Managing RMS TEMPLATES

SERVER 2012

AD RMS uses rights policy templates to enforce a consistent set of policies to protect content.
When configuring AD RMS, you need to develop strategies to ensure that users can still access protected content from a computer that is not connected to the AD RMS cluster.

Rights policy templates allow you to configure standard methods of implementing AD RMS policies across the organization.

For example, you can configure standard templates that grant view-only rights, block the ability to edit, save, and print, or if used with Exchange Server, block the ability to forward or reply to messages.

AD RMS templates support the following rights:

- **Full Control.** Gives a user full control over an AD RMS–protected document.

- **View.** Gives a user the ability to view an AD RMS–protected document.

- **Edit.** Allows a user to modify an AD RMS–protected document.
- **Save.** Allows a user to use the Save function with an AD RMS–protected document.

- **Export (Save as).** Allows a user to use the Save As function with an AD RMS–protected document.

- **Print.** Allows an AD RMS–protected document to be printed.

- **Forward.** Used with Exchange Server. Allows the recipient of an AD RMS–protected message to forward that message.

- **Reply.** Used with Exchange Server. Allows the recipient of an AD RMS–protected message to reply to that message.

- **Reply All.** Used with Exchange Server. Allows the recipient of an AD RMS–protected message to use the Reply All function to reply to that message.

- **Extract.** Allows the user to copy data from the file. If this right is not granted, the user cannot copy data from the file.

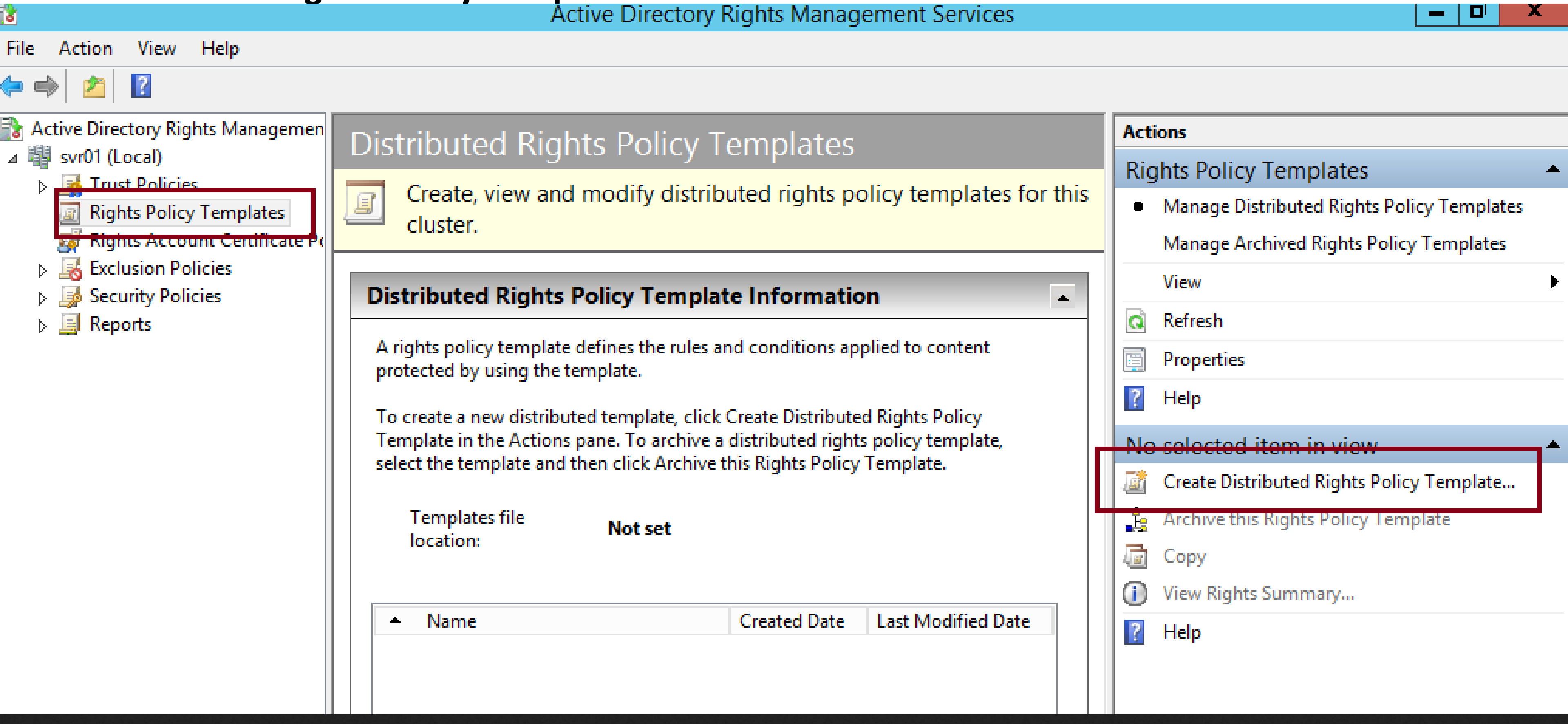
- **Allow Macros.** Allows the user to utilize macros.

- **View Rights.** Allows the user to view assigned rights.

- **Edit Rights.** Allows the user to modify the assigned rights.

Configuring the ADRMS Rights Policy Templates

1 – On the SVR01 server, open Active Directory Rights Management Services console, then **click Rights Policy Templates node and then in the Actions pane, click Create Distributed Rights Policy Template…**



Active Directory Rights Management Services
File
Action
View
Help
Active Directory Rights Managemen
svr01 (Local)
Trust Policies
Rights Policy Templates
Rights Account Certificate Po
Exclusion Policies
Security Policies
Reports
Actions
Rights Policy Templates
Manage Distributed Rights Policy Templates
Manage Archived Rights Policy Templates
View
Refresh
Properties
Help
No selected item in view
Create Distributed Rights Policy Template...
Archive this Rights Policy Template
Copy
View Rights Summary...
Help

Distributed Rights Policy Templates

Create, view and modify distributed rights policy templates for this cluster.

Distributed Rights Policy Template Information

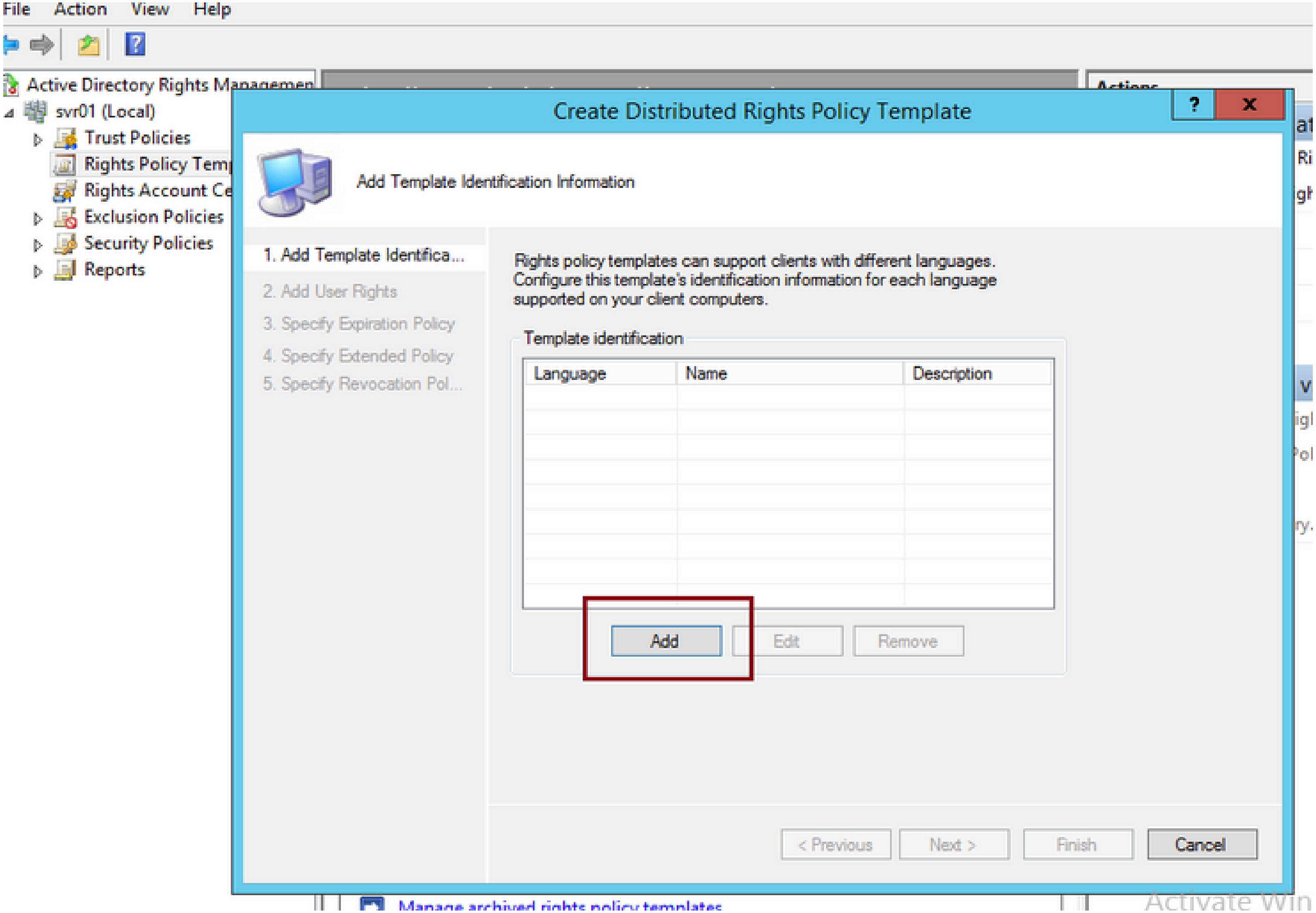
A rights policy template defines the rules and conditions applied to content protected by using the template.

To create a new distributed template, click Create Distributed Rights Policy Template in the Actions pane. To archive a distributed rights policy template, select the template and then click Archive this Rights Policy Template.

Templates file location: **Not set**

Name	Created Date	Last Modified Date

2 – In the Create Distributed Rights Policy Template Wizard box, **on the Add Template Identification information box, click Add…**



Create Distributed Rights Policy Template

Add Template Identification Information

Rights policy templates can support clients with different languages. Configure this template's identification information for each language supported on your client computers.

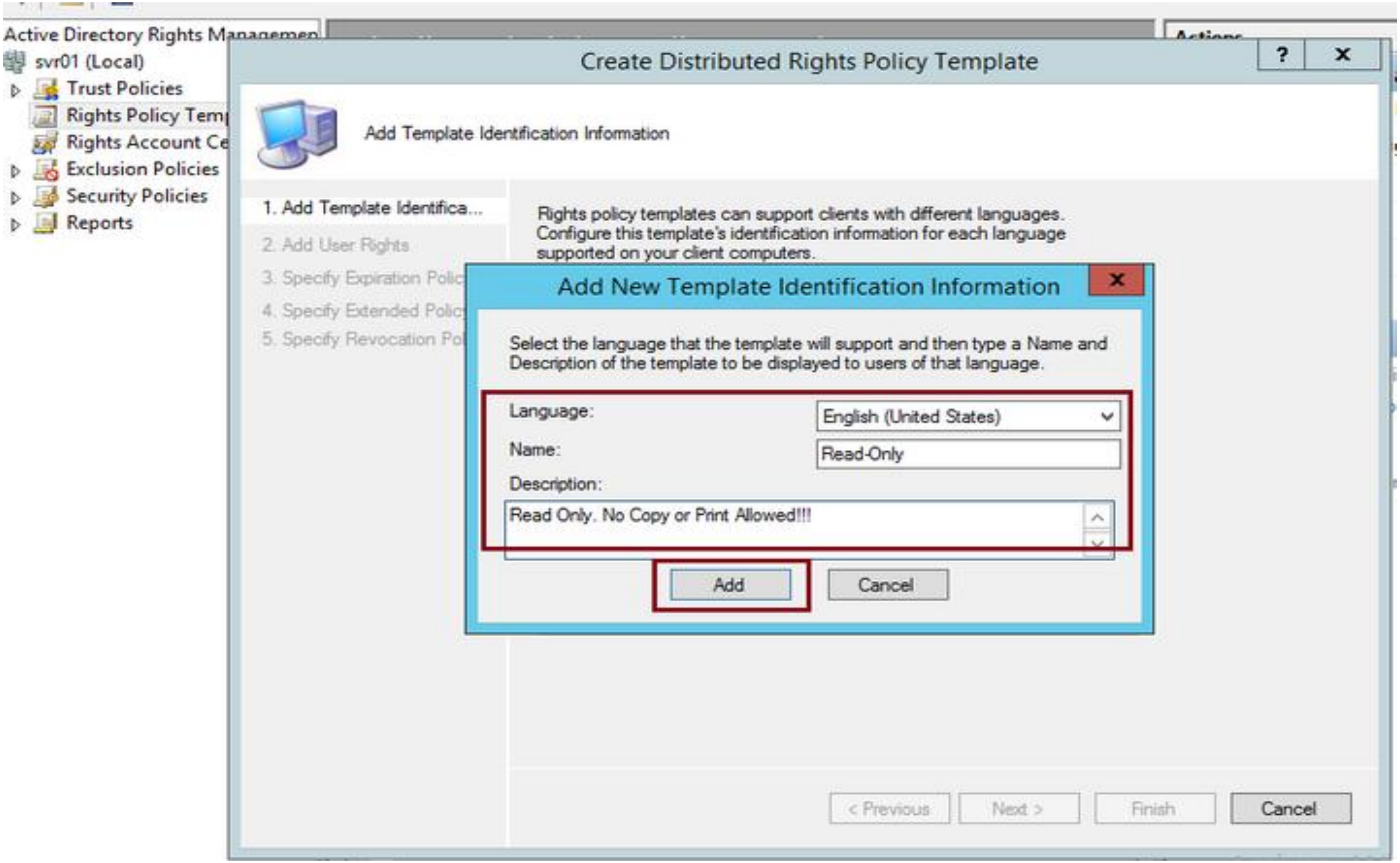
Template identification

Language	Name	Description

3 – On the Add New Template Identification Information box, **enter the following information and then click Add and click Next to proceed…**

— Language: English (United States)

— Name: ReadOnly



Create Distributed Rights Policy Template

Add Template Identification Information

Rights policy templates can support clients with different languages. Configure this template's identification information for each language supported on your client computers.

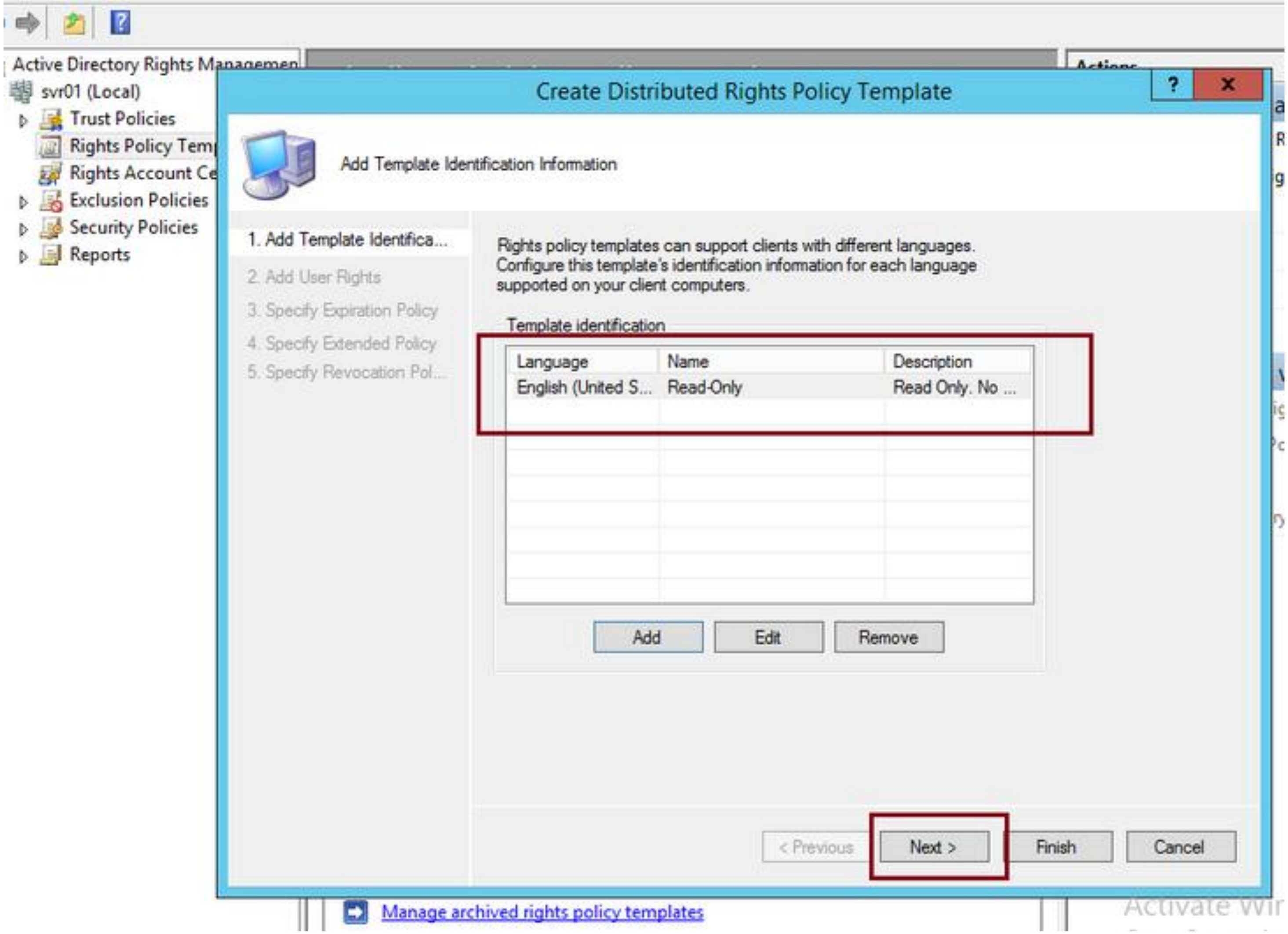
Add New Template Identification Information

Select the language that the template will support and then type a Name and Description of the template to be displayed to users of that language.

Language: English (United States)

Name: Read-Only

Description: Read Only. No Copy or Print Allowed!!!


Active Directory Rights Managemen
svr01 (Local)
Trust Policies
Rights Policy Temp
Rights Account Ce
Exclusion Policies
Security Policies
Reports
Actions
1. Add Template Identifica...
2. Add User Rights
3. Specify Expiration Policy
4. Specify Extended Policy
5. Specify Revocation Pol...
Add
Edit
Remove
< Previous
Next >
Finish
Cancel
Manage archived rights policy templates
Activate Wir

Create Distributed Rights Policy Template

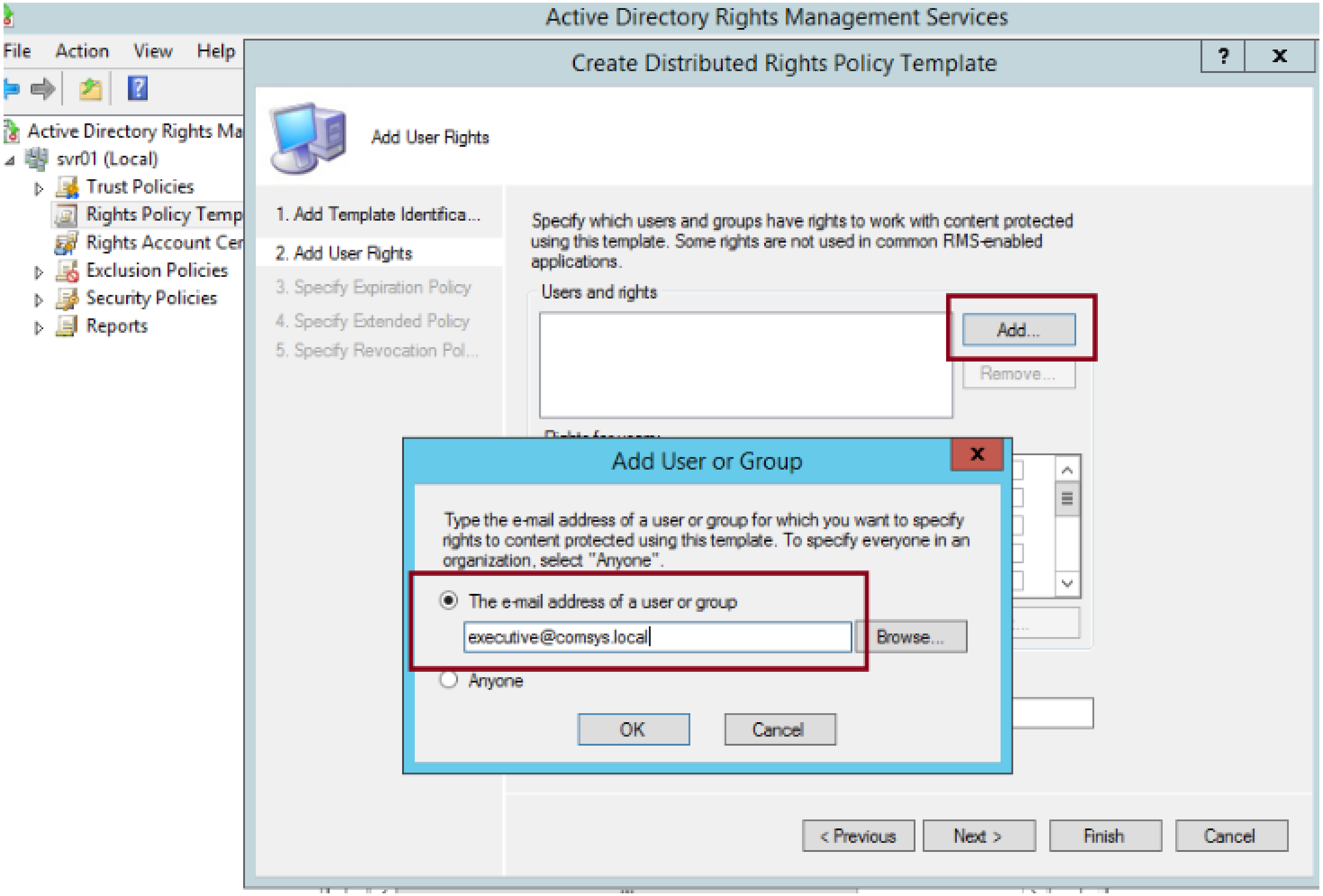
Add Template Identification Information

Rights policy templates can support clients with different languages. Configure this template's identification information for each language supported on your client computers.

Template identification

Language	Name	Description
English (United S...	Read-Only	Read Only. No ...

4 – On the Add User Rights box, click Add, then **on the Add User or Group page, type executives@comsys.local and then click OK to proceed**



Active Directory Rights Management Services
File Action View Help
Active Directory Rights Ma
svr01 (Local)
Trust Policies
Rights Policy Temp
Rights Account Cer
Exclusion Policies
Security Policies
Reports
Create Distributed Rights Policy Template
Add User Rights
1. Add Template Identifica...
2. Add User Rights
3. Specify Expiration Policy
4. Specify Extended Policy
5. Specify Revocation Pol...
Users and rights
Add...
Remove...
< Previous
Next >
Finish
Cancel

Specify which users and groups have rights to work with content protected using this template. Some rights are not used in common RMS-enabled applications.

Add User or Group

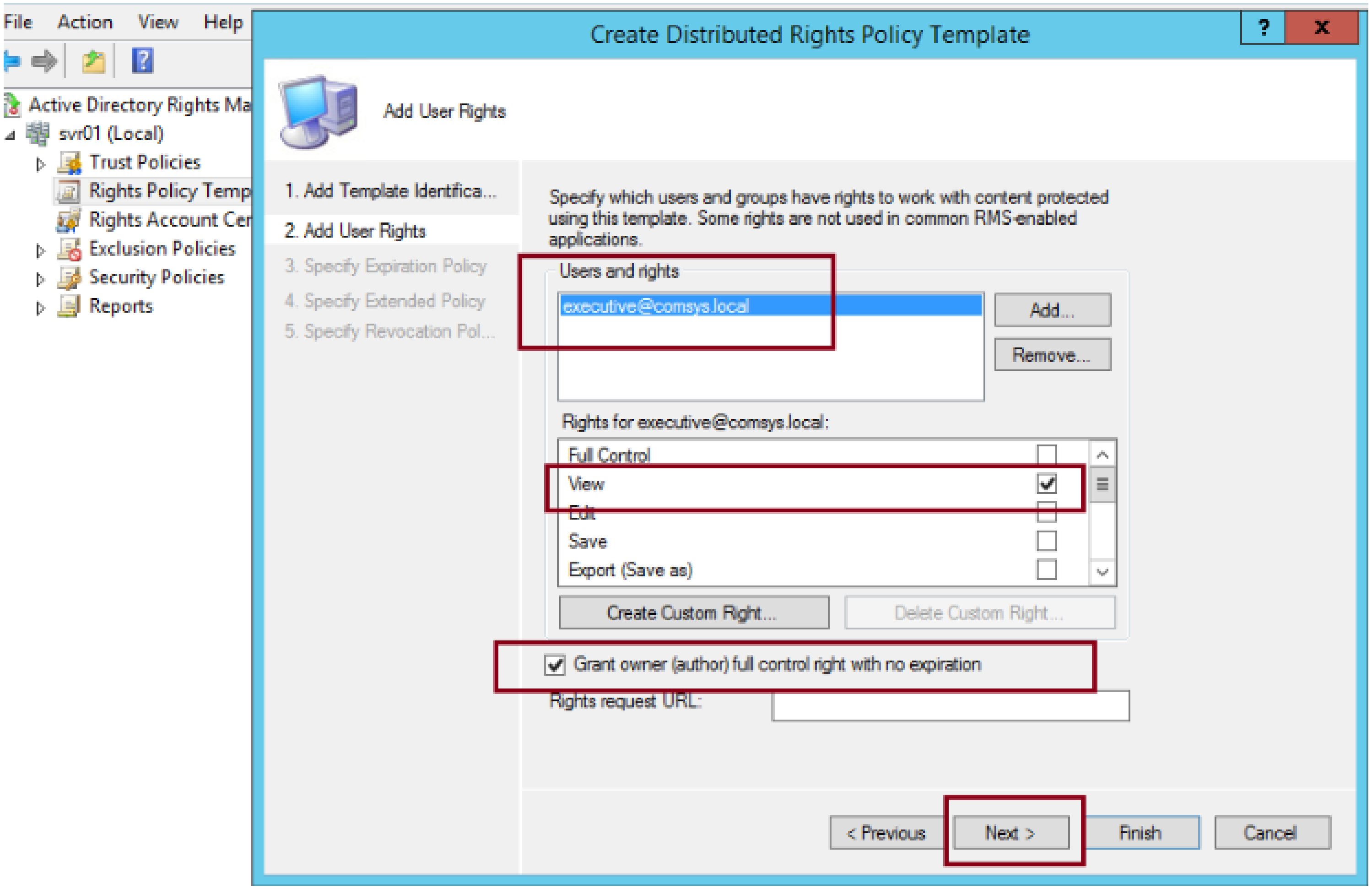
Type the e-mail address of a user or group for which you want to specify rights to content protected using this template. To specify everyone in an organization, select "Anyone".

● The e-mail address of a user or group

executive@comsys.local

○ Anyone

5 – When executives@comsys.local is selected, **under Rights, click View. Verify that Grant owner (author) full control right with no expiration is selected, and then click Next…**



Create Distributed Rights Policy Template

Add User Rights

1. Add Template Identifica...
2. Add User Rights
3. Specify Expiration Policy
4. Specify Extended Policy
5. Specify Revocation Pol...

Specify which users and groups have rights to work with content protected using this template. Some rights are not used in common RMS-enabled applications.

Users and rights

executive@comsys.local

Rights for executive@comsys.local:

Full Control □
View ☑
Edit □
Save □
Export (Save as) □

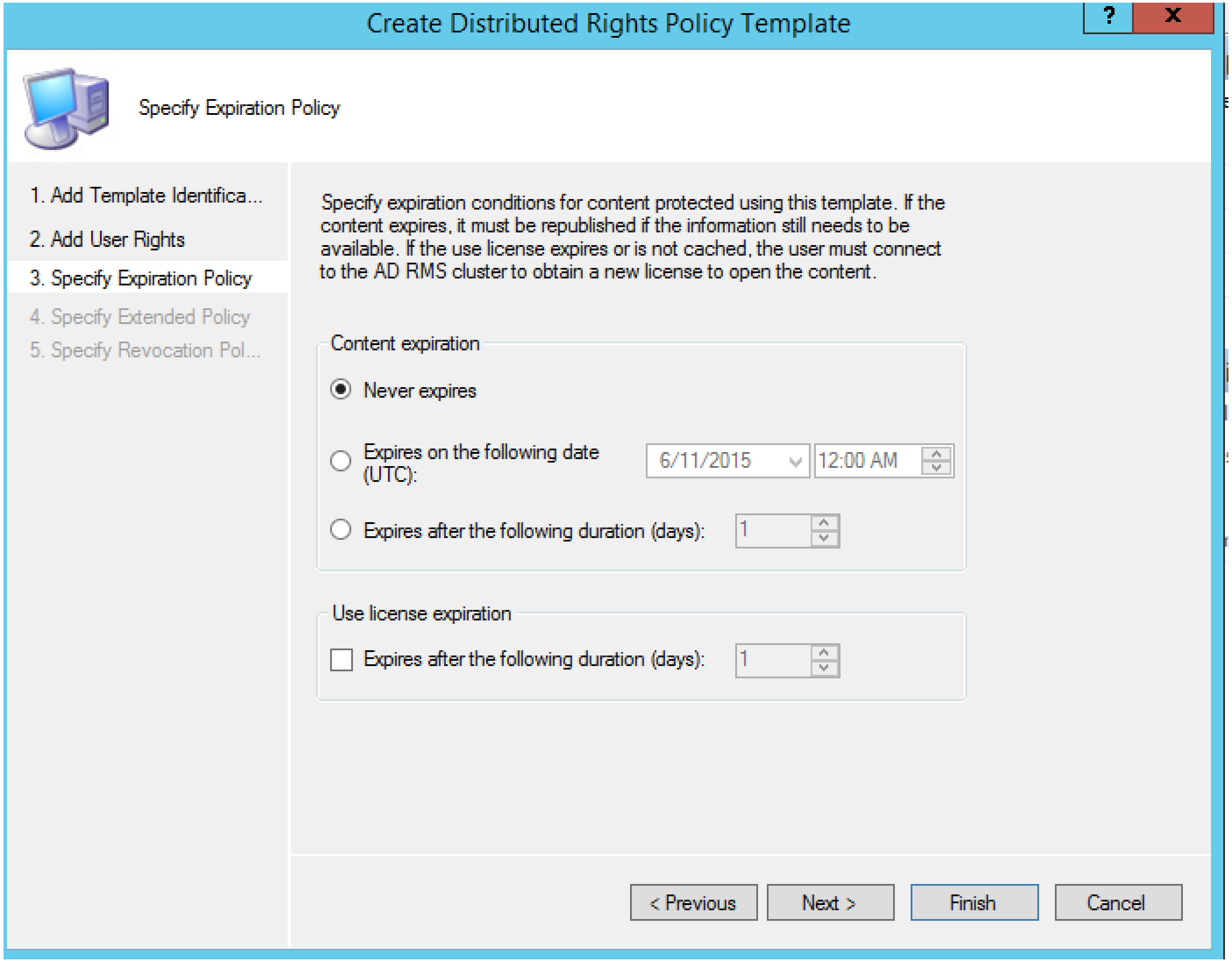
☑ Grant owner (author) full control right with no expiration

Rights request URL:

6 – On the Specify Expiration Policy box, choose the following settings and then click Next:

— Content Expiration: Expires after the following duration (days): 14

— Use license expiration: Expires after the following duration (days): 14



Create Distributed Rights Policy Template

Specify Expiration Policy

1. Add Template Identifica...
2. Add User Rights
3. Specify Expiration Policy
4. Specify Extended Policy
5. Specify Revocation Pol...

Specify expiration conditions for content protected using this template. If the content expires, it must be republished if the information still needs to be available. If the use license expires or is not cached, the user must connect to the AD RMS cluster to obtain a new license to open the content.

Content expiration

● Never expires

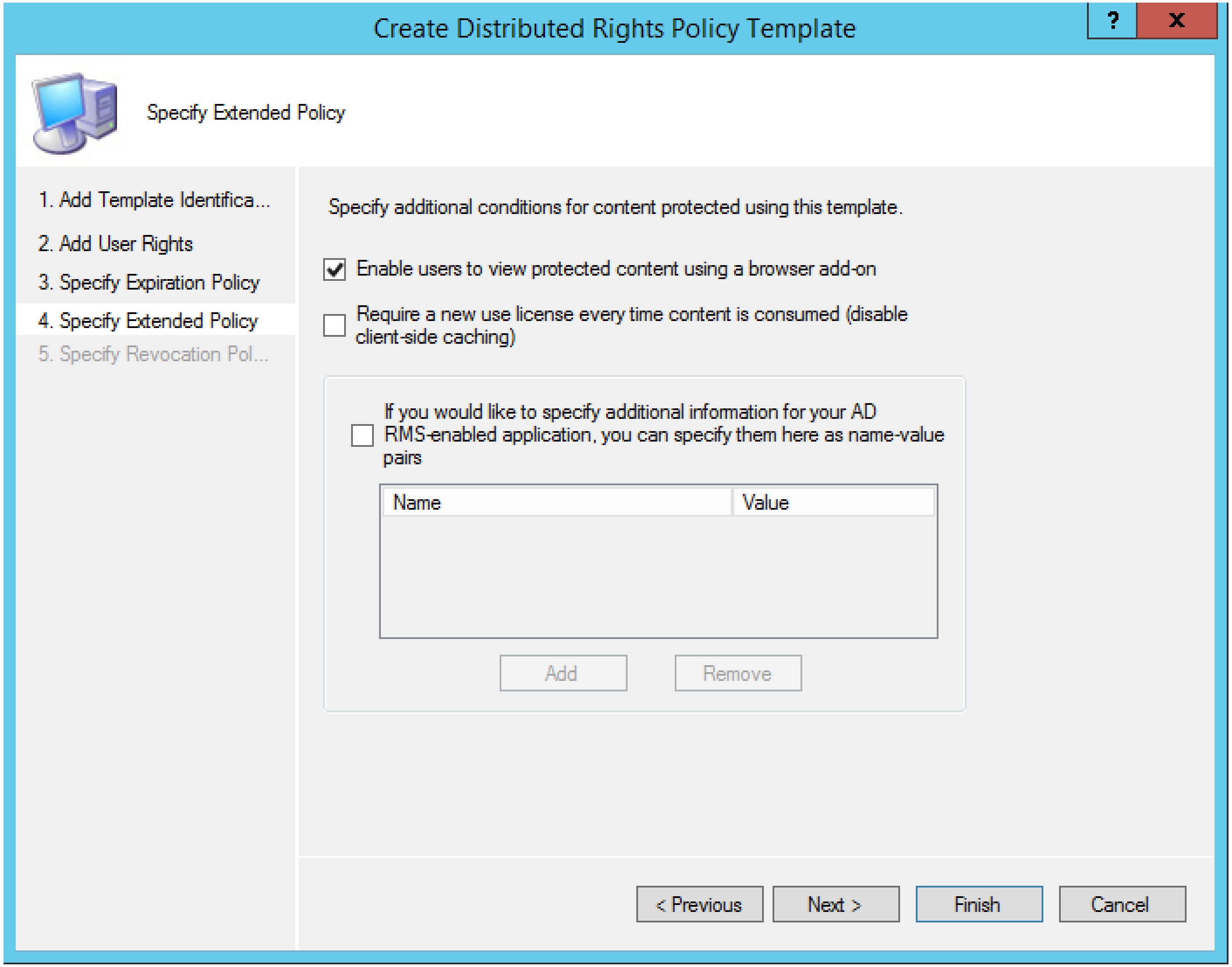
○ Expires on the following date (UTC): 6/11/2015 12:00 AM

○ Expires after the following duration (days): 1

Use license expiration

□ Expires after the following duration (days): 1

7 – On the Specify Extended Policy box, **click Require a new use license every time content is consumed (disable client-side caching), click Next, and then click Finish**



Create Distributed Rights Policy Template

Specify Extended Policy

1. Add Template Identifica...
2. Add User Rights
3. Specify Expiration Policy
4. Specify Extended Policy
5. Specify Revocation Pol...

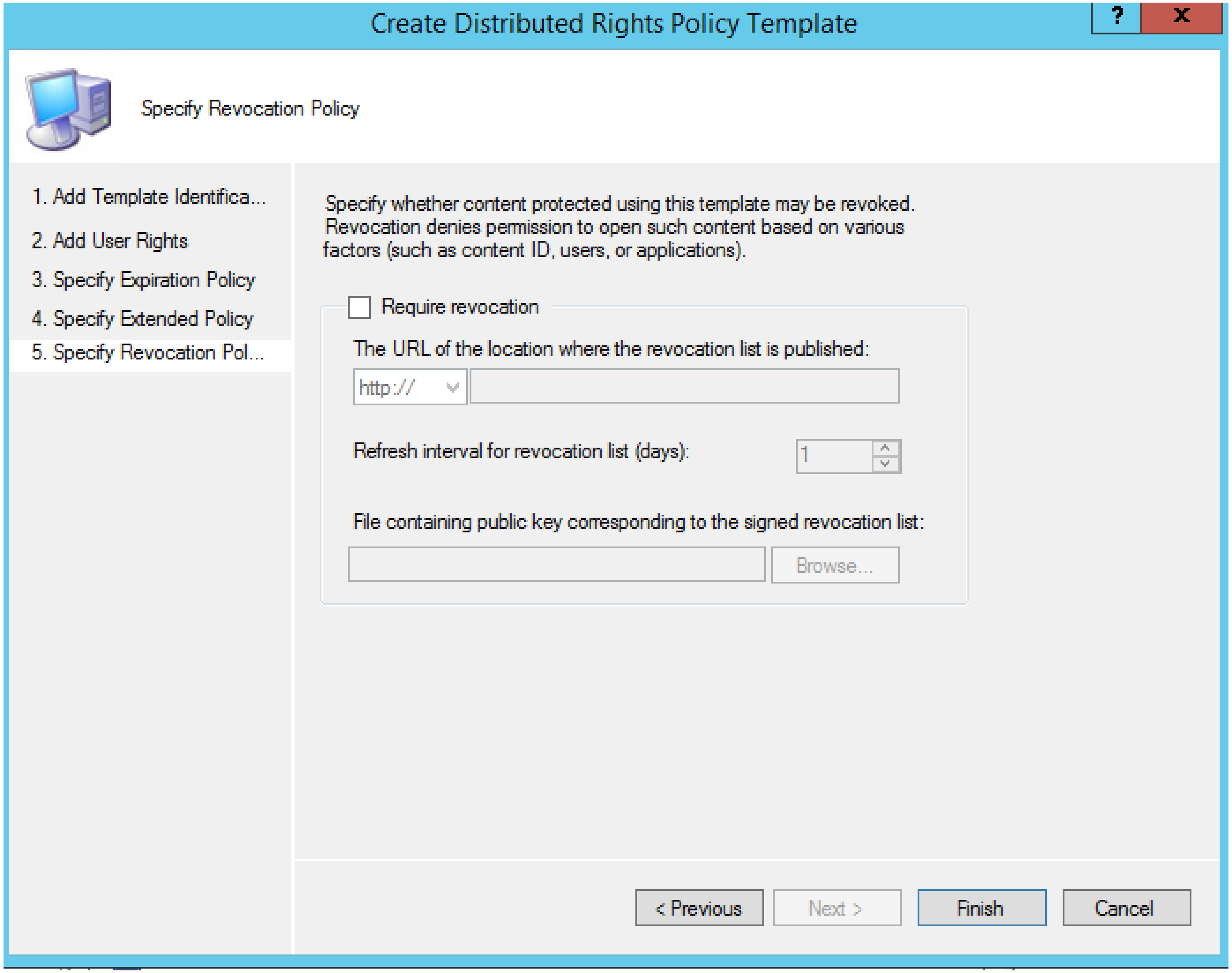
Specify additional conditions for content protected using this template.

☑ Enable users to view protected content using a browser add-on

□ Require a new use license every time content is consumed (disable client-side caching)

□ If you would like to specify additional information for your AD RMS-enabled application, you can specify them here as name-value pairs

Name	Value



Create Distributed Rights Policy Template

Specify Revocation Policy

1. Add Template Identifica...
2. Add User Rights
3. Specify Expiration Policy
4. Specify Extended Policy
5. Specify Revocation Pol...

Specify whether content protected using this template may be revoked. Revocation denies permission to open such content based on various factors (such as content ID, users, or applications).

□ Require revocation

The URL of the location where the revocation list is published:

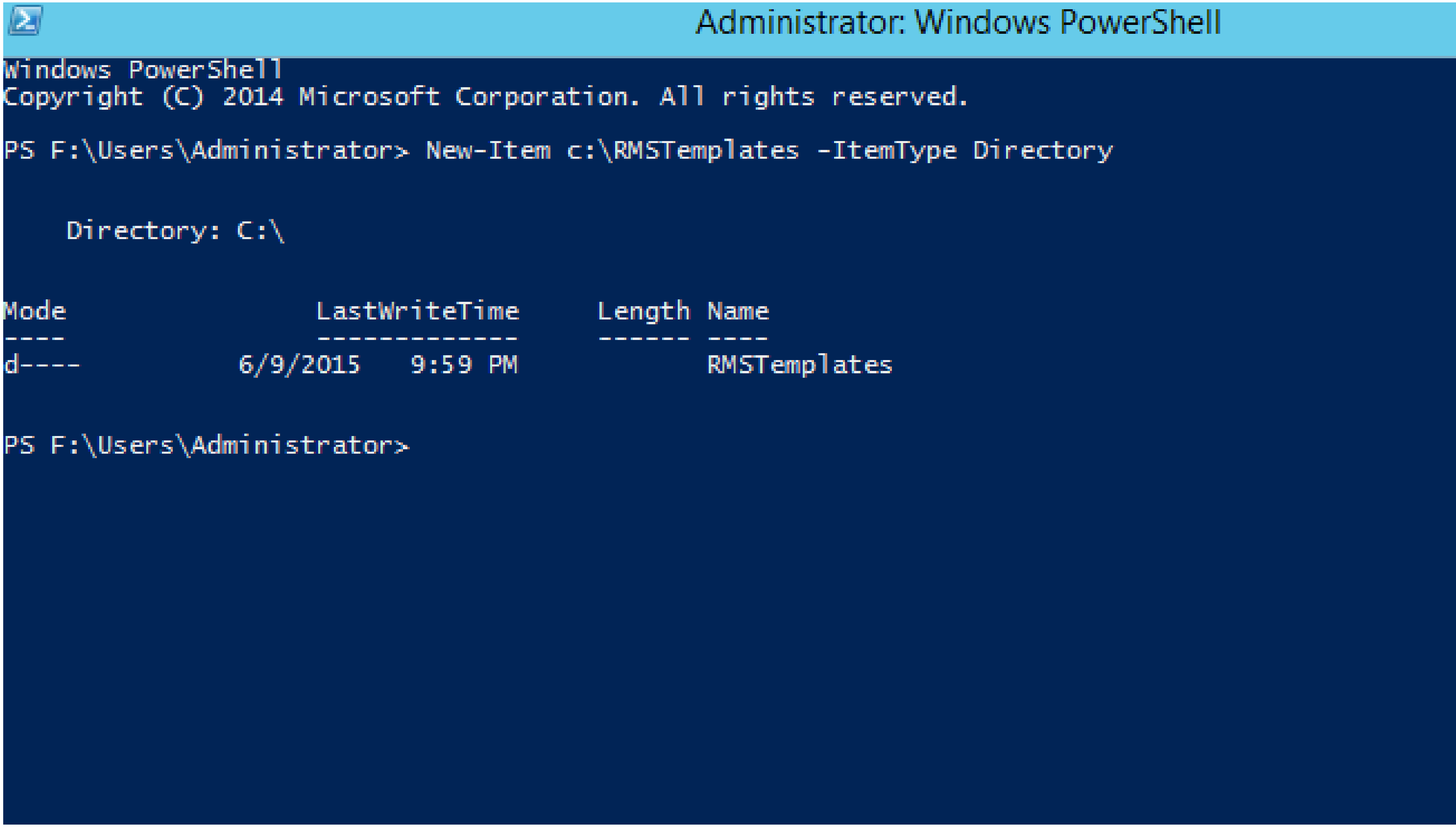
http://

Refresh interval for revocation list (days): 1

File containing public key corresponding to the signed revocation list:

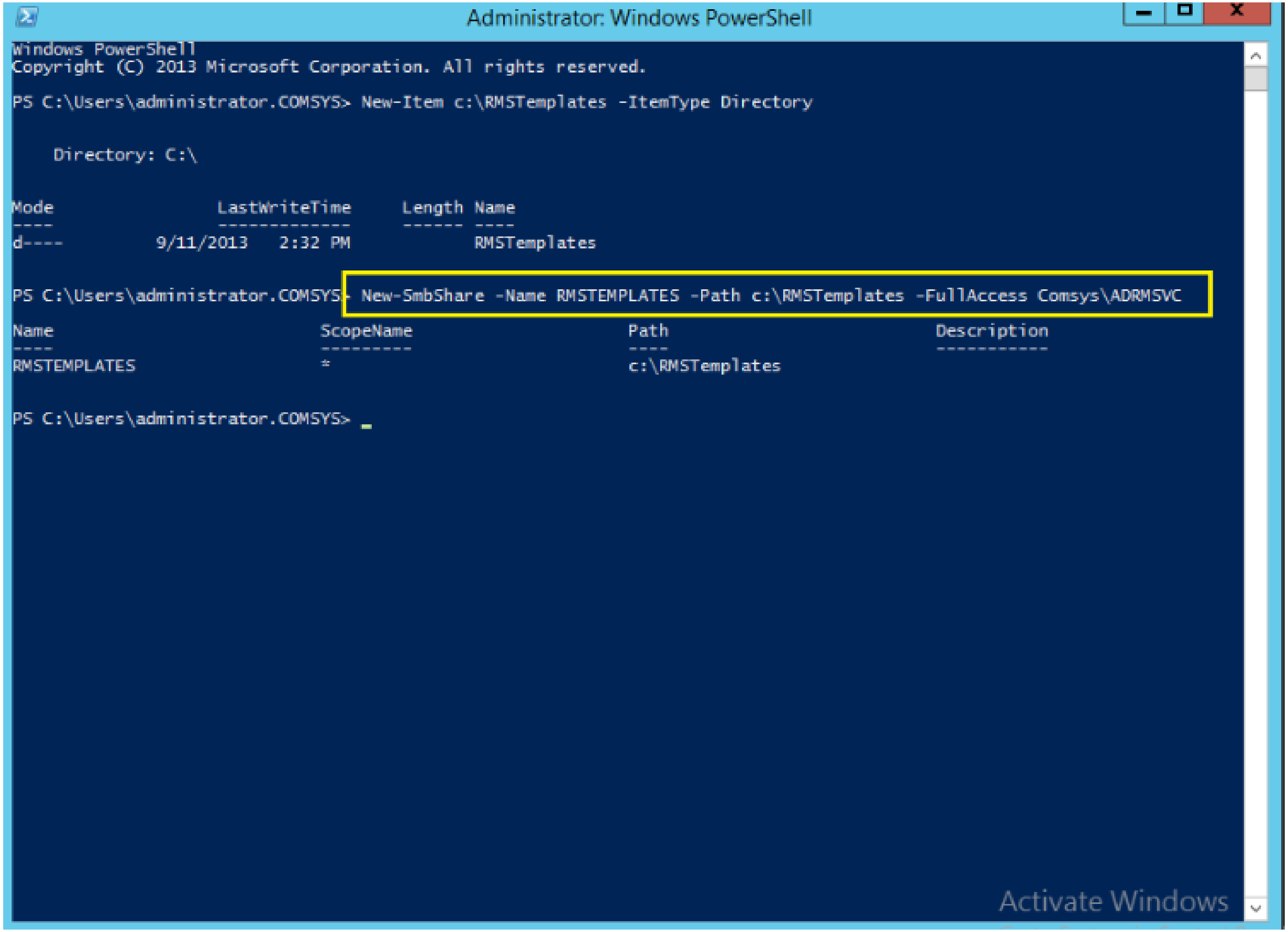
Next step, lets configure the rights policy template distribution…

8 – On the SVR01 Server, open **Windows PowerShell,** and type : **New-Item c:\RMSTemplates -ItemType Directory**



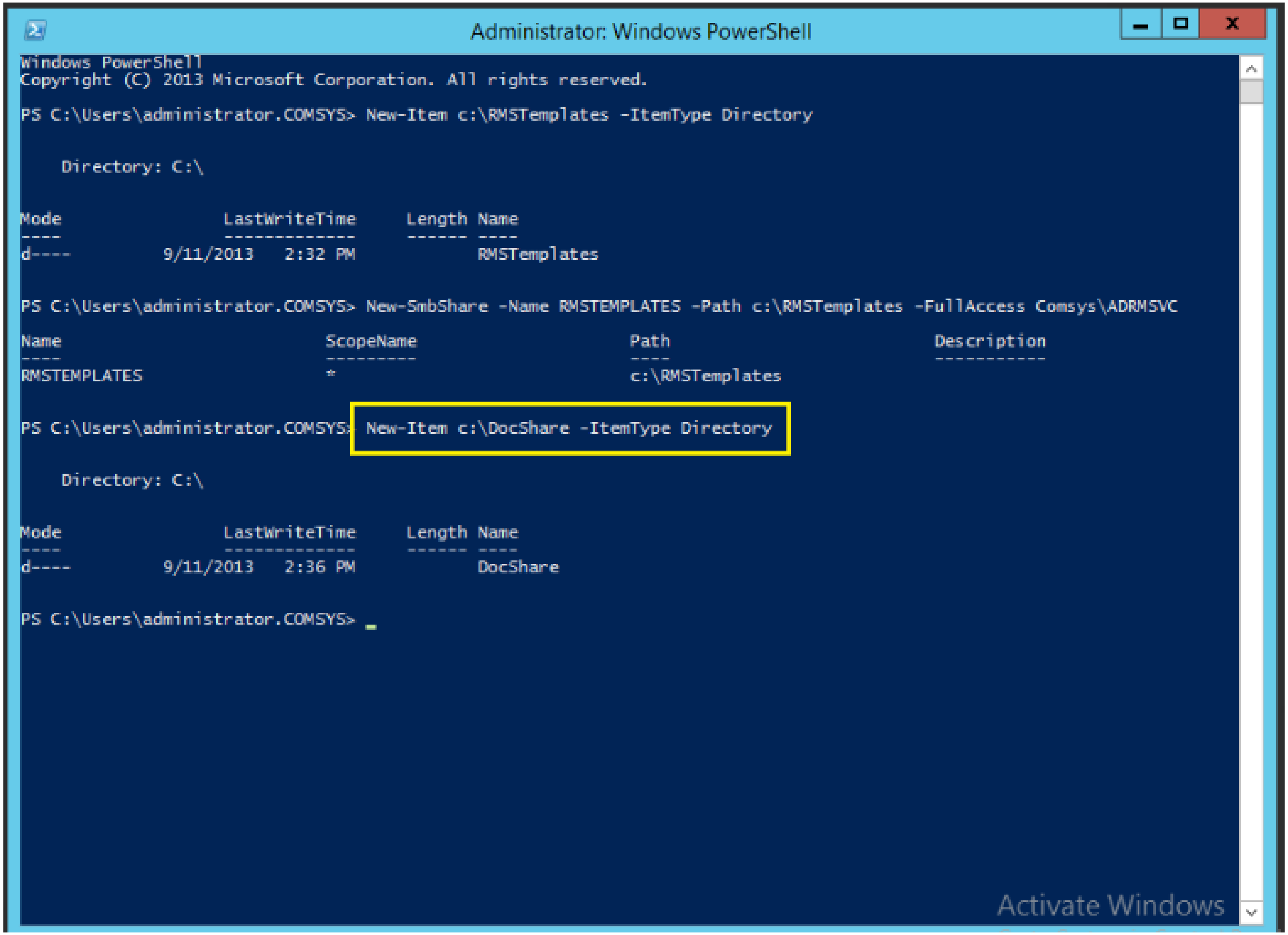
```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS F:\Users\Administrator> New-Item c:\RMSTemplates -ItemType Directory


    Directory: C:\


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d----          6/9/2015   9:59 PM            RMSTemplates


PS F:\Users\Administrator>
```

9 – Next, type **New-SmbShare -Name RMSTEMPLATES -Path c:\RMSTemplates -FullAccess Comsys\ADRMSVC**



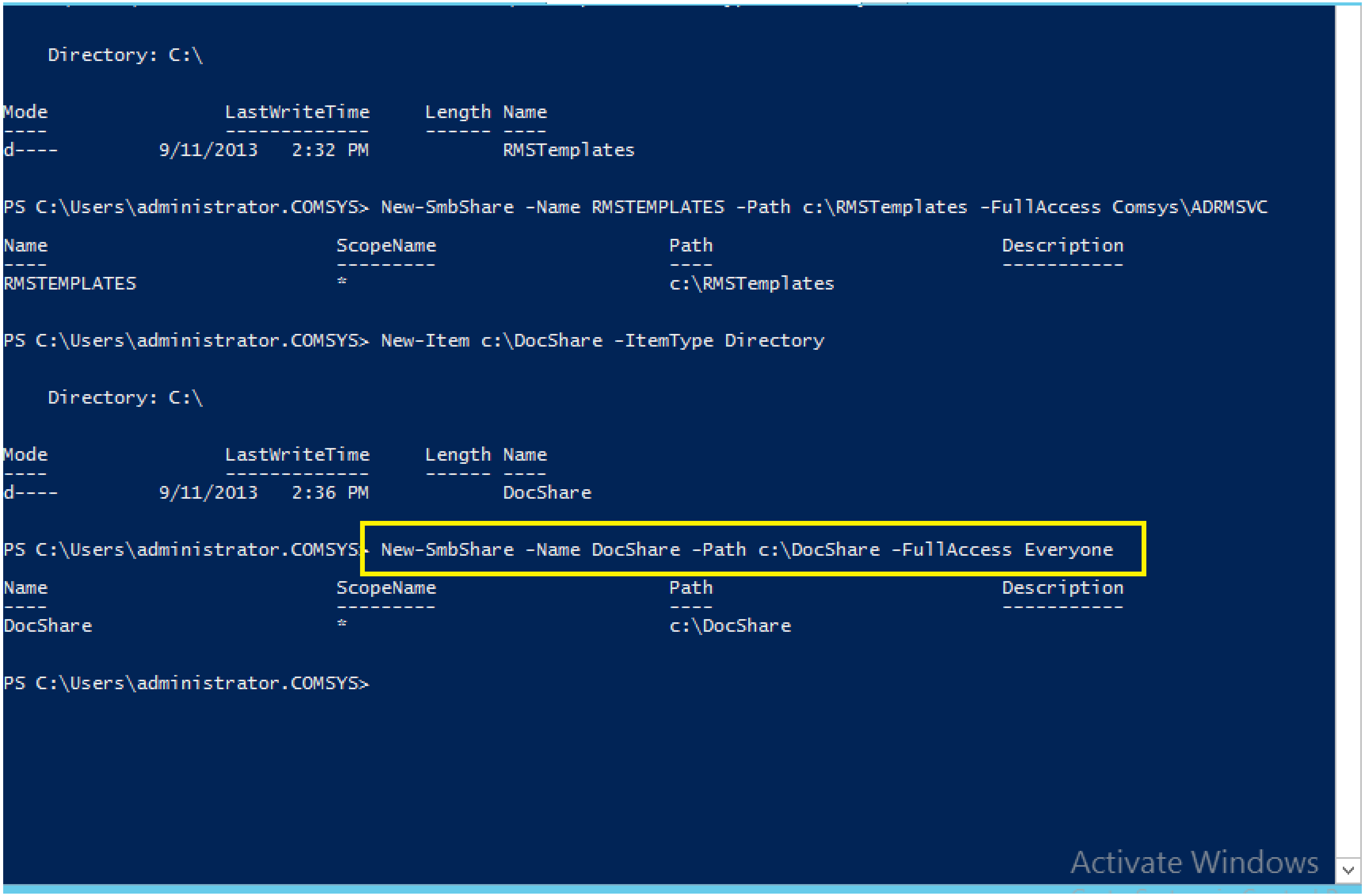
```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\administrator.COMSYS> New-Item c:\RMSTemplates -ItemType Directory


    Directory: C:\


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d----         9/11/2013   2:32 PM            RMSTemplates

PS C:\Users\administrator.COMSYS> New-SmbShare -Name RMSTEMPLATES -Path c:\RMSTemplates -FullAccess Comsys\ADRMSVC

Name                          ScopeName                     Path                          Description
----                          ---------                     ----                          -----------
RMSTEMPLATES                  *                             c:\RMSTemplates


PS C:\Users\administrator.COMSYS> _
```

10- Next type : **New-Item c:\DocShare -ItemType Directory**



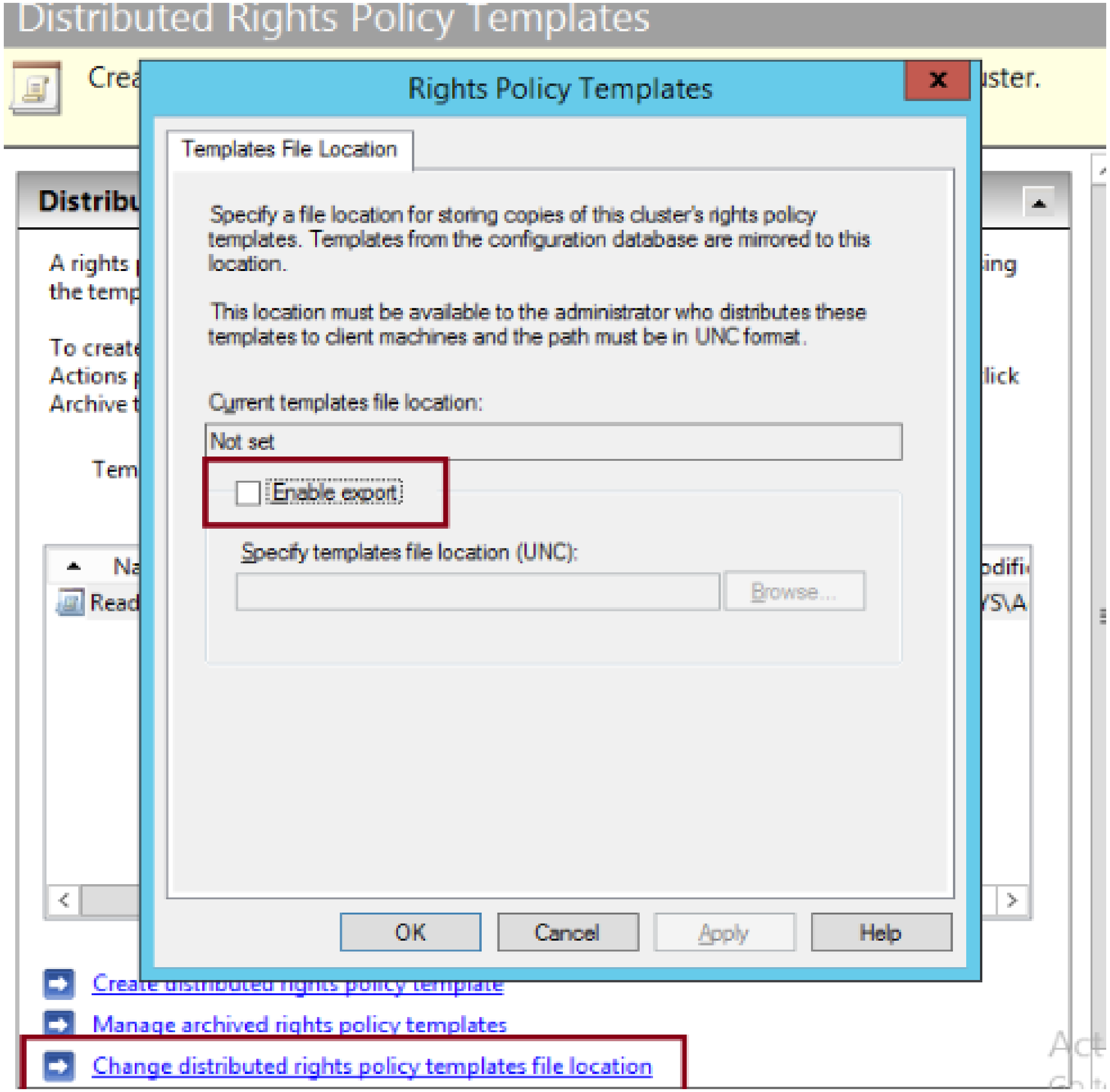
```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\administrator.COMSYS> New-Item c:\RMSTemplates -ItemType Directory


    Directory: C:\


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d----         9/11/2013   2:32 PM            RMSTemplates


PS C:\Users\administrator.COMSYS> New-SmbShare -Name RMSTEMPLATES -Path c:\RMSTemplates -FullAccess Comsys\ADRMSVC

Name                          ScopeName                     Path                          Description
----                          ---------                     ----                          -----------
RMSTEMPLATES                  *                             c:\RMSTemplates


PS C:\Users\administrator.COMSYS> New-Item c:\DocShare -ItemType Directory


    Directory: C:\


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d----         9/11/2013   2:36 PM            DocShare


PS C:\Users\administrator.COMSYS> _
```

11 – Next type : **New-SmbShare -Name docshare -Path c:\DocShare -FullAccess Everyone**



```
    Directory: C:\


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d----         9/11/2013   2:32 PM            RMSTemplates


PS C:\Users\administrator.COMSYS> New-SmbShare -Name RMSTEMPLATES -Path c:\RMSTemplates -FullAccess Comsys\ADRMSVC

Name                          ScopeName                     Path                          Description
----                          ---------                     ----                          -----------
RMSTEMPLATES                  *                             c:\RMSTemplates


PS C:\Users\administrator.COMSYS> New-Item c:\DocShare -ItemType Directory


    Directory: C:\


Mode                LastWriteTime     Length Name
----                -------------     ------ ----
d----         9/11/2013   2:36 PM            DocShare


PS C:\Users\administrator.COMSYS> New-SmbShare -Name DocShare -Path c:\DocShare -FullAccess Everyone

Name                          ScopeName                     Path                          Description
----                          ---------                     ----                          -----------
DocShare                      *                             c:\DocShare


PS C:\Users\administrator.COMSYS>
```

12 – **Exit PowerShell** and open Active Directory Rights Management Services console. On the ADRMS console, click the Rights Policy Templates node, and in the Distributed Rights Policy Templates area, click **Change distributed rights policy templates file location, then in the Rights Policy Templates dialog box, click Enable Export**



Rights Policy Templates

Templates File Location

Specify a file location for storing copies of this cluster's rights policy templates. Templates from the configuration database are mirrored to this location.

This location must be available to the administrator who distributes these templates to client machines and the path must be in UNC format.

Current templates file location:

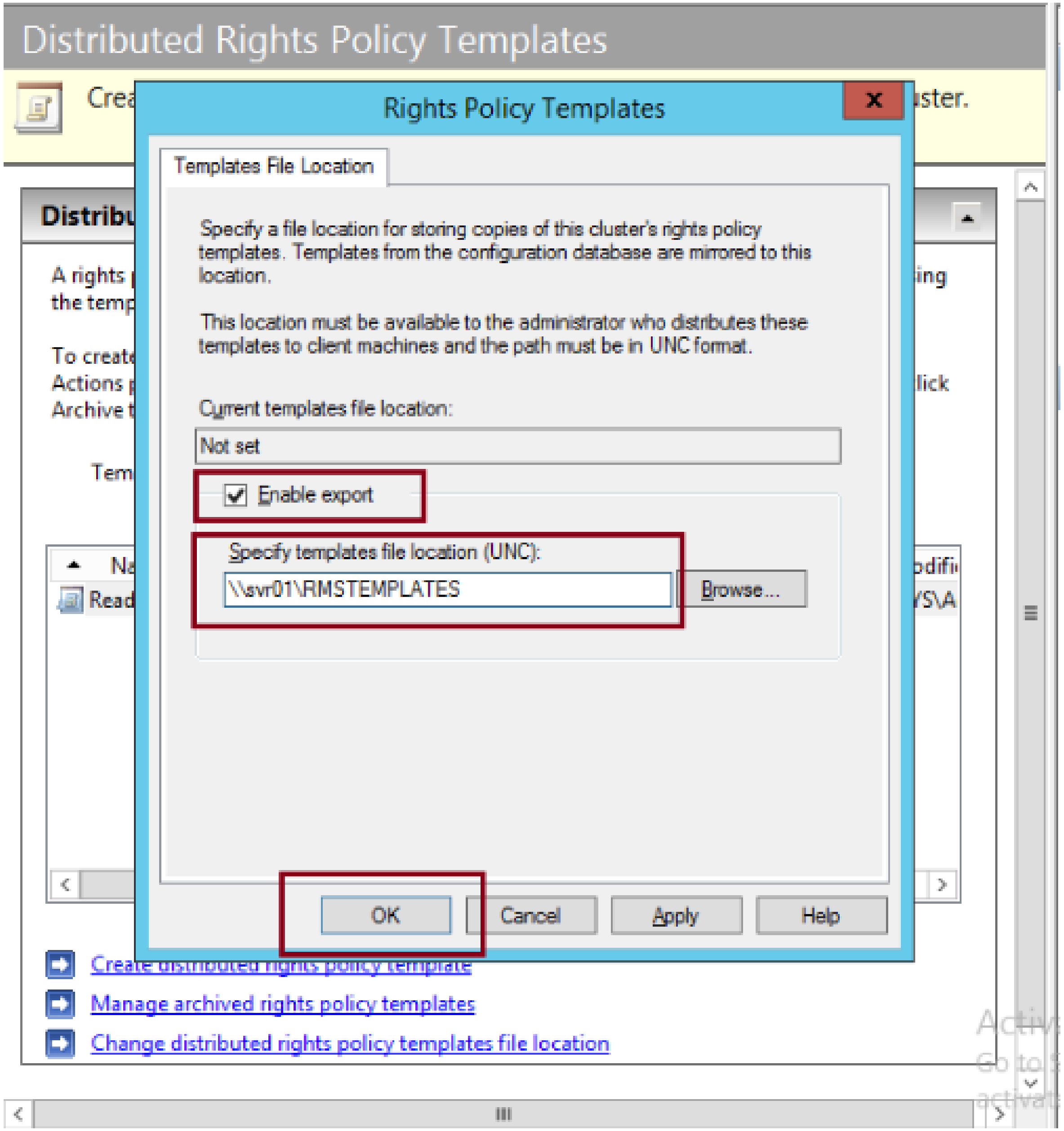
Not set

□ Enable export

Specify templates file location (UNC):

Distributed Rights Policy Templates
Browse...
OK
Cancel
Apply
Help
Create distributed rights policy template
Manage archived rights policy templates
Change distributed rights policy templates file location

13 – Next, in the Specify Templates File Location (UNC), **type \\svr01\RMSTEMPLATES, and then click OK…**



Distributed Rights Policy Templates

Rights Policy Templates

Templates File Location

Specify a file location for storing copies of this cluster's rights policy templates. Templates from the configuration database are mirrored to this location.

This location must be available to the administrator who distributes these templates to client machines and the path must be in UNC format.

Current templates file location:

Not set

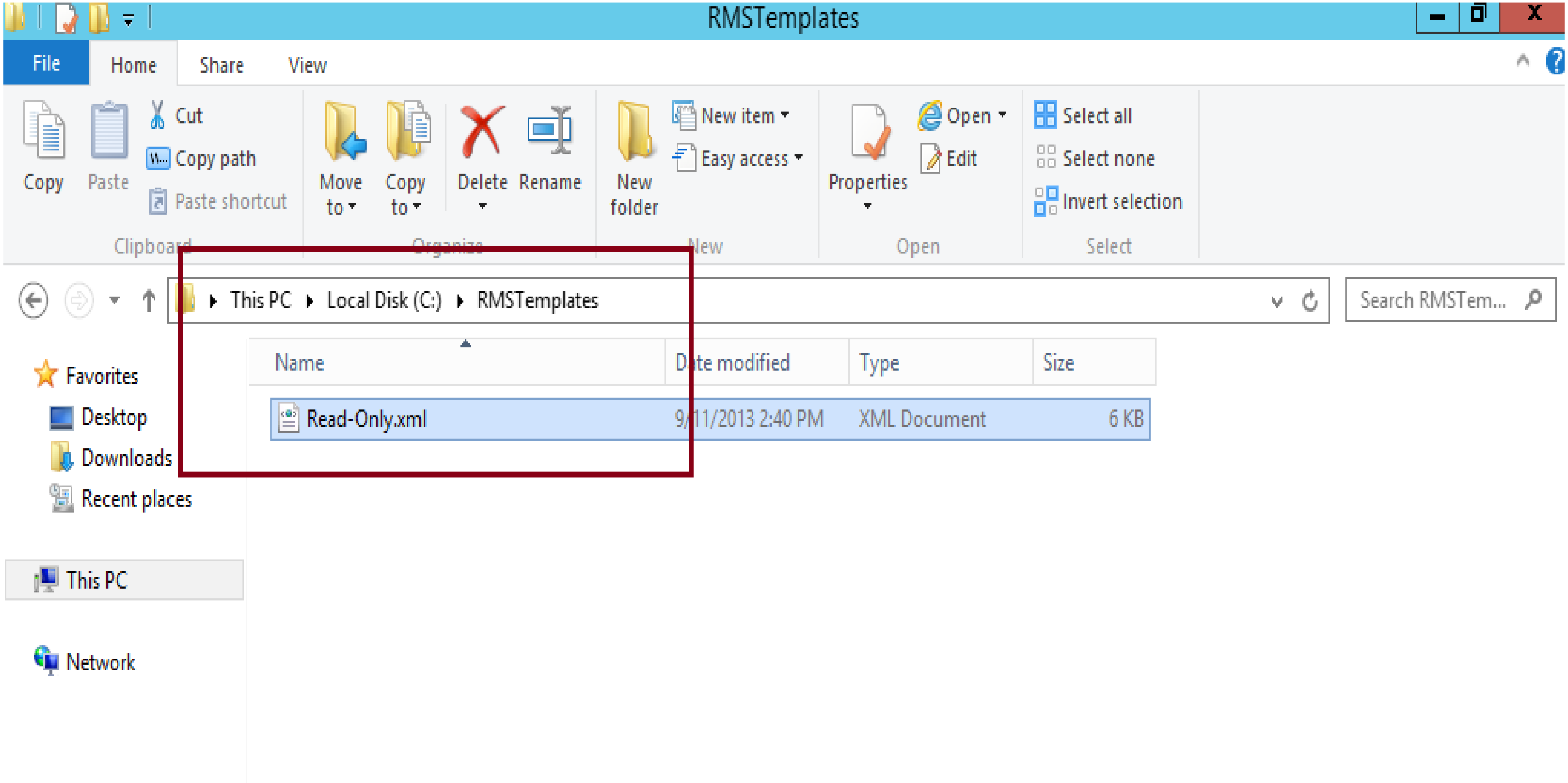
☑ Enable export

Specify templates file location (UNC):

\\svr01\RMSTEMPLATES

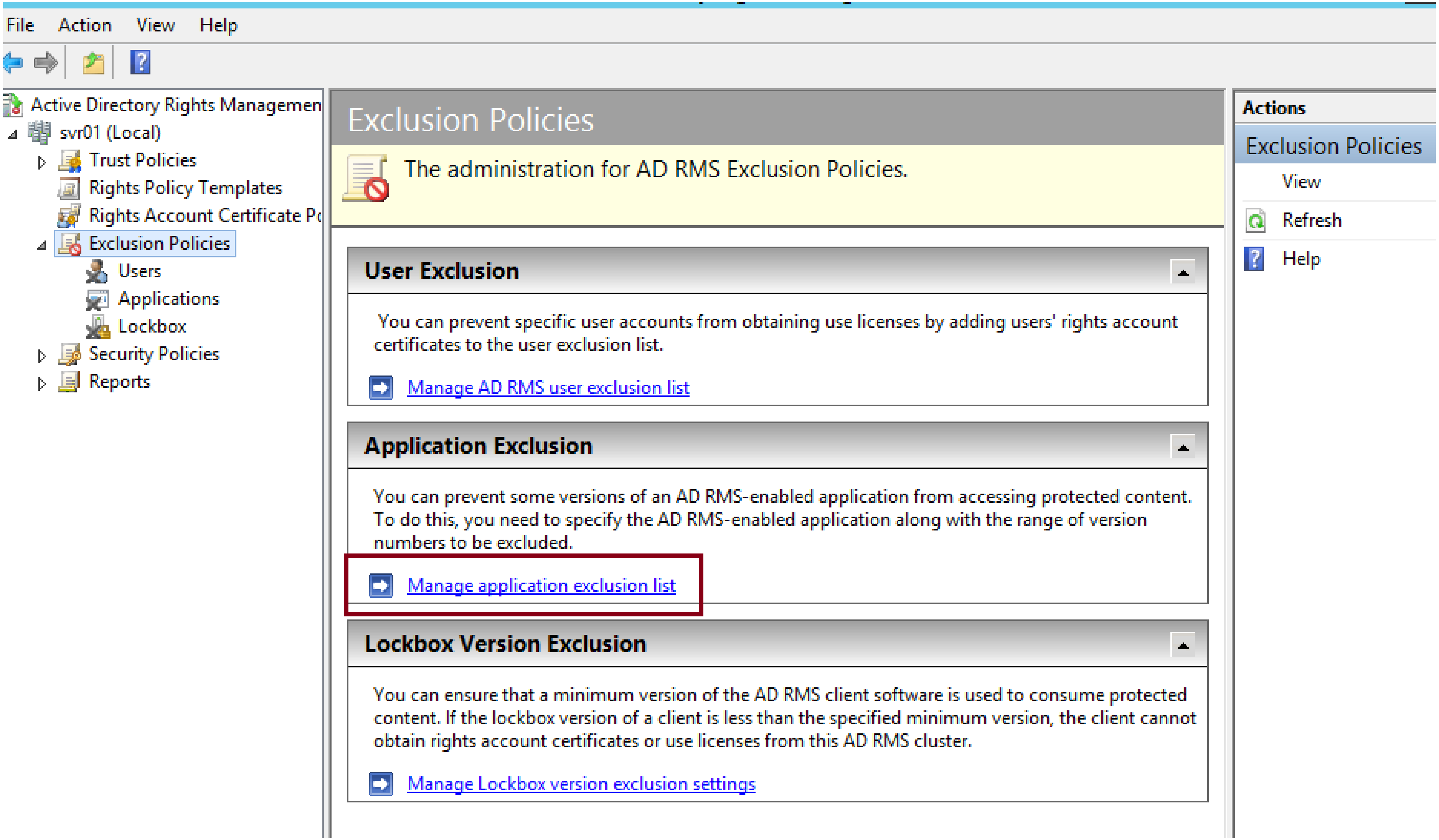
Browse...
OK
Cancel
Apply
Help
Create distributed rights policy template
Manage archived rights policy templates
Change distributed rights policy templates file location

14 – Next, **open Windows Exporer and navigate to the C:\rmstemplates folder, and verify that ReadOnly.xml is present**



Name	Date modified	Type	Size
Read-Only.xml	9/11/2013 2:40 PM	XML Document	6 KB

15 – Next, on the ADRMS Console, **click the Exclusion Policies node, and then click Manage application exclusion list…**



Exclusion Policies

The administration for AD RMS Exclusion Policies.

User Exclusion

You can prevent specific user accounts from obtaining use licenses by adding users' rights account certificates to the user exclusion list.

Manage AD RMS user exclusion list

Application Exclusion

You can prevent some versions of an AD RMS-enabled application from accessing protected content. To do this, you need to specify the AD RMS-enabled application along with the range of version numbers to be excluded.

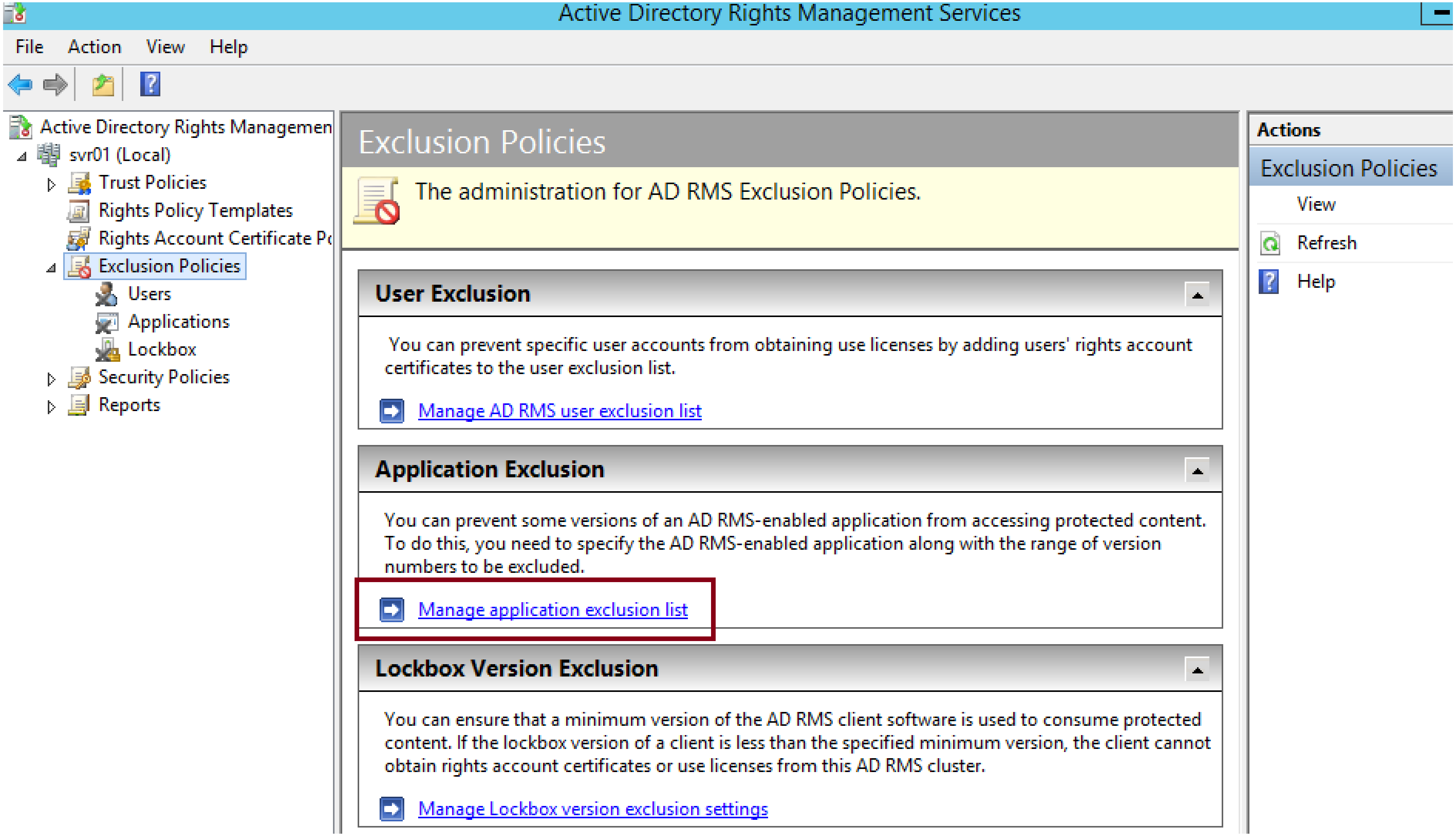
Manage application exclusion list

Lockbox Version Exclusion

You can ensure that a minimum version of the AD RMS client software is used to consume protected content. If the lockbox version of a client is less than the specified minimum version, the client cannot obtain rights account certificates or use licenses from this AD RMS cluster.

Manage Lockbox version exclusion settings

15 – Next, on the ADRMS Console, **click the Exclusion Policies node, and then click Manage application exclusion list…**



Exclusion Policies

The administration for AD RMS Exclusion Policies.

User Exclusion

You can prevent specific user accounts from obtaining use licenses by adding users' rights account certificates to the user exclusion list.

Manage AD RMS user exclusion list

Application Exclusion

You can prevent some versions of an AD RMS-enabled application from accessing protected content. To do this, you need to specify the AD RMS-enabled application along with the range of version numbers to be excluded.

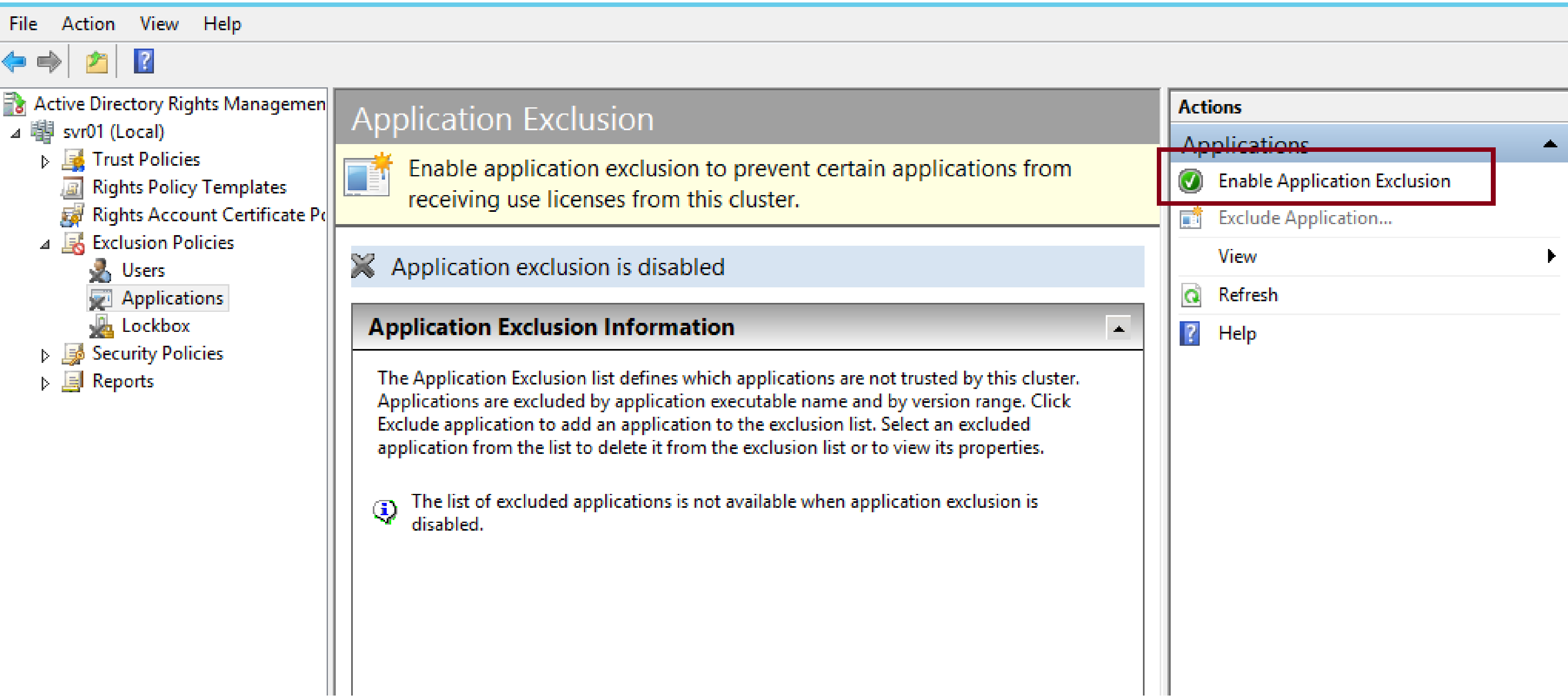
Manage application exclusion list

Lockbox Version Exclusion

You can ensure that a minimum version of the AD RMS client software is used to consume protected content. If the lockbox version of a client is less than the specified minimum version, the client cannot obtain rights account certificates or use licenses from this AD RMS cluster.

Manage Lockbox version exclusion settings

16 – In the Actions pane, click **Enable Application Exclusion…**



Application Exclusion

Enable application exclusion to prevent certain applications from receiving use licenses from this cluster.

Application exclusion is disabled

Application Exclusion Information

The Application Exclusion list defines which applications are not trusted by this cluster. Applications are excluded by application executable name and by version range. Click Exclude application to add an application to the exclusion list. Select an excluded application from the list to delete it from the exclusion list or to view its properties.

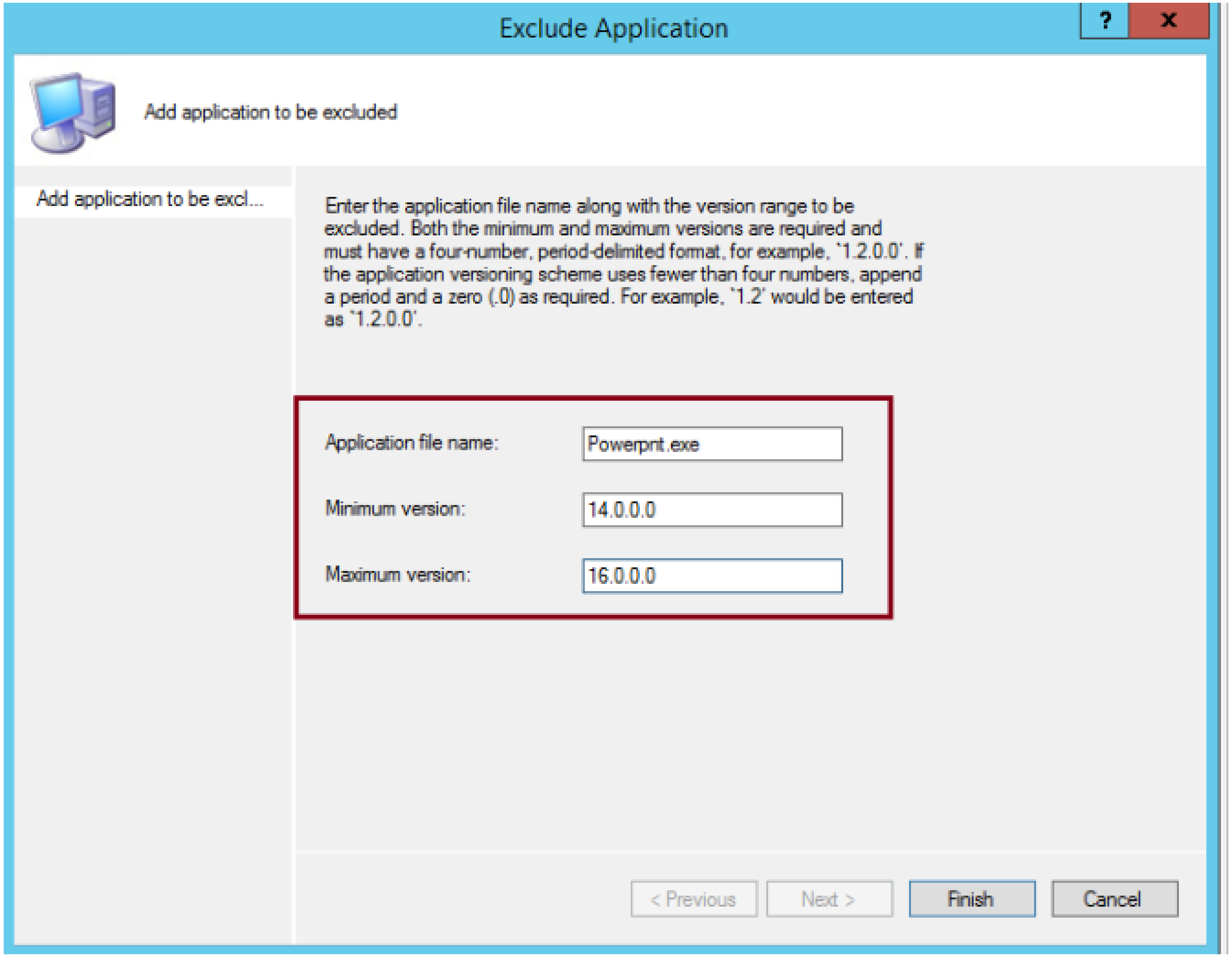
The list of excluded applications is not available when application exclusion is disabled.

17 – In the Actions pane, click **Exclude Application and enter the following information, and then click Finish:**

— Application File name: Powerpnt.exe

— Minimum version: 14.0.0.0

— Maximum version: 16.0.0.0



Exclude Application

Add application to be excluded

Enter the application file name along with the version range to be excluded. Both the minimum and maximum versions are required and must have a four-number, period-delimited format, for example, '1.2.0.0'. If the application versioning scheme uses fewer than four numbers, append a period and a zero (.0) as required. For example, '1.2' would be entered as '1.2.0.0'.

Application file name: Powerpnt.exe

Minimum version: 14.0.0.0

Maximum version: 16.0.0.0