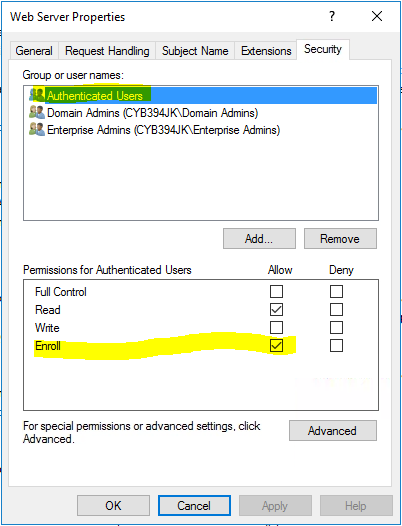
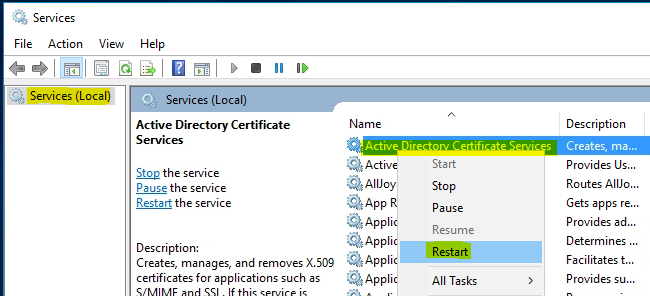
# CYB394 – Lab 4 - Right Management Services

# Part 1 Installing AD RMS

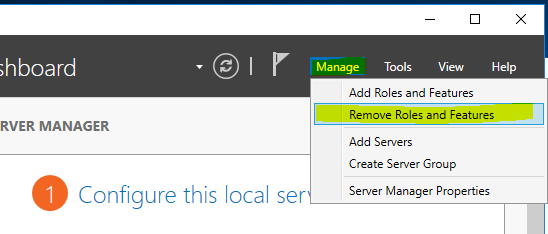
Start SRV1, SRV2, SRV3, & CLIENT1

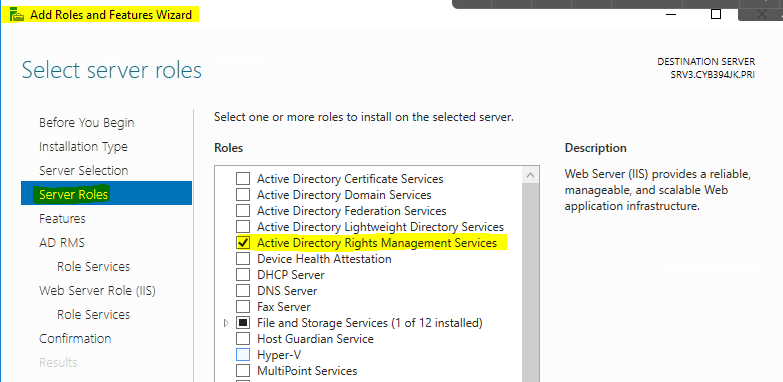
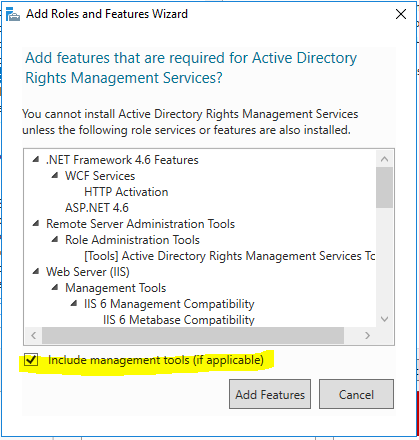
In the first steps we’ll set the SRV2 Certificate Authority to allow enrollment of the Web Server template for Authenticated users. This way it will be available when we need the certificate during the RMS installation.

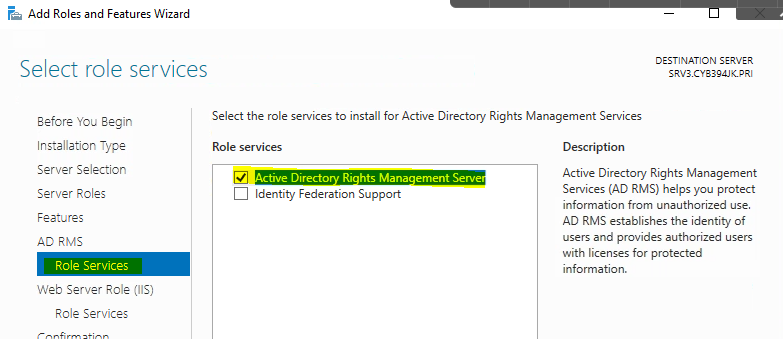
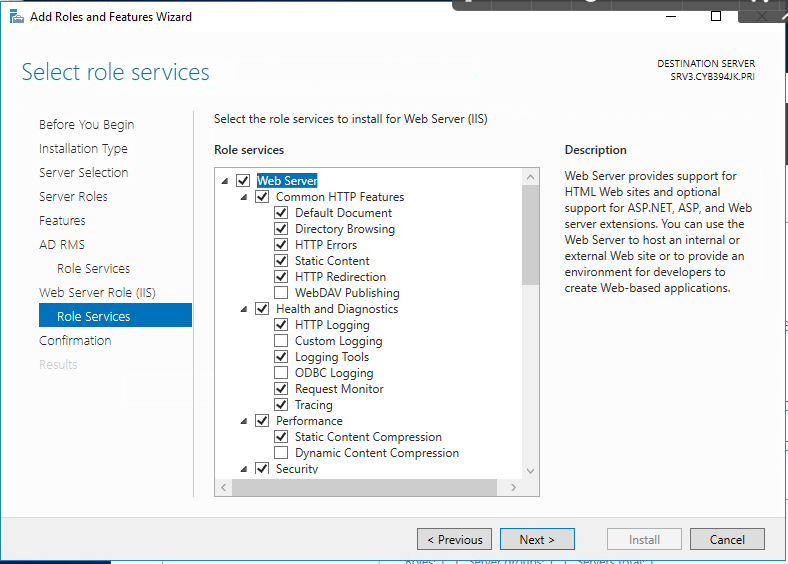
1. **SRV2** -> Server Manager -> Certificate Authority -> Certificate Templates <- Right-click -> Manage -> Web Server -> Properties -> Security -> Authenticated Users -> Enroll -> [OK] -> Close Certificate Authority console windows.  
   
2. Restart the Active Directory Certificate Services service  
   

Now let’s get SRV3 ready for the RMS installation. This first requires that we Remove the IIS web service which will be reinstalled ~~with a modified configuration~~ during the RMS role install.

\*\* Pay Attention to which machines you’re signed into.\*\*

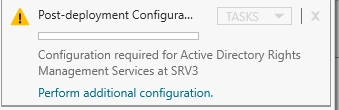
1. **SRV3** sign in with PDAA (Password16) -> Server Manager -> Manage menu (next to Tools menu) -> Remove Roles and Features  
   
2. **Remove the Web Server ISS Role.**
3. **Reboot SRV3** when uninstall is done.
4. SRV3 -> **Delete the [C:\inetpub]** folder
5. SRV3 -> Server Manager -> **Add Roles and Features**
6. Click Next until you are on the Select Server Roles Page
7. Check the **Active Directory Rights Management Services** box and click Next (see screenshot). If prompted to Add Features that are required... review the role services that must be installed for AD RMS to work and **ensure Include management tools** is checked. Click Add Features to return to the Role Services page and click Next.

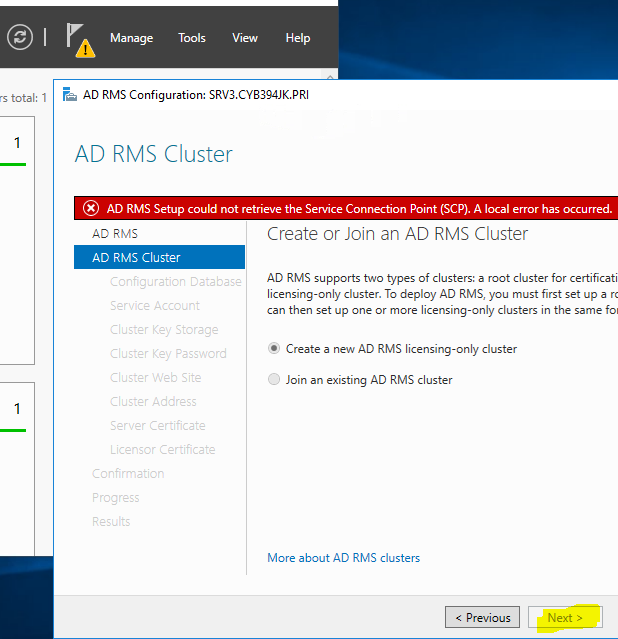
  
  


1. Click Under Role Services make sure that Active Directory Rights Management Server is checked.  
     
     
   Keep Defaults -> [Next]  
   
2. Click next then **[Install]**
3. Once Install is complete you can close the wizard.
4. **Restart SRV3 before continuing.**

# Part 2 Configure RMS

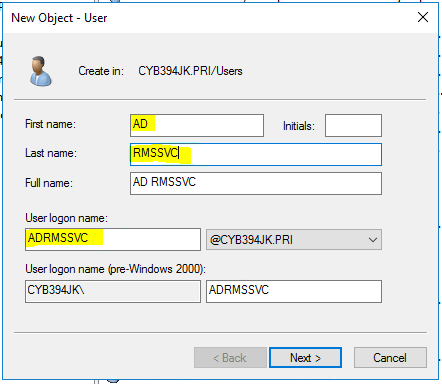
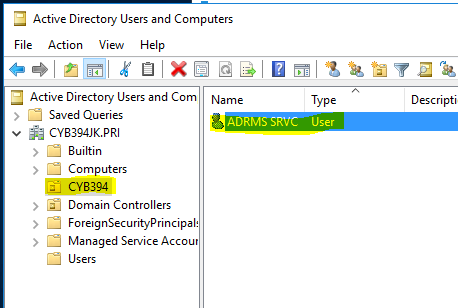
1. **SRV3** -> Server Manager -> Click on the  in server manager
2. Then click **Perform additional configuration**



1. Read the intro screen then click [Next]
2. If you receive the error below, Reboot SRV3 Again  
   
3. Select (\*) **Create a new AD RMS Root Cluster** click [Next]
4. Choose **Use Windows Internal Database on this server** click [Next] -> Proceed to step 7 to create the domain user for the RMS service account.

**We can leave the RMS configuration for a moment to create the Service Account need by RMS.**

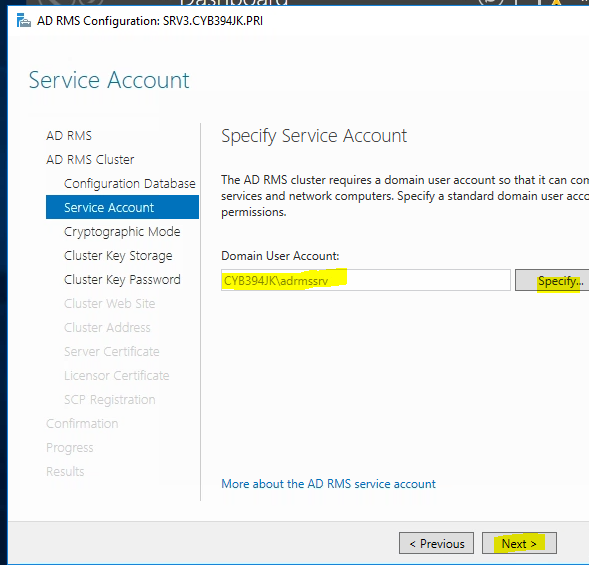
1. **Sign-In to SRV1** -> Server Manager -> Tools -> Active Directory Users and Computers (ADUC)
2. \*\*Create a **new user account inside of the \*\*CYB394 OU\*\*** the user logon name will be ADRMSSVC. With a password of **Password16** and make sure to set the **password to never expire**

That’s it. Done on SRV1.

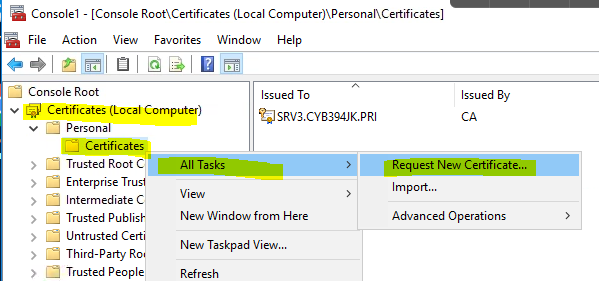
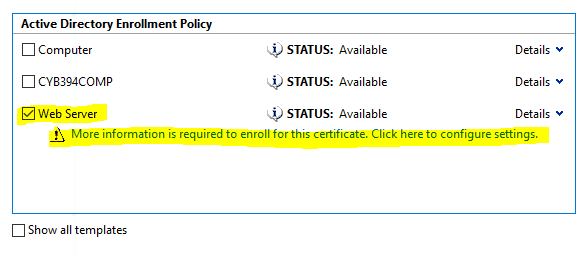
Move Back -> **SRV3** and resuming the RMS configuration, Specify Service Account page.

1. Click Specify and Enter the Domain user (ADRMSSVC) account you just created. Then Click Next



1. Read the Specify Cryptographic Mode description. Then Choose **Cryptographic Mode 2** then click [Next]
2. Choose **Use AD RMS centrally managed key storage.**
3. Under Specify AD RMS Cluster Key Password Type **Password16**
4. Keep **Default Web Site** for the virtual directory
5. Connection Type: (\*) Use an SSL-encrypted connection (https) and in the cluster address type <HTTPS://ADSRMS.CYB394XX.PRI>

Once again, we’re going to leave the RMS configuration to generate a new certificate **Request** for RMS to use. (You did this in the last lab)

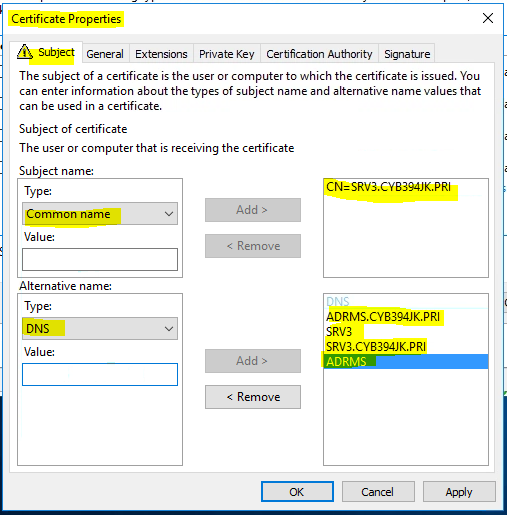
1. **SRV3 -> MMC.EXE** -> File -> Add/Remove Snap-in -> **Certificates** -> [Add] -> **Computer account** -> [Next] -> Local computer -> [Finish] -> [OK].
2. Drill into Personal -> Certificates <-Right-Click -> Request New Certificate ->   
    [Next] -> (**If you receive a Time Sync error at this step, reboot SRV3 again**) -> [Next] -> click **More information is required to enroll for this certificate. Click here to configure settings.**
3. From the [**Subject**] tab, set the Subject Name: Type -> **Common Name** -> SRV3.CYB394XX.PRI  
   Alternative Name: Type -> **DNS** -> Add the following DNS names to the request.

ADRMS.CYB394XX.PRI

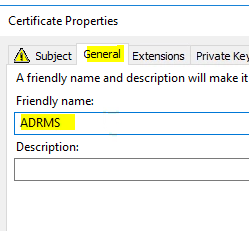
SRV3

SRV3.CYB394XX.PRI

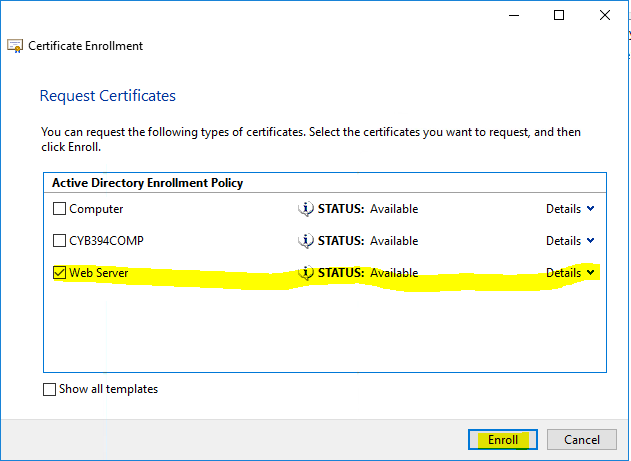
ADRMS



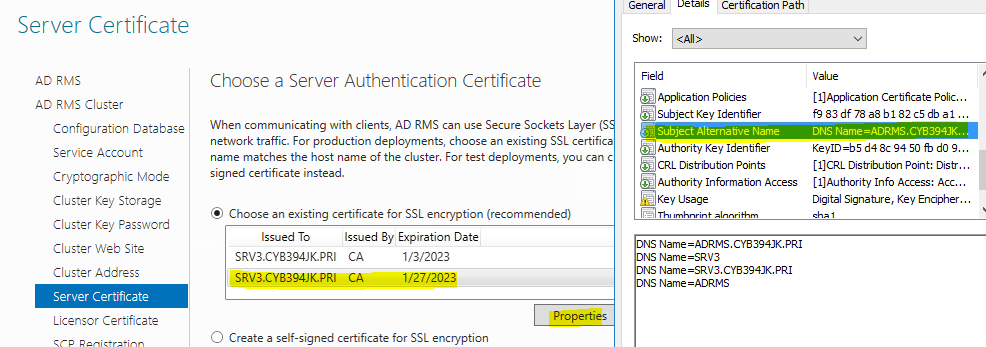
[General] Tab

Have the friendly name be ADRMS  


Click [OK] when done, then [Enroll] -> [Finish]

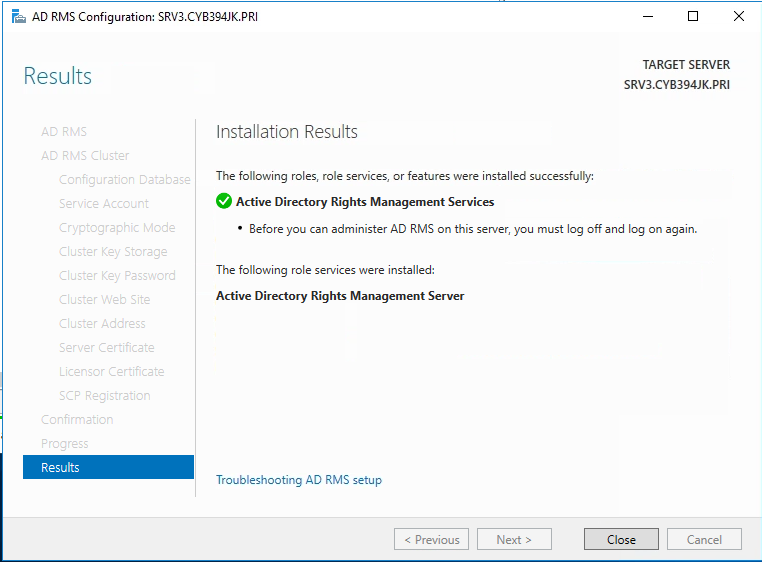


1. Once you have the certificate generated **go back to the RMS configuration page** and **Click the Refresh** Button on Choose an existing Certificate.
2. Verify you are selecting the correct certificate by clicking [**Properties**] then view the **Subject Alternative Name** in the Details Tab



1. Click [Next]
2. (\*) Register the SCP now

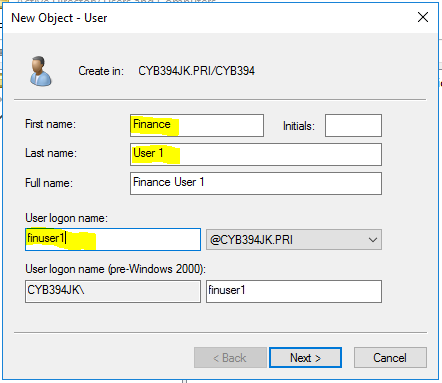
|  |
| --- |
| Screenshot of entire Confirmation page: |

1. Click [Install]  
   
2. **\*\* You MUST RESTART SRV3 NOW \*\***

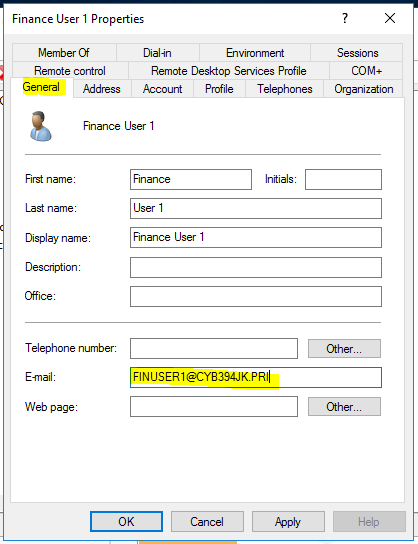
# Part 3 Creating some Users and Groups for RMS

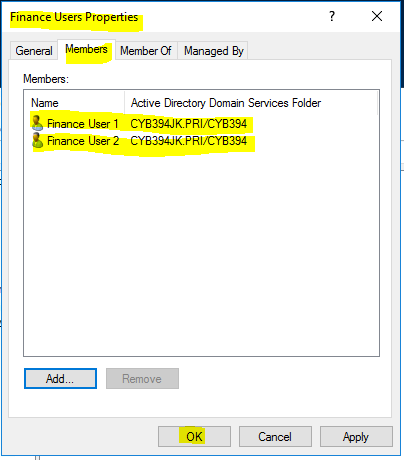
1. **\*\*SRV1** -> Server Manager -> Tools -> DNS
2. Create a CNAME for ADSRMS that points to SRV3.CYB394XX.PRI
3. SRV1 -> Server Manager -> Tools -> ADUC
4. Within the CYB394 OU -> Create a **Global** Security Group called **Finance Users**
5. Create two users Finance User1 and Finance User2 in the

User logon name is finuser1 and finuser2

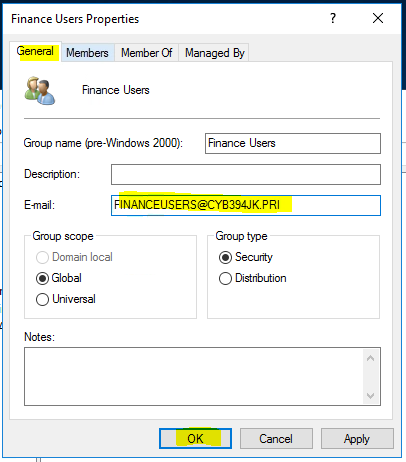


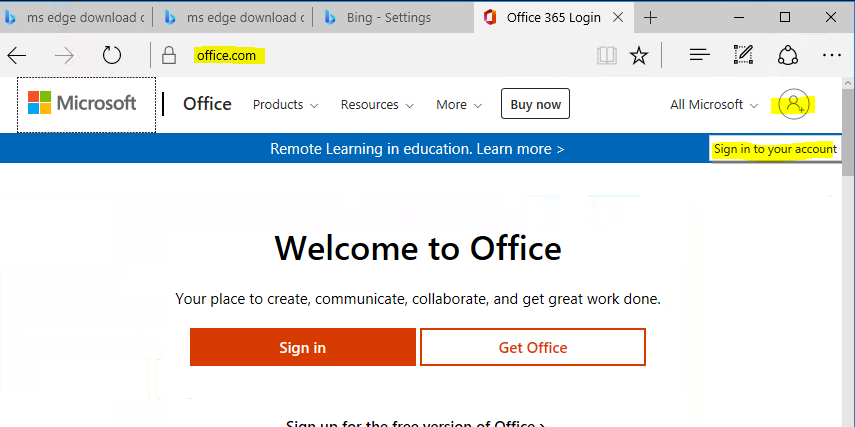
Set the password for each user to be **Password16** and **Password Never Expires**

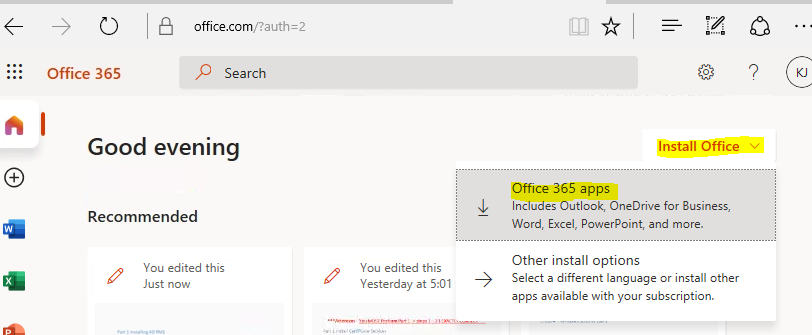
Give each user an email address in the AD properties ex. [FINUSER1@CYB394XX.PRI](mailto:FINUSER1@CYB394XX.PRI)  


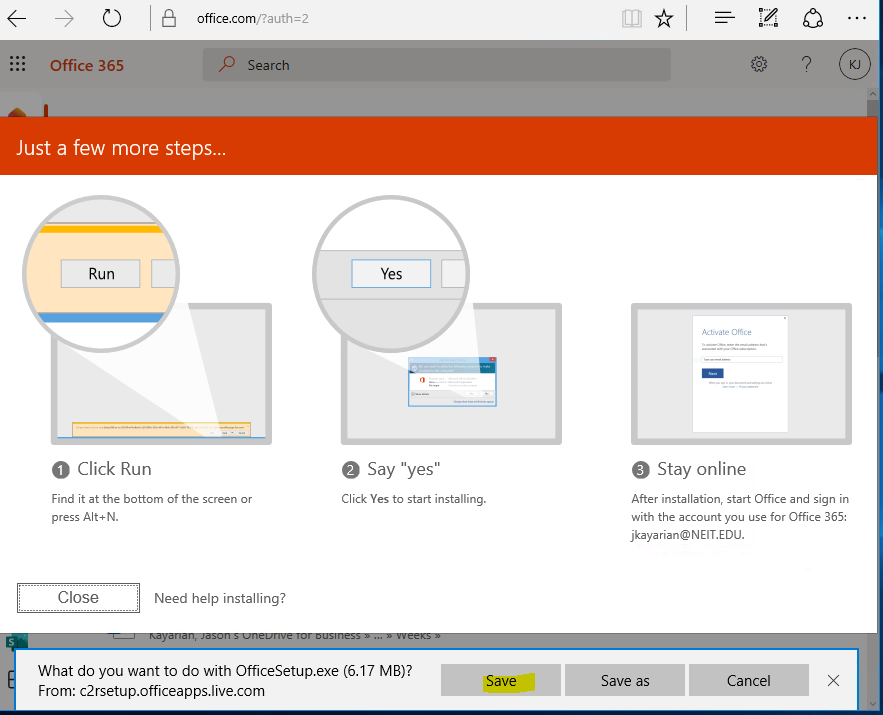
**Add Finance User 1 & 2 to the Finance Users Security Group**  


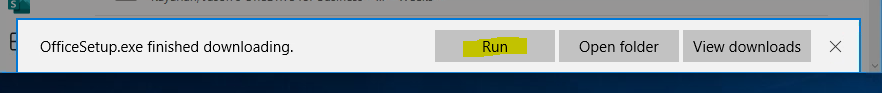
Give the **Finance Security Group an email address** of

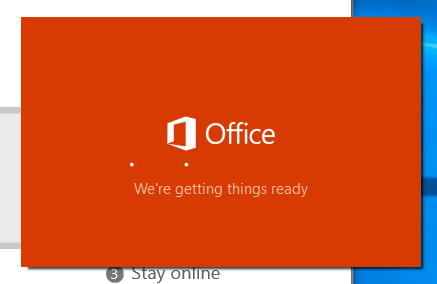
[FINANCEUSERS@CYB394XX.PRI](mailto:FINANCEUSERS@CYB394XX.PRI)  


1. **Power on CLIENT 1**
2. Sign-In to CLIENT1 with FinUser1, pin File Explorer to Taskbar -> Sign Out
3. Sign-In to CLIENT1 with FinUser2, pin File Explorer to Taskbar -> Sign Out
4. Sign-In to CLIENT1 with your PDA (Password16)
5. Start menu -> Microsoft Edge -> Google -> Office 365 Login. Log on with your school account.  
   
6. Once logged on go to the office 365 home page and find the install office link then select **install Office 365 apps**



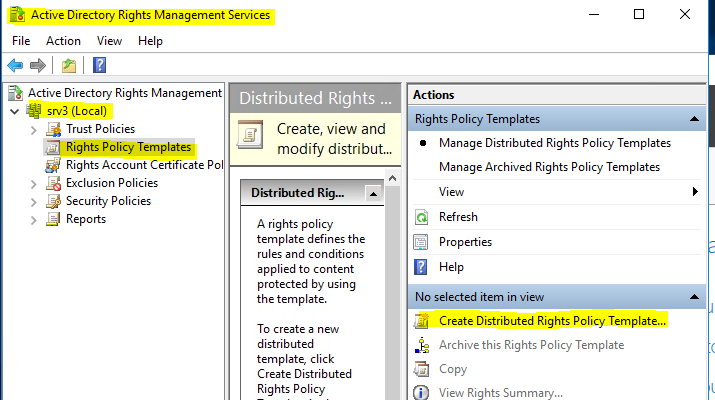


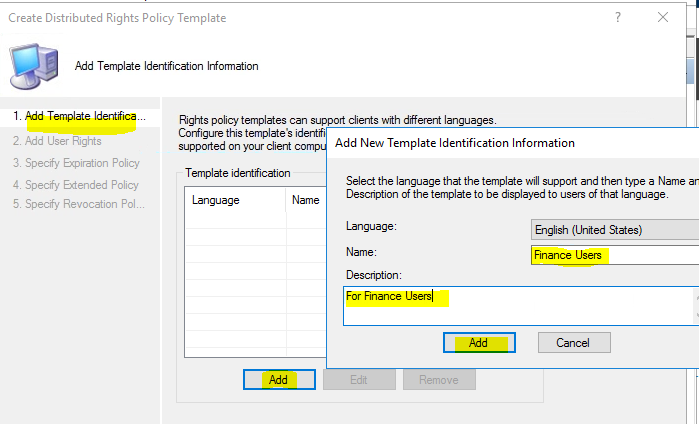


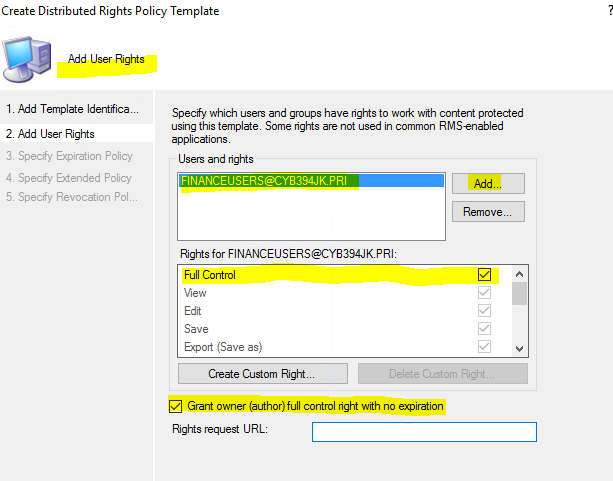


1. Install Office 365 and once the install completes, Sign Out

# Part 4 AD RMS Templates

1. **SRV3** -> Server Manager -> Tools -> **Active Directory Rights Management Services**
2. In the left-hand navigation pane, expand the node for the SRV3 cluster -> **Rights Policy Templates**
3. In the Right-hand nav -> Actions pane, click Create Distributed Rights Policy Template and Click Add  
   
4. Fill in the following

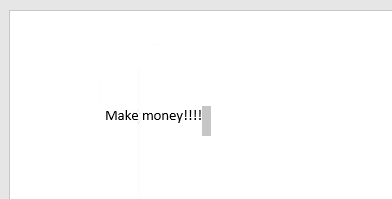


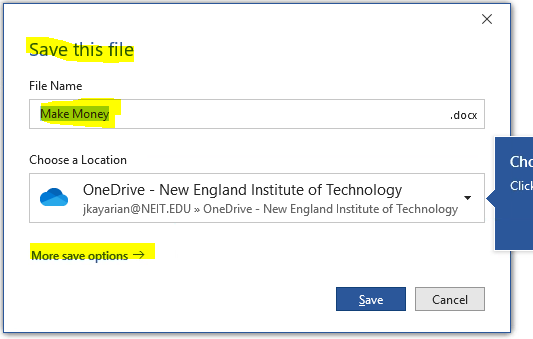
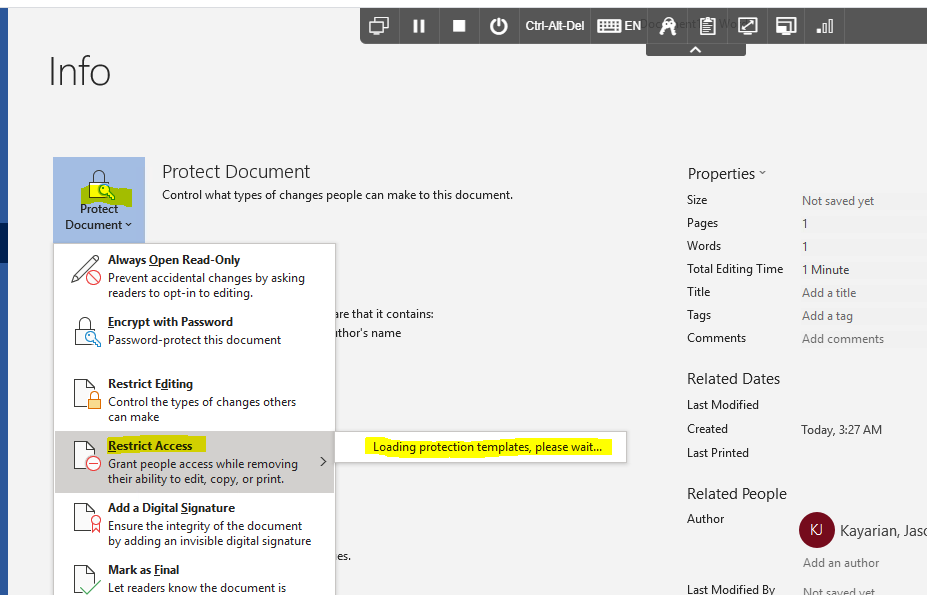
1. Then click [Add] then [Cancel] to close the Add New Template dialog window.
2. Click [Next]
3. In the Add users Rights box type in [FINANCEUSERS@CYB394XX.PRI](mailto:FINANCEUSERS@CYB394XX.PRI)
4. Under Rights grant them full control
5. Optionally, in the Rights request URL text box, type a URL that can be accessed for clients to request additional rights. This request is a manual operation. Leave it blank for now  
     
   Click [Next]
6. **Content expiration -> (\*) Never expires** -> [Next]
7. Keep defaults and click **[Next]** through the rest of the creating process -> **[Finish]**

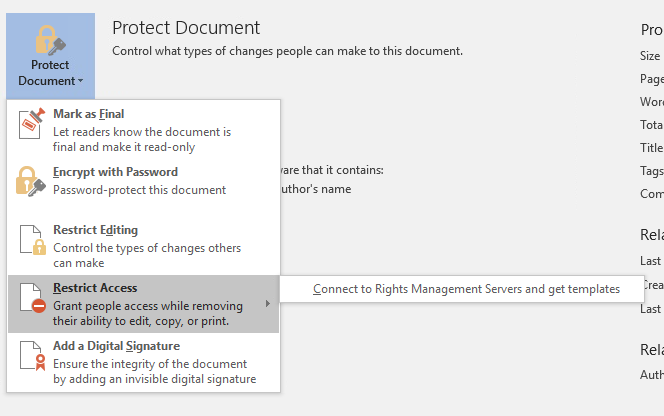
|  |
| --- |
| Screenshot of ADRMS console with new Rights Policy Template: |

# Part 5 Protecting a Word document with RMS

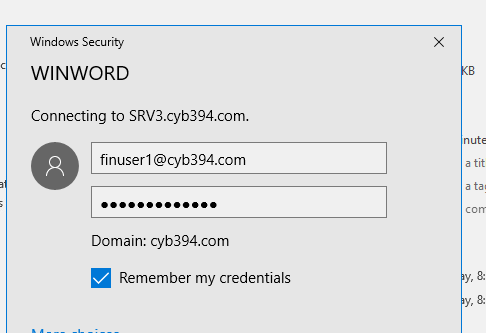
1. Sign In to **CLIENT1 with finuser1** (Password16)
2. Create a new folder on the Local Disk (C:) [C:\makedollars]
3. Launch Microsoft Word -> **Sign In to O365 if needed** -> Accept MS Word licensing policy.
4. Create a new document with the text **Make money!!!!**



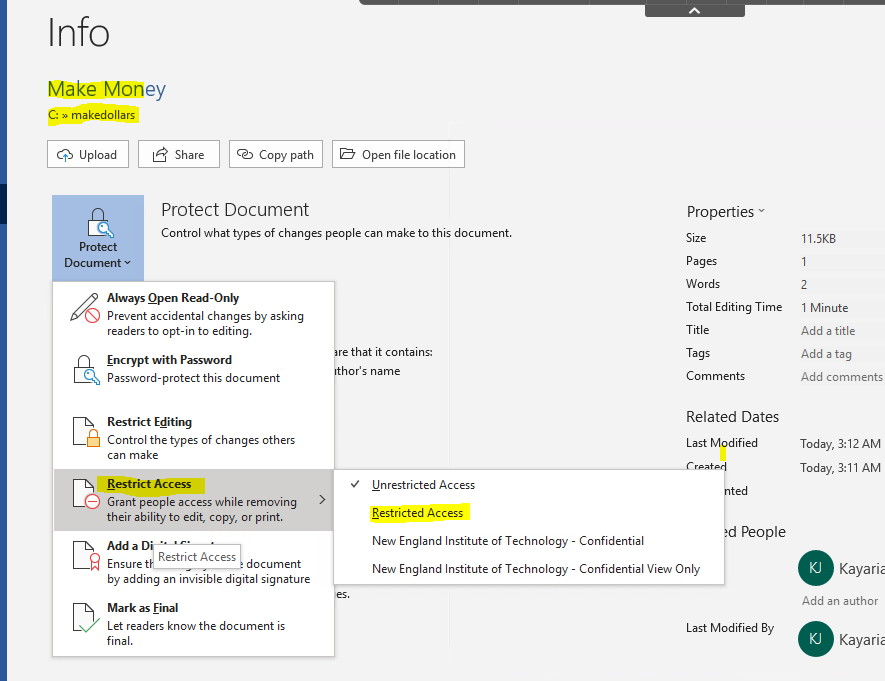
1. Save (Not Close) the document to the C:\makedollars folder. Use the More save options to choose Browse to the C:\makedollars folder.  
   
2. **MS Word -> File -> Info -> Protect Document then select Restrict Access**. Click on **Connect to Rights Management Servers and get templates.  
   Templates may load automatically and the Connect to Right Management and get templates menu may Not appear. If so proceed to Step 10.**



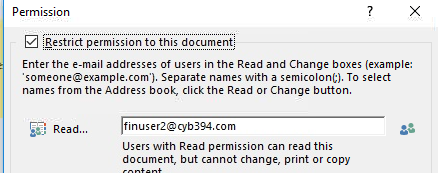
1. If prompted to confirm certificate click OK
2. If prompted for Credentials enter the following in the UPN format (*jdoe@contoso.com*)



1. You may receive an error. Close out of word then open it again. Go back to the Protect document area you should see the following selections

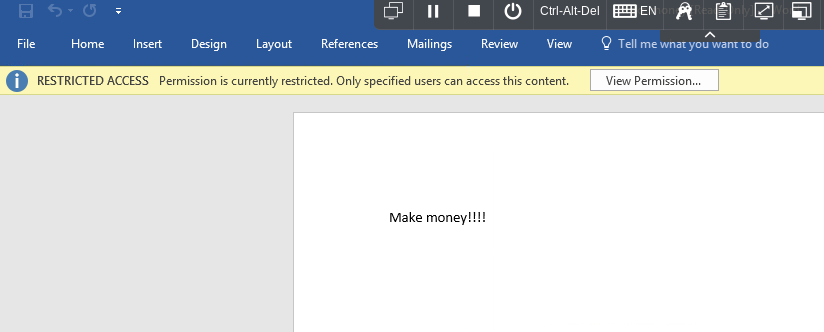


1. Choose Restricted Access
2. In the Read section type FINUSER2@CYB394XX.PRI



1. Click Ok then Save & Close MS Word
2. **Sign Out of CLIENT1**
3. **Sign In -> CLIENT1 as FINUSER2** (Password16)
4. Navigate to the [C:\makedollars] folder and open the Make Money document.
5. Sign In to Activate Office and IF prompted with a certificate click [OK]
6. Then type [FINUSER2@CYB394XX.PRI](mailto:FINUSER2@CYB394XX.PRI) with password of Password16
7. You should now see the document, but you are restricted to read access.

**\*\*\* May say [Change Permissions]**



1. Log off and (Make sure your admin account has an email in AD) logon with your administrator account
2. Attempt to open the word document as an administrator. If prompted enter credentials in the UPN format.

|  |
| --- |
| Screenshot of **RESTRICTED ACCESS** message: |

1. Shutdown All VM’s from the Start Menu