Understanding AD RMS Exclusion Policies

Applies To: Windows Server 2008 R2, Windows Server 2012

You can implement exclusion policies to deny certain entities the ability to acquire certificate and license requests There are three ways to exclude these entities: by user, by application, and by lockbox version.

When an entity is excluded, use licenses that are created by servers in the AD RMS cluster will have that entity specified in the exclusion list. If, after a period of time, you decide to remove an entity that you have previously included in an exclusion policy, you can delete the entity from the exclusion list. Any new certification or licensing requests will not consider this entity as excluded.

We recommend that you do not remove an entity from an exclusion policy until you can be sure that all of the certificates issued before the exclusion policy was created have expired. Otherwise, both the old certificates and the new certificates will allow the content to be decrypted, which might not be what your organization wants.

The procedures in this section are designed to help you define exclusion policies on your AD RMS cluster.

- Exclude Users
- Exclude Applications
- Exclude Lockbox Versions

Exclude Users

You can exclude a user account from obtaining use licenses from an Active Directory Rights Management Services (AD RMS) cluster by specifying either the user's e-mail address or the public key string of the rights account certificate (RAC) associated with the user's RAC.

Users who are not allowed to consume rights-protected content but have e-mail accounts in your Active Directory Domain Services (AD DS) forest should be excluded by their e-mail addresses.

If a user is trusted but his or her AD RMS credentials are compromised, you can exclude only the compromised RAC by excluding its public key. When you do this, AD RMS denies new use license requests that involve that RAC. After you exclude a RAC, the next time that user

attempts to acquire a use license for new content, the request will be denied. To acquire a use license, the user will have to retrieve a new RAC with a new key pair.

If you need to exclude external users, such as Windows Live ID users, federated users, and users identified by a trusted user domain, who are not part of your AD DS forest, you can also specify a RAC to exclude their public keys.

If you add a user to the exclusion list of the AD RMS root cluster, you should also exclude the user on all licensing-only clusters in your organization. Each AD RMS cluster has independent exclusion lists.

Membership in the local **AD RMS Enterprise Administrators** , or equivalent, is the minimum required to complete this procedure.

To exclude a user

1. Open the Active Directory Rights Management Services console and expand the AD RMS cluster.
2. In the console tree, expand **Exclusion Policies** and then click **Users** .
3. In the **Actions** pane, click **Enable User Exclusion.**
4. In the **Actions** pane, click **Exclude user** . The **Exclude User Account** wizard appears.
5. Do one of the following:
    - To exclude a user by e-mail address, click the **Use this option for excluding rights account certificates of internal users who have an Active Directory Domain Services account** option, and then click **Browse** to browse to a user or group in your Active Directory Domain Services directory or type the e-mail address of the user to be excluded.

    - To exclude a user by the public key assigned to the user's rights account certificate, click the **Use this option for excluding rights account certificates of external users who do not have an Active Directory Domain Services account** option, and then type the appropriate rights account certificate public key string in the **Public key string** box.

6. Click **Finish** .

To stop excluding users

1. Open the Active Directory Rights Management Services console and expand the AD RMS cluster.
2. In the console tree, expand **Exclusion Policies** , and then click **Users** .
3. Do one of the following:
    - To disable user exclusion for all user accounts. In the **Actions** pane, click **Disable User Exclusion** . All user accounts previously excluded will be able to acquire AD RMS use licenses.

    - To stop excluding a specific user account. In the results pane, select the excluded user certificate.

4. In the **Actions** pane, click **Delete** , and then click **Yes** to confirm the removal.

Exclude Applications

Applies To: Windows Server 2008 R2, Windows Server 2012

You can specify the version of an AD RMS-enabled application that all licensing requests are checked against. Application exclusion stamps every use license with a condition that the license can bind only to the rights-protected content for which it is issued if the application that is requesting the license is not on the excluded list.

This can be useful, for example, when an enterprise deploys an update for an AD RMS-enabled application. System administrators can use their usual mechanism to cause client computers to install the update. They can then set application exclusion policies that are defined by using the version information of the application. This exclusion policy restricts AD RMS from issuing licenses to clients that are running previous versions of the software.

As with other types of exclusion, you must configure application exclusion on each cluster for which you want it to take effect.

When you apply this exclusion policy on your cluster, clients cannot use the excluded application to request and bind new use licenses to rights-protected content. However, clients can continue to use the excluded application to consume previously licensed files.

Membership in the local **AD RMS Enterprise Administrators** , or equivalent, is the minimum required to complete this procedure.

To exclude applications

1. Open the Active Directory Rights Management Services console and expand the AD RMS cluster.
2. In the console tree, expand **Exclusion Policies** , and then click **Applications** .
3. In the **Actions** pane, click **Enable Application Exclusion** .
4. In the **Actions** pane, click **Exclude Application** . The **Exclude Application** wizard appears.
5. In **Application file name** , type the file name and file name extension (such as example.exe) of the application or component to be excluded.
6. In **Minimum version** , type the minimum version number (in the format *x* . *x* . *x* . *x*) of the application that is not allowed to decrypt rights-protected content.
7. In **Maximum version** , type the maximum version (in the format *x* . *x* . *x* . *x*) of the application that is not allowed to decrypt rights-protected content.
8. Click **Finish** .

Note

AD RMS requires the application version to be specified in a 4-digit period-delimited format (#.#.#.#). However, some applications specify their application version with 2-digit or 3-digit period-delimited numbers. In this case, you should append a .0 as appropriate to make the version number match the format required by AD RMS.

To stop excluding applications

1. Open the Active Directory Rights Management Services console and expand the AD RMS cluster.
2. In the console tree, expand **Exclusion Policies** , and then click **Applications** .
3. Do one of the following:
    - To disable all application exclusions, in the **Actions** pane, click **Disable Application Exclusion** .
    - To disable a specific application exclusion, in the results pane, select the excluded application.
4. In the **Actions** pane, click **Delete** , and then click **Yes** to confirm the removal.

Exclude Lockbox Versions

Applies To: Windows Server 2008 R2, Windows Server 2012

Lockboxes are used to store a user's private key. If a vulnerability is found in a certain version of a lockbox, a new lockbox is released by Microsoft. You can ensure that clients use a minimum version of the Active Directory Rights Management Services (AD RMS) client software by using the lockbox version associated with the client to exclude the previous versions of the AD RMS client software. When you enable this feature, you specify the latest minimum lockbox version that was signed by the Microsoft Activation Service. You then enable lockbox exclusion on the each AD RMS cluster on which you want it to take effect. All certification and licensing requests are checked to make sure that the lockbox meets the minimum version criteria.

If you have enabled an exclusion based on lockbox version, clients that are using a version of the lockbox software earlier than the specified version cannot acquire rights account certificates (RACs) or use licenses because their requests will be denied. These clients must install a new version of the AD RMS client software to acquire a new lockbox that uses the current version of the software.

If a user who has an excluded lockbox was previously issued licenses for content, the user can still consume that content without acquiring a new lockbox.

Membership in the local **AD RMS Enterprise Administrators** , or equivalent, is the minimum required to complete this procedure.

To exclude lockbox versions

1. Open the Active Directory Rights Management Services console and expand the AD RMS cluster.
2. In the console tree, expand **Exclusion Policies** , and then select **Lockbox** .
3. Click **Enable Lockbox Exclusion** to exclude lockbox versions.
4. Click **Change minimum lockbox version** . The **Lockbox** properties sheet opens.
5. In the **Minimum lockbox version** box, type 5.1.0000.0. By setting lockbox exclusion to that minimum version, you will force the Windows RMS clients in your organization to upgrade to the Windows RMS client for SP2 to consume rights-protected content. Click **OK** .

To stop excluding lockbox versions

1. Open the Active Directory Rights Management Services console and expand the AD RMS cluster.
2. In the console tree, expand **Exclusion Policies** , and then select **Lockbox** .
3. Click **Disable Lockbox Exclusion** to stop excluding lockbox versions.

Additional considerations

- You can also perform the task described in this procedure by using Windows PowerShell. For more information about Windows PowerShell for AD RMS, see http://go.microsoft.com/fwlink/?LinkId=136806