

▶ Introduction To Windows Rights Management Services

Tech Tip
by Philip Cox

► Introduction To Windows Rights Management Services

In today's environments, organizations need to find ways to protect information as it passes through many hands. **Windows AD Rights Management Service (RMS)** is one method to implement that protection. RMS can help protect against careless mishandling as well as intentional unauthorized access to data. To help meet regulatory and legal requirements, the service will also assist with accountability and tracking.

RMS is based on the premise that authors will create information and want to control access to it. Also, user will need to "use" information. In RMS, "publishing" is the act of specifying the rights on specific information. That is the "who" (specific users or groups of users) can access the information, and "how" they can access it (i.e., print, edit, read, email, etc.). The process of validating a user's identity and the rights that user has to the information is known as "using". For example, I create a Word document, then assign the right to read the document to all the users in my domain, but only assign the right to print to users in the Managers group. Then when a user tries to access the information, their identity is validated, rights assigned, and the local application enforces those rights.

Some of those that have tried to implement the technology have run into problems, however, and are wondering how to proceed. In this tip, we'll focus on answering some of the more common questions security professionals have run into while implementing RMS:

- How do I allow access to my users when they are remote?
- If I have 2 Active Directory domains, say internal and DMZ, and set up the RMS in the DMZ, can I make my internal AD users "trusted entities" in the DMZ RMS? What is the best method to do this?
- How do I set default permissions for the RMS?

We'll take the questions on individually, but first, we need to set a couple baselines for practical use of an RMS, specifically as implemented using the Windows RMS.

Using RMS and Key Understandings

It is important to understand the following points:

1. If you have consistent connectivity to the RMS, the service will work very well. When you are offline, not so much. In my experience, connectivity to the RMS mother ship makes your life much easier.
2. If you do not have connectivity to the RMS system, you can still protect and "publish" your information, but it is significantly more difficult. You will need to have explicit knowledge of people and groups that need access to the information.
3. You must have connectivity to the RMS system to "use" rights-protected information. Note that you can "use" rights-protected information offline after you gain initial access. This will create a "use" license for that specific piece of information. You need a "use" license for every rights protected piece of information you want to access. There is an option that requires a connection each time, basically disabling client side caching. By default the RMS setup allows client-side caching, which allows documents to be used while offline. It can be set on the document individually or in a template.
4. Rights are granted to a user/computer pair. From a positive standpoint, you can restrict access to a user based on the computer they are accessing the information from --very cool! On the negative side, you need to make sure that you have initially accessed the information from the specific user/computer pair (i.e., got a set of cached credentials for that specific piece of information) while connected to the RMS, before you go offline (noted just above).

► Introduction To Windows Rights Management Services

How do I allow access to my users when they are remote?

RMS uses Web Services to provide the underlying authentication and authorization for the environment. The RMS uses IIS as the front end mechanism to support the Web Services it provides. Given that, there are really two situations here:

1. Accessing the RMS Web Service URL over the Internet
2. No access to the RMS at all (a.k.a. offline)

In scenario 1, you need to ensure the following has been completed:

- Publish the URL of the RMS server externally. The best way to do this securely is to use ISA server or another Web Application firewall type appliance to protect the URL against attacks. If the RMS server is on your internal network, which is highly likely, you do not want to just open the firewall to that URL, you want to protect it in some manner. Using the reverse proxy feature of ISA server is a good method. Also, make sure you use SSL!

Basically you are ensuring users can get to the URL from the Internet. If they have that access, using RMS is effectively the same as being on the corporate network.

In scenario 2, you have to do a couple things differently. First step is before you disconnect from the internal network that has access to the RMS environment. You must:

- Activate your computer
- Create your Rights Account Certificate
- Enroll your client
- Copy Administrative Templates to the local system

The easiest way to do all of these is to open a Microsoft Office application, say Word, then open the following option:

Office Button->Prepare->Restrict Permissions->Manage Credentials.

Once you set up your credentials (note that you need to use your Domain email address), all three of the above steps will be completed for you.

Second, still in scenario 2, you will need to get each document that you will want to access while disconnected, and open them while connected. This process will obtain, and cache, a “use license” for each file that you open, thus allowing you the access when offline. If you do not obtain the “use license” then when you try to open the document, you will get an error about the RMS client not being able to contact the RMS server.

After that, you should be able to use RMS protected documents while “remote.”

If I have 2 Active Directory domains, an internal and DMZ, how would I setup RMS?

The first thing to understand is that an RMS can only provide services to users in its Active Directory domain, not for users in other AD domains. If you want to provide rights management to both domains, you will have to install RMS in each domain. At that point you have two options:

- Create users in each domain, and have them use an account and RMS as appropriate
- Establish trust between the RMS environments

Remember that users can have account certificates (i.e., user/system pair certificates) configured.

In the first scenario, a user would use the specific account (i.e., email address) to authenticate to RMS and create the account certificate, and use it when assigning permissions.

In the second scenario, there are two options:

- **Trusted User Domain (most common):** This allows the licensing servers in one RMS to accept “use” license requests from users in the other RMS. The option allows users to share protected content across the domains. The main consideration is that the user will need

► Introduction To Windows Rights Management Services

connectivity to an RMS server in the “other” environment. If you want to use groups for permission assignment, you will need trust between the Active Directory forests (from a practical standpoint). If you just want to assign permissions to individual users, then Active Directory Trust is not needed. (See [http://technet.microsoft.com/en-us/library/dd983944\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd983944(WS.10).aspx) and <http://technet.microsoft.com/en-us/library/cc753930.aspx> for more information)

- **Trusted Publishing Domain:** This allows the RMS servers on one environment to issue “use” licenses for information that was originally published in another RMS environment. The main difference between TPD and TUD is that in TPD, you don’t need to connect to the RMS of the trusted RMS. The downside is that you need to exchange the private keys of the RMSes. You will also have to set registry entries to force your client to go only to the one RMS. (see [http://technet.microsoft.com/pt-br/library/dd772677\(WS.10\).aspx](http://technet.microsoft.com/pt-br/library/dd772677(WS.10).aspx) and [http://technet.microsoft.com/en-us/library/dd996639\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd996639(WS.10).aspx) for more information)

Think of it this way, a TPD allows an RMS to decrypt content it did not publish, whereas a TUD requires the client to connect to the RMS that published it.

You will also have to open firewall ports for AD Trust and access to the Web Service on the RMS servers.

How do I set default permissions for the RMS?

The default RMS permissions are set using AD RMS Rights Policy Templates. Templates can be used to configure rights and conditions for a pre-defined set of users. The templates also allow you to apply consistent policies to information. We do not have enough space to cover the details of setting and using templates, see [http://technet.microsoft.com/en-us/library/dd772629\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd772629(WS.10).aspx) for more details.

Conclusion

First, let me say that I like RMS. I think it can be used very successfully and if deployed correctly could help many organizations provide access control and accountability that they only dream of currently. With that said, RMS works best when connectivity to the RMS and associated components (i.e., share where Templates are located) is consistent. While you can use some features of RMS offline, my experience is that it is not practical.

About The Author:

Phil Cox is a principal consultant of SystemExperts Corporation, a consulting firm that specializes in system security and management. He is a well-known authority in the areas of system integration and security.

His experience includes Windows, UNIX, and IP-based networks integration, firewall design and implementation and ISO 17799 and PCI compliance. Phil frequently writes and lectures on issues dealing with heterogeneous system integration and compliance with PCI-DSS. He is the lead author of Windows 2000 Security Handbook Second Edition (Osborne McGraw-Hill) and contributing author for Windows NT/2000 Network Security (Macmillan Technical Publishing).