ONESOURCE TAX INFORMATION REPORTING

USER ADMINISTRATION GUIDE

Document Version 2

THOMSON REUTERS®

DOCUMENT HISTORY

VERSION NUMBER	VERSION DATE	SUMMARY
1	May 2016	Initial publication.
2	January 8, 2017	Initial publication of new document format.

TABLE OF CONTENTS

ABOUT ONESOURCE TAX INFORMATION REPORTING USERS

Before a ONESOURCE Tax Information Reporting user can access and use the ONESOURCE Tax Information Reporting application, he or she must be added as a user in ONESOURCE Classic (www.onesourcelogin.com). ONESOURCE Classic provides single sign-on capabilities, which allows users to login one time to access all licensed Thomson Reuters applications without logging in to each application separately.

After the user is added in ONESOURCE Classic, the user has access to the ONESOURCE Tax Information Reporting application. However, for the user to be able to use ONESOURCE Tax Information Reporting , he or she must be provisioned. When a user is provisioned, a user profile is assigned to him or her. User profiles are a group of options and rights that limits a user's access to payer, form and recipient data as well as the features included in the ONESOURCE Tax Information Reporting modules. As such, a user profile is a type of role-based security where a user can be limited to performing only those tasks in ONESOURCE Tax Information Reporting that are necessary for carrying out his or her job responsibilities.

Users who are set up as system administrators in ONESOURCE Classic can add users in ONESOURCE Classic. ONESOURCE Tax Information Reporting security users can authorize new users to use ONESOURCE Tax Information Reporting and modify existing ONESOURCE Tax Information Reporting users so that they can be added to the Admin profile.

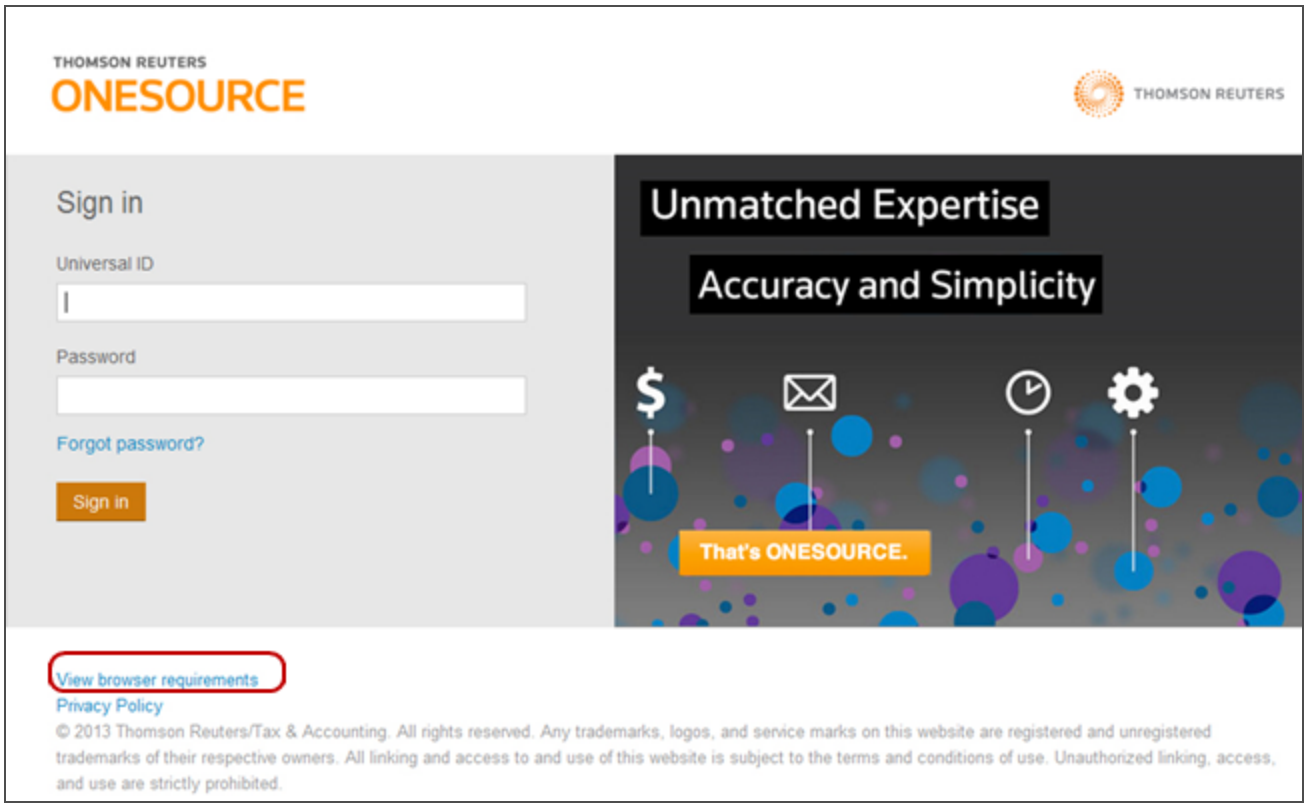
ABOUT THE MICROSOFT SILVERLIGHT PLUG-IN

The administrative sections of ONESOURCE Classic require that you have the Microsoft® Silverlight® plug-in installed on your computer. Silverlight is similar to Microsoft ActiveX®, which and allows greater security in uploading or downloading your files. If you run Microsoft Internet Explorer® on Windows® 10, you will need to turn on Compatibility View for ONESOURCE Tax Information Reporting . See the *Setting Internet Settings* guide, which is posted to the Customer Center, to learn how to turn on Compatibility View.

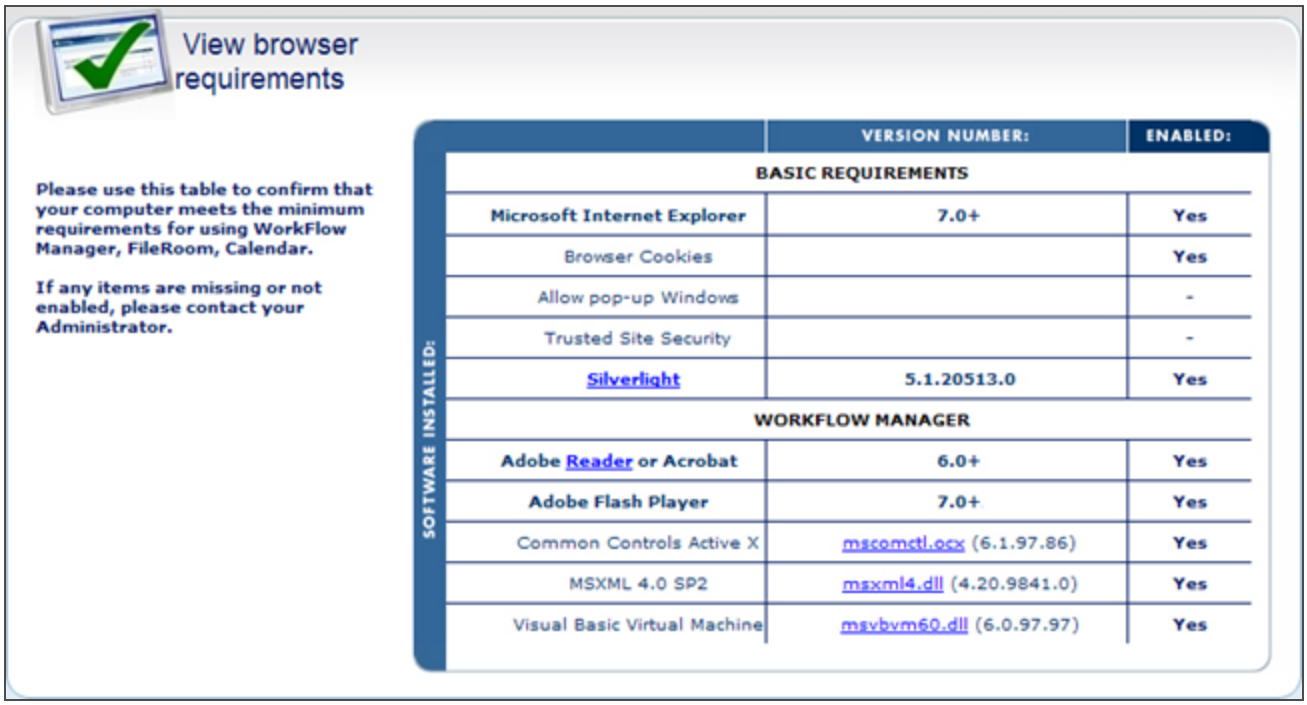
You may need administrative rights to install the Silverlight plug-in on your system. We encourage you to check with your IT department for information on administrative rights and requirements for Silverlight.

To download the Silverlight plug-in:

1. Access ONESOURCE Classic at www.onesourcelogin.com.
2. Click the **View browser requirements** link.



The View browser requirements page displays and shows you the version number and status for the Silverlight plug-in installed on your workstation.



3. Click the **Silverlight** link.
4. Review the Silverlight plug-in information displayed on the Get Microsoft Silverlight page.

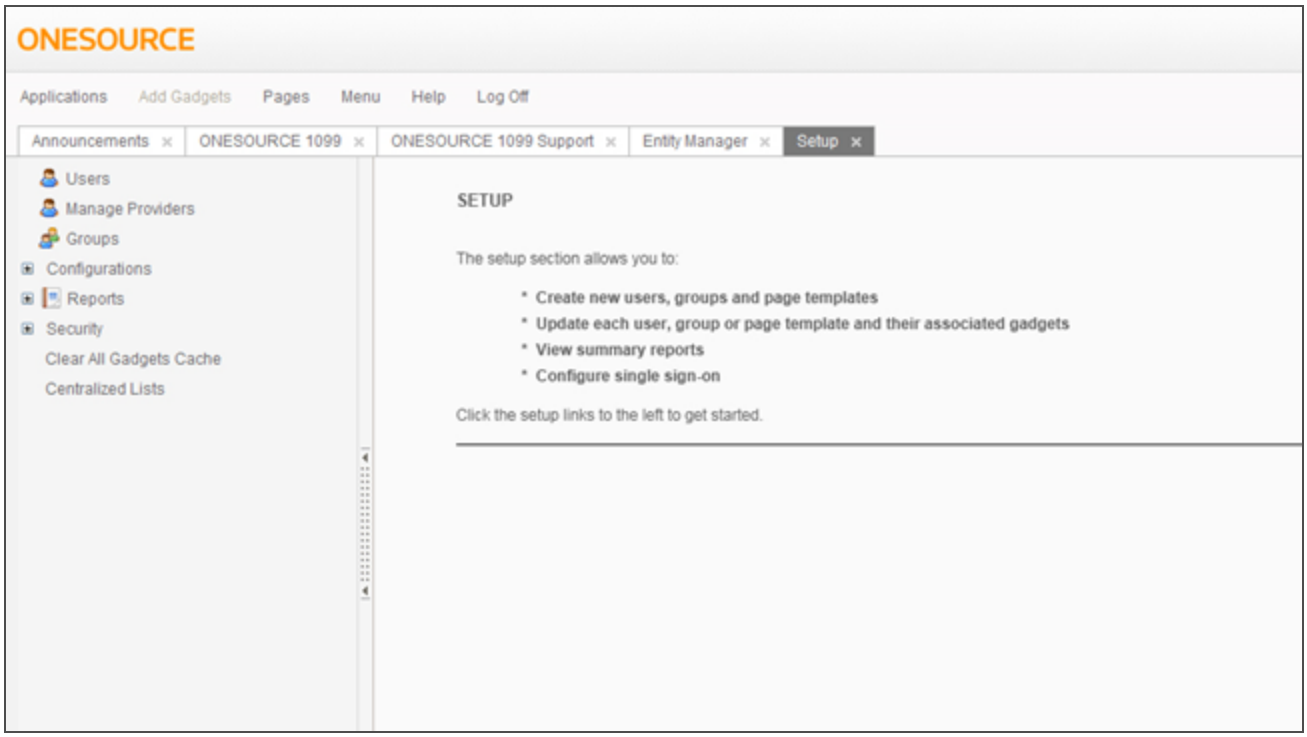
   If the Silverlight plug-in is not installed on your workstation or you need to update the version installed on your workstation, follow the steps listed on the Get Microsoft Silverlight page to complete the download and installation process.
5. Close the Get Microsoft Silverlight page.

ADDING AND PROVISIONING USERS

If you are a ONESOURCE system administrator, you can add users in ONESOURCE Classic. Adding users in ONESOURCE Classic includes assigning Universal IDs and entering initial user passwords.

To add users in ONESOURCE Classic and assign Universal IDs:

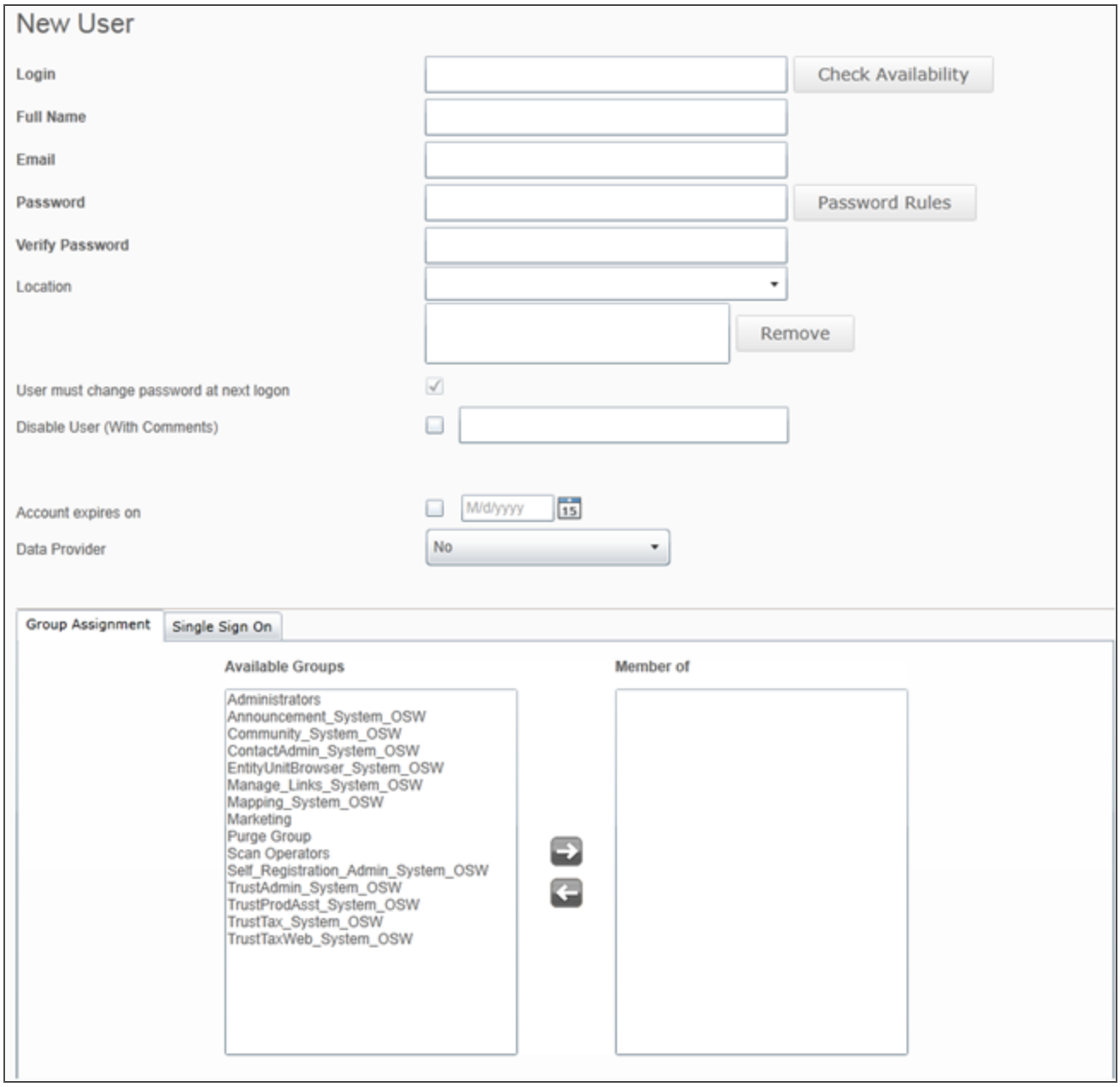
1. From the ONESOURCE Classic menu, click **Menu** then click **Setup**.



2. Click **Users** in the Navigation area.

3. Click **Actions** 

then click **Add New**.



4. Enter the Universal ID for the user in the **Login** field.

Universal IDs must be unique to ONESOURCE Classic. You can determine whether a Universal ID is unique (and available) by clicking **Check Availability**.

5. Enter the user's first and last name, and email address in the **Full Name** and **Email** fields. A valid email address is required. After the user is successfully added to ONESOURCE Classic, a confirmation email is sent to the user's email address so that the user can complete the setup.

6. Enter the user's initial password in the **Password** and **Verify Password** fields.

   Passwords must meet specific criteria. To view the password criteria, click **Password Rules**.

7. If the user you are adding is a contractor or temporary employee and you want to disable access when the employment contract ends, select the **Account expires on** check box then type the date (in mm/dd/yyyy format) the contract ends in the corresponding field. You can also select the date by clicking 15.

8. Click the Group Assignment tab at the bottom of the UserDetails Page.

9. Assign the user to one or more groups. To assign a user to one or more groups, select the groups from the in the **Available Groups** list then click to assign the groups to the user. The assigned group displays in the **Member of** list. To remove the user from a group, select the group name in the **Member of** list then click . The group name moves back to the **Available Groups** list.

   A group in ONESOURCE Classic is similar to a profile in ONESOURCE Tax Information Reporting . Because you are a 1099 client, you will see the 1099 group. Adding a user to the 1099 group grants that user access to ONESOURCE Tax Information Reporting .

10. Click **Create** Create. A message displays, informing you that the user was successfully added to ONESOURCE Classic.

    After you create the user in ONESOURCE Classic and the user has access to ONESOURCE Tax Information Reporting , you will need to open the ONESOURCE Tax Information Reporting application to provision the user in ONESOURCE Tax Information Reporting .

11. Launch ONESOURCE Tax Information Reporting by clicking **Applications** on the ONESOURCE Classic menu then clicking **ONESOURCE Tax Information Reporting**.

12. Provision the new user in ONESOURCE Tax Information Reporting . New users will not be able to access ONESOURCE Tax Information Reporting until you complete this step. To provision a new user:

    a. Click the **Security** module.

    b. Answer the security questions.

c. Click the **New Users** section.

d. Select the user profile for the new user from the **Profile** drop-down list to assign a user profile and any user-specific privileges to each new user.

e. Click **Authorize**.

ONESOURCE CLASSIC SECURITY OPTIONS

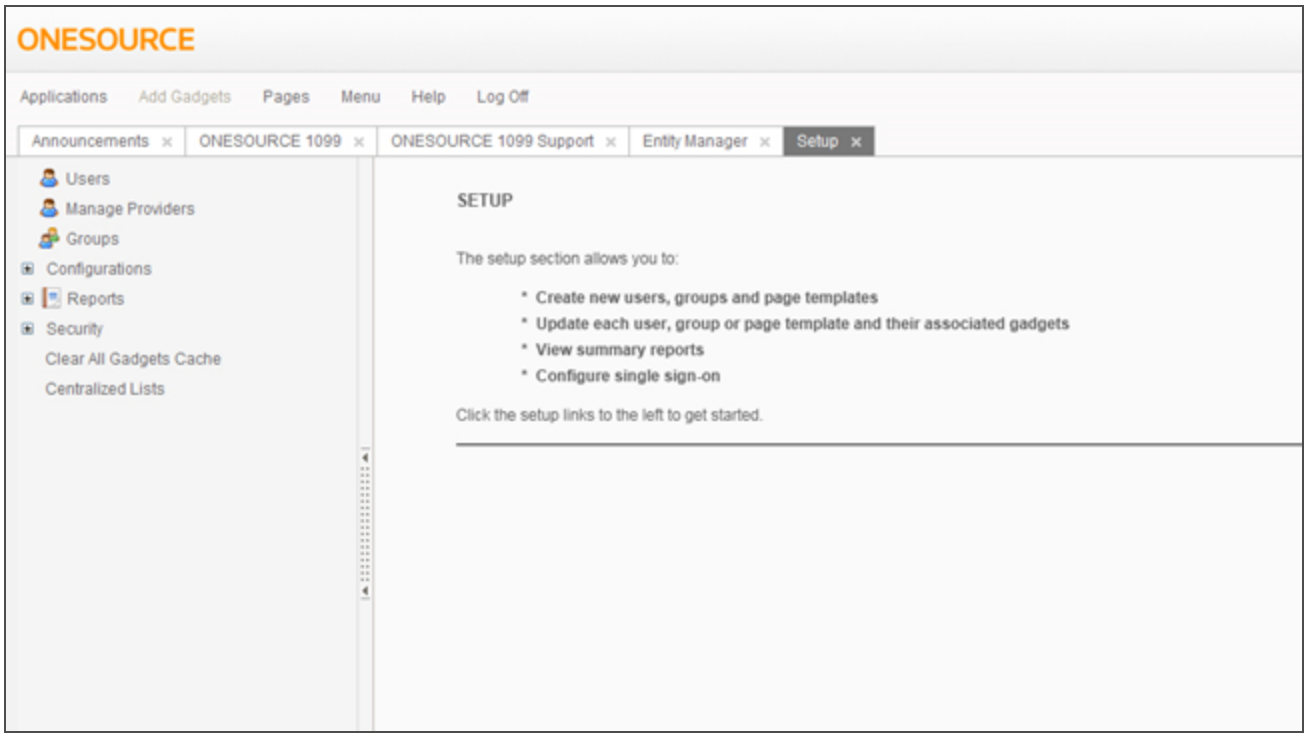
The security options for ONESOURCE Classic include password policies and security thresholds. Password policies are a group of restrictions for user passwords, which include password length, strength, age and re-use. You can use the default ONESOURCE Classic password policy or you can establish and maintain a password policy that is specific to your organization.

Security thresholds are additional security features for preventing unauthorized access. For example, as a system administrator, you can set the number of incorrect passwords users can enter before they are locked out of ONESOURCE Classic.

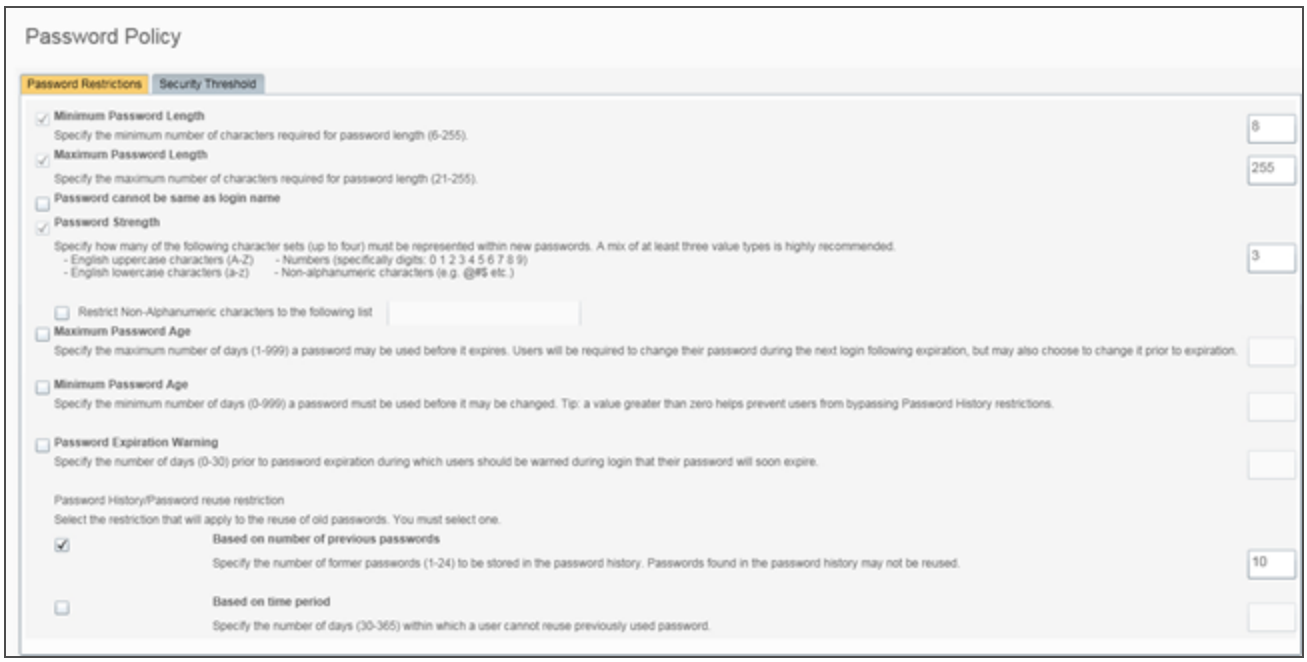
REVIEWING THE DEFAULT ONESOURCE CLASSIC PASSWORD POLICY AND ESTABLISHING YOUR PASSWORD POLICY

To review the default ONESOURCE Classic password policy and establish your password policy:

1. From the ONESOURCE Classic menu, click **Menu** then click **Setup**.



2. In the Navigation area, click **Security** then click **Password Policies**. The Password Policy page displays. The Password Restrictions tab is used to set restrictions for user passwords, including password length, strength, age and re-use.



3. On the Password Restrictions tab, review and, if necessary, set the following required fields:

   - **Minimum Password Length**-Passwords must contain between 6 and 255 characters. The default minimum length is 8 characters.
   - **Maximum Password Length**-Passwords cannot exceed 255 characters. The lowest maximum length is 21 characters.
   - **Password Strength**-Enter the number of character sets that must be used in passwords. At least three character sets are recommended. The character sets include:
     - English uppercase characters (A-Z)
     - English lowercase characters (a-z)
     - Numbers (0-9)
     - Special characters,such as @ # $ % ^ &

For example, if the **Password Strength** field is set to **3**, a valid password would be **Tuesday12** because the password contains an uppercase letter, lowercase letters and numbers.

- **Password History/Password reuse restriction**-Select the corresponding check box for storing old passwords. Old passwords can be stored in one of two ways:
  - **Based on number of previous passwords**-If you select this method and enter, for example, **10** in the corresponding field, then a password that matches one of the previous 10 passwords cannot be used.
  - **Based on time period**-If you select this method and enter, for example, **120** in the corresponding field, then a password that matches a password in the previous 120 days cannot be reused.

4. Review and, if necessary, change the following optional fields:

- **Password cannot be same as login name**-Select this check box to prevent the use of login names in passwords. For example, John Smith cannot use **JohnSmith1** as his password.
- **Restrict non-alphanumeric characters to the following list**-ONESOURCE Classic has no restrictions on non-alphanumeric characters. However, you can limit the characters users can choose from. For example, if this check box is selected and the non-alphanumeric characters are restricted to **$**, **#** and **?**, then a valid password would be Tuesday#12. An invalid password would be Tuesday@12.
- **Maximum Password Age**-Select this check box then enter the maximum number of days (1 to 999) a password can be in use before it expires. Users are required to change their passwords during the next login attempt following expiration. For example, entering **30** would require users to reset their ONESOURCE passwords every 30 days.
- **Minimum Password Age**-Select this check box then enter the minimum number of days (0 to 999) a password must be in use before it can be changed. For example, entering **7** requires the password to have existed for one week before it can be changed.

  Entering a value greater than zero prevents users from bypassing the **Password History/Password reuse restriction**. For example, if the **Based on number of previous passwords** method is set to **10**, then a user could change his or her password 10 times in one day to reinstate the current password. Setting the minimum age to one day requires that a password exist for 24 hours before it can be changed.

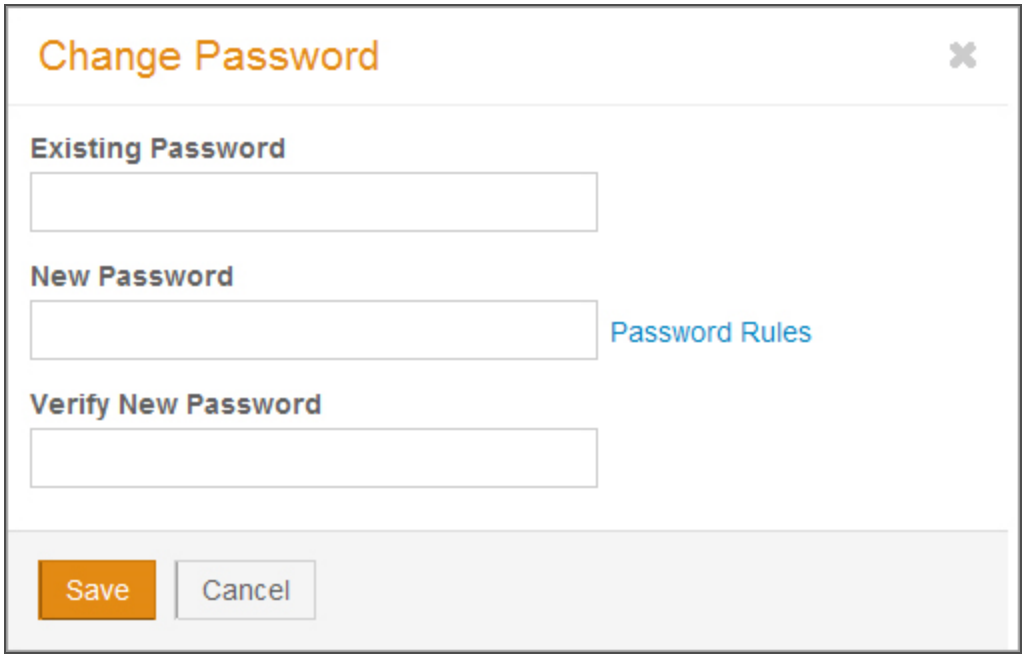
- **Password Expiration Warning**-If a user's password is about to expire, a warning is issued during login. You can specify the number of days (0 to 30) prior to password expiration that users will be warned. For example, entering **5** generates a password expiration warning each time the user logs in during the five days prior to the login expiration date.

5. Click **Save**. If you need to reset your password policy to the default values, click **Reset**.

REVIEWING YOUR PASSWORD RULES IN ONESOURCE CLASSIC

You can review your password rules by completing the following:

1. From the ONESOURCE Classic menu, click **Menu** then click **Options**.
2. Click the **Change Password** link under the **Security Information** heading.

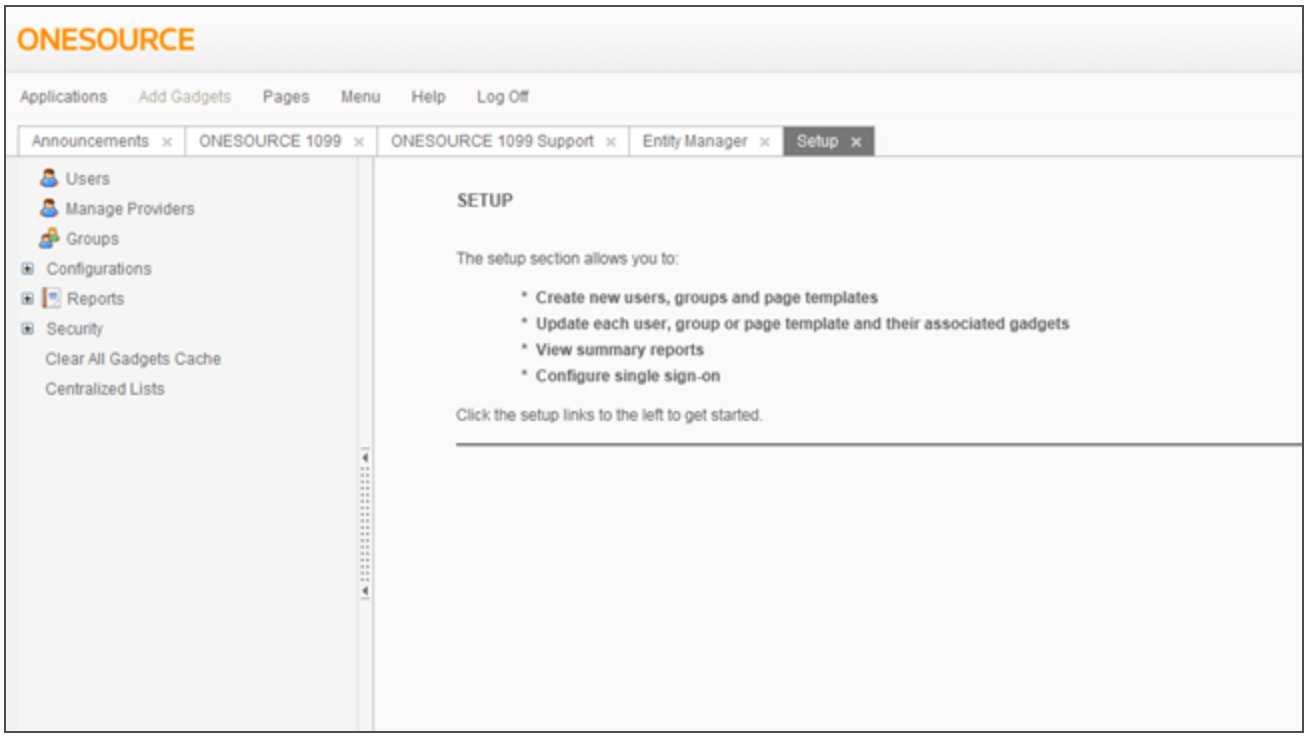


3. Click the **Password Rules** link. Your password rules display.
4. Click **Cancel** or close the Change Password page after you finish reviewing your password rules.

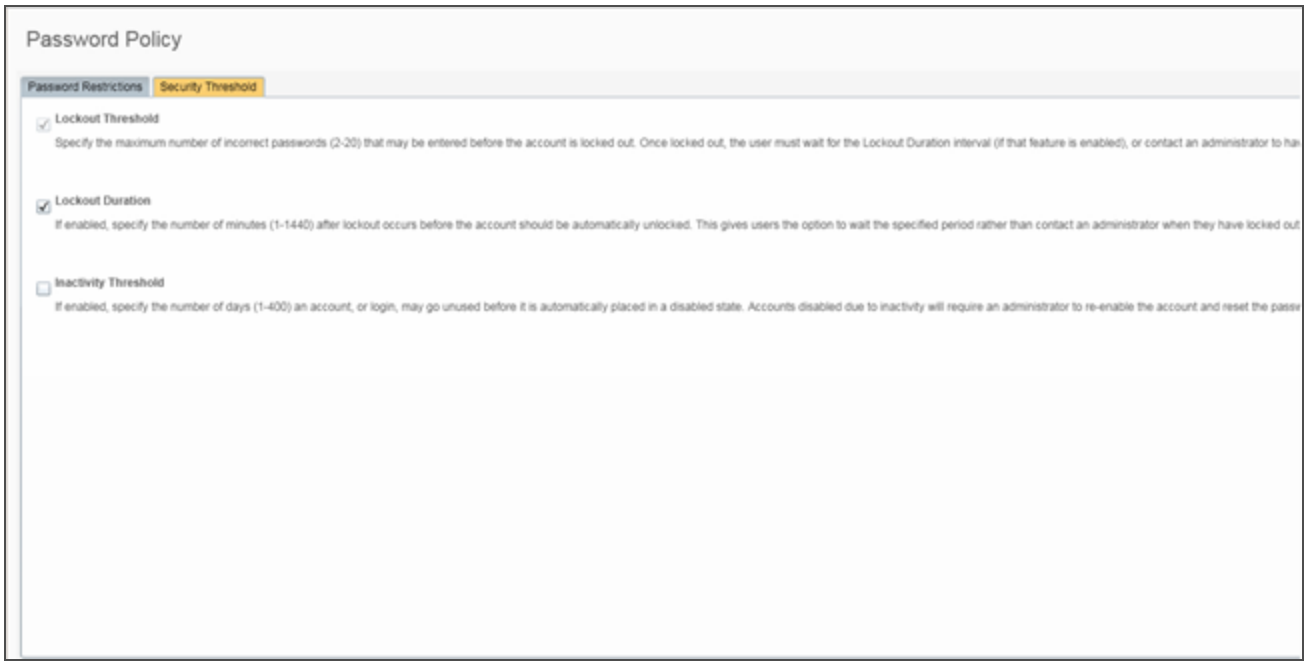
SETTING SECURITY THRESHOLDS

To set security thresholds:

1. From the ONESOURCE Classic menu, click **Menu** then click **Setup**.



2. In the Navigation area, click **Security** then click **Password Policies**.
3. Click the **Security Threshold** tab.



4. Set the **Lockout Threshold** field. This is a required field. Enter the maximum number of incorrect passwords (between 2 and 20) that users can enter before they are locked out. After a user is locked out, the user can:

   - Wait for the **Lockout Duration** interval, then try to login again. This option is available to users only if the **Lockout Duration** check box (see step 6 for details) is selected and a lockout interval is entered.
   - Click the **Forgot password?** link on the ONESOURCE Login screen to reset the password.
   - Contact a system administrator to have the account unlocked.

5. If you want, set the following optional fields:

   - **Lockout Duration**-Select this check box then enter the number of minutes (1 to 1440) that can elapse between when a user is locked out and when the user's password is automatically unlocked. This gives users the option to wait during the specified period rather than resetting their password or contacting a system administrator.
   - **Inactivity Threshold**-Select this check box then enter the number of days (1 to 400) that can elapse without the user logging in before he or she is locked out. A system administrator must re-enable the user and reset the password before the user can login again.

6. Click **Save**. If you need to reset your security thresholds to the system default values, click **Reset**.

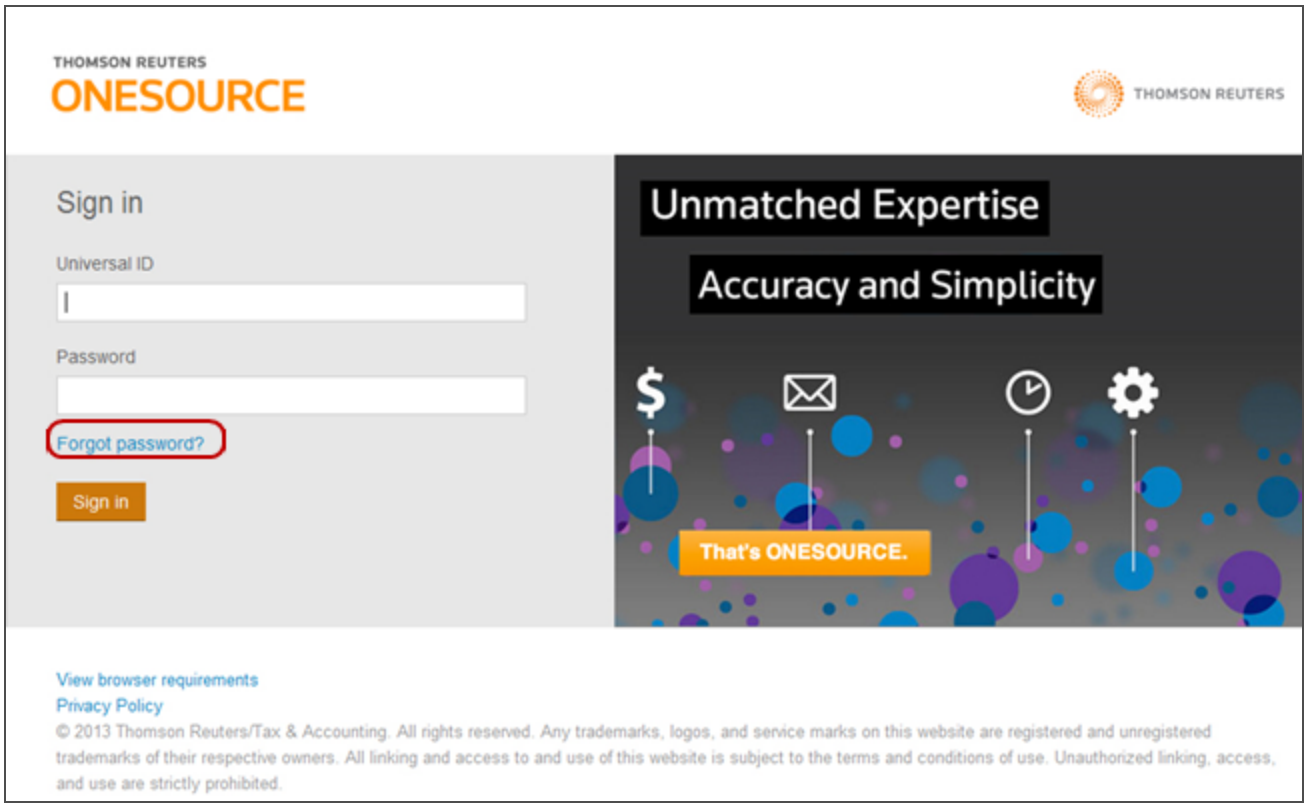
RESETTING ONESOURCE CLASSIC PASSWORDS

ONESOURCE Classic passwords can be reset from the ONESOURCE Classic Login page when a user or ONESOURCE Classic system administrator cannot remember his or her ONESOURCE Classic password, or when the lockout threshold was exceeded. A ONESOURCE Classic system administrator can use the Change Password page in ONESOURCE Classic to change his or her password even though the password is not forgotten.

RESETTING A PASSWORD FROM THE ONESOURCE CLASSIC LOGIN PAGE

To reset a password from the ONESOURCE Classic Login page:

1. Access ONESOURCE Classic at www.onesourcelogin.com.
2. Click the **Forgot password?** link.



A message displays, asking you to enter the email address of the user who needs his or her ONESOURCE Classic password reset.

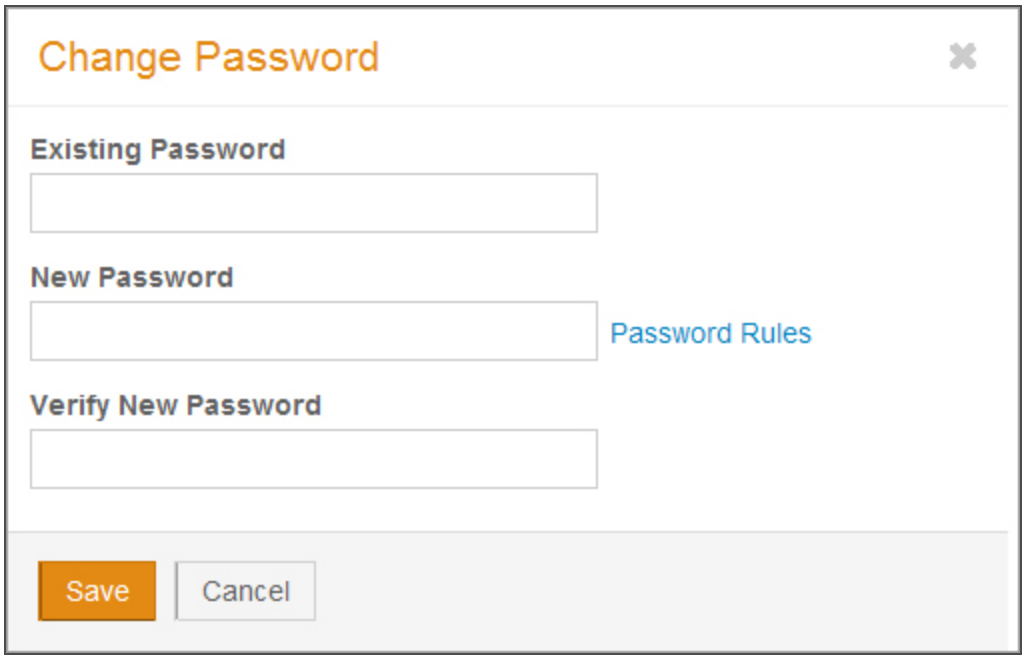
3. Enter the email address of the user who needs his or her ONESOURCE Classic password reset.
4. Click **Send**. Instructions for resetting the ONESOURCE Classic password are sent to the user's email address.

RESET PASSWORD FROM CHANGE PASSWORD PAGE

As a ONESOURCE Classic system administrator, you can use the Change Password page to change your password even though you have not forgotten your password.

To reset a password from the Change Password page:

1. From the ONESOURCE Classic menu, click **Menu** then click **Options**.
2. Click the **Change Password** link under the **Security Information** heading.



3. Enter your existing password in the **Existing Password** field.
4. Type the password you want to use in the **New Password** and **Verify new password** fields.
5. Click **Save**.