BitLocker-to-go Key Recovery

Introduction

This guide provides one of two key recovery options that can be used to unlock BitLocker encrypted USB drives. The approach discussed here leverages the firm’s PKI infrastructure and makes use of one or more Data Recovery Agent (DRA) certificates.

Key Finding

1. You must import the DRA certificate with its private key into the **local Current User Personal Certificates store** where you are performing the unlock operation. You should then delete the certificate after the USB drive has been unlocked (see p.21 for usage)
2. Unlikely the Active Directory Key Recovery option, you are not forced to re-format and then re-enable BitLocker-to-go after the USB drive has been unlocked
3. Found that I was able to implement both the Active Directory and PKI Certificate DRA options without any adverse effects

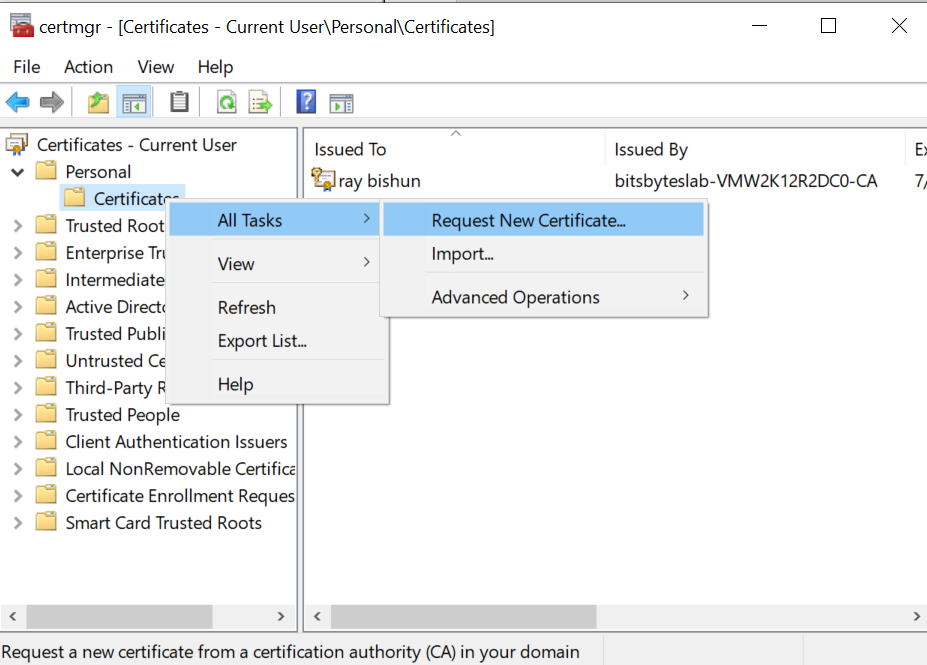
Overview

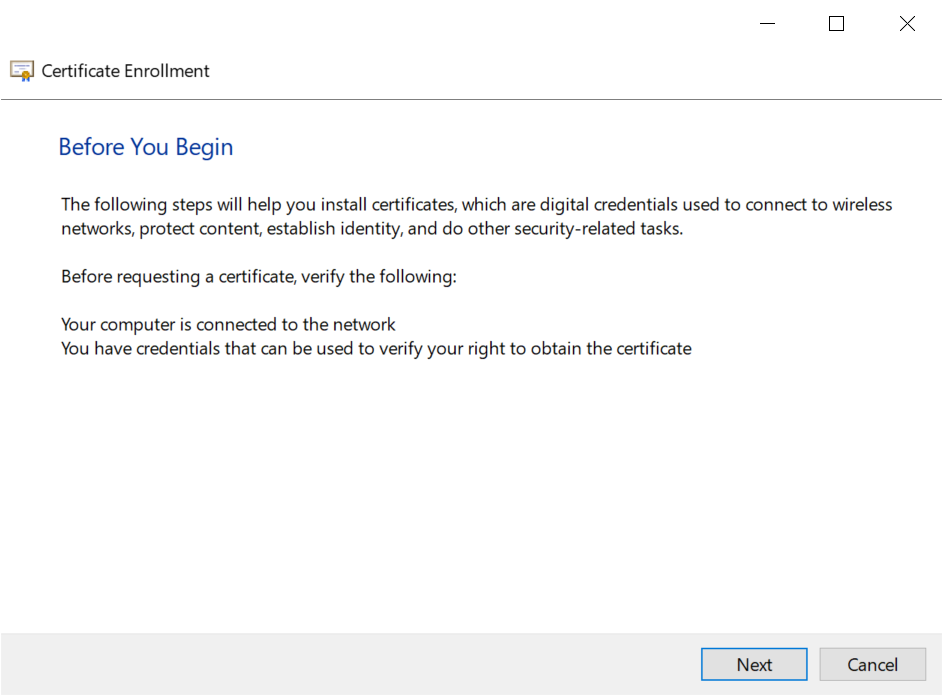
1. Request the DRA certificate
2. Export the DRA certificate
3. Add the DRA certificate to your Group Policy
4. Configure BitLocker Identification
5. Test the Data Recovery Agent

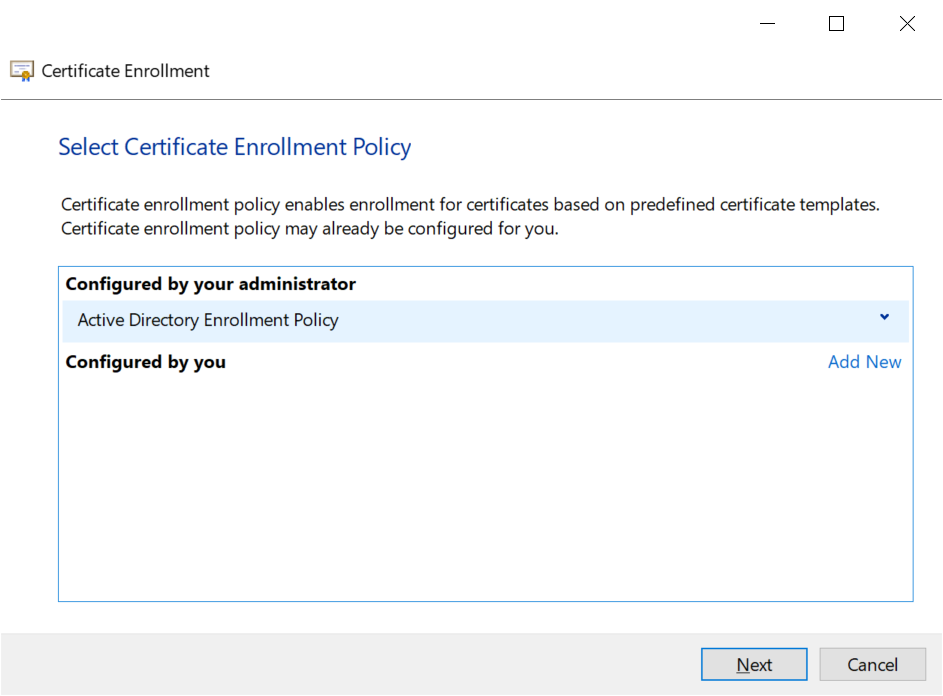
Walkthrough

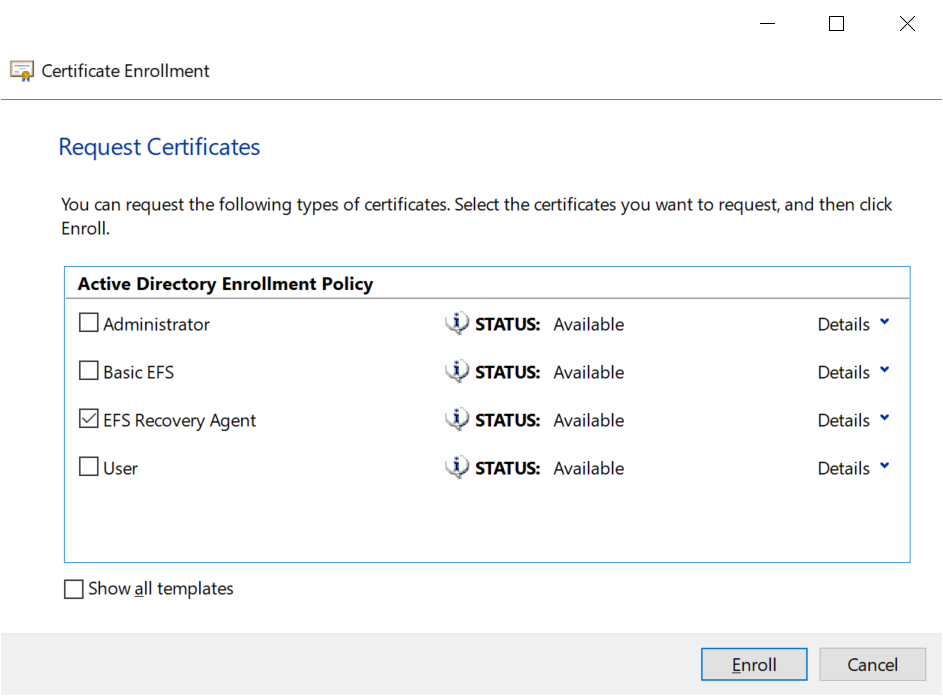
Request the DRA Certificate

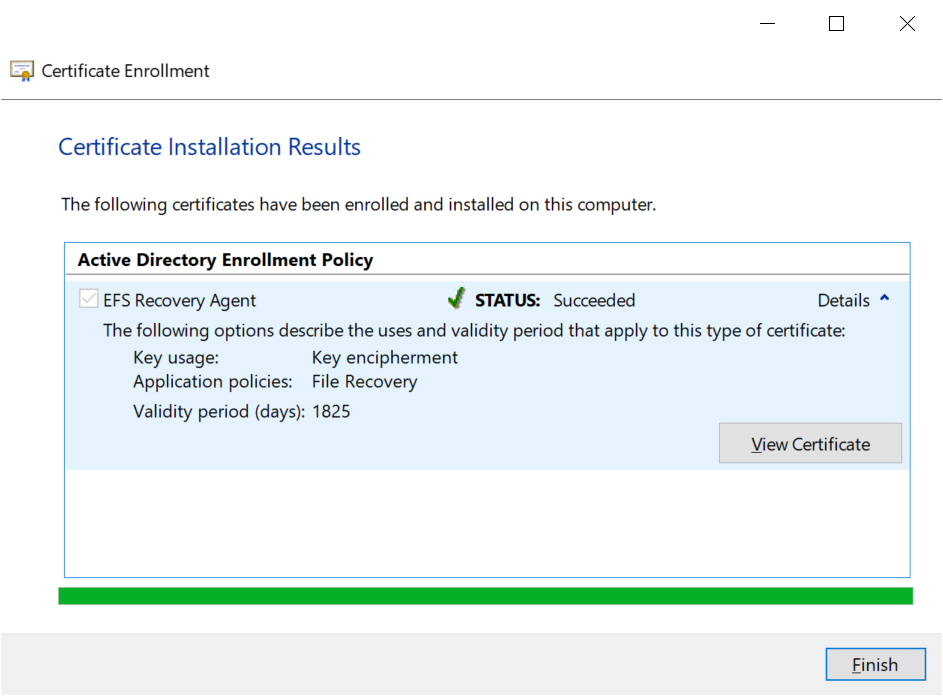
1. certmgr.msc

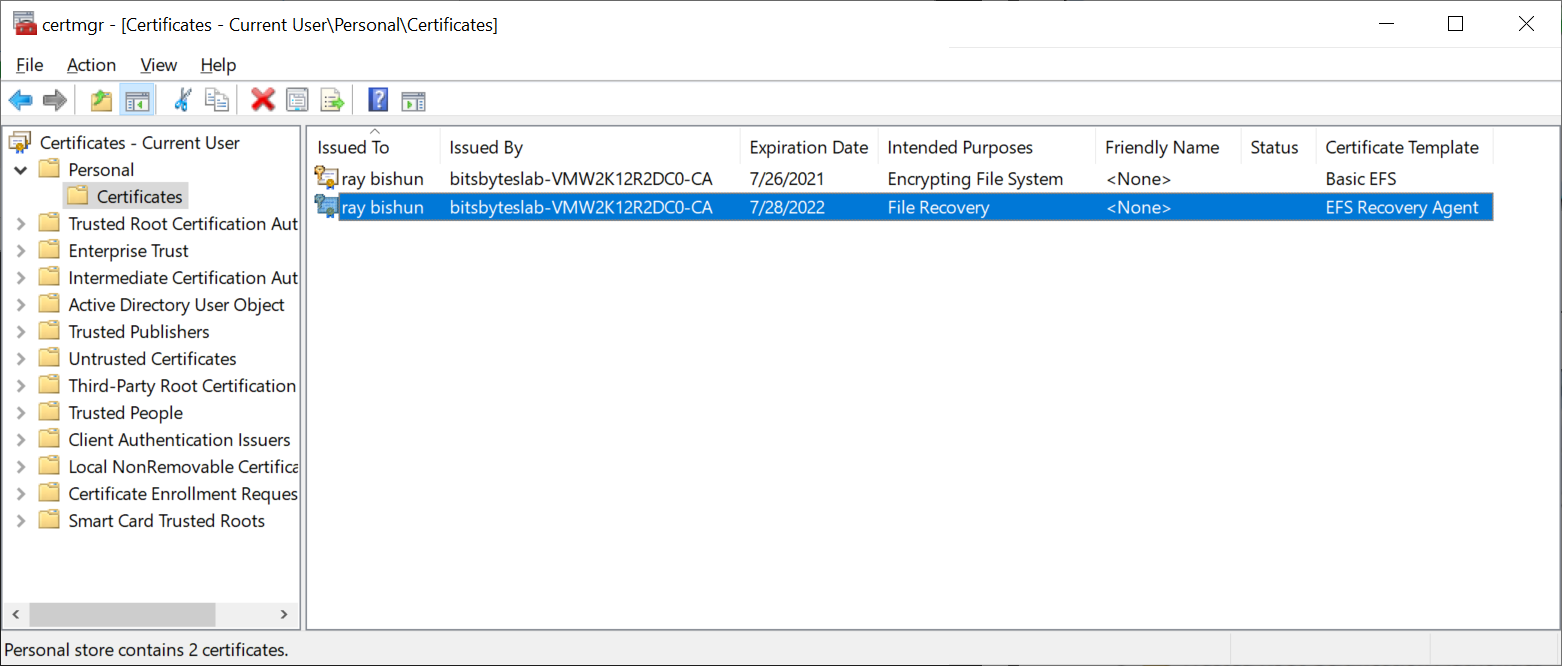




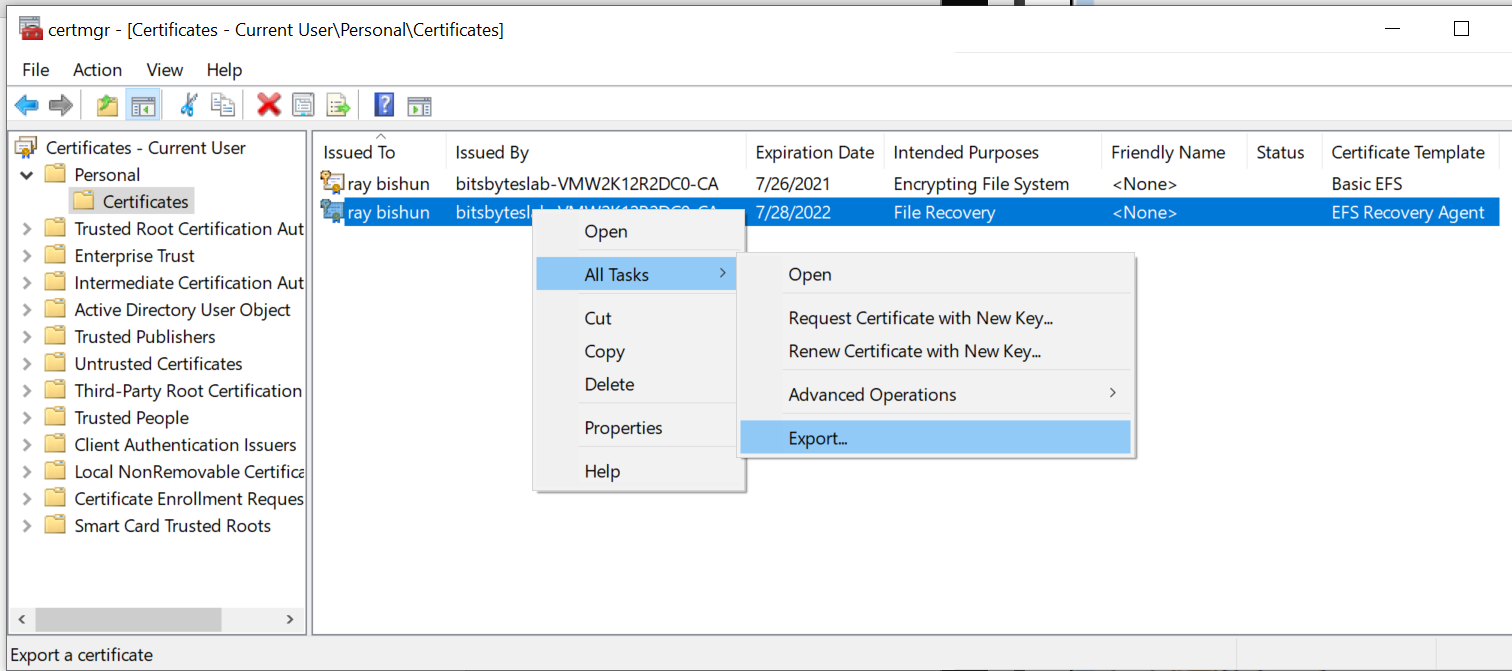


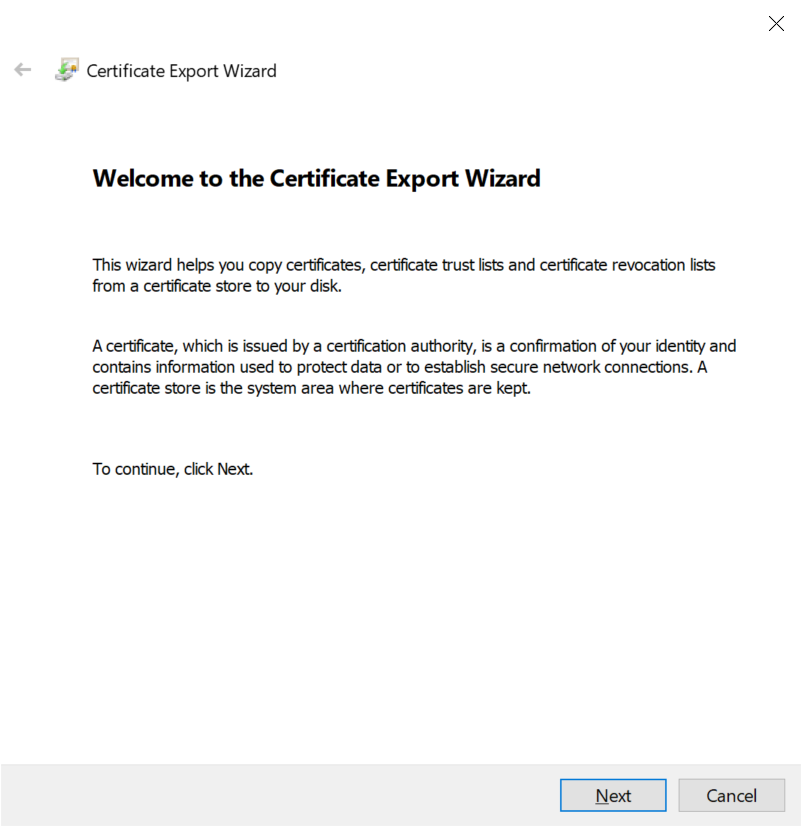


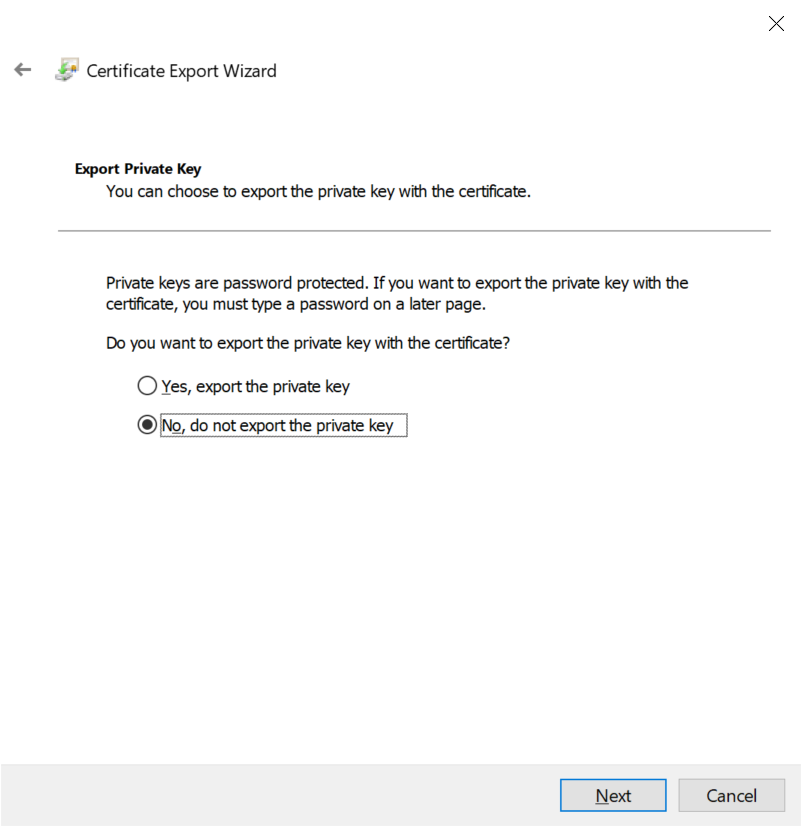


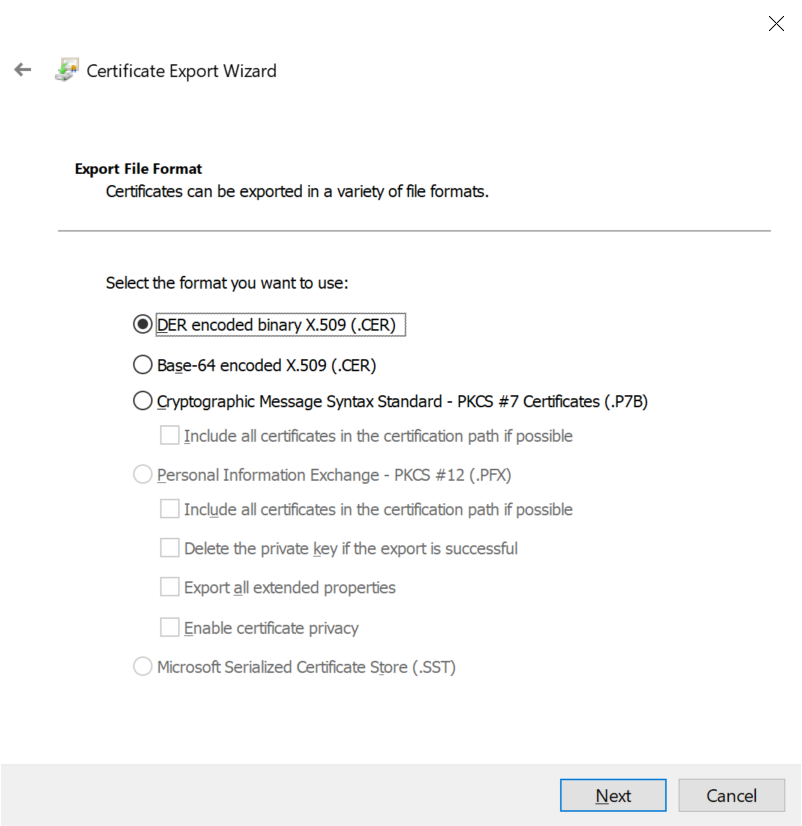


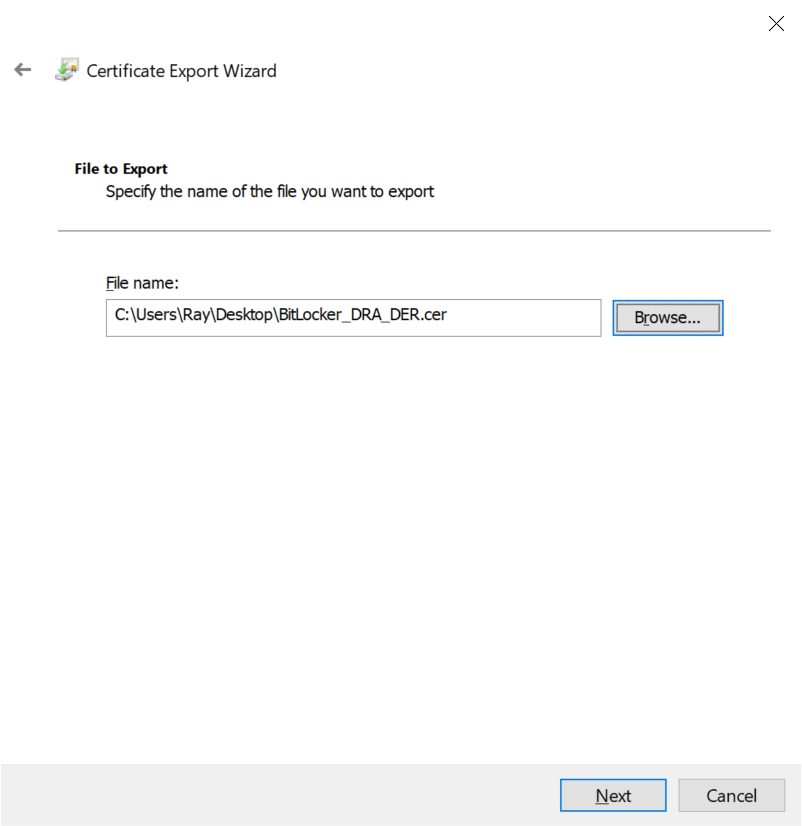
Export the DRA Certificate

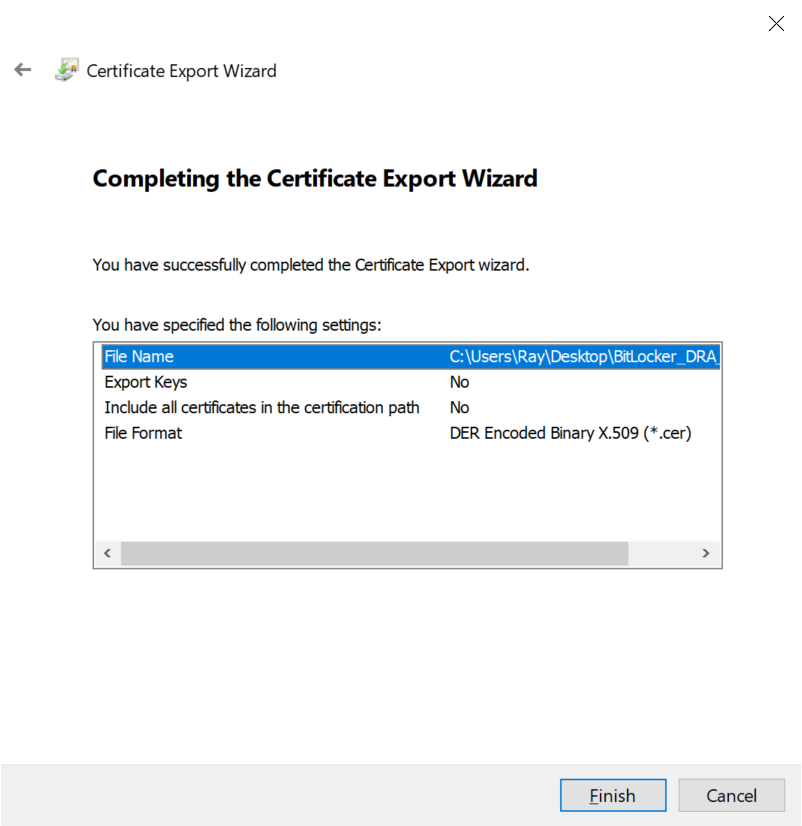


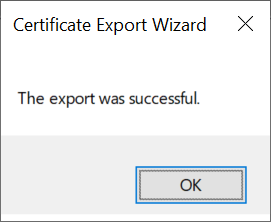






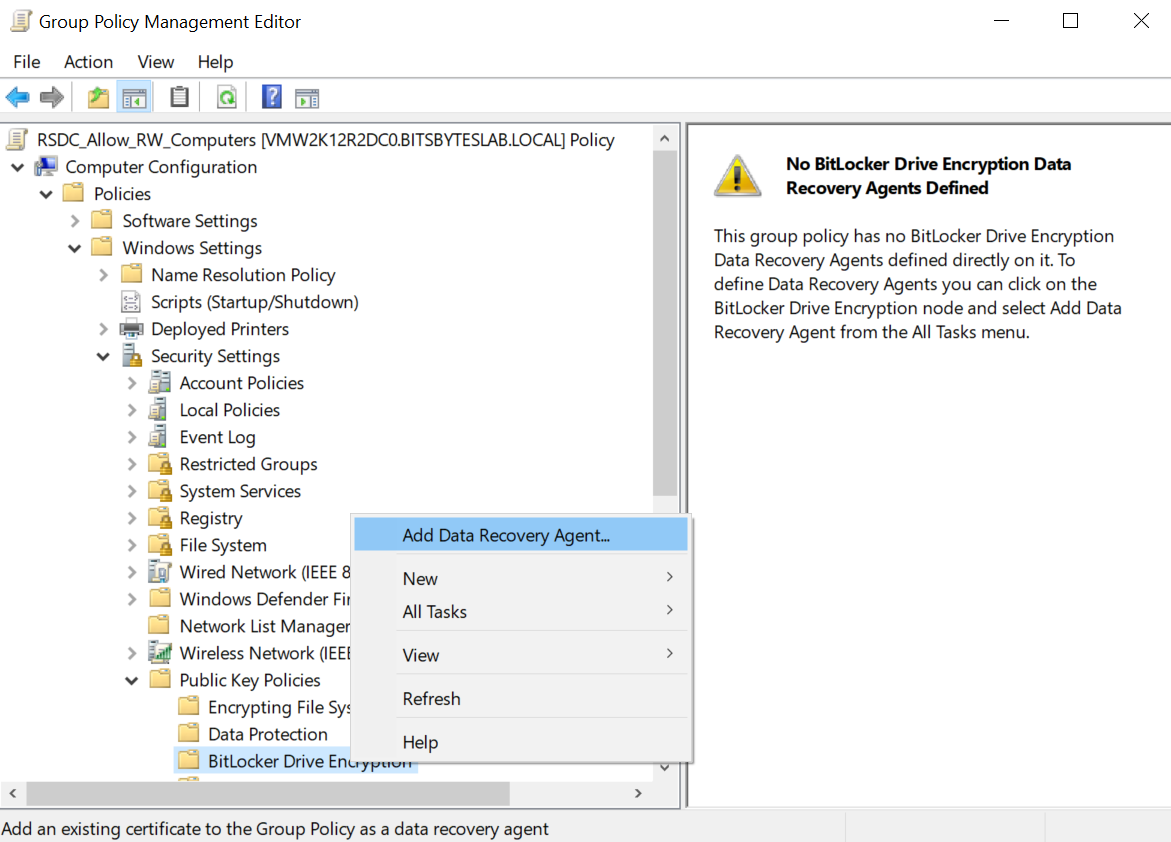




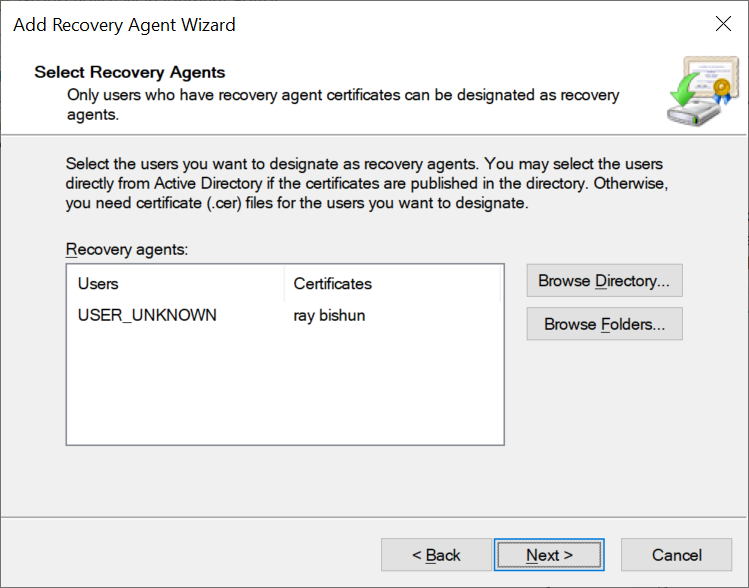


Add the DRA certificate to your Group Policy

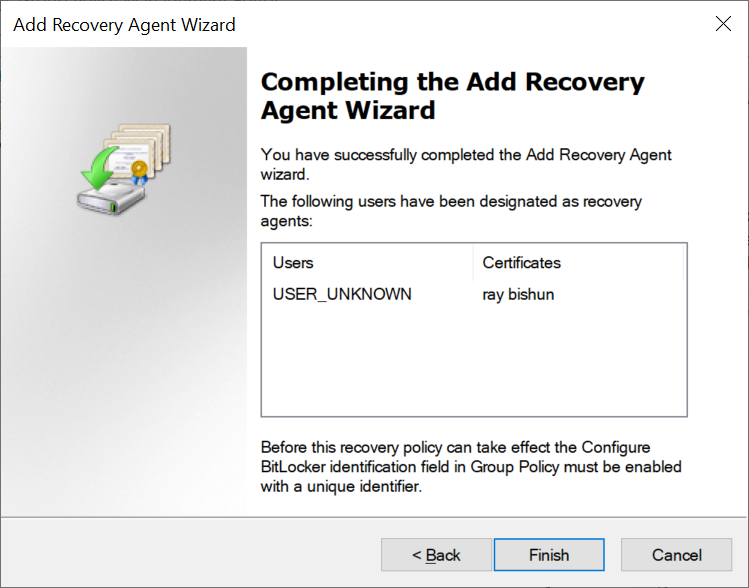
1. gpmc.msc
2. Navigate to the OU where the RSDC\_Allow\_RW\_Computers Group Policy is linked
3. Right-click the RSDC\_Allow\_RW\_Computers Group Policy and select **Edit**
4. Computer Configuration
5. Windows Settings
6. Security Settings
7. Public Key Policies
8. Right-click BitLocker Drive Encryption and select **Add Data Recovery Agent**
9. And proceed as shown below

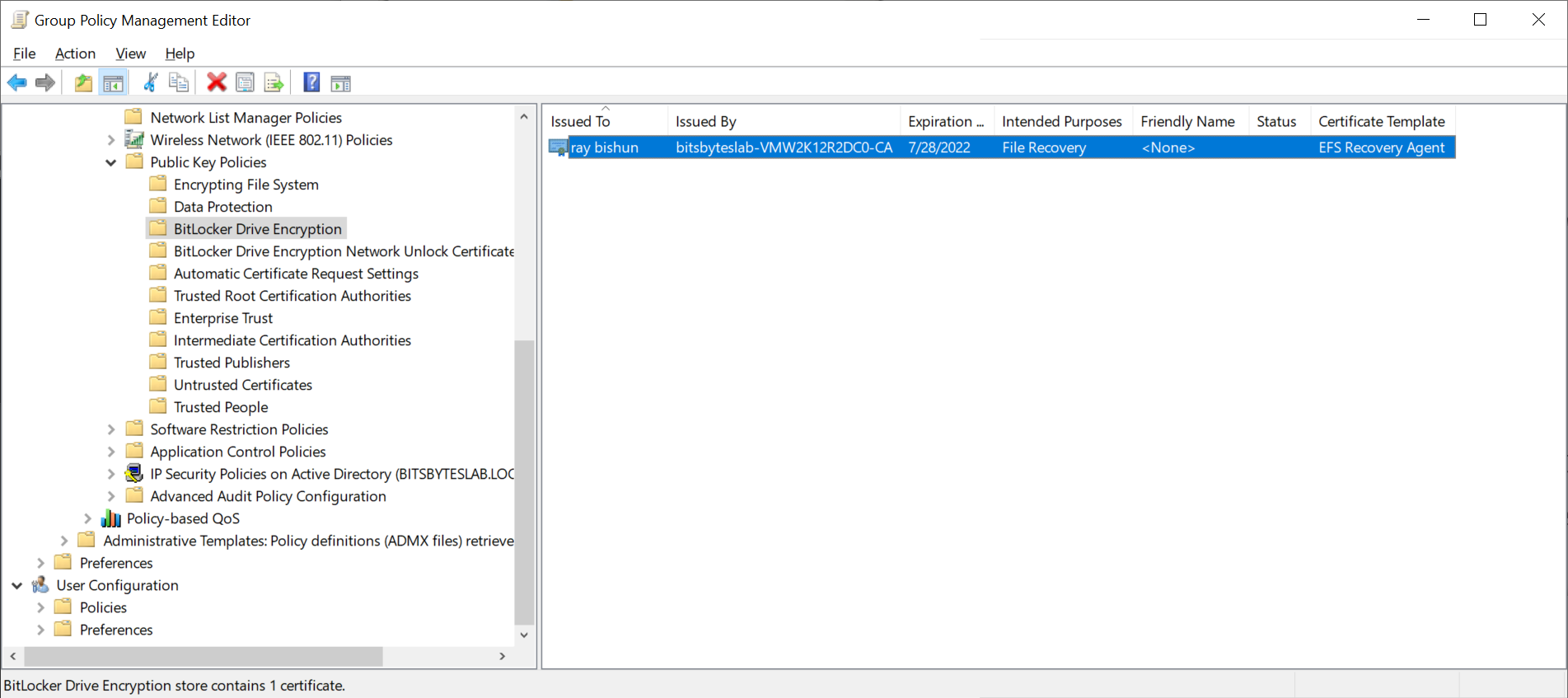






**NOTE**: You should repeat this process to add multiple Data Recovery Agents.

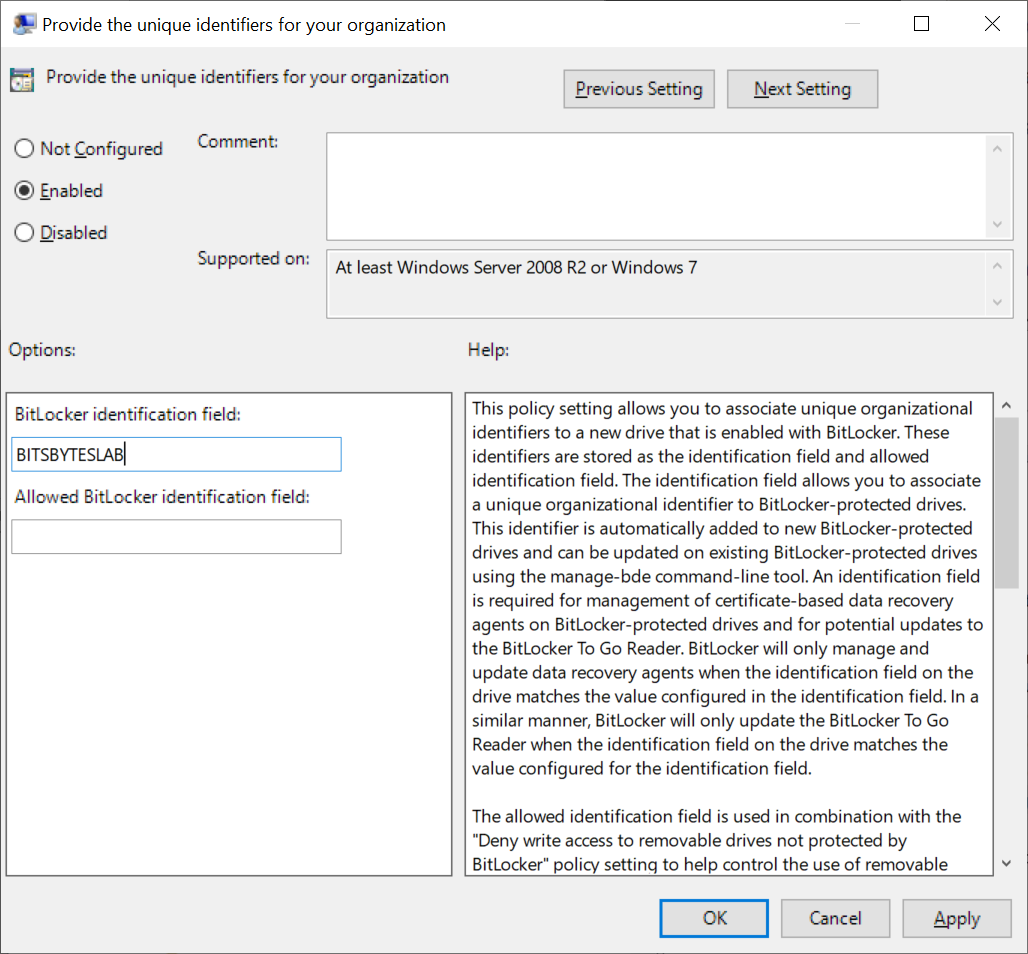




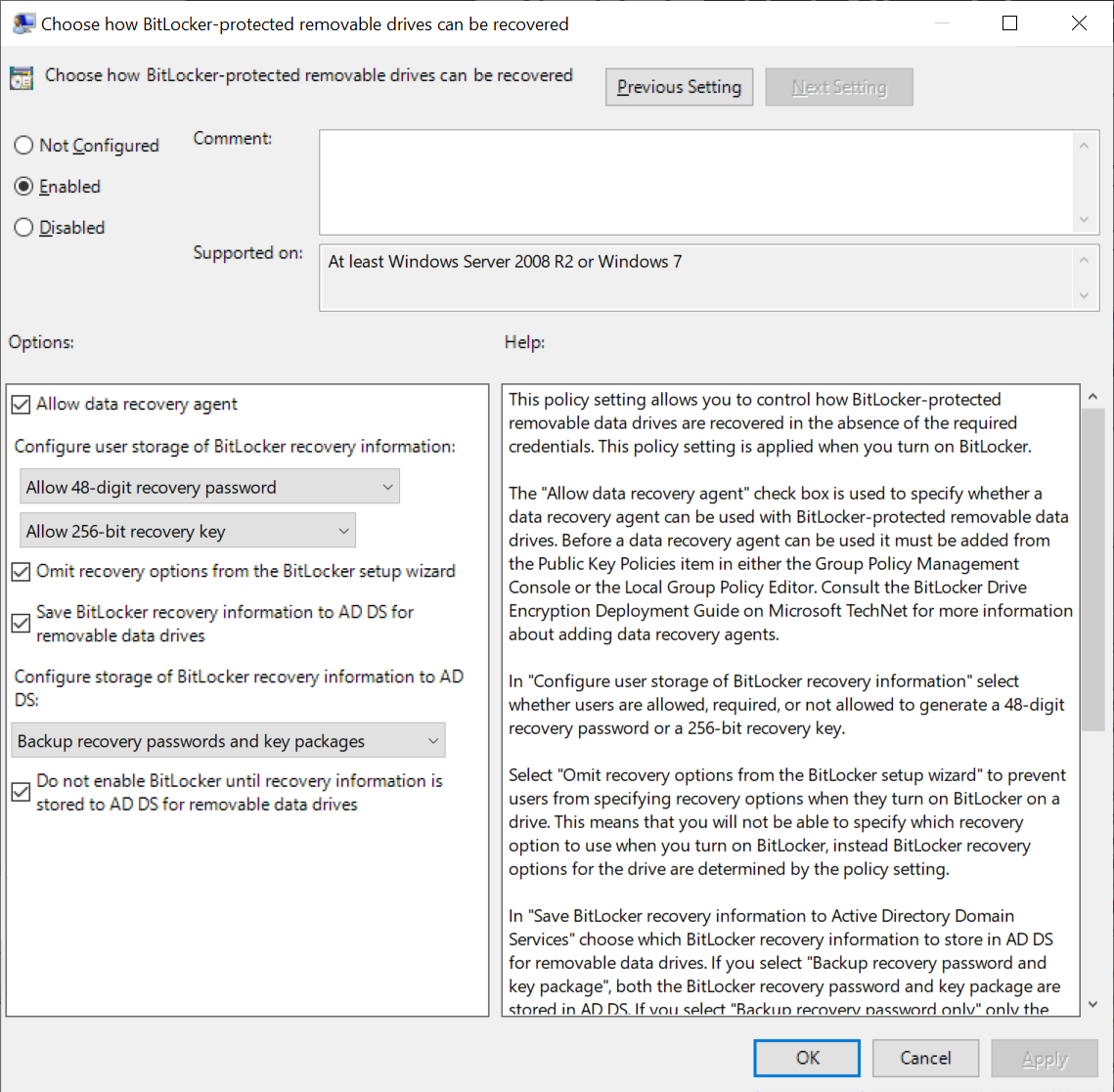
Configure BitLocker Identification

Perform the following steps within the same Group Policy used in this doc, RSDC\_Allow\_RW\_Computers

1. Computer Configuration
2. Administrative Templates
3. Windows Components
4. BitLocker Drive Encryption
5. Provide the unique identifiers for your organization as shown below



1. Removable Data Drives
2. Choose how BitLocker-protected removable drives can be recovered
3. Enable
4. Check **Allow data recovery agent**



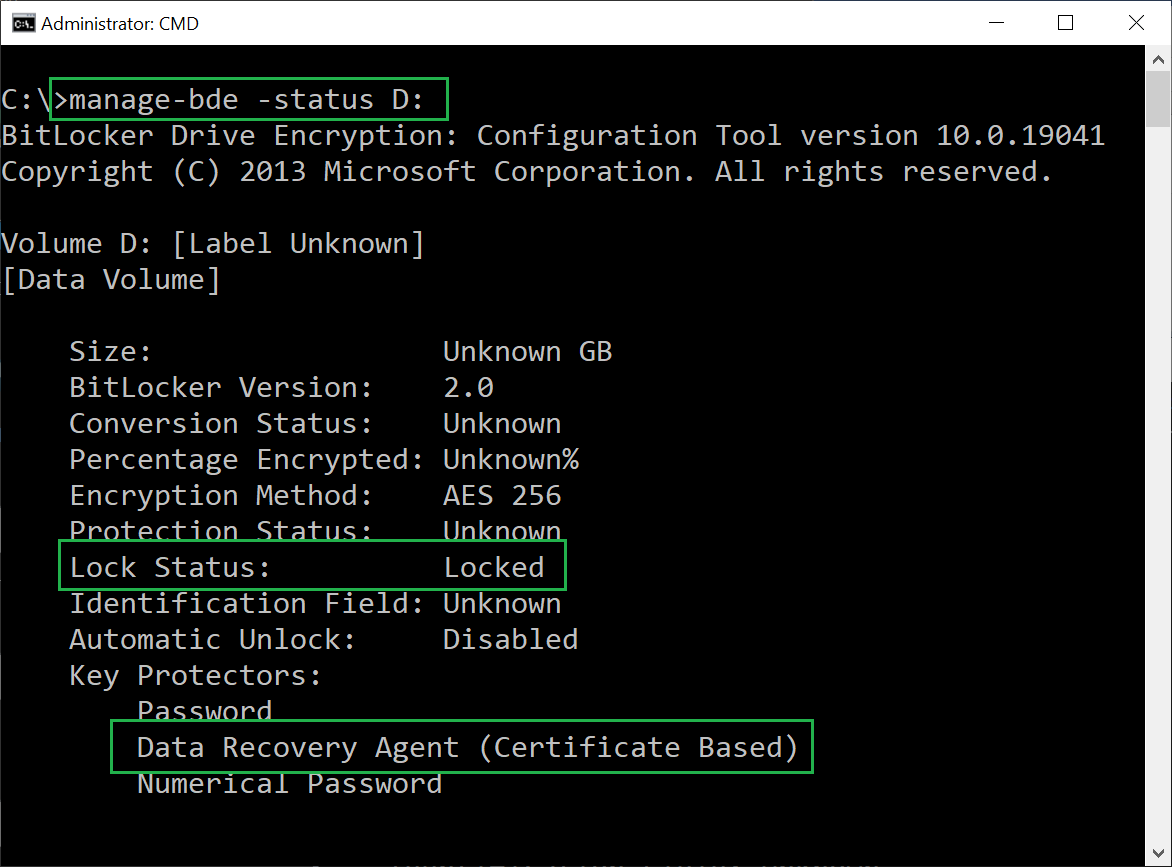
Test the Data Recovery Agent

Perform the following steps to unlock a BitLocker encrypted USB drive.

1. Login into a domain computer using your Active Directory credentials
2. Insert, encrypt and password protect a USB drive using BitLocker-to-go
3. Remove and re-insert the USB drive, but do not unlock the drive
4. Launch a CMD prompt using the **Run as administrator** option, and run:

manage-bde -status D:

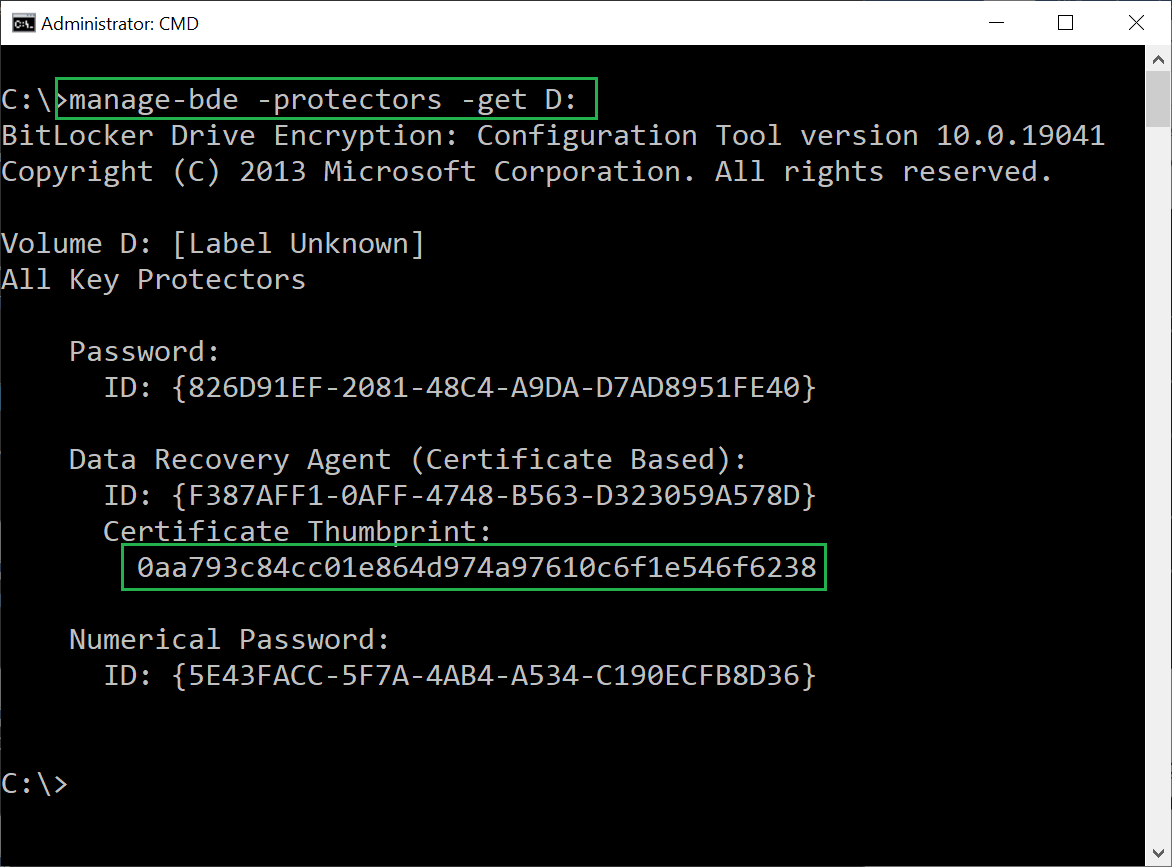
1. Verify that **Data Recovery Agent (Certificate Based)** appears under **Key Protectors**



1. View and copy the **Certificate Thumbprint**:

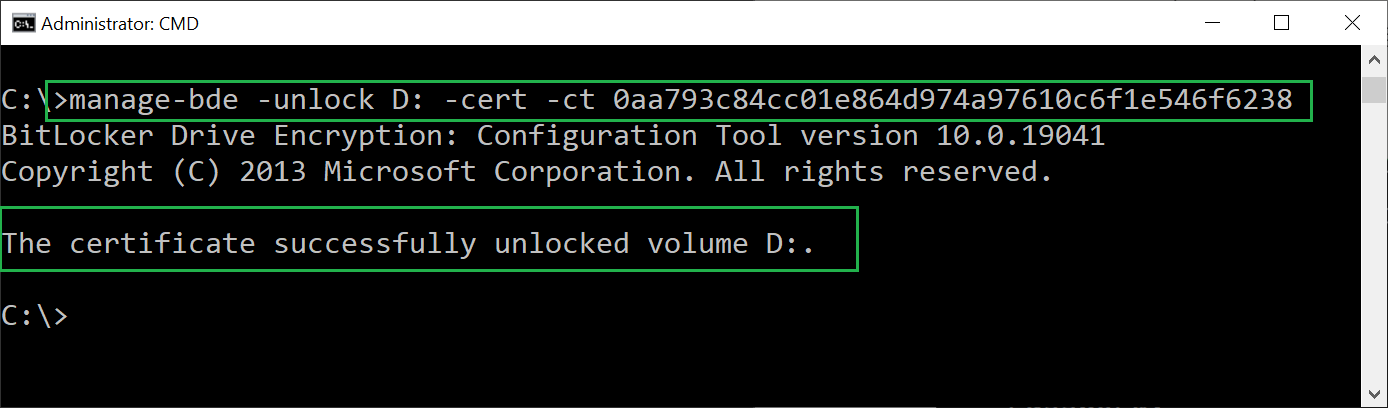
manage-bde -protectors -get D:

1. Tip: in the CMD window, right-click, Mark and select the **Certificate Thumbprint** to copy it to the clipboard



1. NOTE:
   1. You must import the DRA certificate with its private key into the **local Current User Personal Certificates store** where you are performing the unlock operation
   2. You should then delete the certificate after the USB drive has been unlocked
2. Unlock the drive

manage-bde -unlock D: -cert -ct 0aa793c84cc01e864d974a97610c6f1e546f6238



1. manage-bde -status D:

