

Single Sign-On via LDAP Fundamentals Guide May, 2021



Introduction

The software has a number of security features to protect your database from unauthorized viewing and tampering. The front line of defense is your user code and password. These are entered on the login screen after you launch the application.

The software supports Single Sign-On for customers who rely on Active Directory services, using the LDAP protocol. When accessing the software from a workstation with Single Sign-On enabled, the application automatically completes the login for that user. The user does not have to enter their credentials again to gain access to the applications. This document provides details about the setup and use of the Single Sign-On feature.





Setup

To ensure positive identification, the Security Administrator will be required to set up the user accounts in the software so that the User Code matches the Windows Active Directory user code.

Enable Single Sign-On with Windows Active Directory

In order to set up the Single Sign-On via LDAP, there are a few setup steps within the software that allow the application to use Single Sign-On. From the the software home NAV bar:

- 1. Select Setup / Admin
- 2. Select Admin/Security
- 3. Select **Security Admin Parameters** to display the [Administer Security System Settings] Window
- 4. Click the check box next to *Enable Single Sign-On with Windows Active Directory* to display the **SINGLE SIGN-ON** tab

Administer Security System Settings	×
Security Auditing Single Sign On	
Password Security	
Level of Password Complexity Required	
Alpha-Numeric Image: Require passwords to contain at least one	e Letter and one Number
🔿 Alpha Only	
Numeric Only	
Minimum number or characters required for passwords:	6
Number of most recently used passwords to keep in history:	5
Number of days before password expires:	255
Number of login attempts before user account is suspended:	
	3
Period of inactivity (in minutes) to force the session to time out:	120
Enable Single Sign On with Windows Active Directory?	
Database Backup Schedule	
St <u>a</u> rt Time: E <u>n</u> d Time: (Prevent u	user logins during this time frame)
Login Security Warning	
Warning: This system should only be accessed by authorized users!	
Allow users to save exported data files outside their Secure File Folder	0
🚰 Eile Locations 🛛 🚍 Fax / E-Mail 📃 DB Connect Setu	p V OK X Cancel





- 5. Click the table icon to the right of the *Default Active Directory Domain Name* field to search for and select a Default Windows Active Directory Domain Name to be used with LDAP queries for Single Sign-On
- 6. Click the **Configure Single Sign On User Accounts** button to display the [Map User Accounts to Active Directory for Single Sign On] window

curity Auditing Single Sign On		e
Default Active Directory Domain Name:		Ċ
Configure Single Sign On User Accourt	nts	
File Leasting	DB Connect Colum	Course





7. Link the software User (left column) to the Active Directory User (right column) by clicking on the desired user from each column and then clicking the **Map** button



User Login

The software user authentication will be automatic once the system has verified the user against the Windows Active Directory/LDAP system for the currently signed in user. The user will not need to enter their software credentials to gain access to the application if they are signed in with the Windows Active Directory.







Once the user is logged in the top tool bar will no longer have the **1** icon available to the user as a function.

😪 🔜 💊 🔒 🔳 🔳 💼 🗠 🥭 🕗 🤉 🗐

Password Security Parameters

With the Single Sign-On via LDAP enabled, password security is relinquished from the software to the Windows Active Directory authentication. As a result, the following the software password security features will not be relevant:

- Level of Password Complexity Required
- Minimum number of characters required for passwords
- Number of most recently used passwords to keep in history
- Number of days before password expires
- Number of login attempts before user account is suspended
- Periods of inactivity (in minutes) to force the session to time out

NOTE: Protecting patient health information is the responsibility of the client. While the software may provide some of the tools necessary to accomplish this, the client's security policy ultimately establishes the final procedures. Single Sign-On allows healthcare organizations to link network user authentication and access to the software through Windows Active Directory. Client security policies will need to address all of the password security parameters that were previously defined within our software. This would include any changes necessary to the network password or login credentials.

curity Auditing Single Sign On	
Password Security	
Level of Password Complexity Required	
Alpha-Numeric Require passwords to contain at least on the second sec	ne Letter and one Number
🔿 Alpha Only	
💿 Numeric Only	
Minimum number of characters required for passwords:	6
Number of most recently used passwords to keep in <u>h</u> istory:	5
Number of days before password expires:	255
Number of login attempts before user account is suspended:	3
Period of inactivity (in minutes) to force the session to time out:	120
Enable Single Sign On with Windows Active Directory?	
Database Backup Schedule	
Start Time: End Time: (Prevent	user logins during this time frame)
Login Security Warning	
Warning: This system should only be accessed by authorized users!	
Allow users to save exported data files outside their Secure File Fold	er?





System Event Audit Log The System Event Audit Log will record any Single Sign-On attempts.

/20/2012 2:45PM /20/2012 2:44PM	JSHIELDS JSHIELDS	MA	User Login/Logout	1		Cueses
/20/2012 2:44PM /20/2012 2:44PM /20/2012 2:44PM /20/2012 2:44PM /20/2012 2:39PM /20/2012 2:39PM /20/2012 2:39PM /20/2012 2:38PM /20/2012 2:38PM	JSHIELDS JSHIELDS JSHIELDS JSHIELDS JSHIELDS JSHIELDS JSHIELDS JSHIELDS JSHIELDS JSHIELDS JSHIELDS	MA MA MA STUDENT STUDENT STUDENT STUDENT STUDENT STUDENT STUDENT	Security Administration Events User Account Reactivated User Account Viewed User Login/Logout User Login/Logout Node-Authentication Failure User Login/Logout User Login/Logout User Login/Logout		STUDENT MA	Success Success Success Success Success Failure Success Failure Success Failure Failure
/20/2012 2:38PM	JSHIELDS	STUDENT	User Loan/L Sout			Success
Z2U/2012 2.38FM Z2U/2012 2.38FM Z2U/2012 2.38FM Z2U/2012 2.37FM Z0U/2012 2.37FM Z0U/2012 2.37FM Z0U/2012 2.37FM Z0U/2012 2.37FM Z0U/2012 2.48FM Z06/2012 2.48FM Z06/2012 2.47FM Z06/2012 2.42FM Z06/2012 2.42FM Z06/2012 2.42FM Z06/2012 2.42FM Z06/2012 2.42FM Z06/2012 2.41FM	JSHIELDS JSHIELDS	STUDENT STUDENT STUDENT STUDENT STUDENT STUDENT STUDENT STUDENT MA STUDENT MA STUDENT MA STUDENT MA STUDENT MA STUDENT MA STUDENT MA STUDENT	User Login/Logout User Account Inactivated Security Administration E vents User Login/Logout User Login/Logout		STUDENT MA MA MA	Success Success





Select an event from the System Event Audit Log to view the [System Event Audit Details] Window

Event Trx:	830	
Date/Time of Event:	11/20/2012 02:38PM	
UTC (ISO-8601):	2012-11-20T14:38:46-05:00	
Workstation:	JSHIELDS	
Generated by User:	Bates, Christine	
- Event Type:	User Login/Logout	
System Component:	AGILITY	
Application Component:	STIX:Login:UserLogin	
Outcome:	Success	
Description:		
Single Sign-On with Active Directory Successful		*

Inactive User

When an the software user is made inactive, they will no longer be able to log in to the application using Single Sign-On. The user will be presented with a User Login Failed message, and prompted with the software login screen.







Event Trx:	831	
Date/Time of Event:	11/20/2012 02:38PM	
UTC (ISO-8601):	2012-11-20T14:38:51-05:00	
Workstation:	JSHIELDS	
Generated by User:	Bates, Noristine	
Event Type:	Node-Authentication Failure	
System Component:	AGILITY	
Application Component:	STIX:Login:UserLogin	
Outcome:	Failure	
Description:		
Inactive User Account		ж. т

The unsuccessful attempt will be recorded on the System Event Audit Log

Summary

We hope that this guide has been helpful in utilizing the Single Sign-On via LDAP function of the application. If you have questions or need assistance, please contact Net Health Support at: 844-464-9348, Option 3 or <u>ehoccmed-support@nethealth.com</u>.

