User Authentication Methods

WorkPlace 2016

(Version 16.00.00.00 and Greater)
WorkPlace User Authentication Methods

Copyright
Copyright © 2016 Paramount Technologies. All rights reserved. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Paramount Technologies. Notwithstanding the foregoing, the licensee of the software with which this document was provided may make a reasonable number of copies of this document solely for internal use.

Trademarks
WorkPlace is a registered trademark of Paramount Technologies and is registered in the United States and other countries. Microsoft, Windows, Windows Server and Windows Vista are either registered trademarks or trademarks of Microsoft Corporation or its affiliates in the United States and/or other countries. The names of actual companies and products mentioned herein may be trademarks or registered marks - in the United States and/or other countries - of their respective owners. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, e-mail address, logo, person, place, or event is intended or should be inferred.

Intellectual property
Paramount may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Paramount, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Warranty disclaimer
Paramount Technologies disclaims any warranty regarding the sample code contained in this documentation, including the warranties of merchantability and fitness for a particular purpose.

Limitation of liability
The content of this document is furnished for informational use only, is subject to change without notice, and should not be construed as a commitment by Paramount Technologies. Paramount Technologies assumes no responsibility or liability for any errors or inaccuracies that may appear in this manual. Neither Paramount Technologies nor anyone else who has been involved in the creation, production or delivery of this documentation shall be liable for any indirect, incidental, special, exemplary or consequential damages, including but not limited to any loss of anticipated profit or benefits, resulting from the use of this documentation or sample code.

License agreement
Use of this product is covered by a license agreement provided with the software product. If you have any questions, please call the Paramount Technologies Support at 800.725.4408 (in the U.S. or Canada) or +1.800.725.4408.

Publication date
July 2016
WorkPlace User Authentication Methods

**SSO**
Single Sign On. This option allows for usage of 3rd party authentication services such as Windows Live, Google and custom providers. When hosting WorkPlace in the cloud or in a DMZ outside of the internal network this option can provide access to the local Active Directory via Active Directory Federation Services (AFDS). All SQL backend operations are performed using a shared user account. Under this option the user names are the email addresses of the user.

**SQL**
SQL Name and Password are used and passed directly through to the SQL Server. This requires the user to be setup on the SQL server as a physical user and the user must have access to all databases that WorkPlace requires access. It is recommended that the SQL password encryption option is enabled in WorkPlace when using this method. Since the users have access to the databases a user could use Excel or other connectable applications to access WorkPlace data if non-encrypted passwords are allowed.

**SQLSHARED**
SQL Name and Password for authentication only. All backend SQL operations are performed using a shared SQL user account. This method secures access to the physical database as the user account does not have access to any of the physical databases. This method is ideal in environments where other SQL applications are used and a shared SQL name and password are desired.

**NT**
The Active Directory user name that the user logged into Windows with (Integrated Authentication) or the Active Directory user that was entered on the Basic Authentication window (Non-Integrated Authentication) is simply passed through to the SQL Server. This method as well as the SQL option both have the same drawbacks in that the user could use an external application to get access to the SQL databases unless a firewall is enabled. This method also suffers from the Double-Hop syndrome whereas the SQL Server, Web Server and Client machines must all be enabled for delegation at the Active Directory level as standard Kerberos authentication does not allow the client browser to authenticate to the web server and then allow the web server to impersonate the credentials to the SQL server.
WorkPlace User Authentication Methods

**NTSHARED**
The Active Directory user name that the user logged into Windows with (Integrated Authentication) or the Active Directory user that was entered on the Basic Authentication window (Non-Integrated Authentication) is used to identify the user to WorkPlace. The SQL backend operations are all performed using a shared SQL account. This method is the preferred model in larger organizations as the user cannot access the databases via external applications and all password and account management is at the Active Directory level. This option also eliminates the double-hop issue with Active Directory.

**FORMS**
The Active Directory user name that the user logged into Windows with is used to authenticate against the WorkPlace Web Server using IIS Forms Authentication. Once authenticated against the web site, the user’s credentials are passed to the WorkPlace solution which will authenticate against the application level security. All SQL backend operations are all performed using a shared SQL account. This method is a preferred model in larger organizations as the user cannot access the databases via external applications and all password and account management is at the Active Directory level. This option also eliminates the double-hop issue with Active Directory.

**APP**
User accounts and passwords are managed by WorkPlace exclusively and all SQL backend operations are performed using a shared user account. Under this option the user names are the email addresses of the user. The key benefit with this method is that if users forget their passwords they can simply click a “forgot password” button on the logon page and reset their own passwords. This method is ideal for environments where account management at the SQL or NT level is not ideal or empowering the user to manage their own password cuts administrative overhead.