

SolarWinds Technical Reference

Using Active Directory for SolarWinds Authentication

Orion and Microsoft's Active Directory (AD) Integration	1	This paper examines how Microsoft's Active Directory authentication works with Orion Core. This applies to APM 4.0, NPM, and all NPM modules running on Orion Core 2010.2 or newer.
Adding AD Authentication for AD Users	2	
Strategies for Using AD.....	4	
Troubleshooting AD Integration Issues.....	5	
Where to Learn More	6	

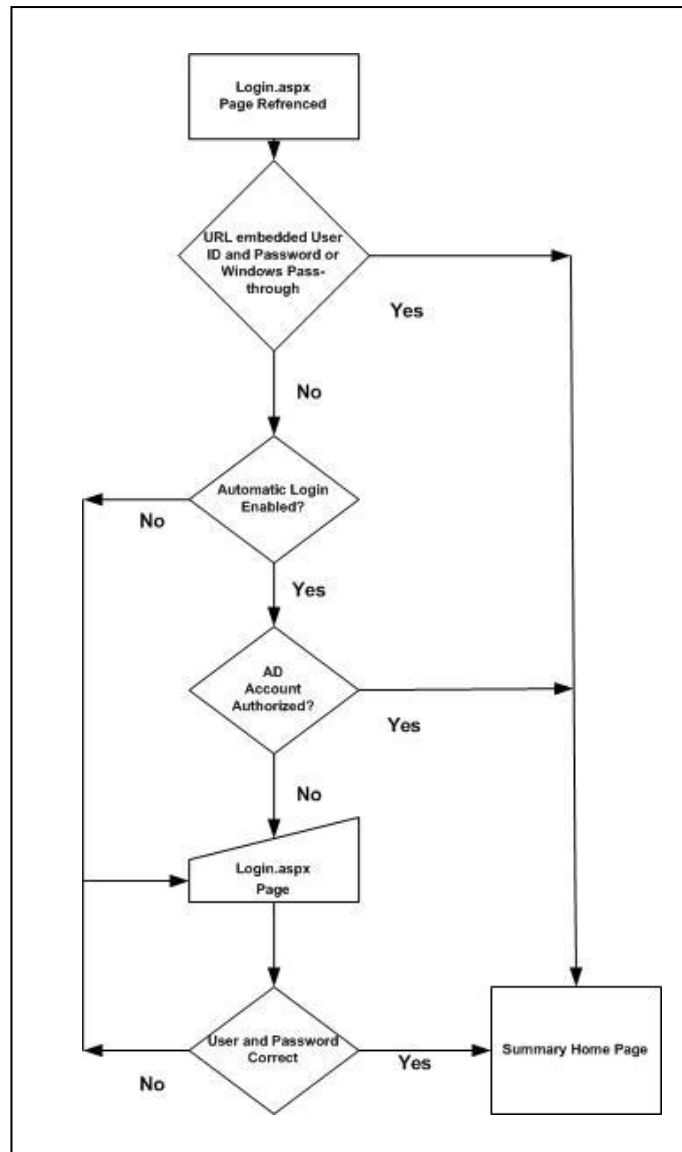
Copyright© 1995-2011 SolarWinds. All rights reserved worldwide. No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of SolarWinds. All right, title and interest in and to the software and documentation are and shall remain the exclusive property of SolarWinds and its licensors. SolarWinds Orion™, SolarWinds Cirrus™, and SolarWinds Toolset™ are trademarks of SolarWinds and SolarWinds.net® and the SolarWinds logo are registered trademarks of SolarWinds All other trademarks contained in this document and in the Software are the property of their respective owners.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Document Revised: 3/31/2011

Orion and Microsoft's Active Directory (AD) Integration

Several SolarWinds products now contain the ability to add user and group access using AD. When a standard such as AD is implemented, the implementer can typically choose from a set of options. This paper is aimed at providing a deeper level of understanding on how AD works with SolarWinds Orion core than that provided by the Administrator's Guides (AGs). The AGs should be used for step-by-step instructions on using AD for authentication, so that will not be addressed here.



The user authentication experience differs depending on how user authentication is set up. For users that have their user name and password embedded in the URL used to access Orion, they will go directly to their product home page, bypassing any other authentication. The experience will be the same for successful AD authentication. Although the Login.aspx page is referenced for all users, the above two types of users will never see the login screen unless authentication fails. If the authentication fails due to issues such as password mismatch with an URL embedded user ID/password or an AD error, these users will be directed to the login.aspx page where they are prompted for a user ID and password. Users that are only defined in Orion and do not use URL embedded authentication will always login from the login.aspx screen.

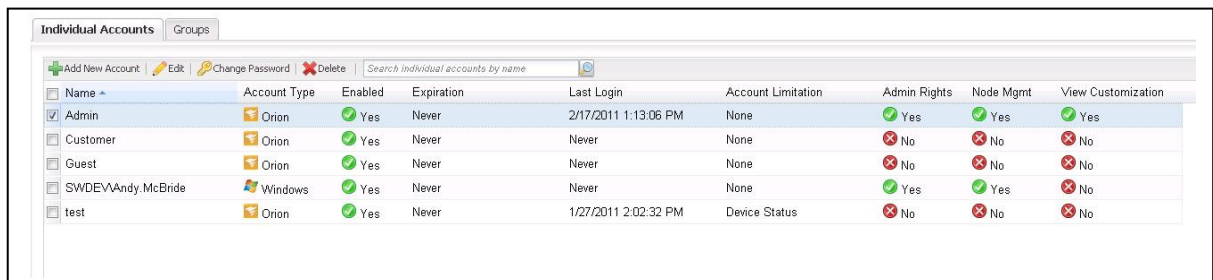
While it may initially seem that using a URL embedded ID and password offers the same features as AD authentication, it should be noted that the ID and password embedded in the URL are in plain text. Anyone who captures packets between the embedded URL user and Orion can discover these user ID and password combinations. Likewise, anyone who views the URL will also have access to the user ID and password.

Some Orion products have had the ability to use Windows Pass-through Security. This feature was implemented as a workaround until SolarWinds AD authentication was developed. For users that have Windows Pass-through Security enabled, the Orion Admin should remove Pass-through security prior to transitioning to AD security. If Windows pass-through is not removed it will interfere with AD login. For more information about pass-through security, see the appropriate [Administrator Guide](#).

When user access is granted from within a web application, the application is responsible for storing and verification of accounts and passwords. When the web application takes advantage of AD authentication, authentication is processed between the application and AD and is transparent to users who are already authenticated into AD. This is commonly known as “single sign-on”.

Adding AD Authentication for AD Users

AD account authentication for Orion is set in the Settings interface under **Accounts > Manage Accounts**. This interface is shown below.



Name	Account Type	Enabled	Expiration	Last Login	Account Limitation	Admin Rights	Node Mgmt	View Customization
<input checked="" type="checkbox"/> Admin	Orion	Yes	Never	2/17/2011 1:13:06 PM	None	Yes	Yes	Yes
<input type="checkbox"/> Customer	Orion	Yes	Never	Never	None	No	No	No
<input type="checkbox"/> Guest	Orion	Yes	Never	Never	None	No	No	No
<input type="checkbox"/> SWDEV\Andy.McBride	Windows	Yes	Never	Never	None	Yes	Yes	No
<input type="checkbox"/> test	Orion	Yes	Never	1/27/2011 2:02:32 PM	Device Status	No	No	No

Orion Manager Users Interface

The top tabs allow you to choose between Individual Accounts and Groups. The screens and options for Group and Individual accounts are the same, so we will examine the Individual Accounts screen only. By choosing the Windows Individual Account tab then clicking **Add New Account**, we are taken to the Add New Account screen shown below.

Add New Account

SELECT TYPE | **ENTER ACCOUNT INFO** | DEFINE SETTINGS

Enter Windows individual account

ACTIVE DIRECTORY OR LOCAL DOMAIN AUTHENTICATION

User name: swdev.local\andy.mcbride
This user has permission to search for accounts on Active Directory or local domain

Password: ••••••••

SEARCH FOR ACCOUNT

User name: swdev* [Search]
Use Domain\Username format

ADD USERS

Select users to add:

Account Name	Selected
SWDEV\jame.colom	<input type="checkbox"/>
SWDEV\jakub.musil	<input type="checkbox"/>
SWDEV\james.lara	<input type="checkbox"/>
SWDEV\jamie.kellerstrass	<input checked="" type="checkbox"/>
SWDEV\Jan.Manek	<input type="checkbox"/>
SWDEV\Jan.Petzelka	<input type="checkbox"/>
SWDEV\Jan.Provail	<input type="checkbox"/>
SWDEV\jan.stoklasa	<input checked="" type="checkbox"/>
SWDEV\Jan.Tauwinkl	<input type="checkbox"/>
SWDEV\Jaroslav.Blazek	<input type="checkbox"/>
SWDEV\jason.ferree	<input checked="" type="checkbox"/>
SWDEV\jane.Huberman	<input type="checkbox"/>

34 matches found

3 accounts selected

SWDEV\jamie.kellerstrass	<input checked="" type="checkbox"/>
SWDEV\jan.stoklasa	<input checked="" type="checkbox"/>
SWDEV\jason.ferree	<input checked="" type="checkbox"/>

< BACK | NEXT > | CANCEL

Windows Add New Individual Account Screen

The top section of the above screen, Active Directory or Local Domain Authentication, is where you specify the account you will use to add users to Orion using AD. This account must have **administrative rights in the domain(s) you will be searching**. The center area of this screen gives you a search box to specify user names, or partial usernames and standard AD wildcard search characters. To begin a search, fill in the top 2 sections we just reviewed and click **Search**. That will populate **Select users to add** with users from the specified domain meeting the specified search criteria. Checking a user in this box will make that user also show up in the accounts selected box. Clicking the red **X** next to a user name will deselect that user. Once all users are selected, clicking next will take you to the Orion account settings page (seen below) where you can specify the Orion product experience for those users.

Add New Account

SELECT TYPE | ENTER ACCOUNT INFO | **DEFINE SETTINGS**

Define settings for Orion individual "billy bob" account

Account Enabled	<input type="checkbox"/> Yes	Disabled accounts cannot log in.
Account Expires	<input type="text" value="Never"/>	This account cannot log in after this date. Enter "Never" for accounts that never expire.
Disable Session Timeout	<input type="checkbox"/> No	If session timeout is disabled, this account will stay logged in indefinitely.
Allow Administrator Rights	<input type="checkbox"/> No	Accounts with Admin rights can Add and Edit other Accounts and reset Passwords.
Allow Node Management Rights	<input type="checkbox"/> No	Accounts with Node Management role can manage nodes.
Allow Account to Customize Views	<input type="checkbox"/> No	Enable this to allow the Account to customize the Views. Any changes made to a View are seen by all Accounts with the same View.
Allow Account to Clear Events, Acknowledge Alerts and Syslogs	<input type="checkbox"/> Yes	Enable this to allow the Account to Acknowledge/Clear Events from the Alerts page.
Allow Browser Integration	<input type="checkbox"/> Yes	Browser Integration allows you to utilize tools on the client browser that are not available in the Orion Web Console. Community strings will not be sent to the browser unless explicitly enabled. Set this to a valid .wav file to enable audible alerts via the web browser.
Alert Sound	<input type="text" value="No Alert Sounds"/>	Set this to a valid .wav file to enable audible alerts via the web browser.
Number of Items in the breadcrumb list	<input type="text" value="50"/>	If this value is set to 0 - all items will be shown within breadcrumbs directly.

Account Limitations

There are no account limitations defined. To create account limitations, click the "Add Limitation" button.

Default Menu Bar and Views

Select the menu bar for this account. To view the contents of each menu bar, go to the [Customize Menu Bars](#) page.

Home Tab Menu Bar	<input type="text" value="Default"/>
Network Tab Menu Bar	<input type="text" value="Network_TabMenu"/>
APM Tab Menu Bar	<input type="text" value="APM_TabMenu"/>
IPAM Tab Menu Bar	<input type="text" value="IPAM_TabMenu"/>
IPSLAM Tab Menu Bar	<input type="text" value="IPSLAM_TabMenu"/>
NTA Tab Menu Bar	<input type="text" value="NTA_TabMenu"/>
Virtualization Tab Menu Bar	<input type="text" value="Virtualization_TabMenu"/>

Orion User Account Settings

Again, AD authentication allows a user or group access to the Orion Web Console but does not directly specify the level of access for that user or group.

Strategies for Using AD

Once AD authentication is in place, the AD authenticated user will be sent to the Orion home page as defined in the existing "Edit *username* Account" page. This means that after access is achieved the same rules and methodologies apply for Orion users and groups as they did before AD authentication was a feature. This flow can be used to greatly simplify user management in Orion.

Most Orion deployments require a handful of levels of access and customization. An administrator can simplify management by creating planning for the user types that are expected to require access. These may be user groups such as "Help Desk", "Management", "WAN Engineers", "NOC Users" and perhaps "Admins". Adding AD groups into the AD domain before adding individuals into the Orion Admin web console can save a lot of administrative work.

Sample Scenario

- Environment - A large number of users require the same access; use the same modules, reports, views, and alerts. A few other users require a high degree of control and customization on a per user basis.
- Solution – Create an AD group for these common users in AD. Then add that AD group into the SolarWinds product and assign the specific privileges with the Admin interface. Then add each of the high level users, using their Individual AD accounts, again granting the level of access required for each user in the Admin interface.

Orion implementations can operate "user administration free" by assigning users to AD groups according to their operational needs. All of the granting or removal of Orion access would be accomplished by AD.

Troubleshooting AD Integration Issues

Problem: I cannot add AD users by entering the user ID and password.

Solution: Users are added by searching for the user account using an authorized administrative account. AD Users are not added by entering the user ID and password of the user you wish to add. For more information, see "Adding Authentication for AD Users" on page 2

Problem: I have added a user to an AD group with restrictions defined in Orion but the restrictions are not being enforced.

Solution; If a user is defined in Orion as an Individual AD user, or a member of multiple AD authenticated groups, and is also a member of an AD Group in Orion, the individual authentication will take precedence over the group, possibly allowing that individual permissions they should not have. Remove the individual AD account from Orion to rectify. For group conflicts, Orion will authenticate using the first valid group discovered.

Problem: The Active Directory or Local Domain Authentication dialog gives one of the below errors:

Login failure: unknown user name or bad password

Login failure: the user has not been granted the requested login type at this computer

Solution: Ensure that the account you are using has administrative rights within the AD tree you are searching. Also, check that you can access the tree you are searching from the domain you are currently in. Check for bad password or locked or expired account.

Problem: I can't find where to add AD access for Network Atlas.

Solution: Network Atlas does not presently support AD authentication.

Problem: I have tried to configure AD integration but the test login always takes me to the login.aspx screen.

Solution: Automatic browser login is controlled by a security setting on the browser. If your browser did not accept Orion setting this, you will have to change it manually. Two settings should be checked. One is for automatic logins from restricted zones; the other is an on/off switch for automatic login.

For Internet Explorer these settings are defined in **Tools > Internet Options > Security > *Zone* > Custom Level > User Authentication > Logon**. The option you are looking to enable is "Automatic logon only in Intranet zone", or "Automatic login with current user name and password". The "Automatic logon only in Intranet zone" setting only works if the SolarWinds web server is in the Local Intranet zone.

Where to Learn More

Orion AD Implementation Resources

- [Orion Common Components Administrator Guide](#)
- [thwack.com “AD login” search thread](#)
- [Orion Product Blog Entry on AD Groups in Orion](#)

Microsoft Active Directory Resources

[Active Directory Users, Computers, and Groups](#)

[What is the Global Catalog](#)

thwack Community

The thwack community has thousands of users who regularly exchange ideas and solutions. Chances are that if you are trying to create a complex alert and having issues, there is a thwack user who has already solved that issue. SolarWinds employees from Development, Support and Product Management regularly interact with SolarWinds product users on thwack, so we may also be able to help you solve your problem there too.