ORACLE®

PRIMAVERA

Primavera Portfolio Management 8.0
Enabling Single Sign-On

Copyright © 1999-2010, Oracle and/or its affiliates.

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.

Oracle is a registered trademark of Oracle Corporation and/or its affiliates. Other names may be trademarks of their respective owners.

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.

This document describes the procedures to follow to enable Primavera® Portfolio Management 7.5 to work with two different types of Single Sign-On:

1. Integrated Windows Authentication
2. Integration with 3rd party Single Sign-On products

Note: in a distributed installation of Primavera® Portfolio Management ("Scale Out"), the below described settings must be made on all Primavera® Portfolio Management application servers.

1. Integrated Windows Authentication

The Primavera® Portfolio Management application can be integrated with Microsoft Windows domain authentication, such that a user, who has been authenticated by a Microsoft Windows domain controller, will automatically be authenticated with Primavera® Portfolio Management as well. By enabling this functionality users will not be prompted for their usernames and passwords by Primavera® Portfolio Management, but will be automatically logged into the Primavera® Portfolio Management application without the need to use the login dialog screen.

Note: This feature works only for users who have logged into a Microsoft Windows domain via NT/Windows 2000 authentication and whose NT/Windows 2000 user name is identical to their login name in Primavera® Portfolio Management. If these do not match exactly, when accessing Primavera® Portfolio Management the user will be presented with the regular Primavera® Portfolio Management login dialog screen, together with the message "invalid username/password".

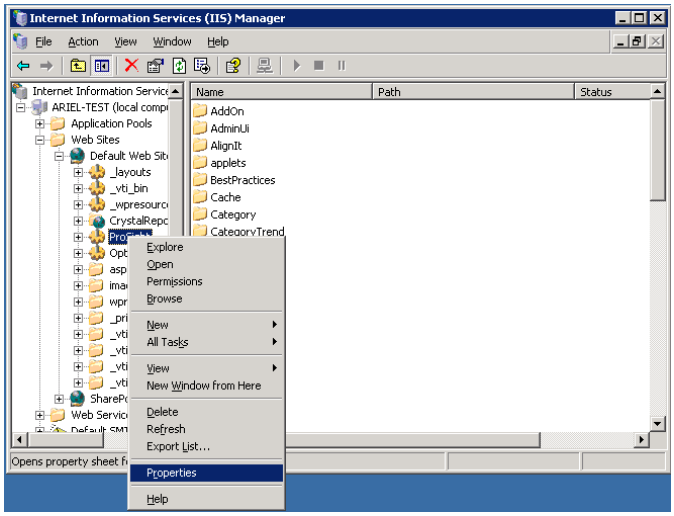
This chapter outlines the process of enabling Integrated Windows Authentication for Primavera® Portfolio Management.

1.1 Open **Internet Information Services (IIS) Manager** by clicking:

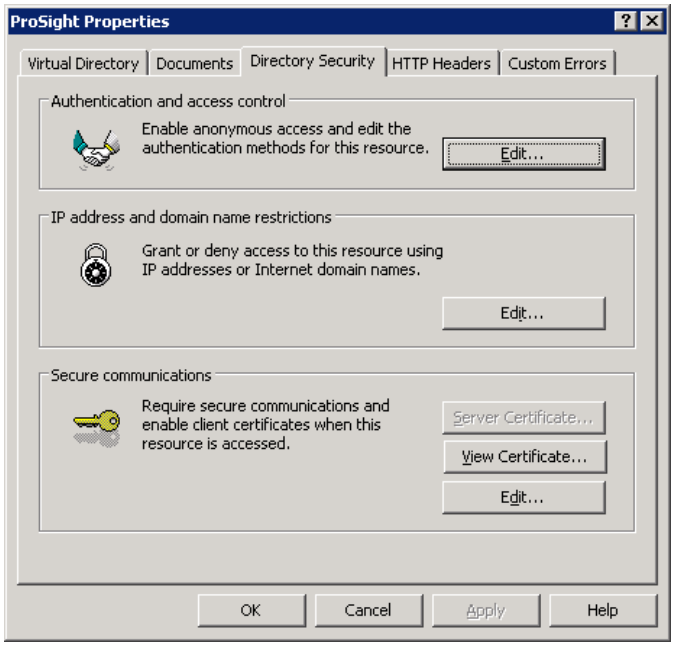
Start -> Programs -> Administrative Tools -> Internet Information Services (IIS) Manager

Navigate to the ProSight virtual directory.

Right-click, then select Properties.



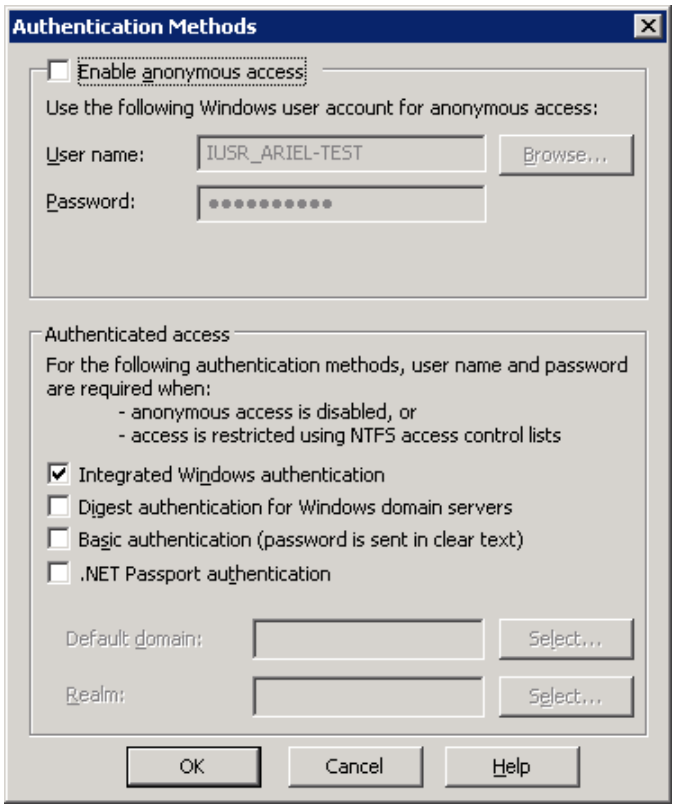
1.2 Select the Directory Security tab, and then click the “Edit…” button located in the area “Anonymous access and authentication control”.



1.3 Uncheck the “Enable anonymous access” checkbox.

Click “OK” to close the “Authentication Methods” dialog, and then click “OK” again to close the “ProSight® Properties” dialog.

This completes the process. Exit the Internet Information Services (IIS) Manager.



2. Integration with 3rd party Single Sign-On products

The Primavera® Portfolio Management application can be integrated with 3rd party Single Sign-On (SSO) products, such that a user, who has been authenticated by a 3rd party SSO product, will automatically be authenticated with Primavera® Portfolio Management as well. By enabling this functionality users will not be prompted for their usernames and passwords by Primavera® Portfolio Management, but will be automatically logged into the Primavera® Portfolio Management application without the need to use the login dialog screen.

Note: This feature works only for users who have logged in using the 3rd party SSO product and whose 3rd party SSO product user name is identical to their login name in Primavera® Portfolio Management. If these do not match exactly, when accessing Primavera® Portfolio Management the user will be presented with the regular Primavera® Portfolio Management login dialog screen, together with the message “invalid username/password”.

This chapter outlines possibilities for enabling integration with 3rd party SSO products for Primavera® Portfolio Management 7.5. For the exact procedure to follow, please refer to the 3rd party SSO product manuals.

a. 3rd party SSO Product Requirements

In order to be able to integrate with Primavera® Portfolio Management, the 3rd party SSO product must be able to fulfill the following requirements:

1. Ability to intercept access to Primavera® Portfolio Management web server through Internet Explorer
2. Ability to set a HTTP header variable to a fixed value
3. Ability to set another HTTP header variable to the name of the authenticated user

Note that Primavera® Portfolio Management does not accept “cookies” as an authentication method.

b. Primavera® Portfolio Management Configuration for integration with 3rd party SSO Product

Primavera® Portfolio Management can be configured to accept any HTTP header variables. The following registry values control the names and values of the HTTP header variables used for integration:

Note: all registry values discussed below may be inserted into the Registry under the key:
HKEY_LOCAL_MACHINE\SOFTWARE\Oracle\Primavera Portfolio Management\Portfolios\Server\UI

Registry Value "SSO Authentication Type HTTP Header Name" (String).
Data: name of the HTTP header variable containing the authentication type.
Default: "AUTH_TYPE"
Explanation: By default, the type of SSO Authentication is carried in the HTTP header variable called "AUTH_TYPE". If, for any reason, a given SSO product is unable to use this particular header variable, this registry entry can be used to cause PPM to look at a different HTTP header variable.
Note: Primavera® Portfolio Management uses the "raw" HTTP header interface. Therefore, under certain circumstances the name of the HTTP header within Primavera® Portfolio Management should be configured with an "HTTP_" prefix.

Registry Value "SSO Authentication Type HTTP Header Value" (String).
Data: value to be assigned to the "SSO Authentication Type HTTP Header" (see above), which indicates that the SSO product will perform user authentication.
Default: "Negotiate"
Explanation: by default, a value of "Negotiate" in the HTTP header variable "AUTH_TYPE" is interpreted by PPM to mean that a SSO product is responsible for user authentication. If, for any reason, a given SSO product assigns a different value to the HTTP header variable, then this registry entry can be used to cause PPM to accept the value which the SSO product assigns.

Registry Value "SSO Authenticated User HTTP Header Name" (String).
Data: name of the HTTP header variable containing the user name of the user authenticated by the SSO product.
Default: "LOGON_USER"
Explanation: by default, the name of the user authenticated by the SSO product, should be placed in a HTTP header variable called "LOGON_USER". If, for any reason, a given SSO product is unable to use this header variable, this registry entry can be used to cause PPM to accept the name of the authenticated user in a different HTTP header variable.
Note: Primavera® Portfolio Management uses the "raw" HTTP header interface. Therefore, under certain circumstances the name of the HTTP header within Primavera® Portfolio Management should be configured with an "HTTP_" prefix.

c. Example

A well known SSO product called Netegrity SiteMinder is able to set "custom HTTP headers". This can be seen in the SiteMinder log file. These "custom HTTP headers", when seen by Primavera® Portfolio Management, are prefixed by "HTTP_". Therefore, a typical Netegrity SiteMinder setup is as follows:

Configure Netegrity SiteMinder to create a custom HTTP header called "AUTH_TYPE", whose value is set to "Negotiate". Also configure Netegrity SiteMinder to create a “Response Attribute” custom HTTP header called "AUTH_USER", and set its value to the login name (id) of the authenticated user. See figure 1.

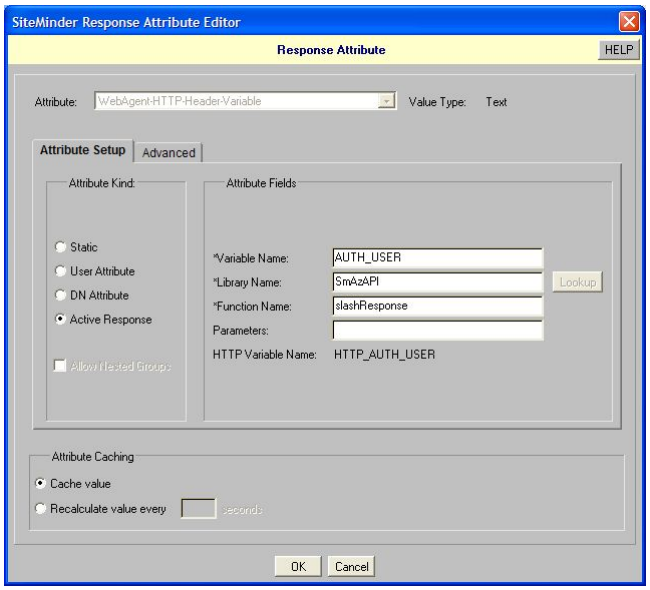


Figure 1

Configure the appropriate Netegrity SiteMinder policy to send these responses. See figure 2.

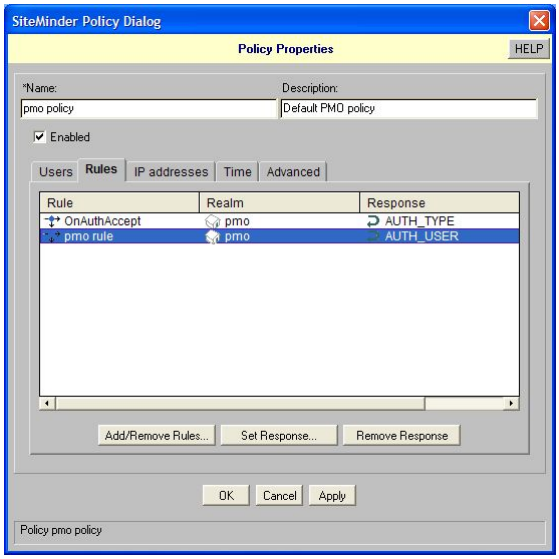


Figure 2

Configure Primavera® Portfolio Management accordingly by creating the following registry string values:

- "SSO Authentication Type HTTP Header Name" should have a value of "HTTP_AUTH_TYPE".
- "SSO Authentication Type HTTP Header Value" should have a value of "Negotiate".
- "SSO Authenticated User HTTP Header Name" should have a value of "HTTP_AUTH_USER".

The above configuration was tested with Netegrity SiteMinder 5.5.