Administration Tool User Management

Overview

◆ Version 2.4.0 and newer software for Codonics Safe Label System® (SLS) Administration Tool (AT) includes support for AT User Management. The 2.4.0 release provided Same Sign-On capability which allowed Active Directory user access to the AT. Customers who used Microsoft Active Directory could utilize their Active Directory server to manage and control users on the AT. Users could then log into the AT with their personal Windows user name and password anywhere on their hospital network.

Prerequisites for Same Sign-On:

AT is installed on a computer that has access to the Microsoft Active Directory server.

Microsoft Active Directory (Windows Server 2003 or newer).

Active Directory URL (e.g., 10.1.3.9) and port number (e.g., 389).

◆ **Microsoft Active Directory (AD)**: is a directory service that Microsoft developed for Windows domain networks. It is included in most Windows Server operating systems as a set of processes and services. AD uses LDAP versions 2 and 3.

◆ In 2.3.0 and earlier software, the AT only provided one user and one role (i.e., Administrator). If you wanted to change the password, you had to log into the AT and change the default password.

AT User Roles and Permissions

As of version 2.6.0 software, there are now five different AT user roles with predefined and selectable permissions. See below and Table 1 for default permissions:

1. **Administrator** has full access to and operability of the AT including setup of the AT user roles, AT user permissions and editing the Active Directory settings.

2. **Super User** has access to and operability of the AT except editing of the AT user roles, AT user permissions and Active Directory settings.

3. **Pharmacist** has access to verify drugs and view and edit the Formulary.

4. **Bio Med** has the access to view, edit devices and download logs in the Device Manager.

5. **Pharmacy Tech** has access to view the Formulary.

Table 1:

User Role	View Formulary	View/Edit Devices	View/Edit SLS Users	View/Edit Configuration	View/Edit Formulary Verify Drugs	Setup AT User roles and permissions and Active Directory
Administrator	Yes	Yes	Yes	Yes	Yes	Yes
Super User	Yes	Yes	Yes	Yes	Yes	No
Pharmacist	Yes	No	No	No	Yes	No
Bio Med	No	Yes	No	No	No	No
Pharmacy Tech	Yes	No	No	No	No	No

AT Active Directory Support

◆ The AT will support and utilize Microsoft Active Directory (Windows Server 2003 or greater) for user management. Adding AT support for Microsoft Active Directory will provide the following:

  ◆ Support for more AT users.

  ◆ Basic User Management tasks (reset passwords, add/remove users from security groups) can be performed on the Active Directory server by a network administrator.

  ◆ AT roles can be predefined based off of specific security groups assigned on the Active Directory.

Setting up AT Users Roles and Permissions using Active Directory

Configuring Active Directory Settings in the AT

1. To enable sites to utilize Active Directory with the AT, contact your IT organization for Active Directory Server information and configuration settings (see Step 7 for all required fields).

NOTE: Sites should create a new security group (i.e., AT Administrator Group) for AT usage so the network administrators can easily move users in and out of groups.

Sites should setup other groups (e.g., Super User Group) based on their roles for that group of AT users who need to access and manage the AT.

HTTPS is recommended when using AT User Management to properly encrypt Active Directory credentials.

2. Install the Administration Tool and log into the AT using the standard Codonics Administrator Username and Password.

CODONICS®

3. Select the Administrator link in the upper right corner of the AT.
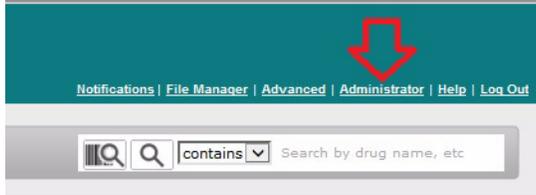
4. The Administration Options dialog will display. Check the box for Allow users to log in via Active Directory.

5. Select Configure Connection Settings.
6. The Configure Active Directory Settings dialog will display.
7. Enter the Server Address of the Active Directory, Port (389 is the default), Authentication Method (UPN or SAM), Domain, Search Base, Group Search Base, AT Administrator Group and Super User Group. Every field is required.
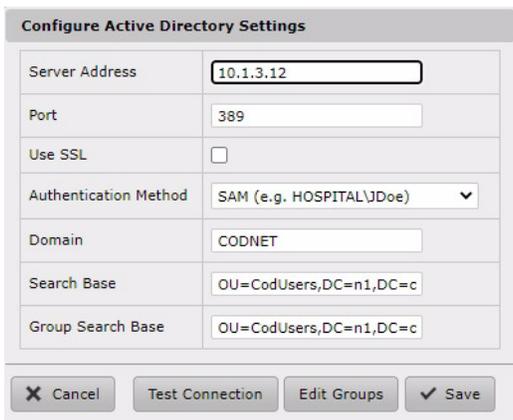
NOTE: The AT and the Active Directory server need to be on the same network.

8. Test the set up by selecting Test Connection, filling in your Active Directory Username and Password and selecting Test.

9. Once you complete a successful test, click the Save button on the Configure Active Directory Settings dialog shown in Step 7.

Setting up User Roles and Permissions

1. Select Administrator in the AT user interface. The Administration Options dialog will be displayed.

2. Select Edit User Roles. The Edit User Roles dialog will be displayed.

CODONICS®

3. You can leave the Name of each role as defined by default (e.g., Super User) or change the Name.

4. You can now enter specific Active Directory groups (e.g., AT_SUPER_USERS) for different groups of people assigned different user roles.

5. Next, you can specify the user privileges that each User Role has by selecting Edit Permissions.

6. The Edit Role Permissions dialog for the role selected is displayed with default AT permissions defined. Below is the dialog displayed for Super User.

7. Modify different permissions by checking/unchecking for each role and select Save each time.

8. Repeat steps 3 through 7 for each role. Once you're satisfied with all your roles and permissions, select Save on the Edit User Roles dialog and then select Update on the Administration Options dialog.

9. If you inadvertently Delete a role but want to add it back in, you can select the Undo button. However, if you select Save before selecting Undo, you will need to create a new role.

CODONICS®

10. If you want to create a new role, you can by selecting Create Role.

NOTE: The AT supports up to a maximum of five roles at one time. In order to add a new role, you may need to Delete an existing role first.

11. Enter a name (e.g., QA) for the new role and then select Edit Permissions.

The Edit Role Permissions dialog will be displayed and you can check what AT permissions you want the new role to have. Then select Save.

12. Then select Update on the Administration Options dialog.

Logging into the AT

◆ Now that the AT is configured for Active Directory, user roles and AT permissions, approved users can log into the AT with their personal Windows login name and password.

◆ If an unapproved user tries to log into the AT or they use an incorrect password, they will be notified on the AT Log In screen.

Setting up Local User Roles and Permissions

For users who want to setup specific AT user roles and permissions but don't want to use or have Active Directory support, the following instructions let you setup local user roles and permissions.

1. Select Administrator in the AT user interface. The Administration Options dialog will be displayed.

2. Select Edit Local User.

3. The Edit Local User dialog will be displayed. Select Create User.

CODONICS®

4. Enter the Username, select a Role (e.g., Super User) from the drop down box and reset their password.

5. Repeat step 4 for all the local users you need to include.

6. Select Save.

7. Next, you can review and specify the AT user permissions that each User Role has by selecting Edit User Roles from the Administration Options dialog.

8. The Edit User Roles dialog will be displayed. Select Edit Permissions.

9. The Edit Role Permissions dialog for the role selected is displayed with default AT permissions defined. Below is the dialog displayed for Super User.

10. Select Save.

11. Repeat steps 8 through 10 for the remaining user roles that require setup.

12. When complete modifying all user roles, select Save on the Edit User Roles dialog and then select Update on the Administration Options dialog.

Logging into the AT

◆ Now that the AT is configured with user roles and AT permissions, approved users can log into the AT with their user name and default password.

◆ Once logged into the AT, the user can change their password by selecting their name on the link in the upper right corner of the AT.

◆ The Account Options dialog is displayed. Select Change Password.

CODONICS®

◆ The Edit User Information dialog is displayed. Enter the Current Password and then enter and confirm a New Password.

Edit User Information.

Change Password

Current Password: [   ]

New Password: [   ]

Confirm New Password: [   ]

✕ Cancel   ✓ Update

◆ If an unapproved user tries to log into the AT or they use an incorrect password, they will be notified on the AT Log In screen.

◆ Forced Logout

◆ Only one user can be logged into the AT at a time.

◆ If an approved user (e.g., person B) logs into the AT while a different user (e.g., person A) is logged in, a warning message will be displayed on the AT user interface indicating to person B that person A is currently logged into the AT.

◆ If person B proceeds, person A will be automatically logged out and will be notified that person B logged into the AT.

AT Event Logging

◆ Enhanced logging is part of the AT including the user that was logged into the AT at the time AT events occurred.

◆ Some examples of events logged per user include importing, adding, editing and deleting drugs in the MDD or Formulary, changing Configuration settings, importing SLS user package, and installing packages to SLSs from the AT Device Manager.

Technical Support

If problems occur during operation, contact Codonics Technical Support at any time.

Phone: +1.440.243.1198

Email: support@codonics.com

Website: www.codonics.com

Get it all with just one call
800.444.1198

CODONICS ®
We bring the future into focus