This paper examines how Active Directory authentication works in SolarWinds Orion Products. The reader should have a working understanding of Active Directory authentication before reading this Technical Reference.
Copyright © 1995-2013 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 HEREBUNDER 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: 7/30/2013
Orion AD Integration

As of Network Performance Monitor (NPM) 10.1, NPM and the Orion modules now have the ability to add user and group access to Orion products via 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 NPM and the Orion modules than that provided by the Administrator’s Guides (AGs). The AGs should be used for step-by-step instructions on using AD for Orion authentication, so that will not be addressed here. The flow chart below shows how the Orion authentication process works with AD.

Figure 1 - Orion Login Process Overview
The user experience differs depending on how user authentication is set up. For users defined in Orion that have their user name and password embedded in the URL they use to access Orion, they will go directly to their Orion home page, bypassing any AD authentication. The same will happen for AD authenticated users. Although the Login.aspx page is referenced for all users, the above two types of users will never see the login screen if the authentication is successful. 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 log in from the login.aspx screen.

While it may 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 ID and password combinations. Likewise, anyone who views the URL will also have access to the ID and password.

Orion products prior to NPM 10.1 had the ability to use Windows Pass-through Security. This feature was implemented as a workaround until AD authentication was developed for the Orion products. Users that have Windows Pass-through Security enabled 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 Common Components 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 applications use a centralize authentication authority, such as AD, the application need only to achieve confirmation from AD that the user or group is authentic. The application is no longer burdened with authentication schemes and the users are not challenged to login to a system where AD allows access.
Adding AD Orion Authentication for AD Users

AD account authentication for Orion is set in the Orion Administrator interface. The following sections provide instructions for adding and configuring AD users in Orion:

- Adding a New User Account
- Configuring User Account Settings

Adding a New User Account

The following procedure adds a new Active Directory user to the Orion Web Console.

To add an AD user accounts:

1. Log into the Orion Web Console using an account with administrative privileges.
2. Click Settings in the top right corner of the web console.
3. Click Web Console Settings in the Settings grouping.
4. Select Enable automatic login for the Windows Account Login setting, and then click Submit.
5. Click Manage Accounts in the User Accounts grouping.

![Orion Manager Users Interface](image)

   **Note:** The screens and options for Group and Individual accounts are the same, so we will examine the Individual Accounts screen only.

7. Select Windows individual account, and then click Next.
By choosing the Individual Account tab and then clicking Add New Account, we are taken to the Add New Account screen shown below.

To add AD accounts into Orion, Orion must give you a way of demonstrating that you have the rights to search for accounts and give you the ability to specify which accounts to add. 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.
Configuring User Account Settings

Once all users are selected, clicking next will take you to the Orion account settings page (seen below) where you can specify the Orion experience for those users.

Add New Account

![Define settings for Orion individual “billy bob” account](image)

Account Enabled: Yes
Account Expires: Never
Disable Session Timeout: No
Allow Administrator Rights: No
Allow Node Management Rights: No
Allow Account to Customize Views: No
Allow Account to Clear Events, Acknowledge Alerts and Syslogs: Yes
Allow Browser Integration: Yes
Alert Sound: No Alert Sounds
Number of Items in the breadcrumbs list: 50

Account Limitations
There are no account limitations defined. To create account limitations, click the “Add Limitation” button.

![Default Menu Bar and Views](image)

Home Tab Menu Bar: Default
Network Tab Menu Bar: Network TabMenu
APM Tab Menu Bar: APM TabMenu
IPAM Tab Menu Bar: IPAM TabMenu
IPSLAM Tab Menu Bar: IPSLAM TabMenu
NTA Tab Menu Bar: NTA TabMenu
Virtualization Tab Menu Bar: Virtualization TabMenu

Figure 4 - Orion User Account Settings

Once AD access has been set up, it is important to understand which components of the overall authentication process are controlled by AD controls and which portions are determined by Orion core. 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 Orion with AD

Once AD authentication is in place, the AD authenticated user will be sent to their 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 Orion management.

Most Orion deployments require a handful of levels of access and customization. An Orion 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 Orion can save a lot of administrative work.

Sample Scenario
The following scenario provides a case for using AD authentication with the Orion Web Console.

- Environment – A large number of Orion 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 Orion and assign the specific privileges with the Orion Admin interface. Then add each of the high level users to Orion using their Individual AD accounts, again granting the level of access required for each user in the Orion Admin interface.

Many Orion implementations could operate “user administration free” by assigning Orion users to AD groups according to their Orion operational needs. All of the granting or removal of Orion access would be accomplished by AD.
Troubleshooting Orion AD Issues

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

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 Orion Authentication for AD Users” on page 2.

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

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.

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

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.

I can’t find where to add AD access for Network Atlas.

Network Atlas does not presently support AD authentication.

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

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 Orion web server is in the Local Intranet zone.
Additional Resources

The following resources are available for further assistance with using Advanced Directory for Orion authentication.

**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.