Net Health®

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.

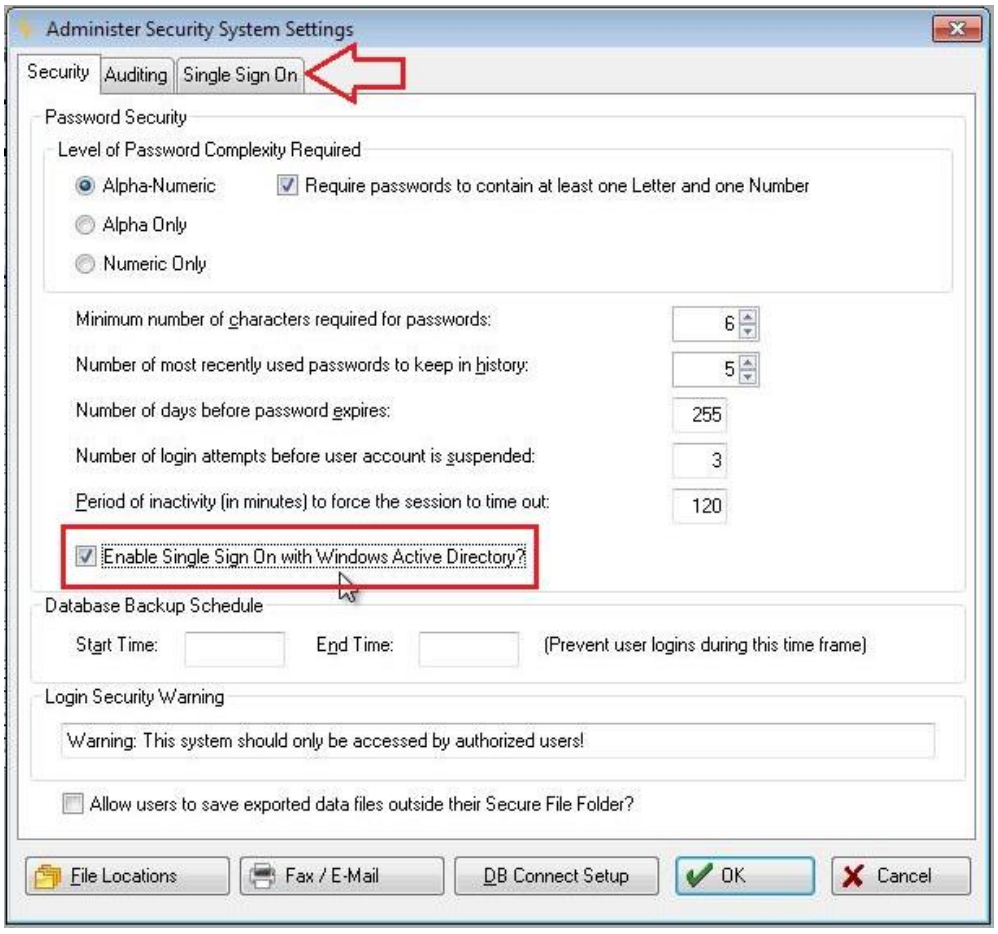
Setup

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.

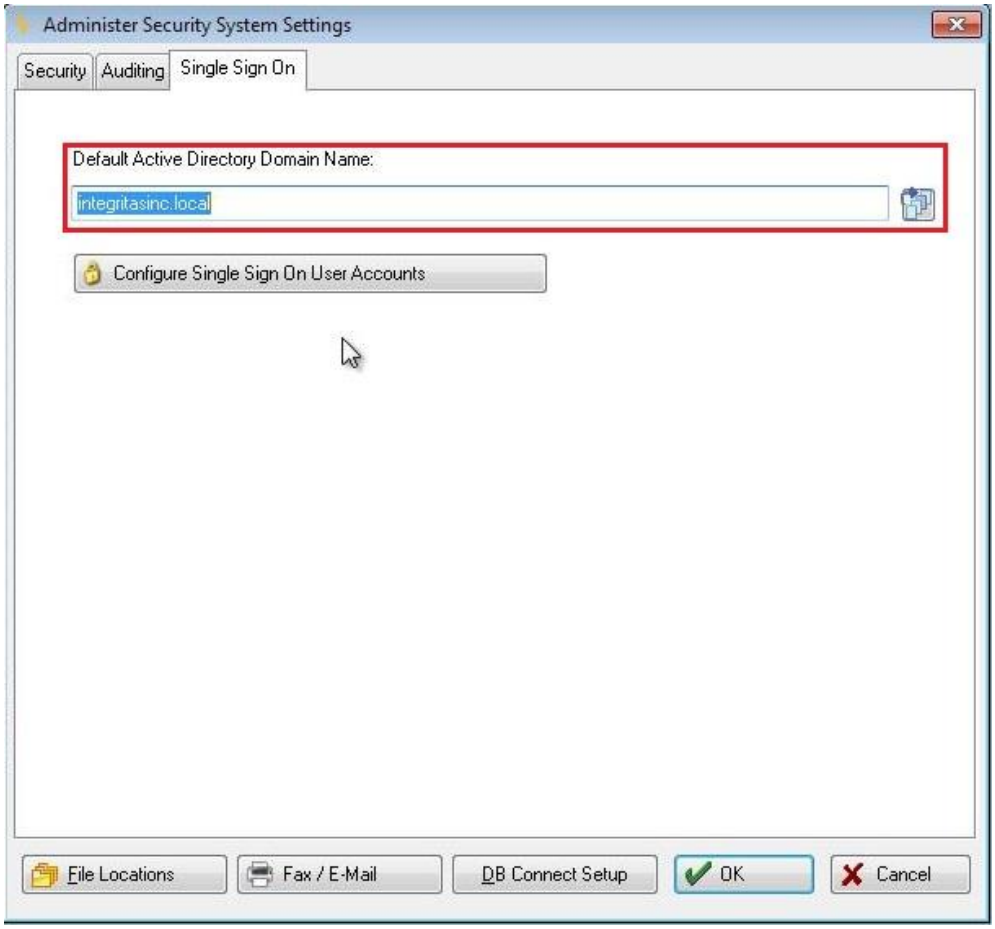
Enable Single Sign-On with Windows Active Directory

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:

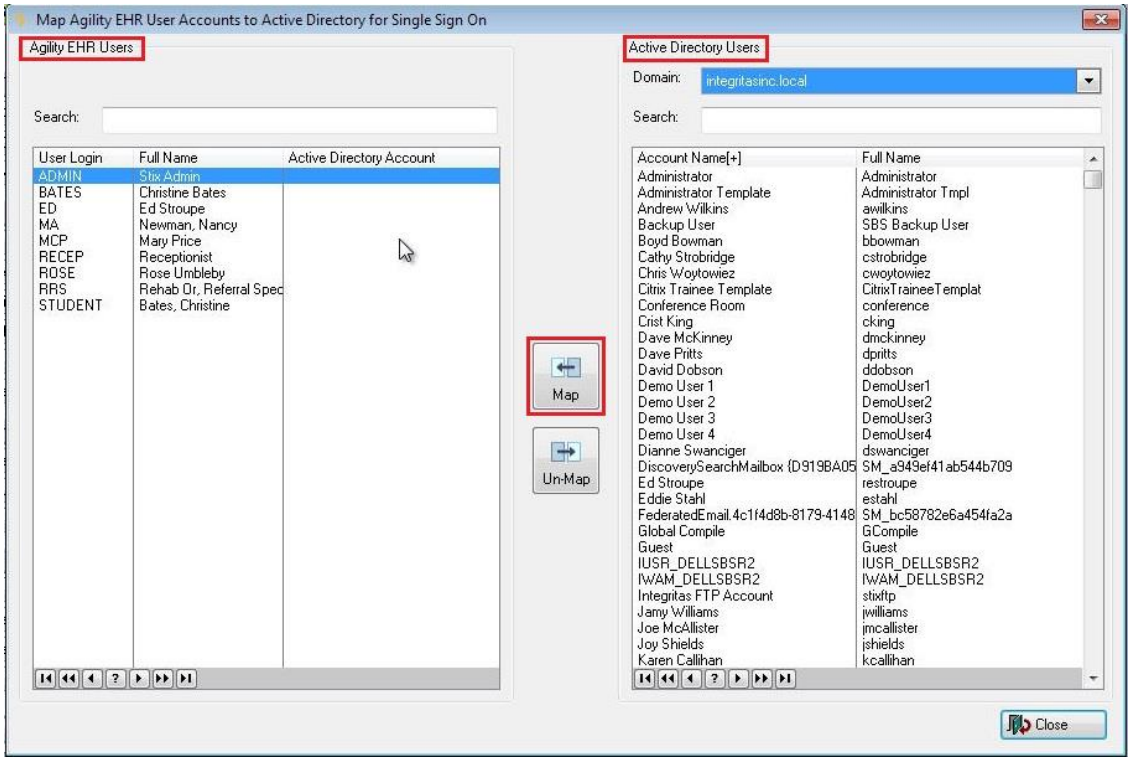
1. Select **Setup / Admin**
2. Select **Admin/Security**
3. Select **Security Admin Parameters** to display the [Administer Security System Settings] Window
4. Click the check box next to *Enable Single Sign-On with Windows Active Directory* to display the **SINGLE SIGN-ON** tab



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



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

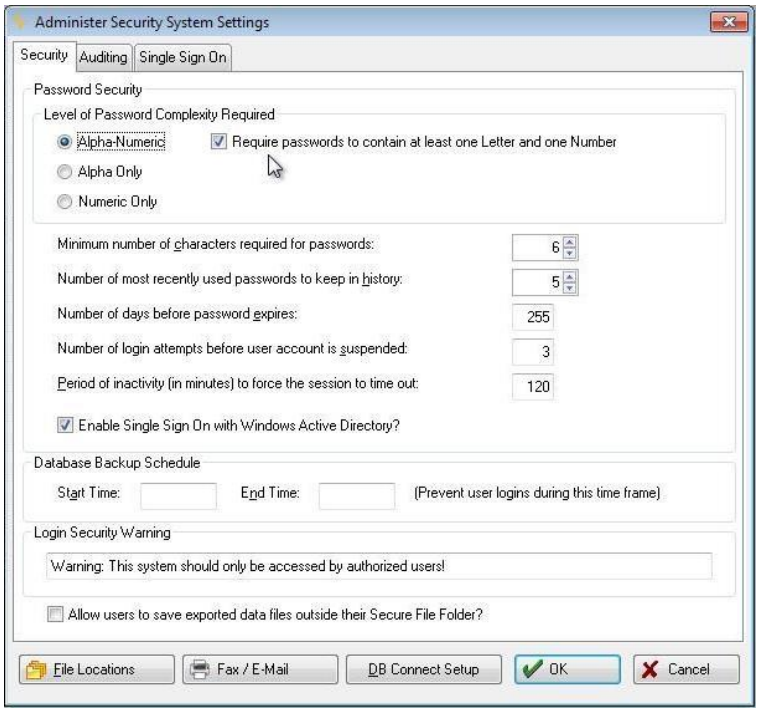
The software user authentication will be automatic once the system has verified the user against the Windows Active Directory/LDAP system for the currently signed in user. The user will not need to enter their software credentials to gain access to the application if they are signed in with the Windows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

Once the user is logged in the top tool bar will no longer have the  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:

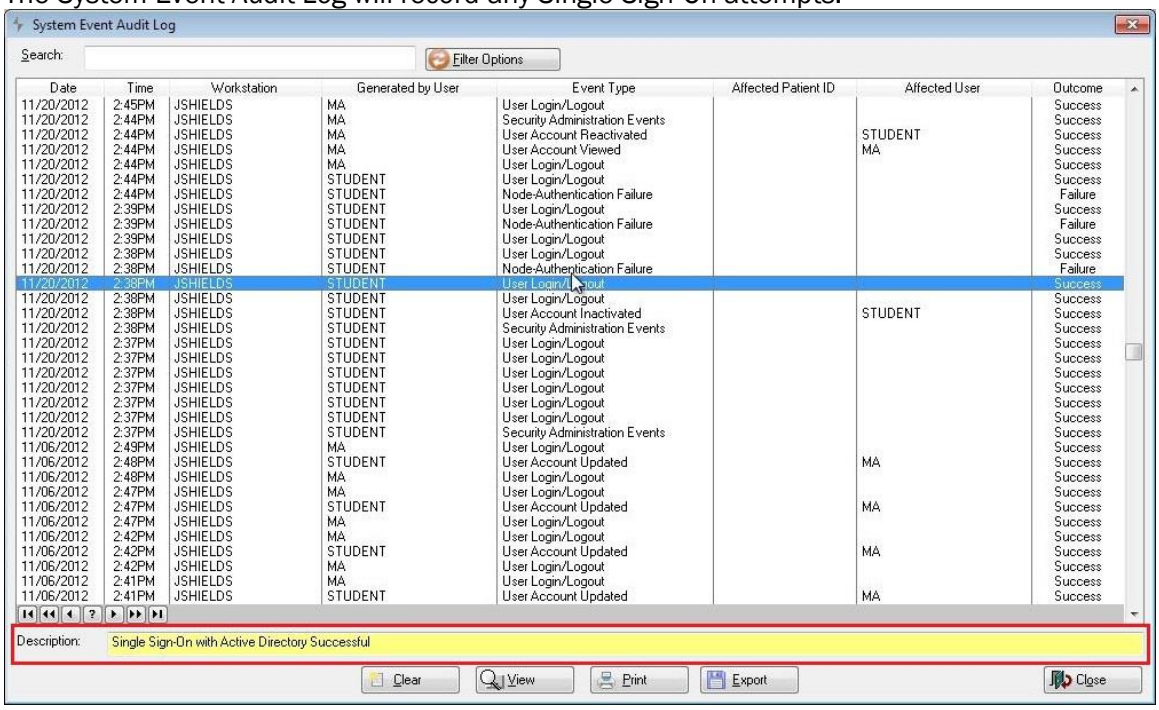
- Level of Password Complexity Required
- Minimum number of characters required for passwords
- Number of most recently used passwords to keep in history
- Number of days before password expires
- Number of login attempts before user account is suspended
- Periods of inactivity (in minutes) to force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

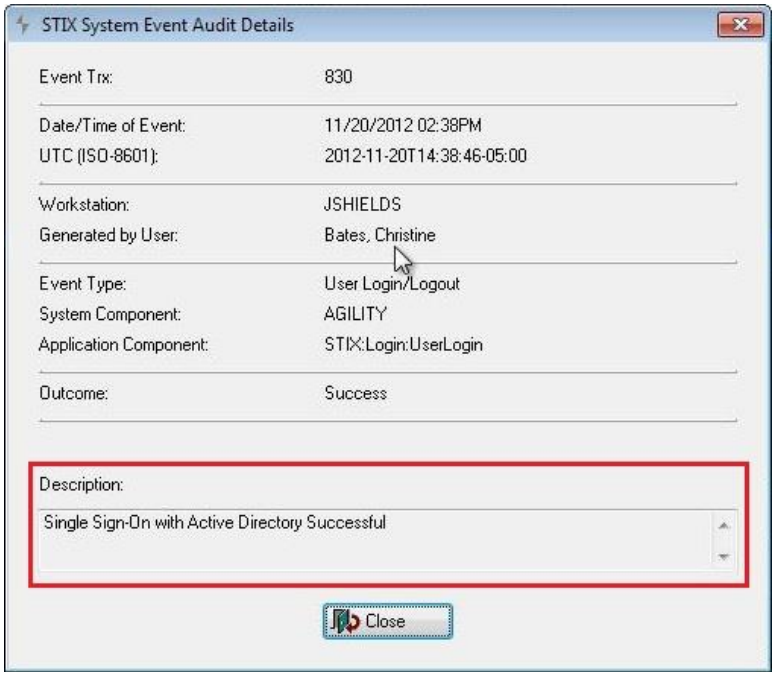


System Event Audit Log

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



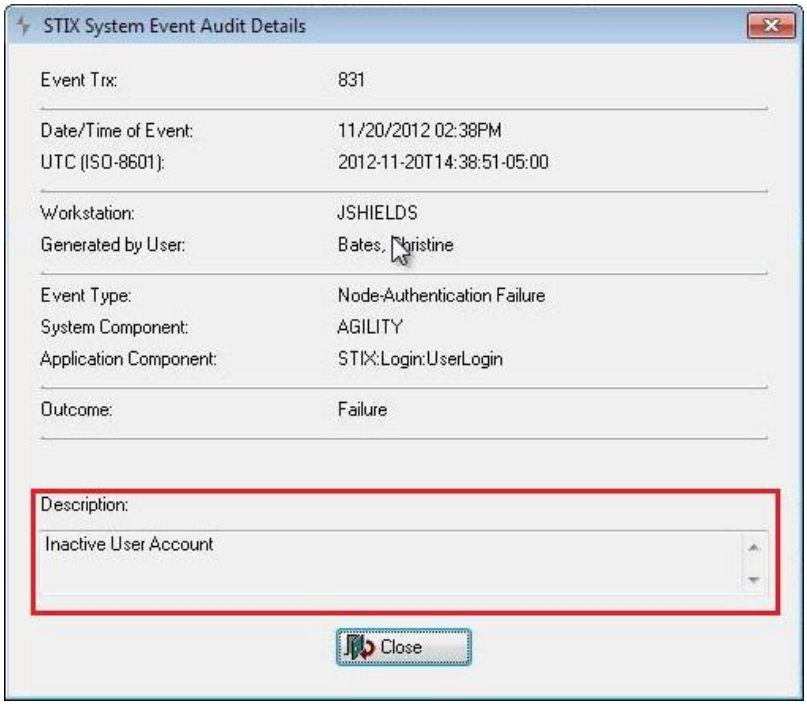
Select an event from the System Event Audit Log to view the [System Event Audit Details] Window



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.

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 ehoccmed-support@nethealth.com.