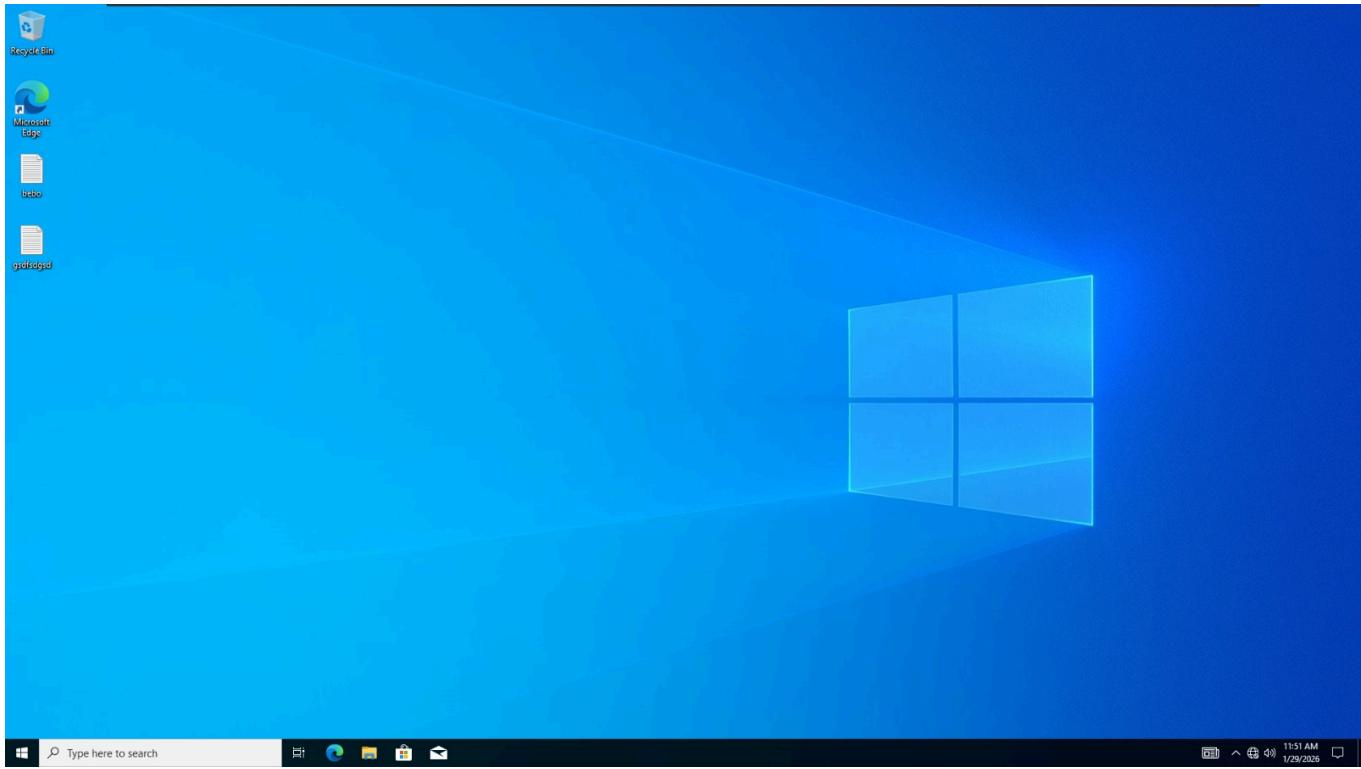
The user performs an initial login on **PC1**. During this session, a test file or folder is created on the desktop. When the user logs out, the local profile is synchronized and uploaded to the centralized **Profiles** folder on the server.



## 5.2. Roaming Verification on PC4 and PC5

The user signs into **PC4** in the **ALEX** domain and **PC5** in the **ISMAILIA** domain. In both instances, the desktop files created on PC1 are immediately visible and accessible. This demonstrates that the roaming profile is successfully retrieved across different child domains, providing a consistent user experience on both branch workstations.





## 6. Delegation

### 6.1 Group Policy Configuration for RDP

In the **Group Policy Management Editor**, the policy "**Allow log on through Remote Desktop Services**" is modified. **User B** is explicitly added to this security setting within the GPO linked to the Domain Controllers. This administrative step overrides the default restriction that prevents non-administrators from logging into a domain controller remotely.

The screenshot shows the Group Policy Management console. The left navigation pane shows a tree structure under 'Forest: iti.local'. The 'Domains' node is expanded, showing 'iti.local' which contains 'Default Domain Policy', 'Remote Login' (selected), 'Domain Controllers', 'Employees', 'FIN', 'HR', 'IT', 'Group Policy Objects', 'WMI Filters', and 'Starter GPOs'. Below 'Domains' are 'Sites', 'Group Policy Modeling', and 'Group Policy Results'. The right pane is titled 'Remote Login' and shows delegation settings. It has tabs for Scope, Details, Settings, and Delegation (selected). A table lists delegation entries:

Name	Allowed Permissions	Inherited
ITI\Domain Admins	Edit settings, delete, modify security	No
ITI\Enterprise Admins	Edit settings, delete, modify security	No
NT AUTHORITY\Authenticated Users	Read (from Security Filtering)	No
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS	Read	No
NT AUTHORITY\SYSTEM	Edit settings, delete, modify security	No

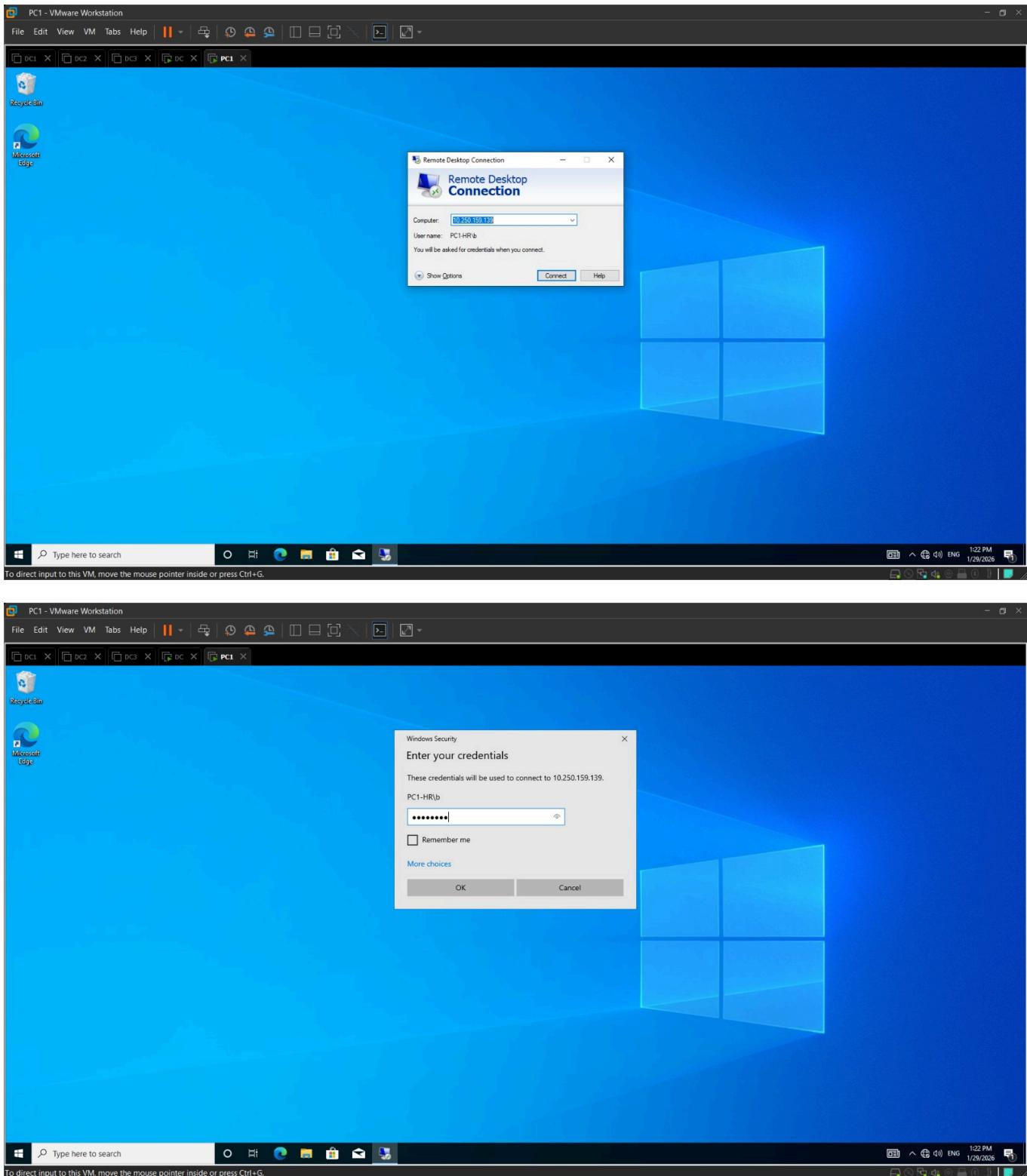
Below the table, sections for 'Computer Configuration (Enabled)' and 'User Configuration (Enabled)' are shown. Under 'Computer Configuration', there are tabs for Policies, Windows Settings, and Security Settings. The Security Settings tab is selected, showing 'Local Policies/ User Rights Assignment' with a single entry:

Policy	Setting
Allow log on through Terminal Services	ITI\B

Under 'User Configuration', it says 'No settings defined.'

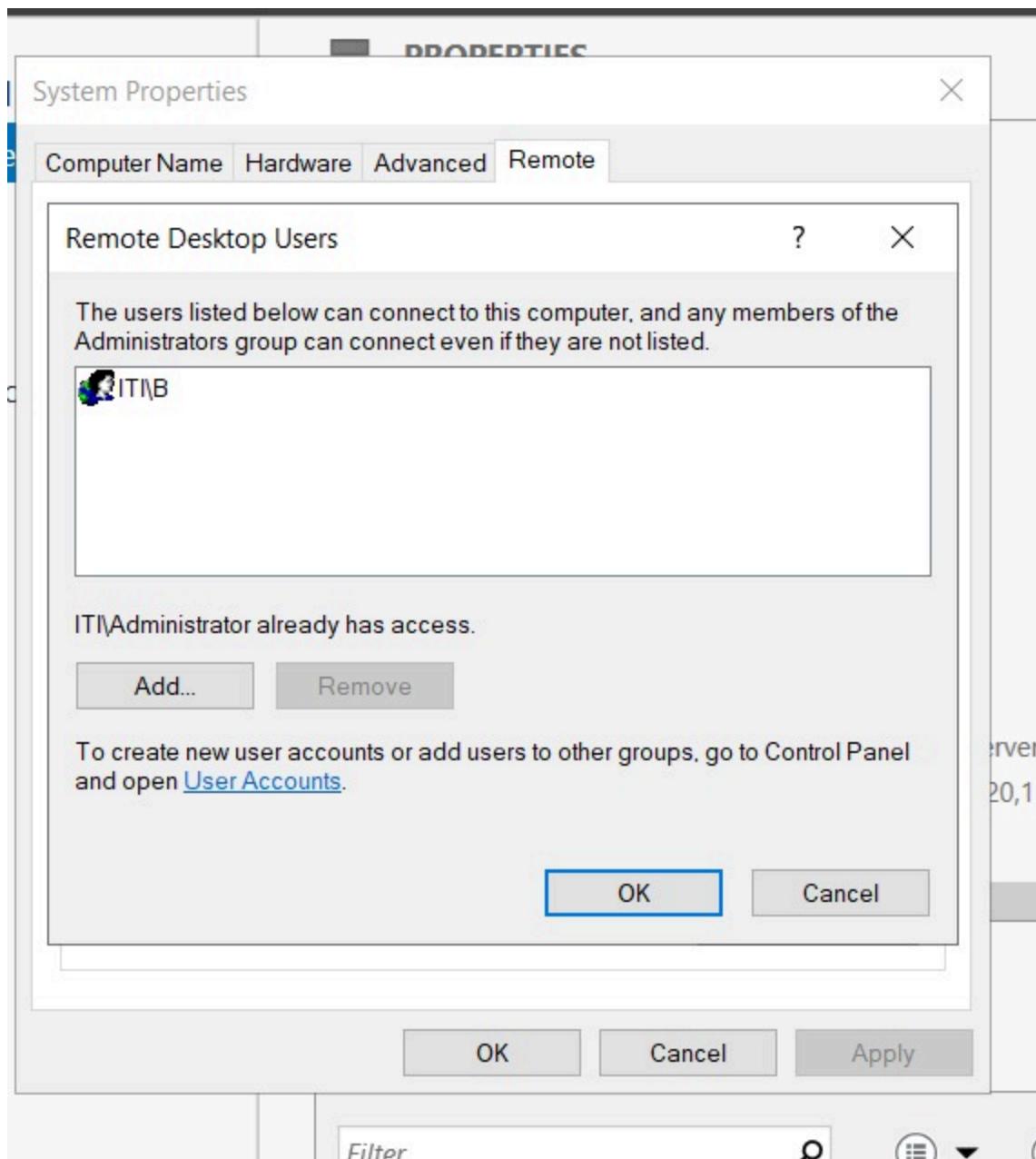
## 6.2 Remote Desktop Connection Setup

The **Remote Desktop Connection** utility is opened on a client workstation, with the target address set to **DC1**. **User B** enters their domain credentials, initiating the authentication process. This visualizes the practical application of the delegation, where a standard user account is used to access server-side resources.



## 6.3. Verification of Remote Access on DC1

The successful remote session on **DC1** is shown, with the desktop environment active for **User B**. This confirms that the delegation settings are correctly applied and that the user can perform managed tasks on the domain controller within their restricted permission set, proving the security configuration is functional.



## 7. Website Check Using Conditional Forwarding

The **DNS Manager** on the **PDC** shows a conditional forwarder configured for the domain **web2.com**. This setting ensures that any DNS queries for this specific domain are automatically forwarded to the IP address **10.250.159.151**, allowing the local network to resolve names for that external or separate infrastructure correctly.

# DNS Manager

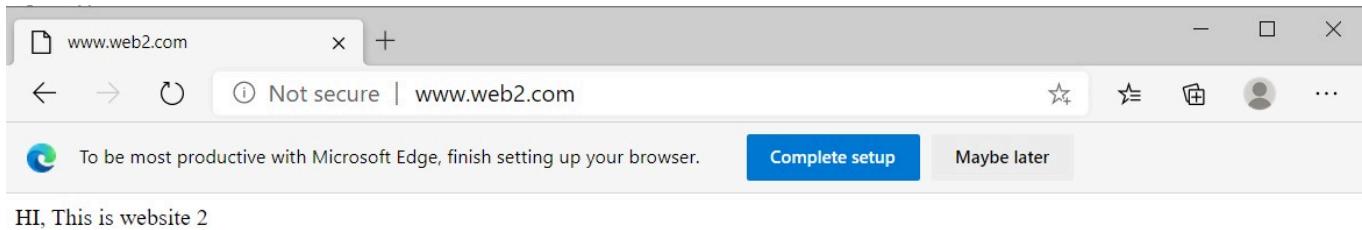


File Action View Help

The screenshot shows the Windows DNS Manager application. On the left, a tree view displays the following structure under the 'DNS' node:

- PDC
  - Forward Lookup Zones
  - Reverse Lookup Zones
  - Trust Points
  - Conditional Forwarders
    - web2.com

In the center-right pane, there is a 'IP Address' section containing the value '10.250.159.151'. At the bottom of the interface, there is a toolbar with icons for various actions like New, Edit, Delete, and Search, along with a 'Filter' button and some dropdown menus.



---

## 8. Script For Creating 50 Users

Automation is implemented using a **PowerShell** script designed to bulk-create user accounts from a CSV file.

- **Script Logic:** The script imports data from `users.csv` and iterates through each entry to create a new Active Directory user with properties including **First Name**, **Last Name**, **Username**, and a secure **Password**.
- **Target Container:** Users are automatically placed within the `OU=Employees,DC=iti,DC=local` organizational unit.
- **Execution Verification:** The PowerShell console displays "Successfully created user" messages for accounts such as **k.anwar**, **n.zaki**, and **h.fawzy**, confirming the batch process completed without errors.

```

$csvPath = "C:\scripts\users.csv"
$container = "OU=Employees,DC=iti,DC=local"
$users = Import-Csv $csvPath
foreach ($user in $users) {
    try {
        $securePassword = ConvertTo-SecureString $user.Password -AsPlainText -Force
        New-ADUser -Name "$($user.Firstname) $($user.Lastname)" `-
            -GivenName $user.Firstname `-
            -Surname $user.Lastname `-
            -SamAccountName $user.Username `-
            -UserPrincipalName "$($user.Username)@iti.local" `-
            -AccountPassword $securePassword `-
            -Enabled $true `-
            -Path $container `-
            -ChangePasswordAtLogon $true
        Write-Host "Successfully created user: $($user.Username)" -ForegroundColor Green
    } catch {
        Write-Host "Error creating user $($user.Username): $($_.Exception.Message)" -ForegroundColor Red
    }
}

```

firstname,Lastname,Username,Password  
 Ahmed,Ali,a.ali,P@ssw0rd2026  
 Sara,Mohamed,s.mohamed,P@ssw0rd2026  
 Omar,Hassan,o.hassan,P@ssw0rd2026  
 Mona,Ibrahim,m.ibrahim,P@ssw0rd2026  
 Youssef,Mahmoud,y.mahmoud,P@ssw0rd2026  
 Laila,Said,l.said,P@ssw0rd2026  
 Khaled,Anwar,k.anwar,P@ssw0rd2026  
 Noura,Zaki,n.zaki,P@ssw0rd2026  
 Hany,Fawzy,h.fawzy,P@ssw0rd2026  
 Amira,Gad,a.gad,P@ssw0rd2026  
 Mostafa,Kamel,m.kamel,P@ssw0rd2026  
 Dina,Adel,d.adel,P@ssw0rd2026  
 Tarek,Nabil,t.nabil,P@ssw0rd2026  
 Mariam,Emad,m.emad,P@ssw0rd2026  
 Ziad,Ashraf,z.ashraf,P@ssw0rd2026  
 Salma,Beda,s.reda,P@ssw0rd2026  
 Wael,Ezzat,w.ezzat,P@ssw0rd2026  
 Heba,Samy,h.samy,P@ssw0rd2026  
 Sherif,Hamdy,s.handy,P@ssw0rd2026  
 Aya,Nasser,a.nasser,P@ssw0rd2026  
 Bassam,Magdy,b.magdy,P@ssw0rd2026  
 Rania,Yasser,r.yasser,P@ssw0rd2026  
 Kareem,Galal,k.galal,P@ssw0rd2026  
 Ghada,Moussa,g.moussa,P@ssw0rd2026  
 Hossam,Taha,h.taha,P@ssw0rd2026  
 Mai,Kamal,m.kamal,P@ssw0rd2026  
 Remy,Farouk,r.farouk,P@ssw0rd2026  
 Engy,Soliman,e.soliman,P@ssw0rd2026  
 Sameh,Sobhy,s.sobhy,P@ssw0rd2026  
 Ola,Amer,o.amer,P@ssw0rd2026

Administrator: Windows PowerShell

```

Successfully created user: k.anwar
Successfully created user: n.zeki
Successfully created user: h.fawzy
Successfully created user: a.gad
Successfully created user: m.kamel
Successfully created user: d.adel
Successfully created user: t.nabil
Successfully created user: m.emad
Successfully created user: z.ashraf
Successfully created user: s.reda
Successfully created user: w.ezzat
Successfully created user: h.samy
Successfully created user: s.handy
Successfully created user: a.nasser
Successfully created user: b.magdy
Successfully created user: r.yasser
Successfully created user: k.galal
Successfully created user: g.moussa
Successfully created user: h.taha
Successfully created user: m.kamal
Successfully created user: r.farouk
Successfully created user: e.soliman
Successfully created user: s.sobhy
Successfully created user: o.amer
Successfully created user: m.abbas
Successfully created user: e.hafiz
Successfully created user: f.nagib
Successfully created user: s.ramadan
Successfully created user: i.rashed
Successfully created user: d.saber
Successfully created user: a.bakr
Successfully created user: r.fathy
Successfully created user: h.shaker
Successfully created user: n.badawy
Successfully created user: k.lofty
Successfully created user: y.wegdy
Successfully created user: m.saad
Successfully created user: a.sadek
Successfully created user: n.refaat
Successfully created user: j.khaliry
Successfully created user: s.aziz
Successfully created user: i.gaber

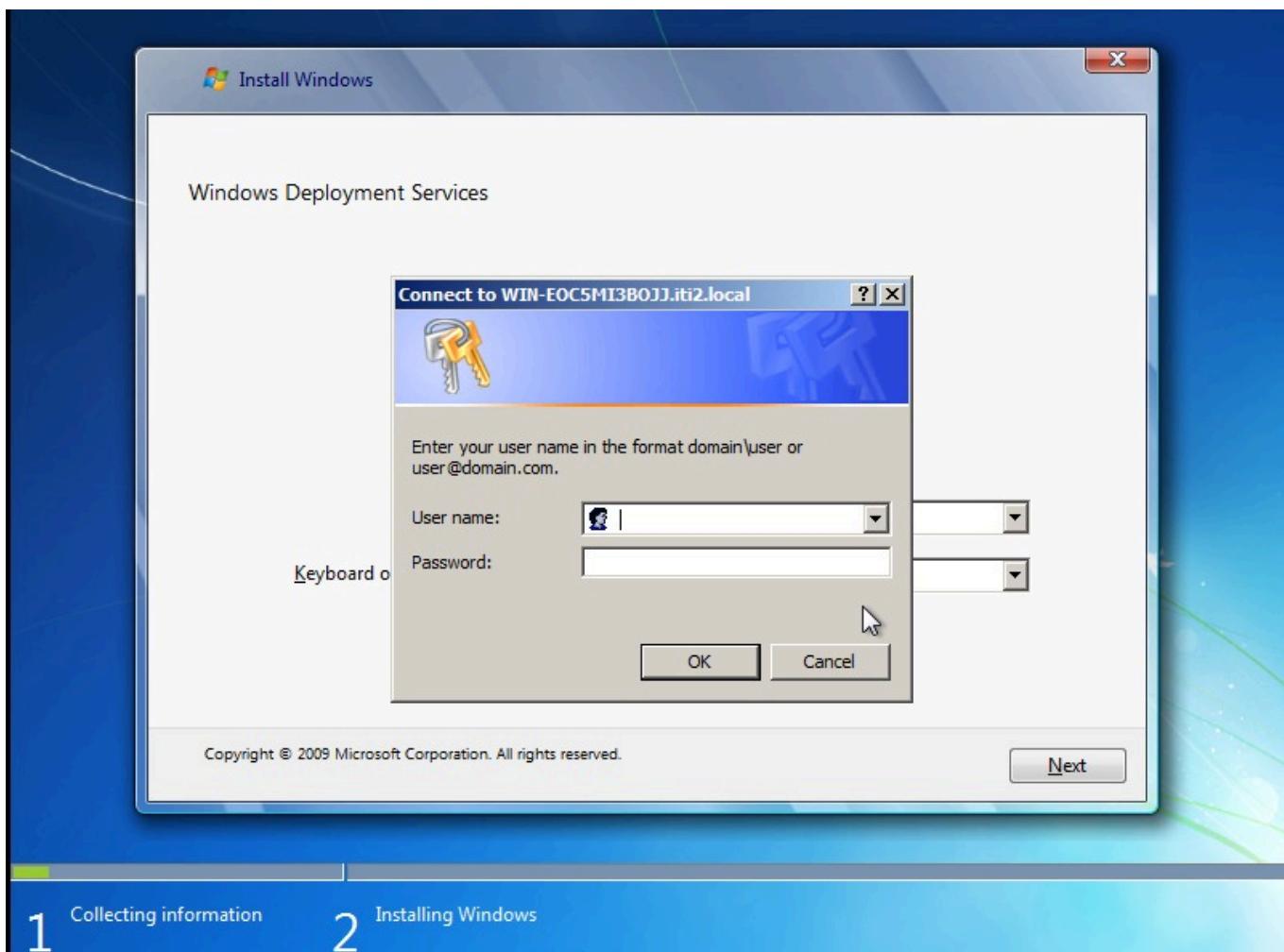
```

## 9. Windows Deployment Services

**Windows Deployment Services (WDS)** is a server role that enables the remote deployment of Windows operating systems. Instead of installing an OS on each machine manually using a physical disk or USB, WDS allows you to "push" the installation over the network to multiple computers simultaneously.

### 9.1. WDS Authentication

This is the **WDS Authentication** screen on the client machine. It requires a user to enter domain credentials (in `domain\user` format) to authorize the connection to the WDS server (**WIN-EOC5MI3BOJJ.iti2.local**) and start the installation.



## 9.2. IP Address Acquisition

A command prompt window shows the results of the `ipconfig` command. It captures the transition from a self-assigned APIPA address (**169.254.90.42**) to a valid network IP address (**192.168.120.128**) provided by the DHCP server.

```
Connection-specific DNS Suffix . . . .
Autoconfiguration IPv4 Address. . . : 169.254.90.42
Subnet Mask . . . . . : 255.255.0.0
Default Gateway . . . . . :

C:\Users\Administrator>ipconfig

Windows IP Configuration

    Ethernet adapter Ethernet0:

        Connection-specific DNS Suffix . . . .
        IPv4 Address. . . . . : 192.168.120.128
        Subnet Mask . . . . . : 255.255.255.0
        Default Gateway . . . . . :

C:\Users\Administrator>ipconfig

Windows IP Configuration

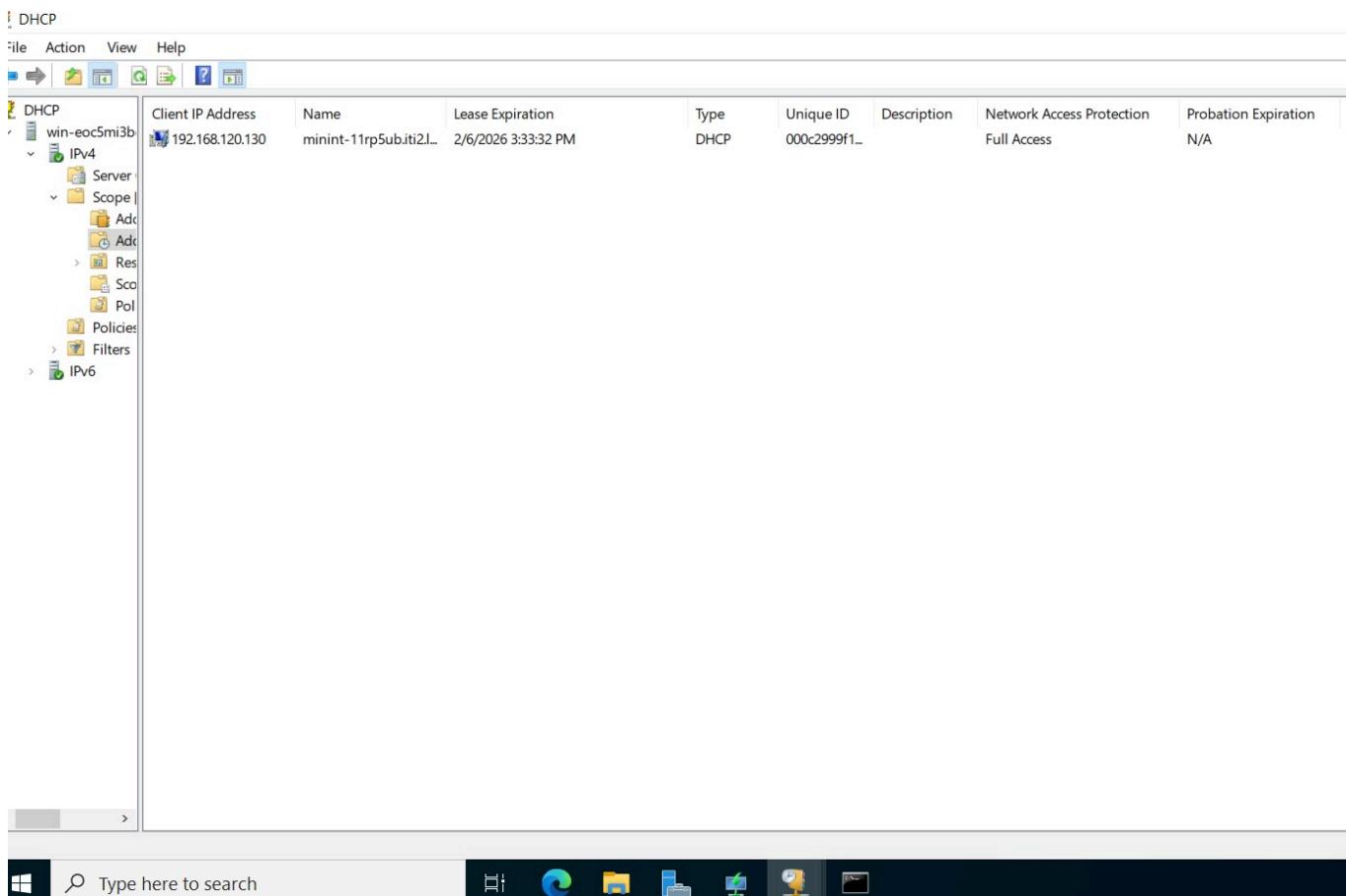
    Ethernet adapter Ethernet0:

        Connection-specific DNS Suffix . . . .
        IPv4 Address. . . . . : 192.168.120.128
        Subnet Mask . . . . . : 255.255.255.0
        Default Gateway . . . . . :

C:\Users\Administrator>
```

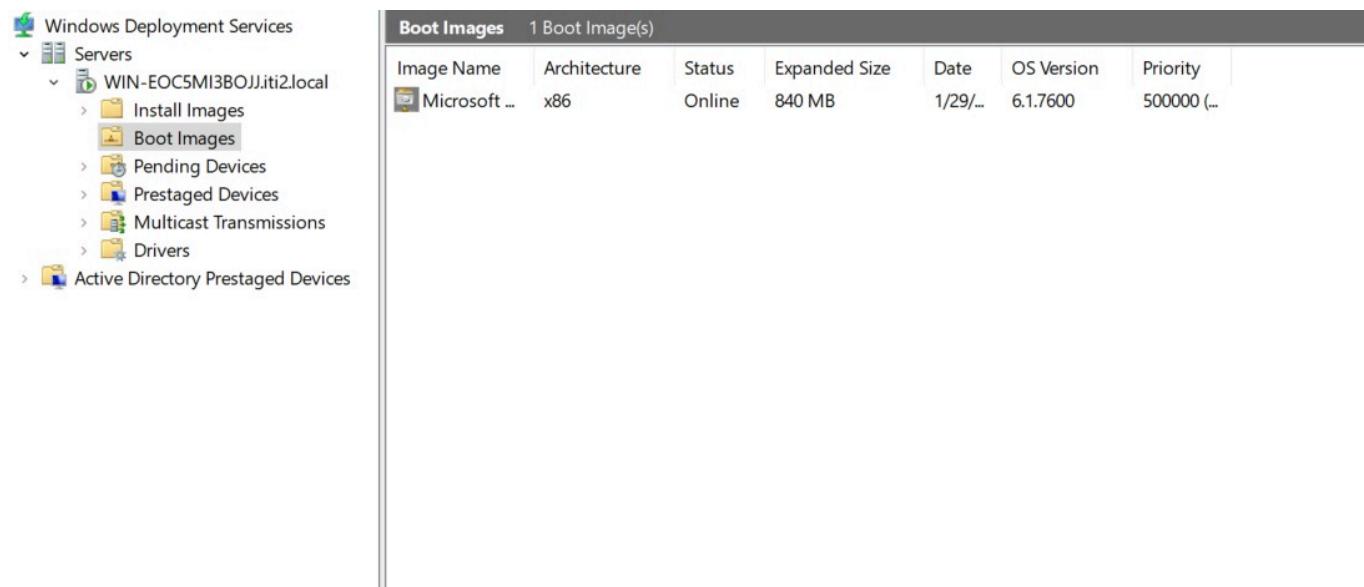
## 9.3. DHCP Lease Verification

The **DHCP Management** console shows the **Address Leases** for the network. It lists a specific client (**minint-11rp5ub.iti2...**) that has been assigned the IP address **192.168.120.130**, which is necessary for the client to communicate during the WDS process.



## 9.4. Boot and Install Image Configuration

The **WDS Manager** displays the **Boot Images** section. It shows one Microsoft Windows Setup (x86) image is "Online" and ready to be used by client computers to boot into the deployment environment.



The **WDS Manager** shows the **Install Images** grouped under **ImageGroup1**. It lists five different versions of Windows 7 (x86) that are available for deployment to workstations on the network.

The screenshot shows the Windows Deployment Services Management console. On the left, the navigation pane displays the following structure:

- Windows Deployment Services
- Servers
  - WIN-EOC5MI3BOJJ.iti2.local
    - Install Images
      - ImageGroup1
    - Boot Images
    - Pending Devices
    - Prestaged Devices
    - Multicast Transmissions
    - Drivers
  - Active Directory Prestaged Devices

The main pane is titled "ImageGroup1 5 Install Image(s)" and contains a table with the following data:

Image Name	Architecture	Status	Expanded Size	Date	OS Version	Priority
Windows 7 ... x86	x86	Online	7622 MB	1/29/...	6.1.7600	500000 (...)
Windows 7 ... x86	x86	Online	8042 MB	1/29/...	6.1.7600	500000 (...)
Windows 7 ... x86	x86	Online	7928 MB	1/29/...	6.1.7600	500000 (...)
Windows 7 ... x86	x86	Online	8078 MB	1/29/...	6.1.7600	500000 (...)
Windows 7 ... x86	x86	Online	7568 MB	1/29/...	6.1.7600	500000 (...)

## 9.5. Deployment Progress

This is the **Installing Windows** progress screen on the client workstation. It confirms that the deployment is active.

