

Windows Integrated Security

Integrated Windows Authentication makes use of a users existing Windows account for security. When using Integrated Windows Authentication, the user does not need to sign in using the Ripplestone login form, but existing Windows user accounts still must be registered in Ripplestone.

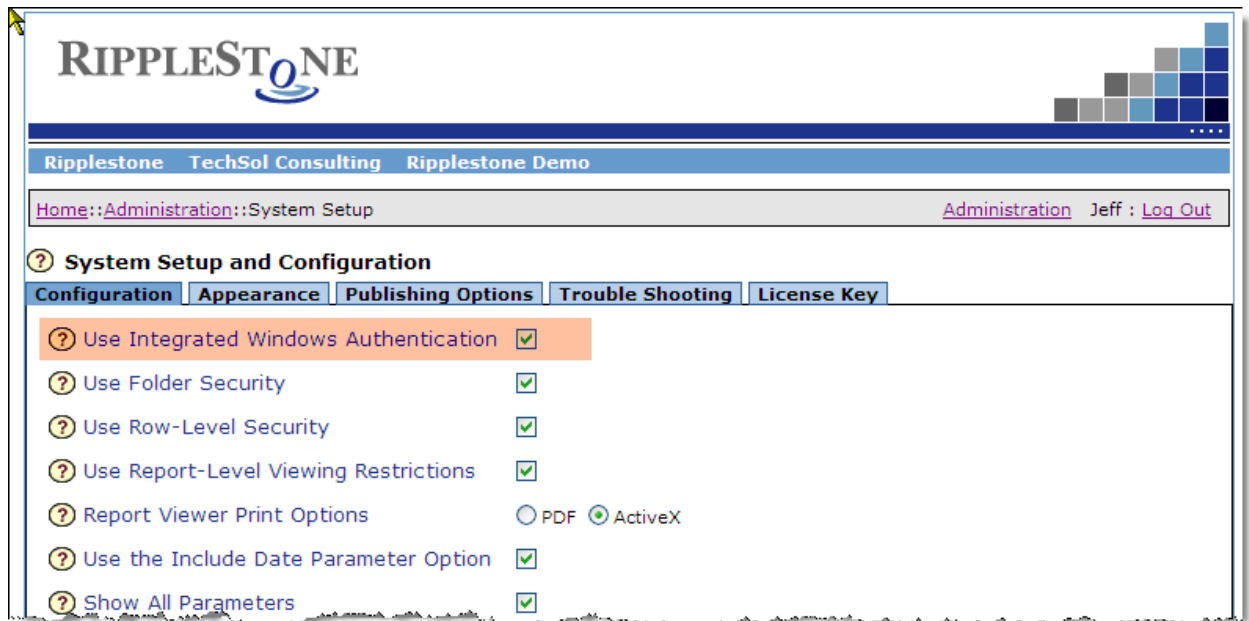
Setup

To enable Integrated Windows Security, perform the following four steps:

1. You need to disallow anonymous access in IIS. Go into IIS and click on the "Ripplestone" virtual directory. Right click and select the "Properties" option. Click on the "Directory Security" tab. Click on the "Edit" button under the box "Anonymous access and authentication control". Uncheck the "Allow anonymous access" box.



- Change the setting in Ripplestone for Integrated Windows Authentication to Yes. This is completed from the System Setup and Configuration page



- Edit the "web.config" file located at C:\Program Files\Ripplestone. Open the web.config file with notepad or a similar text editor. Uncomment the following line

```
<identity impersonate="true"/>
```

This line will follow the line...

```
<authentication mode="Windows"/>.
```

Also make sure that the above line has mode="Windows".

- Make sure that the Windows security on the folders used by Ripplestone is set correctly for each user or group who needs access to Ripplestone. The two folders that need to have security set are C:\Program Files\Ripplestone\Data and C:\Program Files\Ripplestone\ReportFolders. These two folders will need to have permissions for Full Control for the users that will be using Ripplestone. The easiest way to do this is to create a Windows group for the Ripplestone users and then give Full Control to this group for the 2 folders.

You will also need to give Everyone or the Ripplestone Users permission in the C:\Windows\Temp folder. This folder is used by Crystal Reports to store temporary report files.