# Report Exec Enterprise Lightweight Directory Access Protocol (LDAP) Integration

## Contents

## Overview

This document will briefly outline how to setup Report Exec Enterprise to authenticate against the Active Directory (AD) server of the organization using the Lightweight Directory Access Protocol (LDAP).

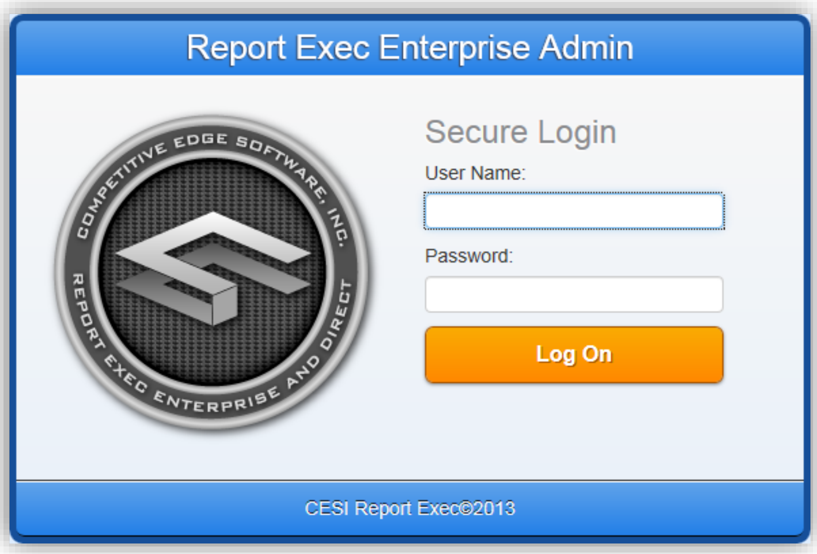
## Technical Support

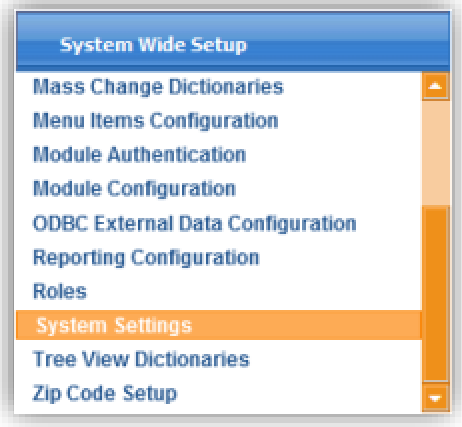
Email support@reportexec.com or call (414) 423-9800 option 2 with questions. The Technical Support Team is in the office 8am – 4pm Central Time.

## Configuring Report Exec Admin

A user requires System Wide Setup access to the Report Exec Admin application in order to configure the LDAP settings.

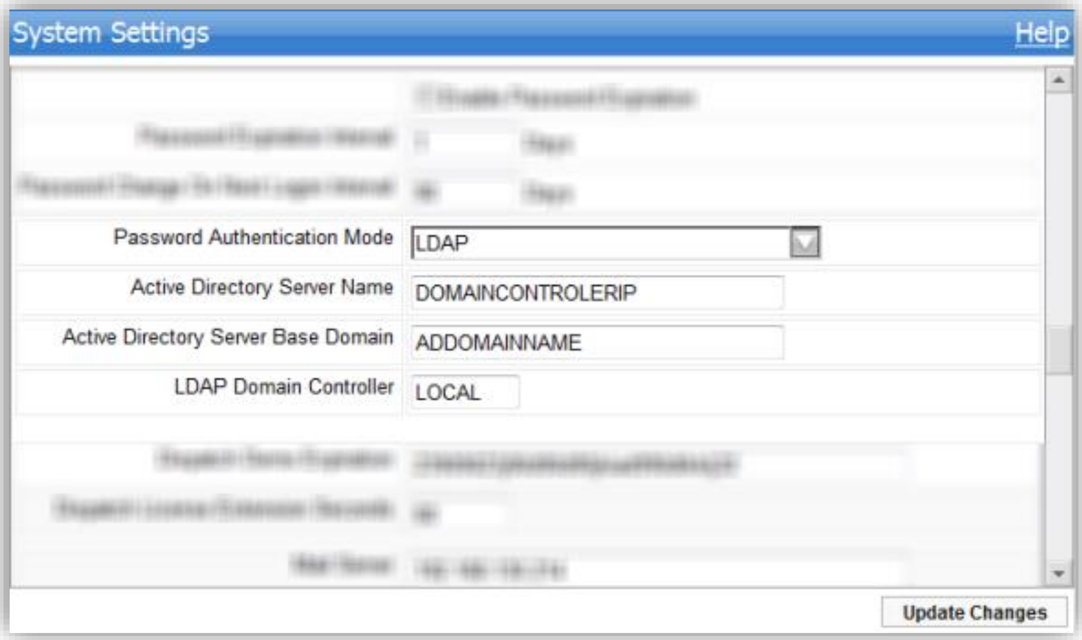
The first step is to log into Report Exec Admin with an account that has been given **System Wide Setup** access to the application.


Report Exec Enterprise Admin
COMPETITIVE EDGE SOFTWARE, INC.
REPORT EXEC ENTERPRISE AND DIRECT
Secure Login
User Name:
Password:
Log On
CESI Report Exec©2013



Once logged into the Admin side of Report Exec, go to **System Wide Setup** > **System Settings**.

In the **System Settings** section, scroll down to the area that has the four labels seen above: **Password Authentication Mode**, **Active Directory Server Name**, **Active Directory Server Base Domain**, and **LDAP Domain Controller**. These are the four fields that need to be configured for LDAP Authentication to work.



| | |
|---|---|
| Password Authentication Mode | LDAP |
| Active Directory Server Name | DOMAINCONTROLERIP |
| Active Directory Server Base Domain | ADDOMAINNAME |
| LDAP Domain Controller | LOCAL |

Fill in these fields with the configuration information for the Active Directory Domain in question, starting with **Password Authentication**. The following is a description of what each field is for:

- **Password Authentication** – The method of how Report Exec will authenticate the user base for the application. The settings in this field are **DB**, **LDAP**, **PING FEDERATE**, and **SITEMINDER**.
  - **DB** - Default option which authenticates directly to the Report Exec database and needs no additional setup other than setting up users in the **Add User** section.
  - **LDAP** - Authenticates against the Active Directory server specified in the Admin settings of Report Exec. An account for each user must be made within Report Exec Admin that exactly matches the user's Active Directory account and this account must be given the necessary Role permissions in Report Exec in order to login to the application. As long as a user has an Active Directory account that matches an account in Report Exec, the user will be able to log into the program. If a user account does not exactly match the Active Directory account, or if the user account was not given the Role permissions in Report Exec to log in, the account will be denied access.
  - **SITEMINDER** - This option was added based on custom work done for a specific organization who uses a third-party application for authentication to any web application on their network. http://www.ca.com/us/default.aspx
  - **PING FEDERATE** - This option was added based on custom work done for a specific organization who uses a third-party application for authentication to any web application on their network. https://www.pingidentity.com/en.html
- **Active Directory Server Name** – The name of the server that the Active Directory resides on. This server will need to be accessed by Report Exec Admin in order to verify if the user has a valid account or not.
- **Active Directory Server Base Domain** – The Domain name that the Active Directory users reside in.
- **LDAP Domain Controller** – This field is always set to **Local** which means that this is the local domain for AD.

## Additional Notes

The entries for LDAP in the System Settings of Report Exec can be quickly checked by running this query against the SQL database:

```
------------------------------------ LDAP Settings Query -----------------------------------
SELECT * FROM dbo.[Data]
WHERE [DataType] in
('AuthenticationMode', 'ADServerName','ADServerBaseDomain','LDAPDomainController')
----------------------------------------------------------------------------------------------
```

## *Single Sign-On (SSO)*

By default, websites in IIS use **Forms Authentication**. This will require a user to manually input their username and password. Users can be automatically logged into the program when accessing the login page of Report Exec if LDAP is enabled and **Windows Authentication** is enabled in IIS for the **CESIReportExec**, **CESIReportExecADMIN**, and **CESIReportExec360** directories.

## *Browser-Specific Settings*

### Mozilla Firefox

In Mozilla Firefox, the browser will prompt a user for Windows credentials when LDAP is activated. The below link explains why:

https://support.mozilla.org/en-US/kb/Firefox%20asks%20for%20user%20name%20and%20password%20on%20internal%20sites

*"This article describes why Firefox may ask for a user name and password on internal/intranet sites (for example, a Sharepoint site) while Internet Explorer doesn't.*

*Many internal sites user NTLM authentication, which reuses your network login as a login for the site. In many organizations, Internet Explorer is configured to allow NTLM on the internal sites, but Firefox is not. You can configure Firefox on Windows to allow certain sites…"*

The following steps need to be taken in order for Firefox to work as expected with LDAP:

1. In the Location bar, enter:
   a. `about:config`
2. From the `about:config` "*This might void your warranty!*" page, click `I'll be careful, I promise!` to continue.
3. In the `about:config` page, search for preference `network.automatic-ntlm-auth.trusted-uris`, and double-click it.
4. In the prompt that comes up, type a list of servers you want to allow, separated by a comma and a space. For example, if you wanted to allow http://myinternalserver and http://anotherinternalserver, you would type:
   a. `myinternalserver, anotherinternalserver`.
5. Press `OK`.