Delegate Access to BitLocker Recovery Keys in Active Directory

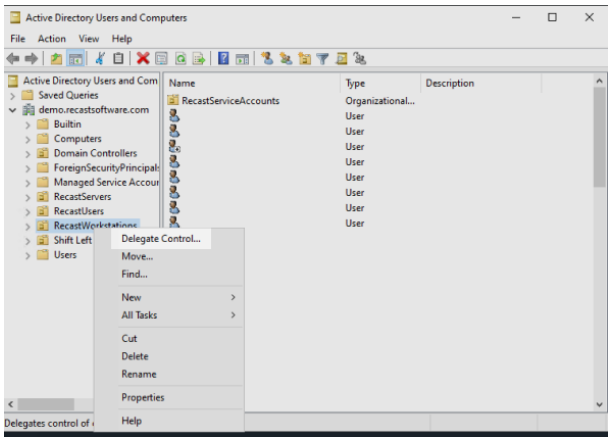
Last Modified on 10.13.23

With Active Directory Domain Services (AD DS), you can use organizational units (OUs) to delegate the administration of objects, such as users or computers, to an individual or group. This approach lets you grant control over tasks at a granular level without modifying the default control given to administrators. In this case, you can give a group of users permission to view BitLocker recovery keys stored in a designated organizational unit in Active Directory.

Before you delegate control, you must have or create an OU and security group to designate.

To delegate access to BitLocker recovery keys:

1. On the Server Manager dashboard, navigate to **AD DS** > **Active Directory Users and Computers**.
2. Right click on the designated organizational unit (OU) and click **Delegate Control**.



3. In the Delegation of Control Wizard, under Users or Groups, click **Add**.
4. Select or add the group being given access to view BitLocker recovery keys and click **OK**.
5. Under Tasks to Delegate, select **Create a custom task to delegate**.
6. Under Active Directory Object Type, select **msFVE-RecoveryInformation objects**.
7. Under Permissions, select **Full Control**.