Domain Controller Prep

The Frame platform supports the ability for your workload VMs to join your on-premises or cloud-based Microsoft Active Directory (AD) environment.

Requirements

- Frame Account with **Windows 10**, **Windows 11**, **Windows Server 2019**, or **Windows Server 2022-based image**.
- The Domain Join feature requires customers use **Windows Server 2008 R2** and **Domain Functional Level** 2008 R2 or higher.
- The Frame account workloads must reside in a VPC/VNET/VLAN with a non-overlapping CIDR with the rest of your network, including where your Windows domain controllers reside. Frame supports subnet masks between `/16` and `/24`.
- The workload VMs to be joined to the domain must be able to reach the domain controller(s).
- Customers using AWS infrastructure must update their AWS IAM role before enabling DJI (as described in the guide listed below).
- Customers using Azure infrastructure must configure their Azure DNS before enabling DJI (as described in the guide listed below).

Considerations

Please consider the following before continuing with this Domain Controller Preparation guide and setup process:

- The Frame user created by Frame must be a local Windows administrator. Any GPO settings that take effect on workload instances must not remove this user from the “Local administrators” group.
- Autologin must be allowed for a local Frame user session to initiate successfully. Any GPO settings that disable this function will prevent domain joined instances from working properly.
- Interactive Logon message must be disabled in GPO settings for successful initiation of a Frame session.
- The domain join feature does not join the Sandbox or any utility servers to the domain. Frame strongly advises that administrators do not manually join the Sandbox or the

utility server to the domain unless there is a specific requirement for an application to function. If either of these two VM types must be joined to the domain, the Frame administrator should enable RDP and create another local Windows admin user in that server. Before the server is joined to the domain, the administrator should verify that they can reach the server using RDP.
- Do not modify the Frame user local admin account password. Modifying the password will cause autologon to fail. For password security options like LAPS, there is a need to exclude the local Frame user.
- Static DNS IPs are not supported and should not be entered in the Sandbox or workload VMs.
- Restricting remote RPC connections to the Windows Security Account Manager (SAM) on a domain controller to Administrators only may introduce issues with renaming computer objects in Active Directory. Delegated rights to the service account will be ignored if this policy is configured
- The local Frame user password is stored in LSA (Local Security Authority) portion of the machine registry that is accessible only to SYSTEM account processes. Some of these secrets are credentials that must persist after reboot and they are stored in encrypted form on the hard disk drive. Credentials stored as LSA secrets might include:
  - Local Frame user password
  - Service account name and password for web proxy

Supported Deployment Models and Systems

To use the Domain Join feature, the workload VMs must have network access to your domain controllers. There are a few architectural models to use for connecting your Frame workloads to your AD domain controllers:

1. If your workloads are in one of the supported public cloud infrastructures, your domain controllers (DCs) can be located in the public cloud or on-premises.
   - If the DCs are on-premises, then an always-on connection from the workload VMs in the public cloud to your on-premises DCs is required. This can be accomplished through a site-to-site VPN, direct connection, or SD-WAN connection. You must bring your own AWS, Azure, or GCP cloud account to establish these types of private network connections since these network connections are setup within the public cloud provider's console. A software client VPN on the workload VMs that require users to authenticate to your on-premises firewall will not satisfy the networking requirements for domain-joined instances.
   - If the DCs are in the public cloud, then you can configure a route from your workload VMs to your DCs. This is typically done with a peering connection between the VPC/VNET containing your workload VMs and the VPC/VNET containing your Domain Controllers.
2. If your workloads are on Nutanix AHV in your on-premises network, then make sure that the workload VMs can route from the workload VLAN to your domain controllers.

In the above architectural models, you will need to configure your networking and firewall rules to enable all ports and protocols corresponding to Active Directory traffic. Such a list can be found online in Microsoft documentation. Please read through this guide thoroughly before beginning the process of connecting your AD environment with your Frame workloads.

> When Frame workload VMs are provisioned, the VMs rely on the DHCP service within your network to obtain their IP addresses and DNS server IP address(es). For customer-managed networking, make sure that you have configured your DHCP service to return the IP addresses of your DNS servers. Otherwise, if no DNS server IP address is provided to the newly provisioned VMs, the VMs may not be able to resolve your domain controller or the Frame Platform FQDNs.

Requirements

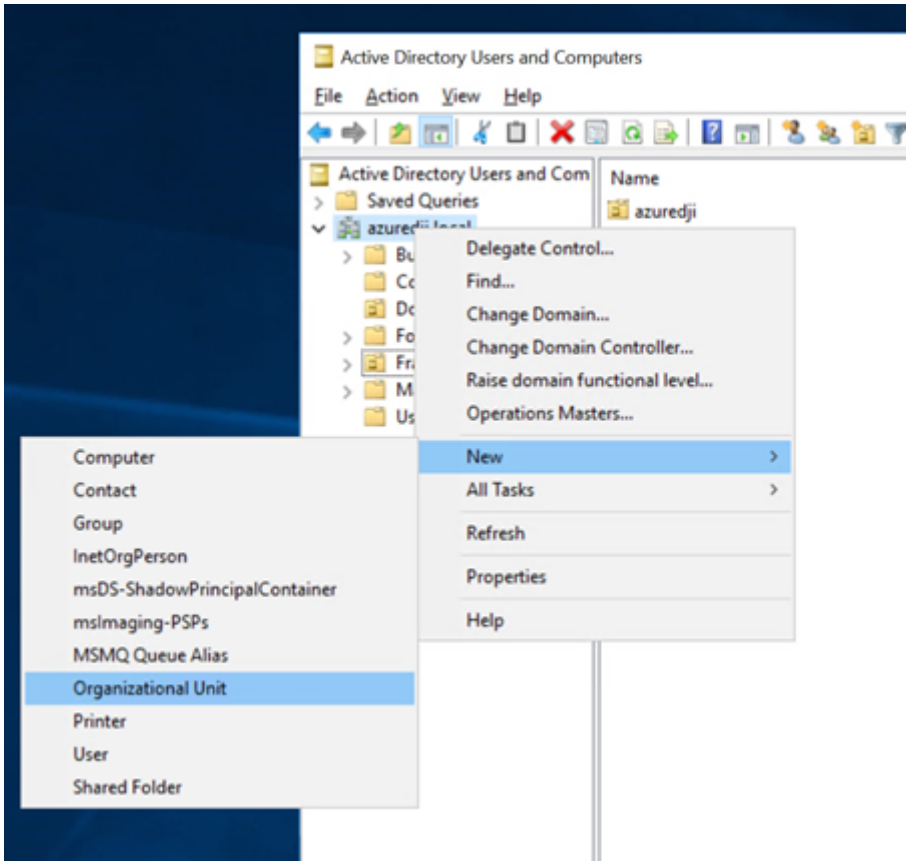
- Organizational Unit (OU) should not have spaces in it (e.g., `FrameAzure1`, not `Frame Azure 1`).
- Service account must own the OU using “Delegate control."
- Service Account must be in UPN format (e.g., `frameserviceaccount@mycompany.com`)

Best Practices

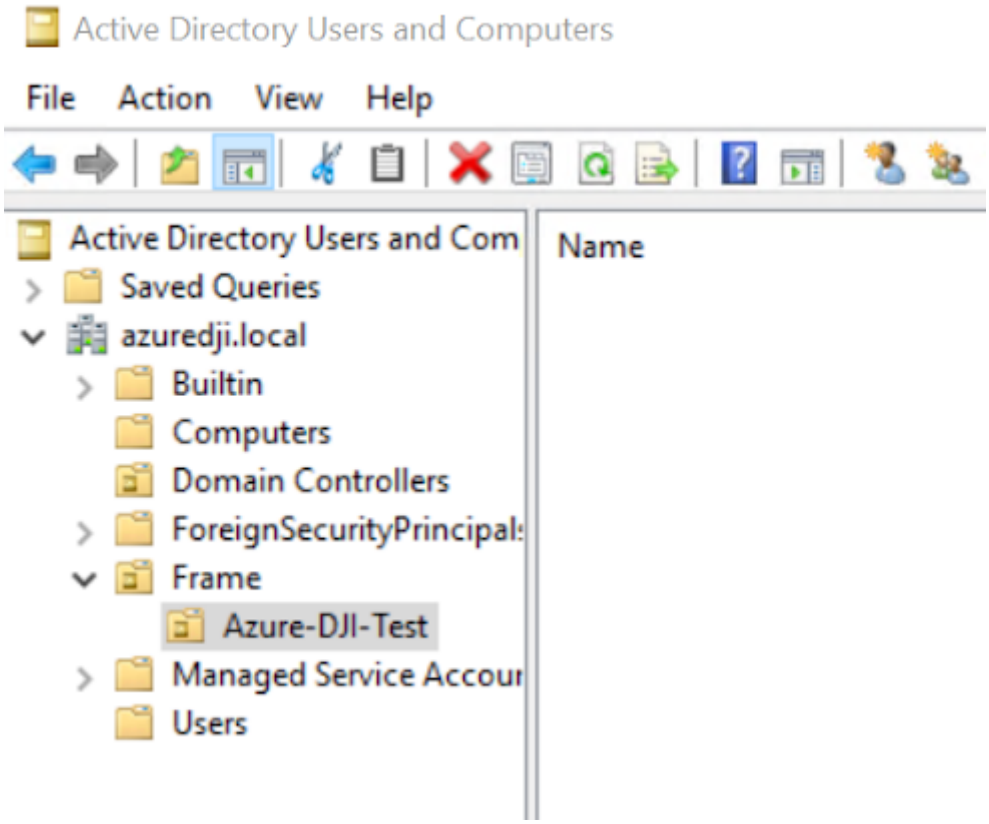
- Customers are responsible for tracking their service account password expiration date and updating the new password in the Domain Settings for the Frame account before the password expires. If the service account password expires, the Frame account publish will fail since the workload VMs will be unable to join to the domain. Alternatively, customers can configure their service account password to not expire.
- During installation and initial configuration, inheritance should be blocked on the Frame OUs. When making policy changes, Nutanix recommends customers create a Development/Staging account to test your policies (in a separate OU) before implementing the policies in the OU for the Production Frame accounts.
- As a best practice, Frame **does not recommend** restricting remote RPC connections to the Windows Security Account Manager (SAM) on a domain controller to Administrators only. Doing so may introduce issues with renaming computer objects in Active Directory. Delegated rights to the service account will be ignored if this policy is configured.

Domain Controller Preparation Procedure

1. Log into your domain controller and open up “Active Directory Users and Computers."
2. Navigate to the “Computers" Organizational Unit (OU), right-click and select “Create a New OU". We recommend that you give this OU a unique name that will help you identify the Frame account that it is tied to. In this example, we have named the OU `Frame-DJI-Test`.

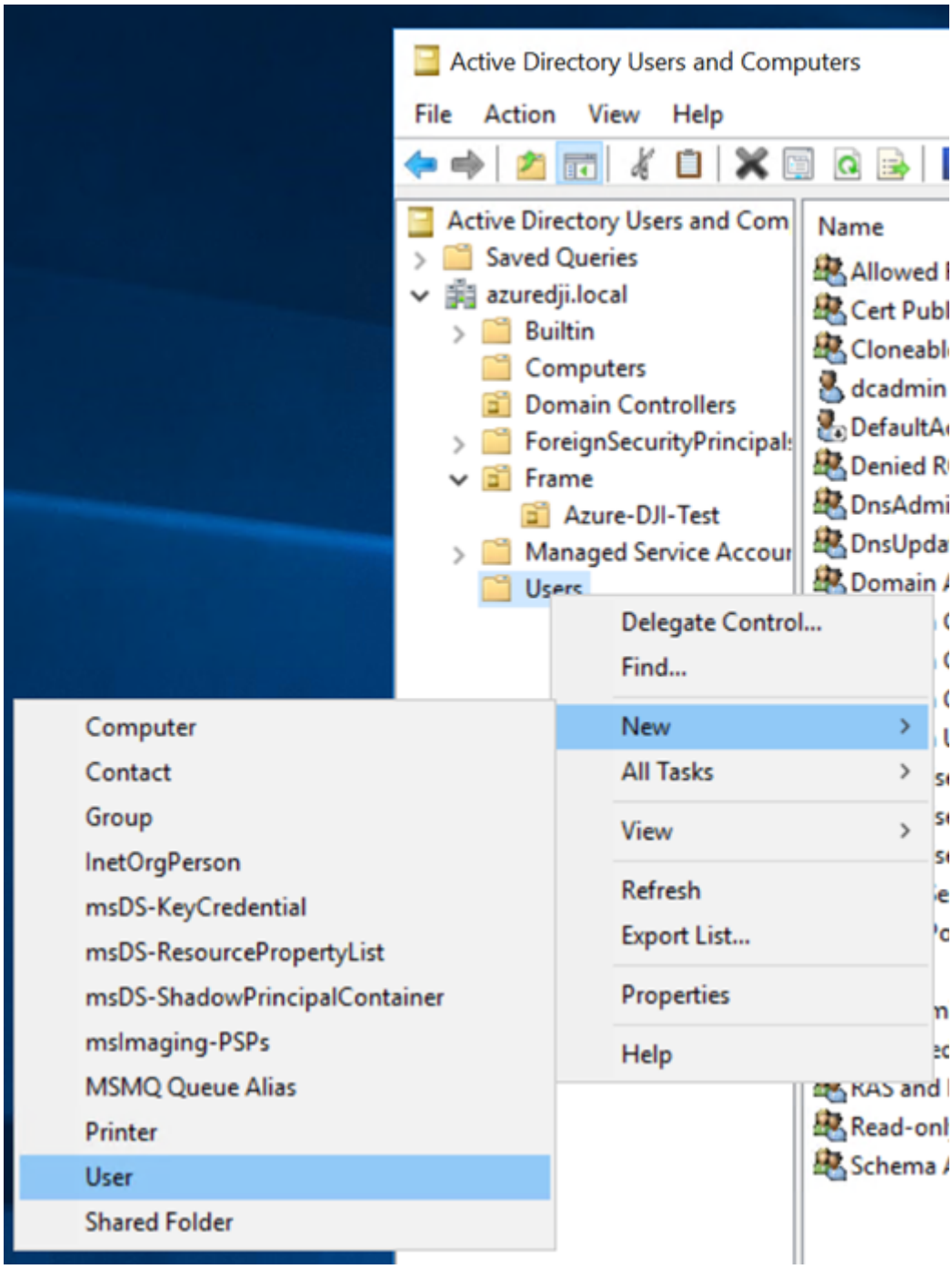


3. In our example, we created a new OU for Frame. Inside of that OU, we created another sub OU with the account name we will be using. This is **strongly recommended** to prevent confusion for situations where multiple Frame accounts are joined to the same domain.

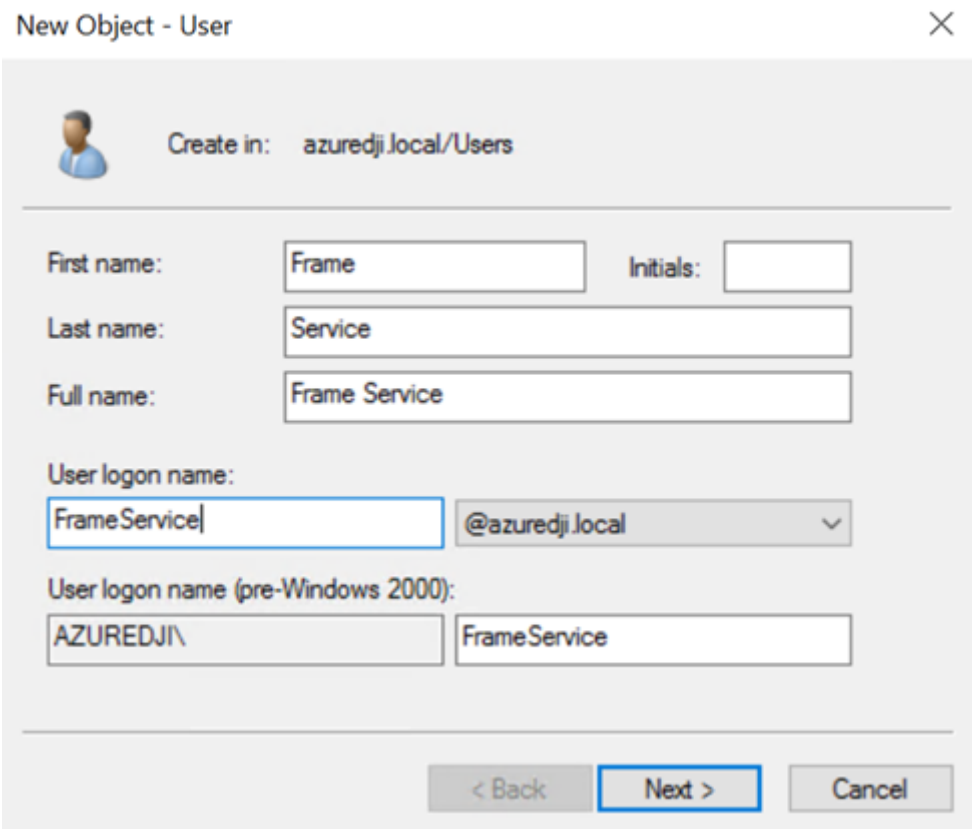


Create Service Account

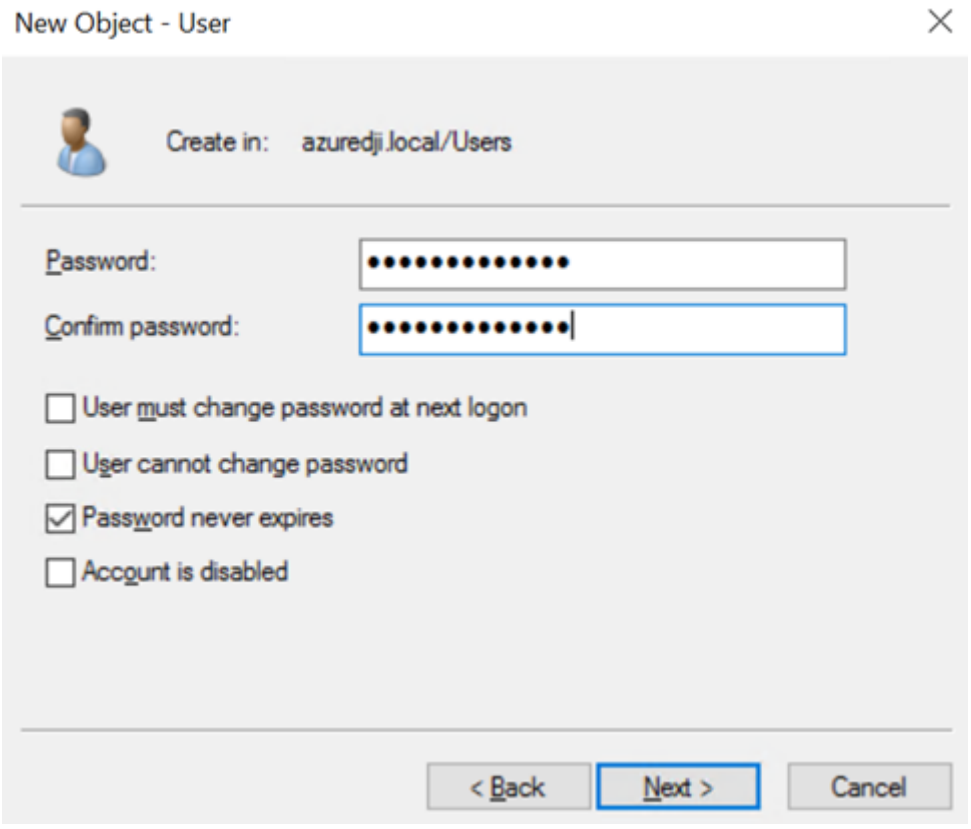
4. Next, we will create a service account to manage the necessary Frame resources. To start this process, we will need to add a new user. It is recommended you create this user where your organization keeps other service accounts. In our example, we will add them directly into the “Users" OU by right-clicking “Users". Select “New" and click “User."



5. Add the necessary information to help you identify what this service account will be used for. Click "Next."



6. Set the desired password for the service account. If your organization allows it, it is recommended to set your service account password to "never expire." Make sure to uncheck "User must change password at next logon" and click "Next" and then "Finish."



:::info Service Account Password Requirements

The service account password must contain 16 characters, with at least one character out of each category:

- Uppercase characters A-Z (Latin alphabet)
- Lowercase characters a-z (Latin alphabet)
- Digits 0-9
- Special characters (!, #, %, etc.)

Characters allowed:

- A – Z
- a - z
- 0 – 9
- `@ # % ^ & \ - _ ! + = [ ] { } | : ‘ , . ? / ` ~ ( ) ; < >`

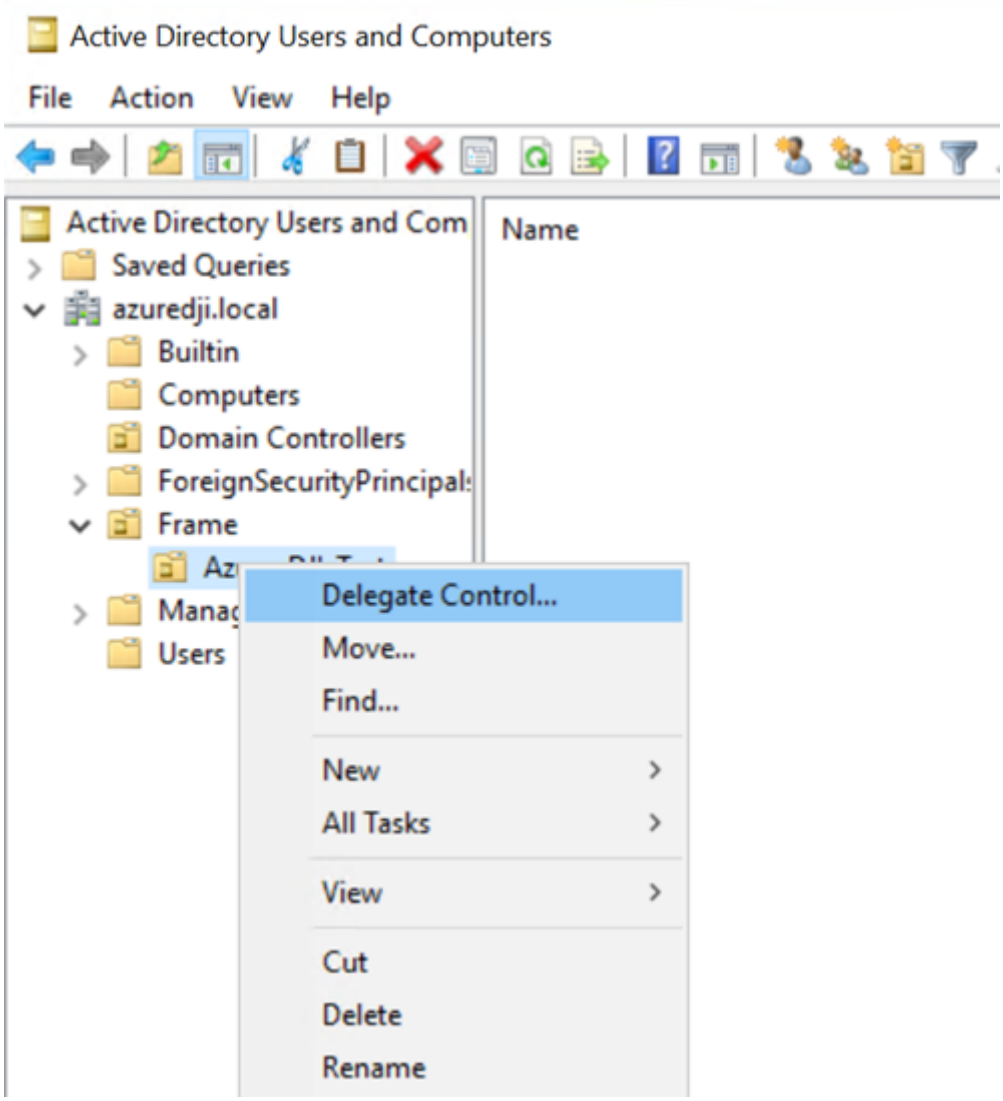
Characters NOT allowed:

- blank space
- `\` backslash
- `$` symbol
- `"` (double quotes)
- Unicode characters

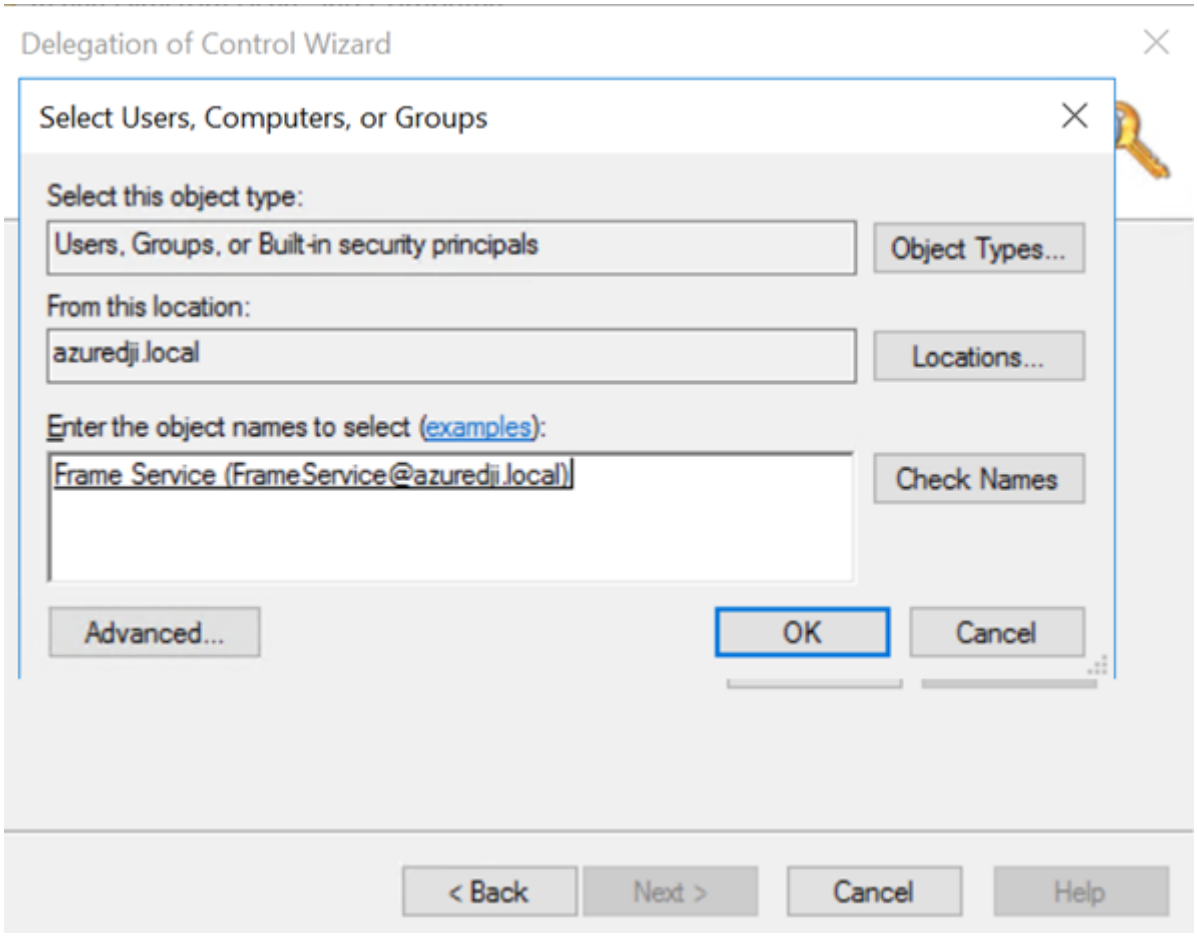
:::

> If the service account password expires, the account will not function until the password is updated. The updated password will then need to be set in the Frame Dashboard as well. If an admin attempts to publish from their Frame account with expired domain join credentials, the publish will fail.

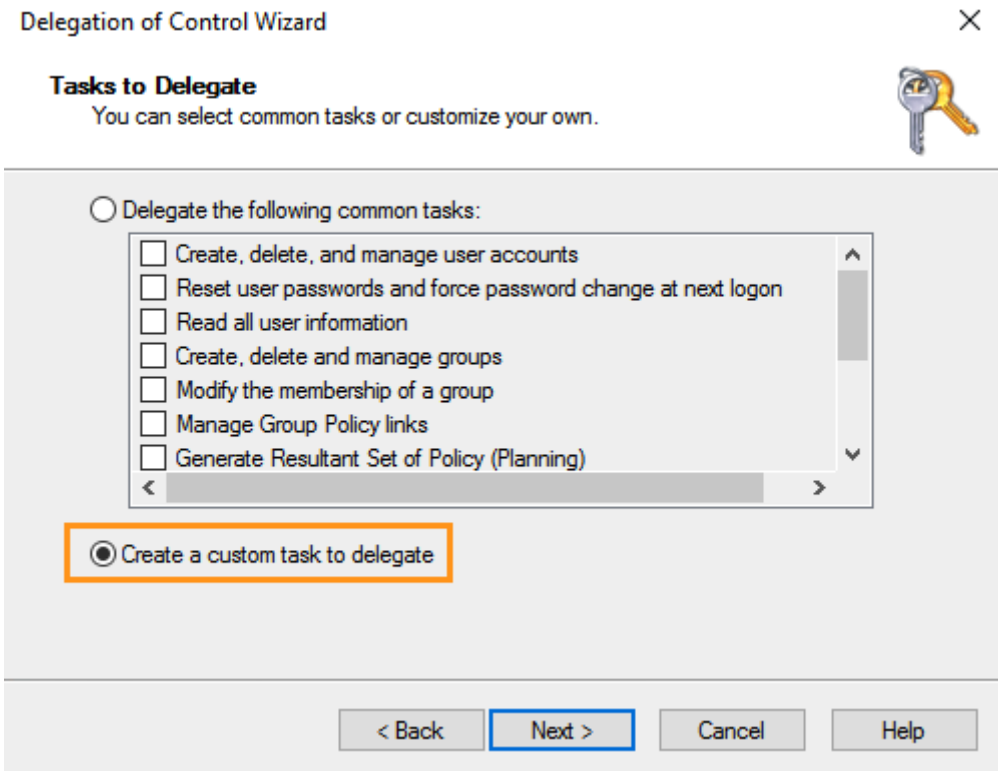
7. Right-click on the newly-created OU and select “Delegate Control…" to open the Delegation of Control Wizard.



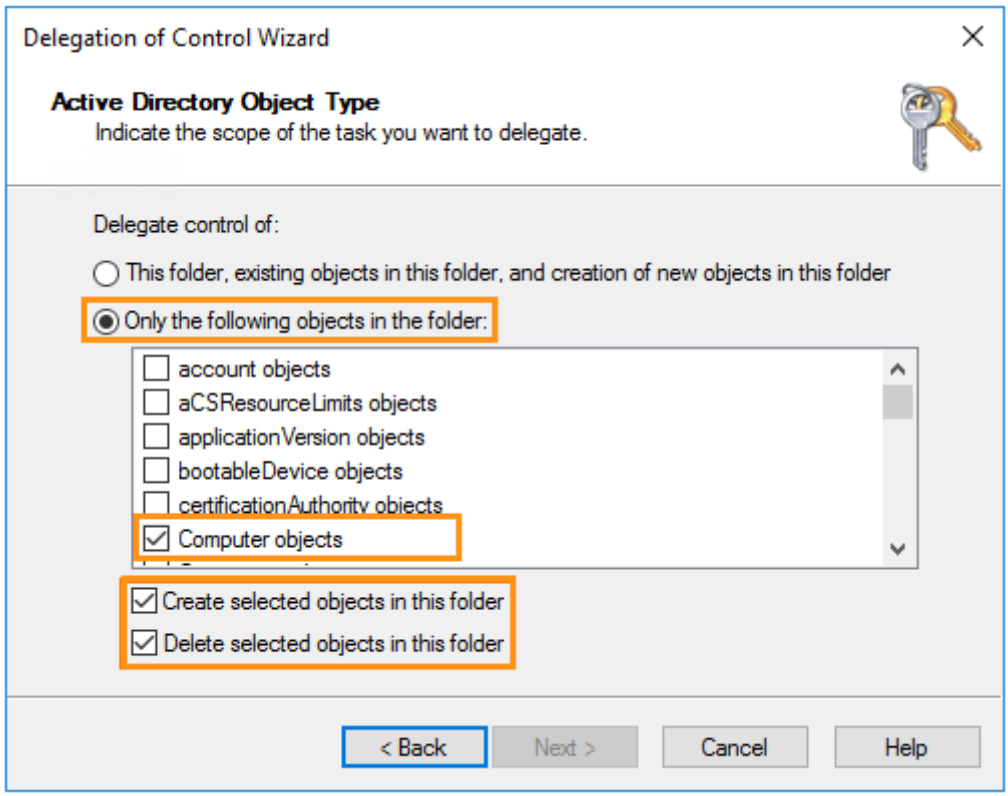
8. Select your Frame service account.



9. On the "Tasks to Delegate" page, select “Create a custom task to delegate" and click “Next."

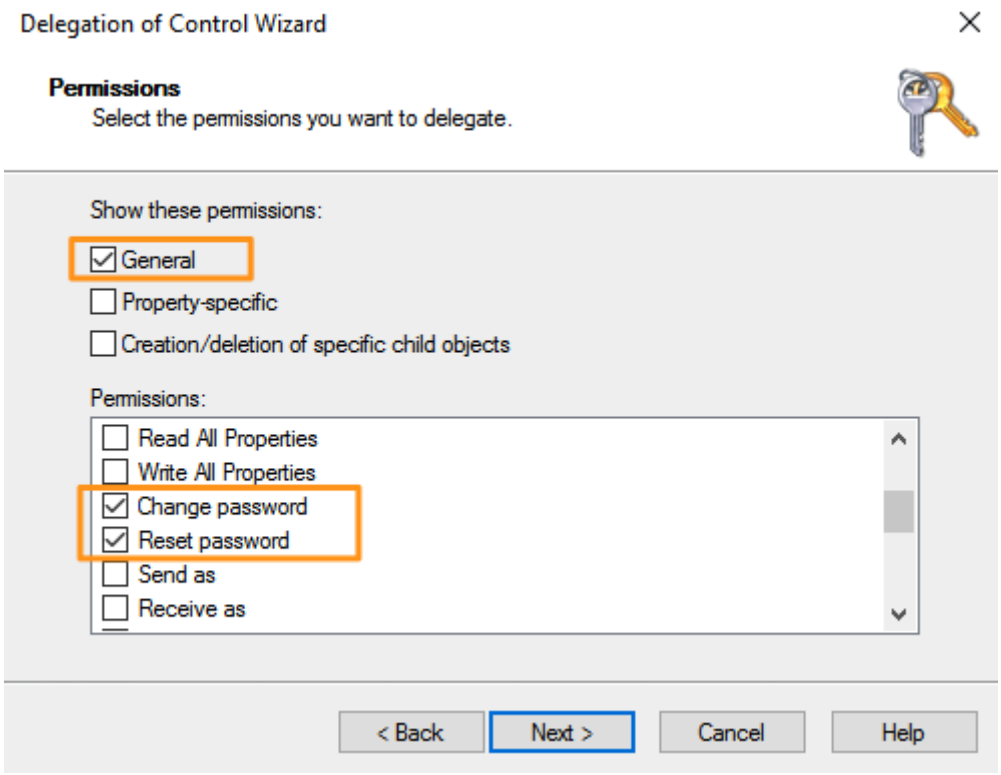


10. On the “Active Directory Object Type” page, select “Only the following objects in this folder” and check “Computer objects.” Then, check “Create selected objects in this folder” and “Delete selected objects in this folder” as shown below.



> The "Delete selected objects in this folder" checkbox **must be checked** in order for Frame to be able to [automatically clean up stale computer objects](ad-cleanup.md) from your domain.

11. On the “Permissions” page of the wizard, with the “General” toggle checked, select both “Change password” and “Reset password.” Complete the wizard by clicking “Next” and then “Finish.”



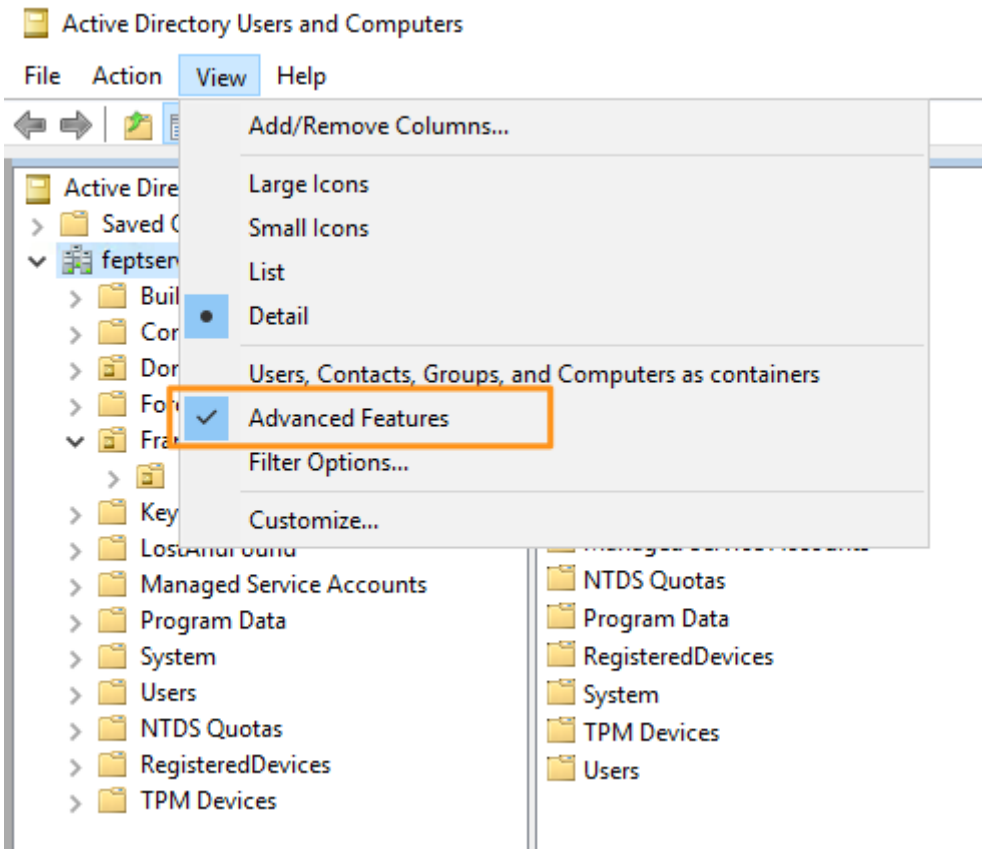
In some circumstances, you may wish to create separate Frame Service accounts for each OU for greater security, scalability, or convenience. This is also supported. To do so, create a Frame service account for each OU and delegate the same permissions as above.

> We recommend setting Loopback Processing Mode on the Frame OU to 'Replace' to help ensure unnecessary and potentially conflicting GPOs (applied to users) are not applied inadvertently. Since your organization may have specific security lockdowns and GPOs, you will need to work with our Support or Solutions Architect teams to ensure that these GPOs do no cause adverse effects to the Frame environment.

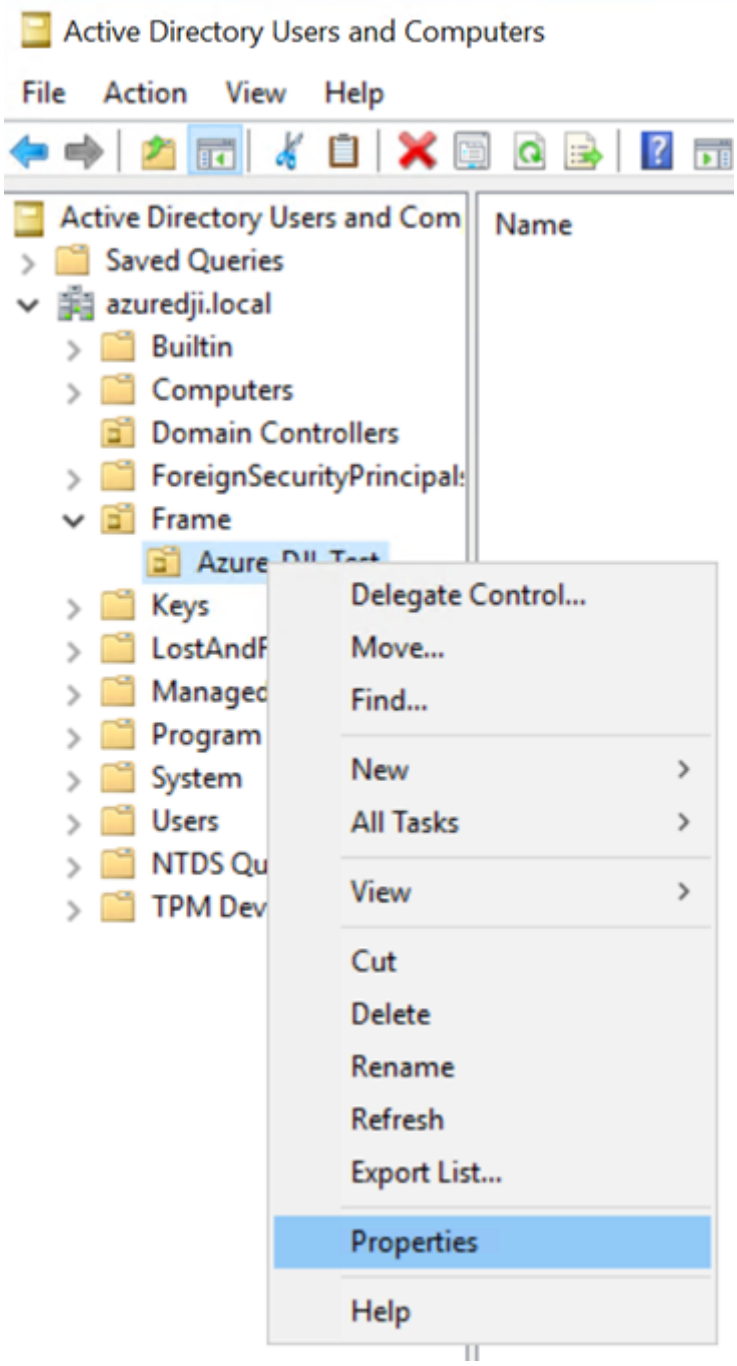
Obtain OU Details

Now we will obtain the necessary OU information needed to integrate with Frame. You will be entering this information into your Dashboard in later steps.

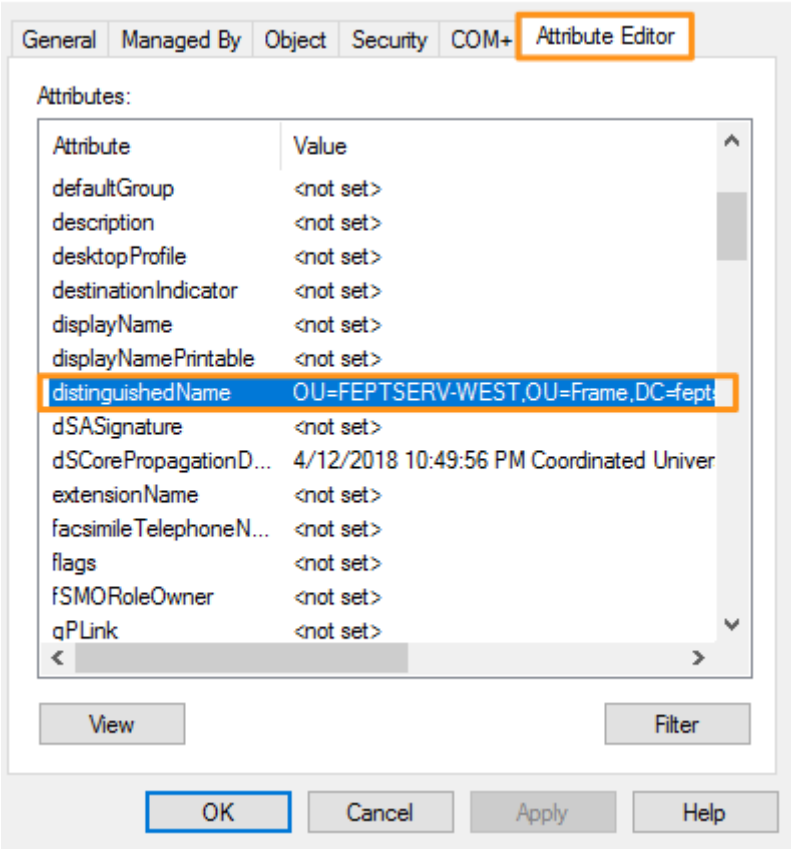
12. In your “Active Directory Users and Computers” console, make sure that “Advanced Features” is checked as shown below. This will enable us to easily retrieve the needed information.



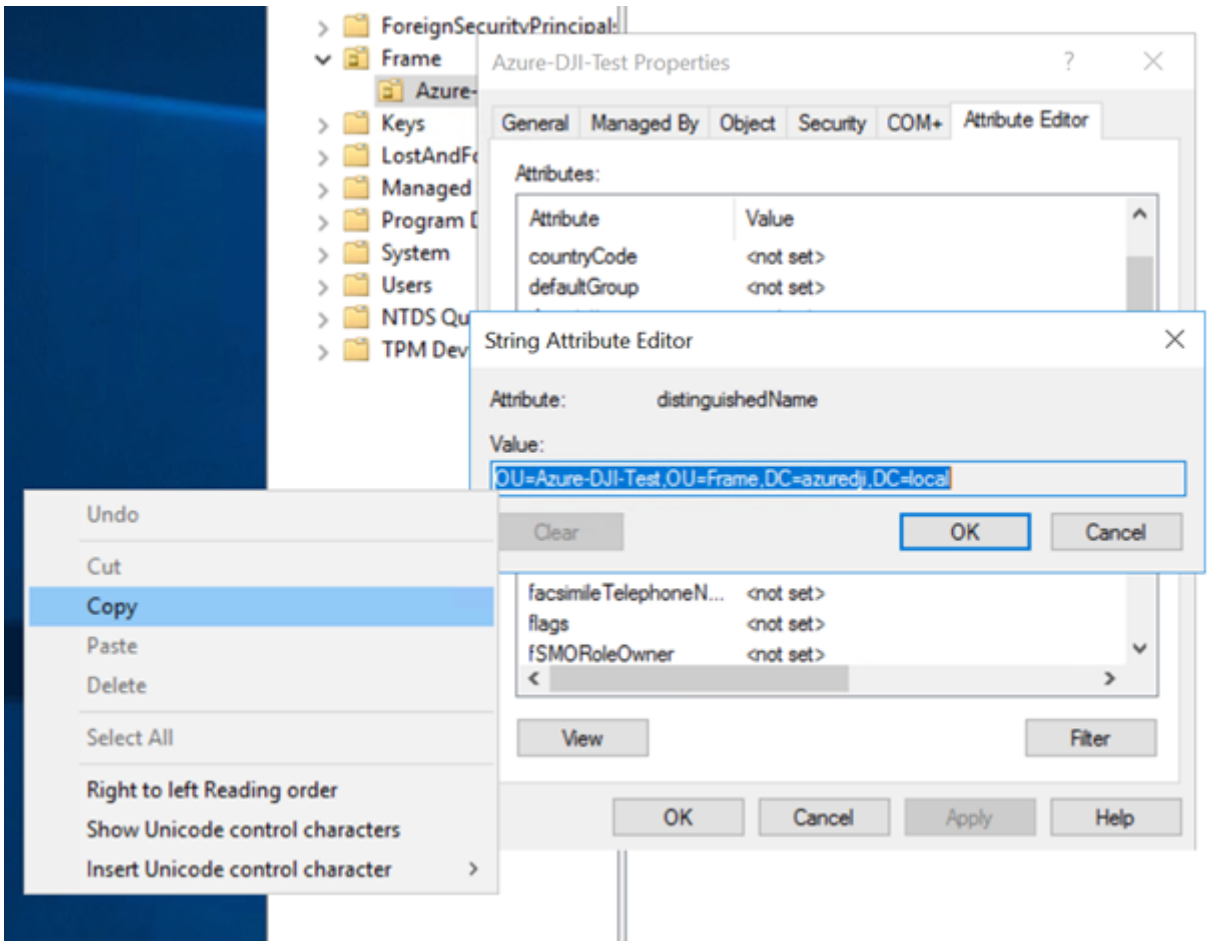
13. Next, right-click on the OU and select “Properties.”



14. Under the “Attribute Editor” tab, double-click “distinguishedName.”



15. Copy this attribute's value to your clipboard and have it ready, as we will need it in order to add your Frame account to your domain in the next guide.



Note

Additional Networking, Firewall, and Routing ConsiderationsAs mentioned at the start of this guide, you will need to ensure that all applicable Active Directory ports and protocols are open along this new network path. More information can be found in Microsoft's official documentation.

Revision #3
Created 1 October 2025 04:51:22
Updated 17 December 2025 15:51:27 by Dominik Conrad