Microsoft Identity and Access Solutions

Information Protection

Microsoft® Identity and Access (IDA) solutions are a set of platform technologies and products that enable customers to manage identities and access privilege. The dramatic rise in cyber crime and the emergence of related new legislative requirements point to the need for better means to protect digital information. Technologies such as Microsoft Active Directory Rights Management Services (AD RMS) provide persistent, secure protection of information regardless of location or transport mechanism.

Business Need

Electronic communications and files are ubiquitous today. The ease of transmitting e-mail messages and information also increases the risk of unauthorized viewing and distribution.

Organizations seek to augment their security strategies by providing persistent protection that remains with the information even after it leaves the corporate network.

Leaks of confidential information can result in loss of intellectual property, compromised ability to compete, unfairness in purchasing and hiring decisions, diminished customer confidence, and more.

Cost of Information Loss

- Loss of intellectual property such as a trade secret, secret recipe, or product designs can have a huge impact on a company's bottom line.
- Loss of competitive advantage through disclosures of strategic plans or M&A info can potentially lead to a loss of revenue and market capitalization.
- Loss of image and credibility through leaked executive or other sensitive e-mail messages can adversely impact a company's revenue and market share.

Solution Overview

Information Protection

- Safeguard sensitive information by enabling information workers to define how the recipient may use the information: open, modify, print, forward, or take other action.
- Create centralized custom usage policy templates such as "Confidential—Read Only" that can be applied directly to information such as financial reports, product specifications, customer data, and e-mail messages.
- Apply persistent protection to help an organization's strategy that has persistent usage policies. This protection remains with the information, no matter where it goes.

Flexible and Customizable

- Through flexible deployment options and developer tools, organizations can tailor their information-protection solutions to fit into their existing infrastructure.
- Microsoft partners extend RMS with protection for collaborative workflows and files or communications in specific business situations.
- A powerful SDK enables organizations to extend RMS.

Product Overview

Active Directory Rights Management Services (AD RMS) is information protection technology that protects your business's confidential information.

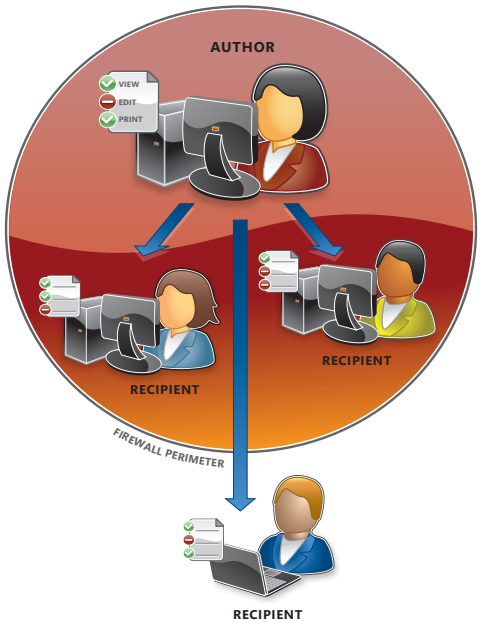
AD RMS includes the server technology that handles certificates and licensing, a desktop update, and the software development kit (SDK). Combining Windows Server™ 2008 features, developer tools, and industry security technologies—including encryption, certificates, and authentication—AD RMS helps organizations create reliable information-protection solutions.

How AD RMS works

Information Author Steps

Establish trusted entities.

- Organizations can specify the entities, including individuals (1), groups of users, computers, or applications that are trusted participants by their AD RMS server.



AD RMS protects information both online and offline, inside and outside of the firewall.

Assign rights to information.

- Using an AD RMS-enabled application, users can easily assign rights (2), such as read-only, to their digital information. These rights reside in a publishing license, which is attached to the information.

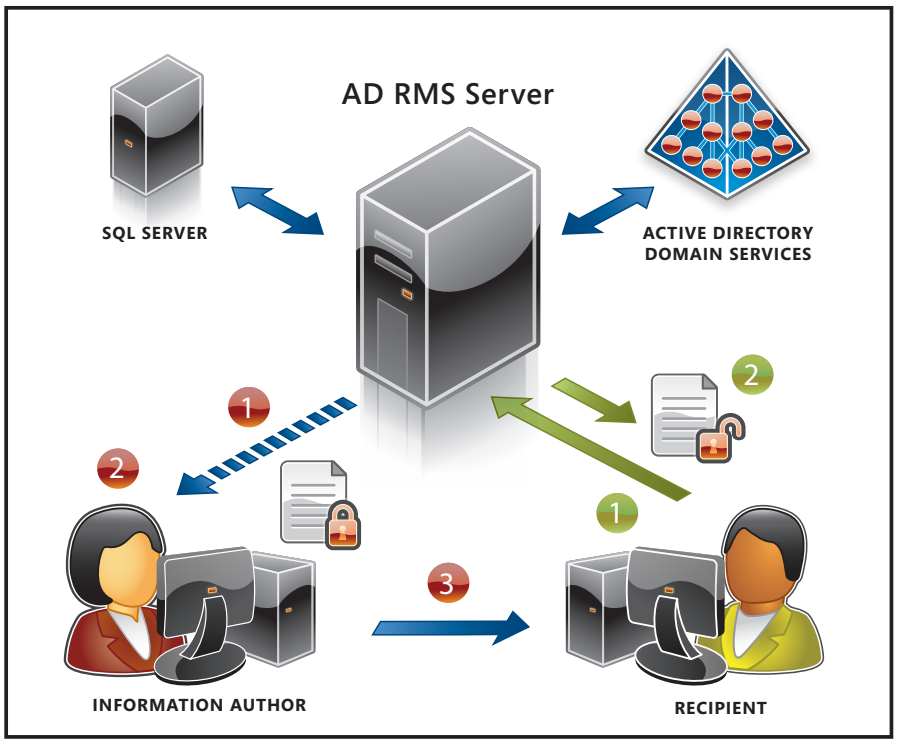
Distribute protected information.

- The application then encrypts the information and the publishing license together. The information and rights remain encrypted during transport (3), extending protection beyond the organization's network.

Recipient Steps

View rights-protected information.

- When the recipient opens rights-protected information, a request goes to the AD RMS server (1) to validate the user's credentials and usage rights. The server issues a use license specifying the rights that apply to the information. The AD RMS-enabled application enforces the usage rights (2) defined by the author or template.



What's new in Windows Server 2008

Windows Server® 2008, Active Directory Rights Management Services (AD RMS) includes a number of functionality and operational improvements over the previous version in Windows Server 2003:

- **Federated Collaboration:** In Windows Server 2008, AD RMS is an Active Directory Federation Services (AD FS) enabled application. This allows enterprises to leverage their established federated relationships to enable collaboration with external entities. For example, an organization that has deployed AD RMS can set up federation with an external entity by using AD FS and can leverage this relationship to share rights-protected content across the two organizations without the need to manage external users within a local domain, leverage Windows Live ID, or require a deployment of AD RMS in both places.
- **Improved installation experiences:** AD RMS is included in Windows Server 2008 as a standard server role. This simplified wizard-based installation performs server validation checks before the installation, which automatically lists and installs all the services that AD RMS depends on during the server role installation. AD RMS also supports server self-enrollment which allows an installation to proceed without having to connect with the Microsoft Enrolment Services as a trust root for content protection, which reduces any operational dependence on network availability
- **Improved administrative experience:** Unlike previous versions, AD RMS administration is done through a MMC snap-in that provides a common management experience as with other server roles. Administrative improvements include centralized template management, and authoring, usage log analysis/reporting and separation of administrative roles with respect to managing the RMS Server.

Additional Resources

www.microsoft.com/InformationProtection

* For creating or viewing rights-protected Microsoft Office documents—spreadsheets, presentations, and e-mail messages—the Professional Edition of the 2007 Microsoft Office system or Office 2003 are required. Other editions allow users to view—but not create—rights-protected Office content.

Windows Server 2008 Active Directory

Microsoft