Oracle Information Rights Management

Oracle IRM Windows Authentication Extension Guide

10gR3

August 2008

Oracle Information Rights Management, Oracle IRM Windows Authentication Extension Guide, 10gR3

Primary Author: Martin Abrahams

Contributing Author: Martin Wykes

The Programs (which include both the software and documentation) contain proprietary information; they are provided under a license agreement containing restrictions on use and disclosure and are also protected by copyright, patent, and other intellectual and industrial property laws. Reverse engineering, disassembly, or decompilation of the Programs, except to the extent required to obtain interoperability with other independently created software or as specified by law, is prohibited.

The information contained in this document is subject to change without notice. If you find any problems in the documentation, please report them to us in writing. This document is not warranted to be error-free. Except as may be expressly permitted in your license agreement for these Programs, no part of these Programs may be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose.

If the Programs are delivered to the United States Government or anyone licensing or using the Programs on behalf of the United States Government, the following notice is applicable:

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the Programs, including documentation and technical data, shall be subject to the licensing restrictions set forth in the applicable Oracle license agreement, and, to the extent applicable, the additional rights set forth in FAR 52.227-19, Commercial Computer Software--Restricted Rights (June 1987). Oracle USA, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

The Programs are not intended for use in any nuclear, aviation, mass transit, medical, or other inherently dangerous applications. It shall be the licensee's responsibility to take all appropriate fail-safe, backup, redundancy and other measures to ensure the safe use of such applications if the Programs are used for such purposes, and we disclaim liability for any damages caused by such use of the Programs.

The Programs may provide links to Web sites and access to content, products, and services from third parties. Oracle is not responsible for the availability of, or any content provided on, third-party Web sites. You bear all risks associated with the use of such content. If you choose to purchase any products or services from a third party, the relationship is directly between you and the third party. Oracle is not responsible for: (a) the quality of third-party products or services; or (b) fulfilling any of the terms of the agreement with the third party, including delivery of products or services and warranty obligations related to purchased products or services. Oracle is not responsible for any loss or damage of any sort that you may incur from dealing with any third party.

Table of Contents

Introduction

This document describes how to activate and configure Windows authentication as an extension to an Oracle IRM deployment based on the Oracle IRM standard rights model.

By default, in the standard rights model, all user accounts are configured to use Oracle IRM username and password authentication (otherwise known as “standard authentication”). This is a simple mechanism that has no dependency on any other part of your corporate infrastructure, and that is equally applicable to both internal and external users.

However, for many deployments there is a requirement to use Windows authentication for internal users. In the standard rights model, this is supported by activating the Windows Authentication extension and making some configuration changes that ensure that the Oracle IRM Management Website is accessible using Windows authentication.

The set of tasks is as follows:

1. Activating the Windows Authentication extension.
2. Configuring the Management Website settings so that the user creation page exposes the new options.
3. Configuring the website folder so that its files are accessible to domain users.
4. If relevant, ensuring that IIS can authenticate Windows user accounts in a Kerberos environment.
5. Configuring browser settings of relevant users so that the Management Website is a Trusted Site.

   This avoids the need for users to specify Windows credentials when accessing the website.

In order for Windows authentication to succeed, the Management Website and Oracle IRM Server (“the license server”) need to be able to verify user credentials by reference to the relevant domain controllers. You need to ensure that the necessary domain control communications are possible from the network location of the Oracle IRM applications. Additional configuration might be required if you use Kerberos authentication in your network.

Activating the Extension

Activating extensions is a **Service Owner** task.

To activate the extension, proceed as follows:

1. Browse to the Oracle IRM Management Website and log in as a **Service Owner**.
2. Go to the **Extensions** page.
3. Click the **Activate** button for the Windows Authentication extension.

When you activate the extension, the management website updates the **Settings** page to expose some new options. You need to configure those options as described in the following section.

Configuring Settings

When you activate the Windows Authentication extension, the **Settings** page exposes some new options.

1. Browse to the Oracle IRM Management Website and log in as a **Service Owner**.
2. Go to the **Settings** page.
3. Use the **Authentication type** settings to control whether the **Users** page allows the creation of user accounts with Oracle IRM ("standard") authentication only, Windows authentication only, or whether the page allows the website user to choose what type of authentication a new account should use.
4. Click Browse to the Oracle IRM Management Website and log in as a **Service Owner**.
5. Click **Save**.

If you chose Windows authentication only, the **Users** page offers an additional field in which you specify the domain account to associate a new Oracle IRM account with.

If you chose Both, the **Users** page provides the option to select the authentication type. If the user selects the Windows option, the field for specifying the domain account appears.

You can change the settings at any time.

Configuring the Website Folder for Domain User Access

Users with administrative rights need to be able to use the management website.

If using Windows authentication, the website folders need to allow **Read** access to domain users, as follows:

1. Start Windows Explorer and browse to the folder containing the Oracle IRM Management Website files, for example, **C:\InetPub\wwwroot\SealedMedia Management**.
2. Select the **smweb** subfolder and access its **Properties** dialog.
3. Use the **Security** tab to add **Read** permissions for the **Domain Users** group.
4. Click **OK**.

Enabling Windows Authentication in a Kerberos Environment

If you use Kerberos authentication in your network, you need to ensure that the management website can authenticate Windows user accounts successfully. There are two options:

1. Enable IIS to authenticate accounts using Kerberos. This might involve configuring a **Service Principal Name**. An MSDN article at http://tinyurl.com/kkxqb provides more information.
2. Enable IIS to authenticate accounts using NTLM in preference to Kerberos. An MSDN article at http://tinyurl.com/jq63f provides more information.

Configuring the Website as a Trusted Site in User Browsers

To avoid the need for users to specify their Windows credentials when they access the SealedMedia Management Website, you can use browser settings to register the website as a Trusted Site, as follows:

1. In Internet Explorer, go to **Tools - Internet Options**.
2. Select the **Security** tab.
3. Select **Trusted Sites** and click the **Sites...** button.
4. Add the management website to the list of sites, for example, **smweb.abc.com**.

   Omitting the protocol prefix (http://) enables the site to remain trusted if you decide to enable SSL.
5. Deselect the **Require server verification (https:) for all sites in this zone** option.
6. Click **Add** and then **OK**.

If you have a large numbers of users, you might use an Active Directory group policy for this configuration.

Conclusion

The configuration of the Windows Authentication option is now complete.

When you use the Oracle IRM Management Website to create user accounts, with Windows authentication, the website uses a different notification email that does not mention a username or password. When users open sealed documents, login is transparent. Similarly, when users access the management website or the management console, login is transparent.