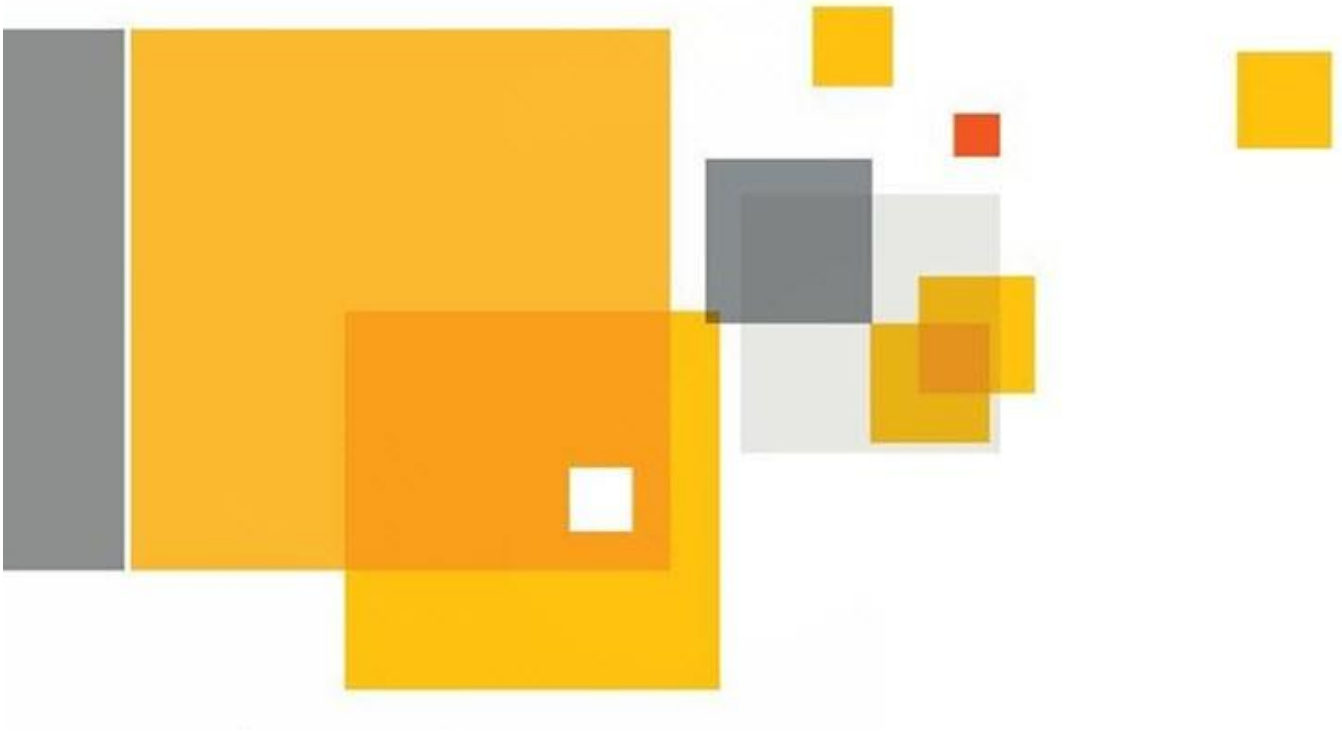


Symantec eDiscovery Platform 7.1.5 Feature Briefing

Microsoft Rights Management Services Integration

This document is about the new Rights Management Services integration feature introduced in Symantec eDiscovery Platform 7.1.5

If you have any feedback or questions about this document please email them to **IIG-TFE@symantec.com** stating the document title.

Feature Description

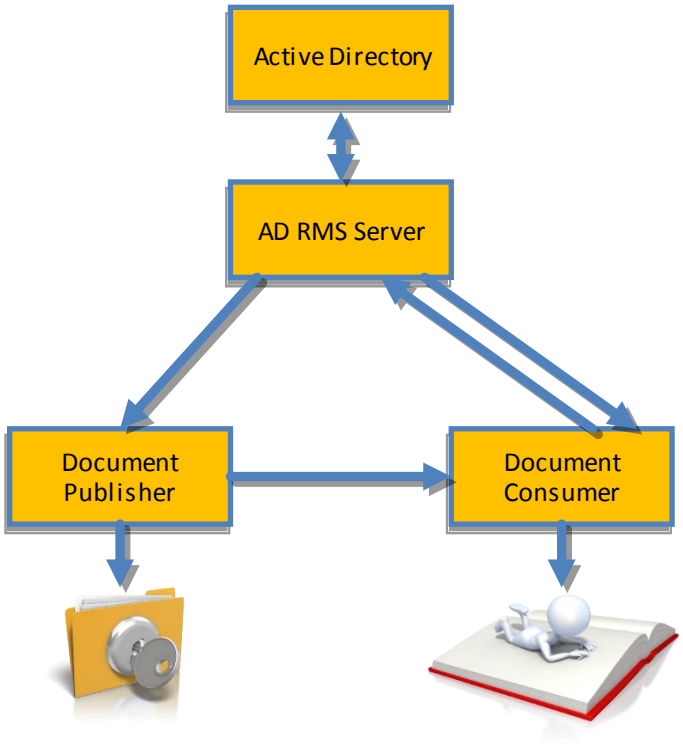
Symantec eDiscovery Platform 7.1.5 introduces a new feature to integrate with Microsoft Rights Management Services (RMS). This feature allows for the decryption of emails and files that have been encrypted by a corporate RMS server so the emails and its content can be processed, indexed reviewed and produced. Documents can be produced in either encrypted or unencrypted format.

Business Value

This feature is designed with users of MS RMS and Symantec eDiscovery Platform in mind. Previously such users were obliged to manually decrypt RMS-encrypted content prior to processing their data in eDiscovery Platform. With the latest release of Symantec eDiscovery Platform 7.1.5 integration with MS RMS has been introduced to allow for the decryption and processing of RMS encrypted emails. This includes email collected from an exchange mailbox, journal and file servers. With this new feature the end to end workflow of identification, collection, processing, review and production is managed completely within the eDiscovery Platform and there is no longer need for manual intervention to decrypt RMS encrypted content.

Underlying Principles

The integration with RMS allows the Symantec eDiscovery platform to act as a client / recipient to the encrypted items. Once the account used to decrypt has the correct use license then the contents can be decrypted and opened



1. The author receives a client and server "licensor certificate" the first time they protect information
2. The author defines a set of usage rights and rules for their file. The application creates a "publishing license" and encrypts the file
3. The author distributes the file to the recipient
4. When the recipient opens the file, the application calls the RMS server which validates the user
5. The RMS server issues a "use license"
6. The "use license" allows the document to be decrypted and opened

Figure 1 – RMS process workflow

Guided Tour

Setting up the link between RMS and the eDiscovery Platform requires some manual steps such as configuring the correct accounts to services and downloading the certificates to each eDiscovery Platform appliance. All of these are configured as part of the installation.

In the eDiscovery Platform interface an account needs to be specified that has the rights to decrypt the content. In most cases a single account is specified that has rights to decrypt all content as this is the preferred method as it allows for a single setup and there is no need to manage different accounts for different sources. A view if the User ID section is provided in Figure 2 and a close-up of the User ID

section is provided in Figure 3

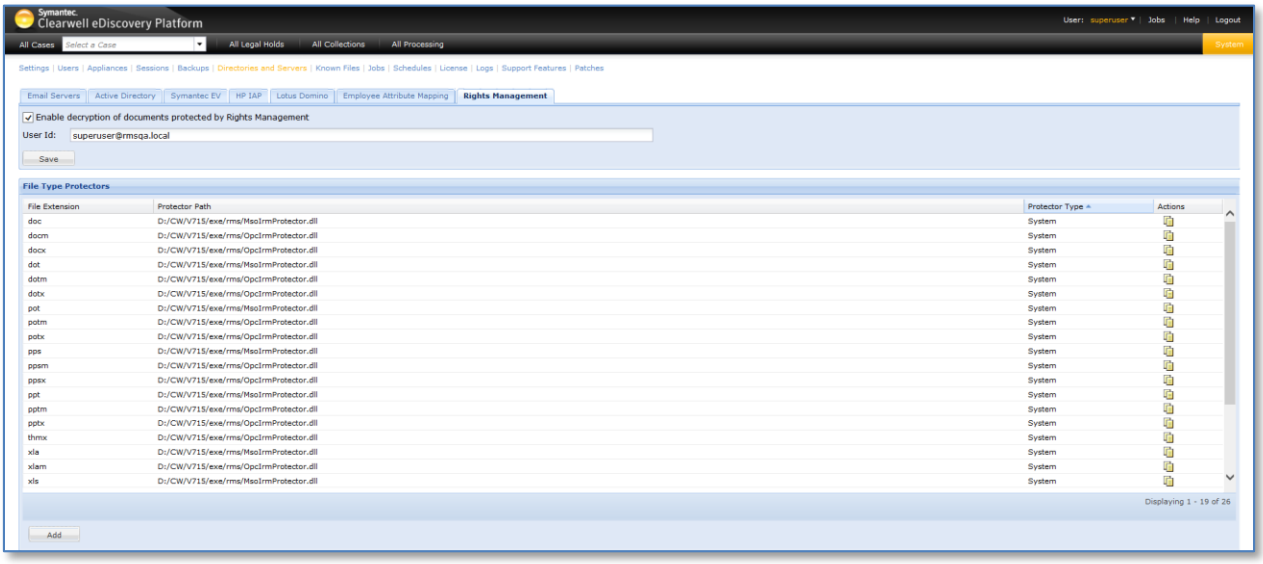


Figure 2 – Rights Management tab

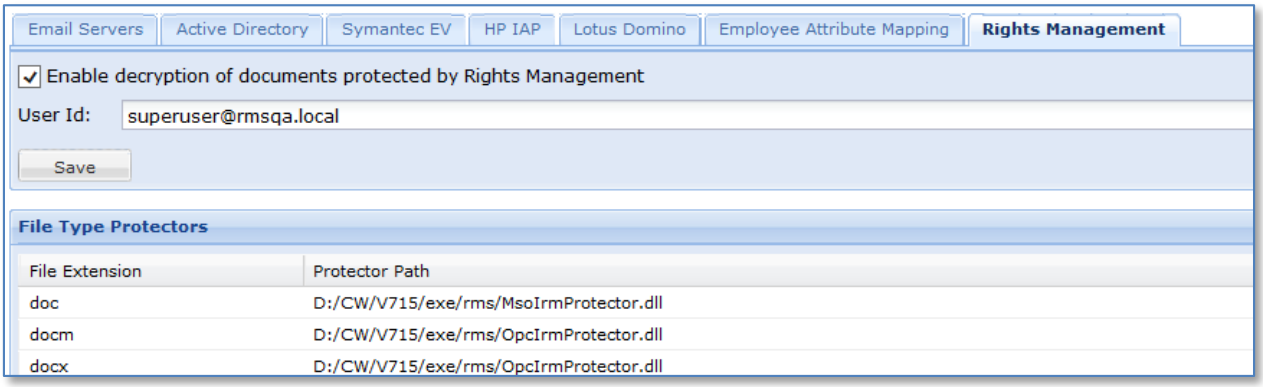


Figure 3 – Rights Management account

The system level settings explained above can be overridden in the case settings if needed as this does allow for a different ID other than the one set at the system level to decrypt content.

This case level override is set under the case processing settings as shown in Figure 4

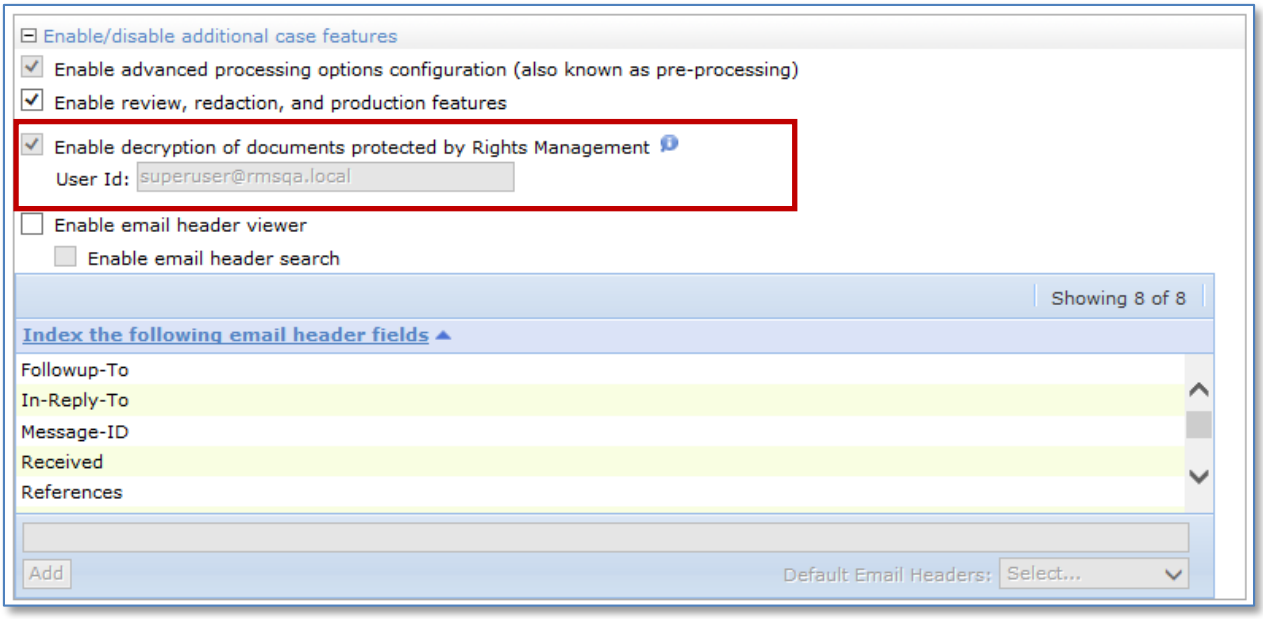


Figure 4 – Case Processing RMS setting

The decryption happens during processing. The workflow was already outlined in Figure 1 where the eDiscovery Appliance represents the Document Consumer. Once processing completes the content can be accessed in the Analysis & Review screen in the same manner as unencrypted content.

There are information icons on the items that were decrypted to inform the reviewer that the content was decrypted by RMS.

As shown in Figure 5 placing the mouse pointer over the RMS icon next to the Doc ID generates balloon text indicating that the message was encrypted by RMS.

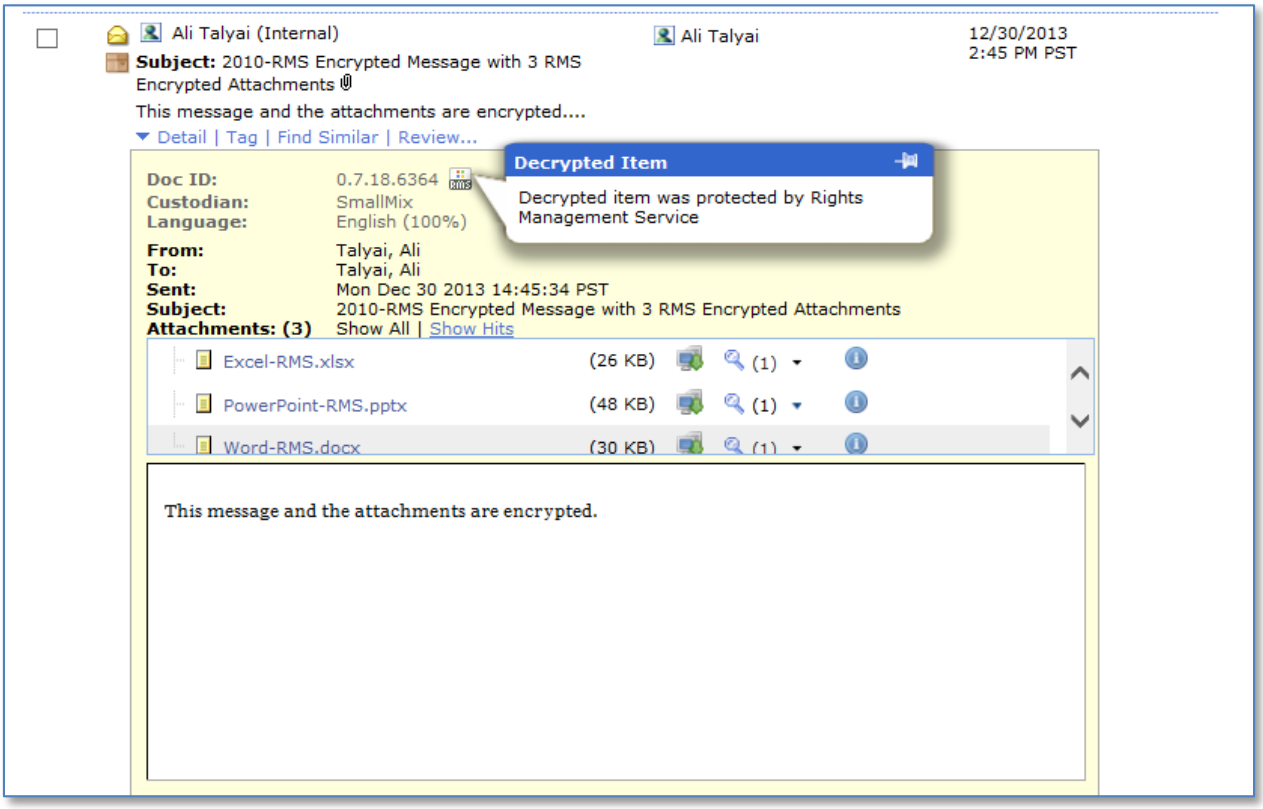


Figure 5 – Encrypted email and some attachments

Similarly, Figure 6 shows that placing the mouse pointer over the blue information icon aligned with each attachment brings up balloon text that tells whether the attachment in question was encrypted prior to processing.

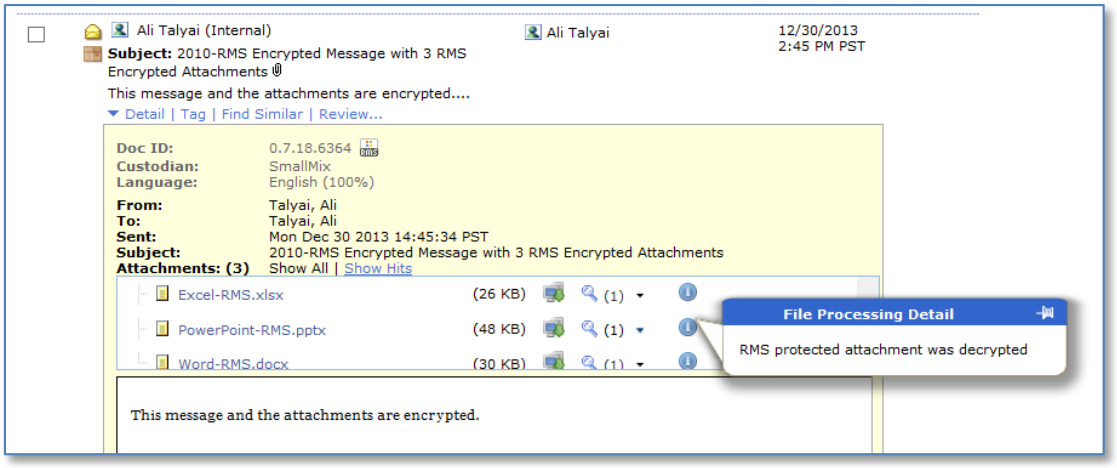


Figure 6 – Decrypted attachment

During Export or production the ability exists to export or produce in native format (encrypted) in decrypted format by marking / unmarking a single check box as shown in Figure 7.

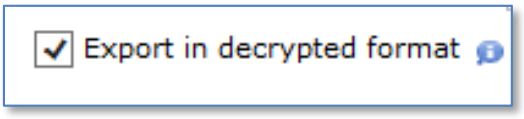


Figure 7 – Export decrypted

Licensing and support considerations

No additional licensing is required. This feature comes included as part of the PPAR module.

About Symantec:

Symantec is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored.

Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at **www.symantec.com**.

For specific country offices and contact numbers, please visit our Web site: **www.symantec.com**

Symantec Corporation
World Headquarters
350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
+1 (800) 721 3934